情報技術セキュリティ評価のための
コモンクライテリア

パート2： セキュリティ機能要件

1999年8月

バージョン2.1

CCIMB-99-032

平成13年1月翻訳第1.2版
情報処理振興事業協会
セキュリティセンター

IPAまえがき

本書の目的

本書は、情報技術セキュリティ評価のための評価基準であるコモンクライテリア(Common Criteria ： CC)バージョン2.1を日本語訳したものである。本書は、情報処理振興事業協会(略称IPA)におけるセキュリティ評価・認証プロジェクトの評価技術タスクフォース(略称CCTF)において、評価作業のための補助資料として作成されたものである。したがって、本翻訳書は、セキュリティ評価の規格書ではないが、情報セキュリティに関心をもつ人にとって、CCを理解するための参考資料として役立つことも期待している。

* CC Version 2.1は、情報セキュリティ技術のセキュリティ評価に関する統一基準であり、カナダ、フランス、ドイツ、オランダ、イギリス、アメリカ６カ国によるCCプロジェクトにより作成された。CC Version 2.1は、国際標準のISO/IEC 15408:1999と同等の評価基準書である。

使用上の注意

本書は、用語及び体裁の統一、記述内容などに不備がある可能性がある。疑問点についてはCC Version 2.1で確認していただきたい。本書は、参照利用されることのみを目的とし公開される。本書の改変、及び他への転載は禁止する。

参考文献

Common Criteria for Information Technology Security Evaluation

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

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

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

著作権について

本書がベースにしているCC Version2.1の著作権は、以下に示す７つの政府機関（“the Common Criteria Project Sponsoring Organizations”と総称）が有している。したがって、CC Version2.1の使用、複製、配布、及び改変の権利は、the Common Criteria Project Sponsoring Organizationsにある。情報処理振興事業協会は、CC Version2.1を日本語翻訳し、参照利用のみを目的として公開することを、the Common Criteria Project Sponsoring Organizationsより許可された。

The Common Criteria Project Sponsoring Organizations:

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

まえがき

情報技術セキュリティ評価のためのコモンクライテリア(CC 2.1)の本バージョンは、国際標準のISO/IEC 15408:1999に合わした改訂版である。さらに、本書は、その使用を促進するために、体裁が整えられている。本文書を使用して書かれたセキュリティ仕様書、及びその仕様書に従っていることを示したIT製品/システムは、ISO/IEC 15408:1999に従っているとみなされる。

CC 2.0は1998年5月に発刊された。続いて、相互承認協定は、調印に加わった組織によって実行された評価結果の相互承認の基礎として、CCを使用することが確立された。

ISO/IEC JTC 1は、1999年6月に、マイナーな、主に編集上の修正をしてCC 2.0を採用した。

CCバージョン2.1は、次のパートから構成される:

- パート1: 概説と一般モデル
- パート2: セキュリティ機能要件
- パート3: セキュリティ保証要件

次の法定通知は、要請により、CCのすべてのパートに記載してある。

以下に示す、またパート1附属書Aに完全に識別した、7つの政府組織(“the Common Criteria Project Sponsoring Organisations”と呼ばれる集団)は、情報技術セキュリティ評価ためのコモンクライテリア バージョン2.1のパート1から3(CC 2.1と呼ぶ)の著作権を共有したまま、ISO/IEC 15408国際標準の継続的な開発/維持の中で、CC 2.1を使用するためにISO/IECに対し、排他的でないライセンスを許可している。ただし、適切と思われる場合にCC 2.1を使用、複製、配布、翻訳及び改変する権利は、the Common Criteria Project Sponsoring Organisationsが保有する。

カナダ:	Communications Security Establishment
フランス:	Service Central de la Sécurité des Systèmes d’Information
ドイツ:	Bundesamt für Sicherheit in der Informationstechnik
オランダ:	Netherlands National Communications Security Agency
英国:	Communications-Electronics Security Group
米国:	National Institute of Standards and Technology
米国:	National Security Agency

目次

図リスト

1 範囲

このパート2に定義されているセキュリティ機能コンポーネントは、プロテクションプロファイル(PP)またはセキュリティターゲット(ST)に表されているTOE ITセキュリティ機能要件に対する基礎である。これらの要件は、評価対象(TOE)の予想される望ましいセキュリティのふるまいを記述し、PPまたはSTに記述されているセキュリティ対策方針を達成することを目的としている。これらの要件は、TOEとの直接の対話(つまり入力、出力)または刺激に対するTOEの応答によって利用者が検出できるセキュリティ特性を記述している。

セキュリティ機能コンポーネントは、TOEの想定される操作環境での脅威に対抗し、識別された組織のセキュリティ方針と前提条件を取り扱うことを目的とするセキュリティ要件を表す。
パート2の対象読者には、セキュアなITシステムと製品の消費者、開発者、評価者が含まれる。パート1 第3章は、CCの対象読者及び対象読者からなるグループによる標準の使用についての追加情報を提供している。これらのグループは、パート2を次のように使うことができる。

- 消費者は、PPまたはSTに記述されているセキュリティ対策方針を達成するための機能要件を表すコンポーネントを選択するときにパート2を使用する。パート1の4.3節は、セキュリティ大作方針とセキュリティ要件との間の関係についてさらに詳細な情報を提供している。
- 開発者は、TOEを構成するときに実際のまたは認識された消費者のセキュリティ要件に応じ、本パートのこれらの要件を理解するための標準的な方法を見出すことができる。また、開発者は、これらの要件を満たすTOEセキュリティ機能とメカニズムをさらに定義するための基礎として、本パートの内容を利用することができる。
- 評価者は、このパートに定義されている機能要件を使用して、PPまたはSTに記述されているTOE機能要件がITセキュリティ対策方針を達成していること、及びすべての依存性が考慮され、満たされていることを検証する。また、評価者は、このパートを使用して、特定のTOEが、記述されている要件を満たしているかどうかの判別を支援しなければならない。

1.1 機能要件の拡張と維持

CC及びここに記述されている関連するセキュリティ機能要件は、ITセキュリティのすべての問題に対する最終的な回答ではない。むしろ、この標準は、市場のニーズを反映した信頼製品またはシステムを作成するために使用できる一般に理解されているセキュリティ機能要件のセットを提供する。これらのセキュリティ機能要件は、要件の指定と評価の最新段階のものとして表される。

このパートには、必ずしもすべての可能なセキュリティ機能要件が含まれているわけではない。むしろ、公表時点でCCの作成者が価値を認識し、合意したセキュリティ機能要件が含まれている。

消費者の理解のしかたとニーズは変化するかもしれないので、CCのこのパートの機能要件は保守されていく必要があろう。PP/ST作成者によっては、CC パート2の機能要件コンポーネントが(まだ)カバーしていないセキュリティニーズを持っているかもしれないと思われる。そのような場合、PP/ST作成者は、パート1の附属書BとCに説明されるように、CCから取り出したものでない機能要件の使用を考慮することが許されている(拡張性と呼ばれる)。

1.2 パート2の構成

第1章はパート2の紹介である。
第2章はCC機能要件のカタログを紹介し、第3章から第13章までは機能クラスを記述している。
附属書Aは、機能コンポーネントの依存性の完全な相互参照表など、機能コンポーネントの潜在的な利用者に興味のある追加情報を提供している。
附属書Bから附属書Mまでは、機能クラスの適用上の注意事項を記述している。これらは、このパートの利用者に対する情報提供資料のリポジトリである。これらは、利用者が適切な操作を行い、適切な監査または文書情報を選択するのを支援する。
PPまたはSTの作成者は、適切な構造、規則、及びガイダンスとしてパート1を参照すべきである。

- パート1の第2章では、CCで使用される用語を定義している。
- パート1の附属書Bでは、PPの構造を定義している。
- パート1の附属書Cでは、STの構造を定義している。

1.3 機能要件のパラダイム

この節では、このパート2のセキュリティ機能要件で使われるパラダイムを記述している。図1.1と図1.2は、パラダイムの主要な概念のいくつかを表している。この節では、これらの図と、示されていない他の主要な概念を文書で説明している。記述されている主要な概念は、ボールド/イタリックで示されている。この節は、パート1の第2章のCC用語集に記述されているいかなる用語に対しても、それを代替したり置き換えることを意図するものではない。

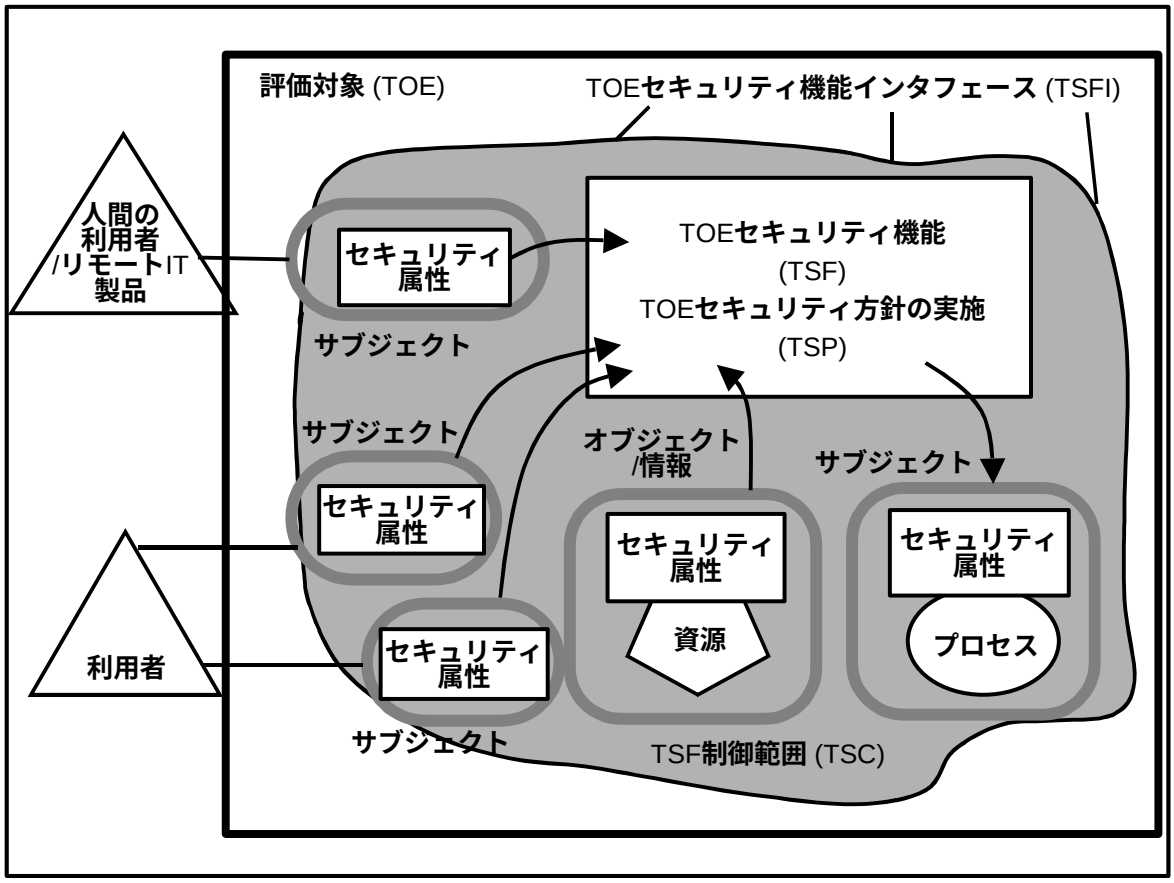


図1.1 - セキュリティ機能要件パラダイム(一体構造のTOE)

このパート2は、***評価対象(TOE)***に指定できるセキュリティ機能要件のカタログである。TOEは、(利用者及び管理者ガイダンス文書と共に)IT製品またはシステムであり、処理と情報の格納に使用でき、評価のサブジェクトとなる電子格納媒体(ディスクなど)、周辺装置(印刷装置など)、計算能力(CPU時間など)などの資源が含まれる。

TOE評価は、定義されている***TOEセキュリティ方針(TSP)***がTOE資源に対して実施されることを主な目的としている。TSPは、TOEが資源へのアクセス、その結果として、TOEが制御するすべての情報とサービスを管理する規則を定義している。

TSPは、複数の***セキュリティ機能方針(SFP)***で構成される。各SFPは、サブジェクト、オブジェクト、及びSFPのもとで制御される操作を定義する制御の有効範囲を持っている。

SFPは、メカニズムが方針を実施し、必要な能力を提供する***セキュリティ機能(SF)***によって実装される。

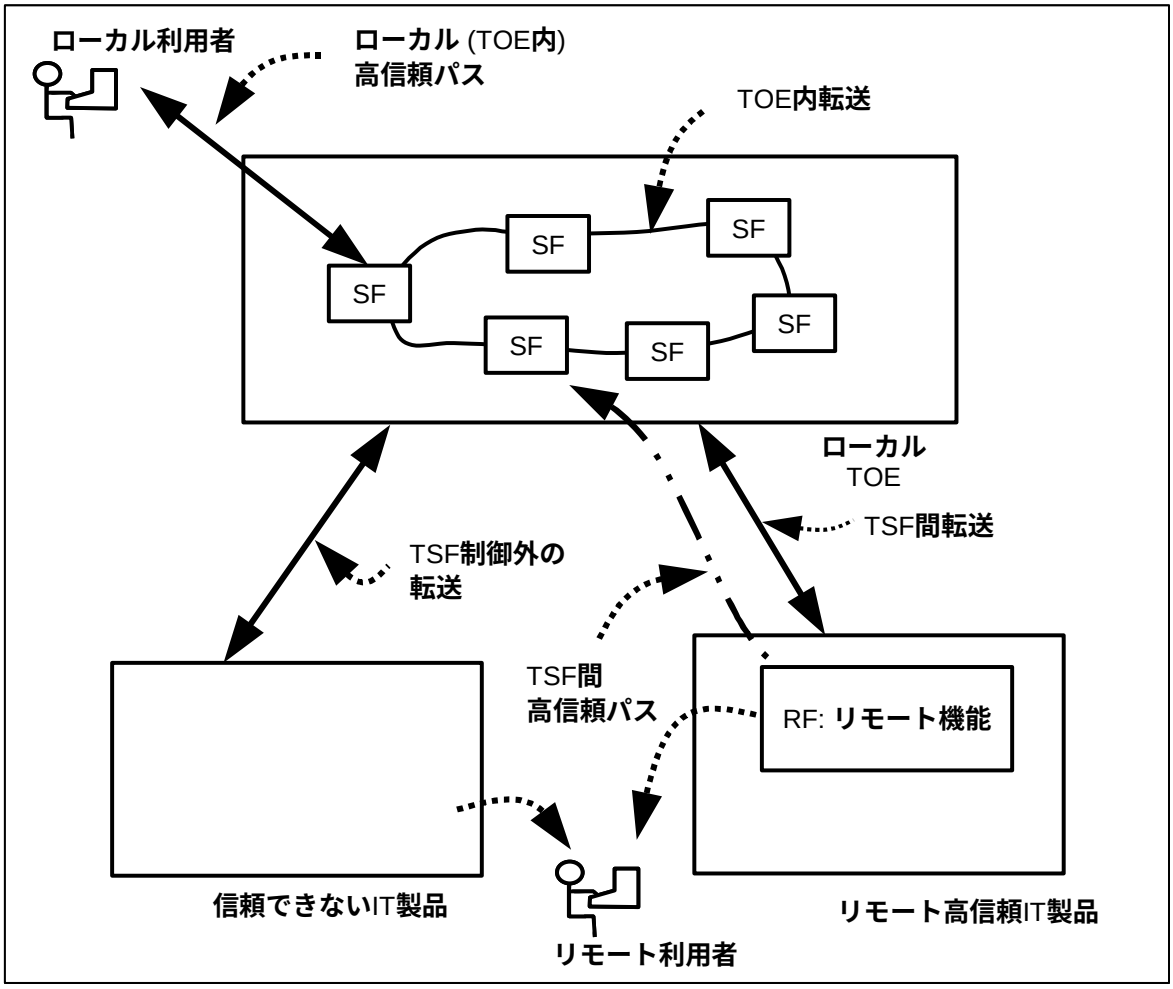


図1.2 - **分散**TOE**におけるセキュリティ機能の図**

TSPを正しく実施するために依存しなければならないようなTOEの部分は、総合して***TOEセキュリティ機能(TSF)***と呼ばれる。TSFは、セキュリティの実施に直接的または間接的に依存するTOEのすべてのハードウェア、ソフトウェア、及びファームウェアから構成される。

リファレンスモニタは、TOEのアクセス制御方針を実施する抽象マシンである。***リファレンス確認メカニズム***は、改ざんされず、いつでも呼び出せ、完全な分析とテストを受けられるよう十分に単純であるという特性を有するリファレンスモニタの概念の具現化例である。***TSF***は、リファレンス確認メカニズムやTOEの操作に必要なその他のセキュリティ機能からなる。

TOEは、ハードウェア、ファームウェア、及びソフトウェアが含まれている一体構造の製品の場合がある。

あるいは、TOEは、内部が複数の分離されたパートからなる分散製品の場合もある。

TOEのこれらのパートのそれぞれは、TOEの特定のサービスを提供し、***内部通信チャネル***を通してTOEの他のパートに接続される。このチャネルは、プロセッサバスのように小さいこともあれば、TOEの内部ネットワークを包含することもある。

TOEが複数のパートからなるとき、TOEの各パートはそれ自体のTSFのパートを持つことができ、それによって利用者及びTSFデータをTSFの他のパートと内部通信チャネルを通して交換することができる。この相互作用は、***TOE内転送***と呼ばれる。この場合、TSFのそれぞれのパートは、TSPを実施する複合TSFを抽象的に形成する。

TOEインタフェースは、特定のTOEにローカライズされるか、または***外部通信チャネル***を通して他のIT製品と相互作用を行うことができる。他のIT製品とのこれらの外部相互作用は、次の二つの形式をとることができる。

a) 「リモート高信頼IT製品」のセキュリティ方針とローカルTOEのTSPは、管理上、調整され、評価されている。この状態での情報の交換は、個々の高信頼製品のTSFの間で行われるため、***TSF間転送***と呼ばれる。

b) リモートIT製品は評価されていないかも知れず、図1.2に「信頼できないIT製品」として示されている。これは、そのセキュリティ方針が不明なためである。この状態での情報の交換は、リモートIT製品にTSFが存在しない(あるいはその方針の特性が不明である)ため、***TSF制御外への転送***と呼ばれる。

TOEに対してあるいはTOEの内部で発生し得るもので、TSPの規則についての主題となる相互作用のセットを、***TSF制御範囲(TSC)***と呼ぶ。TSCには、TOE内のサブジェクト、オブジェクト、及び操作に基づく定義された相互作用のセットが含まれるが、TOEのすべての資源が含まれる必要はない。

インタフェースのセットは、対話型(マンマシンインタフェース)であろうとプログラム型(アプリケーションプログラミングインタフェース)であろうと、それを通してTSFによって調停される資源がアクセスされるか、または情報がTSFから取得される場合には、***TSFインタフェース(TSFI)***と呼ばれる。TSFIでは、TSP実施の準備をするTOE機能の境界を定義する。

利用者はTOEの外側、したがって、TSCの外側に位置する。ただし、サービスがTOEによって行われることを要求するため、利用者はTSFIを通してTOEと対話を行う。パート2のセキュリティ機能要件に関係する利用者のタイプには、***人間の利用者***と***外部ITエンティティ***の2つがある。人間の利用者はさらに、TOE装置(ワークステーションなど)を通してTOEと直接対話を行う***ローカルの人間の利用者***と、別のIT製品を通してTOEと間接的に対話を行う***リモートの人間の利用者***に区別される。

利用者とTSF間の対話の期間は、利用者***セション***と呼ばれる。利用者セションの確立は、各種の考慮事項、例えば、利用者の認証、時刻、TOEにアクセスする方法、利用者ごとに許される同時セションの数などに基づいて制御できる。

CCの本パートでは、「***許可された(authorised)***」という用語を、操作を行うのに必要な権利や特権を有する利用者を表すために使用する。したがって、「***許可利用者***」という用語は、利用者がTSPによって定義されている操作を実行できることを示している。

管理者の義務の分離を求める要件を表すために、適切なパート2セキュリティ機能コンポーネント(ファミリFMT_SMRからの)は、管理的な***役割***が必要なことを明示的に述べている。役割とは、利用者とTOEとの間に許可された相互作用を確立する、事前に定義された規則のセットである。TOEは、いくつかの役割の定義をサポートする。例えば、TOEのセキュアな操作に関係する役割には、「監査管理者」と「利用者アカウント管理者」が含まれるかもしれない。

TOEには、情報の処理と格納に使用される資源が含まれる。TSFの主な目的は、TOEが制御する資源と情報に対してTSPを完全に正しく実施することである。

TOE資源は、多くの異なる方法で構成され、利用され得る。ただし、パート2では、望ましいセキュリティ特性の指定が可能なように特別な区別を行っている。資源から生成され得るすべてのエンティティは、二つの方向のいずれかに特徴付けられる。エンティティは、能動的であるかもしれず、これは、そのエンティティが、TOEの内部で生じるアクションの原因であり、情報に対して実施される操作を引き起こすことを意味する。さもなければ、エンティティは、受動的であるかもしれず、これは、エンティティが、情報の発生源か情報の格納先となるコンテナであることを意味する。

能動的なエンティティは***サブジェクト***と呼ばれる。TOEには、次に示すようないくつかのタイプのサブジェクトが存在する可能性がある。

a) 許可利用者を代行して働く、TSPのすべての規則に従うサブジェクト(例えば、UNIXプロセス)

b) 複数の利用者を代行してアクションを行う、特定の機能プロセスの働きをするサブジェクト(例えば、クライアント/サーバアーキテクチャに見られる機能)

c) TOE自体の一部として働くサブジェクト(例えば、高信頼プロセス)

パート2は、上記のタイプのサブジェクト上でのTSPの実施について記述する。

受動エンティティ(例えば、情報コンテナ)は、パート2セキュリティ機能要件では***オブジェクト***と呼ばれる。オブジェクトは、サブジェクトが実行する操作の対象である。サブジェクト(能動エンティティ)が操作(例えば、プロセス間通信)の対象である場合、サブジェクトは、オブジェクトの働きもする。

オブジェクトは、***情報***を含むことができる。この概念は、FDPクラスで記述されている情報フロー制御方針を指定するために必要となる。

利用者、サブジェクト、情報及びオブシェクトは、TOEが正しくふるまうことができるようにする情報が含まれるある種の***属性***を所有する。ファイル名などのいくつかの属性は、

情報(TOEを利用者が簡単に使用できるようにする)を提供することを意図しているが、アクセス制御情報など、その他の属性は、特にTSPを実施するために存在する。これら後者の属性は、一般的に「***セキュリティ属性***」と呼ばれる。「属性」という用語は、このパートでは、特に断らない限り、「セキュリティ属性」の用語に代わる簡略表記として使用される。ただし、属性情報の意図する目的には関係なく、TSPの指示に従って、属性を制御する必要がある。

TOEのデータは、利用者データまたはTSFデータのいずれかに分類される。図1.3は、この関係を示している。***利用者データ***は、TSPに従って利用者が操作し、TSFに特別の意味を持たないTOE資源に格納される情報である。例えば、電子メールメッセージの内容は、利用者データである。***TSFデータ***は、TSPの決定を行うときにTSFが使用する情報である。TSFデータは、TSPが許している場合は、利用者の影響を受けることがある。セキュリティ属性、認証データ及びアクセス制御リストエントリは、TSFデータの例である。

アクセス制御SFPや***情報フロー制御SFP***など、データ保護に適用されるいくつかのSFPが存在する。アクセス制御SFPを実装するメカニズムは、制御の範囲内のサブジェクト、オブジェクト及び操作の属性に基づいて方針決定を行う。これらの属性は、サブジェクトがオブジェクトに対して実行することができる操作を制御する規則のセットで使用される。

情報フロー制御SFPを実装するメカニズムは、制御の範囲内のサブジェクトと情報の属性、及び情報に対するサブジェクトの操作を制御する規則のセットに基づいて方針の決定を行う。情報の属性は情報が移動するときも一緒であり、その属性はコンテナの属性と関係付けられるかもしれない(あるいは、マルチレベルデータベースの場合のように関係付けられないかもしれない)。

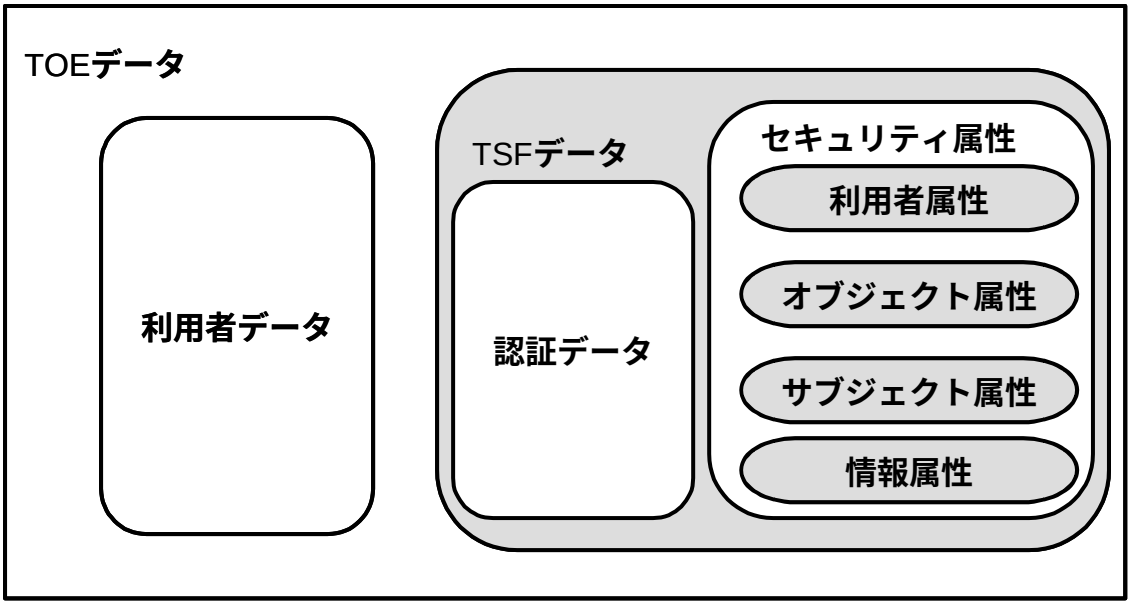


図1.3 - 利用者データとTSFデータとの関係

パート2が記述する二つの特定のタイプのTSFデータは、同じである可能性があるが、必

ずしも同じである必要はない。これらのタイプは、***認証データ***と***秘密(secrets)***である。

認証データは、TOEにサービスを要求する利用者が主張する識別情報を検証するために使用される。認証データの最も一般的な形式はパスワードであり、パスワードを効果的なセキュリティメカニズムとするためには、秘密に保持する必要がある。ただし、認証データのすべての形式を秘密に保持する必要はない。生体認証装置(例えば、指紋読取装置、網膜スキャナ)の場合は、必ずしもデータを秘密に保持する必要はない。むしろ、そのようなデータは、ただ一人の利用者が保持し、偽造できないものである。

CC機能要件で使用される「秘密」という用語は認証データに適用できるが、特定のSFPを実施するために秘密に保持しなければならない他のタイプのデータにも適用される。例えば、チャネルを通して送信される情報の秘密を保持するために暗号に依存する高信頼チャネルメカニズムは、許可されない開示から暗号鍵を秘密に保持する方式が使用される場合に限り、力を発揮する。

そこで、すべてではないがいくつかの認証データは秘密に保持する必要があり、すべてではないがいくつかの秘密は認証データとして使用される。図1.4は、秘密と認証データとの関係を示している。図には、認証データ及び秘密セクションにおいて典型的に見られるデータの種別が示されている。

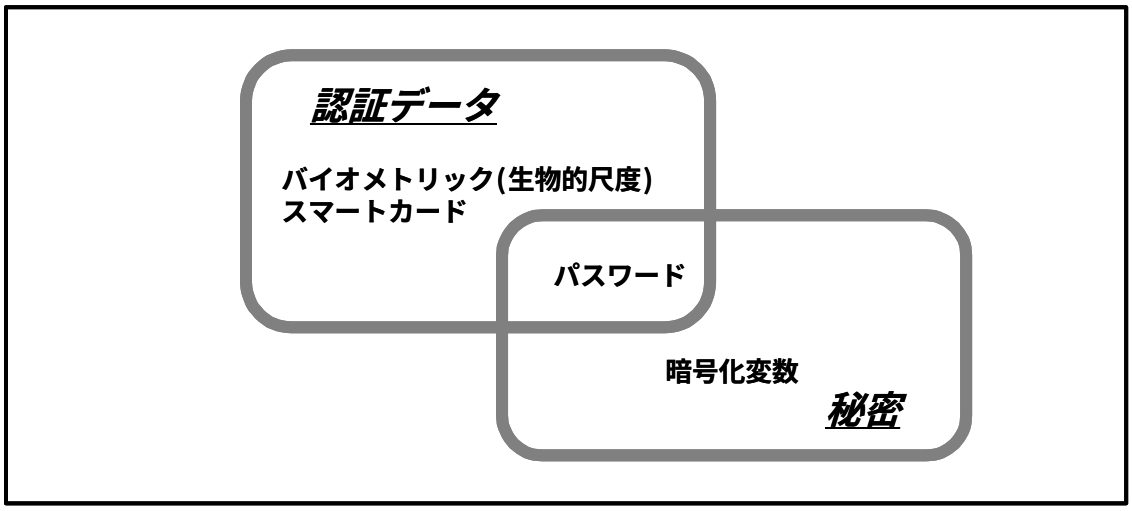


図1.4 - 「認証データ」と「秘密」との関係

2 セキュリティ機能コンポーネント

2.1 概要

この節では、CCの機能要件の内容と表現を定義し、STに含める新しいコンポーネントの要件の構成に関するガイダンスを提供する。機能要件は、クラス、ファミリ、及びコンポーネントで表される。

2.1.1 クラス構造

図2.1は、図の形式で機能クラス構造を示している。各機能クラスには、クラス名、クラスの序説、一つ以上の機能ファミリが含まれる。

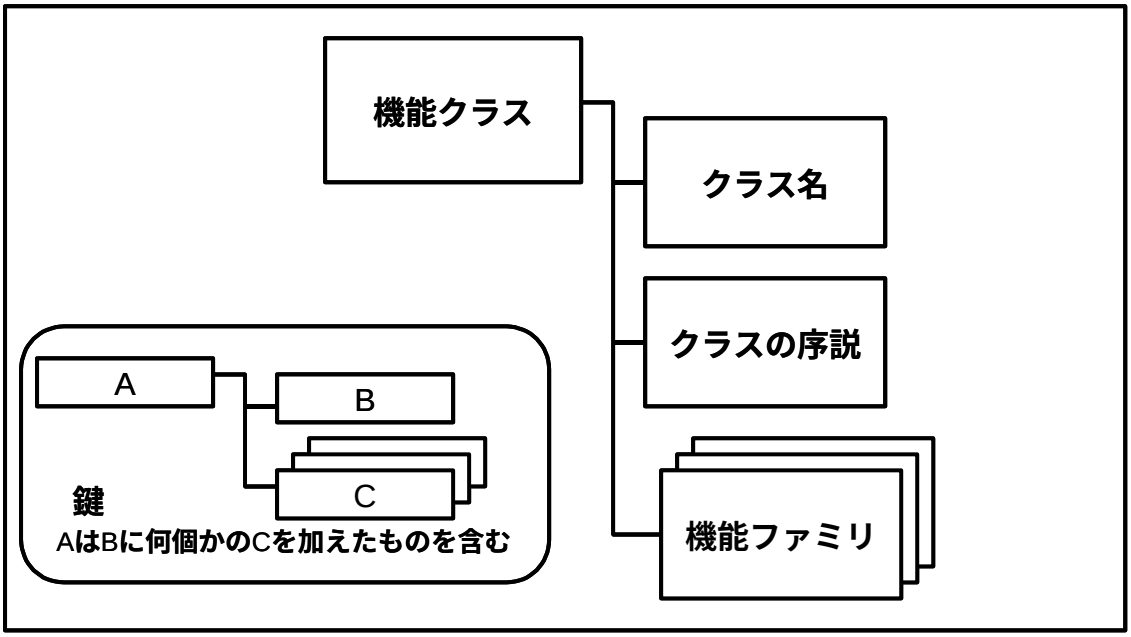


図2.1 - 機能クラス構造

2.1.1.1 クラス名

クラス名の節は、機能クラスを識別し分類するのに必要な情報を提供する。各機能クラスは一意の名前を持つ。分類情報は3文字の短い名前からなる。クラスのこの短い名前は、そのクラスのファミリの短い名前を指定するときに使用される。

2.1.1.2 クラスの序説

クラスの序説は、セキュリティ対策方針を達成するためのこれらのファミリの共通の意図または方法を表す。機能クラスの定義では、要件の指定における形式的な分類方法は反映されない。

クラスの序説には、2.2に説明するように、このクラスのファミリと各ファミリのコンポーネントの階層を記述した図が用意されている。

2.1.2 ファミリ構造

図2.2は、機能ファミリ構造を図の形式で示したものである。

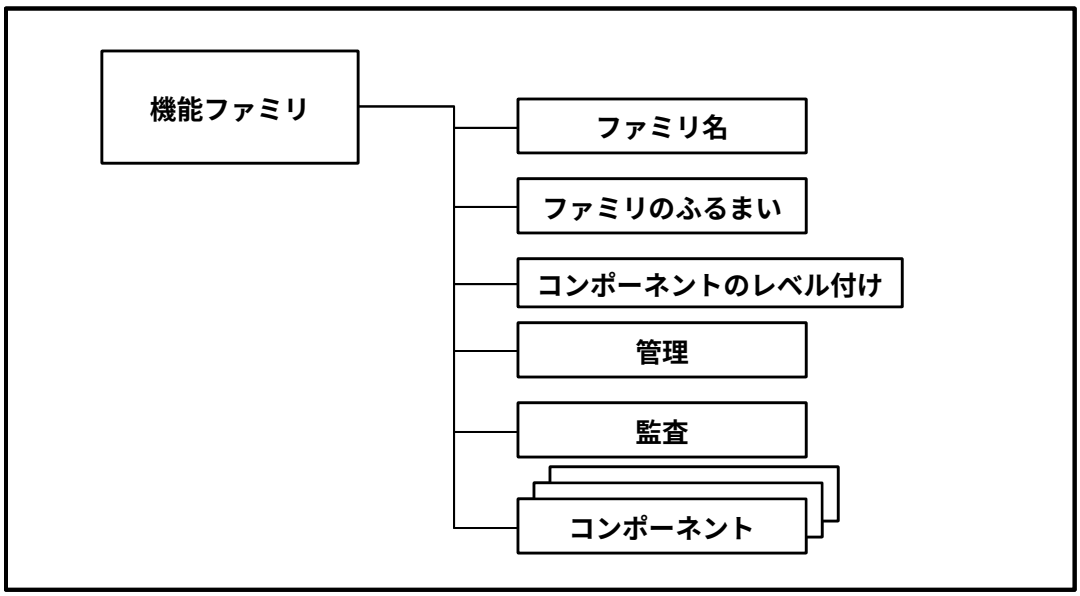


図2.2 - **機能ファミリ構造**

2.1.2.1 ファミリ名

ファミリ名の節は、機能ファミリを識別し分類するのに必要な分類情報と記述情報を提供する。各機能名は一意の名前を持つ。分類情報は7文字の短い名前から構成されており、その最初の3文字はクラスの短い名前と同じもので、その後に下線文字とファミリの短い名前が続き、XXX_YYYのような形式になる。ファミリ名の一意の短い形式は、コンポーネントの主な参照名を提供する。

2.1.2.2 ファミリのふるまい

ファミリのふるまいは、機能ファミリについての叙述的記述であり、そのファミリのセキュリティ対策方針と、機能要件の概括的記述を述べたものである。これらについて以下にさらに詳細に記述する。

a) ファミリの*セキュリティ対策方針*は、このファミリのコンポーネントを組み込んだTOEの助けを借りて解決されるかもしれないセキュリティ問題に対応する。

b) *機能要件*の記述では、コンポーネントに含まれるすべての要件を要約する。この記述は、ファミリが特定の要件に適しているかどうかを評価するPP、ST及び機能パッケージの作成者に向けられたものである。

2.1.2.3 コンポーネントのレベル付け

機能ファミリには、一つ以上のコンポーネントが含まれる。それらはいずれも、選択してPP、ST及び機能パッケージに含めることができる。このセクションの目的は、ファミリがセキュリティ要件の必要な、あるいは有効なパートであると識別された後で、適切な機能コンポーネントを選択するための情報を利用者に提供することである。

機能ファミリを記述するこのセクションでは、使用可能なコンポーネントとこれらの論理的根拠を記述している。コンポーネントの詳細は、各コンポーネントの中に含まれる。

機能ファミリ内でのコンポーネント間の関係は、階層関係になっていることもあり、なっていないこともある。もしあるコンポーネントが別のコンポーネントよりも高度のセキュリティを提供していれば、前者は後者のコンポーネントの上位階層となる。

2.2で説明するように、ファミリの記述ではファミリ内におけるコンポーネントの階層の概要が図で示される。

2.1.2.4 管理

*管理*要件には、PP/ST作成者が特定のコンポーネントに対する管理アクティビティとみなす情報が含まれている。管理要件は、管理クラス(FMT)のコンポーネントに詳細に記述されている。
PP/ST作成者は、示された管理要件を選んでもよく、リストされていない他の管理要件を含めてもよい。なぜならば、この情報は参考情報(informative)と考えられるべきものだからである。

2.1.2.5 監査

*監査*要件には、FAUクラス、セキュリティ監査からの要件がPP/STに含まれる場合、PP/ST作成者が選択する監査対象事象が含まれる。これらの要件には、FAU_GEN セキュリティ監査データ生成ファミリのコンポーネントがサポートする各種レベルの詳細としてセキュリティに関する事象が含まれる。例えば、監査注釈には、以下のアクションが含まれる。「最小」- セキュリティメカニズムの成功した使用、「基本」- セキュリティメカニズムのあらゆる使用 (用いられるセキュリティ属性に関する情報は言うまでもなく) 、「詳細」- 変更の前と後の実際の設定値を含む、メカニズムに対して行われたあらゆる設定変更。

監査対象事象の分類は、階層的であることに注意しなければならない。例えば、基本監査生成が必要な場合、「最小」と「基本」の両方に識別されたすべての監査対象事象は、上位レベルの事象が下位レベルの事象よりもさらに詳細を提供する場合を除き、適切な割当て操作を使用してPP/STに含めるべきである。詳細監査生成が必要な場合は、すべての識別された監査対象事象(「最小」、「基本」及び「詳細」)をPP/STに含めるべきである。
FAUクラスでは、監査に関する規則がさらに詳細に説明されている。

2.1.3 コンポーネント構造

図2.3は、機能コンポーネント構造を示している。

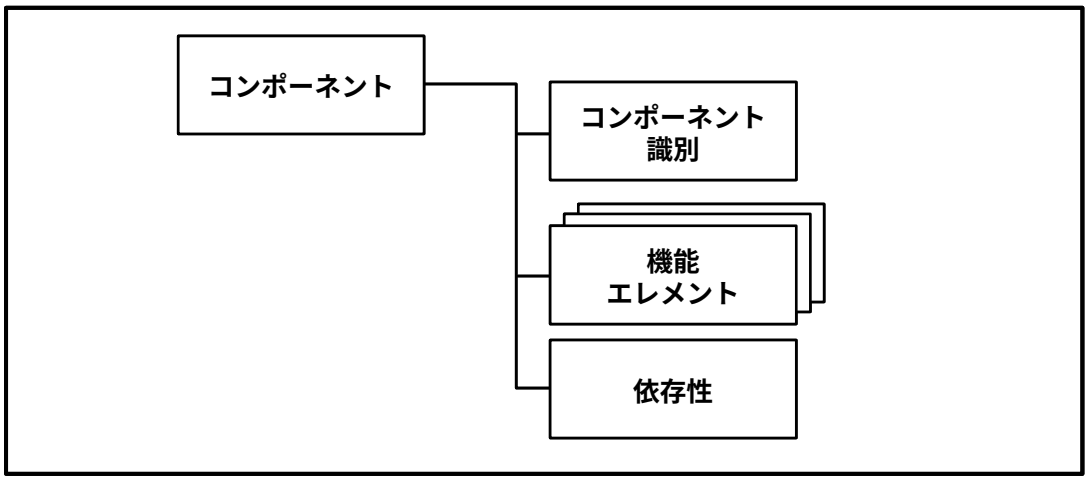


図2.3 - **機能コンポーネント構造**

2.1.3.1 コンポーネントの識別

コンポーネントの識別の節は、コンポーネントを識別、分類、登録及び相互参照するのに必要な記述情報を提供する。以下のものが各機能コンポーネントの一部として提供される。

一意の名前。コンポーネントの目的を表す名前。

短い名前。機能コンポーネント名の一意の短い形式。この短い名前は、コンポーネントの分類、登録及び相互参照のための主な参照名として使用される。この短い名前は、コンポーネントが属するクラスとファミリ及びファミリ内のコンポーネントの数を表す。

*下位階層*リスト。このコンポーネントがそれに対して上位階層にあり、リストに示されたコンポーネントに対する依存性を満たすためにこのコンポーネントを使用できる、他のコンポーネントのリスト。

2.1.3.2 機能エレメント

エレメントのセットが各コンポーネントに提供される。各エレメントは、個別に定義され、自己完結する。
機能エレメントは、それ以上分割しても意味ある評価結果が得られないセキュリティ機能要件である。CCで識別され、認識されている最小のセキュリティ機能要件である。

パッケージやPP、STを作成するとき、コンポーネントから一つだけまたは数個のエレメントだけを選択することは許されない。コンポーネントのエレメントの完全なセットを選択して、PP、STまたはパッケージに含めなければならない。

機能エレメント名の一意の短い形式が提供される。例えば、要件名FDP_IFF.4.2は、F - 機能要件、DP - クラス「利用者データ保護」、_IFF - ファミリ「情報フロー制御機能」、.4 - 4番目のコンポーネントで名前は「不正情報フローの部分的排除」、.2 - コンポーネントの2番目のエレメントを意味する。

2.1.3.3 依存性

機能コンポーネント間の依存性は、コンポーネントが自己完結型でなく、適切に機能するために他のコンポーネントの機能または他のコンポーネントとの相互作用に依存するときに生じる。

各機能コンポーネントは、他の機能コンポーネント及び保証コンポーネントへの依存の完全なリストを提供する。あるコンポーネントは、「依存性: なし」と表示する。依存されたコンポーネントは、次々に他のコンポーネントに依存することができる。コンポーネントに提供されるリストは、直接依存するコンポーネントである。それは、この要件がジョブを適切に実行するのに必要となる機能要件への単なる参照である。間接に依存するコンポーネント、つまり、依存されたコンポーネントの結果として依存するコンポーネントは、パート2の附属書Aに示されている。ある場合には、提示されたいくつかの機能要件の中から、依存するコンポーネントを任意選択するようになる。この場合、それぞれの機能要件が、依存性を満たすのに十分である(例えば、FDP_UIT.1を参照)。

依存性リストは、識別されたコンポーネントに関係するセキュリテイ要件を満たすのに必要な最小の機能コンポーネントまたは保証コンポーネントを識別する。識別されたコンポーネントの上位階層のコンポーネントも、依存性を満たすために使用することができる。

パート2に示されている依存性は標準的なものである。それらは、PP/STの中で満たされなければならない。特別の状況では、示された依存性が適用できない場合がある。PP/ST作成者は、それが適用されない根拠を示すことにより、依存されるコンポーネントを機能パッケージ、PPまたはSTから除外することができる。

2.1.4 許可された機能コンポーネント操作

PP、STまたは機能パッケージで要件の定義に使用する機能コンポーネントは、このパートの第3章から第13章に指定されているものとまったく同じとすることも、あるいは特定のセキュリティ対策方針に合わせて修整することもできる。ただし、これらの機能コンポーネントの選択と修整は、識別されたコンポーネントの依存性を考慮しなければならないため複雑なものになる。そこで、この修整は、承認された操作のセットだけに限定される。

許可された操作のリストは、各機能コンポーネントに含まれる。必ずしもすべての操作がすべての機能コンポーネントに許されるとは限らない。

許可された操作は、次のセットから選択される。

- 繰返し: コンポーネントを各種の操作で一度以上使用することが可能
- 割付: 識別されたパラメタの指定が可能
- 選択: リストからの一つ以上のエレメントの指定が可能
- 詳細化: 詳細の追加が可能

2.1.4.1 繰返し

同じ要件の異なる面(例えば、複数の利用者タイプの識別)を取り扱う必要がある場合、

各々の面を取り扱うためにパート2からの同じコンポーネントの繰返し使用が許される。

2.1.4.2 割付

ある機能コンポーネントのエレメントにはパラメタまたは変数が含まれており、PP/ST作成者は特定のセキュリティ対策方針を達成するためにPPまたはSTに組み入れる方針または値のセットを指定することができる。これらのエレメントは、各パラメタ及びそのパラメタに割り付けることができる値の制約を明確に識別する。

受け入れ可能な値が明確に記述または列挙されるエレメントの面は、いずれもパラメタで表すことができる。パラメタは、要件を特定の値または値の範囲に限定する属性または規則である。例えば、指定されたセキュリティ対策方針に基づいて、機能コンポーネントのエレメントは、特定の操作を数回実行すべきことを示すことができる。この場合、割付は、パラメタに使用する数字または数字の範囲を提供する。

2.1.4.3 選択

これは、コンポーネントのエレメントの範囲を限定するために、リストから一つ以上の項目を指定する操作である。

2.1.4.4 詳細化

すべての機能コンポーネントのエレメントに対して、PP/ST作成者は、セキュリティ対策方針を達成するために、追加の詳細を指定することにより受け入れ可能な実装のセットを制限することができる。エレメントの詳細化は、これらの技術的な詳細を追加することである。

STの中では、サブジェクトとオブジェクトという用語の意味を説明することにより、TOEを意味あるものにする必要がある。そのため、詳細化が行われる。

他の操作と同様、詳細化が全く新しい要件を課すことはない。セキュリティ対策方針に基づいて、要件、規則、定数または条件に対して詳述、解釈、または特別の意味を適用する。詳細化は、要件を実装するために考えられる受け入れ可能な機能またはメカニズムのセットをさらに限定するだけであり、それを増加させるようなことは全くない。詳細化では新しい要件を作成することは認めないため、コンポーネントに関係する依存性のリストが増加することはない。PP/ST作成者は、この要件に依存する他の要件の依存性の必要性が満たされるように注意しなければならない。

2.2 コンポーネントカタログ

この節のコンポーネントのグループ化は、何らかの正式な分類学を反映したものではない。パート2には、ファミリとコンポーネントのクラスが含まれる。それらは、関連する機能または目的に基づいておおまかにグループ化され、アルファベット順に示される。各クラスの始めには各クラスの分類を示す説明図が付いており、それには各クラスのファミリと各ファミリのコンポーネントが示される。図は、コンポーネント間に存在する階層関係を見るのに便利である。

機能コンポーネントの記述において、一つの節は、コンポーネントと他のコンポーネント間の依存性を識別する。

各クラスには、図2.4と同様のファミリの階層を記述した図が提供される。図2.4では、最初のファミリであるファミリ1に3つの階層コンポーネントが含まれており、この場合コンポーネント2とコンポーネント3はいずれもコンポーネント1に対する依存性を満たすものとして使用できる。また、コンポーネント3は、コンポーネント2の上位階層関係にあり、同様にコンポーネント2に対する依存性を満たすものとして使用できる。

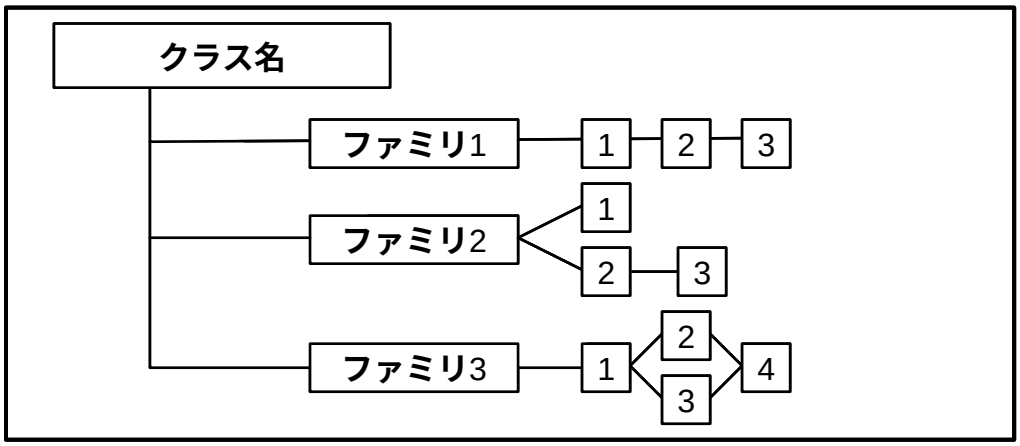


図2.4 - **サンプルクラスのコンポーネント構成図**

ファミリ2には3つのコンポーネントが存在するが、それらすべてが階層関係にあるわけではない。コンポーネント1と2は、他のコンポーネントの上位階層関係にはない。コンポーネント3は、コンポーネント2の上位階層関係にあり、コンポーネント2への依存性を満たすものとして使用されるが、コンポーネント1の依存性を満たすものとしては使用されない。

ファミリ3では、コンポーネント2、3、及び4がコンポーネント1の上位階層関係にある。コンポーネント2と3はいずれもコンポーネント1の上位階層関係にあるが、同等のものではない。コンポーネント4は、コンポーネント2とコンポーネント3の両方に対して上位階層関係にある。

これらの図は、ファミリの文章を補足し、関係の識別を容易にするためのものである。それらは、各コンポーネントにおける階層関係の必須の要求事項である各コンポーネントの

「依存性」の注釈に置き換わるものではない。

2.2.1 コンポーネント変更の強調表示

ファミリ内のコンポーネント間の関係は、**ボールド**表記を用いて強調表示される。このボールド表記では、すべての新しい要件をボールドで表示する必要がある。階層型のコンポーネントでは、前のコンポーネントの要件を超えて強化または変更されたとき、要件及び/または依存性がボールドで表示される。加えて、前のコンポーネントを超えて、新しい、あるいは強化された脅威、適用上の注釈、及び/または許可された操作もまた、**ボールド**タイプを用いて強調表示される。

3 クラスFAU: セキュリティ監査

セキュリティ監査は、セキュリティ関連のアクティビティ(例えば、TSPによって制御できる事象)に関連する情報の認識、記録、格納、分析を含む。監査結果記録は、どのようなセキュリティ関連のアクティビティが実施されているか、及び誰が(どの利用者が)そのアクティビティに責任があるかを限定するために検査され得るものである。

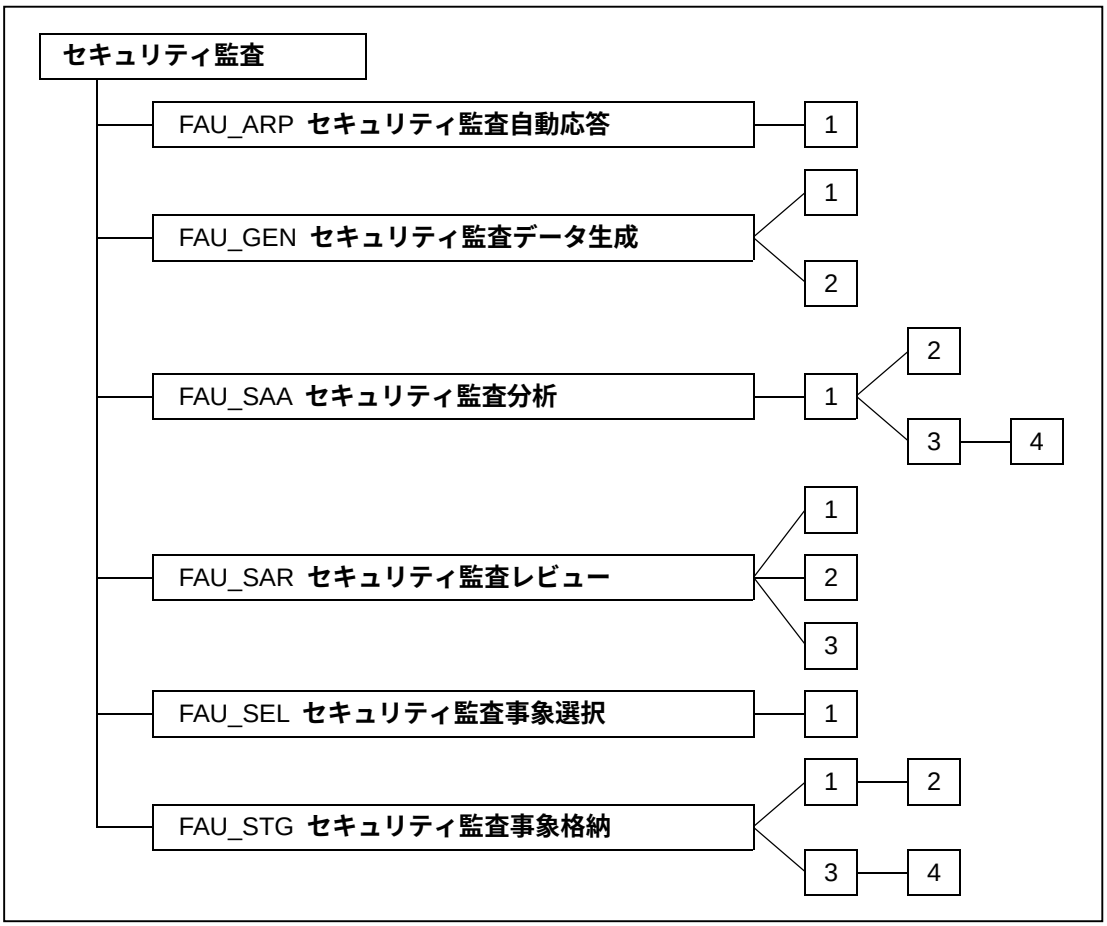


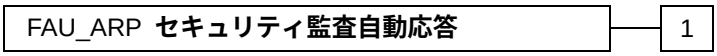
図3.1 - **セキュリティ監査クラスのコンポーネント構成**

3.1 セキュリティ監査自動応答(FAU_ARP)

ファミリのふるまい

このファミリでは、セキュリティ侵害の可能性が検出された場合、自動的に応答するようなTSFにおける要件を定義している。

コンポーネントのレベル付け



FAU_ARP.1 セキュリティアラームでは、TSFは、セキュリティ侵害の可能性が検出された場合にアクションをとらなければならない。

管理: FAU_ARP.1

以下のアクションはFMTの管理機能と考えられる:

a) アクションの管理(追加、除去、改変)。

監査: FAU_ARP.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 切迫したセキュリティ侵害によってとられるアクション。

FAU_ARP.1 セキュリティアラーム

下位階層: なし

FAU_ARP.1.1 **TSFは、セキュリティ侵害の可能性が検出された場合、[割付: 混乱を最小にする*アクションのリスト*]を実行しなければならない。**

依存性: **FAU_SAA.1 侵害の可能性の分析**

3.2 セキュリティ監査データ生成(FAU_GEN)

ファミリのふるまい

このファミリでは、TSFの制御下で発生するセキュリティ関連事象を記録するための要件を定義している。このファミリは、監査レベルを識別し、TSFによる監査対象としなければならない事象の種別を列挙し、さまざまな監査記録種別の中で規定されるべき監査関連情報の最小セットを識別する。

コンポーネントのレベル付け

FAU_GEN.1 監査データ生成は、監査対象事象のレベルを定義し、各記録ごとに記録されねばならないデータのリストを規定する。

FAU_GEN.2 利用者識別情報の関連付けでは、TSFは、監査対象事象を個々の利用者識別情報に関連付けなければならない。

管理: FAU_GEN.1、FAU_GEN.2
予見される管理アクティビティはない。

監査: FAU_GEN.1、FAU_GEN.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象とすべき識別されたアクションはない。

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) **監査機能の起動と終了;**
b) **監査の[選択:** ***最小、基本、詳細、指定なし*****]レベルのすべての監査対象事象; 及び**
c) **[割付:** ***上記以外の個別に定義した監査対象事象*****]。**

FAU_GEN.1.2 TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び
b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*]

依存性: **FPT_STM.1 高信頼タイムスタンプ**

FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1 TSFは、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性: **FAU_GEN.1 監査データ生成**
FIA_UID.1 識別のタイミング

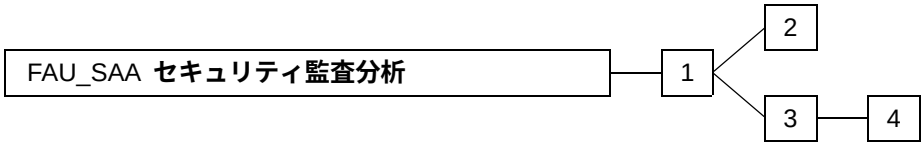
3.3 セキュリティ監査分析(FAU_SAA)

ファミリのふるまい

このファミリでは、実際のセキュリティ侵害あるいはその可能性を探す、システムアクティビティや監査データを分析する自動化された手段に対する要件を定義している。

この検出に基づいてとられるアクションは、それが必要とするようにFAU_ARPファミリを用いて特定することができる。

コンポーネントのレベル付け



FAU_SAA.1 侵害の可能性の分析では、固定した規則セットに基づく基本閾値による検出が要求される。

FAU_SAA.2 プロファイルベースに基づく異常検出では、TSFはシステム利用の個々の*プロファイル*を維持する(プロファイルとは、*プロファイルターゲットグループ*のメンバによって実行される利用の履歴パターンをいう)。プロファイルターゲットグループとは、そのTSFと対話する一人あるいは複数の個々人(例えば、単一利用者、一つのグループIDあるいはグループアカウントを共有する複数の利用者、ある割り付けられた役割に沿って運用する利用者、一つのシステムあるいはネットワークノード全体の利用者)のグループをいう。プロファイルターゲットグループの各メンバには、そのメンバの現在のアクティビティが、プロファイルに書かれた確立した利用パターンとどれくらいよく対応するかを表す個々の*疑惑率*が割り付けられる。この分析は、ランタイムで、あるいは後収集バッチモード分析で実行される。

FAU_SAA.3 単純攻撃の発見において、TSFは、TSPの実施に対して重大な脅威を表す特徴的事象の発生を検出できねばならない。特徴的事象に対するこの探索は、リアルタイムあるいは後収集バッチモード分析で行える。

FAU_SAA.4 複合攻撃の発見において、TSFは、多段階の侵入シナリオを表現しかつ検出できねばならない。TSFは、システム事象(複数の人間によって実行されているかもしれない)と、侵入シナリオ全体をあらわすものとして既知の事象シーケンスとを比較することができる。TSFは、TSPの侵害の可能性を示す特徴的事象あるいは事象シーケンスがいつ見つかったかを示すことができねばならない。

管理: FAU_SAA.1

以下のアクションはFMTの管理機能と考えられる:

a) 規則のセットから規則を(追加、改変、削除)することによる規則の維持。

管理: FAU_SAA.2

以下のアクションはFMTの管理機能と考えられる:

a) プロファイルターゲットグループにおける利用者グループの維持(削除、改変、追加)。

管理: FAU_SAA.3

以下のアクションはFMTの管理機能と考えられる:

a) システム事象のサブセットの維持(削除、改変、追加)。

管理: FAU_SAA.4

以下のアクションはFMTの管理機能と考えられる:

a) システム事象のサブセットの維持(削除、改変、追加);

b) システム事象のシーケンスのセットの維持(削除、改変、追加)。

監査: FAU_ SAA.1、FAU_ SAA.2、FAU_ SAA.3、FAU_ SAA.4

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: すべての分析メカニズムの活性化/非活性化。

b) 最小: ツールによって実行される自動応答。

FAU_SAA.1 侵害の可能性の分析

下位階層: なし

FAU_SAA.1.1 TSFは、監査事象のモニタに規則のセットを適用し、これらの規則に基づきTSP侵害の可能性を示すことができなければならない。

FAU_SAA.1.2 TSFは、監査事象をモニタするための以下の規則を実施しなければならない;

a) セキュリティ侵害の可能性を示すものとして知られている[割付: 定義された*監査対象事象のサブセット*]をすべて合わせた、あるいは組み合わせたもの;

b) [割付: *その他の規則*]。

依存性: **FAU_GEN.1 監査データ生成**

FAU_SAA.2　プロファイルに基づく異常検出

下位階層:　FAU_SAA.1

FAU_SAA.2.1　**TSFは、システム利用法のプロファイルを維持できなければならない。ここで個々のプロファイルは、[割付:** ***プロファイルターゲットグループ*** **を特定]のメンバーによって実施された利用の履歴パターンを表す。**

FAU_SAA.2.2　**TSFは、その動作がプロファイルに記録されている各利用者に関連付けられた疑惑率を維持できねばならない。ここで疑惑率とは、利用者の現在の動作が、プロファイル中に表示された設置済みの使用パターンと一致しないと見られる度合いを表す。**

FAU_SAA.2.3　**TSFは、利用者の疑惑率が以下のような閾値の条件[割付:** ***異例な動作がTSFにより報告される条件*** **]を超えた場合、TSPの侵害が差し迫っていることを通知できなければならない。**

依存性:　FAU_UID.1 **識別のタイミング**

FAU_SAA.3　単純攻撃の発見

下位階層:　FAU_SAA.1

FAU_SAA.3.1　**TSFは、TSP侵害を示しているかもしれない以下のような特徴的事象(signature events)[割付:** ***システム事象のサブセット*** **]の内部表現を維持できなければならない。**

FAU_SAA.3.2　**TSFは、特徴的事象を、[割付:** ***システムのアクティビティを決定するのに使用される情報を特定*** **]を検査することにより判別できるシステムのアクティビティの記録と比較できなければならない。**

FAU_SAA.3.3　**TSFは、システム事象がTSP侵害の可能性を示す特徴的事象と合致した場合、TSPの侵害が差し迫っていることを通知できなければならない。**

依存性:　**なし**

FAU_SAA.4　複合攻撃の発見

下位階層:　FAU_SAA.3

FAU_SAA.4.1　TSFは、**以下のような既知の侵入シナリオの事象シーケンス[割付:** ***既知の侵入シナリオが発生していることを示すシステム事象のシーケンス***

のリスト **]及び**以下のTSP侵害を示しているかもしれない特徴的事象[割付: *システム事象のサブセット*]の内部表現を維持できなければならない。

FAU_SAA.4.2　TSFは、特徴的事象**及び事象シーケンス**を、[割付: *システムのアクティビティを決定するのに使用される情報*]を検査することにより判別できるシステムのアクティビティの記録と比較できなければならない。

FAU_SAA.4.3　TSFは、**システムのアクティビティ**がTSP侵害の可能性を示す特徴的事象**または事象シーケンス**と合致した場合、TSPの侵害が差し迫っていることを通知できなければならない。

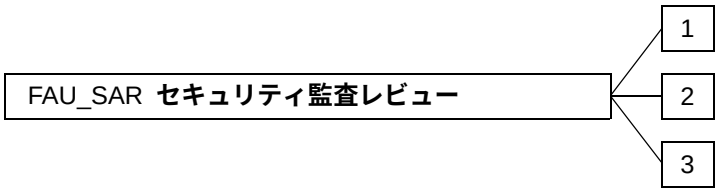
依存性:　　**なし**

3.4 セキュリティ監査レビュー(FAU_SAR)

ファミリのふるまい

このファミリでは、権限のある利用者が監査データをレビューする際の助けとなる監査ツールのための要件を定義している。

コンポーネントのレベル付け



FAU_SAR.1　監査レビューは、監査記録からの情報読み出し能力を提供する。

FAU_SAR.2　限定監査レビューは、FAU_SAR.1で識別された者を除き、それ以外に情報を読み出せる利用者はいないことを要求する。

FAU_SAR.3　選択可能監査レビューは、基準に基づき、レビューされる監査データを選択する監査レビューツールを要求する。

管理: FAU_ SAR.1

以下のアクションはFMTの管理機能と考えられる:

a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。

管理: FAU_SAR.2、FAU_SAR.3

予見される管理アクティビティはない。

監査: FAU_ SAR.1

セキュリティ監査データ生成(FAU_GEN)がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 監査記録からの情報の読み出し。

監査: FAU_SAR.2

セキュリティ監査データ生成(FAU_GEN)がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 監査記録からの成功しなかった情報読み出し。

監査: FAU_SAR.3

セキュリティ監査データ生成(FAU_GEN)がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 詳細: 閲覧に使用されるパラメタ。

FAU_SAR.1 監査レビュー

このコンポーネントは、許可利用者に情報を取得し解釈する能力を提供する。人間の利用者が対象の場合、この情報は人間が理解できる表現である必要がある。外部ITエンティティが対象の場合、情報は電子的形式として曖昧さなく表現される必要がある。

下位階層: なし

FAU_SAR.1.1 **TSFは、[割付: *許可利用者*]が、[割付: *監査情報のリスト*]を監査記録から読み出せるようにしなければならない。**

FAU_SAR.1.2 **TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。**

依存性: **FAU_GEN.1 監査データ生成**

FAU_SAR.2 限定監査レビュー

下位階層: なし

FAU_SAR.2.1 **TSFは、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。**

依存性: **FAU_SAR.1 監査レビュー**

FAU_SAR.3 選択可能監査レビュー

下位階層: なし

FAU_SAR.3.1 **TSFは、[割付: *論理的な関連の基準*]に基づいて、監査データを[選択: *検索、分類、並べ替え*]する能力を提供しなければならない。**

依存性: **FAU_SAR.1 監査レビュー**

3.5 セキュリティ監査事象選択(FAU_SEL)

ファミリのふるまい

このファミリでは、TOEの動作中に監査される事象を選択するための要件を定義している。このファミリは監査対象事象のセットから、事象を含めたり除外したりするための要件を定義している。

コンポーネントのレベル付け

FAU_SEL **セキュリティ監査事象選択**	1

FAU_SEL.1　選択的監査は、PP/ST作成者によって特定される属性に基づき、監査される事象のセットから事象を含めたり除外する能力を要求する。

管理: FAU_SEL.1

以下のアクションはFMTの管理機能と考えられる:

a) 監査事象を閲覧/改変する権限の維持。

監査: FAU_SEL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小:監査データ収集機能が作動している間に生じる、監査設定へのすべての改変。

FAU_SEL.1　選択的監査

下位階層:　なし

FAU_SEL.1.1　TSFは以下のような属性に基づいて、監査事象のセットから監査対象事象を含めたり、除外したりすることができなければならない:

a) [選択: ***オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別*****]**

b) [***割付:** ***監査の選択性の基礎となる追加属性リスト*****]。**

依存性:　**FAU_GEN.1 監査データ生成**

FMT_MTD.1 TSFデータの管理

3.6 セキュリティ監査事象格納(FAU_STG)

ファミリのふるまい

このファミリでは、セキュアな監査証跡を生成あるいは維持するための要件を定義している。

コンポーネントのレベル付け

FAU_STG.1 保護された監査証跡格納において、要件は監査証跡に関わるものである。監査証跡は、不当な削除及び/または改変から保護されることになる。

FAU_STG.2 監査データ可用性の保証は、望ましくない条件の発生において、TSFが監査データに対して維持する保証を規定する。

FAU_STG.3 監査データ損失の恐れ発生時のアクションは、監査証跡が閾値を超えたときにとられるアクションを規定する。

FAU_STG.4 監査データ損失の防止は、監査証跡が満杯になったときのアクションを規定する。

管理: FAU_ STG.1

予見される管理アクティビティはない。

管理: FAU_ STG.2

以下のアクションはFMTの管理機能と考えられる:

a) 監査格納機能を制御するパラメタの維持。

管理: FAU_ STG.3

以下のアクションはFMTの管理機能と考えられる:

a) 閾値の維持;
b) 監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。

管理: FAU_ STG.4

以下のアクションはFMTの管理機能と考えられる:

a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。

監査: FAU_ STG.1、FAU_ STG.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査すべき識別されたアクションはない。

監査: FAU_ STG.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象とすべきである:
a) 基本: 閾値を超えたためにとられるアクション。

監査: FAU_ STG.4
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
a) 基本: 監査格納失敗によってとられるアクション。

FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1 **TSFは、格納された監査記録を不正な削除から保護しなければならない。**

FAU_STG.1.2 **TSFは、監査記録の改変を[選択: *防止*、*検出*]できねばならない。**

依存性: **FAU_GEN.1 監査データ生成**

FAU_STG.2 監査データ可用性の保証

下位階層: FAU_STG.1

FAU_STG.2.1 TSFは、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.2.2 TSFは、監査記録の改変を[選択: *防止*、*検出*]できねばならない。

FAU_STG.2.3 **TSFは、[選択: *監査格納の領域枯渇*、*失敗*、*攻撃*]という状況が生じた場合、[割付: 救済する*監査記録の数値尺度*]の監査記録が維持されることを保証しなければならない 。**

依存性: **FAU_GEN.1 監査データ生成**

FAU_STG.3　監査データ損失の恐れ発生時のアクション

下位階層:　なし

FAU_STG.3.1　**TSFは、監査証跡が[割付: *事前に定義された限界*]を超えた場合、[割付: *監査格納失敗の恐れ発生時のアクション*]をとらなければならない。**

依存性:　**FAU_STG.1 保護された監査証跡格納**

FAU_STG.4　監査データ損失の防止

下位階層:　FAU_STG.3

FAU_STG.4.1　**TSFは、監査証跡が満杯になった場合、[選択: *監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き*]及び[割付: *監査格納失敗時にとられるその他のアクション*]を行わねばならない。**

依存性:　**FAU_STG.1 保護された監査証跡格納**

4 クラスFCO: 通信

このクラスには、データ交換に携わるパーティの識別情報の保証に特に関係する二つのファミリがある。これらのファミリは、送信情報の発信者の識別情報の保証(発信の証明)及び、送信情報の受信者の識別情報の保証(受信の証明)に関係する。これらのファミリは、発信者がメッセージを送ったことを否定できないこと、また受信者がメッセージを受け取ったことを否定できないことを保証する。

図4.1は、このクラスのコンポーネント構成を示す。

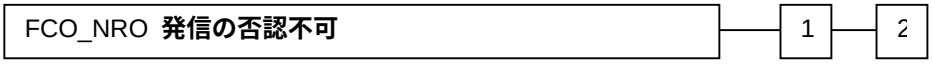
図4.1 - 通信クラスのコンポーネント構成

4.1 発信の否認不可(FCO_NRO)

ファミリのふるまい

発信の否認不可は、情報の発信者が情報を送ったことを否定できないようにする。このファミリは、データ交換中に情報を受け取るサブジェクトに対して、TSFが、情報の発信元の証拠が提供されることを保証する方法を提供することを要求する。この証拠は、このサブジェクトまたは他のサブジェクトのいずれかによって検証され得る。

コンポーネントのレベル付け



FCO_NRO.1　発信の選択的証明は、TSFが情報の発信元の証拠を要求する能力をサブジェクトに提供することを要求する。

FCO_NRO.2　発信の強制的証明は、TSFが送信済み情報に対する発信元の証拠を常に生成することを要求する。

管理: FCO_NRO.1、FCO_NRO.2

以下のアクションはFMTにおける管理機能と考えられる:

a) 情報種別、フィールド、発信者属性及び証拠の受信者に対する変更の管理。

監査: FCO_NRO.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 発信元の証拠が生成されることを要求した利用者の識別情報。
b) 最小: 否認不可サービスの呼出。
c) 基本: 情報、宛先、提供された証拠のコピーの識別。
d) 詳細: 証拠の検証を要求した利用者の識別情報。

監査: FCO_NRO.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 否認不可サービスの呼出。
b) 基本: 情報、宛先、提供された証拠のコピーの識別。
c) 詳細: 証拠の検証を要求した利用者の識別情報。

FCO_NRO.1　発信の選択的証明

下位階層: なし

FCO_NRO.1.1 **TSFは、送信された[割付: *情報種別のリスト*]の発信元の証拠を[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]の要求により生成できなければならない。**

FCO_NRO.1.2 **TSFは、情報の発信者の[割付: *属性のリスト*]と証拠が適用される情報の[割付: *情報フィールドのリスト*]を関係付けることができなければならない。**

FCO_NRO.1.3 **TSFは、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]へ、[割付: 発信元の証拠における制限]の範囲で、情報の発信元の証拠を検証する能力を提供しなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FCO_NRO.2 発信の強制的証明

下位階層: FCO_NRO.1

FCO_NRO.2.1 TSFは、送信された[割付: *情報種別のリスト*]に対する発信元の証拠の**生成を常に実施**しなければならない。

FCO_NRO.2.2 TSFは、情報の発信者の[割付: *属性リスト*]を証拠が適用される情報の[割付: *情報フィールドのリスト*]に関係付けることができなければならない。

FCO_NRO.2.3 TSFは、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]へ、[割付: 発信元の証拠における制限]の範囲で、情報の発信元の証拠を検証する能力を提供しなければならない。

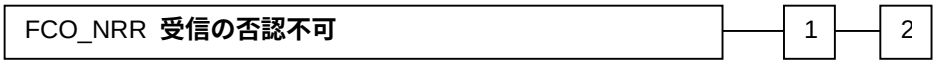
依存性: **FIA_UID.1 識別のタイミング**

4.2 受信の否認不可(FCO_NRR)

ファミリのふるまい

受信の否認不可は、情報の受信者が情報の受信を否定できないようにする。このファミリは、データ交換中に情報を送信するザブジェクトに対して、TSFが、情報の受信先の証拠が提供されることを保証する方法を提供することを要求する。この証拠は、このサブジェクトまたは他のサブジェクトによって検証され得る。

コンポーネントのレベル付け



FCO_NRR.1　受信の選択的証明は、TSFが情報の受信の証拠を要求する能力をサブジェクトに提供することを要求する。

FCO_NRR.2　受信の強制的証明は、TSFが受信済み情報の受信の証拠を常に生成することを要求する。

管理: FCO_NRR.1、FCO_NRR.2

以下のアクションはFMTの管理機能と考えられる:

a) 情報種別、フィールド、発信者属性及び、証拠の第三者受信者の変更の管理。

監査: FCO_NRR.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 受信の証拠が生成されることを要求した利用者の識別情報。
b) 最小: 否認不可サービスの呼出。
c) 基本: 情報、宛先、提供される証拠のコピーの識別。
d) 詳細: 証拠の検証を要求した利用者の識別情報。

監査: FCO_NRR.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 否認不可サービスの呼出。
b) 基本: 情報、宛先、提供される証拠のコピーの識別。
c) 詳細: 証拠の検証を要求した利用者の識別情報。

FCO_NRR.1　受信の選択的証明

下位階層: なし

FCO_NRR.1.1 **TSFは、受信した[割付: *情報種別のリスト*]の受信の証拠を、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]の要求により生成できなければならない。**

FCO_NRR.1.2 **TSFは、情報の受信者の[割付: *属性リスト*]をその証拠が適用される情報の[割付: *情報フィールドのリスト*]に関係付けることができなければならない。**

FCO_NRR.1.3 **TSFは、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]へ[割付: 受信の証拠における制限]の範囲で、情報受信の証拠を検証する能力を提供しなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FCO_NRR.2 受信の強制的証明

下位階層: FCO_NRR.1

FCO_NRR.2.1 TSFは、受信した[割付: *情報種別のリスト*]の受信の証拠**生成を実施**しなければならない。

FCO_NRR.2.2 TSFは、情報の受信者の[割付: *属性のリスト*]を証拠が適用される情報の[割付: *情報フィールドのリスト*]に関係付けることができなければならない。

FCO_NRR.2.3 TSFは、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]へ[割付: 受信の証拠における制限]の範囲で、情報受信の証拠を検証する能力を提供しなければならない。

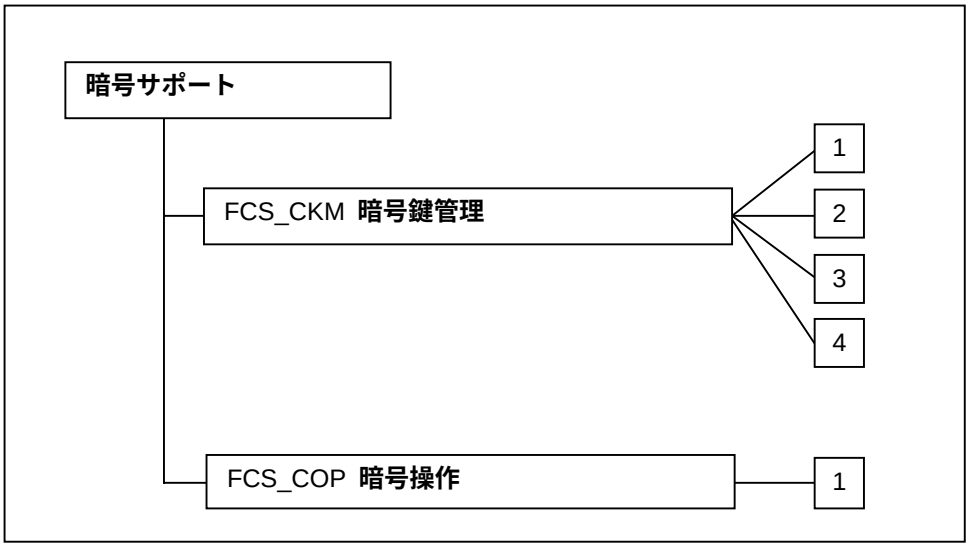
依存性: **FIA_UID.1 識別のタイミング**

5 クラスFCS: 暗号サポート

TSFは、いくつかの高レベルのセキュリティオブジェクティブを満たすための助けとして、暗号機能を用いるかもしれない。この中には以下のものが含まれる(これだけに限定されない): 識別と認証、否認不可、高信頼パス、高信頼チャネル及びデータ分離。このクラスは、TOEが暗号機能を実装するときに利用され、その実装は、ハードウェア、ファームウェア及び/またはソフトウェアなどに対して行われる。

FCSクラスは、FCS_CKM(暗号鍵管理)と、FCS_COP(暗号操作)の2個のファミリから構成される。FCS_CKMファミリは暗号鍵の管理的側面を扱い、一方FCS_COPファミリはこれらの暗号鍵の操作面の利用に関係している。

図5.1は、このクラスのコンポーネント構成を示す。

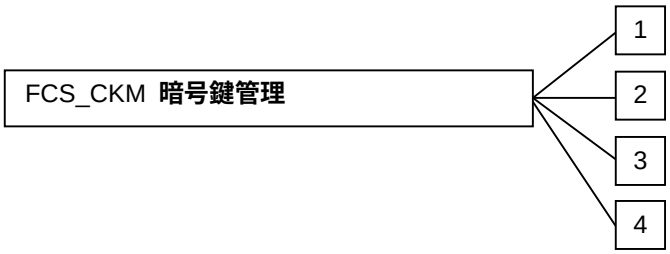


5.1 暗号鍵管理(FCS_CKM)

ファミリのふるまい

暗号鍵は、そのライフサイクルを通して管理されねばならない。このファミリは、このライフサイクルをサポートするためのものであり、結果的に以下の行為のための要求を定義する: 暗号鍵生成、暗号鍵配付、暗号鍵アクセス、暗号鍵破棄。このファミリは、暗号鍵の管理に対する機能要件があるときは、常に含められるべきである。

コンポーネントのレベル付け



FCS_CKM.1 暗号鍵生成は、指定された標準に基づく特定のアルゴリズムと鍵長に従って暗号鍵が生成されることを要求する。

FCS_CKM.2 暗号鍵配付は、指定された標準に基づく特定の配付方法に従って暗号鍵が配付されることを要求する。

FCS_CKM.3 暗号鍵アクセスは、指定された標準に基づく特定のアクセス方法に従って暗号鍵がアクセスされることを要求する。

FCS_CKM.4 暗号鍵破棄は、指定された標準に基づく特定の破棄方法に従って暗号鍵が破棄されることを要求する。

管理: FCS_CKM.1、 FCS_CKM.2、FCS_CKM.3、FCS_CKM.4

以下のアクションはFMTにおける管理機能と考えられる:

a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。

監査: FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.4

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 動作の成功と失敗。
b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェ

クトの値。

FCS_CKM.1　暗号鍵生成

下位階層:　なし

FCS_CKM.1.1　**TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。**

依存性:　**[FCS_CKM.2 暗号鍵配付**
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.2　暗号鍵配付

下位階層:　なし

FCS_CKM.2.1　**TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵配付方法[割付: *暗号鍵配付方法*]に従って、暗号鍵を配付しなければならない。**

依存性:　**[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.3　暗号鍵アクセス

下位階層:　なし

FCS_CKM.3.1　**TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵アクセス方法[割付: *暗号鍵アクセス方法*]に従って、[割付: *暗号鍵アクセスの種別*]を行わなければならない。**

依存性:　**[FDP_ITC.1 セキュリティ属性なし利用者データインポート**
または
FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 **TSFは、以下の[割付:*標準のリスト*]に合致する、指定された暗号鍵破棄方法[割付: *暗号鍵破棄方法*]に従って、暗号鍵を破棄しなければならない。**

依存性: **[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

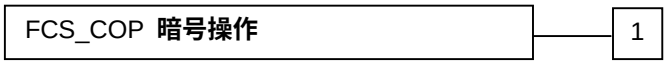
5.2 暗号操作(FCS_COP)

ファミリのふるまい

暗号操作が正しく機能するためには、操作は指定されたアルゴリズムと指定された長さの暗号鍵に従って実行されねばならない。暗号操作を実行する要求があるときは、いつでもこのファミリが含まれねばならない。

典型的な暗号操作は、データの暗号化/復号、ディジタル署名の生成と検証、完全性のための暗号的チェックサムの生成と検証、セキュアハッシュ(メッセージダイジェスト)、暗号鍵の暗号化及び/または復号、暗号鍵交換などである。

コンポーネントのレベル付け



FCS_COP.1 暗号操作は、特定されたアルゴリズムと特定された長さの暗号鍵に従って暗号操作が実行されることを要求する。特定されたアルゴリズムと暗号鍵長は、割り付けられた標準に基づくことができる。

管理: FCS_COP.1
これらのコンポーネントについて予見される管理アクティビティはない。

監査: FCS_COP.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 成功と失敗及び暗号操作の種別。
b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 **TSFは、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。**

依存性: **[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**
または
FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

6 クラスFDP: 利用者データ保護

このクラスは、利用者データ保護に関係したTOEセキュリティ機能とTOEセキュリティ機能方針に対する要件を特定するファミリからなる。FDPは、インポート・エクスポート中及び蓄積中のTOE内利用者データに対応する4つのファミリのグループ(以下に示す)に分割され、利用者データに直接関係するセキュリティ属性も同様である。
このクラスのファミリは、４つのグループから構成される。

(a) 利用者データ保護におけるセキュリティ機能方針:
- FDP_ACC アクセス制御方針; 及び
- FDP_IFC 情報フロー制御方針。

これらのファミリのコンポーネントは、PP/ST作成者が、セキュリティオブジェクティブに対処するために必要な利用者データ保護セキュリティ機能方針の名前の設定や方針の制御範囲の定義をすることを許している。これらの方針の名前は、このあと、「アクセス制御方針」や「情報フロー制御方針」における割付や選択といった操作を必要とする機能コンポーネント全体に対して使われることになる。名前を付けられたアクセス制御や情報フロー制御のSFPの機能を定義する規則については、FDP_ACFとFDP_IFFファミリにおいて(それぞれで)定義される。

(b) 利用者データ保護の形態:
- FDP_ACF アクセス制御機能;
- FDP_IFF 情報フロー制御機能;
- FDP_ITT TOE内転送;
- FDP_RIP 残存情報保護;
- FDP_ROL ロールバック; 及び
- FDP_SDI 蓄積データ完全性。

(c) オフライン格納、インポート及びエクスポート:
- FDP_DAU データ認証;
- FDP_ETC TSF制御外へのエクスポート; 及び
- FDP_ITC TSF制御外からのインポート。

これらのファミリのコンポーネントは、TSC内へあるいは外への信頼できる転送を扱う。

(d) TSF間通信:
- FDP_UCT TSF間利用者データ機密転送保護; 及び
- FDP_UIT TSF間利用者データ完全性転送保護。

これらのファミリのコンポーネントは、TOEのTSFと他の高信頼IT製品間の通信を扱う。

図6.1と図6.2は、このクラスのコンポーネント構成を示す。

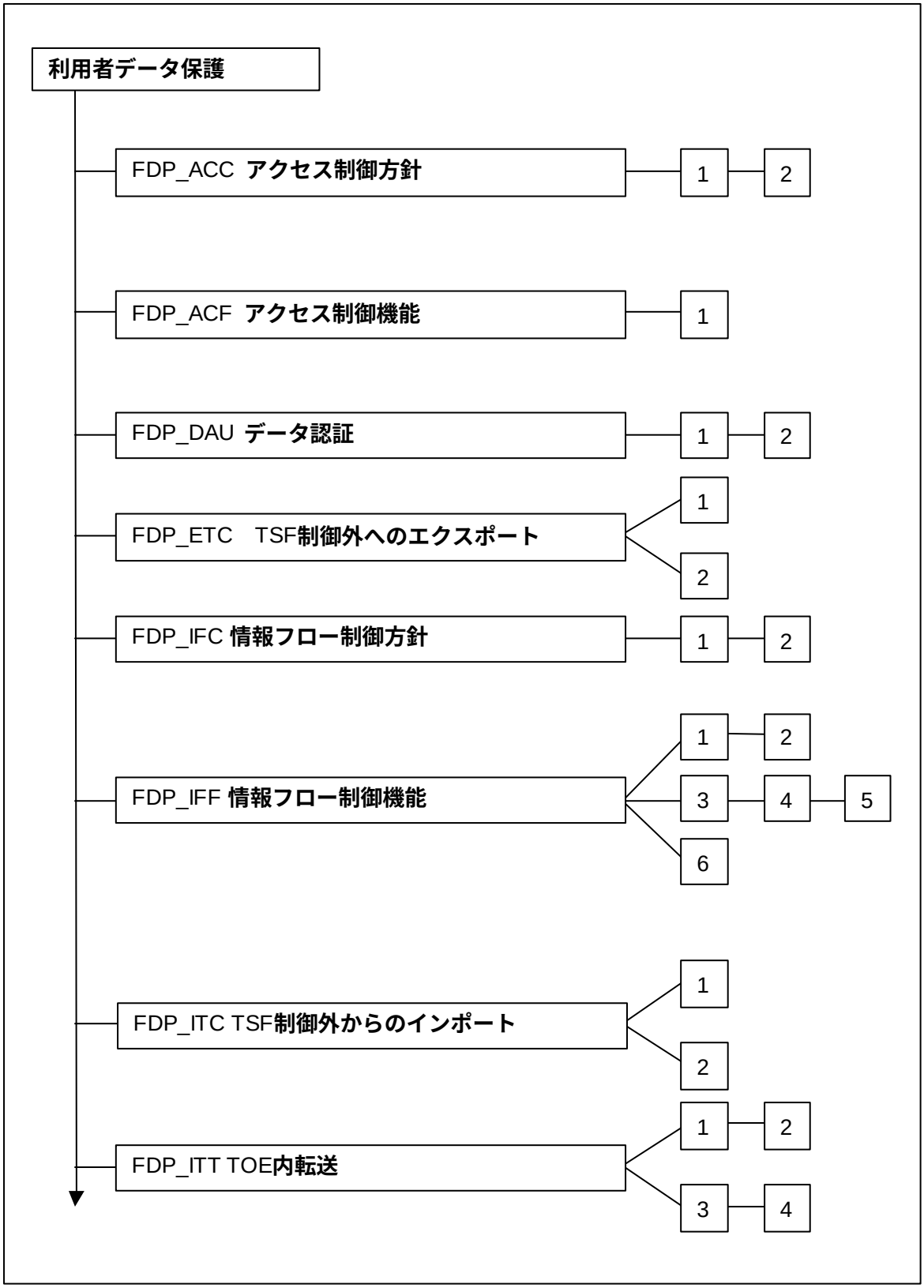
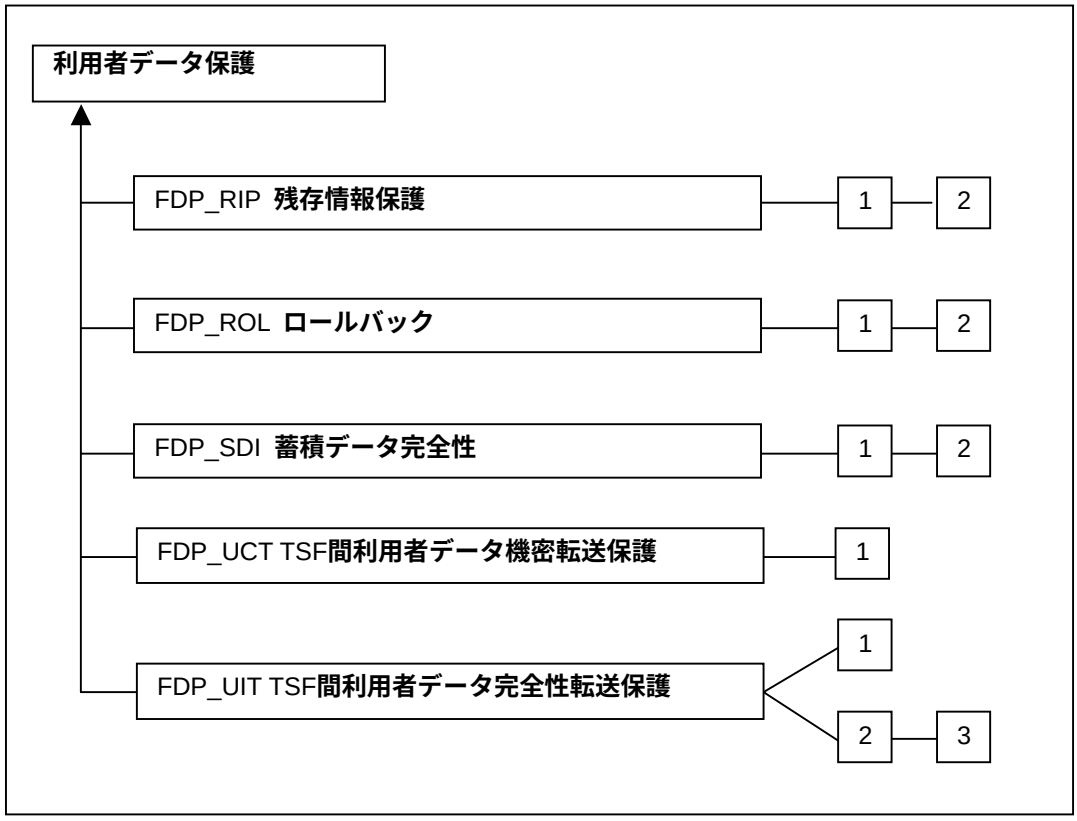


図6.1 - **利用者データ保護クラスのコンポーネント構成**

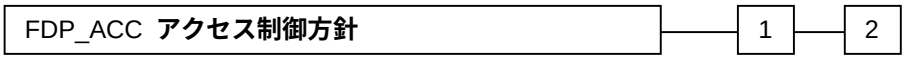

利用者データ保護
FDP_RIP 残存情報保護
1
2
FDP_ROL ロールバック
1
2
FDP_SDI 蓄積データ完全性
1
2
FDP_UCT TSF間利用者データ機密転送保護
1
FDP_UIT TSF間利用者データ完全性転送保護
1
2
3

6.1 アクセス制御方針(FDP_ACC)

ファミリのふるまい

このファミリは、アクセス制御SFPを(名前で)識別し、TSPの識別されたアクセス制御部分を形成する方針の制御範囲を定義する。この制御範囲は、三つのセットによって特徴付けられる: 方針の制御下にあるサブジェクト、方針の制御下にあるオブジェクト、及び、方針でカバーされた、制御されたサブジェクトと制御されたオブジェクト間の操作である。本基準は、複数の方針が、各々一意の名前を持って存在することを許している。これは、各々の名前を付けたアクセス制御方針に対して、このファミリのコンポーネントを一つずつ繰り返すことで実現できる。アクセス制御SFPの機能を定義する規則は、FDP_ACFやFDP_SDIといった他のファミリによって定義される。FDP_ACCにおいて識別されたアクセス制御SFPの名前は、「アクセス制御SFP」の割付または選択が必要な操作を有する残りの機能コンポーネント全体を通して使われることになる。

コンポーネントのレベル付け



FDP_ACC.1　サブセットアクセス制御は、TOEにおけるオブジェクトのサブセットについて適用可能な操作のサブセットに対し、識別された各アクセス制御SFPが適切なものであることを要求する。

FDP_ACC.2　完全アクセス制御は、そのSFPがカバーするサブジェクトとオブジェクトについてのすべての操作を、識別された各アクセス制御SFPがカバーすることを要求する。さらに、TSCのすべてのオブジェクトと操作が、最低でも一つの識別されたアクセス制御SFPでカバーされることが要求される。

管理: FDP_ACC.1、FDP_ACC.2
このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_ACC.1、FDP_ACC.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FDP_ACC.1　サブセットアクセス制御

下位階層:　なし

FDP_ACC.1.1　TSFは、[割付: *サブジェクト、オブジェクト、及びSFPで扱われるサ*

ブジェクトとオブジェクト間の操作のリスト]に対して[割付: *アクセス制御SFP*]を実施しなければならない。

依存性: **FDP_ACF.1 セキュリティ属性によるアクセス制御**

FDP_ACC.2 完全アクセス制御

下位階層: FDP_ACC.1

FDP_ACC.2.1 TSFは、[割付: *アクセス制御SFP*]を[割付: *サブジェクト及びオブジェクトのリスト*]及びSFPでカバーされるサブジェクトとオブジェクト間のすべての操作に対して実施しなければならない。

FDP_ACC.2.2 TSFは、TSC内の任意のサブジェクトとTSC内の任意のオブジェクト間のすべての操作がアクセス制御SFPでカバーされることを保証しなければならない。

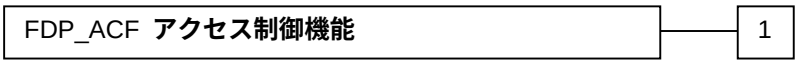
依存性: **FDP_ACF.1 セキュリティ属性によるアクセス制御**

6.2 アクセス制御機能(FDP_ACF)

ファミリのふるまい

このファミリでは、FDP_ACCで名前を付けられたアクセス制御方針を実装することができる特定の機能に対する規則を記述する。FDP_ACCは、方針の制御範囲を特定する。

コンポーネントのレベル付け



このファミリはセキュリティ属性の利用方法と方針の性質を扱う。このファミリのコンポーネントは、FDP_ACCで識別されたようなSFPを実装する機能についての規則を記述するために使われることを意図している。PP/ST作成者は、TOEにおいて複数の方針を扱うため、このコンポーネントを繰返して使用してよい。

FDP_ACF.1 セキュリティ属性に基づくアクセス制御は、TSFが、セキュリティ属性と名前を付けられた属性グループに基づくアクセスを実施することを許可する。さらに、TSFは、セキュリティ属性に基づいてオブジェクトへのアクセスを明示的に正当化あるいは拒否する能力を持ってもよい。

管理: FDP_ACF.1

以下のアクションはFMTの管理機能と考えられる:

a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。

監査: FDP_ACF.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: SFPで扱われるオブジェクトに対する操作の実行における成功した要求。
b) 基本: SFPで扱われるオブジェクトに対する操作の実行におけるすべての要求。
c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1 **TSFは、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御SFP*]を実施しなければならない。**

FDP_ACF.1.2 **TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の*規則*を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。**

FDP_ACF.1.3 **TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。**

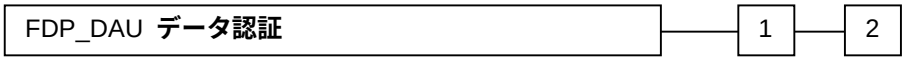
FDP_ACF.1.4 **TSFは、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。**

依存性: FDP_ACC.1 **サブセットアクセス制御**
FMT_MSA.3 **静的属性初期化**

6.3 データ認証(FDP_DAU)

ファミリのふるまい
データ認証は、あるエンティティが情報の真正性についての責任を持つ(例えば、ディジタル署名によって)ことを許可する。このファミリは、特定のデータユニットの有効性を保証する方法を提供する。このデータユニットは、情報の内容が捏造されたり欺瞞的に改変されたりしていないことを検証するのに使える。FAUクラスと異なり、このファミリは、転送中のデータよりもむしろ「静的」なデータに適用されることを意図している。

コンポーネントのレベル付け



FDP_DAU.1　基本データ認証は、TSFがオブジェクト(例えば文書)の情報の内容の真正性の保証を生成できることを要求する。

FDP_DAU.2　保証人識別情報付きデータ認証は、追加として、真正性の保証を提供するサブジェクトの識別情報をTSFが確立できることを要求する。

管理: FDP_DAU.1、FDP_DAU.2
以下のアクションはFMT管理における管理機能と考えられる:

a) データ認証が適用され得るオブジェクトに対する割付や改変が、システムにおいて設定可能である。

監査: FDP_DAU.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 有効性の証拠の生成成功。
b) 基本: 有効性の証拠の生成不成功。
c) 詳細: 証拠を要求したサブジェクトの識別情報。

監査: FDP_DAU.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 有効性の証拠の生成成功。
b) 基本: 有効性の証拠の生成不成功。
c) 詳細: 証拠を要求したサブジェクトの識別情報。
d) 詳細: 証拠を生成したサブジェクトの識別情報。

FDP_DAU.1　基本データ認証

下位階層:　なし

FDP_DAU.1.1　**TSFは、[割付: *オブジェクトまたは情報種別のリスト*]の有効性の保証として使用できる証拠を生成する能力を提供しなければならない。**

FDP_DAU.1.2　**TSFは、示された情報の有効性の証拠を検証する能力を[割付: *サブジェクトのリスト*]に提供しなければならない。**

依存性:　**なし**

FDP_DAU.2　保証人識別情報付きデータ認証

下位階層:　FDP_DAU.1

FDP_DAU.2.1　TSFは、[割付: *オブジェクトまたは情報種別のリスト*]の有効性の保証として使用できる証拠を生成する能力を提供しなければならない。

FDP_DAU.2.2　TSFは、示された情報の有効性の証拠**及び証拠を生成した利用者の識別情報**を検証する能力を[割付: *サブジェクトのリスト*]に提供しなければならない。

依存性:　**FIA_UID.1 識別のタイミング**

6.4 TSF制御外へのエクスポート(FDP_ETC)

ファミリのふるまい

このファミリは、セキュリティ属性と保護の両方が、明示的に保持されるかあるいはいったんエクスポートされたあとでは無視できるよう、TOEから利用者データをエクスポートする機能を定義する。このファミリは、エクスポートにおける制約及びエクスポートされた利用者データとセキュリティ属性の関連に関係する。

コンポーネントのレベル付け

FDP_ETC.1　セキュリティ属性なし利用者データのエクスポートは、TSFの外部に利用者データをエクスポートするときに、TSFが適切なSFPを実施することを要求する。本機能によってエクスポートされる利用者データは、関連するセキュリティ属性なしでエクスポートされる。

FDP_ETC.2　セキュリティ属性付き利用者データのエクスポートは、セキュリティ属性とエクスポートされる利用者データを正確かつあいまいさなく関連付ける機能を用いる適切なSFPをTSFが実施することを要求する。

管理: FDP_ETC.1

このコンポーネントについて予見される管理アクティビティはない。

管理: FDP_ETC.2

以下のアクションはFMT管理の管理機能と考えられる。

a) 追加のエクスポート制御規則は、定義された役割の利用者により、設定可能である。

監査: FDP_ETC.1、FDP_ETC.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 情報エクスポート成功。
b) 基本: 情報をエクスポートするすべての試み。

FDP_ETC.1　セキュリティ属性なし利用者データのエクスポート

下位階層: なし

FDP_ETC.1.1 **TSFは、SFP(s)制御下にある利用者データをTSCの外部にエクスポートするとき、[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。**

FDP_ETC.1.2 **TSFは、利用者データに関係したセキュリティ属性なしで利用者データをエクスポートしなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、あるいは**
FDP_IFC.1 サブセット情報フロー制御]

FDP_ETC.2 セキュリティ属性付き利用者データのエクスポート

下位階層: **なし**

FDP_ETC.2.1 **TSFは、SFP(s)制御下にある利用者データをTSCの外部にエクスポートするとき、[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。**

FDP_ETC.2.2 **TSFは、利用者データに関係したセキュリティ属性と共に利用者データをエクスポートしなければならない。**

FDP_ETC.2.3 **TSFは、セキュリティ属性がTSCの外部にエクスポートされるとき、それがエクスポートされる利用者データに曖昧さなく関係付けられることを保証しなければならない。**

FDP_ETC.2.4 **TSFは、利用者データがTSCからエクスポートされるとき、以下の規則を実施しなければならない: [割付: *追加エクスポート制御規則*]。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、または**
FDP_IFC.1 サブセット情報フロー制御]

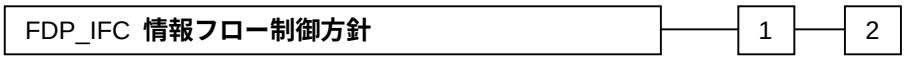
6.5 情報フロー制御方針(FDP_IFC)

ファミリのふるまい

このファミリは、情報フロー制御SFPを(名前で)識別し、TSPの識別された情報フロー制御部分を形成する方針の制御範囲を定義する。この制御範囲は、以下の三つのセットによって特徴付けられる: 方針の制御下のサブジェクト、方針の制御下の情報、及び制御された情報を、方針によってカバーされる制御されたサブジェクトへ(あるいはサブジェクトから)流れさせる操作。本基準は、複数の方針が、各々一意の名前を持って存在することを許している。これは、各々の名前を付けた情報フロー制御方針に対し、このファミリからのコンポーネントを一つずつ繰り返すことで実現できる。情報フロー制御SFPの機能を定義する規則は、FDP_IFFやFDP_SDIといった他のファミリによって定義される。FDP_IFCにおいて識別された情報フロー制御SFPの名前は、「情報フロー制御SFP」の割付または選択が必要な操作を有する残りの機能コンポーネント全体を通して使われることになる。

TSFのメカニズムは、情報フロー制御SFPに従って情報の流れを制御する。情報のセキュリティ属性を変更する操作は情報フロー制御SFPに違反するので、通常は許可されない。しかしながら、明示的に特定される場合、このような操作が情報フロー制御SFPの例外として許可されることがある。

コンポーネントのレベル付け



FDP_IFC.1　サブセット情報フロー制御は、TOEにおける情報フローのサブセットについて適用可能な操作のサブセットに対し、識別された各情報フロー制御SFPが適切なものであることを要求する。

FDP_IFC.2　完全情報フロー制御は、そのSFPがカバーするサブジェクトと情報についてのすべての操作を、識別された各情報フロー制御SFPがカバーすることを要求する。さらに、TSCのすべての情報フローと操作が、最低でも一つの識別された情報フロー制御SFPでカバーされることが要求される。FPT_RVM.1コンポーネントと連動して、これはリファレンスモニタの「常に呼び出された」側面を与える。

管理: FDP_IFC.1、FDP_IFC.2

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_IFC.1、FDP_IFC.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれている場合でも、監査対象とすべき識別された事象はない。

FDP_IFC.1　サブセット情報フロー制御

下位階層:　なし

FDP_IFC.1.1　**TSFは、[割付: サブジェクト、情報、及び、SFPによって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]に対して[割付: 情報フロー制御SFP]を実施しなければならない。**

依存性:　**FDP_IFF.1 単純セキュリティ属性**

FDP_IFC.2　完全情報フロー制御

下位階層:　FDP_IFC.1

FDP_IFC.2.1　TSFは、[割付: *サブジェクトと情報のリスト*]及び**SFPによって扱われるサブジェクトに、またはサブジェクトから情報の流れを引き起こすすべての操作に対して**[割付: *情報フロー制御SFP*]を実施しなければならない。

FDP_IFC.2.2　**TSFは、TSCのどのサブジェクトに、またはどのサブジェクトから、TSCの何らかの情報の流れを引き起こすすべての操作が、情報フロー制御SFPによって扱われることを保証しなければならない。**

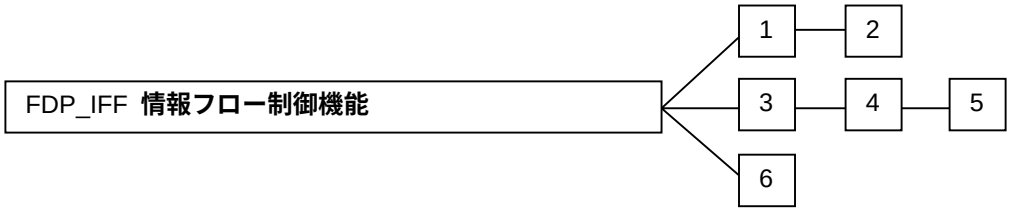
依存性:　**FDP_IFF.1 単純セキュリティ属性**

6.6 情報フロー制御機能(FDP_IFF)

ファミリのふるまい

このファミリは、FDP_IFCで名前付された(また方針の制御範囲も特定しているが、)情報フロー制御SFPを履行できる特定の機能についての規則を述べる。これは、二種類の要件からなる: 一つは共通の情報フロー機能の問題を扱い、他方は不正な情報フロー(すなわち隠れチャネル)を扱う。この区別は、不正な情報フローに関係する問題が、ある意味で、情報フロー制御SFPの残りの部分と直交しているために生じたものである。この性質によって、不正な情報フローは情報フロー制御SFPを回避し、その結果として方針を侵害することになる。そのようなわけで、この発生を制限あるいは防止するための特別な機能が必要になる。

コンポーネントのレベル付け



FDP_IFF.1 単純セキュリティ属性は、情報とその情報を流したり受け取ったりするサブジェクトにおけるセキュリティ属性を要求する。単純セキュリティ属性は、この機能によって実施されなければならない規則を特定し、この機能によってセキュリティ属性がどのように引き出されるかを記述する。

FDP_IFF.2 階層的セキュリティ属性は、TSPにおけるすべての情報フロー制御SFPが、格子を形成する階層的セキュリティ属性の使用を要求することによって、FDP_IFF.1 単純セキュリティ属性の要件をさらに詳しく規定する。

FDP_IFF.3 制限付き不正情報フローは、SFPが不正情報フローを扱うことを要求するが、それを排除することは必要としない。

FDP_IFF.4 不正情報フローの部分的排除は、SFPがいくらかの不正情報フロー(全部を必要とはしない)の排除を扱うことを要求する。

FDP_IFF.5 不正情報フローなしは、SFPがすべての不正情報フローの排除を扱うことを要求する。

FDP_IFF.6 不正情報フロー監視は、SFPが、特定された不正情報フローについてその最大容量を監視することを要求する。

管理: FDP_IFF.1、FDP_IFF.2
以下のアクションはFMT管理の管理機能と考えられる:

a) 明示的なアクセスに基づく決定に使われる属性の管理。

管理: FDP_IFF.3、FDP_IFF.4、FDP_IFF.5
これらのコンポーネントについて予見される管理アクティビティはない。

管理: FDP_IFF.6
以下のアクションはFMT管理における管理機能と考えられる:

a) モニタ機能の有効化及び無効化。
b) モニタの対象となる最大容量の改変。

監査: FDP_IFF.1、FDP_IFF.2、FDP_IFF.5
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 要求された情報フローを許可する決定。
b) 基本: 情報フローに対する要求に関するすべての決定。
c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。
d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。

監査: FDP_IFF.3、FDP_IFF.4、FDP_IFF.6
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 要求された情報フローを許可する決定。
b) 基本: 情報フローに対する要求に関するすべての決定。
c) 基本: 識別された不正情報フローチャネルの利用。
d) 詳細: 情報フローの実施の決定をする上で用いられる特定のセキュリティ属性。
e) 詳細: 方針目的(policy goal)に基づいて流れた、情報の特定のサブセット(例えば、対象物の劣化の監査)。
f) 詳細: 特定した値を超える推定最大容量を持つ、識別された不正情報フローチャネルの利用。

FDP_IFF.1 単純セキュリティ属性

下位階層: なし

FDP_IFF.1.1 **TSFは、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御SFP*]を実施しなければならない: [割付: *セキュリティ属性の最小数及び種別*]。**

FDP_IFF.1.2 **TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]。**

FDP_IFF.1.3 **TSFは、[割付: *追加の情報フロー制御SFP規則*]を実施しなければならない。**

FDP_IFF.1.4 **TSFは、以下の[割付: *追加のSFP能力のリスト*]を提供しなければならない。**

FDP_IFF.1.5 **TSFは、以下の規則に基づいて、情報フローを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]**

FDP_IFF.1.6 **TSFは、次の規則に基づいて、情報フローを明示的に拒否しなければならない: [割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]**

依存性: **FDP_IFC.1 サブセット情報フロー制御**
FMT_MSA.3 静的属性初期化

FDP_IFF.2 階層的セキュリティ属性

下位階層: FDP_IFF.1

FDP_IFF.2.1 TSFは、以下の種別のサブジェクト及び情報のセキュリティ属性に基づいて、[割付: *情報フロー制御SFP*]を実施しなければならない: [割付: *セキュリティ属性の最小数及び種別*]

FDP_IFF.2.2 TSFは、**セキュリティ属性の間の順序関係に基づく**以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]。

FDP_IFF.2.3 TSFは、[割付: *追加の情報フロー制御SFP*規則]を実施しなければならない。

FDP_IFF.2.4 TSFは、以下の[割付: *追加のSFP能力のリスト*]を提供しなければならない。

FDP_IFF.2.5 TSFは、以下の規則に基づいて、情報フローを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいて、明示的に情報フローを承認するための規則*]

FDP_IFF.2.6 TSFは、次の規則に基づいて、情報フローを明示的に拒否しなければならない: [割付: *セキュリティ属性に基づいて明示的に情報フローを拒否するための規則*]

FDP_IFF.2.7 **TSFは、以下の関係を任意の二つの有効な情報フロー制御セキュリティ属性に対して実施しなければならない。**

a) 二つの有効なセキュリティ属性を考えたとき、セキュリティ属性が同じであるか、一方のセキュリティ属性が他方よりも上か、またはセキュリティ属性が比較不能であるかどうかを判別する順序付け機能が存在する; 及び

b) 任意の二つの有効なセキュリティ属性を考えたとき、この二つの有効なセキュリティ属性より上かまたは同等である有効なセキュリティ属性が存在するという「最小の上限」がセキュリティ属性のセットに存在する;及び

c) 任意の二つの有効なセキュリティ属性を考えたとき、この二つの有効なセキュリティ属性より下かまたは同等である有効なセキュリティ属性が存在するという「最大の下限」が、セキュリティ属性のセットに存在する。

依存性: FDP_IFC.1 **サブセット情報フロー制御**
FMT_MSA.3 **静的属性初期化**

FDP_IFF.3 制限付き不正情報フロー

下位階層: **なし**

FDP_IFF.3.1 **TSFは、[割付: *不正情報フロー種別*]の容量を[割付: *最大容量*]に制限する[割付: *情報フロー制御SFP*]を実施しなければならない。**

依存性: **AVA_CCA.1 隠れチャネル分析**
FDP_IFC.1 サブセット情報フロー制御

FDP_IFF.4　不正情報フローの部分的排除

下位階層:　FDP_IFF.3

FDP_IFF.4.1　**TSFは、[割付: *不正情報フロー種別*]の容量を[割付: *最大容量*]に制限する[割付: *情報フロー制御SFP*]を実施しなければならない。**

FDP_IFF.4.2　TSFは、以下の種別の[割付: *不正情報フロー種別の空でないリスト*]を防止しなければならない。

依存性:　AVA_CCA.1 **隠れチャネル分析**
FDP_IFC.1 **サブセット情報フロー制御**

FDP_IFF.5　不正情報フローなし

下位階層:　FDP_IFF.4

FDP_IFF.5.1　**TSFは、[割付: *情報フロー制御SFPの名前*]を回避する不正情報フローが存在しないことを保証しなければならない。**

依存性:　**AVA_CCA.3 徹底的隠れチャネル分析**
FDP_IFC.1 **サブセット情報フロー制御**

FDP_IFF.6　不正情報フロー監視

下位階層:　**なし**

FDP_IFF.6.1　**TSFは、[割付: *不正情報フローの種別のリスト*]が[割付: *最大容量*]を超えるのを監視するために[割付: *情報フロー制御SFP*]を実施しなければならない。**

依存性:　**AVA_CCA.1 隠れチャネル分析**
FDP_IFC.1 サブセット情報フロー制御

6.7 TSF制御外からのインポート(FDP_ITC)

ファミリのふるまい

このファミリは、適切なセキュリティ属性を持ちかつ適切に保護された利用者データをTOEに導入するためのメカニズムを規定する。ここでは、インポート時の制限、望ましいセキュリティ属性の決定、及び利用者データに関連付けられたセキュリティ属性の解釈について述べる。

コンポーネントのレベル付け

このファミリは、アクセス制御と情報制御方針のためのインポートされた利用者データのセキュリティ属性の保存に対応する二つのコンポーネントから成る。

コンポーネントFDP_ITC.1 セキュリティ属性なし利用者データのインポートは、セキュリティ属性が正しく利用者データに対応し、かつオブジェクトと分離して供給されることを要求する。

コンポーネント FDP_ITC.2 セキュリティ属性付き利用者データのインポートは、セキュリティ属性が正しく利用者データに対応し、かつTSC外からインポートされる利用者データに正確で曖昧さなく関連付けられることを要求する。

管理: FDP_ITC.1、FDP_ITC.2

以下のアクションはFMT管理における管理機能と考えられる:

a) インポートに対して使用される追加の制御規則の改変。

監査: FDP_ITC.1、FDP_ITC.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 任意のセキュリティ属性を含む、利用者データの成功したインポート。
b) 基本: 任意のセキュリティ属性を含む、利用者データをインポートするすべての試み。
c) 詳細: 許可利用者によって提供される、インポートされる利用者データに対するセキュリティ属性の仕様。

FDP_ITC.1　セキュリティ属性なし利用者データのインポート

下位階層:　なし

FDP_ITC.1.1　**TSFは、SFPに従って制御され、TSC外から利用者データをインポートするときは、[割付: *アクセス制御SFP及び/または情報フロー制御SFP*]を実施しなければならない。**

FDP_ITC1.2　**TSFは、TSC外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。**

FDP_ITC.1.3　**TSFは、SFPに従って制御され、TSC外から利用者データをインポートするときは、以下の規則を実施しなければならない: [割付: *追加のインポート制御規則*]。**

依存性:　**[FDP_ACC.1 サブセットアクセス制御、または**
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.3 静的属性初期化

FDP_ITC.2　セキュリティ属性付き利用者データのインポート

下位階層:　なし

FDP_ITC.2.1　**TSFは、SFPに従って制御され、TSC外から利用者データをインポートするときは、[割付: *アクセス制御SFP及び/または 情報フロー制御SFP*]を実施しなければならない。**

FDP_ITC.2.2　**TSFは、インポートされる利用者データに関連付けられたセキュリティ属性を使用しなければならない。**

FDP_ITC2.3　**TSFは、使用されるプロトコルが、受け取るセキュリティ属性と利用者データ間の曖昧さのない関連性を備えていることを保証しなければならない。**

FDP_ITC.2.4　**TSFは、インポートされる利用者データのセキュリティ属性の解釈が、利用者データの生成元によって意図されたとおりであることを保証しなければならない。**

FDP_ITC.2.5　**TSFは、SFPに従って制御され、利用者データをTSC外からインポートするときは、以下の規則を実施しなければならない: [割付: *追加のインポート制御規則*]。**

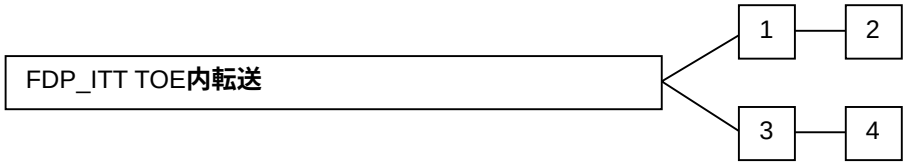
依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF間高信頼チャネル、または
FTP_TRP.1 高信頼パス]
FPT_TDC.1 TSF間基本TSFデーター貫性

6.8 TOE内転送(FDP_ITT)

ファミリのふるまい

このファミリは、利用者データが内部チャネルを通ってTOEのパーツ間で転送される場合の利用者データの保護に対応する要件を提供する。これは、利用者データが外部チャネルを通って異なるTSF間を転送されるときの利用者データ保護を提供するFDP_UCT及びFDP_UITファミリ、TSFの制御外へまたは制御外からのデータ転送に対応するFDP_ETC及びFDP_ITCと対照的と言えよう。

コンポーネントのレベル付け



FDP_ITT.1 基本内部転送保護は、利用者データが、TOEのパーツ間で転送されるときに保護されることを要求する。

FDP_ITT.2 属性による転送分離は、最初のコンポーネントに加えて、SFP関連属性の値に基づくデータの分離を要求する。

FDP_ITT.3 完全性監視は、識別された完全性誤りに対して、SFがTOEのパーツ間で転送される利用者データを監視することを要求する。

FDP_ITT.4 属性に基づく完全性監視は、SFP関連属性によって完全性監視の形態を変えられるようにすることで、三番目のコンポーネントをさらに詳しく規定する。

管理: FDP_ITT.1、FDP_ITT.2

以下のアクションはFMT管理における管理機能と考えられる:

a) TSFが、TOEの物理的に分離されたパーツ間で転送中の利用者データを保護する複数の方法を提供する場合、TSFは、使用される方法を選択できる、あらかじめ定義された役割を提供することができる。

管理: FDP_ITT.3、FDP_ITT.4

以下のアクションはFMT管理における管理機能と考えられる:

a) 完全性誤り検出時に取られるアクションの仕様は設定可能である。

監査: FDP_ITT.1、FDP_ITT.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査

対象にすべきである:

a) 最小: 使用された保護方法の識別を含む、利用者データの成功した転送。
b) 基本: 使用された保護方法と生じたいかなる誤りも含む、利用者データを転送するためのすべての試み。

監査: FDP_ITT.3、FDP_ITT.4

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:

a) 最小: 使用された完全性保護方法の識別を含む、利用者データの成功した転送。
b) 基本: 使用された完全性保護方法と生じたいかなる誤りも含む、利用者データを転送するためのすべての試み。
c) 基本: 完全性保護方法を変更しようとする不当な試み。
d) 詳細: 完全性誤り検出時にとられるアクション

FDP_ITT.1 基本内部転送保護

下位階層: なし

FDP_ITT.1.1 **TSFは、利用者データがTOEの物理的に分離されたパート間を転送される場合、その[選択: *暴露*、改変、*使用不可*]を防ぐための[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、または**
FDP_IFC.1 サブセット情報フロー制御]

FDP_ITT.2 属性による転送分離

下位階層: FDP_ITT.1

FDP_ITT.2.1 TSFは、利用者データがTOEの物理的に分離されたパート間を転送される場合、その[選択: 暴露、改変、使用不可]を防ぐための[割付: アクセス制御SFP(s)及び/または情報フロー制御SFP(s)]を実施しなければならない。

FDP_ITT.2.2 **TSFは、TOEの物理的に分離されたパート間を転送される場合、以下の値に基づいて、SFPによって制御されるデータを分離しなければならない: [割付: *分離を要求するセキュリティ属性*]。**

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]

FDP_ITT.3 完全性監視

下位階層: なし

FDP_ITT.3.1 **TSFは、以下の誤り: [割付: *完全性誤り*]について、TOEの物理的に分離されたパート間を転送される利用者データを監視するための[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。**

FDP_ITT.3.2 **データ完全性誤りの検出において、TSFは、[割付: *完全性誤りにおいてとられるアクションを特定*]しなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、または**
FDP_IFC.1 サブセット情報フロー制御]
FDP_ITT.1 基本内部転送保護

FDP_ITT.4 属性に基づく完全性監視

下位階層: FDP_ITT.3

FDP_ITT.4.1 TSFは、**以下の属性: [割付: *分離転送チャネルを要求するセキュリティ属性*]に基づいて、**以下の誤り: [割付: *完全性誤り*]について、TOEの物理的に分離されたパート間を転送される利用者データを監視するための[割付: *アクセス制御SFP及び/または情報フロー制御SFP*]を実施しなければならない。

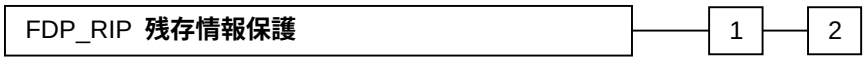
FDP_ITT.4.2 データ完全性誤りの検出において、TSFは[割付: *完全性誤りにおいてとられるアクションを特定*]しなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FDP_ITT.2 属性による転送分離

6.9 残存情報保護(FDP_RIP)

ファミリのふるまい
このファミリは、削除された情報が再びアクセスできないこと、及び新たに生成されたオブジェクトがアクセスされるべきでない情報を含まないことを保証するための必要性に対応する。このファミリは、論理的に削除されたり解放されたが、TOE中にまだ存在するかもしれない情報の保護を要求する。

コンポーネントのレベル付け



FDP_RIP.1 サブセット残存情報保護は、TSC内の定義されたオブジェクトのサブセットが、資源の割当てあるいは割当て解除において、どの資源のどの残存情報内容も利用できないことをTSFが保証することを要求する。

FDP_RIP.2 全残存情報保護は、すべてのオブジェクトが、資源の割当てあるいは割当て解除において、どの資源のどの残存情報内容も利用できないことをTSFが保証することを要求する

管理: FDP_RIP.1、FDP_RIP.2
以下のアクションはFMT管理における管理機能と考えられる:

a) いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOEにおいて設定可能にされる。

監査: FDP_RIP.1、FDP_RIP.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FDP_RIP.1 サブセット残存情報保護

下位階層: なし

FDP_RIP.1.1 **TSFは、以下のオブジェクト[選択: への*資源の割当て*、*からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト*]。**

依存性: なし

FDP_RIP.2　　全残存情報保護

下位階層:　　**FDP_RIP.1**

FDP_RIP.2.1　　TSFは、**すべてのオブジェクト**[selection選択: への*資源の割当て*、*からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

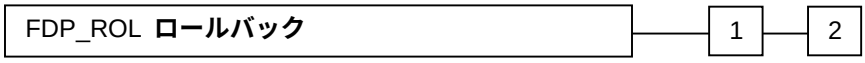
依存性:　　**なし**

6.10 ロールバック(FDP_ROL)

ファミリのふるまい

ロールバック操作とは、時間間隔など、なんらかの制限によって境界を決められた、最後の操作あるいは一連の操作をもとどおりにし、以前の分かっている状態へ戻すことを意味する。ロールバックは、利用者データの完全性を保持するために一つの操作または一連の操作の影響を元に戻す能力を提供する。

コンポーネントのレベル付け



FDP_ROL.1 基本ロールバックは、定義された境界内で、限られた数の操作をロールバックまたは元に戻す必要性に対応する。

FDP_ROL.2 高度ロールバックは、定義された境界内で、すべての操作をロールバックまたは元に戻す必要性に対応する。

管理: FDP_ROL.1、FDP_ROL.2

以下のアクションはFMT管理における管理機能と考えられる:

a) ロールバック実行が許される境界限度は、TOE内の設定可能項目にし得る。
b) ロールバック操作を実行する許可は、明確に定義された役割に制限できる。

監査: FDP_ROL.1、FDP_ROL.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: すべての成功ロールバック操作。
b) 基本: ロールバック操作をしようとするすべての試み。
c) 詳細: ロールバックされる操作の種別の識別を含む、ロールバック操作をしようとするすべての試み。

FDP_ROL.1 基本ロールバック

下位階層: なし

FDP_ROL.1.1 **TSFは、[割付: *オブジェクトのリスト*]に対する[割付: *操作のリスト*]のロールバックを許可するために、[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。**

FDP_ROL.1.2 **TSFは、[割付: *ロールバック実行が許される境界限界*]内で操作がロールバックされることを許可しなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]**

FDP_ROL.2 高度ロールバック

下位階層: FDP_ROL.1

FDP_ROL.2.1 TSFは、[割付: *オブジェクトのリスト*]に対する**すべての操作**のロールバックを許可するために、[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。

FDP_ROL.2.2 TSFは、[割付: *ロールバックを実行できる境界限界*]内で操作がロールバックされることを許可しなければならない。

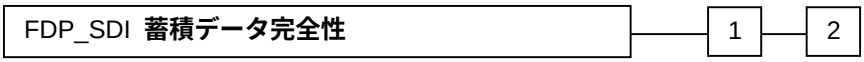
依存性: [FDP_ACC.1 **サブセットアクセス制御、または**
FDP_IFC.1 **サブセット情報フロー制御**]

6.11 蓄積データ完全性(FDP_SDI)

ファミリのふるまい

このファミリは、TSC内部で蓄積されている間の利用者データ保護に対応する要件を提供する。完全性誤りは、メモリや記憶装置の利用者データに影響を及ぼすかもしれない。このファミリは、TOE内転送時の完全性誤りから利用者データを保護するFDP_ITT TOE内転送とは異なるものである。

コンポーネントのレベル付け



FDP_SDI .1 蓄積データ完全性監視では、識別された完全性誤りに対して、TSC内部に蓄積された利用者データをSFが監視することを要求する。

FDP_SDI.2 蓄積データ完全性監視及びアクションでは、誤り検出の結果として取られるアクションを考慮することによって、前述のコンポーネントに追加能力を加える。

管理: FDP_SDI.1

このコンポーネントについて予見される管理アクティビティはない。

管理: FDP_SDI.2

以下のアクションはFMT管理における管理機能と考えられる:

a) 完全性誤り検出においてとられるアクションは設定可能である。

監査: FDP_SDI.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 利用者データ完全性チェックの成功した試み(検査結果の表示を含む)。
b) 基本: 利用者データ完全性チェックのすべての試み(実行されたときは、検査結果の表示を含む)。
c) 詳細: 生じた完全性誤りの種別。

監査: FDP_SDI.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 利用者データ完全性チェックの成功した試み(検査結果の表示を含む)。
b) 基本: 利用者データ完全性チェックのすべての試み(実行されたときは、検査結果の表示を含む)。

c) 詳細: 生じた完全性誤りの種別。
d) 詳細: 完全性誤り検出においてとられたアクション。

FDP_SDI.1 蓄積データ完全性監視

下位階層: なし

FDP_SDI.1.1 **TSFは、すべてのオブジェクトにおける[割付: *完全性誤り*]について、以下の属性に基づき、TSC内の蓄積された利用者データを監視しなければならない: [割付: *利用者データ属性*]。**

依存性: **なし**

FDP_SDI.2 蓄積データ完全性監視及びアクション

下位階層: FDP_SDI.1

FDP_SDI.2.1 TSFは、すべてのオブジェクトにおける[割付: *完全性誤り*]について、以下の属性に基づき、TSC内の蓄積された利用者データを監視しなければならない: [割付: *利用者データ属性*]。

FDP_SDI.2.2 **データ完全性誤り検出時に、TSFは[割付: *とられるアクション*]を行なわねばならない。**

依存性: **なし**

6.12 TSF間利用者データ機密転送保護(FDP_UCT)

ファミリのふるまい

このファミリは、利用者データが外部チャネルを用いて別のTOEあるいは別のTOEの利用者間で転送されるとき、その利用者データの機密を保証する要件を定義する。

コンポーネントのレベル付け

FDP_UCT TSF間利用者データ機密転送保護	1

FDP_UCT.1 基本データ交換機密において、目標は、通過する利用者データの暴露からの保護を提供することである。

管理: FDP_UCT.1

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_UCT.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報。
b) 基本: データ交換メカニズムを使用しようとした、非許可利用者あるいはサブジェクトの識別情報。
c) 詳細: 送信あるいは受信された利用者データの識別に利用可能な名前、あるいはそれ以外のインデックス情報の参照。これはその情報に関連するセキュリティ属性を含むことができる。

FDP_UCT.1 基本データ交換機密

下位階層: なし

FDP_UCT.1.1 TSFは、不当な暴露から保護した様態でオブジェクトの[選択: *送信*、*受信*]を行なえるようにするために、[割付: *アクセス制御SFP(s)及び/あるいは情報フロー制御SFP(s)*]を実施しなければならない。

依存性: [FTP_ITC.1 TSF間高信頼チャネル、または
FTP_TRP.1 高信頼パス]
[FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]

6.13 TSF間利用者データ完全性転送保護(FDP_UIT)

ファミリのふるまい

このファミリは、TSFと他の高信頼IT製品間を通過する利用者データに対し、完全性を提供し、かつ検出可能な誤りから回復するための要件を定義する。最低限、このファミリは、改変に対する利用者データの完全性を監視する。さらに、このファミリは、検出された完全性誤りを訂正する各種の方法をサポートする。

コンポーネントのレベル付け

FDP_UIT.1 データ交換完全性は、送信される利用者データの、改変、削除、挿入、及びリプレイ誤りの検出に対応する。

FDP_UIT.2 発信側データ交換回復は、発信側高信頼IT製品の助けを借りた、受信側TSFによるオリジナル利用者データの回復に対応する。

FDP_UIT.3 着信側データ交換回復は、発信側高信頼IT製品の助けを借りずに、受信側TSF自身によるオリジナルの利用者データの回復に対応する。

管理: FDP_UIT.1、FDP_UIT.2、FDP_UIT.3

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_UIT.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報。
b) 基本: データ交換メカニズムの使用を試みる、不当な利用者あるいはサブジェクトの識別情報。
c) 基本: 送信あるいは受信された利用者データの識別に利用できる名前、あるいはそれ以外のインデックス情報の参照。これは利用者データに関連するセキュリティ属性を含むことができる。
d) 基本: 利用者データの送信を妨害する識別された試み。
e) 詳細: 送信された利用者データに対する、検出された改変の種別及び/あるいは影響。

監査: FDP_UIT.2, FDP_UIT.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報(identity)。
b) 最小: 検出された誤りの型を含む、誤りからの成功した回復。
c) 基本: データ交換メカニズムの使用を試みる、不当な利用者あるいはサブジェクトの識別情報(identity)。
d) 基本: 送信あるいは受信された利用者データの識別に利用できる名前、あるいはそれ以外のインデックス情報の参照。これは利用者データに関連するセキュリティ属性を含むことができる。
e) 基本: 利用者データの送信を妨害する識別された試み。
f) 詳細: 送信された利用者データに対する、検出された改変の種別及び/あるいは影響。

FDP_UIT.1 データ交換完全性

下位階層: なし

FDP_UIT.1.1 **TSFは、利用者データを[選択: *改変*、*消去*、*挿入*、*リプレイ*]誤りから保護した形で[選択: *送信*、*受信*]できるようにするために、[割付: *アクセス制御SFP(s)及び/あるいは情報フロー制御SFP(s)*]を実施しなければならない。**

FDP_UIT.1.2 **TSFは、利用者データ受信において、[選択: : *改変*、*消去*、*挿入*、*リプレイ*]が生じたかどうかを判定できなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF間高信頼チャネル、または
FTP_TRP.1 高信頼パス]**

FDP_UIT.2 発信側データ交換回復

下位階層: なし

FDP_UIT.2.1 **TSFは、発信側高信頼IT製品の助けを借りて[割付: *回復可能誤りリスト*]から回復できるようにするために、[割付: *アクセス制御SFP(s)及び/あるいは情報フロー制御SFP(s)*]を実施しなければならない。**

依存性: [FDP_ACC.1 **サブセットアクセス制御、または**

FDP_IFC.1 **サブセット情報フロー制御**]
FDP_UIT.1 データ交換完全性
FTP_ITC.1 TSF間高信頼チャネル

FDP_UIT.3 着信側データ交換回復

下位階層: FDP_UIT.2

FDP_UIT.3.1 TSFは、**発信側高信頼IT製品の助けを借りずに**[割付: *回復可能誤りリスト*]から回復できるようにするために、[割付: *アクセス制御SFP(s)及び/または情報フロー制御SFP(s)*]を実施しなければならない。

依存性: [FDP_ACC.1 **サブセットアクセス制御、または**
FDP_IFC.1 **サブセット情報フロー制御**]
FDP_UIT.1 **データ交換完全性**
FTP_ITC.1 TSF**間高信頼チャネル**

7 クラスFIA: 識別と認証

このクラスのファミリは、請求された利用者の識別情報を確立し検証するための機能に対する要件に対応する。

識別と認証は、利用者が適切なセキュリティ属性(例えば、識別情報、グループ、役割、セキュリティまたは完全性レベル)に関連付けられることを保証することが要求される。

曖昧さのない許可利用者の識別と、利用者及びサブジェクトとセキュリティ属性の正しい関連付けは、意図したセキュリティ方針を実施するために重要である。このクラスのファミリは、利用者の識別情報の判定と検証、TOEとやり取りするための利用者の権限の判定、及び各々の許可利用者に対するセキュリティ属性の正しい関連付けを取り扱う。要件の他のクラス(例えば、利用者データ保護、セキュリティ監査)は、それが有効となるためには、利用者の正確な識別と認証に依存する。

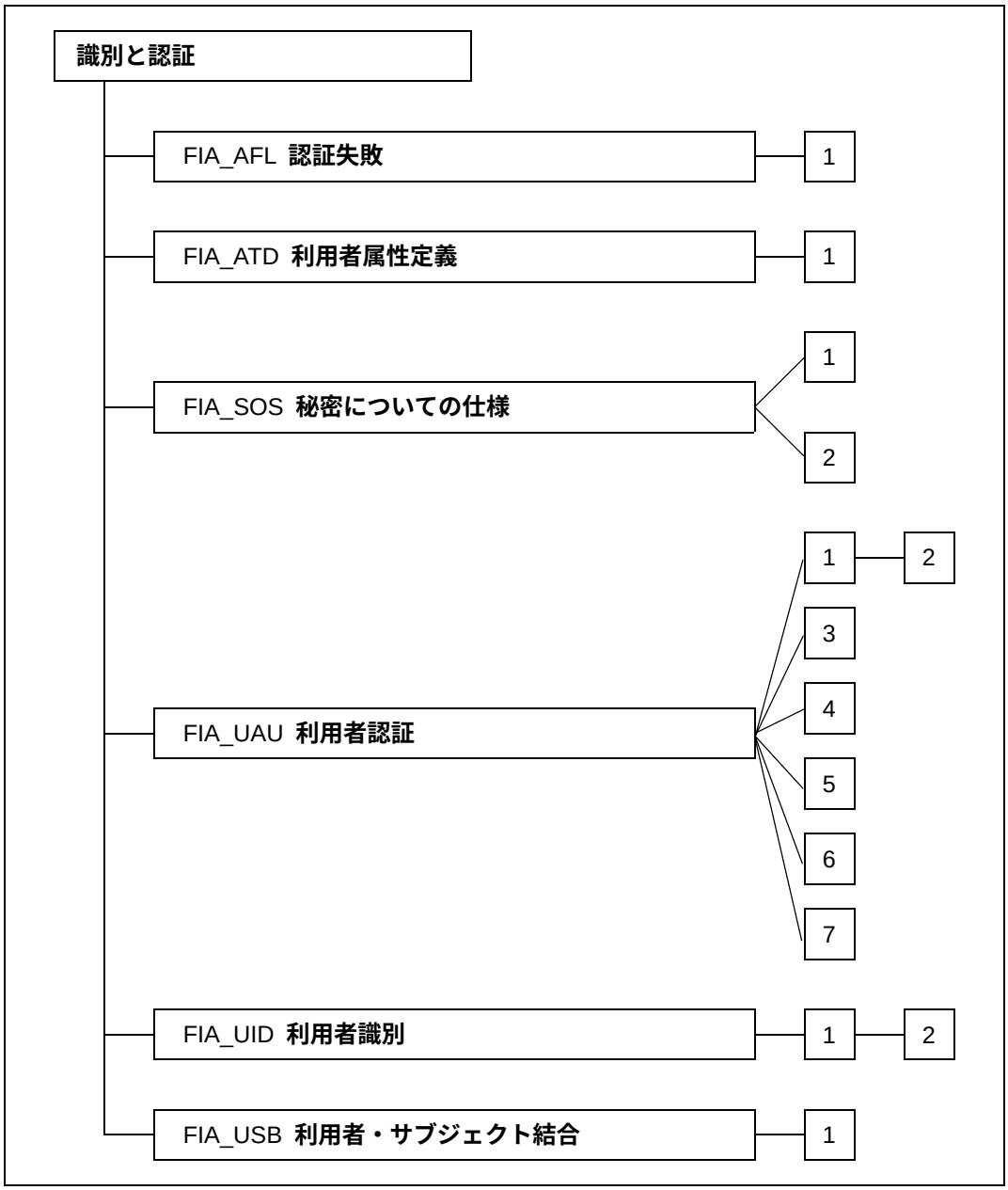


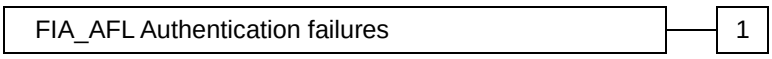
図7.1 - **識別と認証クラスのコンポーネント構成**

7.1 認証失敗(FIA_AFL)

ファミリのふるまい

このファミリは、不成功の認証試行数についての値と、認証試行の失敗におけるTSFアクションの定義に対する要件を含む。パラメタは、失敗した認証の数と時間の閾値を含むが、それだけに限定されない。

コンポーネントのレベル付け



FIA_AFL.1は、利用者の不成功の認証試行が特定した数になったあと、セション確立プロセスを終了できることを要求する。また、セション確立プロセスの終了後、その試行が行われた利用者アカウントあるいはエントリポイント(例えば、ワークステーション)を、管理者定義の条件になるまでTSFが無効にできることも要求される。

管理: FIA_AFL.1

以下のアクションはFMTにおける管理機能と考えられる:

a) 不成功の認証試行に対する閾値の管理
b) 認証失敗の事象においてとられるアクションの管理

監査: FIA_AFL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 **TSFは、[割付: *認証事象のリスト*]に関して、[割付: *回数*]回の不成功認証試行が生じたときを検出しなければならない。**

FIA_AFL.1.2 **不成功の認証試行が定義した回数に達するか上回ったとき、TSFは、[割付: アクションのリスト]をしなければならない。**

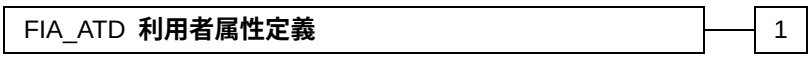
依存性: **FIA_UAU.1 認証のタイミング**

7.2 利用者属性定義(FIA_ATD)

ファミリのふるまい

すべての許可利用者は、利用者識別情報以外に、TSPを実施するために使われるセキュリティ属性のセットを持つかもしれない。このファミリはセキュリティ属性を利用者に関連付けるための要件を定義するものであり、TSPを支えるものとして必要とされる。

コンポーネントのレベル付け



FIA_ATD.1 利用者属性定義は、各利用者に対する利用者セキュリティ属性を個別に管理できるようにする。

管理: FIA_ATD.1

以下のアクションはFMTにおける管理機能と考えられる:

a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。

監査: FIA_ATD.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 **TSFは、個々の利用者に属する以下のセキュリティ属性のリスト[割付: *セキュリティ属性のリスト*]を維持しなければならない。**

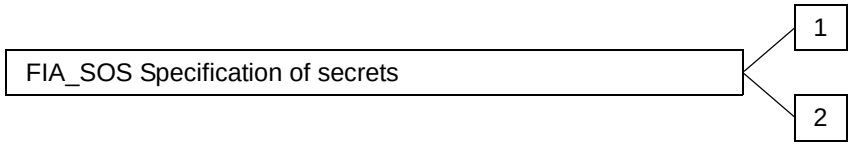
依存性: **なし**

7.3 秘密についての仕様(FIA_SOS)

ファミリのふるまい

このファミリは、定義された尺度を満たすため、提供された秘密と生成された秘密について定義される品質尺度を実施するメカニズムに対する要件を定義する。

コンポーネントのレベル付け



FIA_SOS.1 秘密の検証は、秘密が定義された品質尺度に合っていることをTSFが検証することを要求する。

FIA_SOS.2 TSF秘密生成は、定義された品質尺度に合った秘密をTSFが生成できることを要求する。

管理: FIA_SOS.1

以下のアクションはFMTにおける管理機能と考えられる:

a) 秘密の検証に使用される尺度の管理。

管理: FIA_SOS.2

以下のアクションはFMTにおける管理機能と考えられる:

a) 秘密の生成に使用される尺度の管理。

監査: FIA_SOS.1、FIA_SOS.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFによる、テストされた秘密の拒否;
b) 基本: TSFによる、テストされた秘密の拒否または受け入れ;
c) 詳細: 定義された品質尺度に対する変更の識別。

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSFは、秘密が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。

依存性: **なし**

FIA_SOS.2 TSF秘密生成

下位階層: なし

FIA_SOS.2.1 **TSFは、[割付: *定義された品質尺度*]に合致する秘密を生成するメカニズムを提供しなければならない。**

FIA_SOS.2.2 **TSFは、[割付: *TSF機能のリスト*]に対し、TSF生成の秘密の使用を実施できなければならない。**

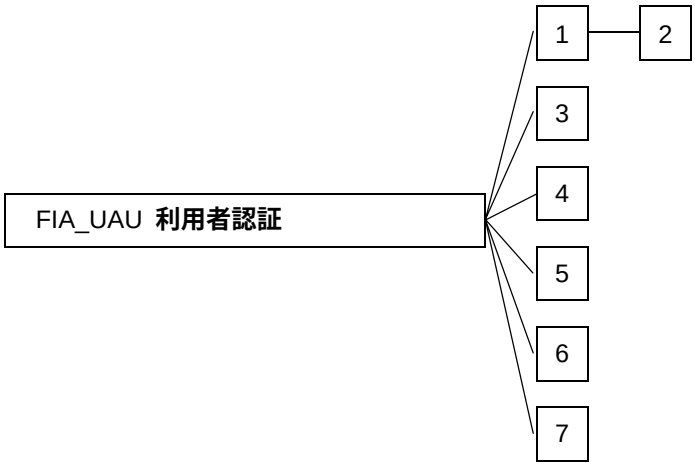
依存性: **なし**

7.4 利用者認証(FIA_UAU)

ファミリのふるまい

このファミリは、TSFがサポートされる利用者認証メカニズムの種別を定義する。またこのファミリは、利用者認証メカニズムが基づくべき要求された属性も定義する。

コンポーネントのレベル付け



FIA_UAU.1 認証のタイミングは、利用者の識別情報の認証の前に、利用者があるアクションを実行することを認める。

FIA_UAU.2 アクション前の利用者認証は、TSFがアクションを許可する前に、利用者が自分自身を認証することを要求する。

FIA_UAU.3 偽造されない認証は、偽造やコピーされたことのある認証データの使用を、認証メカニズムが検出及び防止できることを要求する。

FIA_UAU.4 単一使用認証メカニズムは、単一使用の認証データで動作する認証メカニズムを要求する。

FIA_UAU.5 複数の認証メカニズムは、特定の事象に対して利用者識別情報を認証するために、異なる認証メカニズムが提供され、使用されることを要求する。

FIA_UAU.6 再認証は、利用者の再認証を必要とする事象を特定する能力を要求する。

FIA_UAU.7 保護された認証フィードバックは、認証の間、限定されたフィードバック情報だけが利用者に提供されることを要求する。

管理: FIA_UAU.1
以下のアクションはFMTにおける管理機能と考えられる:
管理者による認証データの管理;
関係する利用者による認証データの管理;
利用者が認証される前にとられるアクションのリストを管理すること。

管理: FIA_UAU.2
以下のアクションはFMTにおける管理機能と考えられる。
管理者による認証データの管理;
このデータに関係する利用者による認証データの管理。

管理: FIA_UAU.3、 FIA_UAU.4、 FIA_UAU.7
予見される管理アクティビティはない。

管理: FIA_UAU.5
以下のアクションはFMTにおける管理機能と考えられる。
認証メカニズムの管理;
認証に対する規則の管理。

管理: FIA_UAU.6
以下のアクションはFMTにおける管理機能と考えられる。
許可管理者が再認証を要求できる場合、管理に再認証要求を含める。

監査: FIA_UAU.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれている場合、以下のアクションを監査対象にすべきである。
最小: 認証メカニズムの不成功になった使用;
基本: 認証メカニズムのすべての使用。
詳細: 利用者認証以前に行われたすべてのTSF調停アクション

監査: FIA_UAU.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
最小: 認証メカニズムの不成功になった使用;
基本: 認証メカニズムのすべての使用。

監査: FIA_UAU.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
最小: 不正な認証データの検出;
基本: 不正なデータについて、直ちにとられたすべての手段とチェックの結果。

監査: FIA_UAU.4
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 認証データを再使用する試み。

監査: FIA_UAU.5
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 認証の最終決定;
b) 基本: 最終決定で共に用いられた、各々の稼動したメカニズムの結果。

監査: FIA_UAU.6
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 再認証の失敗;
b) 基本: すべての再認証試行。

監査: FIA_UAU.7
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FIA_UAU.1 認証のタイミング

下位階層: なし

FIA_UAU.1.1 **TSFは、利用者が認証される前に利用者を代行して行われる[割付: *TSF調停アクションのリスト*]を許可しなければならない。**

FIA_UAU.1.2 **TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1 TSFは、その利用者を代行する**他のTSF調停アクション**を許可する前に、各利用者に認証が成功することを要求しなければならない。
(翻訳者注釈: 原文は上記のとおりであるが、これではFIA_UAU.1.2と

同一の要件となって、上位階層としては不適当である。正しくは、「TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に**自分自身を認証**することを要求しなければならない。」であるべきと思われる。)

依存性: FIA_UID.1 **識別のタイミング**

FIA_UAU.3 偽造されない認証

下位階層: なし

FIA_UAU.3.1 **TSFは、TSFの利用者によって偽造された認証データの使用を[選択: *検出または防止*]しなければならない。**

FIA_UAU.3.2 **TSFは、TSFの他の利用者からコピーされた認証データの使用を[選択: *検出または防止*]しなければならない。**

依存性: **なし**

FIA_UAU.4 単一使用認証メカニズム

下位階層: なし

FIA_UAU.4.1 **TSFは、[割付: *識別された認証メカニズム*]に関係する認証データの再使用を防止しなければならない。**

依存性: **なし**

FIA_UAU.5 複数の認証メカニズム

下位階層: なし

FIA_UAU.5.1 **TSFは、利用者認証をサポートするため、[割付: *複数の認証メカニズムのリスト*]を提供しなければならない。**

FIA_UAU.5.2 **TSFは、[割付: *複数の認証メカニズムがどのように認証を提供するかを記述する規則*]に従って、利用者が主張する識別情報を認証しなければならない。**

依存性: **なし**

FIA_UAU.6　再認証

下位階層:　なし

FIA_UAU.6.1　**TSFは、条件[割付: *再認証が要求される条件のリスト*]のもとで利用者を再認証しなければならない。**

依存性:　**なし**

FIA_UAU.7　保護された認証フィードバック

下位階層:　なし

FIA_UAU.7.1　**TSFは、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。**

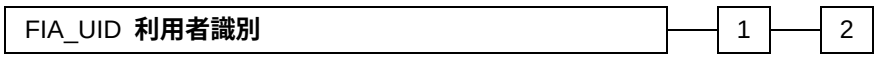
依存性:　FIA_UAU.1 **認証のタイミング**

7.5 利用者識別(FIA_UID)

ファミリのふるまい

このファミリは、利用者が自分自身を識別することが要求されねばならない条件を定義するものであり、この識別は、TSFが調停しかつ利用者認証を必要とする他のすべてのアクションの前に行われる。

コンポーネントのレベル付け



FIA_UID.1 識別のタイミングは、利用者がTSFによって識別される前に利用者があるアクションを実行することを認める。

FIA_UID.2 アクション前の利用者識別は、TSFがなんらかのアクションを認める前に、利用者が自分自身を識別することを要求する。

管理: FIA_UID.1

以下のアクションはFMTにおける管理機能と考えられる:

a) 利用者識別情報の管理;
b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。

管理: FIA_UID.2

以下のアクションはFMTにおける管理機能と考えられる:

a) 利用者識別情報の管理。

監査: FIA_UID.1、FID_UID.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用;
b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。

FIA_UID.1 識別のタイミング

下位階層: なし

FIA_UID.1.1 TSFは、利用者が識別される前に利用者を代行して実行される[割付: *TSF調停アクションのリスト*]を許可しなければならない。

FIA_UID.1.2 **TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。**

依存性: **なし**

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1 TSFは、その利用者を代行する**他のTSF調停アクション**を許可する前に、各利用者に自分自身を識別することを要求しなければならない。
(翻訳者注: 原文は上記のとおりであるが、FAI_UID.1.2からの変更部分としては適切でない。正しくは、「他のTSF調停アクション」ではなく、「自分自身を識別」の部分がボールド表記になるべきと思われる。)

依存性: **なし**

7.6 利用者・サブジェクト結合(FIA_USB)

ファミリのふるまい

認証された利用者は、TOEを使用するため、通常はサブジェクトを動作させる。利用者のセキュリティ属性は(全面的または部分的に)このサブジェクトに関連付けられる。このファミリは、利用者のセキュリティ属性と利用者を代行して動作するサブジェクトとの関連付けを生成し維持するための要件を定義する。

コンポーネントのレベル付け

FIA_USB.1 利用者・サブジェクト結合は、利用者のセキュリティ属性と利用者を代行して動作するサブジェクトとの関連付けの維持を要求する。

管理: FIA_USB.1

以下のアクションはFMTにおける管理機能と考えられる:

a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。

監査: FIA_USB.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。
b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1 **TSFは、適切な利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。**

依存性: **FIA_ATD.1 利用者属性定義**

8 クラスFMT: セキュリティ管理

このクラスは、TSFのいくつかの側面(セキュリティ属性、TSFデータと機能)の管理を特定することを意図したものである。実施権限(capability)の分離のような、異なる管理の役割とこれらの相互の影響を特定することができる。

このクラスはいくつかの目的を持つ:

a) TSFデータの管理、例えばバナーはこれに含まれる;

b) セキュリティ属性の管理、例えばアクセス制御リスト、実施権限リスト(capability list)、はこれに含まれる;

c) TSFの機能の管理、例えば機能の選択、TSFのふるまいに影響を与える規則や条件はこれに含まれる;

d) セキュリティ役割の定義。

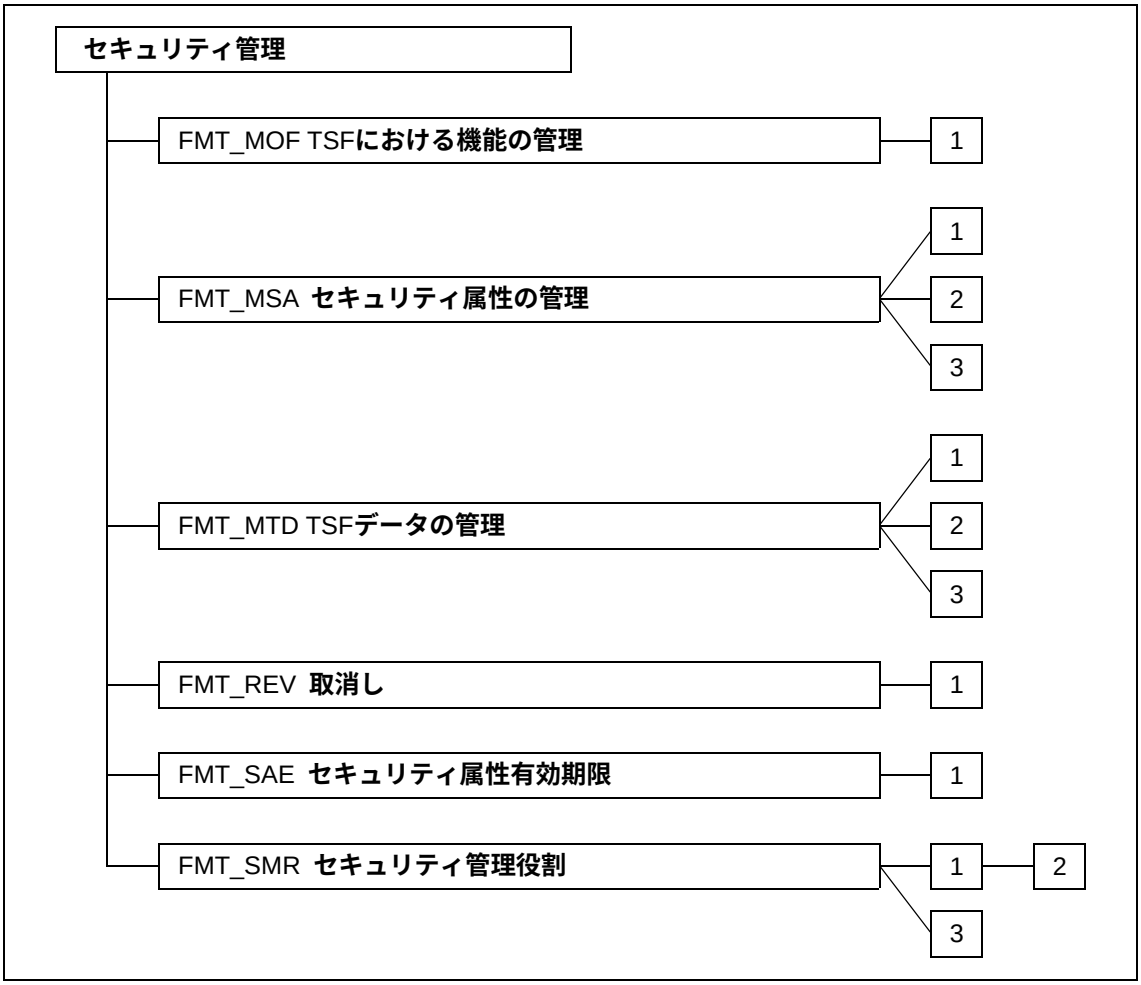


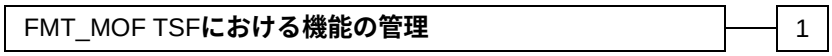
図8.1 - **セキュリティ管理クラスのコンポーネント構成**

8.1 TSFにおける機能の管理(FMT_MOF)

ファミリのふるまい

このファミリは、許可利用者がTSFにおける機能の管理を統括できるようにする。TSFにおける機能の例として、監査機能、多重認証機能がある。

コンポーネントのレベル付け



FMT_MOF.1 セキュリティ機能のふるまいの管理は、許可利用者(役割)が、規則を使用するか、あるいは管理可能にし得る特定の条件を持つ、TSFにおける機能のふるまいを管理することを許可する。

管理: FMT_MOF.1

以下のアクションはFMT管理における管理機能と考えられる:

a) TSFの機能と相互に影響を及ぼし得る役割のグループを管理すること;

監査: FMT_MOF.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: TSFの機能のふるまいにおけるすべての改変。

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1 **TSFは、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。**

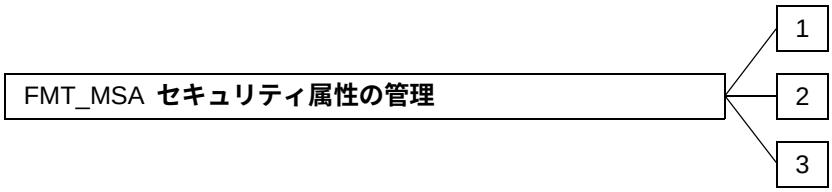
依存性: **FMT_SMR.1 セキュリティ役割**

8.2 セキュリティ属性の管理(FMT_MSA)

ファミリのふるまい

このファミリは、許可利用者がセキュリティ属性の管理を統括することを許可する。この管理には、セキュリティ属性を見たり改変したりする実施権限を含められる。

コンポーネントのレベル付け



FMT_MSA.1 セキュリティ属性の管理は、許可利用者(役割)が、特定されたセキュリティ属性を管理することを認める。

FMT_MSA.2 セキュアなセキュリティ属性は、セキュリティ属性に割り付けられた値が、セキュアな状態に関して有効であることを保証する。

FMT_MSA.3 静的属性初期化は、セキュリティ属性のデフォルト値が、本来の性質として適切に許可的(permissive)あるいは制限的(restrictive)のどちらかになっていることを保証する。

管理: FMT_MSA.1

以下のアクションはFMT管理における管理機能と考えられる:

a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。

管理: FMT_MSA.2

このコンポーネントについて予見される追加の管理アクティビティはない。

管理: FMT_MSA.3

以下のアクションはFMT管理における管理機能と考えられる:

a) 初期値を特定できる役割のグループを管理すること;
b) 所定のアクセス制御SFPに対するデフォルト値の許可的あるいは制限的設定を管理すること。

監査: FMT_MSA.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: セキュリティ属性の値の改変すべて。

監査: FMT_MSA.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: セキュリティ属性に対して提示され、拒否された値すべて;
b) 詳細: セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。

監査: FMT_MSA.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。
b) 基本: セキュリティ属性の初期値の改変すべて。

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1 **TSFは、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付: *その他の操作*]]をする能力を[割付: *許可された識別された役割*]に制限するために[割付: *アクセス制御SFP*、*情報フロー制御SFP*]を実施しなければならない。**

依存性: **[FDP_ACC.1 サブセットアクセス制御または**
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.2 セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1 **TSFは、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。**

依存性: **ADV_SPM.1 非形式的TOEセキュリティ方針モデル**
[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MSA.3　静的属性初期化

下位階層:　なし

FMT_MSA.3.1 **TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択:** ***制限的、許可的、その他の特性*****]デフォルト値を与える[割付:** ***アクセス制御SFP、情報フロー制御SFP*****]を実施しなければならない。**

FMT_MSA.3.2　**TSFは、オブジェクトや情報が生成されるとき、[割付:** ***許可された識別された役割*****]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。**

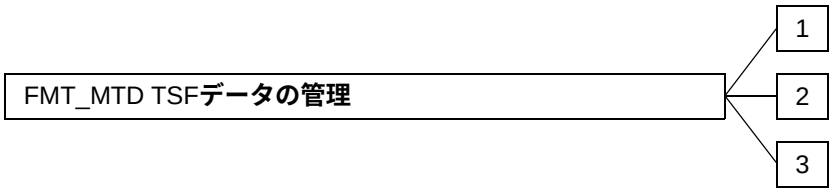
依存性:　**FMT_MSA.1 セキュリティ属性の管理**
FMT_SMR.1 セキュリティの役割

8.3 TSF**データの管理**(FMT_MTD)

ファミリのふるまい

このファミリは、許可利用者(役割)がTSFデータの管理を統括することを許可する。TSFデータの例として、監査情報、クロック、システム構成、その他のTSF設定パラメタがある。

コンポーネントのレベル付け



FMT_MTD.1 TSFデータの管理は、許可利用者がTSFデータを管理することを許可する。

FMT_MTD.2 TSFデータにおける限界値の管理は、TSFデータが限界値に達するか超過した場合にとられるアクションを特定する。

FMT_MTD.3 セキュアなTSFデータは、TSFデータに割り付けられた値がセキュアな状態に関して有効であることを保証する。

管理: FMT_MTD.1

以下のアクションはFMT管理における管理機能と考えられる:

a) TSFデータと相互に影響を及ぼし得る役割のグループを管理すること。

管理: FMT_MTD.2

以下のアクションはFMT管理における管理機能と考えられる:

a) TSFデータにおける限界値に影響を及ぼし得る役割のグループを管理すること。

管理: FMT_MTD.3

このコンポーネントについて、予見される追加の管理アクティビティはない。

監査: FMT_MTD.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: TSFデータの値のすべての改変。

監査: FMT_MTD.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクション

を監査対象にすべきである:

a) 基本: TSFデータにおける限界値のすべての改変;

b) 基本: 限界値違反が起きたときにとられるアクションにおけるすべての改変。

監査: FMT_MTD.3

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFデータのすべての拒否された値。

FMT_MTD.1 TSFデータの管理

下位階層: なし

FMT_MTD.1.1 **TSFは、[割付: *TSFデータのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、[割付: *その他の操作*]]する能力を[割付: *許可された識別された役割*]に制限しなければならない。**

依存性: **FMT_SMR.1 セキュリティ役割**

FMT_MTD.2 TSFデータにおける限界値の管理

下位階層: なし

FMT_MTD.2.1 **TSFは、[割付: *TSFデータのリスト*]に限界値を指定することを[割付: *許可された識別された役割*]に制限しなければならない。**

FMT_MTD.2.2 **TSFは、TSFデータが指示された限界値に達するか、それを超えた場合、以下のアクションをとらねばならない: [割付: *とられるアクション*]。**

依存性: **FMT_MTD.1 TSFデータの管理**
FMT_SMR.1 セキュリティ役割

FMT_MTD.3 セキュアなTSFデータ

下位階層: なし

FMT_MTD.3.1 **TSFは、TSFデータとしてセキュアな値だけが受け入れられることを保証しなければならない。**

依存性: **ADV_SPM.1 非形式的TOEセキュリティ方針モデル**

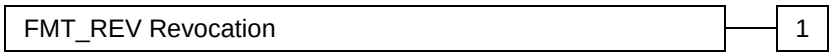
FMT_MTD.1 TSFデータの管理

8.4 取消し(FMT_REV)

ファミリのふるまい

このファミリは、TOE内のいろいろなエンティティのセキュリティ属性の取消しに対応する。

コンポーネントのレベル付け



FMT_REV.1 取消しは、時間上のある点で実施されるセキュリティ属性の取消しを規定する。

管理: FMT_REV.1

以下のアクションはFMT管理における管理機能と考えられる:

a) セキュリティ属性の取消しを実施できる役割のグループを管理すること;
b) 取消し可能な利用者、サブジェクト、オブジェクト及びその他の資源のリストを管理すること;
c) 取消し規則を管理すること。

監査: FMT_REV.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: セキュリティ属性取消し不成功;
b) 基本: セキュリティ属性を取り消そうとするすべての試み。

FMT_REV.1 取消し

下位階層: なし

FMT_REV.1.1 **TSFは、TSCの範囲内で、[選択: *利用者*、*サブジェクト*、*オブジェクト*、*その他追加の資源*]に関連したセキュリティ属性を取り消す能力を、[割付: *許可された識別された役割*]に制限しなければならない。**

TSF_REV.1.2 **TSFは、規則[割付: *取消し規則の明細*]を実施しなければならない。**

依存性: **FMT_SMR.1 セキュリティ役割**

8.5 セキュリティ属性有効期限(FMT_SAE)

ファミリのふるまい

このファミリは、セキュリティ属性の有効性に対して時間制限を実施する能力に対応する。

コンポーネントのレベル付け

FMT_SAE.1 時限付き許可は、許可利用者が特定のセキュリティ属性について有効期限の時間を特定するための権限を提供する。

管理: FMT_SAE.1

以下のアクションはFMT管理における管理機能と考えられる:

a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること;
b) 有効期限の時間が過ぎたときにとられるアクション。

監査: FMT_SAE.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 属性に対する有効期限の時間の特定;
b) 基本: 属性の有効期限切れによってとられるアクション。

FMT_SAE.1 時限付き許可

下位階層: なし

FMT_SAE.1.1 **TSFは、[割付: *有効期限がサポートされるはずのセキュリティ属性のリスト*]に対する有効期限の時間を特定する能力を、[割付: *許可された識別された役割*]に制限しなければならない。**

FMT_SAE.1.2 **これらセキュリティ属性の各々について、TSFは、示されたセキュリティ属性に対する有効期限の時間後、[割付: *各々のセキュリティ属性に対してとられるアクションのリスト*]を行えなければならない。**

依存性: **FMT_SMR.1 セキュリティ役割**
FPT_STM.1 高信頼タイムスタンプ

8.6 セキュリティ管理役割(FMT_SMR)

ファミリのふるまい

このファミリは、利用者への異なる役割の割付けの管理を意図している。セキュリティ管理に関するこれらの役割の実施権限は、このクラスの他のファミリで記述される。

コンポーネントのレベル付け

FMT_SMR.1 セキュリティ役割は、TSFが認識するセキュリティに関する役割を特定する。

FMT_SMR.2 セキュリティ役割における制限は、役割の特定に加えて、役割間の関係を制御する規則があることを特定する。

FMT_SMR.3 負わせる役割は、TSFに、役割を負わせるという明示的な要求が与えられることを要求する。

管理: FMT_SMR.1

以下のアクションはFMT管理における管理機能と考えられる:

a) 役割の一部をなす利用者のグループの管理。

管理: FMT_SMR.2

以下のアクションはFMT管理における管理機能と考えられる:

a) 役割の一部をなす利用者のグループを管理すること;
b) 役割が満たさなければならない条件を管理すること。

管理: FMT_SMR.3

このコンポーネントに対して予見される追加の管理アクティビティはない。

監査: FMT_SMR.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 役割の一部をなす利用者のグループに対する改変;
b) 詳細: 役割の権限の使用すべて。

監査: FMT_SMR.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 役割の一部をなす利用者のグループに対する改変;
b) 最小: 役割に対して与えられた条件のために成功しなかった、その役割を使用する試み;
c) 詳細: 役割の権限の使用すべて。

監査: FMT_SMR.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 役割を負わせる明示的な要求。

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 **TSFは、役割[割付: *許可された識別された役割*]を維持しなければならない。**

FMT_SMR.1.2 **TSFは、利用者を役割に関連づけなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FMT_SMR.2 セキュリティ役割における制限

下位階層: **FMT_SMR.1**

FMT_SMR.2.1 TSFは、役割[割付: *許可された識別された役割*]を維持しなければならない。

FMT_SMR.2.2 TSFは、利用者を役割に関連付けなければならない。

FMT_SMR.2.3 **TSFは、条件[割付: *異なる役割に対する条件*]が満たされていることを保証しなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FMT_SMR.3 負わせる役割

下位階層: なし

FMT_SMR.3.1 **TSFは、以下の役割を負わせるために、明示的な要求をしなければならない: [割付: *役割*]。**

依存性: **FMT_SMR.1 セキュリティ役割**

9 クラスFPR: プライバシー

このクラスは、プライバシー要件を含む。これらの要件は、他の利用者による識別情報の露見と悪用から利用者を保護する。

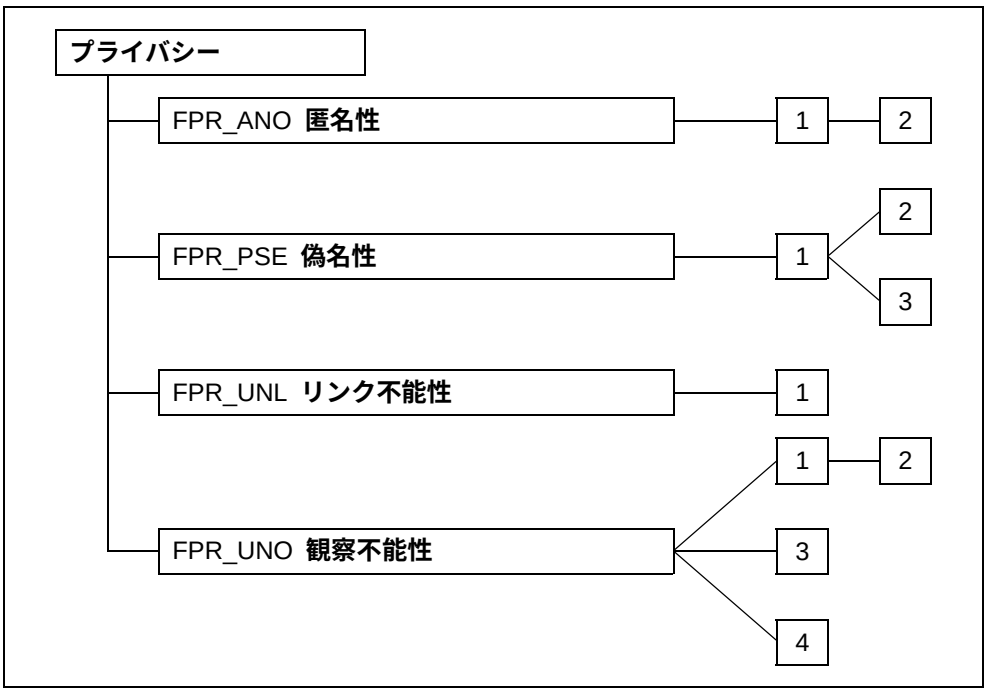


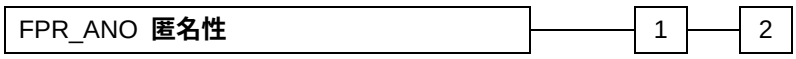
図9.1 - **プライバシークラスのコンポーネント構成**

9.1 匿名性(FPR_ANO)

ファミリのふるまい

このファミリは、利用者が利用者の識別情報を暴露することなく、資源やサービスを使用できるようにする。匿名性に対する要件は、利用者識別情報の保護を提供することである。匿名性は、サブジェクト識別情報の保護を意図したものではない。

コンポーネントのレベル付け



FPR_ANO.1 匿名性は、あるサブジェクトまたは操作に結び付けられた利用者の識別情報を、他の利用者やサブジェクトが判別できないことを要求する。

FPR_ANO.2 情報を請求しない匿名性は、TSFが利用者識別情報を要求しないことを保証することによって、FPR_ANO.1の要件を強化する。

管理: FPR_ANO.1、FPR_ANO.2

これらのコンポーネントに対する予見される管理アクティビティはない。

監査: FPR_ANO.1、FPR_ANO.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 匿名メカニズムの呼出。

FPR_ANO.1 匿名性

下位階層: なし

FPR_ANO.1.1 **TSFは、[割付: *利用者及び/またはサブジェクトのセット*]が[割付: *サブジェクト及び/または操作及び/またはオブジェクトのリスト*]に結合されている実際の利用者名を判別できないことを保証しなければならない。**

依存性: なし

FPR_ANO.2 情報を請求しない匿名性

下位階層: FPR_ANO.1

FPR_ANO.2.1 TSFは、[割付: *利用者及び/またはサブジェクトのセット*]が[割付: *サブジェクト及び/または操作及び/またはオブジェクトのリスト*]に結合された実際の利用者名を判別できないことを保証しなければならない。

FPR_ANO.2.2 **TSFは、実際の利用者名の参照を請求せずに[割付: *サブジェクトのリスト*]に[割付: *サービスのリスト*]を提供しなければならない。**

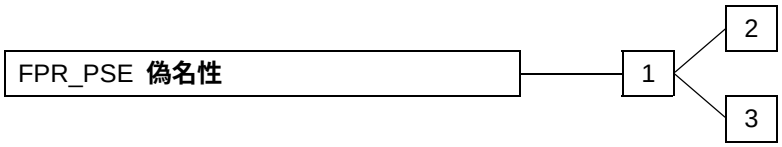
依存性: **なし**

9.2 **偽名性**(FPR_PSE)

ファミリのふるまい

このファミリは、利用者がその利用者識別情報を暴露することなく資源やサービスを使用できるが、その使用に対しては責任を取り得ることを保証する。

コンポーネントのレベル付け



FPR_PSE.1 偽名性は、あるサブジェクトあるいは操作に結び付けられたある利用者の識別情報について、利用者及び/またはサブジェクトのセットはそれを判別することができないが、この利用者はそのアクションに対して責任を取り得ることを要求する。

FPR_PSE.2 可逆偽名性は、提供された別名に基づき、TSFが元の利用者識別情報を判別する能力を備えることを要求する。

FPR_PSE.3 別名偽名性は、利用者識別情報の別名に対するある構成規則にTSFが従うことを要求する。

管理: FPR_PSE.1、FPR_PSE.2、FPR_PSE.3

これらのコンポーネントに対する予見される管理アクティビティはない。

監査: FPR_PSE1、FPR_PSE.2、FPR_PSE.3

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 利用者識別情報の分析を要求したサブジェクト/利用者は監査されるべきである。

FPR_PSE.1 偽名性

下位階層: **なし**

FPR_PSE.1.1 **TSFは、[割付: *利用者及び/またはサブジェクトのセット*]が、[割付: *サブジェクト及び/または操作及び/またはオブジェクトのリスト*]に結合された実利用者名を判別できないことを保証しなければならない。**

FPR_PSE.1.2 **TSFは、[割付: *サブジェクトのリスト*]に対して、実利用者名の[割付: *別名の数*]個の別名を提供できなければならない。**

FPR_PSE.1.3 **TSFは、[選択: *利用者の別名を決定し、利用者から別名を受け入れ*]かつそれが[割付: *別名の尺度*]に適合していることを検証しなければならない。**

依存性: **なし**

FPR_PSE.2 可逆偽名性

下位階層: FPR_PSE.1

FPR_PSE.2.1 TSFは、[割付: *利用者及び/またはサブジェクトのセット*]が、[割付: *サブジェクト及び/または操作及び/またはオブジェクトのリスト*]に結合された実利用者名を判別できないことを保証しなければならない。

FPR_PSE.2.2 TSFは、[割付: *サブジェクトのリスト*]に対して、実利用者名の[割付: *別名の数*]個の別名を提供できなければならない。

FPR_PSE.2.3 TSFは、[選択: *利用者の別名を決定し、利用者から別名を受け入れ*]かつそれが[割付: *別名の尺度*]に適合していることを検証しなければならない。

FPR_PSE.2.4 **TSFは、以下の[割付: *条件のリスト*]のもとでだけ、[選択: *許可利用者*、[割付: *信頼できるサブジェクトのリスト*]]に、提供された別名に基づいて利用者識別情報を判別する能力を提供しなければならない。**

依存性: **FIA_UID.1 識別のタイミング**

FPR_PSE.3 別名偽名性

下位階層: FPR_PSE.1

FPR_PSE.3.1 TSFは、[割付: *利用者及び/またはサブジェクトのセット*]が[割付: *サブジェクト及び/または操作及び/またはオブジェクトのリスト*]に結合された実利用者名を判別できないことを保証しなければならない。

FPR_PSE.3.2 TSFは、[割付: *サブジェクトのリスト*]に対して、実利用者名の[割付: *別名の数*]個の別名を提供できなければならない。

FPR_PSE.3.3 TSFは、[選択: *利用者の別名を決定し*、*利用者から別名を受け入れ*]かつそれが[割付: *別名の尺度*]に適合していることを検証しなければならない。

FPR_PSE.3.4 **TSFは、以下の[割付: *条件のリスト*]のもとでは、実利用者名に対して以前に提供された別名と同一の別名を提供しなければならず、そうでない場合は、提供される別名は、以前に提供された別名と無関係でなければならない。**

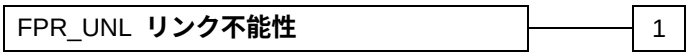
依存性: **なし**

9.3 リンク不能性(FPR_UNL)

ファミリのふるまい

このファミリは、一人の利用者が資源やサービスを複数使用できるが、他人はこれらの使用を一緒にリンクすることができないことを保証する。

コンポーネントのレベル付け



FPR_UNL.1 リンク不能性は、そのシステムにおいて、同一の利用者がある特定の操作(複数形)の原因になっているかどうかを、利用者及び/またはサブジェクトが判別できないことを要求する。

管理: FPR_UNL.1

以下のアクションはFMTにおける管理機能と考えられる:

a) リンク不能性機能の管理。

監査: FPR_UNL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: リンク不能性メカニズムの呼出。

FPR_UNL.1 リンク不能性

下位階層: **なし**

FPR_UNL.1.1 **TSFは、[割付: *利用者及び/またはサブジェクトのセット*]は、[割付: *操作のリスト*]が[選択: *同じ利用者によって生じた、以下のように関係する*[割付: *関係のリスト*]]かどうかを判別できないことを保証しなければならない。**

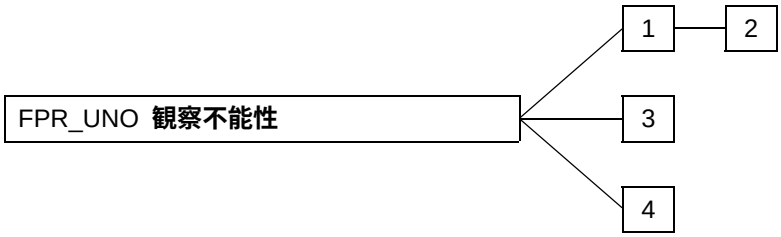
依存性: **なし**

9.4 観察不能性(FPR_UNO)

ファミリのふるまい

このファミリは、利用者が資源やサービスを使用でき、その際に他の利用者、特に第三者は、その資源やサービスが使用されていることを観察できないことを保証する。

コンポーネントのレベル付け



FPR_UNO.1 観察不能性は、利用者及び/またはサブジェクトが、ある操作が実行されていることを判別できないことを要求する。

FPR_UNO.2 観察不能性に影響する情報の配置は、TOE内の情報に関係するプライバシーの集中化を避ける特定のメカニズムをTSFが提供することを要求する。もしセキュリティの弱体化が生じると、そのような集中化は観察不能性に影響を与える可能性がある。

FPR_UNO.3 情報を請求しない観察不能性は、観察不能性の弱体化に利用されるかもしれない情報に関係するプライバシーをTSFが取得しようとしないことを要求する。

FPR_UNO.4 許可利用者観察可能性は、資源及び/またはサービスの利用を観察する権限を、一人またはそれ以上の許可利用者にTSFが提供することを要求する。

管理: FPR_UNO.1、FPR_UNO.2
以下のアクションはFMTの管理機能と考えられる:

a) 観察不能機能のふるまいの管理。

管理: FPR_UNO.3
これらのコンポーネントに対する予見される管理アクティビティはない。

管理: FPR_UNO.4
以下のアクションはFMTの管理機能と考えられる:

a) 操作の発生を判別できる許可利用者のリスト。

監査: FPR_UNO.1、FPR_UNO.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 観察不能性メカニズムの呼出。

監査: FPR_UNO.3

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

監査: FPR_UNO.4

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 利用者またはサブジェクトによる資源またはサービスの使用の観察。

FPR_UNO.1 観察不能性

下位階層: なし

FPR_UNO.1.1 **TSFは、[割付: *利用者及び/またはサブジェクトのリスト*]が[割付: *保護された利用者及び/またはサブジェクトのリスト*]による[割付: *オブジェクトのリスト*]に対する操作[割付: *操作のリスト*]を観察できないことを保証しなければならない。**

依存性: **なし**

FPR_UNO.2 観察不能性に影響する情報の配置

下位階層: FPR_UNO.1

FPR_UNO.2.1 TSFは、[割付: *利用者及び/またはサブジェクトのリスト*]が[割付: *保護された利用者及び/またはサブジェクトのリスト*]による[割付: *オブジェクトのリスト*]に対する操作[割付: *操作のリスト*]を観察できないことを保証しなければならない。

FPR_UNO.2.2 **TSFは、その情報が使われる間、以下の条件が保たれるようTOEの異なるパートに[割付: *観察不能性関連情報*]を配置しなければならない: [割付: *条件のリスト*]。**

依存性: **なし**

FPR_UNO.3　情報を請求しない観察不能性

下位階層:　なし

FPR_UNO.3.1　**TSFは、[割付: *プライバシー関係情報*]の参照を請求することなく、[割付: *サービスのリスト*]を[割付: *サブジェクトのリスト*]に提供しなければならない。**

依存性:　**FPR_UNO.1 観察不能性**

FPR_UNO.4　許可利用者観察可能性

下位階層:　なし

FPR_UNO.4.1　**TSFは、[割付: *許可利用者のセット*]に[割付: *資源及び/またはサービスのリスト*]の利用を観察する能力を提供しなければならない。**

依存性:　**なし**

10 クラスFPT: TSFの保護

本クラスは、TSF(TSP特定のものから独立)を提供するメカニズムの完全性と管理、及びTSFデータ(TSFデータの特定の内容から独立)の完全性に関連する機能要件のファミリを含む。ある意味で、本クラスのファミリはFDP(利用者データ保護)クラスのコンポーメントと重複しているように見えるかもしれない; これらは同じメカニズムを使って実装されていることすらあり得る。しかしながら、FDPは利用者データ保護に焦点を当てているのに対し、FPTはTSFデータ保護に焦点を当てている。実際、FPTクラスのコンポーネントでは、TOEにおけるSFPが改ざんやバイパスされ得ないという要件を提供することが必要とされている。

本クラスの観点から、TSFに対する次の３つの重要な部分がある。

a) TSFの*抽象*マシン、これは評価の実行において特定のTSFを実装した仮想あるいは物理マシン。

b) TSFの*実装*、これは抽象マシン上で実行するもので、TSPを実施するメカニズムを実装する。

c) TSFの*データ*、これはTSPの実施のガイドとなる管理用のデータベース。

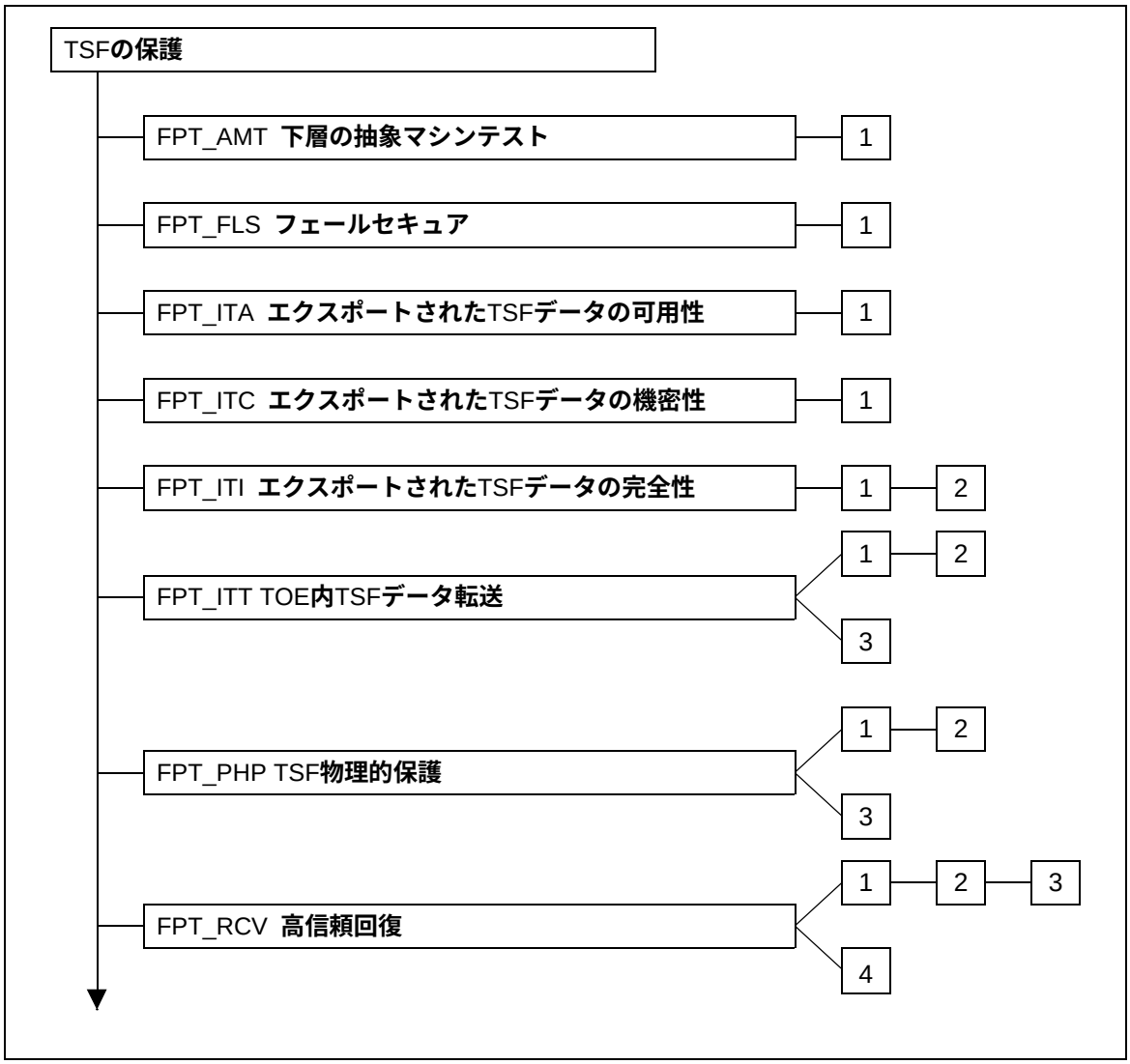


図10.1 - TSF**の保護クラスのコンポーネント構成**

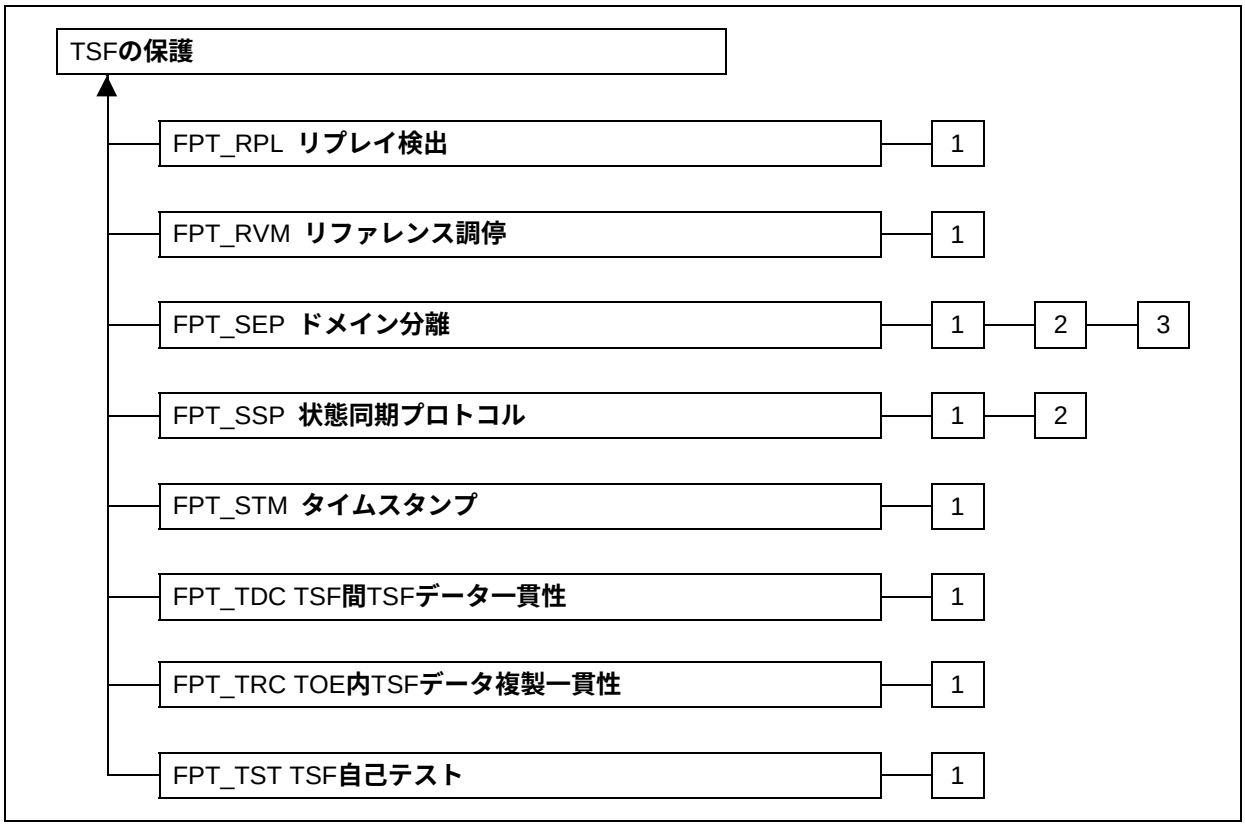


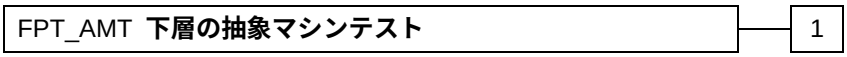
図10.2 - TSF**の保護クラスのコンポーネント構成(続き)**

10.1 下層の抽象マシンテスト(FPT_AMT)

ファミリのふるまい

このファミリは、TSFが依存する下層抽象マシンについて作られたセキュリティ想定を実証するテストをTSFが実行するための要件を定義する。この「抽象」マシンは、ハードウェア/ファームウェアプラットフォームでも、仮想マシンとして動作する、内容がわかりかつ査定された、何らかのハードウェア/ソフトウェアの組み合わせでもよい。

コンポーメントのレベル付け



FPT_AMT.1 抽象マシンテストは、下層の抽象マシンのテストを規定する。

管理: FPT_AMT.1

以下のアクションはFMTの管理機能と考えられる:

a) 初期立ち上げ中、定期的間隔、特定の状態下など、抽象マシンテストが行われる条件の管理;
b) 必要ならば、時間間隔の管理。

監査: FPT_AMT.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 下層のマシンのテストの実行とテストの結果。

FPT_AMT.1 抽象マシンテスト

下位階層: なし

FPT_AMT.1.1 **TSFは、TSFの下層にある抽象マシンによって提供されるセキュリティ想定の正しい操作を実証するために、[選択: *初期立ち上げ中*、*通常操作中に定期的に*、*許可利用者の要求で*、*その他の条件*」に、テストのスイートを走らせなければならない。**

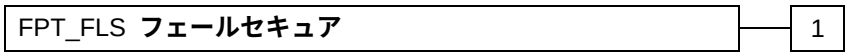
依存性: **なし**

10.2 フェールセキュア(FPT_FLS)

ファミリのふるまい

このファミリの要件は、TSF中の識別された障害のカテゴリの事象において、TOEがそのTSPを侵害しないことを保証する。

コンポーネントのレベル付け



このファミリは一つのコンポーネント - FPT_FLS.1 セキュアな状態を保持する障害 - だけから成り、これは、識別された障害に直面したときにTSFがセキュアな状態を保持することを要求する。

管理: FPT_FLS.1

予見される管理アクティビティはない。

監査: FPT_FLS.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: TSFの障害。

FPT_FLS.1 セキュアな状態を保持する障害

下位階層: なし

FPT_FLS..1.1 **TSFは、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: [割付: *TSFにおける障害の種別のリスト*]。**

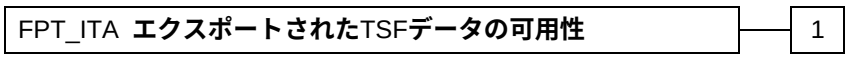
依存性: **ADV_SPM.1 非形式的TOEセキュリティ方針モデル**

10.3 エクスポートされたTSFデータの可用性(FPT_ITA)

ファミリのふるまい

このファミリはTSFとリモート高信頼IT製品間を流れるTSFデータの可用性の損失を防ぐ規則を定義する。このデータは、例えば、パスワード、キー、監査データ、あるいはTSF実行コードなどのTSFに重要なデータである。

コンポーネントのレベル付け



このファミリは、FPT_ITA.1 定義された可用性尺度以内のTSF間可用性のコンポーネント一つだけから成る。このコンポーネントは、識別された蓋然性の度合いに対し、リモート高信頼IT製品に提供されるTSFデータの可用性をTSFが保証することを要求する。

管理: FPT_ITA.1

以下のアクションはFMTの管理機能と考えられる:

a) リモート高信頼IT製品で使用できなければならないTSFデータの種別のリストの管理。

監査: FPT_ITA.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TOEに要求されたときのTSFデータの欠落。

FPT_ITA.1 定義された可用性尺度内のTSF間可用性

下位階層: なし

FPT_ITA.1.1 **TSFは、与えられた以下の条件[割付: *可用性を保証する条件*]の[割付: *定義された可用性尺度*]以内で、リモート高信頼IT製品に提供される[割付: *TSFデータの種別のリスト*]の可用性を保証しなければならない。**

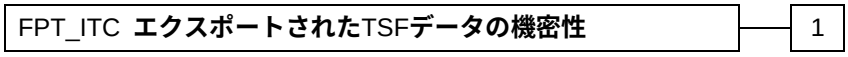
依存性: **なし**

10.4 エクスポートされたTSFデータの機密性(FPT_ITC)

ファミリのふるまい

このファミリは、TSFとリモート高信頼IT製品間の送信中の、不正な暴露からのTSFデータの保護に対する規則を定義する。このデータは、例えば、パスワード、キー、監査データ、あるいはTSF実行コードなどのTSFに重要なデータである。

コンポーネントのレベル付け



このファミリは、FPT_ITC.1 送信中のTSF間機密性のコンポーネント一つだけから成り、これは、TSFとリモート高信頼IT製品間で送信されるデータが、通過中の暴露から保護されることをTSFが保証することを要求する。

管理: FPT_ITC.1

予見される管理アクティビティはない。

監査: FPT_ITC.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_ITC.1 送信中のTSF間機密性

下位階層: なし

FPT_ITC.1.1 **TSFは、TSFからリモート高信頼IT製品に送信されるすべてのTSFデータを、送信中の不当な暴露から保護しなければならない。**

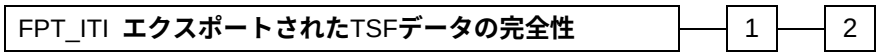
依存性: **なし**

10.5 エクスポートされたTSFデータの完全性(FPT_ITI)

ファミリのふるまい

このファミリは、TSFとリモート高信頼IT製品間で送信中のTSFデータの、不正な改変からの保護に対する規則を定義する。このデータは、例えば、パスワード、キー、監査データ、TSF実行コードなどのTSFに重要なデータである。

コンポーネントのレベル付け



FPT_ITI.1 TSF間改変の検出は、リモート高信頼IT製品は使用されるメカニズムを知っているとの想定のもとに、TSFとリモート高信頼IT製品間の送信中のTSFデータの改変を検出する能力を提供する。

FPT_ITI.2 TSF間改変の検出と訂正は、リモート高信頼IT製品は使用されるメカニズムを知っているとの想定のもとに、リモート高信頼IT製品に対し、改変の検出だけでなく改変されたTSFデータを訂正する能力も提供する。

管理: FPT_ITI.1

予見される管理アクティビティはない。

管理: FPT_ITI.2

以下のアクションはFMTの管理機能と考えられる:

a) 転送中に改変されたらTSFが訂正を試みるべきTSFデータの種別の管理;
b) TSFデータが転送中に改変されたらTSFが取り得るアクションの種別の管理。

監査: FPT_ITI.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 送出TSFデータの改変の検出。
b) 基本: 送出TSFデータの改変の検出において取られるアクション。

監査: FPT_ITI.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 送出TSFデータの改変の検出;
b) 基本: 送出TSFデータの改変の検出において取られるアクション。
c) 基本: 訂正メカニズムの使用。

FPT_ITI.1 TSF間改変の検出

下位階層: なし

FPT_ITI.1.1 **TSFは、以下の尺度の範囲で、TSFとリモート高信頼IT製品間で送出中のすべてのTSFデータの改変を検出する能力を提供しなければならない: [割付: *定義された改変尺度*]。**

FPT_ITI.1.2 **TSFは、TSFとリモート高信頼IT製品間で送られるすべてのTSFデータの完全性を検証し、かつ改変が検出された場合には[割付: *取られるアクション*]を実行する能力を提供しなければならない。**

依存性: **なし**

FPT_ITI.2 TSF間改変の検出と訂正

下位階層: FPT_ITI.1

FPT_ITI.2.1 TSFは、以下の尺度の範囲で、TSFとリモート高信頼IT製品間で送出中のすべてのTSFデータの改変を検出する能力を提供しなければならない: [割付: *定義された改変尺度*]。

FPT_ITI.2.2 TSFは、TSFとリモート高信頼IT製品間で送られるすべてのTSFデータの完全性を検証し、かつ改変が検出された場合には[割付: *取られるアクション*]を実行する能力を提供しなければならない。

FPT_ITI.2.3 **TSFは、TSFとリモート高信頼IT製品間を送られるすべてのTSFデータの[割付: *改変の種別*]を訂正する能力を提供しなければならない。**

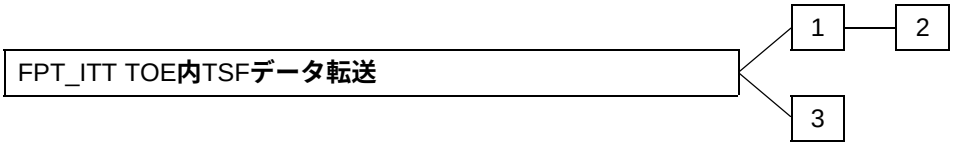
依存性: **なし**

10.6 TOE内TSFデータ転送(FPT_ITT)

ファミリのふるまい

このファミリは、TSFデータが内部チャネルを通して一つのTOEの分離したパーツ間を転送されるときのTSFデータの保護に対応する要件を提供する。

コンポーネントのレベル付け



FPT_ITT.1 基本TSF内データ転送保護は、TOEの分離したパーツ間で送信されるときにTSFデータが保護されることを要求する。

FPT_ITT.2 TSFデータ転送分離は、TSFが、利用者データを送信中のTSFデータから分離することを要求する。

FPT_ITT.3 TSFデータ完全性監視は、TOEの分離したパーツ間で送信されるTSFデータが、識別された完全性誤りについて監視されることを要求する。

管理: FPT_ITT.1

以下のアクションはFMTの管理機能と考えられる:

a) TSFが保護すべき改変の種別の管理;
b) TSFの異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムの管理。

管理: FPT_ITT.2

以下のアクションはFMTの管理機能と考えられる:

a) TSFが保護すべき改変の種別の管理;
b) TSFの異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムの管理;
c) 分離メカニズムの管理。

管理: FPT_ITT.3

以下のアクションはFMTの管理機能と考えられる:

a) TSFが(その改変から)保護すべき改変の種別の管理;
b) TSFの異なるパーツ間の通過におけるデータ保護を提供するために使われるメカニズムの管理;
c) TSFが検出を試みるべきTSFデータの改変の種別の管理;
d) 取られるアクションの管理。

監査: FPT_ITT.1、FPT_ITT.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

監査: FPT_ITT.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFデータの改変の検出;
b) 基本: 完全性誤りの検出に引き続いてとられるアクション。

FPT_ITT.1 基本TSF内データ転送保護

下位階層: なし

FPT_ITT.1.1 **TSFは、TSFデータがTOEの別々のパーツ間で送られる場合、TSFデータを[選択: *暴露*、*改変*]から保護しなければならない。**

依存性: **なし**

FPT_ITT.2 TSFデータ転送分離

下位階層: FPT_ITT.1

FPT_ITT.2.1 TSFは、データがTOEの別々のパーツ間で送られる場合、TSFデータを[選択: *暴露*、*改変*]から保護しなければならない。

FPT_ITT.2.2 **TSFは、データがTOEの別々のパーツ間で送られる場合、利用者データをTSFデータから分離しなければならない。**

依存性: **なし**

FPT_ITT.3 TSFデータ完全性監視

下位階層: なし

FPT_ITT.3.1 **TSFは、TOEの別々のパーツ間で送られるTSFデータに対し、[選択: *データの改変*、*データの置き換え*、*データの順序変え*、*データの削除*、[割付: *その他の完全性誤り*]]を検出できなければならない。**

FPT_ITT.3.2 **データ完全性誤りの検出において、TSFは、以下のアクション[割付:**

取られるアクションを指定]を取らねばならない。

依存性: **FPT_ITT.1 基本TSF内データ転送保護**

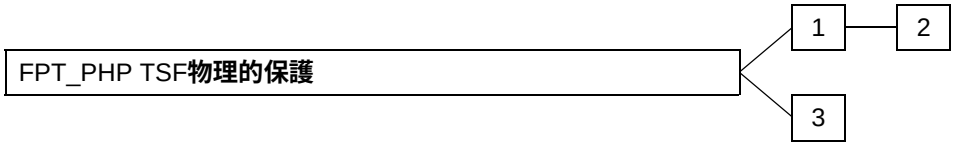
10.7 TSF物理的保護(FPT_PHP)

ファミリのふるまい

TSF物理的保護コンポーネントは、TSFに対する不正な物理的アクセスの制限、及びTSFの不正な物理的改変あるいは置き換えに対する阻止と抵抗に言及する。

このファミリのコンポーネントの要件は、物理的な改ざんと干渉からTSFが保護されることを保証する。これらのコンポーネントの要件を満たすことは、結果として、TSFがパッケージ化され、かつ、物理的改ざんを検出可能な、あるいは物理的改ざんへの抵抗が強制されるような形で使われることになる。これらのコンポーネントがなければ、物理的損害を防ぎ得ない環境において、TSFの保護機能はその有効性を失う。このファミリはまた、TSFがどのようにして物理的な改ざんの試みに対応しなければならないかに関する要件を提供する。

コンポーネントのレベル付け



FPT_PHP.1 物理的攻撃の受動的検出は、TSFの装置やTSFのエレメントがいつ改ざんを受けたかを示すという特色を備える。しかしながら、改ざんの通知は自動的ではない; 許可利用者は、セキュリティ管理機能を呼び出すか、あるいは改ざんが起きたかどうかを決定する手動の検査を実施せねばならない。

FPT_PHP.2 物理的攻撃の通知は、識別された物理的侵入のサブセットに対して、改ざんの自動通知に備える。

FPT_PHP.3 物理的攻撃への抵抗は、TSFの装置やTSFのエレメントの物理的改ざんを防止し、あるいはそれに抵抗するという特色を備える。

管理: FPT_PHP.1、FPT_PHP.3
予期される管理アクティビティはない。

管理: FPT_PHP.2
以下のアクションはFMTの管理機能と考えられる:

a) 侵入について通知される利用者または役割の管理;
b) 指定された利用者または役割に、侵入について通知すべき装置のリストの管理。

管理: FPT_PHP.3
以下のアクションはFMTの管理機能と考えられる:

a) 物理的干渉に対する自動応答の管理。

監査: FPT_PHP.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: IT手段による検出であれば、侵入の検出。

監査: FPT_PHP.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: 侵入の検出。

監査: FPT_PHP.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_PHP.1 物理的攻撃の受動的検出

下位階層: なし

FPT_PHP.1.1 **TSFは、TSFを弱体化する恐れがある物理的干渉についての曖昧さのない検出を提供しなければならない。**

FPT_PHP.1.2 **TSFは、TSFの装置やTSFのエレメントに物理的干渉が生じたかどうかを決定する能力を提供しなければならない。**

依存性: **FMT_MOF.1 セキュリティ機能のふるまいの管理**

FPT_PHP.2 物理的攻撃の通知

下位階層: FPT_PHP.1

FPT_PHP.2.1 TSFは、TSFを弱体化する恐れがある物理的な干渉についての曖昧さのない検出を提供しなければならない。

FPT_PHP.2.2 TSFは、TSFの装置やTSFのエレメントに物理的干渉が生じたかどうかを決定する能力を提供しなければならない。

FPT_PHP.2.3 **[割付: *能動的検出が要求されるTSF装置/エレメントのリスト*]に対し、TSFは、装置とエレメントを監視し、かつTSFの装置またはTSFのエレメントに物理的干渉が生じたとき、[割付: *指示された利用者または役割*]に通知しなければならない。**

依存性: FMT_MOF.1 **セキュリティ機能のふるまいの管理**

FPT_PHP.3 物理的攻撃への抵抗

下位階層: なし

FPT_PHP.3.1 **TSFは、TSPが侵害されないよう自動的に対応することによって、[割付: *TSF装置/エレメントのリスト*]への[割付: *物理的な干渉のシナリオ*]に抵抗しなければならない。**

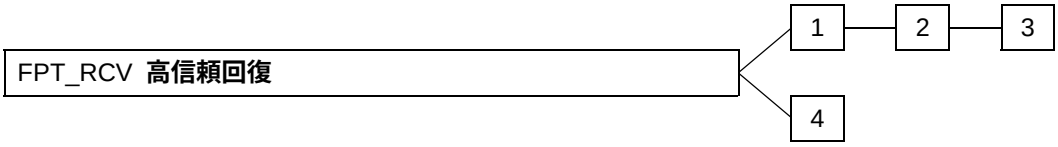
依存性: **なし**

10.8 高信頼回復(FPT_RCV)

ファミリのふるまい

このファミリの要件は、保護の弱体化なくTOEが立ち上がることを決定できること、かつ操作の中断後、保護の弱体化なく回復できることを保証する。TSFの立ち上がりの状態がそれに続く状態の保護を決定するので、このファミリは重要である。

コンポーネントのレベル付け



FPT_RCV.1 手動回復は、セキュアな状態に戻るために、人間の介入を必要とするメカニズムだけをTOEが提供することを認める。

FPT_RCV.2 自動回復は、少なくともサービス中断の一つの種別に対して、人間の介入なしのセキュアな状態への回復を提供する; 他の中断に対する回復は、人間の介入を必要とするかもしれない。

FPT_RCV.3 過度の損失のない自動回復は、これも自動回復のために提供されるものであるが、しかし、保護オブジェクトの過度の損失を許さないことで要件を強化している。

FPT_RCV.4 機能回復は、特別なSFレベルへの回復のため、TSFデータのセキュアな状態への成功裏の完了、あるいはロールバックの保証を提供する。

管理: FPT_RCV.1

以下のアクションはFMTの管理機能と考えられる:

a) メンテナンスモードにおける修復能力に誰がアクセスできるかの管理。

管理: FPT_RCV.2、FPT_RCV.3

以下のアクションはFMTの管理機能と考えられる:

a) メンテナンスモードにおける修復能力に誰がアクセスできるかの管理;
b) 自動的な手順で処理される障害/サービス中断のリストの管理。

管理: FPT_RCV.4

予期される管理アクティビティはない。

監査: FPT_RCV.1、FPT_RCV.2、FPT_RCV.3

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 障害またはサービス中断が発生した事実;
b) 最小: 通常動作の再開;
c) 基本: 障害またはサービス中断の種別。

監査: FPT_RCV.4
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: 可能ならば、セキュリティ機能の障害後にセキュアな状態へ復帰できないこと;
b) 基本: 可能ならば、セキュリティ機能の障害の検出。

FPT_RCV.1 手動回復

下位階層: なし

FPT_RCV.1.1 **障害またはサービス中断後、TSFは、TOEをセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。**

依存性: **FPT_TST.1 TSFテスト**
AGD_ADM.1 管理者ガイダンス
ADV_SPM.1 非形式的TOEセキュリティ方針モデル

FPT_RCV.2 自動回復

下位階層: FPT_RCV.1

FPT_RCV.2.1 障害またはサービス中断からの**自動回復が不可能な場合**、TSFはTOEをセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。

FPT_RCV.2.2 **[割付: *障害/サービス中断のリスト*]に対し、TSFは、自動化された手順によるTOEのセキュアな状態への復帰を保証しなければならない。**

依存性: FPT_TST.1 TSFテスト
AGD_ADM.1 管理者ガイダンス
ADV_SPM.1 非形式的TOEセキュリティ方針モデル

FPT_RCV.3 過度の損失のない自動回復

下位階層: FPT_RCV.2

FPT_RCV.3.1 障害またはサービス中断からの自動回復が不可能な場合、TSFはTOE

をセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。

FPT_RCV.3.2 [割付: *障害/サービス中断のリスト*]に対し、TSFは、自動化された手順によるTOEのセキュアな状態への復帰を保証しなければならない。

FPT_RCV.3.3 **障害またはサービス中断から回復するためにTSFによって提供される機能は、TSC内のTSFデータまたはオブジェクトの損失が[割付: *量の明示*]を超えることなくセキュアな初期状態が回復されることを保証しなければならない。**

FPT_RCV.3.4 **TSFは、オブジェクトが回復可能であったか、否かを決定する能力を提供しなければならない。**

依存性: FPT_TST.1 TSF**テスト**
AGD_ADM.1 **管理者ガイダンス**
ADV_SPM.1 **非形式的**TOE**セキュリティ方針モデル**

FPT_RCV.4 機能回復

下位階層: なし

FPT_RCV.4.1 **TSFは、[割付: *SF及び障害シナリオのリスト*]が、SFが成功裏に完了するか、あるいは指示された障害シナリオに対して、一致しかつセキュアな状態に回復するかの特性を持つことを保証しなければならない。**

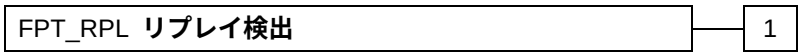
依存性: **ADV_SPM.1 非形式的TOEセキュリティ方針モデル**

10.9 リプレイ検出(FPT_RPL)

ファミリのふるまい

このファミリは、さまざまな種別のエンティティ(例えば、メッセージ、サービス要求、サービス応答)に対するリプレイの検出と、それに続く訂正のためのアクションに対応する。リプレイが検出できるような場合は、このファミリは効果的にリプレイを防止する。

コンポーネントのレベル付け



このファミリは一つだけのコンポーネント、FPT_RPL.1 リプレイ検出から成り、これは、識別されたエンティティのリプレイをTSFが検出できねばならないことを要求する。

管理: FPT_RPL.1

以下のアクションはFMTの管理機能と考えられる:

a) リプレイが検出されなくてはならない識別されたエンティティのリストの管理;
b) リプレイの場合にとる必要があるアクションのリストの管理。

監査: FPT_RPL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: 検出されたリプレイ攻撃。
b) 詳細: 特定のアクション(複数形)に基づいてとられるアクション(単数形)。

FPT_RPL.1 リプレイ検出

下位階層: なし

FPT_RPL.1.1 **TSFは、以下のエンティティに対するリプレイを検出しなければならない: [割付: *識別されたエンティティのリスト*]。**

FPT_RPL.1.2 **TSFは、リプレイが検出された場合、[割付: *特定のアクションのリスト*]をしなければならない。**

依存性: **なし**

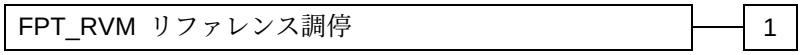
10.10 リファレンス調停(FPT_RVM)

ファミリのふるまい

このファミリの要件は、伝統的なリファレンスモニタの「いつでも呼び出せる」側面に対応する。このファミリの目標は、与えられたSFPに関して、方針の実施を要求するすべてのアクションが、SFPに対するTSFによって有効性を確認されることを保証することである。もし、SFPを実施するTSFの部分もFPT_SEP(ドメイン分離)とADV_INT(TSF内部)の適切なコンポーネントの要件に合致するならば、TSFのその部分は、そのSFPに対する「リファレンスモニタ」を提供する。

もし、いかなる、あるいはすべてのそのSFPに関する信頼できないサブジェクトによって要求されたすべての実施可能なアクション(例えば、オブジェクトへのアクセス)が、成功する前にSFPによって有効性を確認されるならば、そしてその場合だけ、SFPを実装するTSFは、不正な操作に対して効果的な保護を提供する。もし、TSFによって実施され得るアクションが間違って実施されたり間違ってバイパスされると、全体のSFPの実施は弱体化されよう。そのとき、サブジェクトは、さまざまな不正な方法(例えば、あるサブジェクトまたはオブジェクトに対するアクセスチェックを回避、アプリケーションによって保護されると想定されたオブジェクトに対するチェックをバイパス、意図された有効期間を超えたアクセス権限を保持、監査されるアクションの監査をバイパス、あるいは認証をバイパス)によってSFPをバイパスできよう。注意しなければならないのは、特定のSFPに関していわゆる「高信頼サブジェクト」と呼ばれるいくつかのサブジェクトは、それら自身がSFPの実施における信頼を与え、SFPの調停をバイパスしてしまうかもしれない点である。

コンポーネントのレベル付け



このファミリは一つのコンポーネント、FPT_RVM.1 TSPの非バイパス性だけから成り、これはTSPにおけるすべてのSFPに対する非バイパス性を要求する。

管理: FPT_RVM.1
予見される管理アクティビティはない。

監査: FPT_RVM.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_RVM.1 TSPの非バイパス性

下位階層: なし

FPT_RVM.1.1　TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性:　なし

10.11 **ドメイン分離**(FPT_SEP)

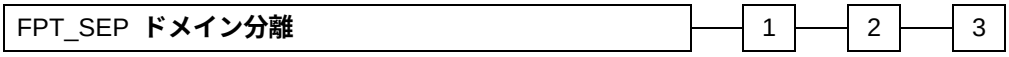
ファミリのふるまい

このファミリのコンポーネントは、少なくとも一つのセキュリティドメインがTSF自身の実行のために利用でき、かつ信頼できないサブジェクトによる外部の干渉と改ざん(例えば、TSFコードやデータ構造の改変による)からTSFが保護されることを保証する。このファミリの要件を満たすことでTSFは自己保護型になり、これは、信頼できないサブジェクトはTSFを改変したり損害を与えたりできないことを意味する。

このファミリは以下のものを要求する:

a) TSFのセキュリティドメイン(「保護ドメイン」)の資源と、ドメイン外のサブジェクト及び拘束されないエンティティは、保護されたドメインの外部のエンティティが保護されたドメイン内のTSFデータやTSFコードを観察したり改変したりできないように分離される。
b) ドメイン間の転送は、保護ドメインへの勝手な進入や復帰ができないように管理される。
c) アドレスによって保護ドメインへ渡される利用者やアプリケーションのパラメタは保護ドメインのアドレス空間に関して確認され、値によって渡されるものは、保護ドメインが期待する値に関して確認される。
d) サブジェクトのセキュリティドメインは、TSFを介して管理された共有を除き、他と異なる。

コンポーネントのレベル付け



FPT_SEP.1 TSFドメイン分離は、TSFのための区分された保護ドメインを提供し、かつTSC内のサブジェクト間の分離を提供する。

FPT_SEP.2 SFPドメイン分離は、TOEの非TSF部分に対するドメインにしたのと同様に、SFPの方針に対してリファレンスモニタとして動作する、識別されたSFPのセットのための区分されたドメイン(複数形)と、TSFの残りの部分に対する一つのドメインに、TSFがさらに小分割されることを要求する。

FPT_SEP.3 完全リファレンスモニタは、TOEの非TSF部分に対するドメインにしたのと同様に、TSP実施のための区分されたドメイン(複数形)と、TSFの残りの部分に対する一つのドメインがあることを要求する。

管理: FPT_SEP.1、FPT_SEP.2、FPT_SEP.3
予見される管理アクティビティはない。

監査: FPT_SEP.1、FPT_SEP.2、FPT_SEP.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_SEP.1 TSFドメイン分離

下位階層: なし

FPT_SEP.1.1 **TSFは、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。**

FPT_SEP.1.2 **TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。**

依存性: **なし**

FPT_SEP.2 SFPドメイン分離

下位階層: FPT_SEP.1

FPT_SEP.2.1 TSFの**分離できない部分**は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.2.2 TSFは、TSC内でサジェクトのセキュリティドメイン間の分離を実施しなければならない。

FPT_SEP.2.3 **TSFは、[割付: *アクセス制御及び/または情報フロー制御SFP(複数形)のリスト*]に関連するTSFのパートを、TSFの他の部分による干渉や改ざん、及びそれらSFP*(複数形)*に関して信頼できないサブジェクトによる干渉や改ざんから保護する、それらSFP(複数形)自身の実行のためのセキュリティドメイン内に維持しなければならない。**

依存性: **なし**

FPT_SEP.3 完全リファレンスモニタ

下位階層: FPT_SEP.2

FPT_SEP.3.1 TSFの分離できない部分は、それ自身の実行のため、信頼できないサ

ブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.3.2 TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

FPT_SEP.3.3 TSFは、**アクセス制御及び/または情報フロー制御SFP(複数形)を実施するTSFのパート**を、TSFの他の部分による干渉や改ざん、及び**TSP**に関して信頼できないサブジェクトによる干渉や改ざんから**それらSFP(複数形)を**保護する、**そのパート**自身の実行のためのセキュリティドメイン内に維持しなければならない。

依存性: **なし**

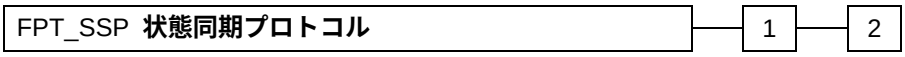
10.12 状態同期プロトコル(FPT_SSP)

ファミリのふるまい

分散システムは、システムのパーツ間の状態において潜在的な差異が生じること、通信における遅延があることによって、一体化したシステムよりも複雑さを増すかもしれない。ほとんどの場合、分散した機能間の状態の同期は、単純なアクションでなく、交換プロトコルを必要とする。これらのプロトコルの分散環境に悪意が存在すれば、さらに複雑な防御的プロトコルが要求される。

FPT_SSPは、この信頼できるプロトコルを使用するTSFのある重要なセキュリティ機能についての要件を制定する。FPT_SSPは、TOE(例えば、ホスト)の二つの分散したパーツが、あるセキュリティ関連のアクションのあとで、同期した状態を持つことを保証する。

コンポーネントのレベル付け



FPT_SSP.1 単純信頼肯定応答は、データ受信による単純な承認だけを要求する。

FPT_SSP.2 相互信頼肯定応答は、データ交換の相互承認を要求する。

管理: FPT_SSP.1、FPT_SSP.2
予見される管理アクティビティはない。

監査: FPT_SSP.1、FPT_SSP.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 予期されたときの肯定応答受信失敗。

FPT_SSP.1 単純信頼肯定応答

下位階層: なし

FPT_SSP.1.1 **TSFは、TSFの他のパートから要求されたとき、改変されていないTSFデータ送信の受信の肯定応答をしなければならない。**

依存性: **FPT_ITT.1 基本TSF内データ転送保護**

FPT_SSP.2 相互信頼肯定応答

下位階層: FPT_SSP.1

FPT_SSP.2.1 TSFは、TSFの他のパートから要求されたとき、改変されていないTSFデータ送信の受信の肯定応答をしなければならない。

FPT_SSP.2.2 **TSFは、TSFの関連するパーツが、肯定応答を使って、異なるパーツ間で送信されたデータの正確な状態を知ることを保証しなければならない。**

依存性: FPT_ITT.1 **基本**TSF**内データ転送保護**

10.13 タイムスタンプ(FPT_STM)

ファミリのふるまい

このファミリは、TOEでの高信頼タイムスタンプ機能に対する要件に対応する。

コンポーネントのレベル付け

このファミリは一つだけのコンポーネント、FPT_STM.1 高信頼タイムスタンプから成り、これは、TSFがTSF機能のために高信頼タイムスタンプを提供することを要求する。

管理: FPT_STM.1

以下のアクションはFMTの管理機能と考えられる:

a) 時間の管理。

監査: FPT_STM.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである。

a) 最小: 時間の変更;
b) 詳細: タイムスタンプの提供。

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1 **TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。**

依存性: **なし**

10.14　TSF間TSFデーター貫性(FPT_TDC)

ファミリのふるまい

分散あるいは複合システム環境において、TOEはTSFデータ(例えば、データに関連したSFP属性、監査情報、識別情報)を他の高信頼IT製品と交換するする必要があるかもしれない。このファミリは、TOEのTSFと他の高信頼IT製品間で、これらの属性の共有及び一貫した解釈のための要件を定義する。

コンポーネントのレベル付け

FPT_TDC.1 TSF間基本TSFデータ一貫性は、TSFがTSF間の属性の一貫性を保証する能力を提供することを要求する。

管理: FPT_TDC.1

予見される管理アクティビティはない。

監査: FPT_TDC.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFデータ一貫性メカニズムの成功した使用。
b) 基本: TSFデータ一貫性メカニズムの使用。
c) 基本: TSFデータがどのように解釈されたかの識別。
d) 基本: 改変されたTSFデータの検出。

FPT_TDC.1　TSF間基本TSFデーター貫性

下位階層:　なし

FPT_TDC.1.1　**TSFは、TSFと他の高信頼IT製品間で共有される場合に[割付: *TSFデータ種別のリスト*]を一貫して解釈する能力を提供しなければならない。**

FPT_TDC.1.2　**TSFは、他の高信頼IT製品からのTSFデータを解釈するとき、[割付: *TSFが適用する解釈規則のリスト*]を使用しなければならない。**

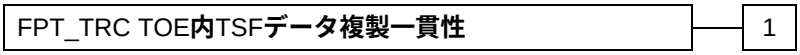
依存性:　**なし**

10.15　TOE**内**TSF**データ複製一貫性**(FPT_TRC)

ファミリのふるまい

このファミリの要件は、TSFデータがTOE内で複製される場合、TSFデータの一貫性を保証することを求めている。もし、TOEのパーツ間の内部チャネルが運用不能になると、そのようなデータは一貫性を失うかもしれない。もし、TOEの内部構造がネットワーク化されており、TOEネットワーク接続のパーツが切断されると、パーツが非活性状態になるときにこのようなことが生じるかもしれない。

コンポーネントのレベル付け



このファミリはただ一つのコンポーネント、FPT_TRC.1 TSF内一貫性から成り、これは、複数の場所で複製されるTSFデータの一貫性をTSFが保証することを要求する。

管理: FPT_TRC.1

予見される管理アクティビティはない。

監査: FPT_TRC.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 再接続時に一貫性を回復すること。
b) 基本: TSFデータ間の一貫性欠如の検出。

FPT_TRC.1　TSF内一貫性

下位階層:　なし

FPT_TRC.1.1　**TSFは、TOEのパート間で複製される場合、TSFデータが一貫していることを保証しなければならない。**

FPT_TRC.1.2　**複製されたTSFデータを含むTOEのパートが切り離される場合、TSFは、再接続において[割付: *TSFデータ複製の一貫性に依存するSFのリスト*]に対するいかなる要求についてもそれを処理する前に、複製されたTSFデータの一貫性を保証しなければならない。**

依存性:　**FPT_ITT.1 基本TSF内データ転送保護**

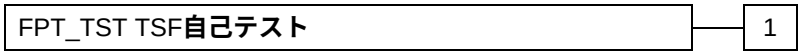
10.16　TSF**自己テスト**(FPT_TST)

ファミリのふるまい

このファミリは、ある期待される正しい運用に関する、TSFの自己テストのための要件を定義する。例として、実施機能に対するインタフェースや、TOEの重要なパーツにおける抜き取りの計算的操作がある。これらのテストは、立ち上げ時、定期的、許可利用者の要求によって、あるいはその他の条件が合致したときに実行される。自己テストの結果としてTOEによって取られるアクションは、別のファミリで定義される。

このファミリの要件もまた、(他のファミリによって扱われる)TOEの運用を必ずしも停止しない種々の障害による、TSF実行コード(すなわち、TSFソフトウェア)とTSFデータの劣化を検出することが求められる。このような障害は必ず防止されるとは限らないので、これらのチェックが実行されなければならない。予見されない障害モードやハードウエア、ファームウエア、ソフトウエアの設計における関連した見落とし、あるいは不適切な論理及び/または物理的保護に起因するTSFの悪意ある変造などが原因で、このような障害が生じ得る。

コンポーネントのレベル付け



FPT_TST.1 TSFテストは、TSFの正しい運用をテストする能力を提供する。これらのテストは、立ち上げ時、定期的、許可利用者の要求によって、あるいはその他の条件が合致したときに実行することができる。また、これは、TSFデータと実行コードの完全性を検証する能力を提供する。

管理: FPT_TST.1

以下のアクションはFMTの管理機能と考えられる:

a) 初期立ち上げ中、定期間隔、あるいは特定の条件下など、TSF自己テストが動作する条件の管理;
b) 必要ならば、時間間隔の管理。

監査: FPT_TST.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本: TSF自己テストの実行とテストの結果。

FPT_TST.1　TSFテスト

下位階層:　なし

FPT_TST.1.1 **TSFは、TSFの正常動作を実証するために、[選択: *初期立ち上げ中*、*通常運用中定期的に*、*許可利用者の要求時に*、*条件*[割付: *自己テストが作動すべき条件*]下で]自己テストのスイートを実行しなければならない。**

FPT_TST.1.2 **TSFは、許可利用者に、TSFデータの完全性を検証する能力を提供しなければならない。**

FPT_TST.1.3 **TSFは、許可利用者に、格納されているTSF実行コードの完全性を検証する能力を提供しなければならない。**

依存性: **FPT_AMT.1 抽象マシンテスト**

11 クラスFRU: 資源利用

このクラスは、処理能力及び/または格納容量など、必要な資源の可用性をサポートする三つのファミリからなる。耐障害性ファミリは、TOE障害による能力利用不可に対する保護を提供する。サービス優先度ファミリは、資源が、より重要なあるいは時間的制約の厳しいタスクに割当てられ、優先度の低いタスクによって専有され得ないことを保証する。資源割当てファミリは、利用できる資源に制限を設け、利用者が資源を独占するのを防ぐ。

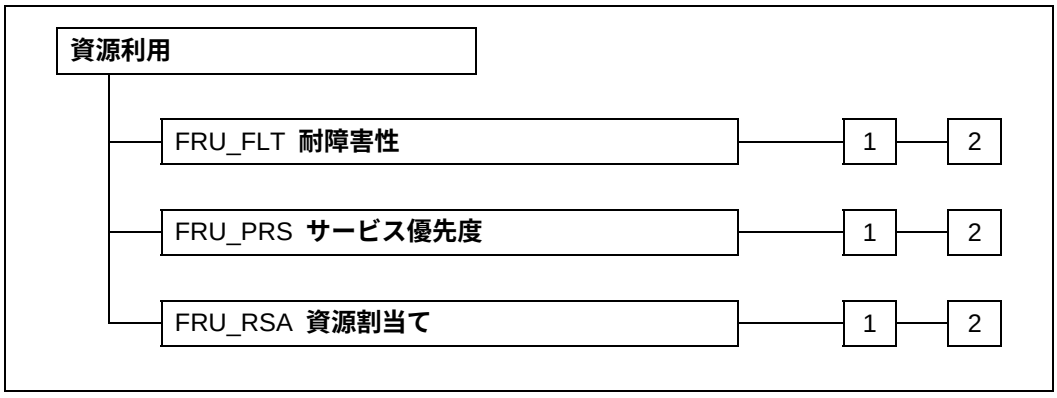


図11.1 - 資源利用クラスのコンポーネント構成

11.1 耐障害性(FRU_FLT)

ファミリのふるまい

このファミリの要件は、障害発生時においても、TOEが正しい運用を維持することを保証することである。

コンポーネントのレベル付け

FRU_FLT.1 機能削減された耐障害性は、識別した障害発生時に、TOEが、識別した能力の正しい運用を続けることを要求する。

FRU_FLT.2 制限付き耐障害性は、識別した障害発生時に、TOEがすべての能力の正しい運用を続けることを要求する。

管理: FRU_FLT.1、FRU_FLT.2

予見される管理アクティビティはない。

監査: FRU_FLT.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFに検出されたあらゆる障害。
b) 基本: 障害によって中断されたすべてのTOE機能。

監査: FRU_FLT.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFに検出されたあらゆる障害。

FRU_FLT.1 機能削減された耐障害性

下位階層: なし

FRU_FLT.1.1 TSFは、以下の障害[割付: *障害の種別のリスト*]が生じたとき、[割付:

***TOE機能(capabilities)のリスト*]の動作を保証しなければならない。**

依存性: **FPT_FLS.1 セキュアな状態を保持する障害**

FRU_FLT.2 制限付き耐障害性

下位階層: FRU_FLT.1

FRU_FLT.2.1 TSFは、以下の障害[割付: *障害の種別のリスト*]が生じたとき、**すべてのTOE機能(capabilities)**の動作を保証しなければならない。

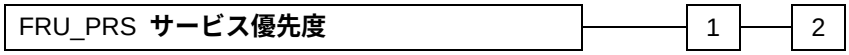
依存性: FPT_FLS.1　セキュアな状態を保持する障害

11.2 サービス優先度(FRU_PRS)

ファミリのふるまい

このファミリの要件は、低優先度アクティビティによって引き起こされる過度の干渉や遅延を受けることなく、TSC内の高優先度アクティビティが常にその動作を完遂できるよう、利用者とサブジェクトによるTSC内の資源利用をTSFが管理することを認める。

コンポーネントのレベル付け



FRU_PRS.1 制限付きサービス優先度は、サブジェクトによるTSC内の資源のサブセットの利用に対して優先度を提供する。

FRU_PRS.2 完全サービス優先度は、サブジェクトによるTSC内の全資源の利用に対して優先度を提供する。

管理: FRU_PRS.1、FRU_PRS.2

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) TSFにおける各サブジェクトへの優先度割付け。

監査: FRU_PRS.1、FRU_PRS.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 割当てられた優先度の使用に基づいた操作の拒否。

b) 基本: サービス機能の優先度を呼び出す割当て機能を使おうとするすべての試み。

FRU_PRS.1 制限付きサービス優先度

下位階層: なし

FRU_PRS.1.1 TSFは、TSFにおける各サブジェクトに優先度を割付けなければならない。

FRU_PRS.1.2 TSFは、[割付: *制御下にある資源*]への各アクセスが、優先度を割り付

けられたサブジェクトに基づいて調停されねばならないことを保証しなければならない。

依存性: **なし**

FRU_PRS.2 完全サービス優先度

下位階層: FRU_PRS.1

FRU_PRS.2.1 TSFは、TSFにおける各サブジェクトに優先度を割付けなければならない。

FRU_PRS.2.2 TSFは、**すべての共用可能資源**へのアクセスが、優先度を割り付けられたサブジェクトに基づいて調停されねばならないことを保証しなければならない。

依存性: **なし**

11.3 資源割当て(FRU_RSA)

ファミリのふるまい

このファミリの要件は、不正な資源専有のためにサービス拒否が生じないよう、利用者とサブジェクトによる資源利用をTSFが管理することを認める。

コンポーネントのレベル付け

FRU_RSA.1 最大割当ては、利用者及びサブジェクトが制御下にある資源を専有しないことを保証する、割当てメカニズムのための要件を提供する。

FRU_RSA.2 最小及び最大割当ては、利用者及びサブジェクトが、少なくとも最小限の特定された資源を常に持ち、かつ制御下にある資源を専有できないことを保証する、割当てメカニズムのための要件を提供する。

管理: FRU_RSA.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最大限度を特定すること。

管理: FRU_RSA.2

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最小及び最大限度を特定すること。

監査: FRU_RSA.1、FRU_RSA.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 資源制限による割当て操作の拒否。
b) 基本: TSF制御下にある資源に対して資源割当て機能を使おうとするすべての試み。

FRU_RSA.1 最大割当て

下位階層: なし

FRU_RSA.1.1 **TSFは、[選択: *個々の利用者*、*定義された利用者のグループ*、*サブジェクト*]が[選択: *同時に*、*特定した時間の間*]使用できる、以下の資源[割付: *制御下にある資源*]の最大割当てを実施しなければならない。**

依存性: **なし**

FRU_RSA.2 最小及び最大割当て

下位階層: FRU_RSA.1

FRU_RSA.2.1 TSFは、[選択: *個々の利用者*、*定義された利用者のグループ*、*サブジェクト*]が[選択: *同時に*、*特定した時間の間*]使用できる、以下の資源[割付: *制御下にある資源*]の最大割当てを実施しなければならない。

FRU_RSA.2.2 **TSFは、[選択: *個々の利用者*、*定義された利用者のグループ*、*サブジェクト*]が[選択: *同時に*、*特定した時間の間*]使用できる、各[割付: *制御下にある資源*]の最小量の提供を保証しなければならない。**

依存性: **なし**

12 クラスFTA: TOEアクセス

このファミリは、利用者セションの確立を制御する機能要件を特定する。

図12.1は、このクラスのコンポーネント構成を示す。

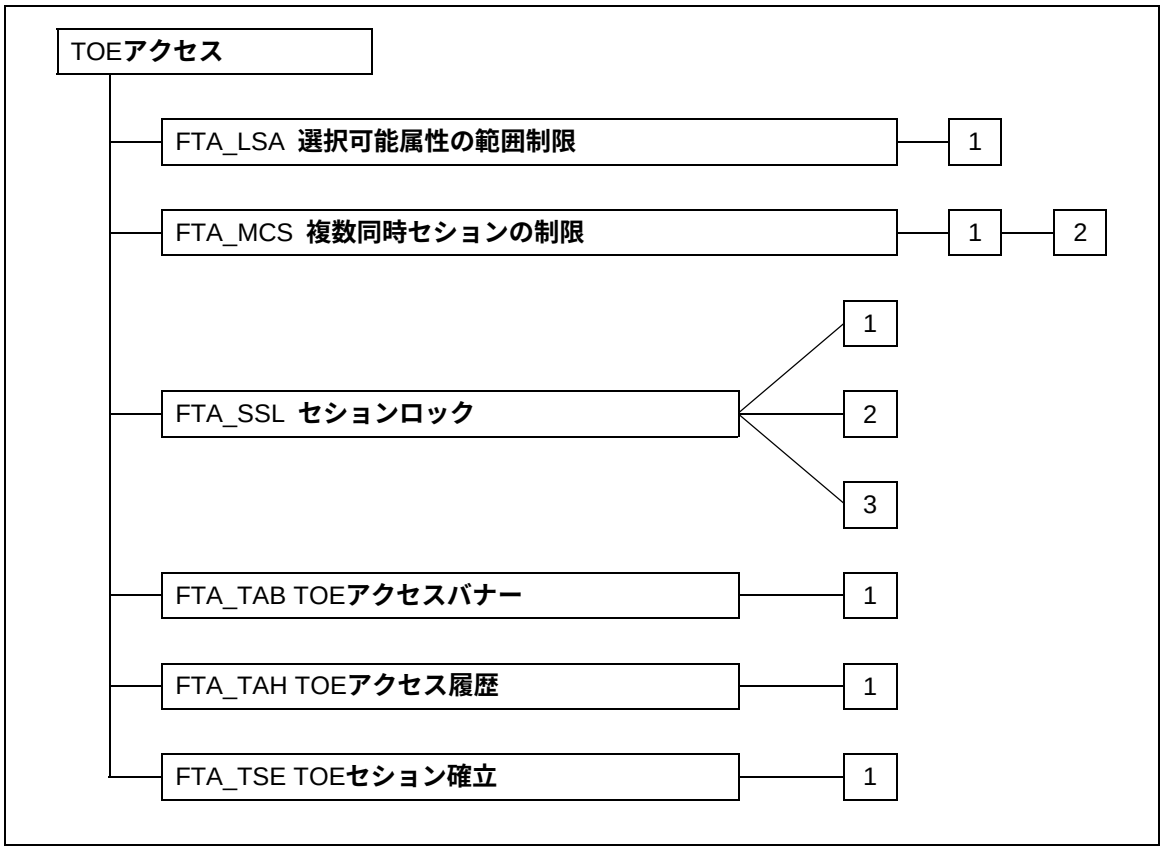


図12.1 - TOE**アクセスクラスのコンポーネント構成**

12.1 選択可能属性の範囲制限(FTA_LSA)

ファミリのふるまい

このファミリは、利用者がセションのため選択できるセションセキュリティ属性の範囲を制限する要件を定義する。

コンポーネントのレベル付け

FTA_LSA.1 選択可能属性の範囲制限は、セション確立中のセションセキュリティ属性の範囲をTOEが制限するための要件を提供する。

管理: FTA_LSA.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 管理者によるセションセキュリティ属性の範囲の管理。

監査: FTA_LSA.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: セションセキュリティ属性の選択におけるすべての失敗した試み;
b) 基本: セションセキュリティ属性の選択におけるすべての試み;
c) 詳細: 各セションセキュリティ属性の値の取得。

FTA_LSA.1 選択可能属性の範囲制限

下位階層: なし

FTA_LSA.1.1 **TSFは、[割付: *属性*]に基づき、セションセキュリティ属性[割付: *セションセキュリティ属性*]の範囲を制限しなければならない。**

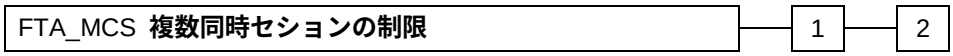
依存性: **なし**

12.2 複数同時セションの制限(FTA_MCS)

ファミリのふるまい

このファミリは、同一利用者に属する同時セションの数に対する制限を設ける要件を定義する。

コンポーネントのレベル付け



FTA_MCS.1 複数同時セションの基本制限は、TSFのすべての利用者に適用する制限を提供する。

FTA_MCS.2 複数同時セションの利用者属性ごと制限は、関連したセキュリティ属性に基づく同時セション数の制限を特定する能力を要求することによって、FTA_MCS.1を拡張する。

管理: FTA_MCS.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 管理者による最大許可同時利用者セション数の管理。

管理: FTA_MCS.2

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 管理者による最大許可同時利用者セション数運営規則の管理。

監査: FTA_MCS.1、FTA_MCS.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 複数同時セションの制限に基づく新しいセションの拒否。

b) 詳細: 現時点の同時利用者セション数及び利用者セキュリティ属性の取得。

FTA_MCS.1 複数同時セションの基本制限

下位階層: なし

FTA_MCS.1.1 TSFは、同一利用者に属する同時セションの最大数を制限しなければならない。

FTA_MCS.1.2 TSFは、デフォルトで、利用者あたり[割付: *デフォルト数*]セションの制

限を実施しなければならない。

依存性: **FIA_UID.1 識別のタイミング**

FTA_MCS.2 複数同時セションの利用者属性ごと制限

下位階層: FTA_MCS.1

FTA_MCS.2.1 TSFは、**規則[割付: *最大同時セション数の規則*]に従って**、同一利用者に属する同時セションの最大数を制限しなければならない。

FTA_MCS.2.2 TSFは、デフォルトで、利用者あたり[割付: *デフォルト数*]セションの制限を実施しなければならない。

依存性: FIA_UID.1 **識別のタイミング**

12.3 セションロック(FTA_SSL)

ファミリのふるまい

このファミリは、TSF起動及び利用者起動の、対話セションのロック及びロック解除のための能力をTSFが提供するための要件を定義する。

コンポーネントのレベル付け

FTA_SSL.1 TSF起動セションロックは、利用者の動作がない特定した時間後の、システム起動の対話セションロックを含む。

FTA_SSL.2 利用者起動ロックは、利用者が、利用者自身の対話セションのロックとロック解除するための能力を提供する。

FTA_SSL.3 TSF起動による終了は、TSFが、利用者の動作がない特定した時間後にセションを終了するための要件を提供する。

管理: FTA_SSL.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 個々の利用者についてロックアウトを生じさせる利用者が非アクティブである時間の特定;
b) ロックアウトを生じさせる利用者が非アクティブであるデフォルト時間の特定;
c) セションをロック解除する前に生じるべき事象の管理。

管理: FTA_SSL.2

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) セションをロック解除する前に生じるべき事象の管理。

管理: FTA_SSL.3

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定;
b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の

特定。

監査: FTA_SSL.1、FTA_SSL.2
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである。

a) 最小: セションロックメカニズムによる対話セションのロック。
b) 最小: 対話セションの、成功したロック解除。
c) 基本: 対話セションのロック解除におけるすべての試み。

監査: FTA_SSL.3
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: セションロックメカニズムによる対話セションの終了。

FTA_SSL.1 TSF起動セションロック

下位階層: なし

FTA_SSL.1.1 **TSFは、[割付: *利用者が非アクティブである時間間隔*]の後、以下によって対話セションをロックしなければならない:**

a) 表示装置を消去するか上書きして、現在の内容を読めなくする;
b) 利用者のデータアクセス/表示装置について、セションのロック解除以外のいかなる動作も禁止する。

FTA_SSL.1.2 **TSFは、セションのロック解除に先立ち、以下の事象を生じさせることを要求しなければならない: [割付: *生じさせる事象*]。**

依存性: **FIA_UAU.1 認証のタイミング**

FTA_SSL.2 利用者起動ロック

下位階層: なし

FTA_SSL.2.1 **TSFは、利用者自身の対話セションの利用者起動ロックを、以下によって許可しなければならない:**

a) 表示装置を消去するか上書きして、現在の内容を読めなくする;
b) 利用者のデータアクセス/表示装置について、セションのロック解除以外のいかなる動作も禁止する。

FTA_SSL.2.2 **TSFは、セションのロック解除に先立ち、以下の事象を生じさせることを要求しなければならない: [割付: *生じさせる事象*]。**

依存性: **FIA_UAU.1 認証のタイミング**

FTA_SSL.3 TSF起動による終了

下位階層: なし

FTA_SSL.3.1 **TSFは、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。**

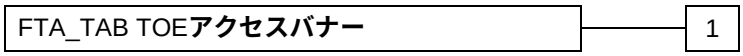
依存性: **なし**

12.4 TOE**アクセスバナー**(FTA_TAB)

ファミリのふるまい

このファミリは、利用者に対し、TOEの適切な利用に関する、設定可能な勧告的警告メッセージを表示する要件を定義する。

コンポーネントのレベル付け



FTA_TAB.1 デフォルトTOEアクセスバナーは、TOEアクセスバナーに対する要件を提供する。このバナーは、セションの確立のための対話に先立って表示される。

管理: FTA_TAB.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 許可管理者によるバナーの維持。

監査: FTA_TAB.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FTA_TAB.1 デフォルトTOEアクセスバナー

下位階層: なし

FTA_TAB.1.1 **利用者セション確立前に、TSFは、TOEの不正な使用に関する勧告的警告メッセージを表示しなければならない。**

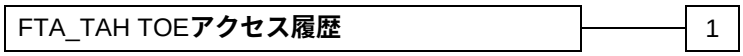
依存性: **なし**

12.5 TOE**アクセス履歴**(FTA_TAH)

ファミリのふるまい

このファミリは、セション確立の成功時に、利用者のアカウントにアクセスした成功及び不成功の試みの履歴を、TSFが利用者に対して表示するための要件を定義する。

コンポーネントのレベル付け



FTA_TAH.1 TOEアクセス履歴は、セションを確立するための以前の試みに関連する情報をTOEが表示するための要件を提供する。

管理: FTA_TAH.1

予見させる管理アクティビティはない。

監査: FTA_TAH.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FTA_TAH.1 TOE**アクセス履歴**

下位階層: なし

FTA_TAH.1.1 **セション確立の成功時、TSFは、その利用者に対する最後の成功したセション確立の[選択: *日付*、*時刻*、*方法*、*場所*]を表示しなければならない。**

FTA_TAH.1.2 **セション確立の成功時、TSFは、最後の不成功のセション確立の試みの[選択: *日付*、*時刻*、*方法*、*場所*]、及び最後に成功したセション確立以後の不成功な試みの数を表示しなければならない。**

FTA_TAH.1.3 **TSFは、利用者に情報をレビューする機会を与えることなく利用者インタフェースからアクセス履歴情報を消去してはならない。**

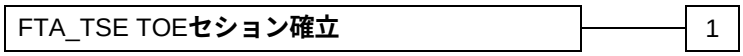
依存性: **なし**

12.6 TOE**セション確立**(FTA_TSE)

ファミリのふるまい

このファミリは、TOEとセションを確立するための利用者許可を拒否する要件を定義する。

コンポーネントのレベル付け



FTA_TSE.1 TOEセション確立は、属性に基づき、利用者がTOEにアクセスするのを拒否する要件を提供する。

管理: FTA_TSE.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 許可管理者によるセション確立条件の管理。

監査: FTA_TSE.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: セション確立メカニズムによるセション確立の拒否。
b) 基本: 利用者セション確立におけるすべての試み。
c) 詳細: 選択されたアクセスパラメタ(例:アクセスの場所、アクセスの日時)の値の取得。

FTA_TSE.1 TOE**セション確立**

下位階層: なし

FTA_TSE.1.1 TSFは、[割付: *属性*]に基づきセション確立を拒否できなければならない。

依存性: **なし**

13 クラスFTP: 高信頼パス/チャネル

このクラスのファミリは、利用者とTSF間の高信頼通信パス、及びTSFと他の高信頼IT製品間の高信頼通信チャネルのための要件を提供する。高信頼パスとチャネルは、以下の共通の性質を持つ:

- 通信パスは、TSFデータとコマンドの識別されたサブセットをTSFの残りの部分と利用者データから隔離する内部及び外部の通信チャネルを(そのコンポーネントに対して適切に)使用して構成される。

- 通信パスの使用は、利用者及び/またはTSFによって(そのコンポーネントに対して適切に)開始されることができる。

- 通信パスは、利用者が正しいTSFと通信しているということと、TSFが正しい利用者と通信しているということの(そのコンポーネントに対して適切に)保証を提供する能力を持つ。

このパラダイムにおいて、**高信頼チャネル**は、チャネルのどちらの側からでも開始することができる通信チャネルであり、チャネルの両端の識別情報に関して、否認不可の性質を提供する。

高信頼パスは、利用者が、TSFとの保証された直接対話を通して機能を実行する手段を提供する。高信頼パスは、通常、最初の識別及び/または認証のような利用者アクションのために望ましいものであるが、利用者セション中の別のときにも必要になることがある。高信頼パス交換は、利用者あるいはTSFによって開始されることができる。 高信頼パスを介した利用者応答は、信頼できないアプリケーションによる改変やそれへの暴露から保護されていることが保証される。

図13.1は、このクラスのコンポーネント構成を示す。

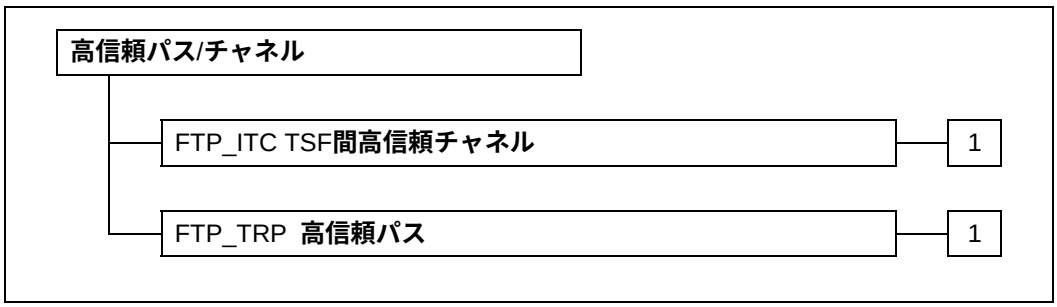


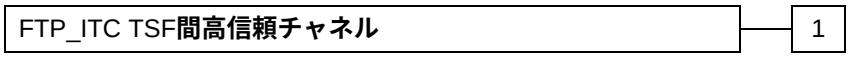
図13.1 - **高信頼パス/チャネルクラスのコンポーネント構成**

13.1 TSF**間高信頼チャネル**(FTP_ITC)

ファミリのふるまい

このファミリは、セキュリティ上の重要な操作のために、TSFと他の高信頼IT製品間に高信頼チャネルを生成するための要件を定義する。このファミリは、TOEと他の高信頼IT製品間で利用者あるいはTSFデータのセキュアな通信に対する要求があるときは、常に含まれるべきである。

コンポーネントのレベル付け



FTP_ITC.1 TSF間高信頼チャネルは、TSFが、それ自身と他の高信頼IT製品間に高信頼通信チャネルを提供することを要求する。

管理: FTP_ITC.1

以下のアクションはFMTにおける管理機能と考えられる:

a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定。

監査: FTP_ITC.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 高信頼チャネル機能の失敗。
b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。
c) 基本: 高信頼チャネル機能のすべての使用の試み。
d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

FTP_ITC.1 TSF**間高信頼チャネル**

下位階層: なし

FTP_ITC.1.1 **TSFは、それ自身とリモート高信頼IT製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。**

FTP_ITC.1.2 **TSFは、[選択: *TSF*、*リモート高信頼IT製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。**

FTP_ITC.1.3 **TSFは、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。**

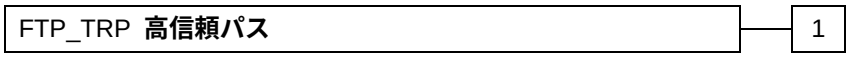
依存性: **なし**

13.2 高信頼パス(FTP_TRP)

ファミリのふるまい

このファミリは、利用者とTSF間に高信頼通信を確立し維持するための要件を定義する。高信頼パスは、どのようなセキュリティ関連の対話に対しても要求されるかも知れない。高信頼パス交換は、TSFとの対話の間に利用者によって開始されることもあり、高信頼パスを介してTSFが利用者との通信を確立することもある。

コンポーネントのレベル付け



FTP_TRP.1 高信頼パスは、PP/STの著者により定義された事象のセットに対して、TSFと利用者間に高信頼パスが提供されることを要求する。利用者及び/またはTSFは、信頼パスを開始する能力を持つことができる。

管理: FTP_TRP.1

以下のアクションはFMTにおける管理機能と考えられる:

a) もしサポートされていれば、高信頼パスを要求するアクションの設定。

監査: FTP_TRP.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 高信頼パス機能の失敗。
b) 最小: もし得られれば、すべての高信頼パス失敗に関係する利用者の識別情報。
c) 基本: 高信頼パス機能の使用についてのすべての試み。
d) 基本: もし得られれば、すべての高信頼パス呼出に関係する利用者の識別情報。

FTP_TRP.1 高信頼パス

下位階層: なし

FTP_TRP.1.1 **TSFは、それ自身と[選択: *リモート*、*ローカル*]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。**

FTP_TRP.1.2 **TSFは、[選択: *TSF*、*ローカル利用者*、*リモート利用者*]が、高信頼パスを介して通信を開始することを許可しなければならない。**

FTP_TRP.1.3 **TSFは、[選択:** ***最初の利用者認証*****、[割付:** ***高信頼パスが要求される他のサービス*****]]に対して、高信頼パスの使用を要求しなければならない。**

依存性: **なし**

附属書A

(参考)

セキュリティ機能要件適用上の注釈

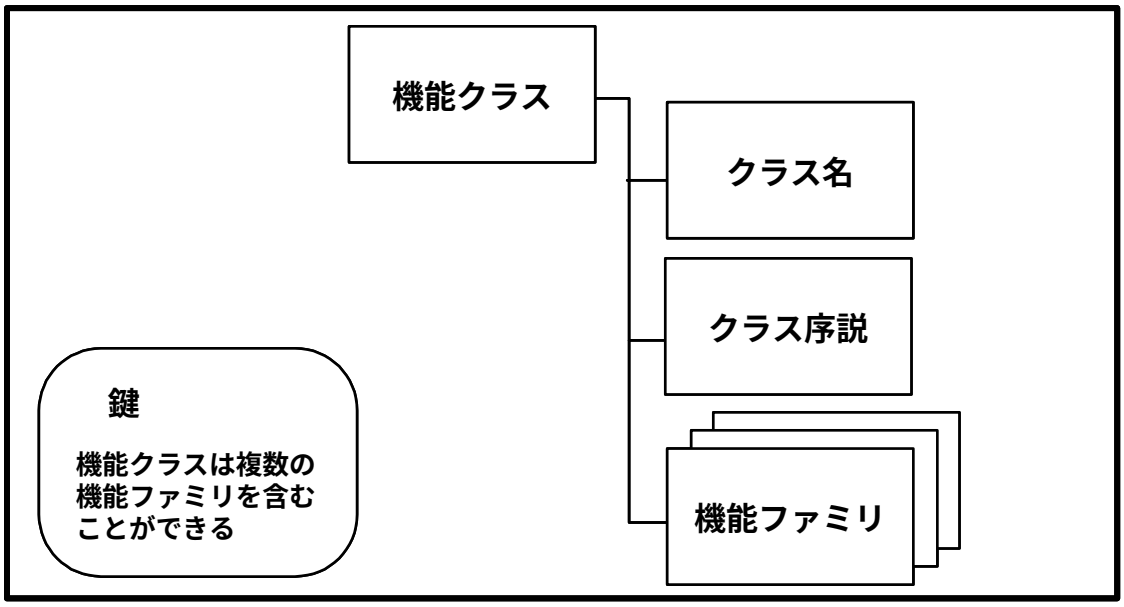
この附属書は、パート2本文に記載されたファミリ及びコンポーネントについての参考情報を載せたもので、コンポーネントを使用する利用者、開発者あるいは評価者によって必要となろう。適切な情報を見つけ出すのに便利なよう、附属書におけるクラス、ファミリ、及びコンポーネントの表現は、パート2の本文と同様である。この附属書は参考情報となる節だけを取り上げているので、附属書におけるクラス、ファミリ、及びコンポーネントの構造は、パート2の本文におけるものと異なっている。

A.1　注釈の構造

この節は、CCの機能要件に関係する注釈の内容と表現を定義する。

A.1.1　クラス構造

次の図A.1は、この附属書における機能クラス構造を表している。



図A.1 - 機能クラス構造

A.1.1.1　クラス名

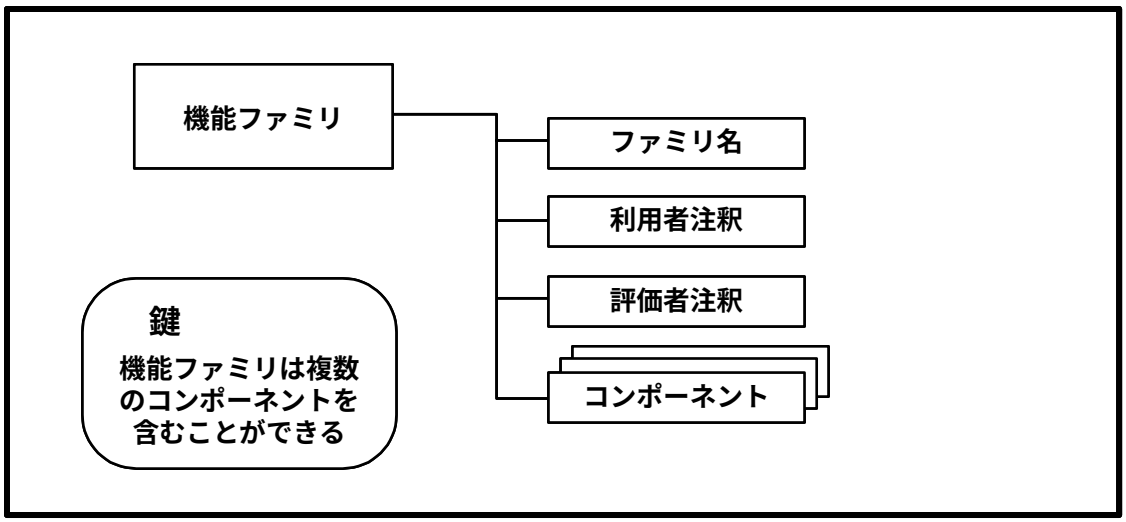
これは、CCのパート2で定義された、クラスの一意な名前である。

A.1.1.2 クラス序説

この附属書におけるクラス序説は、クラスのファミリとコンポーネントの使用についての情報を提供する。この情報は、各クラスにおけるファミリ、及び各ファミリにおけるコンポーネント間の階層関係を示す、各クラスの組織を記述した参考図をもって完結する。

A.1.2 ファミリ構造

図A.2は、適用上の注釈のために、図形式で機能ファミリ構造を表したものである。



図A.2 - 適用上の注釈のための機能ファミリ構造

A.1.2.1 ファミリ名

これは、CCのパート2で定義された、ファミリの一意な名前である。

A.1.2.2 利用者のための注釈

*利用者のための注釈*には、そのファミリの潜在的な利用者、つまりPP、ST及び機能パッケージの作成者、及び機能コンポーネントを具体化するTOEの開発者が関心を持つ追加情報が書かれる。書かれたものは参考情報であり、そのコンポーネントを使用するときに特別な注意が要求されるような、使用及び領域の制限についての警告が含まれるかもしれない。

A.1.2.3 評価者のための注釈

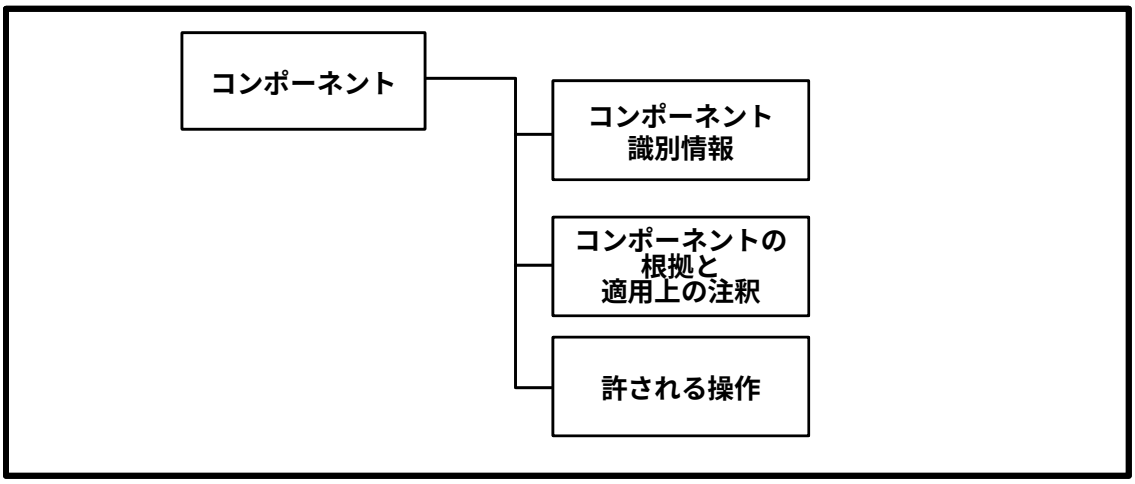
*評価者のための注釈*には、そのファミリのコンポーネントへの準拠を主張するTOEの開発者及び評価者が関心を持つ情報が書かれる。書かれたものは参考情報であり、TOEを評価するうえで特別な注意が必要となるかもしれないさまざまな領域をカバーできる。こ

れは、評価者にとって特別な関心ごとである注意や警告はもちろん、意味の明確化と要件を解釈するための方法の詳細化を含めることができる。

これら利用者のための注釈及び評価者のための注釈は必須ではなく、適切な場合にだけ記述される。

A.1.3 コンポーネント構造

図A.3は、適用上の注釈のための機能コンポーネント構造を表す。



図A.3 - 機能コンポーネント構造

A.1.3.1 コンポーネント識別情報

これは、CCのパート2で定義された、コンポーネントの一意な名前である。

A.1.3.2 コンポーネントの根拠と適用上の注釈

コンポーネントに関係したいかなる特定の情報も、この節に書くことができる。

- *根拠*は、根拠における一般的な記述を特定のレベルに対して詳細化する根拠の詳述を含み、レベル固有の敷衍が要求される場合にだけ使用されるべきである。
- *適用上の注釈*は、それが特定のコンポーネントに付随するものであるので、説明的に制限をつけるような形で付加的な詳細情報を記す。この詳細情報は、この附属書のA.1.2節に記述した、利用者のための注釈、及び/または評価者のための注釈に付随させることができる。この詳細情報は、依存性の性質を説明するために使用することができる(例えば、共有情報、あるいは共有動作)。

この節は必須のものではなく、適切な場合にだけ記述される。

A.1.3.3 **許可された操作**

各コンポーネントのこの部分は、コンポーネントの許可された操作に関するガイダンスが書かれる。

この節は必須のものではなく、適切な場合にだけ記述する。

A.2 依存性

表A.1-機能コンポーネントに対する依存性の表は、それらの直接的、間接的、あるいは自由選択の依存性を示す。ある機能コンポーネントが依存する各々のコンポーネントは、列に配置される。各機能コンポーネントは、行に配置される。表のセルにおける値は、列に書かれたコンポーネントが、行に書かれたコンポーネントによって、直接的に要求されるか(クロス「x」で表示)、間接的に要求されるか(ダッシュ「-」で表示)、あるいは自由選択的に要求されるか(「o」で表示)を示す。自由選択の依存性を持つコンポーネントの例はFDP_ETC.1で、これは、FDP_ACC.1あるいはFDP_IFC.1のどちらかを要求する。それで、FDP_ACC.1が存在すれば、FDP_IFC.1は必要ではなく、その逆もある。もし文字がなければ、そのコンポーネントは他のコンポーネントに依存しない。

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FAU_ARP.1					-	x																											-					
FAU_GEN.1																																	x					
FAU_GEN.2					x																		x										-					
FAU_SAA.1					x																												-					
FAU_SAA.2																							x															
FAU_SAA.3																																						
FAU_SAA.4																																						
FAU_SAR.1					x																												-					
FAU_SAR.2					-		x																										-					
FAU_SAR.3					-		x																										-					
FAU_SEL.1					x																		-				x	-				-					
FAU_STG.1					x																												-					
FAU_STG.2					x																												-					
FAU_STG.3					-			x																									-					
FAU_STG.4					x																												-					

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FCO_NRO.1																							x															
FCO_NRO.2																							x															
FCO_NRR.1																							x															
FCO_NRR.2																							x															
FCS_CKM.1	-								-	o	x	o	-	-	-	-	-						-		-	x	-		-									
FCS_CKM.2	-								o	-	x	-	-	-	-	-	o						-		-	x	-		-									
FCS_CKM.3	-								o	-	x	-	-	-	-	-	o						-		-	x	-		-									
FCS_CKM.4	-								o	-	-	-	-	-	-	-	o						-		-	x	-		-									
FCS_COP.1	-								o	-	x	-	-	-	-	-	o						-		-	x	-		-									
FDP_ACC.1													-	x	-	-							-		-		-		-									
FDP_ACC.2													-	x	-	-							-		-		-		-									
FDP_ACF.1													x	-	-	-							-		-		x		-									
FDP_DAU.1																																						
FDP_DAU.2																							x															
FDP_ETC.1													o	-	o	-							-		-		-		-									
FDP_ETC.2													o	-	o	-							-		-		-		-									
FDP_IFC.1													-	-	-	x							-		-		-		-									
FDP_IFC.2													-	-	-	x							-		-		-		-									
FDP_IFF.1													-	-	x	-							-		-		x		-									
FDP_IFF.2													-	-	x	-							-		-		x		-									
FDP_IFF.3			x										-	-	x	-							-		-		-		-									
FDP_IFF.4			x										-	-	x	-							-		-		-		-									
FDP_IFF.5				x									-	-	x	-							-		-		-		-									
FDP_IFF.6			x										-	-	x	-							-		-		-		-									
FDP_ITC.1													o	-	o	-							-		-		x		-									
FDP_ITC.2													o	-	o	-							-		-		-		-						x		o	o
FDP_ITT.1													o	-	o	-							-		-		-		-									

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FDP_ITT.2													o	-	o	-						-		-		-		-									o	o
FDP_ITT.3													o	-	o	-		x				-		-		-		-									o	o
FDP_ITT.4													o	-	o	-			x			-		-		-		-									o	o
FDP_RIP.1																																						
FDP_RIP.2																																						
FDP_ROL.1													o	-	o	-						-		-		-		-									o	o
FDP_ROL.2													o	-	o	-						-		-		-		-									o	o
FDP_SDI.1																																						
FDP_SDI.2																																						
FDP_UCT.1													o	-	o	-						-		-		-		-									o	o
FDP_UIT.1													o	-	o	-						-		-		-		-									o	o
FDP_UIT.2													o	-	o	-				x		-		-		-		-									x	
FDP_UIT.3													o	-	o	-				x		-		-		-		-									x	
FIA_AFL.1																					x	-																
FIA_ATD.1																																						
FIA_SOS.1																																						
FIA_SOS.2																																						
FIA_UAU.1																						x																
FIA_UAU.2																						x																
FIA_UAU.3																																						
FIA_UAU.4																																						
FIA_UAU.5																																						
FIA_UAU.6																																						
FIA_UAU.7																					x	-																
FIA_UID.1																																						
FIA_UID.2																																						
FIA_USB.1																				x																		

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_MTD.3	FMT_REV.1	FMT_SAE.1	FMT_SMR.1	FMT_SMR.2	FMT_SMR.3	FPR_ANO.1	FPR_ANO.2	FPR_PSE.1	FPR_PSE.2	FPR_PSE.3	FPR_UNL.1	FPR_UNO.1	FPR_UNO.2	FPR_UNO.3	FPR_UNO.4	FPT_AMT.1	FPT_FLS.1	FPT_ITA.1	FPT_ITC.1	FPT_ITI.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FMT_MOF.1																							-					x																													
FMT_MSA.1													o	-	o	-							-		-		-		x																													
FMT_MSA.2	x												o	-	o	-							-		x		-		x																													
FMT_MSA.3													-	-	-	-							-		x		-		x																													
FMT_MTD.1																							-						x																													
FMT_MTD.2																							-					x	x																													
FMT_MTD.3	x																						-					x	-																													
FMT_REV.1																							-						x																													
FMT_SAE.1																							-						x			x																											
FMT_SMR.1																							x																																			
FMT_SMR.2																																																													
FMT_SMR.3																							-						x																													
FPR_ANO.1																																																											
FPR_ANO.2																																																											
FPR_PSE.1																																																											
FPR_PSE.2																							x																																			
FPR_PSE.3																																																											
FPR_UNL.1																																																											
FPR_UNO.1																																																											
FPR_UNO.2																																																											
FPR_UNO.3																																																											
FPR_UNO.4																																																											
FPT_AMT.1																																																											
FPT_FLS.1	x																																																										
FPT_ITA.1																																																											
FPT_ITC.1																																																											
FPT_ITI.1																																																											

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FPT_ITI.2																																					
FPT_ITT.1																																					
FPT_ITT.2																																					
FPT_ITT.3																																x					
FPT_PHP.1																							-	x				-									
FPT_PHP.2																							-	x				-									
FPT_PHP.3																																					
FPT_RCV.1	x	x																												-					x		
FPT_RCV.2	x	x																												-					x		
FPT_RCV.3	x	x																												-					x		
FPT_RCV.4	x																																				
FPT_RPL.1																																					
FPT_RVM.1																																					
FPT_SEP.1																																					
FPT_SEP.2																																					
FPT_SEP.3																																					
FPT_SSP.1																																x					
FPT_SSP.2																																x					
FPT_STM.1																																					
FPT_TDC.1																																					
FPT_TRC.1																																x					
FPT_TST.1																														x							
FRU_FLT.1	-																														x						
FRU_FLT.2	-																														x						
FRU_PRS.1																																					
FRU_PRS.2																																					
FRU_RSA.1																																					

表A.1 - 機能コンポーネントの依存性

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPR_UNO.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FRU_RSA.2																																						
FTA_LSA.1																																						
FTA_MCS.1																							x															
FTA_MCS.2																							x															
FTA_SSL.1																						x	-															
FTA_SSL.2																						x	-															
FTA_SSL.3																																						
FTA_TAB. 1																																						
FTA_TAH.1																																						
FTA_TSE. 1																																						
FTP_I TC. 1																																						
FTP_TRP. 1																																						

附属書B

(参考)

機能クラス、ファミリ、コンポーネント

以下の附属書CからMは、このパート2の本文で定義された機能クラスに対する適用上の注釈を提供する。

附属書C

(参考)

セキュリティ監査(FAU)

CC監査ファミリは、PP/ST作成者が利用者のアクティビティの監視に対する要件を定義することを許し、場合によっては、実際の、可能性がある、あるいはすぐにも起こりそうなTSP侵害の検出に対する要件の定義を認める。TOEのセキュリティ監査機能は、セキュリティ関連事象の監視に役立つものとして定義され、かつ、セキュリティ侵害に対する抑止として働く。監査ファミリの要件は、分析ツール、侵害警報及びリアルタイム分析はもとより、監査データ保護、記録フォーマット及び事象選択を含む機能についても触れている。監査証跡は、直接的(例えば人間が読めるフォーマットで監査証跡を保存)であれ、間接的(例えば監査分類整理ツールを使う)であれ、その両方であれ、人間が読めるフォーマットで提供されるべきである。

セキュリティ監査要件の作成時、PP/ST作成者は、監査ファミリとコンポーネント間の内部関係に注意を払うべきである。ファミリ/コンポーネントの依存関係リストに準拠した監査要件のセットを特定したとしても、結果として監査機能が不完全なものになる可能性がある(例えば、監査機能がセキュリティ関連の事象をすべて監査するよう要求しながら、それらを、個々の利用者あるいはオブジェクトのような妥当な基準に基づいて制御するための選択ができない)。

分散環境での監査要件:

ネットワーク及びその他の大規模システムに対する監査要件の実装は、スタンドアロンシステムで必要とされるものと大きく異なることがある。システムがより大きく、より複雑かつアクティブになるほど、収集するものの解釈が(あるいは、格納することすら)難しくなるので、どの監査データを集めるか、それをどう管理すべきかについていっそうよく考える必要が出てくる。監査事象の、時間でソートされたリストあるいは「証跡」という従来の概念は、多数の事象が同時に恣意的に発生するグローバルな非同期ネットワークには適用できないかもしれない。

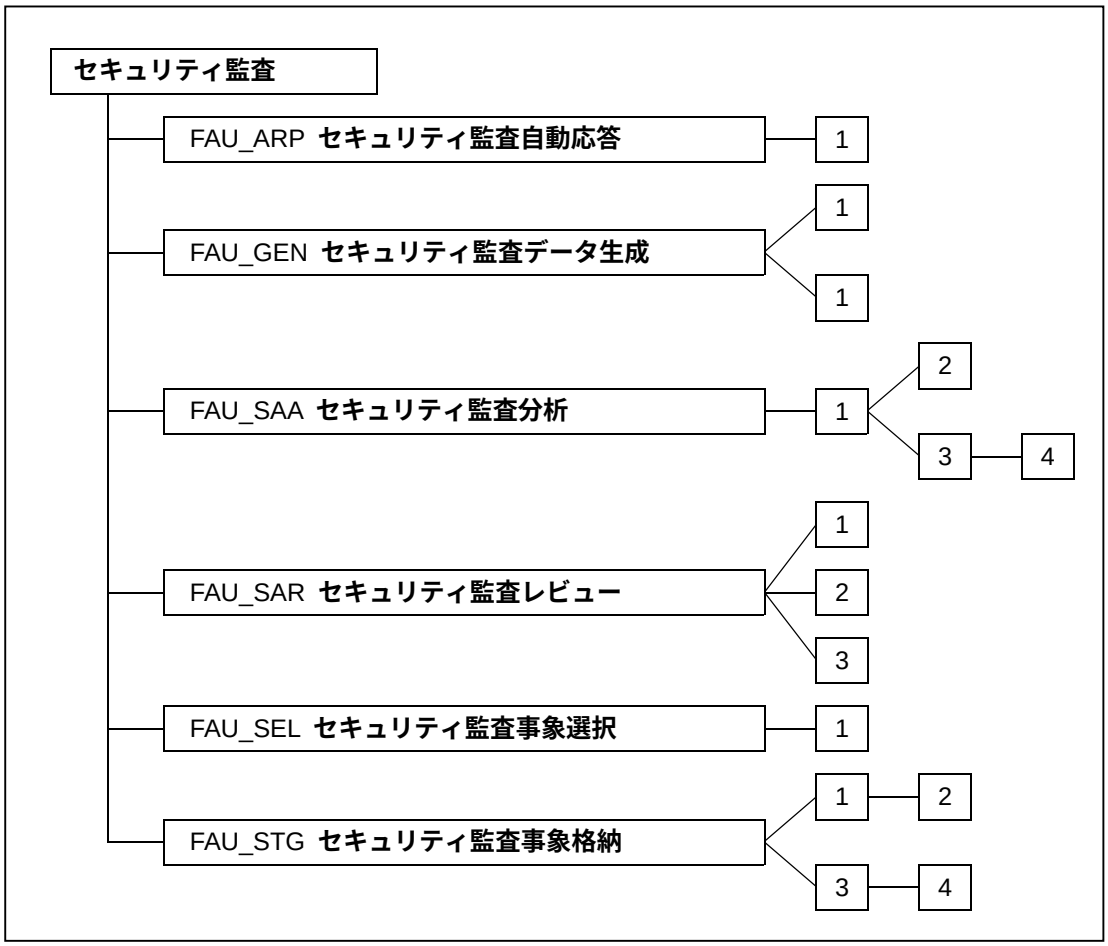
また、分散TOEの異なるホストやサーバは、異なる命名方針や値を持つかもしれない。監査レビューのためのシンボリック名表現は、重畳と「名前の衝突」を避けるため、ネットワーク全体での取り決めの必要があるかもしれない。

監査リポジトリが分散システムにおいて有用な機能を提供するには、一つの多目的監査リポジトリ - その部分部分が、潜在的に多様性を持つ許可利用者からアクセスできるもの - が必要かもしれない。

最後に、許可利用者による権限の悪用は、管理者のアクションに関連する監査データの

ローカルな格納を体系的に避けることによって対処する必要がある。

図C.1は、セキュリティ監査クラスのコンポーネント構成を示している。



図C.1 - セキュリティ監査クラスのコンポーネント構成

C.1　セキュリティ監査自動応答(FAU_ARP)

セキュリティ監査自動応答ファミリは、監査事象を扱うための要件を記述する。この要件には、警報またはTSFアクション(自動応答)の要件を含めることができる。例えば、TSFには、リアルタイム警報の生成、違反プロセスの終了、サービスの停止、利用者アカウントの切り離し/無効化などを含めることができる。

適用上の注釈

ある監査事象は、もしFAU_SAAコンポーネントによってそのように示されていれば、「セキュリティ侵害の可能性」と定義される。

FAU_ARP.1　セキュリティアラーム

利用者のための適用上の注釈

警報の事象において、追求アクションのためのアクションがとられるべきである。このアクションは、許可利用者に通知したり、可能な封じ込めアクションのセットを許可利用者に提示したり、あるいは修正アクションをとったりするものにできる。PP/ST作成者は、アクションのタイミングについて注意深く考慮すべきである。

操作

割付:

FAU_ARP.1.1において、PP/ST作成者は、セキュリティ侵害の可能性が発生した場合にとるアクションを特定すべきである。そのようなリストの例: 「許可利用者に通知する、セキュリティ侵害の可能性を生じさせたサブジェクトを停止する」。また、とられるべきアクションを許可利用者が特定できると特定することもできる。

C.2 **セキュリティ監査データ生成**(FAU_GEN)

セキュリティ監査データ生成ファミリは、セキュリティ関連事象に対してTSFが生成すべき監査事象を特定するための要件を含む。

このファミリは、監査サポートを要求するすべてのコンポーネントへの依存性を持たない形式で提示される。各コンポーネントは、詳しく説明された監査セクションを持ち、その機能分野に対して監査される事象を列挙する。PP/ST作成者がPP/STを組み立てる際、監査領域に書かれた事項がこのコンポーネントの変数を完成させるのに使われる。このように、ある機能領域に対して何が監査され得るかの詳細は、その機能領域においてローカライズされる。

監査対象事象のリストは、全面的にPP/ST内の他の機能ファミリに依存する。そのため、各ファミリの定義は、そのファミリ特有の監査対象事象のリストを含むべきである。その機能ファミリで特定された監査対象事象リスト内の各々の監査対象事象は、そのファミリで特定された監査事象生成のレベルの一つ(すなわち、最小、基本、詳細)に対応すべきである。これは、適切な監査対象事象がすべてPP/STの中で特定されることを保証するのに必要な情報をPP/ST作成者に提供する。次の例は、どのようにして監査対象事象が適切な機能ファミリの中で特定されるかを示す。

> 「FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:
>
> a) 最小: 利用者セキュリティ属性管理機能の成功した使用;
>
> b) 基本: 利用者セキュリティ属性管理機能を使用しようとするすべての試み;
>
> c) 基本: どの利用者セキュリティ属性が改変されたかの識別;
>
> d) 詳細: 特定の機密属性データ項目(パスワードや暗号鍵など)を除き、属性の新しい値は保存されるべきである。」

選択した機能コンポーネントごとに、そのコンポーネントで指定されている監査対象事象は、FAU_GENで指定されたレベル及びそれ以下のレベルで監査対象とすべきである。例えば、先の例で「基本」がFAU_GENで選択された場合、a)、b)、及びc)を監査対象とすべきである。

監査対象事象の分類は階層的であることに注意しなければならない。例えば、「基本監査生成」が必要とされる場合、「最小」または「基本」のどちらかに識別されるすべての監査対象事象は、適切な割付操作を使用してPP/STに含まれねばならない。ただし、上位レベルの事象が単に下位レベルの事象を詳細化しているだけの場合は除かれる。「詳細監査事象」が必要とされる場合は、すべての識別された監査対象事象(最小、基本、及び詳細)がPP/STに含まれねばならない。

PP/ST作成者は、所定の監査レベルで要求されるものを超えた他の監査対象事象を含めるような決定をすることができる。例えば、他のPP/STの制約と競合していくつかの能力が使えなくなるため(例えば、入手できないデータの収集が要求されるなど)、「基本」能力の大半を持っていながら、そのPP/STは「最小」監査機能だけを要求することがある。

適用上の注釈

監査対象事象を生成する機能は、PPまたはSTにおいて、機能要件として特定されるべきである。

以下は、各PP/ST機能コンポーネント内で監査対象と定義されるべき事象の種別の例である。

a) TSC範囲内で、サブジェクトのアドレス空間に対するオブジェクトの導入;

b) オブジェクトの削除;

c) アクセス権あるいは能力の配付あるいは取消し;

d) サブジェクトあるいはオブジェクトセキュリティ属性の変更;

e) サブジェクトからの要求の結果としてTSFが実行する方針チェック;

f) 方針チェックをバイパスするアクセス権の使用;

g) 識別と認証機能の使用;

h) オペレータ及び/または許可利用者が行うアクション(例えば、人間が読めるラベルのようなTSF保護メカニズムの抑制);

i) リムーバブルメディアに対するデータのインポート/エクスポート(例えば、印刷出力、テープ、ディスケット)。

FAU_GEN.1　監査データ生成

利用者のための適用上の注釈

このコンポーネントは、監査記録が生成されるべき監査対象事象及び監査記録の中で提供される情報を識別するための要件を定義する。

TSPが個々の利用者識別情報を監査事象に関連付けることを要求しない場合は、FAU_GEN.1が、それ自身によって使われてもよいことがある。これは、PP/STがプライバシー要件も包含する場合に適切であろう。利用者識別情報が組み込まれねばならない場合は、FAU_GEN.2が追加されて使われよう。

評価者のための適用上の注釈

FPT_STMへの依存性が存在する。該当するTOEで正確な時間が重要でない場合は、この依存性の削除を正当化し得る。

操作

選択:

FAU_GEN.1.1bでは、PP/ST作成者は、PP/STに含まれる他の機能コンポーネントの監査セクションで呼び出される監査対象事象のレベルを選択すべきである。このレベルは、「最小」、「基本」、「詳細」、または「指定なし」である。もし、「指定なし」を選択した場合、PP/ST作成者は、すべての必要な監査対象事象をFAU_GEN.1.1cに書き入れるべきであり、エレメントのこのパート(b項)は全体を削除できる。

割付:

FAU_GEN.1.1cでは、PP/ST作成者は、監査対象事象のリストに含められるその他の特別に定義された監査対象事象のリストを割り付けるべきである。これらの事象は、特定のアプリケーションプログラミングインタフェース(API)の使用を通して生成される事象はもとより、FAU_GEN.1.1bで要求されるものより監査レベルの高い機能要件の監査対象事象などが考えられる。

FAU_GEN.1.2bでは、PP/ST作成者は、PP/STに含まれる監査対象事象ごとに、監査事象記録に含まれるその他の監査関連情報のリストを割り付けるべきである。

FAU_GEN.2　利用者識別情報の関連付け

利用者のための適用上の注釈

このコンポーネントは、個々の利用者識別情報のレベルに対して監査対象事象の内容をどこまでとるべきかの要件に対応する。このコンポーネントは、FAU_GEN.1 監査データ生成に追加する形で使われるべきである。

監査とプライバシー要件の間には、潜在的な対立が存在する。監査の目的のためには、誰がアクションを実行したのかを知ることが望ましいかもしれない。利用者は、彼/彼女のアクションを自分だけにとどめて、他人(例えば、求人側)に識別されたくないかもしれない。また、利用者識別情報を保護すべきであることが組織のセキュリティ方針で要求されているかもしれない。このような場合、監査とプライバシーに対するセキュリティ対策方針は互いに矛盾することがある。そのため、もしこの要件が選択され、かつプライバシーが重要であるならば、利用者の偽名性のコンポーネントを含めることが考慮されてよい。偽名に基づく実利用者名の判断の要件は、プライバシークラスで特定される。

C.3　セキュリティ監査分析(FAU_SAA)

このファミリは、実際のセキュリティ侵害あるいはその可能性を探す、システムアクティビティ及び監査データを分析する自動化された手段の要件を定義する。この分析は、侵入検出や、切迫したセキュリティ侵害への自動応答をサポートして働くこともある。

切迫していると思われる侵害あるいは侵害の可能性を検出してTSFが実行するアクションは、FAU_ARP セキュリティ監査自動応答コンポーネントで定義される。

適用上の注釈

リアルタイム分析のために、監査データを自動処理に適したフォーマットに変換してよいが、許可利用者のレビューのため、それに適する別のフォーマットにも変換できる。

FAU_SAA.1　侵害の可能性の分析

利用者のための適用上の注釈

このコンポーネントは、監査対象事象のセット - その発生または発生したものの格納がTSPの侵害可能性を示すために保持される - と、侵害分析を実行するために使用されるあらゆる規則を特定するのに使われる。

操作

割付:

FAU_SAA.1.2.aにおいて、PP/ST作成者は、その発生または発生の格納がTSPの侵害の可能性を示すものとして検出する必要がある、定義された監査対象事象のサブセットを識別すべきである。

割付:

FAU_SAA.1.2.bにおいて、PP/ST作成者は、TSFがその監査証跡分析に使用すべきあらゆる他の規則を特定すべきである。それらの規則は、ある時間の期間(例えば、その日の間、存続時間など)にその事象が発生する必要があることを表すような特定の要件を含めることができる。

FAU_SAA.2　プロファイルに基づく異常検出

*プロファイル*とは、利用者及び/またはサブジェクトのふるまいの特性を示す構造体である; それは、利用者/サブジェクトがさまざまな方法でどのようにTSFと対話するかを表現する。使用パターン(例えば、例外の発生パターン、資源の利用パターン(いつ、どれを、どのように)、実行するアクションのパターン)は、利用者/サブジェクトが関与するさまざまな種別のアクティビティに関して設定される。プロファイルにさまざまな種別のアクティビティを記録する方法(例えば、資源の量、事象カウンタ、タイマ)は、*プロファイル尺度*と呼ばれる。

各プロファイルは、*プロファイルターゲットグループ*のメンバによる予期される使用パターンを表現する。このパターンは、過去の使用(履歴パターン)、あるいは類似したターゲットグループの利用者における通常の使用(予期されるふるまい)に基づくものとすることができる。プロファイルターゲットグループは、TSFと対話する一人または複数の利用者に対応する。プロファイルグループの各メンバのアクティビティは、分析ツールがそのプロファイルに記述された使用パターンを設定するのに使われる。以下は、プロファイルターゲットグループのいくつかの例である。

a) **単一利用者アカウント**: 利用者あたり一つのプロファイル;

b) **グループIDまたはグループアカウント**: 同一のグループIDを所有するか、または同一のグループアカウントを使って操作する全利用者に対して一つのプロファイル;

c) **操作上の役割**: 決められた操作上の役割を共有する全利用者に対して一つのプロファイル;

d) **システム**: システムの全利用者に対して一つのプロファイル。

一つのプロファイルターゲットグループの各メンバに、固有の*疑惑率*が割り付けられる。これは、グループプロファイルの中で表現された、確立した使い方のパターンに対して、メンバの新しいアクティビティがどの程度の近さで関連付けられるかを表す。

例外検出ツールをどこまで精巧にするかは、PP/STが要求するプロファイルターゲットグループの数と、要求されるプロファイル尺度の複雑さによって、大きく左右される。

このコンポーネントは、その発生または発生の累積がTSPに対する侵害の可能性を示す監査対象事象と、侵害分析を実行するのに使われるあらゆる規則を特定するために使われる。この事象あるいは規則のセットは、事象あるいは規則の追加、改変あるいは削除によって、許可利用者が修正することができる。

PP/ST作成者は、何のアクティビティがTSFによって監視されるべきか、及び/または分析されるべきかを、具体的に列挙すべきである。また、そのアクティビティに関連するどのような情報が使用プロファイルの構築に必要なのかを、具体的に識別すべきである。

FAU_SAA.2は、TSFがシステムの使い方のプロファイルを維持することを要求する。維持という用語は、例外検出機構が、プロファイルターゲットのメンバによって実行される新しいアクティビティに基づいて、使い方のプロファイルを能動的に更新するという意味合いを含んでいる。ここでは、利用者アクティビティを表す尺度はPP/ST作成者によって定義されるということが重要である。例えば、一人の人間が実行可能なアクションが千個存在するかもしれないが、例外検出機構は、そのアクティビティのサブセットを監視することを選択するかもしれない。例外的なアクティビティは、非例外的なアクティビティと全く同様にプロファイルに統合される(そのツールがそれらのアクションを監視していると仮定する)。4カ月前には例外的に見えたかもしれないできごとが、利用者の職務の変化に伴い、時間の経過とともに例外的でなくなることも(その逆も)ある。もしプロファイル

更新アルゴリズムに例外的なアクティビティが入らないようにしてしまうと、TSFは、このような概念のものを捕らえることができなくなろう。

許可利用者が疑惑率の重大性を理解できるよう、管理上の告知が提供されるべきである。

PP/ST作成者は、疑惑率をどのように解釈するか、及び例外的アクティビティがFAU_ARPメカニズムに示される際の条件を定義すべきである。

操作

割付:

FAU_SAA.2.1において、PP/ST作成者は、プロファイルターゲットグループを特定すべきである。一つのPP/STは、複数のプロファイルターゲットグループを含むことができる。

FAU_SAA.2.3において、PP/ST作成者は、TSFによって例外的アクティビティが報告される条件を特定すべきである。条件として、疑惑率がある値に到達することを含めてもよく、あるいは観察された例外的アクティビティの種別に基づいてもよい。

FAU_SAA.3　単純攻撃の発見

利用者のための適用上の注釈

実際のところ、セキュリティ侵害が切迫していることを分析ツールが確信を持って検出できることは、よくても稀でしかない。しかしながら、重要であるために、常にそれだけを取り出してレビューする価値のあるシステム事象がいくつか存在する。そのような事象の例として、鍵となるTSFセキュリティデータファイル(例えばパスワードファイル)の削除や、管理特権を取得しようとするリモート利用者といったアクティビティがあげられる。これらの事象は、その他のシステムアクティビティと区分され、その発生が侵入アクティビティを示唆している、*特徴的事象(signature events)*と呼ばれる。

与えられるツールの複雑さは、特徴的事象の基本セットの識別においてPP/ST作成者が定義する割付に大きく依存しよう。

PP/ST作成者は、分析を実行するために、どのような事象をTSFが監視すべきかを具体的に列挙すべきである。PP/ST作成者は、その事象が特徴的事象に対応づけされるかどうかを決めるために、その事象に関係するどのような情報が必要なのかを、具体的に識別すべきである。

許可利用者が、事象の重要性、及びとり得る適切な対応を理解できるような管理上の通知が提供されるべきである。

これらの要件の詳細化において、システムのアクティビティを監視するための唯一の入力を監査データに依存するのを避ける努力がなされた。これは、システムアクティビティの分析を監査データの使用だけによらずに行う侵入検出ツールがすでに開発されていること

を踏まえて行われたものである(それ以外の入力データの例として、ネットワークデータグラム、資源/アカウントデータ、あるいはさまざまなシステムデータの組み合わせがあげられる)。

FAU_SAA.3のエレメントは、即時攻撃発見を実装するTSFが、アクティビティが監視されているTSFと同一であることを要求しない。そのため、そのシステムアクティビティが分析されているシステムと独立して動作する侵入検出コンポーネントを開発することができる。

操作

割付:

FAU_SAA.3.1において、PP/ST作成者は、その発生がTSP侵害の可能性を示すシステム事象の基本サブセットを、他のすべてのシステムアクティビティと分離して識別すべきである。そのような事象として、TSPに対する侵害が自明なもの、あるいは、その発生が、アクションが是認されるほど重要であるものが含まれる。

FAU_SAA.3.2において、PP/ST作成者は、システムアクティビティを決定するために使われる情報を特定すべきである。この情報は、TOEにおいて発生したシステムアクティビティを、分析ツールによって決定するために使われる入力データである。このデータには、監査データ、監査データと他のシステムデータとの組み合わせ、あるいは監査データ以外のデータから構成されるものを含めることができる。PP/ST作成者は、入力データの中で、何のシステム事象と事象属性が監視され続けるのかを正確に定義すべきである。

FAU_SAA.4　複合攻撃の発見

利用者のための適用上の注釈

実際のところ、セキュリティ侵害が切迫していることを分析ツールが確信を持って検出できることは、よくてもまれでしかない。しかしながら、重要であるために、常にそれだけを取り出してレビューする価値のあるシステム事象がいくつか存在する。そのような事象の例として、鍵となるTSFセキュリティデータファイル(例えばパスワードファイル)の削除や、管理特権を取得しようとするリモート利用者といったアクティビティがあげられる。これらの事象は、その他のシステムアクティビティと区分され、その発生が侵入アクティビティを示唆している、*特徴的事象*と呼ばれる。事象シーケンスとは、侵入アクティビティを示しているかもしれない、順序付けられた特徴的事象のセットである。

与えられるツールの複雑さは、特徴的事象及び事象シーケンスの基本セットの識別においてPP/ST作成者が定義する割付に大きく依存しよう。

PP/ST作成者は、TSFによって表される特徴的事象及び事象シーケンスの基本セットを定義すべきである。システム開発者は、特徴的事象及び事象シーケンスの定義を追加するこ

とができる。

PP/ST作成者は、分析を実行するために、何の事象がTSFによって監視されるべきかを具体的に列挙すべきである。PP/ST作成者は、その事象が特徴的事象に対応づけされるかどうかを決めるために、その事象に関係するどのような情報が必要なのかを、具体的に識別すべきである。

許可利用者が、事象の重要性及びとり得る適切な対応を理解できるような管理上の通知が提供されるべきである。

システムのアクティビティを監視するのに、単一の入力として監査データに依存することを避けるため、これらの要件の具体化における努力がなされた。これは、システムアクティビティの分析を監査データの使用だけによらずに行う侵入検出ツール(それ以外の入力データの例として、ネットワークデータグラム、資源/アカウントデータ、あるいはさまざまなシステムデータの組み合わせがあげられる)がすでに開発されていることを踏まえて行われたものである。そのため、PP/ST作成者は、システムアクティビティを監視するのに使用する入力データの種別を特定することによって、レベル付けをする必要がある。

FAU_SAA.4のエレメントは、複合攻撃発見を実装するTSFが、アクティビティが監視されているTSFと同一であることを要求しない。そのため、そのシステムアクティビティが分析されているシステムと独立して動作する侵入検出コンポーネントを開発することができる。

操作

割付:

FAU_SAA.4.1において、PP/ST作成者は、その発生が既知の侵入シナリオを表すシステム事象のシーケンスリストの基本セットを識別すべきである。これらの事象シーケンスは、既知の侵入シナリオを表す。システム事象が実行されるときにそれらが既知の侵入事象シーケンスに結合(対応づけ)できるよう、シーケンスの中に表わされる各事象は、監視されるシステム事象に対応付けられるべきである。

FAU_SAA.4.1において、PP/ST作成者は、その発生がTSP侵害の可能性を示すシステム事象の基本サブセットを、他のすべてのシステムアクティビティと分離して識別すべきである。そのような事象として、TSPに対する侵害が自明なもの、あるいは、その発生が、アクションが是認されるほど重要であるものが含まれる。

FAU_SAA.4.2において、PP/ST作成者は、システムアクティビティを決定するために使われる情報を特定すべきである。この情報は、TOEにおいて発生したシステムアクティビティを、分析ツールによって決定するために使われる入力データである。このデータには、監査データ、監査データと他のシステムデータとの組み合わせ、あるいは監査データ以外のデータから構成されるものを含

めることができる。PP/ST作成者は、入力データの中で、何のシステム事象と事象属性が監視され続けるのかを正確に定義すべきである。

C.4　セキュリティ監査レビュー(FAU_SAR)

セキュリティ監査レビューファミリは、監査情報のレビューに関連する要件を定義する。

以下の機能は、例えば選択的にレビューを行えることを含む、格納前あるいは格納後の監査選択を許可すべきである;

- 一人あるいはそれ以上の利用者のアクション(例えば、識別、認証、TOEの入力、アクセス制御アクション);
- 特定のオブジェクトまたはTOE資源に対して実行されるアクション;
- 監査された例外の特定のセットすべて; あるいは
- 特定のTSP属性に関連付けられるアクション。

適用上の注釈

各監査レビューの区別は、それが持つ機能に基づく。監査レビューは、監査データを表示する能力(だけ)に限定される。選択可能レビューはより高度であり、監査データのレビュー前に、単一の基準あるいは論理関係(すなわち、論理積/論理和)を用いた複数の基準に基づく検索、監査データの分類、監査データのフィルタを行う能力を要求する。

FAU_SAR.1　監査レビュー

利用者のための適用上の注釈

このコンポーネントでは、利用者及び/または許可利用者が監査記録を読み出せることを特定するのに用いられる。該当する監査記録は、利用者に適した方法で提供される。さまざまな種別の利用者(人間の利用者、機械の利用者)が存在しており、そのニーズはさまざまに異なっている可能性がある。

表示可能な監査記録の内容を特定することができる。

操作

割付:

FAU_SAR.1.1において、PP/ST作成者は、この機能を使用可能な許可利用者を特定すべきである。PP/ST作成者は、セキュリティの役割(「FMT_SMR.1　セキュリティの役割」を参照)を必要に応じて特定することができる。

FAU_SAR.1.1において、PP/ST作成者は、指定した利用者が監査記録から取得できる情報の種別を特定すべきである。その例として、「すべての」、「サブジェクト識別情報」、「該当利用者を参照している監査記録内のすべての情報」などがある。

FAU_SAR.2　**限定監査レビュー**

利用者のための適用上の注釈

このコンポーネントは、FAU_SAR.1で識別されていないどの利用者も監査記録を読み出すことができないことを特定する。

FAU_SAR.3　**選択可能監査レビュー**

利用者のための適用上の注釈

このコンポーネントは、レビューされるべき監査データの選択を実行することが可能であるべきことを特定するのに使用される。もし複数の基準に基づく場合は、それらの基準は論理的な関係(すなわち、「論理積」あるいは「論理和」)で相互に関係するべきであり、ツールは監査データを適切に扱う(例えば、分類あるいはフィルタ)能力を提供すべきである。

操作

選択:

FAU_SAR.3.1に対し、PP/ST作成者は、検索、分類及び/または並べ替えがTSFによって実行され得るかどうかを選択すべきである。

割付:

FAU_SAR.3.1に対し、PP/ST作成者は、レビューのための監査データの選択に使用される基準を、できるだけ論理的な関係を付けて割り付けるべきである。論理的な関係は、操作が、個別の属性かあるいは属性の集まりに基づいてなされるかを特定するためのものである。この割付の例として、「アプリケーション、利用者アカウント及び/またはロケーション」のようなものがある。この場合は、アプリケーション、利用者アカウント及びロケーションの三つの属性の任意の組み合わせを用いて、操作の特定が可能となる。

C.5　セキュリティ監査事象選択(FAU_SEL)

セキュリティ監査対象事象選択ファミリは、監査対象事象になり得るもののどれが監査されるべきかを識別する能力に関係する要件を提供する。監査対象事象は、FAU_GEN セキュリティ監査データ生成ファミリで定義されるが、それらの事象は、選択可能として、このコンポーネントにおいて、監査されるものと定義されるべきである。

適用上の注釈

このファミリは、選択されるセキュリティ監査対象事象の粒度を適切に定義することで、監査証跡が大きすぎて使えなくならないように保てることを保証する。

FAU_SEL.1　選択的監査

利用者のための適用上の注釈

このコンポーネントは、監査されるべき事象の選択に使用される基準を定義する。それらの基準は、利用者属性、サブジェクト属性、オブジェクト属性、あるいは事象種別に基づいて、監査対象事象のセットから、事象の包含あるいは除外を許可できる。

個々の利用者識別情報の存在は、このコンポーネントでは想定されない。これは、TOEとして、ルータのような利用者についての認識を持たないかもしれないものを認める。

分散環境に対しては、監査されるべき事象の選択基準として、ホスト識別情報を使用することができる。

管理機能 FMT_MTD.1 TSFデータの管理は、選択を問合せあるいは修正する、許可利用者の権利を扱う。

操作

選択:

FAU_SEL.1.1aに対して、PP/ST作成者は、監査の選択性が基づくところのセキュリティ属性が、オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、あるいは事象種別に関係するかどうかを選択すべきである。

割付:

FAU_SEL.1.1bに対して、PP/ST作成者は、監査の選択性が基づくところのあらゆる追加属性を特定すべきである。

C.6　セキュリティ監査事象格納(FAU_STG)

セキュリティ監査事象格納ファミリは、システム障害、攻撃、及び/または格納空間の枯渇に起因する監査情報の損失を制御する要件を含め、あとで使用するために監査データを格納するための要件を記述する。

FAU_STG.1　保護された監査証跡格納

利用者のための適用上の注釈

分散環境において、監査証跡はTSC内にあるが、必ずしも監査データの生成機能と同じ場所にあるとは限らないので、PP/ST作成者は、監査記録を監査証跡に格納する前に、その記録の発信者の認証、あるいは記録の発信元の否認不可を要求することができる。

TSFは、許可されない削除や改変から監査証跡を保護する。システムによっては、所定の期間、監査者(役割)が監査記録の削除を許可されないこともあることを注記しておく。

操作

選択:

FAU_STG.1.2において、PP/ST作成者は、監査証跡に対する改変を、TSFに禁止させるかあるいは検出させるだけにするかを特定すべきである。

FAU_STG.2　監査データ可用性の保証

利用者のための適用上の注釈

PP/ST作成者は、監査証跡をどの尺度に準拠させるのかを、このコンポーネントで特定することができる。

分散環境において、監査証跡はTSC内にあるが、必ずしも監査データの生成機能と同じ場所にあるとは限らないので、PP/ST作成者は、監査記録を監査証跡に格納する前に、その記録の発信者の認証、あるいは記録の発信元の否認不可を要求することができる。

操作

選択:

FAU_STG.2.2において、PP/ST作成者は、監査証跡に対する改変を、TSFに禁止させるかあるいは検出させるだけにするかを特定すべきである。

FAU_STG.2.3において、PP/ST作成者は、TSFが監査データの定義された総量を維持し続けることができねばならない条件を特定すべきである。この条件は次のどれでもよい: 監査格納枯渇、障害、攻撃。

割付:

FAU_STG.2.3において、PP/ST作成者は、監査証跡に関してTSFが保証しなければならない数値尺度を特定すべきである。この数値尺度は、保持しなければならない記録の数や、記録の維持を保証する時間を具体的にあげることで、データの損失を制限する。数値尺度の例として、100,000件の監査記録を格納できることを示す「100,000」などがある。

FAU_STG.3　**監査データ消失の恐れ発生時のアクション**

利用者のための適用上の注釈

このコンポーネントは、事前に定義してある所定の限界値を監査証跡が超えた場合にとられるアクションを要求する。

操作

割付:

FAU_STG.3.1において、PP/ST作成者は、あらかじめ定義された制限値を示すべきである。もし、管理機能がこの数は許可利用者によって変更されるかもしれないことを示している場合は、この値はデフォルト値となる。PP/ST作成者は、この制限値を許可利用者に定義させることを選択することができる。その場合、割付は、例えば「許可利用者が限界値を設定する」のように書ける。

FAU_STG.3.1において、PP/ST作成者は、しきい値を超えたことで切迫した監査格納障害が示された場合に取られるべきアクションを特定すべきである。アクションとして、許可利用者への通知などが含まれる。

FAU_STG.4　**監査データ損失の防止**

利用者のための適用上の注釈

このコンポーネントは、監査証跡が一杯になった場合のTOEのふるまいを特定する: 監査記録が無視される、あるいは監査対象事象が起きないようTOEが凍結される。要件は、また、その要件がどのように具現化されたとしても、この効果に特別の権限を持つ許可利用者は、監査対象事象(アクション)の生成を継続できることも述べる。これは、そうしないと、許可利用者がシステムをリセットすることすらできなくなるからである。監査格納枯渇の場合では、TSFによってとられるアクションの選択に熟慮が払われるべきであり、それは、事象の無視はTOEの可用性を高めるが、記録がとられず利用者が分からない状態でアクションの実行を許可してしまうことにもなるからである。

操作

選択:

FAU_STG.4.1において、PP/ST作成者は、TSFが監査記録をそれ以上格納できなくなったとき、TSFが監査対象アクションを無視しなければならないかどうか、あるいは監査対象アクションが発生するのを防ぐべきかどうか、あるいは最も古い監査記録から上書きすべきかどうかを選択すべきである。

割付:

FAU_STG.4.1において、PP/ST作成者は、許可利用者へ通知するなど、監査格納障害の場合にとられるべきその他のアクションを特定すべきである。

附属書D

(参考)

通信(FCO)

このクラスは、情報を伝送する際に使用するTOEに関して特に興味深い要件を記述する。このクラスの中のファミリでは、否認不可を扱う。

図D.1 - 通信クラスのコンポーネント構成

図D.1は、通信クラスのコンポーネント構成を示している。

このクラスでは、「情報」という概念を使用する。この「情報」は通信の対象となるオブジェクトとして解釈すべきであり、その中には電子メールのメッセージ、ファイル、または定義された一連の属性種別を含めることもできる。

「受信証明(proof of receipt)」及び「発信証明(proof of origin)」という用語は、文献ではよく使われている。しかし、「証明(proof)」という用語は、正式には数学上の理論的な説明の一形態として解釈することもできる。このクラスの中のコンポーネントで「証明」という用語が使われている場合は、事実上、TSFが否認不可型の情報伝送を実証していることの「証拠」として解釈する。

D.1 **発信の否認不可**(FCO_NRO)

発信の否認不可は、ある情報の発信者の識別情報について、利用者/サブジェクトに証拠を提供するための要件を定義する。発信の証拠(ディジタル署名など)が発信者と送られた情報とをつなぐ証拠を提供するため、発信者は、情報を送信したことを否認することができない。受信者あるいは第三者は、発信の証拠を検証できる。この証拠は、偽造可能であるべきではない。

利用者のための注釈

もし情報または関連付けられている属性が何らかの方法で変更されると、発信の証拠の確認が失敗するかもしれない。そのため、PP/ST作成者は、FDP_UIT.1 データ交換完全性のような完全性に関する要件をPP/STに含めることを考慮すべきである。

否認不可には各種の役割が関連しており、それぞれの役割は一つあるいは複数のサブジェクトにおいて組み合わせることができる。最初の役割は、発信の証拠を要求するサブジェクトである(FCO_NRO.1 発信の選択的証明の場合だけ)。2番目の役割は、発信の証拠の提供先となる受信者や他のサブジェクト(公証人など)である。3番目の役割は、発信の証拠の検証を要求するサブジェクト、例えば、受信者あるいは調停者などの第三者である。

PP/ST作成者は、発信の証拠の有効性を検証するのに必要な条件を特定しなければならない。特定される条件の例は、証拠の検証は24時間以内にされねばならない、というものである。従って、これらの条件は、証拠の提供を数年間可能にするなど、法的な要求に対する否認不可の修整を可能にする。

ほとんどの場合、受信者の識別情報が、送信を受信した利用者の識別情報になる。場合によっては、PP/ST作成者は、利用者の識別情報がエクスポートされるのを望まないことがある。そのような場合、PP/ST作成者は、このクラスを含めるのが適切かどうか、あるいは伝送サービスプロバイダの識別情報あるいはホストの識別情報が使用されるべきかどうかを考慮しなければならない。

利用者の識別情報に加えて(あるいはその代わりに)、PP/ST作成者は、情報が送信された時間をより重要と考えるかもしれない。例えば、提案の要求は、よく検討してもらうために、ある日付より前に送信しなければならない。そのような例では、これらの要件は、タイムスタンプ表示(発信の時間)を提供するようカスタマイズすることができる。

FCO_NRO.1 **発信の選択的証明**

操作

割付:

FCO_NRO.1.1において、PP/ST作成者は、発信機能機能の証拠に、例えば電子メールメッセージなど、情報サブジェクトの種別を記入すべきである。

選択:

FCO_NRO.1.1において、PP/ST作成者は、発信の証拠を要求できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRO.1.1において、PP/ST作成者は、選択によっては、発信*の証拠を要求できる第三者を特定すべきである。第三者とは、調停者、裁判官、法的機関などがなり得る。 *(*: 【訳者注】CC V.2.1及びISO/IEC 15408では 'receipt' となっているが、 'origin' が正しいと思われる。)*

FCO_NRO.1.2において、PP/ST作成者は、情報にリンクすべき属性; 例えば、発信者識別情報、発信時刻、発信場所、のリストを記入すべきである。

FCO_NRO.1.2において、PP/ST作成者は、メッセージ本文など、その属性が発信の証拠を提供する、情報内の情報フィールドのリストを記入すべきである。

選択:

FCO_NRO.1.3において、PP/ST作成者は、発信の証拠を検証できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRO.1.3において、PP/ST作成者は、選択によっては、発信の証拠を検証できる第三者を特定すべきである。

FCO_NRO.1.3において、PP/ST作成者は、その証拠を検証できる制限についてのリストを記入すべきである。例えば、証拠は24時間の範囲内でだけ検証されるなど。「直ちに」や「無制限」を割り付けることは許される。

FCO_NRO.2 **発信の強制的証明**

操作

FCO_NRO.2.1において、PP/ST作成者は、選択によっては、発信*の証拠を要求できる第三者を特定すべきである。第三者とは、調停者、裁判官、法的機関などがなり得る。

FCO_NRO.2.2において、PP/ST作成者は、情報にリンクすべき属性; 例えば、発信者識別情報、発信時刻、発信場所、のリストを記入すべきである。

FCO_NRO.2.2において、PP/ST作成者は、メッセージ本文など、その属性が発信の証拠を提供する、情報内の情報フィールドのリストを記入すべきである。

選択:

FCO_NRO.2.3において、PP/ST作成者は、発信の証拠を検証できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRO.2.3において、PP/ST作成者は、選択によっては、発信の証拠を検証できる第三者を特定すべきである。

FCO_NRO.2.3において、PP/ST作成者は、その証拠を検証できる制限についてのリストを記入すべきである。例えば、証拠は24時間の範囲内でだけ検証されるなど。「直ちに」や「無制限」を割り付けることは許される。

D.2 **受信の否認不可**(FCO_NRR)

受信の否認不可は、受信者が情報を受信したことの証拠を他の利用者/サブジェクトに提供するための要件を定義する。受信の証拠(ディジタル署名など)が、受信者属性とその情報をつなぐ証拠を提供するため、受信者は、情報を受信したことを否認することができない。発信者あるいは第三者は、受信の証拠を検証できる。この証拠は、偽造可能であるべきではない。

利用者のための注釈

情報が受信されたという証拠の提供は、必ずしも情報が読まれた、あるいは理解されたことを意味せず、単に配信されたことを示すことに注意すべきである。

もし情報あるいは関連する属性が何らかの方法で変えられると、元の情報に関する受信の証拠の確認が失敗するかもしれない。そのため、PP/ST作成者は、FDP_UIT.1 データ交換完全性のような完全性に関する要件をPP/STに含めることを考慮すべきである。

否認不可ではいくつかの異なる役割が用いられ、各々は一つまたは複数のサブジェクトにおいて組み合わせることができる。最初の役割は、受信の証拠を要求するサブジェクトである(FCO_NRR.1 受信の選択的証明の場合だけ)。2番目の役割は、受信者及び/または証拠が提供される他のサブジェクト(例えば公証人)である。3番目の役割は、受信の証拠の検証を要求するサブジェクト、例えば、発信者あるいは調停者などの第三者である。

PP/ST作成者は、受信の証拠の有効性を検証するのに必要な条件を特定しなければならない。特定される条件の例は、証拠の検証は24時間以内にされねばばならない、というものである。従って、これらの条件は、証拠の提供を数年間可能にするなど、法的な要件に対する否認不可の修整を可能にする。

ほとんどの場合、受信者の識別情報が、送信を受信した利用者の識別情報になる。場合によっては、PP/ST作成者は、その利用者の識別情報がエクスポートされるのを望まないことがある。そのような場合、PP/ST作成者は、このクラスを含めるのが適切かどうか、あるいは伝送サービスプロバイダの識別情報あるいはホストの識別情報が使用されるべきかどうかを考慮しなければならない。

利用者識別情報に加えて(あるいはその代わりに)、PP/ST作成者は、情報が受信された時間をより重要と考えるかもしれない。例えば、提案が所定の日付で締め切られる場合、よく検討してもらうためには、発注は所定の日付までに受信されねばならない。そのような例では、これらの要件は、タイムスタンプ表示(受信の時間)を提供するようカスタマイズすることができる。

FCO_NRR.1 **受信の選択的証明**

操作

割付:

FCO_NRR.1.1において、PP/ST作成者は、受信機能の証拠に対する情報サブジェクトの種別、例えば電子メールのメッセージ、を記入すべきである。

選択:

FCO_NRR.1.1において、PP/ST作成者は、受信の証拠を要求できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRR.1.1において、PP/ST作成者は、選択によっては、受信の証拠を要求できる第三者を特定すべきである。第三者とは、調停者、裁判官、法的機関などがなり得る。

FCO_NRR.1.2において、PP/ST作成者は、情報にリンクすべき属性; 例えば、受信者識別情報、受信時刻、受信場所などのリストを記入すべきである。

FCO_NRR.1.2において、PP/ST作成者は、メッセージ本文など、その属性が受信の証拠を提供する、情報内の情報フィールドのリストを記入すべきである。

選択:

FCO_NRO.1.3において、PP/ST作成者は、受信の証拠を検証できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRO.1.3において、PP/ST作成者は、選択によっては、受信の証拠を検証できる第三者を特定すべきである。

FCO_NRO.1.3において、PP/ST作成者は、その証拠を検証できる制限についてのリストを記入すべきである。例えば、証拠は24時間の範囲内でだけ検証されるなど。「直ちに」や「無制限」を割り付けることは許される。

FCO_NRR.2 **受信の強制的証明**

操作

割付:

FCO_NRR.2.1において、PP/ST作成者は、受信機能の証拠に対する情報サブジェクトの種別、例えば電子メールのメッセージ、を記入すべきである。

FCO_NRR.2.2において、PP/ST作成者は、情報にリンクすべき属性; 例えば、受信者識別情報、受信時刻、受信場所などのリストを記入すべきである。

FCO_NRR.2.2において、PP/ST作成者は、メッセージ本文など、その属性が受信の証拠を提供する、情報内の情報フィールドのリストを記入すべきである。

選択:

FCO_NRO.2.3において、PP/ST作成者は、受信の証拠を検証できる利用者/サブジェクトを特定すべきである。

割付:

FCO_NRO.2.3において、PP/ST作成者は、選択に依存よっては、受信の証拠を検証できる第三者を特定すべきである。第三者とは、調停者、裁判官、法的機関などがなり得る。

FCO_NRO.2.3において、PP/ST作成者は、その証拠を検証できる制限についてのリストを記入すべきである。例えば、証拠は24時間の範囲内でだけ検証されるなど。「直ちに」や「無制限」を割り付けることは許される。

附属書E

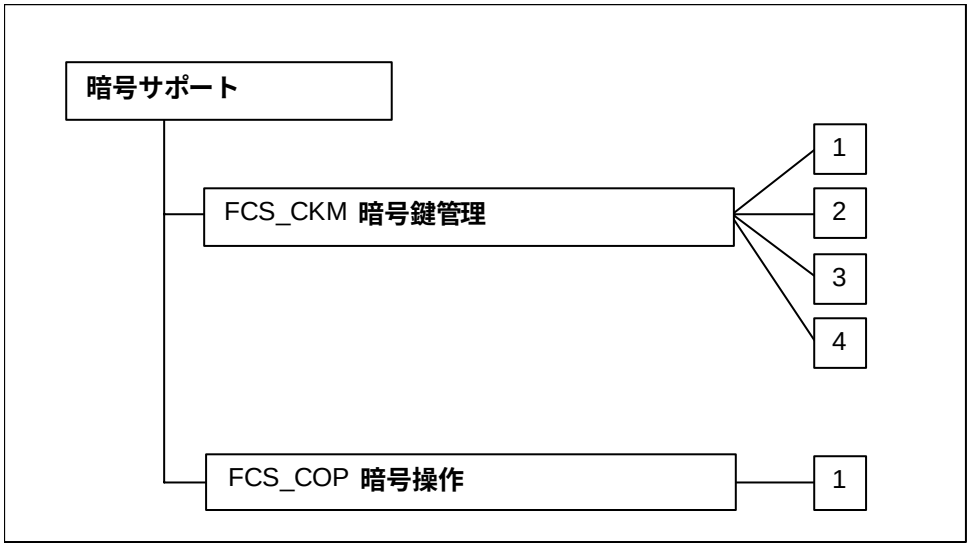
(参考)

暗号サポート(FCS)

TSFは、いくつかの高レベルのセキュリティ対策方針を満たすのを助けるため、暗号機能を採用することができる。これらは以下のものである(ただし、限定されない): 識別と認証、否認不可、高信頼パス、高信頼チャネル、及びデータ分離。このクラスは、TOEが暗号機能を実装する場合に使用され、その実装は、ハードウェア、ファームウェア、及び/またはソフトウェアにおいて行われる。

FCSクラスは二つのファミリから構成される: FCS_CKM 暗号鍵管理及びFCS_COP暗号操作。FCS_CKMファミリは暗号鍵の管理面に対応し、FCS_COPファミリは、それらの暗号鍵の運用上の使用に関連する。

図E.1は、このクラスのコンポーネント構成を示している。



図E.1 - 暗号サポートクラスのコンポーネント構成

TOEで実装する暗号鍵生成方法ごとに、もしあれば、PP/ST作成者はFCS_CKM.1のコンポーネントを選択すべきである。

TOEで実装する暗号鍵配付方法ごとに、もしあれば、PP/ST作成者はFCS_CKM.2のコンポーネントを選択すべきである。

TOEで実装する暗号鍵アクセス方法ごとに、もしあれば、PP/ST作成者はFCS_CKM.3のコンポーネントを選択すべきである。

TOEで実装する暗号鍵破棄方法ごとに、もしあれば、PP/ST作成者はFCS_CKM.4のコンポーネントを選択すべきである。

TOEで実行する暗号操作(ディジタル署名、データ暗号化、鍵交換、セキュアハッシュなど)ごとに、もしあれば、PP/ST作成者はFCS_COP.1のコンポーネントを選択すべきである。

暗号機能は、FCOクラスにおいて特定された対策方針を満たすために、かつFDP_DAU、FDP_SDI、FDP_UCT、FDP_UIT、FIA_SOS、FIA_UAUファミリにおけるさまざまな対策方針を満たすために使用できる。暗号機能がそれ以外のクラスに対する対策方針を満たすために使われる場合は、個々の機能コンポーネントが、暗号機能が満たさねばならない対策方針を特定する。FCSクラスにおける対策方針は、TOEの暗号機能が消費者によって求められるときに使用されるべきである。

E.1　暗号鍵管理(FCS_CKM)

利用者のための注釈

暗号鍵は、その寿命全体を通して管理されねばならない。暗号鍵のライフサイクルにおいて発生する典型的な事象としては(それだけに限定されないが)、生成、配付、登録、格納、アクセス(例えば、バックアップ、エスクロー、アーカイブ、回復)及び破棄がある。

最小限、暗号鍵は少なくとも次の段階を経るべきである: 生成、格納及び破棄。TOEはすべての鍵のライフサイクルに関与する必要はないので、他の段階を含めるかどうかは、実際に用いられる鍵管理戦略に依存する(例えば、TOEは、暗号鍵の生成と配付だけを行うかもしれない)。

このファミリは、暗号鍵のライフサイクルをサポートすることを意図し、その結果として以下のアクティビティに対する要件を定義する: 暗号鍵生成、暗号鍵配付、暗号鍵アクセス、及び暗号鍵破棄。このファミリは、暗号鍵の管理に対する機能要件が存在する場合は、必ず含まれるべきである。

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、監査される事象の文脈において:

a) オブジェクト属性は、暗号鍵に割り付けられた利用者、利用者の役割、暗号鍵が使われる暗号操作、暗号鍵識別子及び暗号鍵有効期間を含むことができる。

b) オブジェクト値は、(共通あるいは秘密暗号鍵のような)すべての機密上の重要情報を除き、暗号鍵及びパラメタの値を含むことができる。

典型的に、暗号鍵を生成するために乱数が使われる。この場合、FIA_SOS.2 TSF秘密生成コンポーネントの代わりに、FCS_CKM.1 暗号鍵生成が使用されるべきである。暗号鍵生成以外の目的で乱数生成が要求される場合、FIA_SOS.2 TSF秘密生成コンポーネントが使用されるべきである。

FCS_CKM.1　暗号鍵生成

利用者のための適用上の注釈

このコンポーネントは、暗号鍵長と暗号鍵の生成に使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠ことでよい。それは、暗号鍵長と暗号鍵を生成するのに使用する方法(例えばアルゴリズム)を特定するために使われるべきである。同一の方法で複数の鍵長のものに対しては、コンポーネントの一つの具体例だけが必要である。鍵長は、さまざまなエンティティに対して、共通であっても異なっていてもよく、その方法に対する入力であっても出力であってもよい。

操作

割付:

FCS_CKM.1.1において、PP/ST作成者は、使用する暗号鍵生成アルゴリズムを特定すべきである。

FCS_CKM.1.1において、PP/ST作成者は、使用する暗号鍵長を特定すべきである。特定される鍵長は、アルゴリズム及びその意図された使用に対して適切であるべきである。

FCS_CKM.1.1において、PP/ST作成者は、暗号鍵の生成に使用する方法を提示する割り付けられた標準を特定すべきである。その割り付けられた標準は、なし、一つ、あるいは複数の実際の標準出版物で構成されていればよく、その例として、国際、国内、業界、あるいは組織の標準がある。

FCS_CKM.2 **暗号鍵配付**

利用者のための適用上の注釈

このコンポーネントは、暗号鍵を配付するのに使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。

操作

割付:

FCS_CKM.2.1において、PP/ST作成者は、使用する暗号鍵の配付方法を規定すべきである。

FCS_CKM.2.1において、PP/ST作成者は、暗号鍵を配付するために使用する方法を提示する割り付けられた標準を特定すべきである。その割り付けられた標準は、なし、一つ、あるいは複数の実際の標準出版物で構成されていればよく、その例として、国際、国内、業界、あるいは組織の標準がある。

FCS_CKM.3 **暗号鍵アクセス**

利用者のための適用上の注釈

このコンポーネントは、暗号鍵へのアクセスに使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。

操作

割付:

FCS_CKM.3.1において、PP/ST作成者は、使用する暗号鍵アクセスの種別を特

定すべきである。暗号鍵アクセスの種別の例として、暗号鍵バックアップ、暗号鍵アーカイブ、暗号鍵エスクロー、暗号鍵回復などがある(ただし、これらに限定されない)。

FCS_CKM.3.1において、PP/ST作成者は、使用する暗号鍵に対するアクセス方法を特定すべきである。

FCS_CKM.3.1において、PP/ST作成者は、暗号鍵にアクセスするために使用する方法を提示する割り付けられた標準を特定すべきである。その割り付けられた標準は、なし、一つ、あるいは複数の実際の標準出版物で構成されていればよく、その例として、国際、国内、業界、あるいは組織の標準がある。

FCS_CKM.4 **暗号鍵破棄**

利用者のための適用上の注釈

このコンポーネントは、暗号鍵の破棄に使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。

操作

割付:

FCS_CKM.4.1において、PP/ST作成者は、暗号鍵を破棄するために使用する方法を特定すべきである。

FCS_CKM.4.1において、PP/ST作成者は、暗号鍵を破棄するために使用する方法を提示する割り付けられた標準を特定すべきである。その割り付けられた標準は、なし、一つ、あるいは複数の実際の標準出版物で構成されていればよく、その例として、国際、国内、業界、あるいは組織の標準がある。

E.2　暗号操作(FCS_COP)

利用者のための注釈

暗号操作は、それに関連付けられた操作の暗号モード(一つまたは複数)を持つことができる。そのような場合は、暗号モード(一つまたは複数)が特定されなければならない。操作の暗号モードの例として、暗号ブロック連鎖、出力フィードバックモード、電子コードブックモード、及び暗号フィードバックモードがある。

暗号操作は、一つまたは複数のTOEセキュリティサービスをサポートするために使用することができる。FCS_COPコンポーネントは、以下のような場合に、複数回繰返す必要があるかもしれない。

a) セキュリティサービスが使われる利用者アプリケーション

b) 異なる暗号アルゴリズム及び/または暗号鍵長の使用

c) そこで操作されるデータの種別及び/または機密上の重要性

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、監査される暗号操作事象の文脈において:

a) 暗号操作の種別は、ディジタル署名生成及び/または検証、完全性及び/またはチェックサムの検証に対する暗号チェックサム生成、セキュアハッシュ(メッセージダイジェスト)計算、データ暗号化及び/または復号、暗号鍵暗号化及び/または復号、暗号鍵交換及び乱数生成、を含むことができる。

b) サブジェクト属性は、サブジェクト役割(一つまたは複数)及びそのサブジェクトに関連する利用者(1名または複数名)を含むことができる。

c) オブジェクト属性は、暗号鍵に割り付けられた利用者、利用者役割、暗号鍵が使用される暗号操作、暗号鍵識別子、及び暗号鍵有効期間を含むことができる。

FCS_COP.1　暗号操作

利用者のための適用上の注釈

このコンポーネントは、使用される暗号アルゴリズムと鍵長が、割り付けられた標準に基づくことができる特定の暗号操作(一つまたは複数)を実行することを要求する。

操作

割付:

FCS_COP.1.1において、PP/ST作成者は、実行する暗号操作を特定すべきであ

る。典型的な暗号操作は、ディジタル署名生成及び/または完全性及び/またはチェックサムの検証に対する暗号チェックサム生成、セキュアハッシュ(メッセージダイジェスト)計算、データ暗号化及び/または復号、暗号鍵暗号化及び/または復号、暗号鍵交換及び乱数生成を含む。暗号操作は、利用者データ及びTSFデータに対して実行できる。

FCS_COP.1.1において、PP/ST作成者は、使用する暗号アルゴリズムを特定すすべきである。典型的な暗号アルゴリズムには、DES、RAS、IDEAが含まれるが、それらだけに限定されない。

FCS_COP.1.1において、PP/ST作成者は、使用する暗号鍵長を特定すべきである。特定された鍵長は、アルゴリズム及びその使用意図に適切であるべきである。

FCS_COP.1.1において、PP/ST作成者は、識別された暗号操作(一つまたは複数)がどのように実行されるかを提示する割り付けられた標準を特定すべきである。その割り付けられた標準は、なし、一つ、あるいは複数の実際の標準出版物で構成されていればよく、その例として、国際、国内、業界、あるいは組織の標準がある。

附属書F

(参考)

利用者データ保護(FDP)

このクラスには、利用者データの保護に関連したTOEセキュリティ機能及びTOEセキュリティ機能方針に関する要件を特定するファミリが含まれる。FDPは利用者データを保護するためのコンポーネントを特定し、FIAは利用者に関連する属性を保護するコンポーネントを定義し、FPTはTSF情報を保護するコンポーネントを特定するという点において、このクラスは、FIA及びFPTと異なる。

このクラスには、従来の必須アクセス制御: Mandatory Access Control(MAC)あるいは従来の裁量アクセス制御: Discretionary Access Control(DAC)に対する明示的な要件は含まない; ただし、そのような要件は、このクラスからのコンポーネントを使って構成することができる。

FDPでは、機密性、完全性、あるいは可用性を明示的には扱わないが、それは、これらがたいていの場合に方針とメカニズム中に織り込まれているからである。しかしながら、TOEセキュリティ方針は、PP/STにおけるこれら三つの目的を適切にカバーしていなければならない。

このクラスの最後の側面は、「操作」の観点からアクセス制御を特定するという点である。操作は、特定のオブジェクトに対する特定のアクセスの種別として定義される。これらの操作が「読み出し」及び/または「書き込み」操作のように記述されるか、あるいは「データベース更新」のようなより複雑な操作として記述されるかどうかは、PP/ST作成者の抽出化のレベルに依存する。

アクセス制御方針とは、情報コンテナに対するアクセスを制御する方針である。属性は、そのコンテナの属性を表す。情報がいったんコンテナから外部に出ると、アクセス者はその情報を改変することが自由になり、その情報を、異なる属性を持つ異なるコンテナに書き込むこともできる。一方、情報フロー方針では、コンテナと独立した情報へのアクセスを制御する。情報の属性は、コンテナの属性と関連付けられていることがある(あるいは、マルチレベルデータベースの場合のように、そうでないこともある)が、情報が動くとそれと一緒に移動する。アクセス者は、明示的な許可を持たない場合、情報の属性を変えることができない。

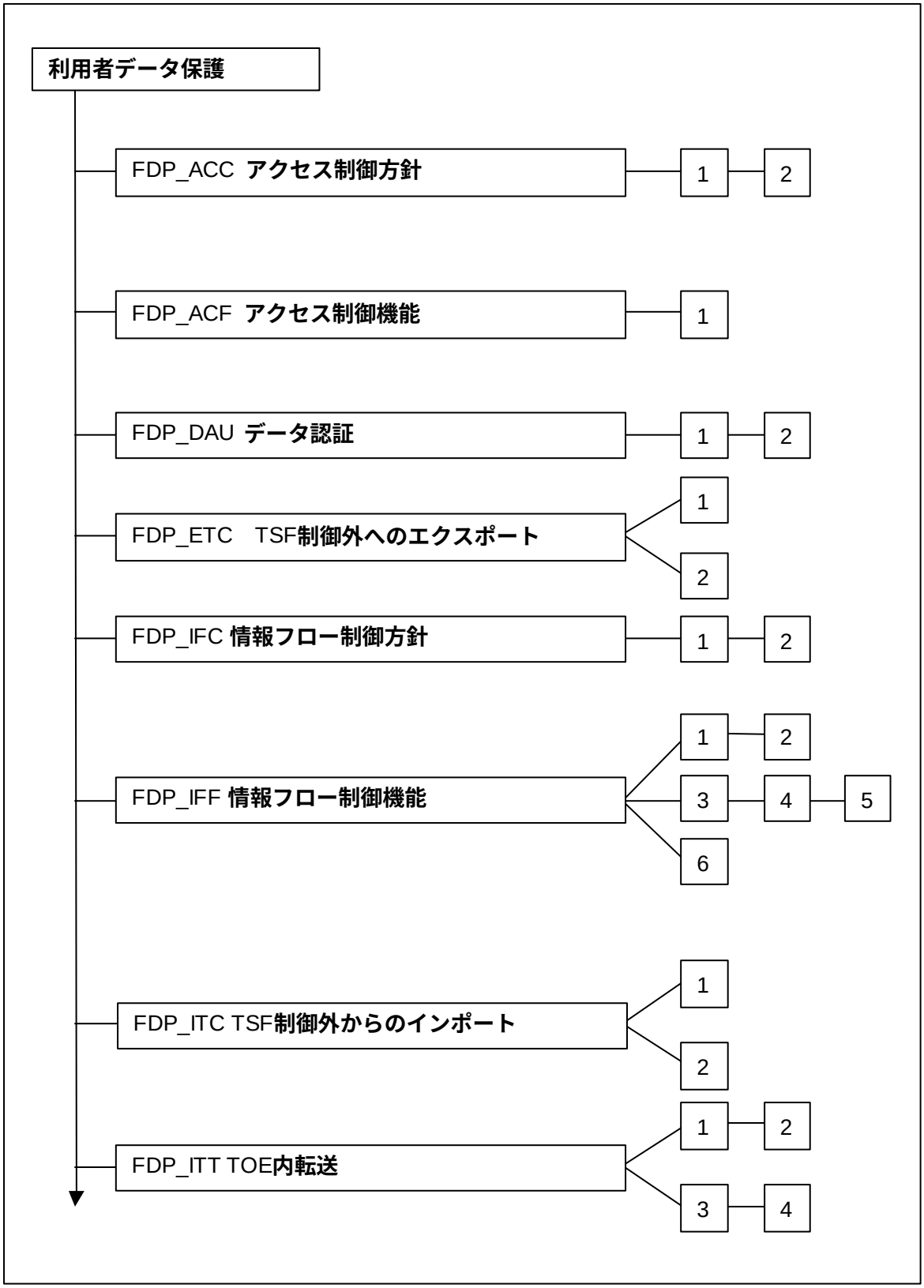
このクラスは、普通に想像されるような、ITアクセス方針の完全な分類学を意図するものではない。ここに含まれる方針は、単に、実システムについての一般に知られている経験から得られる、要件特定のための基礎となるような方針である。ここでの定義には入らない、他の意向に沿った形式があってもよい。

例えば、情報フローに対して、利用者が課する(及び利用者が定義する)制御を適用するような実現形態が考えられる(一例として、「部外者禁止」処置警告を自動で実現できるようなもの)。そのような概念は、FDPコンポーネントに対する詳細化または拡張として扱うこともできる。

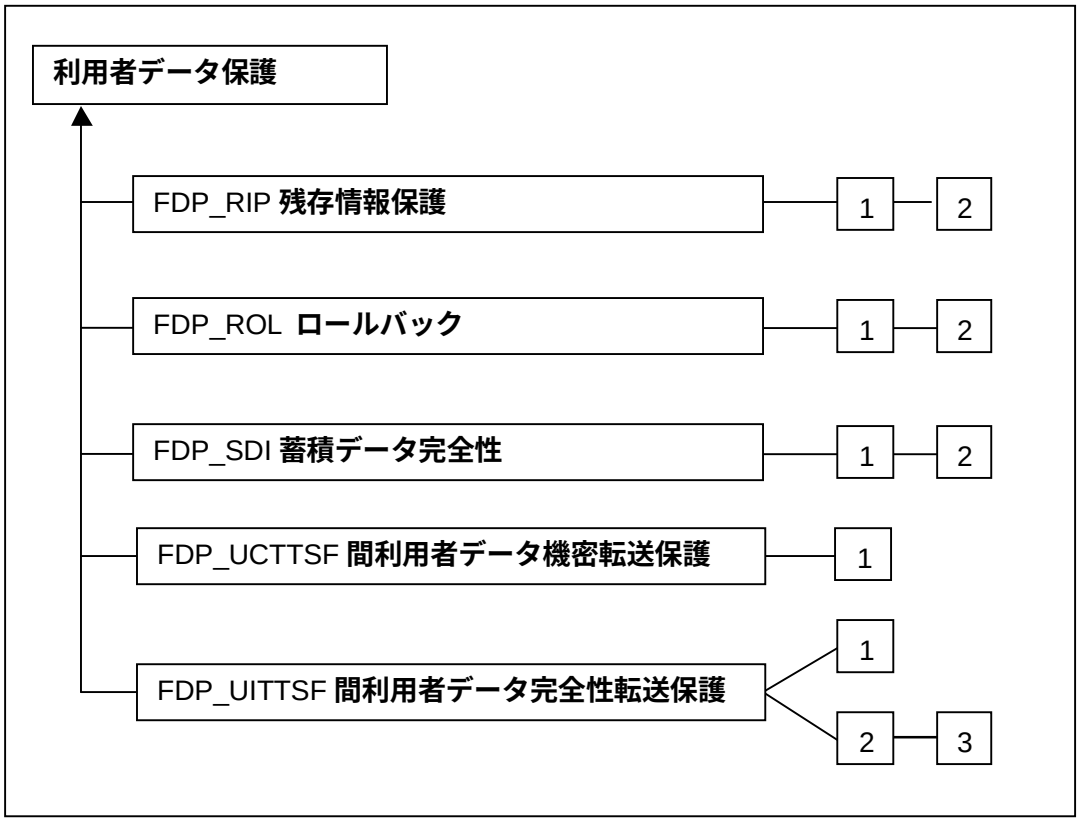
最後に、FDPのコンポーネントをながめるときは、これらのコンポーネントは、他の目的に役立つ、あるいは役立ち得るメカニズムによって実現されるかもしれない機能に対する要件であることを覚えておくことが重要である。例えば、アクセス制御メカニズムの基礎として、ラベル(FDP_IFF.1)を使うアクセス制御方針(FDP_ACC)を作成することが可能である。

TOEセキュリティ方針は、多数のセキュリティ機能方針(SFP)を含めることができ、各々は二つの方針指向のコンポーネントFDP_ACC、及びFDP_IFCによって識別される。これらの方針は、TOE要件を満たすため、典型的に、機密性、完全性、及び可用性の側面を必要に応じて考慮する。すべてのオブジェクトが、少なくとも一つのSFPでカバーされ、かつ複数のSFPを実装することで競合が生じないことを保証するよう注意が払われるべきである。

図F.1及び図F.2は、このクラスのコンポーネント構成を示す。



図F.1 - 利用者データ保護クラスのコンポーネント構成



図F.2 - 利用者データ保護クラスのコンポーネント構成(続き)

FDPクラスのコンポーネントを使ってPP/STを作成する場合、以下の情報が、クラスのどこを見るか、何を選択するかのガイダンスを提供する。

FDPクラスの要件は、SFPを実現するセキュリティ機能(SFと省略される)の観点から定義される。TOEは複数のSFPを同時に実装できるので、PP/ST作成者は、他のファミリで参照できるように、各々のSFPの名前を特定しなければならない。選択した各コンポーネントでこの名前を使用すれば、該当機能の要件の定義の一部としてそれを使用していることを示すことができる。これによって、PP/ST作成者は、対象となるオブジェクト、対象となる操作、許可利用者など、操作の範囲を容易に示すことができる。

コンポーネントを具現化したものは、一つのSFPだけに適用できる。そのため、あるSFPがコンポーネントの中で定義されれば、このSFPはこのコンポーネント中のすべてのエレメントに適用される。必要ならば、異なる方針を説明するために、PP/STの中でそのコンポーネントを複数回具現化することができる。

このファミリからコンポーネントを選択する鍵は、FDP_ACC及びFDP_IFCという二つの方針コンポーネントから適切なコンポーネントを選択できるよう、完全に定義されたTOEセキュリティ方針を持つことである。FDP_ACCとFDP_IFCのそれぞれにおいて、すべてのアクセス制御方針とすべての情報フロー制御方針に名前を付ける。さらに、これらのコンポーネントの制御の範囲は、このセキュリティ機能の対象となるサブジェクト、

オブジェクト、及び操作の観点から特定される*。これらの方針の名前は、「アクセス制御SFP」あるいは「情報フロー制御SFP」を割付または選択することが必要な操作を持つ、他の機能コンポーネント全体において使用されることを想定している。名前を付けられたアクセス制御SFP及び情報フロー制御SFPの機能を定義する規則は、FDP_ACFファミリ及びFDP_IFFファミリで(それぞれ)定義される。 *(* 訳者注: 原文では文章に動詞が抜けているため、適切と思われる語を補完した。)*

以下のステップは、PP/STの構築において、このクラスがどのように適用されるかのガイダンスである。

a) 実施される方針を、FDP_ACCファミリ、及びFDP_IFCファミリから識別する。これらのファミリは、方針に対する制御範囲、制御の粒度を定義し、かつ方針に付随する規則を識別することができる。

b) コンポーネントを識別し、方針コンポーネント内で適用可能な操作をすべて実行する。割付操作は、判明している詳細さのレベルによって、一般的(「すべてのファイル」のような記述で)あるいは詳細に(「ファイル『A』、『B』」、など)実行することができる。

c) FDP_ACCファミリ及びFDP_IFCファミリから名前付けした方針ファミリに対応する、FDP_ACFファミリ及びFDP_IFFファミリからのすべての適用可能な機能コンポーネントを識別する。名前付けした方針によって実施される規則を、そのコンポーネントに定義させる操作を実行する。これにより、そのコンポーネントは、希望する、あるいは組み立てるべき選択された機能の要件に合致するようになる。

d) セキュリティ管理者だけ、オブジェクトの所有者だけなど、その機能の元でセキュリティ属性を管理かつ変更できるのは誰であるかを特定する。FMTセキュリティ管理クラスから適切なコンポーネントを選択し、操作を実行する。足りない特性を識別するため、ここでは、いくつかまたはすべての変更は高信頼パスを介して実行されなければならないなど、詳細化が役立つかもしれない。

e) 新しいオブジェクト及びサブジェクトに対する初期値のため、FMTセキュリティ管理クラスから適切なコンポーネントを識別する。

f) FDP_ROLファミリから、適用可能なロールバックコンポーネントすべてを識別する。

g) FDP_RIPファミリから、適用可能な残存情報保護要件をすべて識別する。

h) FDP_ITC及びFDP_ETCファミリから、適用可能なインポートあるいはエクスポートコンポーネントすべてと、インポート及びエクスポート時にセキュリティ属性がどのように扱われるかを識別する。

i) FDP_ITTファミリから、適用可能な内部TOE通信コンポーネントをすべて選択する。

j) FDP_SDIから、格納された情報の完全性保護のための要件をすべて識別する。

k) FDP_UCTあるいはFDP_UITファミリから、適用可能なTSF間通信コンポーネントをすべて識別する。

F.1 アクセス制御方針(FDP_ACC)

このファミリは、サブジェクトとオブジェクトの対話における裁量的制御の概念に基づいている。この制御の範囲と目的は、アクセス者(サブジェクト)の属性、アクセスされるコンテナ(オブジェクト)の属性、アクション(操作)、及び関連するアクセス制御規則に基づいている。

利用者のための注釈

このファミリのコンポーネントは、従来の裁量アクセス制御 Discretionary Access Control(DAC)メカニズムによって実施されるアクセス制御SFP(名前によって)の識別が可能である。さらに、識別されたアクセス制御SFPがカバーする、サブジェクト、オブジェクト、及び操作を定義する。アクセス制御SFPの機能を定義する規則は、FDP_ACF及びFDP_RIPのような他のファミリによって定義する。FDP_ACCで定義したアクセス制御SFPの名前は、「アクセス制御SFP」の割付または選択を必要とする操作を持つ、他の機能コンポーネント全体において使用されることを想定している。

アクセス制御SFPは、サブジェクト、オブジェクト、及び操作という3点セットをカバーする。そのため、一つのサブジェクトが複数のアクセス制御SFPによってカバーされることは可能だが、それは、異なる操作あるいは異なるオブジェクトに関してだけである。もちろん、オブジェクトと操作にも同じことが言える。

アクセス制御SFPを実施するアクセス制御機能の危険な側面は、アクセス制御の判断に関わる属性を利用者が改変できてしまうところにある。FDP_ACCファミリは、このような側面に対応していない。これらの要件の一部は、未定義のままになっているが、詳細化として追加することが可能で、それ以外は、FMTクラス: FMT セキュリティ管理など、どれか他のファミリとクラスの中でカバーされる。

FDP_ACCには監査要件がなく、それは、このファミリがアクセス制御SFPの要件を特定するものであるためである。監査要件は、このファミリで識別するアクセス制御SFPを満たす機能を特定するファミリの中に存在する。

このファミリは、PP/ST作成者にさまざまな方針を特定させることができる。例えば、一つの制御範囲に適用する固定アクセス制御SFP、異なる制御範囲に対して定義できる可変アクセス制御SFPがある。アクセス制御方針を複数個特定するために、別々の操作とオブジェクトのサブセットに対して、このファミリのコンポーネントをPP/STの中で複数回繰返すことができる。これは、TOEを、複数の方針を持ち、各々が特定のセットの操作とオブジェクトのセットに対応するようにさせられる。言い換えれば、PP/ST作成者は、TSFが実施する各アクセス制御SFPごとに、ACCコンポーネントにおいて必要な情報を特定すべきである。例えば、あるTOEが三つのアクセス制御SFPを持ち、各々がTOE内でオブジェクトとサブジェクトと操作の一つのサブセットだけをカバーしているとき、TOEは、三つのアクセス制御SFPごとに一つのFDP_ACC.1 サブセットアクセス制御コンポーネントを持ち、全部で三つのFDP_ACC.1コンポーネントが必要となる。

FDP_ACC.1　**サブセットアクセス制御**

利用者のための適用上の注釈

オブジェクト及びサブジェクトという言葉は、TOEの中の共通のエレメントを指す。方針を実現可能なものにするには、エンティティが明確に識別されなければならない。PPの場合、オブジェクトと操作は、名前付けされたオブジェクト、データリポジトリ、アクセスを監視する、などのような種別として表現することができる。特定のシステムに対しては、これらの共通的な用語(サブジェクト、オブジェクト)は、例えばファイル、レジスタ、ポート、デーモン、オープンコールなどのように、詳細化しなければならない。

このコンポーネントは、あるオブジェクトのサブセットに対する完全に定義された操作のセットを方針がカバーすることを特定する。セット外のいかなる操作に対しても制約はない - それに対して、他の操作が制御されるオブジェクトに対する操作を含む。

操作

割付:

FDP_ACC.1.1において、PP/ST作成者は、TSFによって実施される、一意に名前付けされたアクセス制御SFPを特定すべきである。

PFDP_ACC.1.1において、P/ST作成者は、そのSFPでカバーされるサブジェクト、オブジェクト、及びオブジェクトとサブジェクト間の操作のリストを特定すべきである。

FDP_ACC.2　**完全アクセス制御**

利用者のための適用上の注釈

このコンポーネントは、オブジェクトに対するすべての可能な操作(そのSFPに含まれるもの)が、一つのアクセス制御SFPでカバーされることを要求する。

PP/ST作成者は、オブジェクトとサブジェクトの各組み合わせが一つのアクセス制御SFPでカバーされてていることを実証しなければならない。

操作

割付:

FDP_ACC.2.1において、PP/ST作成者は、TSFによって実施される、一意に名前付けされたアクセス制御SFPを特定すべきである。

FDP_ACC.2.1において、PP/ST作成者は、SFPによってカバーされるサブジェクトとオブジェクトのリストを特定すべきである。これらのサブジェクトとオブジェクト間のすべての操作はそのSFPでカバーされる。

F.2　**アクセス制御機能**(FDP_ACF)

このファミリは、方針の制御の範囲を特定するFDP_ACCで名前付けされたアクセス制御方針の実現が可能な、特定の機能のための規則を記述する。

利用者のための注釈

このファミリは、PP/ST作成者に、アクセス制御に対する規則を記述する能力を提供する。これは、オブジェクトに対するアクセスが取り替えられないシステムというものに帰着する。そのようなオブジェクトの例として、「本日のメッセージ」がある。これは、全員が読めるが、許可管理者しか変更できない。また、このファミリは、PP/ST作成者に、一般的なアクセス制御規則に対する例外を提供する規則を記述できるようにする。そのような例外では、オブジェクトに対するアクセスを、明示的に許可したり拒否したりする。

二人制御、操作の順序規則、あるいは除外制御といった他の可能な機能を特定するような明示的なコンポーネントはない。しかしながら、従来のDACメカニズムはいうまでもなく、これらのメカニズムは、アクセス制御規則を注意深く立案することで、現存のコンポーネントで表現することができる。

容認できる各種のアクセス制御SFは、このファミリでは、次のように特定できる。

- アクセス制御リスト(ACL)
- 時間によるアクセス制御仕様
- 発信源によるアクセス制御仕様
- 所有者管理のアクセス制御属性

FDP_ACF.1　**セキュリティ属性によるアクセス制御**

利用者のための適用上の注釈

このコンポーネントは、サブジェクト及びオブジェクトに関連したセキュリティ属性に基づいてアクセス制御を調停するメカニズムの要件を提供する。各オブジェクトとサブジェクトは、場所、作成時間、アクセス権(例: アクセス制御リスト(ACL))など、関連する属性のセットを持っている。このコンポーネントは、PP/ST作成者が、アクセス制御調停に使用する属性を特定できるようにする。このコンポーネントは、これらの属性を使って、アクセス制御規則を特定できるようにする。

PP/ST作成者が割り付けることができる属性の例が、以下の段落で示される。

識別情報属性は、調停のために使用される、利用者、サブジェクト、またはオブジェクトに関連付けられる。このような属性の例としては、サブジェクトの作成に使用されるプログラムイメージの名前や、そのプログラムイメージに割り付けられるセキュリティ属性などがある。

時間属性は、その日のある時間内、その週のある曜日間、またはある暦年内に許可される

アクセスを特定するのに使うことができる。

*場所属性*は、その場所が、操作を要求する場所と操作が実行される場所のいずれか、あるいは両方であるかを特定できる。これは、TSFの論理インタフェースを端末の場所やCPUの場所といった場所に変換する内部表に基づいて可能になる。

*グルーピング属性*は、一つの利用者グループを、アクセス制御の目的に対する操作に関連付けられるようにする。必要なら、定義可能なグループの最大数、一つのグループの最大のメンバ数、ある利用者が同時に組み入れられるグループの最大個数を特定するために、詳細化操作が使われるべきである。

このコンポーネントは、また、セキュリティ属性に基づいて、オブジェクトに対するアクセスを明示的に許可あるいは拒否できるアクセス制御セキュリティ機能に対する要件を提供する。これは、TOE内の特権、アクセス権、またはアクセスの許可を提供するのに使用できる。そのような特権、権限、または許可は、利用者、サブジェクト(利用者またはアプリケーションを代表する)、及びオブジェクトに適用できる。

操作

割付:

FDP_ACF.1.1において、PP/ST作成者は、TSFが実施するアクセス制御SFP名を特定すべきである。アクセス制御SFPの名前と、その方針に対する制御の範囲は、FDP_ACCからのコンポーネントで定義される。

FDP_ACF.1.1において、PP/ST作成者は、セキュリティ属性及び/またはその機能が規則の特定において使用するセキュリティ属性の名前付きグループを特定すべきである。例えば、そのような属性には、利用者識別情報、サブジェクト識別情報、役割、1日の中の時刻、場所、ACL、あるいはPP/ST作成者が特定するその他の属性などがある。セキュリティ属性の名前付きグループは、複数のセキュリティ属性を参照する便利な方法を提供するために特定されることができる。名前付きグループは、FMT_SMR セキュリティ管理の役割で定義された「役割」と、それに関連するすべての属性を、サブジェクトに関係付ける有用な方法を提供できる。言い換えれば、各役割は、属性の名前付きグループに関連させられる。

FDP_ACF.1.2において、PP/ST作成者は、制御されたオブジェクトに対する制御された操作を用いる、制御されたサブジェクトと制御されたオブジェクト間のアクセスを管理するSFP規則を特定すべきである。これらの規則は、いつアクセスが承認されるかあるいは拒否されるかを特定する。これは、一般的なアクセス制御機能(例えば、典型的な許可ビット)や小さく分割したアクセス制御機能(例えば、ACL)を特定することができる。

FDP_ACF.1.3において、PP/ST作成者は、セキュリティ属性に基づいて、アクセスを明示的に許可するために使われる、サブジェクトからオブジェクトへの

アクセスを明示的に許可するための規則を特定すべきである。これらの規則は、FDP_ACF.1.1で特定されたものに追加されるものである。それらはFDP_ACF.1.1における規則に対する例外を入れることを意図しているため、FDP_ACF.1.3に含められる。アクセスを明示的に許可する規則の一例は、サブジェクトと関連付ける特権ベクタである。これは、特定されたアクセス制御SFPがカバーするオブジェクトに対するアクセスを常に承認する。このような機能が不要な場合、PP/ST作成者は「なし」と特定すべきである。

FDP_ACF.1.4において、PP/ST作成者は、セキュリティ属性に基づいて、サブジェクトからオブジェクトへのアクセスを明示的に拒否するための規則を特定すべきである。これらの規則は、FDP_ACF.1.1で特定されたものに追加されるものである。それらは、FDP_ACF.1.1における規則に対する例外を入れることを意図しているため、FDP_ACF.1.4に含められる。アクセスを明示的に拒否する規則の一例は、サブジェクトと関連付ける特権ベクタである。これは、特定されたアクセス制御SFPがカバーするオブジェクトに対するアクセスを常に拒否する。このような機能が不要な場合、PP/ST作成者は「なし」と特定すべきである。

F.3　**データ認証**(FDP_DAU)

このファミリは、「静的」データの認証に使用できる特定の機能を記述する。

利用者のための注釈

このファミリのコンポーネントは、「静的」データ認証の要件があるとき、すなわち、データは署名されるが送信されないところで使われるべきである(FCO_NROファミリは、データ交換時に受信した情報の発信の否認不可を提供することに注意)。

FDP_DAU.1　**基本的データ認証**

利用者のための適用上の注釈

このコンポーネントは、情報内容の有効性あるいは真正性の検証に使用され得る、最も確実な文書のハッシュ値を生成するような単方向ハッシュ関数(暗号チェックサム、指紋、メッセージダイジェスト)によって満たすことができる。

操作

割付:

FDP_DAU.1.1において、PP/ST作成者は、TSFがそれに対してデータ認証の証拠を生成できねばならないオブジェクトまたは情報種別のリストを特定すべきである。

FDP_DAU.1.2において、PP/ST作成者は、直前のエレメントで識別したオブジェクトのデータ認証の証拠を検証できるようなサブジェクトのリストを特定すべきである。サブジェクトのリストは、サブジェクトが既知の場合、非常に特定的なものとなることがあり、あるいは、より一般的で、識別された役割のように、サブジェクトの「種別」を参照するものにもできる。

FDP_DAU.2　**保証人識別付きデータ認証**

利用者のための適用上の注釈

このコンポーネントは、追加的に、真正性の保証を提供する利用者(例えば、信頼できる第三者; trusted third party)の識別情報を検証できることを要求する。

操作

割付:

FDP_DAU.2.1において、PP/ST作成者は、TSFがそれに対してデータ認証の証拠を生成できねばならないオブジェクトまたは情報種別のリストを特定すべきである。

FDP_DAU.2.2において、PP/ST作成者は、**データ認証の証拠を作成した利用者の識別情報に加えて、**直前のエレメントで識別したオブジェクトのデータ認証の証拠を検証できるようなサブジェクトのリストを特定すべきである。

F.4　TSF制御外へのエクスポート(FDP_ETC)

このファミリは、TOEから利用者データをエクスポートする機能を定義するもので、そのセキュリティ属性は、明示的に保持されるか、あるいはエクスポートされるたあと無視される。これらのセキュリティ属性の一貫性は、FPT_TDC TSF間TSFデータ一貫性が対応する。

FDP_ETCは、エクスポートの制限、及びエクスポートされる利用者データとセキュリティ属性の関連に関するものである。

利用者のための注釈

このファミリ、及び対応するインポートファミリ FDP_ITCは、その制御範囲内あるいは範囲外へ転送される利用者データをTOEがどのように扱うかに対応する。原則として、このファミリは、利用者データのエクスポートと、それに関連するセキュリティ属性に関するものである。

ここでは、次のようなさまざまなアクティビティが関係する。

a) セキュリティ属性なしで利用者データをエクスポートする;

b) セキュリティ属性を含めて利用者データをエクスポートする。両者はは互いに関連付けられており、セキュリティ属性はあいまいさなくエクスポートされる利用者データを表す。

複数のSFP(アクセス制御及び/または情報フロー制御)がある場合、名前付けされたSFPごとにこれらのコンポーネントを繰り返すことが適切かもしれない。

FDP_ETC.1　セキュリティ属性なし利用者データのエクスポート

利用者のための適用上の注釈

このコンポーネントは、セキュリティ属性のエクスポートなしの利用者データのエクスポートを特定するのに使われる。

操作

割付:

FDP_ETC.1.1において、PP/ST作成者は、利用者データのエクスポート時に実施するアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。この機能がエクスポートする利用者データは、これらのSFPの割付によって範囲が決められる。

FDP_ETC.2 **セキュリティ属性付き利用者データのエクスポート**

利用者のための適用上の注釈

利用者データは、そのセキュリティ属性といっしょにエクスポートされる。セキュリティ属性は、利用者データとあいまいさなく関連付けられている。この関連付けは、いくつかの方法で達成できる。利用者データとセキュリティ属性を物理的に並べる(例えば同一のフロッピー)方法もあれば、セキュア署名などの暗号技術を使ってセキュリティ属性と利用者データを関連付けるという方法もある。FTP_ITC TSF間高信頼チャネルを使用すれば、他方の高信頼IT製品がセキュリティ属性を正しく受信したことを保証でき、一方、FPT_TDC TSF間TSFデータ一貫性は、それらの属性が正しく解釈することを確実にするために使うことができる。さらに、FTP_TRP高信頼パスは、エクスポートが適切な利用者によって起動されることを確かめるために使用できる。

操作

割付:

FDP_ETC.2.1において、PP/ST作成者は、利用者データのエクスポート時に実施するアクセス制御SFP(一つまたは複数)や情報フロー制御SFP(一つまたは複数)を特定すべきである。この機能でエクスポートする利用者データの範囲は、これらのSFPの割付によって決められる。

FDP_ETC.2.4において、PP/ST作成者は、追加的なエクスポート制御規則をすべて、あるいは追加的なエクスポート制御規則がない場合は「なし」を特定すべきである。これらの規則は、FDP_ETC.2.1で選択したアクセス制御SFP及び/または情報フローSFPに加えて、TSFによって実施される。

F.5　情報フロー制御方針(FDP_IFC)

このファミリは、情報フロー制御SFPの識別をカバーし、かつ各々に対して、SFPの制御範囲を特定する。

この目的を満たすセキュリティ方針の例:

- Bell and La Padulaセキュリティモデル[B&L]
- Biba完全性モデル[Biba]
- 干渉不可(Non-Interference) [Gogu1、Gogu2]

利用者のための注釈

このファミリのコンポーネントは、TOE内に見られる従来の必須アクセス制御メカニズムで実施される情報フロー制御SFPを識別できる。しかしながら、それらは従来のMACメカニズムを越え、干渉不可の方針及び状態遷移の識別及び記述に使うことができる。さらに、TOE内の各情報フロー制御SFPに対して、方針の制御下のサブジェクト、方針の制御下の情報、及び制御されたサブジェクトへ/からの制御された情報フローを生じさせる操作を定義する。情報フロー制御SFPの規則を定義する機能は、FDP_IFF及びFDP_RIPなどの他のファミリで定義される。このFDP_IFCにおいて名前付けされた情報フロー制御SFP*は、「情報フロー制御SFP」の割付または選択を必要とする操作を持つ残りの機能コンポーネント全体において使用されることを想定している。 *(* 訳者注: 原文では「アクセス制御SFP」と書かれているが、「情報フロー盛業SFP」の間違いと思われる。)*

これらのコンポーネントは全く柔軟である。これらのコンポーネントは、フロー制御のドメインを特定することができ、そのメカニズムがラベルに基づくという必要はない。情報フロー制御コンポーネントの別のエレメントでは、方針に対して程度が異なる例外が許される。

各SFPは三点セット: サブジェクト、情報、及びサブジェクトへ/から情報の流れを生じさせる操作、をカバーする。情報フロー制御方針によっては、細かさが非常に低レベルで、オペレーティングシステム内のプロセスの用語でサブジェクトを明示的に記述することもある。別の情報フロー制御方針では、高レベルで、利用者の総称的な意味や入出力チャネルでサブジェクトを記述することもある。情報フロー制御方針の細かさのレベルが高すぎると、望まれるITセキュリティ機能を明確に定義できないかもしれない。そのような場合は、情報フロー制御方針のそのような記述を、セキュリティ対策方針に含めるほうが適切である。そうすれば、望まれるITセキュリティ機能を、それらのセキュリティ対策方針をサポートするものとして特定できる。

2番目のコンポーネント(FDP_IFC.2 完全情報フロー制御)では、各情報フロー制御SFPは、そのSFPのカバーする情報が、そのSFPのカバーするサブジェクトへ/からの流れを生じる可能性のあるすべての操作をカバーする。さらに、すべての情報フローは、一つのSFP

でカバーされる必要がある。従って、情報フローを生じさせるアクションごとに、そのアクションを許可するかどうかを定義する規則のセットが存在する。ある情報フローに対して、適用可能な複数のSFPが存在するとすると、用いられるすべてのSFPは、フローが生じる前にこのフローを許可しなければならない。

情報フロー制御SFPは、完全に定義された操作のセットをカバーする。SFPのカバー範囲は、いくつかの情報フローに関しては「完全」かもしれず、あるいはその情報フローに影響を与えるいくつかの操作だけに対応するものかもしれない。

アクセス制御SFPは、情報を入れたオブジェクトへのアクセスを制御する。情報フロー制御SFPは、コンテナと独立した、情報に対するアクセスを制御する。その情報の属性は、コンテナの属性と関係付けられていることもあるが(あるいは、マルチレベルデータベースの場合のようにそうでないこともある)、情報が流れるときにそれと一緒にある。明示的な権限がない場合、アクセス者はその情報の属性を変更することができない。

情報のフロー及び操作は、複数のレベルで表現することができる。STの場合、情報のフロー及び操作は、システムに固有なレベルで特定されることがある: 既知のIPアドレスに基づいてファイアウォールを通過するTCP/IPパケット。PPでは、情報のフロー及び操作は、種別として表現されることがある: 電子メール、データリポジトリ、アクセスを監視、等々。

このファミリのコンポーネントは、異なる操作及びオブジェクトのサブセットに対して、PP/STの中で複数回適用することができる。これは、TOEに、各々特定のオブジェクト、サブジェクト、及び操作のセットに対応する複数の方針を持たせることができる。

FDP_IFC.1　サブセット情報フロー制御

利用者のための適用上の注釈

このコンポーネントは、情報フロー制御方針が、TOE内で可能な操作のサブセットに適用されることを要求する。

操作

割付:

FDP_IFC.1.1において、PP/ST作成者は、TSFが実施する一意に名前付けされた情報フロー制御SFPを特定すべきである。

FDP_IFC.1.1において、PP/ST作成者は、SFPがカバーする制御されたサブジェクトへ/から、制御された情報の流れを生じさせるサブジェクト、情報、及び操作のリストを特定すべきである。上記のように、サブジェクトのリストは、PP/ST作成者の必要に応じて、さまざまな細かさのレベルであってよい。例えば、利用者、マシン、プロセスを特定することができる。情報は、電子メール、ネットワークプロトコル、あるいはアクセス制御方針において特定されたもの

と同様、さらに特定化したオブジェクトなどのデータを参照することができる。もし、特定された情報がアクセス制御方針の対象であるオブジェクト内に含まれる場合は、特定された情報がそのオブジェクトへ/から流せるようになる前に、そのアクセス制御方針と情報フロー制御方針の両方が実施されなければならない。

FDP_IFC.2　完全情報フロー制御

利用者のための適用上の注釈

このコンポーネントは、SFPに含まれるサブジェクトへ/から情報を流れさせるすべての可能な操作を要求する。

PP/ST作成者は、情報フローとサブジェクトの各組み合わせが情報フロー制御SFPによってカバーされることを実証しなければならない。

操作

割付:

FDP_IFC.2.1において、PP/ST作成者は、TSFが実施する一意に名前付けされた情報フロー制御SFPを特定すべきである。

FDP_IFC.2.1において、PP/ST作成者は、SFPがカバーするサブジェクトと情報のリストを特定すべきである。サブジェクトへ/から情報を流れさせるすべての操作はSFPによってカバーされなければならない。上記のように、サブジェクトのリストは、PP/ST作成者の必要に応じて、さまざまな細かさのレベルであってよい。例えば、利用者、マシン、プロセスを特定することができる。情報は、電子メール、ネットワークプロトコル、あるいはアクセス制御方針において特定されたものと同様、さらに特定化したオブジェクトなどのデータを参照することができる。もし、特定された情報がアクセス制御方針のサブジェクトであるオブジェクト内に含まれる場合は、特定された情報がそのオブジェクトへ/から流せるようになる前に、そのアクセス制御方針と情報フロー制御方針の両方が実施されなければならない。

F.6　情報フロー制御機能(FDP_IFF)

このファミリは、FDP_IFC、これは方針の制御の範囲も特定するが、で名前付けされた情報フロー制御SFPを実現できる特定の機能についての規則を記述する。二つの「ツリー」から構成され、一つは共通の情報フロー制御機能問題に対応し、他方は、一つあるいは複数の情報フロー制御SFPに関する不正な情報フロー(すなわち隠れチャネル)に対応する。この区分が生じる理由は、不正な情報フローに関する問題が、ある意味で、SFPの残りの部分に直交しているからである。不正な情報フローとは、方針を侵害したフローであり、これは方針の問題ではない。

利用者のための注釈

信頼できないソフトウェアを考えると、暴露や改変に対する強力な保護を実現するために、情報フローにおける制御が必要になる。アクセス制御だけでは不十分なのは、それがコンテナに対するアクセスを制御するだけだからである。中に入れた情報が、制御なしでシステム全体を流れるのを許してしまう。

このファミリでは、「不正な情報フローの種別」という語句を使用する。この語句は、「格納チャネル」や「タイミングチャネル」のようなフローの分類を指す場合にも使用することができる。また、PP/ST作成者のニーズを反映した改善された分類を指すこともできる。

このコンポーネントの柔軟性は、FDP_IFF.1及びFDP_IFF.2における特権方針の定義が、特定のSFPの全部または一部について、制御されたバイパスを認めることを可能にする。もしSFPのバイパスを事前に定義しておくアプローチが必要ならば、PP/ST作成者は、特権方針の組み込みを考慮すべきである。

FDP_IFF.1　単純セキュリティ属性

利用者のための適用上の注釈

このコンポーネントでは、情報における、及び情報を流れさせるサブジェクトとその情報の受信者としてふるまうサブジェクトにおける、セキュリティ属性を規定する。情報のコンテナの属性が情報フロー制御の判断の一部に関与すべきことが望ましいか、あるいはそれらがアクセス制御方針でカバーされていれば、それらもまた考慮されるべきである。このコンポーネントは、実施実施するキー規則を特定し、どのようにセキュリティ属性が導出されるかを記述する。例えば、TSPにおける少なくとも一つの情報フロー制御SFPが、Bell and LaPadulaセキュリティ方針モデル[B&L]で定義されるようにラベルに基づき、かつこれらのセキュリティ属性が階層を形成しないとき、このコンポーネントが使用されるべきである。

このコンポーネントは、セキュリティ属性をどのように割り付けるかの詳細(すなわち利用者対プロセス)を特定しない。必要に応じて、追加方針及び機能要件の特定を認めるような割付を持たせることで、方針における柔軟性を提供する。

このコンポーネントはまた、情報フロー制御機能がセキュリティ属性に基づいて情報フローを明示的に許可及び拒否できる要件を規定する。これは、このコンポーネントで定義した基本方針に対する例外をカバーする特権方針の実現に使用することができる。

操作

割付:

FDP_IFF.1.1において、PP/ST作成者は、TSFによって実施される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対する制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.1.1において、PP/ST作成者は、その機能が規則を特定するために使用するセキュリティ属性の最少数と種別を特定すべきである。例えば、そのような属性には、サブジェクト識別子、サブジェクトの機密(sensitivity)レベル、サブジェクトの取扱許可(clearance)レベル、情報の機密レベルなどがある。セキュリティ属性の各種別の最少数は、環境の必要性をサポートするのに十分であるべきである。

FDP_IFF.1.2において、PP/ST作成者は、各操作ごとに、サブジェクトとTSFが実施する情報セキュリティ属性の間で保持しなければならない、セキュリティ属性に基づく関係を特定すべきである。

FDP_IFF.1.3において、PP/ST作成者は、TSFが実施する情報フロー制御SFPの追加規則を特定すべきである。追加規則がないときは、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.1.4において、PP/ST作成者は、TSFが提供することになっている追加SFP能力をすべて特定すべきである。追加能力がないときは、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.1.5において、PP/ST作成者は、セキュリティ属性に基づいて、明示的に情報フローを許可する規則を特定すべきである。これらの規則は、前に書かれたエレメントで特定されたものに追加されるものである。これらは、前に書かれた規則に対する例外を含めることを意図しているので、FDP_IFF.1.5に含められている。明示的に情報フローを許可する規則の一例として、既に特定されたSFPがカバーする情報に対して情報フローを生じさせる能力を常時サブジェクトに認める、そのサブジェクトに関連付けられた特権ベクタがある。このような能力が不要な場合、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.1.6において、PP/ST作成者は、セキュリティ属性に基づいて、明示的に情報フローを拒否する規則を特定すべきである。これらの規則は、前に書かれたエレメントで特定されたものに追加されるものである。これらは、前に書かれた規則に対する例外を含めることを意図しているので、FDP_IFF.1.6に含められている。明示的に情報フローを拒否する規則の一例として、既に特定され

たSFPがカバーする情報に対して情報フローを生じさせる能力を常時サブジェクトに拒否する、そのサブジェクトに関連付けられた特権ベクタがある。このような能力が不要な場合、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.2 **階層的セキュリティ属性**

利用者のための適用上の注釈

このコンポーネントは、TSPにおけるすべての情報フロー制御SFPが、格子(lattice)を形成する階層的セキュリティ属性を使用することを要求する。

例えば、TSPにおける少なくとも一つの情報フロー制御SFPがBell and LaPadulaのセキュリティ方針モデル[B&L]で定義されるようにラベルに基づき、かつ階層を形成する場合は、これが使用されるべきである。

FDP_IFF.2.5で識別される階層的関係要件は、FDP_IFF.2.1で識別された情報フロー制御SFPの情報フロー制御セキュリティ属性にだけ適用される必要があることに注意することが重要である。このコンポーネントは、アクセス制御SFPなどの他のSFPに適用するためのものではない。

前述のコンポーネントと同様に、このコンポーネントも、明示的な情報フローの許可または拒否を認める規則をカバーする特権方針を実現するために使用することができる。

複数の情報フロー制御SFPが特定され、かつ互いに関係しないこれら自身のセキュリティ属性を持つ場合は、PP/ST作成者は、このコンポーネントをこれらの各SFPごとに一回ずつ繰り返すべきである。さもないと、要求された関係が存在せずに、FDP_IFF.2.5のサブ項目に矛盾が生じるかもしれない。

操作

割付:

FDP_IFF.2.1において、PP/ST作成者は、TSFによって実施される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対する制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.2.1において、PP/ST作成者は、その機能が規則を特定するために使用するセキュリティ属性の最少数と種別を特定すべきである。例えば、そのような属性には、サブジェクト識別子、サブジェクトの機密レベル、サブジェクトの取扱許可レベル、情報の機密レベルなどがある。セキュリティ属性の各種別の最少数は、環境の必要性をサポートするのに十分であるべきである。

FDP_IFF.2.2において、PP/ST作成者は、各操作ごとに、サブジェクトとTSFが実施する情報セキュリティ属性の間で保持しなければならない、セキュリティ属性に基づく関係を特定すべきである。**これらの関係は、セキュリティ属性間**

の順序に基づくべきである。

FDP_IFF.2.3において、PP/ST作成者は、TSFが実施する情報フロー制御SFPの追加規則を特定すべきである。追加規則がないときは、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.2.4において、PP/ST作成者は、TSFが提供することになっている追加SFP能力をすべて特定すべきである。追加能力がないときは、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.2.5において、PP/ST作成者は、セキュリティ属性に基づいて、明示的に情報フローを許可する規則を特定すべきである。これらの規則は、前に書かれたエレメントで特定されたものに追加されるものである。これらは、前に書かれた規則に対する例外を含めることを意図しているので、FDP_IFF.2.5に含められている。明示的に情報フローを許可する規則の一例として、既に特定されたSFPがカバーする情報に対して情報フローを生じさせる能力を常時サブジェクトに認める、そのサブジェクトに関連付けられた特権ベクタがある。このような能力が不要な場合、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.2.6において、PP/ST作成者は、セキュリティ属性に基づいて、明示的に情報フローを拒否する規則を特定すべきである。これらの規則は、前に書かれたエレメントで特定されたものに追加されるものである。これらは前に書かれた規則に対する例外を含めることを意図しているので、FDP_IFF.2.6に含められている。明示的に情報フローを拒否する規則の一例として、既に特定されたSFPがカバーする情報に対して情報フローを生じさせる能力を常時サブジェクトに拒否する、そのサブジェクトに関連付けられた特権ベクタがある。このような能力が不要な場合、PP/ST作成者は「なし」と特定すべきである。

FDP_IFF.3　制限付き不正情報フロー

利用者のための適用上の注釈

不正情報フローの制御を要求する少なくとも一つ以上のSFPがフローの除去を要求しないとき、このコンポーネントが使用されるべきである。

特定された不正情報フローに対して、ある最大容量が提供されるべきである。加えて、PP/ST作成者は、不正情報フローが監査されねばならないかどうかを特定することができる。

操作

割付:

FDP_IFF.3.1において、PP/ST作成者は、TSFによって実施される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対す

る制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.3.1において、PP/ST作成者は、最大容量制限に対するサブジェクトである不正情報フローの種別を特定すべきである。

FDP_IFF.3.1において、PP/ST作成者は、すべての識別された不正情報フローに対して許可された最大容量を特定すべきである。

FDP_IFF.4 不正情報フローの部分的排除

利用者のための適用上の注釈

不正情報フローの制御を要求するすべてのSFPが、いくつかの(すべてである必要はない)不正情報フローの除去を要求するとき、このコンポーネントが使用されるべきである。

操作

割付:

FDP_IFF.4.1において、PP/ST作成者は、TSFによって実施される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対する制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.4.1において、PP/ST作成者は、最大容量制限に対するサブジェクトである不正情報フローの種別を特定すべきである。

FDP_IFF.4.1において、PP/ST作成者は、すべての識別された不正情報フローに対して許可された最大容量を特定すべきである。

FDP_IFF.4.2において、PP/ST作成者は、除去される不正情報フローの種別を特定すべきである。このコンポーネントはいくつかの不正情報フローが除去されるようになっていることを要求するので、そのリストは、空であってはならない。

FDP_IFF.5 不正情報フローなし

利用者のための適用上の注釈

不正情報フローの制御を要求するSFPが、すべての不正情報フローの除去を要求するとき、このコンポーネントが使用されるべきである。しかしながら、すべての不正情報フローを除去することがTOEの通常の機能動作に与えるかもしれない潜在的な影響を、PP/ST作成者は注意深く考慮すべきである。TOE内の不正情報フローと通常の機能との間に間接的な関係が存在し、すべての不正情報フローを除去することが期待したとおりの機能が得られない結果につながるかもしれないことをが、多くの実際のアプリケーションで示されている。

操作

割付:

FDP_IFF.5.1において、PP/ST作成者は、不正情報フローが除去される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対する制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.6 **不正情報フロー監視**

利用者のための適用上の注釈

このコンポーネントは、特定した容量を超える不正情報フローの使用を監視する能力をTSFが提供することが求められるときに使用されるべきである。そのようなフローを監査することが求められる場合、このコンポーネントは、FAU_GEN セキュリティ監査データ生成ファミリのコンポーネントによって使用される監査事象源として役立つ。

操作

割付:

FDP_IFF.6.1において、PP/ST作成者は、TSFによって実施される情報フロー制御SFPを特定すべきである。情報フロー制御SFPの名前、及びその方針に対する制御の範囲は、FDP_IFCからのコンポーネントにおいて定義される。

FDP_IFF.6.1において、PP/ST作成者は、最大容量の超過に対して監視される、不正情報フローの種別のリストを特定すべきである。

FDP_IFF.6.1において、PP/ST作成者は、それを超えるとTSFによって不正情報フローが監視される最大容量を特定すべきである。

F.7　TSF制御外からのインポート(FDP_ITC)

このファミリは、利用者データのセキュリティ属性が保持できるような、TSCの外部からTOEに利用者データをインポートするためのメカニズムを定義する。これらのセキュリティ属性の一貫性は、FPT_TDC TSF間TSFデータ一貫性で対応される。

FDP_ITCは、インポート時の制限、利用者指定のセキュリティ属性、及びセキュリティ属性の利用者データとの関連付けに関係する。

利用者のための注釈

このファミリ及び対応するエクスポートファミリFDP_ETCファミリは、TOEがその制御外の利用者データをどのように扱うかに対応する。このファミリは、利用者データのセキュリティ属性の割付と抽出に関係する。

ここでは、さまざまなアクティビティが関係する:

a) 形式化されていない媒体(例えば、フロッピーディスク、テープ、スキャナ、ビデオ、あるいはオーディオ信号)から、セキュリティ属性を含めずに、及びその内容を示すために媒体に物理的な印をつけずに、利用者データをインポートすること;

b) セキュリティ属性を含めて媒体から利用者データをインポートし、そのオブジェクトのセキュリティ属性が適切であることを検証すること;

c) 利用者データとセキュリティ属性の関係を保護するための暗号封印技術を使用して、セキュリティ属性を含めて媒体から利用者データをインポートすること。

このファミリは、利用者データをインポートしてよいかどうかの判断には関係しない。これは、インポートされる利用者データと組み合せるセキュリティ属性の値に関係する。

利用者データのインポートに関しては、二つの可能性がある: 利用者データが、あいまいさなく信頼できるオブジェクトセキュリティ属性(セキュリティ属性の値と意味が改変されない)と組み合わされるか、あるいは、インポート源から信頼できるセキュリティ属性が得られない(あるいは、セキュリティ属性がまったくない)。このファミリは、両方の場合に対応する。

信頼できるセキュリティ属性が利用可能であれば、これらは、物理的な手段(セキュリティ属性が同じ媒体上にある)によるか、あるいは論理的な手段(セキュリティ属性は別に配付されるが、暗号チェックサムのような一意のオブジェクト識別情報を持つ)によって、利用者データと関連付けることができる。

このファミリは、SFPによって要求されるように、利用者データのインポート及びセキュリティ属性との関連付けの維持に関係する。他のファミリは、このファミリの範囲を超え

た、一貫性、高信頼チャネル、完全性といったインポートの他の側面に関係する。さらに、FDP_ITCは、インポート媒体のインタフェースに関係するだけである。FDP_ETCは、その媒体の他端(発生源)に対する責任を持つ。

インポート要件としてよく知られているものは、次のようなものである:

a) セキュリティ属性なしで利用者データをインポートすること;

b) セキュリティ属性を含む利用者データをインポートすること。両者は互いに関連付けられ、セキュリティ属性はあいまいさなくインポートされる情報を代表する。

これらのインポート要件は、ITの制限及び組織のセキュリティ方針に依存して、人間の介在あり、あるいはなしでTSFによって扱われるかもしれない。例えば、利用者データが「機密」チャネル上で受信される場合は、オブジェクトのセキュリティ属性は「機密」に設定される。

複数のSFP(アクセス制御及び/または情報フロー制御)がある場合は、各々の名前付きSFPごとにこれらのコンポーネントを繰り返すことが適切かもしれない。

FDP_ITC.1 セキュリティ属性なし利用者データのインポート

利用者のための適用上の注釈

このコンポーネントは、利用者データに関連付けられた信頼できる(あるいは何でも)セキュリティ属性を持たない利用者データのインポートを特定するのに使用される。この機能は、インポートされた利用者データのセキュリティ属性がTSFの中で初期化されることを要求する。PP/ST作成者がインポートに関する規則を特定することも許される。環境によっては、これらの属性が、高信頼パスあるいは高信頼チャネルのメカニズムを介して供給されるのが適切かもしれない。

操作

割付:

FDP_ITC.1.1において、PP/ST作成者は、利用者データがTSCの外部からインポートされるときに実施されるアクセス制御SFP及び/または情報フロー制御SFPを特定すべきである。この機能がインポートする利用者データは、これらのSFPの割付によって範囲が決められる。

FDP_ITC.1.3において、PP/ST作成者は、すべての追加インポート制御規則を特定するか、あるいは追加インポート制御規則がなければ「なし」を特定すべきである。これらの規則は、FDP_ITC.1.1で選択したアクセス制御SFP及び/または情報フロー制御SFPに追加されて、TSFによって実施される。

FDP_ITC.2　セキュリティ属性付き利用者データのインポート

利用者のための適用上の注釈

このコンポーネントは、信頼できるセキュリティ属性が関連付けられた利用者データのインポートを特定するのに用いられる。この機能は、インポート媒体上でオブジェクトと正確かつあいまいさなく関連付けられるセキュリティ属性をあてにする。インポートされると、それらのオブジェクトはそれらの同じ属性を持つようになる。これは、FPT_TDCにそのデータの一貫性の保証を要求する。PP/ST作成者は、インポートのための規則を特定することもできる。

操作

割付:

FDP_ITC.2.1において、PP/ST作成者は、利用者データをTSCの外部からインポートするときに実施するアクセス制御SFP及び/または情報フロー制御SFPを特定すべきである。この機能がインポートする利用者データは、これらのSFPの割付によって範囲を決められる。

FDP_ITC.2.5において、PP/ST作成者は、すべての追加インポート制御規則を特定するか、あるいは追加インポート制御規則がない場合は「なし」を特定すべきである。これらの規則は、FDP_ITC.2.1で選択されたアクセス制御SFP及び/または情報フロー制御SFPに追加して、TSFによって実施される。

F.8　TOE内転送(FDP_ITT)

このファミリは、内部チャネルを介してTOEのパーツ間で利用者データが転送されるときの、利用者データの保護に対応する要件を提供する。これは、FDP_UCT及びFDP_UITファミリと対比でき、それらは、外部チャネルを介して別々のTSF間で利用者データが転送されるときの利用者データに対する保護を提供し、そしてFDP_ETC及びFDP_ITCは、TSF制御外へ/からのデータの転送に対応する。

利用者のための注釈

このファミリの要件は、TOE内での通過に際して、利用者データにとって望ましいセキュリティをPP/ST作成者が特定できるようにする。このセキュリティは、暴露、改変、または可用性の損失に対する保護であってもよい。

このファミリが適用すべき物理的分離の度合いの判断は、意図する使用環境に依存する。敵対的環境では、システムバスだけで分離されたTOEのパーツ間の転送から生じる危険があるかもしれない。もっと穏やかな環境では、より伝統的なネットワーク媒体を通した転送が許される。

複数のSFP(アクセス制御及び/または情報フロー制御)がある場合は、これらのコンポーネントを名前付きSFPごとに一つ繰り返すのが適切かもしれない。

FDP_ITT.1　基本内部転送保護

操作

割付:

FDP_ITT.1.1において、PP/ST作成者は、転送される情報をカバーするアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。

選択:

FDP_ITT.1.1において、PP/ST作成者は、伝送中の利用者データに対してTSFが発生を防止すべき伝送誤りの種別を特定すべきである。選択肢は、暴露、改変、使用の損失である。

FDP_ITT.2　属性による転送分離

利用者のための適用上の注釈

このコンポーネントは、例えば、各種の取扱許可レベルを備えた情報にさまざまな形態の保護を提供する場合に使用することができる。

転送時のデータの分離を達成する方法の一つは、論理的または物理的な分離チャネルを使用することである。

操作

割付:

FDP_ITT.2.1において、PP/ST作成者は、転送される情報をカバーするアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。

選択:

FDP_ITT.2.1において、PP/ST作成者は、伝送中の利用者データに対してTSFが発生を防止すべき転送誤りの種別を特定すべきである。選択肢は、暴露、改変、使用の損失である。

割付:

FDP_ITT.2.2において、PP/ST作成者は、TOE内の物理的に分離されたパーツ間を送信されるデータを、いつ分離するかを決定するために使用する値であるセキュリティ属性を特定すべきである。一例は、ある所有者の識別情報に関連付けられた利用者データが、異なる所有者の識別情報に関連付けられた利用者データから分離して転送されるという場合である。この場合、そのデータの所有者の識別情報の値は、そのデータをいつ転送のために分離するかを決定するために使われるものとなる。

FDP_ITT.3　完全性監視

利用者のための適用上の注釈

このコンポーネントは、FDP_ITT.1あるいはFDP_ITT.2との組み合わせにおいて使用される。これは、TSFが、受信した利用者データ(及びその属性)を完全性に対してチェックすることを保証する。FDP_ITT.1あるいはFDP_ITT.2は、データが改変から保護されるような(FDP_ITT.3がどんな改変でも検出できるような)形でデータを提供する。

PP/ST作成者は、検出されねばならない誤りの種別を特定しなければならない。PP/ST作成者は、以下のものを考慮すべきである: データの改変、データの置換、データの回復不能な順序変更、データのリプレイ、不完全なデータ、その他の完全性誤り。

PP/ST作成者は、障害検出時にTSFがとるべきアクションを特定しなければならない。例: 利用者データを無視、データを再要求、許可管理者へ通知、他の回線へトラヒックを切り替え。

操作

割付:

FDP_ITT.3.1において、PP/ST作成者は、転送されかつ完全性誤りに対して監視される情報をカバーするアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。

FDP_ITT.3.1において、PP/ST作成者は、利用者データの転送において監視される、発生可能性のある完全性誤りの種別を特定すべきである。

FDP_ITT.3.2において、PP/ST作成者は、完全性誤りに遭遇したときにTSFがとるアクションを特定すべきである。一例は、TSFは利用者データの再発行を要求すべき、といったものである。FDP_ITT.3.1で特定したSFPは、TSFによってとられるアクションとして実施される。

FDP_ITT.4 属性に基づく完全性監視

このコンポーネントは、FDP_ITT.2との組み合わせで使用される。これは、TSFが受信した利用者データ、それは(特定されたセキュリティ属性に基づいて)分離されたチャネルで転送されたもの、の完全性をチェックすることを保証する。これは、PP/ST作成者が、完全性誤りの検出においてとられるアクションを特定することを認める。

例えば、このコンポーネントは、異なる完全性誤り検出と、異なる完全性レベルでの情報に対するアクションを提供するのに使用できる。

PP/ST作成者は、検出されねばならない誤りの種別を特定しなければならない。PP/ST作成者は、以下のものを考慮すべきである: データの改変、データの置換、データの回復不能な順序変更、データのリプレイ、不完全なデータ、その他の完全性誤り。

PP/ST作成者は、完全性誤り監視を必要とする属性 (及び関連する転送チャネル) を特定すべきである。

PP/ST作成者は、障害検出時にTSFがとるべきアクションを特定しなければならない。例: 利用者データを無視、データを再要求、許可管理者へ通知、他の回線へトラヒックを切り替え。

操作

割付:

FDP_ITT.4.1において、PP/ST作成者は、転送されかつ完全性誤りに対して監視される情報をカバーするアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。

FDP_ITT.4.1において、PP/ST作成者は、利用者データの転送において監視され

る、発生可能性のある完全性誤りの種別を特定すべきである。

FDP_ITT.4.1において、PP/ST作成者は、分離転送チャネルを必要とするセキュリティ属性のリストを特定すべきである。このリストは、セキュリティ属性と伝送チャネルに基づき、どの利用者データの完全性誤りを監視するのかを判断するために使用される。このエレメントは、FDP_ITT.2 属性による転送分離に直接関係する。

FDP_ITT.4.2において、PP/ST作成者は、完全性誤りに遭遇したときにTSFがとるアクションを特定すべきである。一例は、TSFは利用者データの再発行を要求すべき、といったものである。FDP_ITT.3.1で特定したSFPは、TSFによってとられるアクションとして実施される。

F.9　残存情報保護(FDP_RIP)

このファミリは、削除された情報が二度とアクセスされないこと、及び新しく作成したオブジェクトがTOE内で前に使用されたオブジェクトからの情報を含まないことに対応する。ただし、このファミリは、オフラインで格納されたオブジェクトには対応しない。

利用者のための注釈

このファミリは、論理的に削除または解放された情報(その利用者には利用できないが、システム内にまだ存在し、回復可能かもしれない)に対する保護を要求する。特に、これは、TSF再使用可能資源の一部としてオブジェクトに含まれ、オブジェクトの破棄が、必ずしも資源あるいは資源の内容の破棄と同一ではないような情報を含む。

また、これは、システム内の異なるサブジェクトによって順次再利用される資源にも適用される。例えば、ほとんどのオペレーティングシステムは、典型的に、システム内でのプロセスをサポートするハードウェアレジスタ(資源)に依存する。プロセスが「実行」状態から「スリープ」状態にスワップされるとき(またはその逆)、これらのレジスタは、異なるサブジェクトによって順次再利用される。この「スワップ」アクションは、資源の割当てあるいは解除とは考えられないかもしれないが、FDP_RIPは、このような事象及び資源に適用することもできる。

FDP_RIPは、典型的に、現時点で定義された、あるいはアクセス可能であるオブジェクトに含まれない情報に対するアクセスを制御する; しかし、これがあてはまらないこともある。例えば、オブジェクト「A」がファイルであり、オブジェクト「B」はファイルがその上にあるディスクとする。オブジェクト「A」を削除した場合、オブジェクト「A」内の情報が依然としてオブジェクト「B」の一部であるとしても、それは、FDP_RIPの制御下にある。

FDP_RIPは、オンラインオブジェクトにだけ適用され、テープにバックアップが採取されるようなオフラインオブジェクトには適用されないという点の注意が重要である。例えば、TOEの中でファイルを削除した場合、割当て解除において残存情報が存在しないことを要求するために、FDP_RIPを適用できる。しかし、TSFでは、オフラインバックアップ上に存在する同一ファイルにまでこの実施を拡張することができない。そのため、その同一ファイルは、利用可能な状態のままになる。これが問題になる場合、PP/ST作成者は、オフラインオブジェクトに対応するための管理ガイダンスをサポートするような、適切な環境の対策方針が正しくなされていることを確認すべきである。

アプリケーションがオブジェクトをTSFに解放した時点で(すなわち、割当ての解除において)、残存情報を消去することを要求するためにFDP_RIPが適用される場合、FDP_RIPとFDP_ROLで衝突が発生し得る。従って、ロールバックするための情報が存在しなくなるという理由で、FDP_RIPでの「割当て解除」の選択は、FDP_ROLと併用されるべきでない。他方の「割当てにおいて利用できなくすること」の選択は、FDP_ROLと併用されてもよいが、ロールバックが行われる前に、該当する情報を保持し

た資源が新しいオブジェクトに割当てられてしまうというリスクがある。それが発生するような場合は、ロールバックは可能でなくなる。

利用者が呼び出せる機能ではないため、FDP_RIPには監査要件がない。割当てや割当て解除される資源の監査は、アクセス制御SFPや情報フロー制御SFPの操作の一部として監査対象となる。

このファミリは、アクセス制御SFP(一つまたは複数)または情報フロー制御SFP(一つまたは複数)の中で特定されたオブジェクトに対して、PP/ST作成者によって特定されたように適用されるべきである。

FDP_RIP.1　部分残存情報保護

利用者のための適用上の注釈

このコンポーネントは、TOEにおけるオブジェクトのサブセットに対して、それらのオブジェクトに割当てられた、あるいはそれらのオブジェクトから割当て解除された資源中に、利用可能な残存情報が存在しないことをTSFが保証することを要求する。

操作

選択:

FDP_RIP.1.1において、PP/ST作成者は、残存情報保護機能を呼び出す事象、それへの資源の割当てあるいはそれからの資源の割当て解除を特定すべきである。

割付:

FDP_RIP.1.1において、PP/ST作成者は、残存情報保護を必要とするオブジェクトのリストを特定すべきである。

FDP_RIP.2　全残存情報保護

利用者のための適用上の注釈

このコンポーネントは、TOEにおける**すべてのオブジェクト**に対して、それらのオブジェクトに割当てられた、あるいはそれらのオブジェクトから割当て解除された資源中に、利用可能な残存情報が存在しないことをTSFが保証することを要求する。

操作

選択:

FDP_RIP.2.1において、PP/ST作成者は、残存情報保護機能を呼び出す事象、それへの資源の割当てあるいはそれからの資源の割当て解除を特定すべきである。

F.10　ロールバック(FDP_ROL)

このファミリは、明確に定義された有効な状態に戻るという必要性、ファイルに対する改変を元に戻す、あるいはデータベースの場合のように完了しなかった一連のトランザクションを元に戻すような利用者の必要性に対応する。

このファミリは、最後のアクションのセットを利用者が元に戻した後で、明確に定義された有効な状態に利用者が戻るのを、あるいは分散データベースにおいて、すべての分散したデータベースの複製を失敗した操作の前の状態に戻すのを補助することを意図している。

資源の割当てをオブジェクトから解除した時点での内容の利用不可をFDP_RIPが実施する場合、FDP_RIPとFDP_ROLが衝突する。従って、ロールバックするための情報が存在しなくなるという理由で、FDP_RIPはFDP_ROLと併用できない。資源をオブジェクトに割当てた時点での内容の利用不可をFDP_RIPが実施する場合だけ、FDP_RIPはFDP_ROLと併用できる。これは、操作のロールバックを成功させるために、FDP_ROLメカニズムは、TOE内にまだ残っているかもしれない以前の情報にアクセスできる可能性を持つからである。

ロールバック要件は、ある制限によって境界が決められる。例えば、テキストエディタでは、典型的に、決められた数までのコマンドのロールバックを認める。別の例はバックアップである。バックアップテープを順繰りに使用する場合、あるテープが再利用された後では、その情報はもはやアクセスできない。これもまた、ロールバック要件における境界を持つ。

FDP_ROL.1　基本ロールバック

利用者のための適用上の注釈

このコンポーネントは、利用者またはサブジェクトが、あらかじめ定義されたオブジェクトのセットに対する操作のセットを元に戻すことを認める。元に戻すのは、例えばある文字数までとか、ある時間制限までなど、ある制限内だけ可能である。

操作

割付:

FDP_ROL.1.1において、PP/ST作成者は、ロールバック操作の実行時に実施されるアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。これは、特定されたSFPを回避するのにロールバックが使用されないことを確実にするために必要である。

FDP_ROL.1.1において、PP/ST作成者は、ロールバックし得る操作のリストを特定すべきである。

FDP_ROL.1.1において、PP/ST作成者は、ロールバック方針の対象となるオブジェクトのリストを特定すべきである。

FDP_ROL.1.2において、PP/ST作成者は、ロールバック操作を実行し得る境界制限を特定すべきである。その境界は、例えば、過去2分間に実行された操作は元に戻せるなど、あらかじめ定義した期間として特定できる。他に、許される操作の最大数、あるいはバッファのサイズとして境界を定義することもできる。

FDP_ROL.2　高度ロールバック

利用者のための適用上の注釈

このコンポーネントは、すべての操作にロールバックする能力のTSFによる提供を実施する; しかしながら、利用者は、それらの一部にだけロールバックの選択ができる。

操作

割付:

FDP_ROL.2.1において、PP/ST作成者は、ロールバック操作の実行時に実施されるアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。これは、特定されたSFPを回避するのにロールバックが使用されないことを確実にするために必要である。

FDP_ROL.2.1において、PP/ST作成者は、ロールバック方針の対象となるオブジェクトのリストを特定すべきである。

FDP_ROL.2.2において、PP/ST作成者は、ロールバック操作を実行し得る境界制限を特定すべきである。その境界は、例えば、過去2分間に実行された操作は元に戻せるなど、あらかじめ定義した期間として特定できる。他に、許される操作の最大数、あるいはバッファのサイズとして境界を定義することもできる。

F.11　蓄積データ完全性(FDP_SDI)

このファミリでは、TSC内に格納されている間の利用者データの保護に対応する要件を提供する。

利用者のための注釈

ハードウェアの不調や誤りがメモリに格納されたデータに影響を与えるかもしれない。このファミリでは、これら意図しない誤りを検出するための要件を提供する。TSC内の格納装置に格納されている間の利用者データの完全性も、このファミリで対応される。

サブジェクトがデータを改変するのを防ぐためには、(このファミリよりも、)FDP_IFFあるいはFDP_ACFファミリが要求される。

このファミリは、TOE内で転送される間の完全性誤りから利用者データを保護するFDP_ITT TOE内転送とは異なるものである。

FDP_SDI.1　蓄積データ完全性監視

利用者のための適用上の注釈

このコンポーネントは、完全性誤りに対して、媒体に格納されたデータを監視する。PP/ST作成者は、監視の基礎として使われる、異なる種類の利用者データ属性を特定できる。

操作

割付:

FDP_SDI.1.1において、PP/ST作成者は、TSFが検出する完全性誤りを特定すべきである。

FDP_SDI.1.1において、PP/ST作成者は、監視のためのの基礎として使われる利用者データ属性を特定すべきである。

FDP_SDI.2　蓄積データ完全性監視及びアクション

利用者のための適用上の注釈

このコンポーネントは、完全性誤りに対して、媒体に格納されたデータを監視する。PP/ST作成者は、完全性誤りが検出された場合にどのアクションがとられるべきかを特定できる。

操作

割付:

FDP_SDI.1.1において、PP/ST作成者は、TSFが検出する完全性誤りを特定すべきである。

FDP_SDI.1.1において、PP/ST作成者は、監視のためのの基礎として使われる利用者データ属性を特定すべきである。

FDP_SDI.2.2において、PP/ST作成者は、完全性誤りが検出された場合にとられるべきアクションを特定すべきである。

F.12　TSF**間利用者データ機密転送保護**(FDP_UCT)

このファミリは、TOEと別の高信頼IT製品の間で外部チャネルを使って利用者データを転送するときに、その機密性を保証するための要件を定義する。機密性は、二つの端点間の通過における、利用者データの許可されない暴露を防止することによって実施される。端点は、TSFあるいは利用者であってよい。

利用者のための注釈

このファミリは、通過中の利用者データの保護に対する要件を提供する。それに対して、FTP_ITCはTSFデータを扱う。

FDP_UCT.1　**基本データ交換機密性**

利用者のための適用上の注釈

TSFは、交換される利用者データ暴露から保護する能力を持つ。

操作

割付:

FDP_UCT.1.1において、PP/ST作成者は、利用者データの交換時に実施されるアクセス制御SFP(一つまたは複数)及び/または情報フロー制御SFP(一つまたは複数)を特定すべきである。特定された方針は、誰がデータを交換でき、どのデータが交換され得るかについて判断するために実施される。

選択:

FDP_UCT.1.1において、PP/ST作成者は、利用者データを送信あるいは受信するメカニズムにこのエレメントを適用するかどうかを特定すべきである。

F.13　TSF間利用者データ完全性転送保護(FDP_UIT)

このファミリは、TSFと他の高信頼IT製品間の通過において利用者データに完全性を提供し、かつ検出可能な誤りから回復するための要件を定義する。最低限、このファミリは、改変に対する利用者データの完全性を監視する。さらに、このファミリは、検出された完全性誤りを訂正するためのさまざまな方法をサポートする。

利用者のための注釈

このファミリは、通過に際しての利用者データの完全性を提供するための要件を定義する; 一方、FPT_ITIはTSFデータを扱う。

FDP_UCTは利用者データの機密性に対応するので、FDP_UITとFDP_UCTは、互いに対をなす。従って、FDP_UITを実現するのと同じメカニズムが、FDP_UCTやFDP_ITCのような他のファミリの実現に使える可能性がある。

FDP_UIT.1　データ交換完全性

利用者のための適用上の注釈

TSFは基本的に、利用者データに対する改変を検出できるようなやり方で、利用者データを送信または受信する基本能力を持つ。改変からの回復を試みるようなTSFメカニズムに対する要件はない。

操作

割付:

FDP_UIT.1.1において、PP/ST作成者は、送信データまたは受信データに対して実施されるアクセス制御SFP(一つまたは複数)や情報フロー制御SFP(一つまたは複数)を特定すべきである。特定された方針は、誰がデータを送信あるいは受信でき、どのデータが送信あるいは受信され得るかについて判断するために実施される。

選択:

FDP_UIT.1.1において、PP/ST作成者は、オブジェクトを送信または受信するTSFにこのエレメントを適用するかどうかを特定すべきである。

FDP_UIT.1.1において、PP/ST作成者は、データが改変、削除、挿入、あるいはリプレイから保護されるべきかどうかを特定すべきである。

FDP_UIT.1.2において、PP/ST作成者は、改変、削除、挿入、あるいはリプレイの種別の誤りが検出されるかどうかを特定すべきである。

FDP_UIT.2　**発信側データ交換回復**

利用者のための適用上の注釈

このコンポーネントは、もし必要ならば、他の高信頼IT製品の助けを借りて、識別された伝送誤りのセットから回復する能力を提供する。他の高信頼IT製品はTSCの外部にあので、TSFはそのふるまいを制御できない。しかしながら、回復の目的のために他の高信頼IT製品と協働する能力を提供できる。例えば、誤りが検出された場合に、TSFは、発信源の高信頼IT製品がそのデータを再送することに依存する機能を持てるであろう。このコンポーネントは、そのような誤り回復に対処するためのTSFの能力を扱う。

操作

割付:

FDP_UIT.2.1において、PP/ST作成者は、利用者データの回復時に実施するアクセス制御SFP(一つまたは複数)や情報フロー制御SFP(一つまたは複数)を特定すべきである。特定した方針は、どのデータが回復され得るか、どのようにして回復され得るかを決定するために実施される。

FDP_UIT.2.1において、PP/ST作成者は、発信源の高信頼IT製品の助けを借りて、TSFが元の利用者データを回復できる完全性誤りのリストを特定すべきである。

FDP_UIT.3　**着信側データ交換回復**

利用者のための適用上の注釈

このコンポーネントは、識別された伝送誤りのセットから回復するための能力を提供する。このタスクは、発信源の高信頼IT製品の助けを借りずになされる。例えば、ある程度の誤りが検出される場合、伝送プロトコルは、そのプロトコル内で利用可能なチェックサムとその他の情報に基づき、TSFがその誤りから回復するのを許すのに十分なほど強固でなければならない。

操作

割付:

FDP_UIT.3.1において、PP/ST作成者は、利用者データの回復時に実施するアクセス制御SFP(一つまたは複数)や情報フロー制御SFP(一つまたは複数)を特定すべきである。特定した方針は、どのデータが回復され得るか、どのようにして回復され得るかを決定するために実施される。

FDP_UIT.3.1において、PP/ST作成者は、**受信側**TSFが、**単独で**元の利用者データを回復できる完全性誤りのリストを特定すべきである。

附属書G

(参考)

識別と認証(FIA)

一般のセキュリティ要件は、TOEにおける機能を実行する人間やエンティティをあいまいさなく識別することになっている。これは、各利用者が主張する識別情報の立証だけでなく、各利用者が、本当に当人がそう主張している者かの検証も必要とする。これは、利用者当人に関連付けられているものとしてTSFが認識している情報をTSFに提供することを利用者に要求することによって達成される。

このクラスのファミリでは、主張された利用者識別情報の立証と検証を行うための機能の要件に対応する。「識別と認証」は、適切なセキュリティ属性(識別情報、グループ、役割、セキュリティあるいは完全性レベルなど)に利用者が関連付けられていることを保証するために要求される。

許可利用者のあいまいさのない識別、及びセキュリティ属性の利用者及びサブジェクトとの正確な関連付けは、セキュリティ方針の実施のためにきわめて重要である。

FIA_UIDファミリは、利用者の識別情報の判断に対応する。

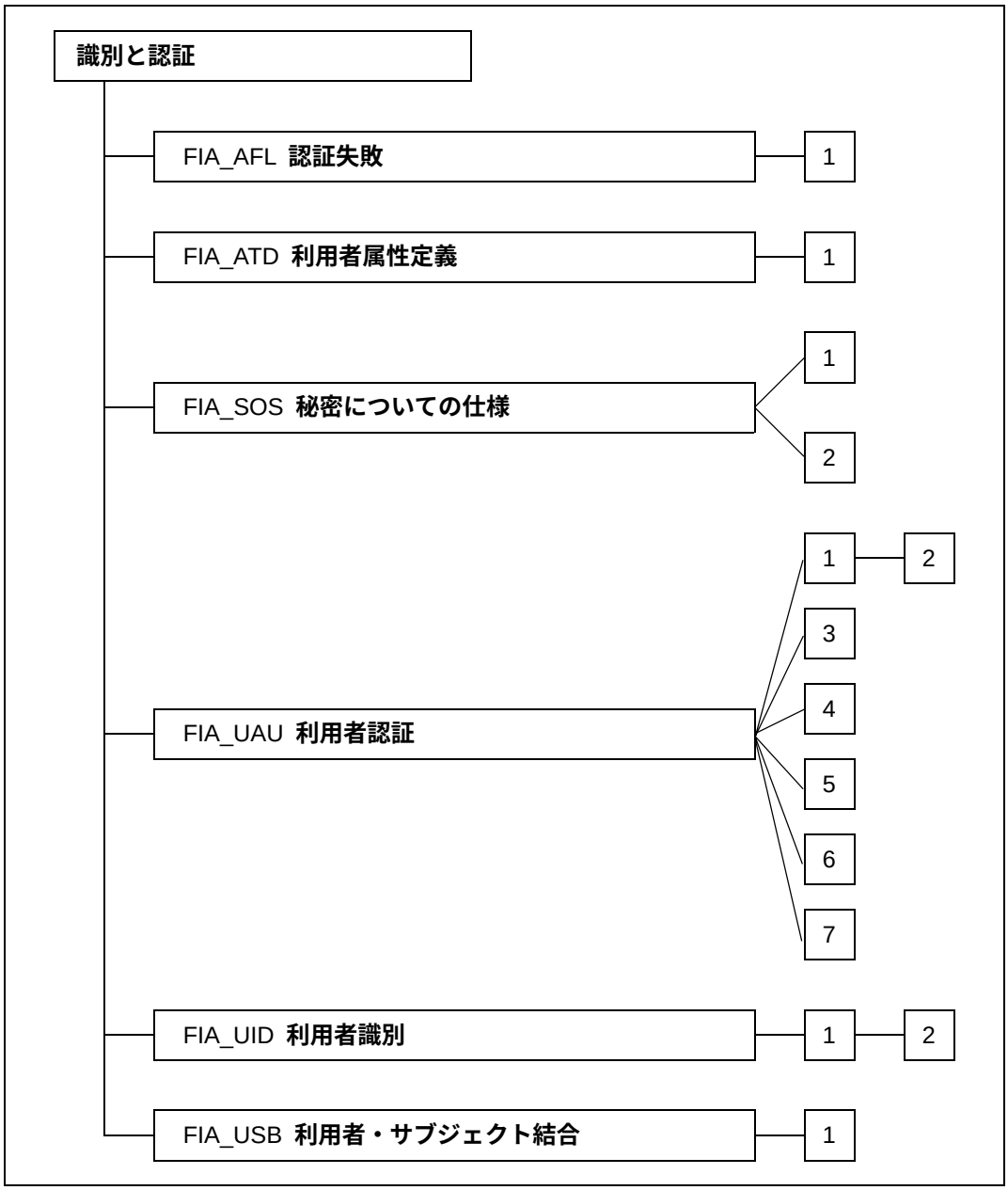
FIA_UAUファミリは、利用者の識別情報の検証に対応する。

FIA_AFLファミリは、不成功認証試行の繰返しにおける制限の定義に対応する。

FIA_ATDファミリは、TSPの実施時に使用する利用者属性の定義に対応する。

FIA_USBファミリは、各許可利用者に対するセキュリティ属性の正しい関連付けに対応する。

FIA_SOSファミリは、定義された尺度を満たすような秘密の生成及び検証に対応する。



図G.1 - 識別と認証クラスのコンポーネント構成

G.1 認証失敗(FIA_AFL)

このファミリは、認証の試行に関する値、及び認証の試行が失敗した場合のTSFアクションの定義についての要件に対応する。パラメタは、試行回数及び時間のしきい値を含むが、それに限定されない。

セション確立プロセスは、実際の実装とは独立した、セション確立を実行するための利用者との対話である。不成功認証試行回数が指定のしきい値を超えると、利用者アカウントあるいは端末(あるいは両方)がロックされる。利用者アカウントが非活性化されると、その利用者はシステムにログオンできない。端末が非活性化されると、その端末(あるいはその端末のアドレス)はどのようなログオンにも使用できない。これらの状況はどちらも、再確立のための条件が満たされるまで続く。

FIA_AFL.1 認証失敗時の取り扱い

利用者のための適用上の注釈

PP/ST作成者は、不成功認証試行回数を定義することができ、あるいはその回数の定義をTOE開発者または許可利用者に任せることを選択できる。不成功認証試行は連続したものである必要はないが、一つの認証事象に関係したものである。そのような認証事象は、ある端末について最後に成功したセション確立からのカウントなどが該当しよう。

PP/ST作成者は、認証に失敗した際にTSFがとらねばならないアクションのリストを特定できる。また、PP/ST作成者が適切と思えば、許可管理者に事象の管理を認めることもできる。これに該当するアクションとしては、端末非活性化、利用者アカウント非活性化、管理者警報などがある。状況を通常状態に戻すべき条件は、そのアクションにおいて特定されなければならない。

サービス拒否を防ぐため、TOEは通常、非活性化できない少なくとも一つの利用者アカウントが存在することを保証する。

PP/ST作成者は、利用者セション確立プロセスを再活性化したり、管理者に警報を送ったりする規則を含め、TSFに対するアクションを詳しく述べることができる。これらのアクションの例: 特定した時間が経過するまで、許可管理者が端末/アカウントを再活性化するまで、失敗した以前の試行に関係する時間(試行に失敗するたびに、非活性化時間を倍にする)。

操作

割付:

FIA_AFL.1.1において、PP/ST作成者は*、事象のきっかけとなる不成功認証試行回数のデフォルト値(満たすか超えたとき)を特定すべきである。PP/ST作成者は、その数を「許可管理者が設定可能な数」と特定することができる。 *(*: 原*

文では "if PP/ST author should specify ..." となっているが、 "if" は誤記と思われる。)

FIA_AFL.1.1において、PP/ST作成者は、認証事象を特定すべきである。これらの認証事象の例: 指定された利用者識別情報に対して、最後の成功した認証以降の不成功認証試行回数、現在の端末に対して、最後の成功した認証以降の不成功認証試行回数、直前の10分間における不成功認証試行回数。少なくとも一つの認証事象が特定されなければならない。

FIA_AFL.1.2において、PP/ST作成者は、しきい値に到達するかあるいは超えた場合にとられるアクションを特定すべきである。これらのアクションは、アカウントを5分間無効にする、端末の非活性化を徐々に長くする(2の不成功試行回数乗の秒数)、あるいは管理者がロックを解除するまでアカウントを非活性化し、同時に管理者に通知するなどがある。アクションは、尺度、及び適用可能な場合はその尺度の存続時間(あるいはその尺度が終了される条件)を特定すべきである。

G.2　利用者属性定義(FIA_ATD)

すべての許可利用者は、その利用者の識別情報以外に、TSPを実施するのに使用されるセキュリティ属性のセットを持つことができる。このファミリは、TSPをサポートするために必要なとき、利用者のセキュリティ属性と利用者を関連付けるための要件を定義する。

利用者のための注釈

個々のセキュリティ方針定義は依存性を持つ。これらの個々の定義は、方針の実施に必要となる属性をリストしたものを含むべきである。

FIA_ATD.1　利用者属性定義

利用者のための適用上の注釈

このコンポーネントは、利用者のレベルに対して維持すべきセキュリティ属性を特定する。これは、リストされたセキュリティ属性は利用者のレベルに割り付けられ、かつ変更可能であることを意味する。言い換えれば、利用者に関連付けられたリストにおけるセキュリティ属性を変更することは、他のすべての利用者のセキュリティ属性への影響を持つべきではない。

セキュリティ属性(グループに対する能力リストなど)が利用者のグループに属する場合、利用者は、対応するグループへの参照(セキュリティ属性として)を持つ必要があろう。

操作

割付:

FIA_ATD.1.1において、PP/ST作成者は、個々の利用者に関連付けられるセキュリティ属性を特定すべきである。そのようなリストの例は、{「取扱許可」、「グループ識別子」、「権限」}などである。

G.3　機密についての仕様(FIA_SOS)

このファミリは、提供された秘密に対して定義された品質尺度を実施する、及び定義された尺度を満たす秘密を生成するメカニズムに対する要件を定義する。このようなメカニズムの例には、利用者が作るパスワードの自動的チェック、あるいは自動化されたパスワード生成などがある。

秘密は、TOEの外部で生成できる(例えば、利用者によって選択され、システムに導入される)。そのような場合、FIA_SOS.1コンポーネントは、外部で生成した秘密が、ある標準、例えば、最小サイズ、辞書に載っていない、及び/または以前に使われていない、に沿っていることを保証するために使用できる。

秘密は、TOEによって生成することもできる。そのような場合、FIA_SOS.2コンポーネントは、その秘密が何らかの特定された尺度に沿うことを保証することをTOEに要求できる。

利用者のための注釈

秘密には、利用者が所持する知識に基づく認証メカニズムのために利用者が提供する認証データが含まれる。暗号鍵が用いられる場合は、このファミリの代わりに、FCSクラスが使用されるべきである。

FIA_SOS.1　**秘密の検証**

利用者のための適用上の注釈

秘密は、利用者が生成できる。このコンポーネントは、利用者が生成した秘密が、ある品質尺度を満たすことが検証できることを保証する。

操作

割付:

FIA_SOS.1.1において、PP/ST作成者は、定義された品質尺度を提供すべきである。品質尺度仕様は、実行されるべき品質チェックの記述といった単純なものでよく、あるいは、秘密が満たさねばならない品質尺度を定義した、政府公表の標準の参照といった公式のものでもよい。品質尺度の例は、容認できる秘密の英数字構造の記述、及び/または容認できる秘密が満たさねばならない空間サイズである。

FIA_SOS.2　TSF**秘密生成**

このコンポーネントは、パスワードを用いる認証のような特定の機能に対して、TSFが秘密を生成することを認める。

利用者のための適用上の注釈

疑似乱数ジェネレータが秘密生成アルゴリズムで使用される場合、高度の予測不可性を持つ出力を提供するランダムデータを入力として受け入れるべきである。このランダムデータ(種)は、システムクロック、システムレジスタ、日付、時刻など多数の利用可能なパラメタから発生させられる。これらの入力から生成される一意な種の数が、少なくとも、生成せねばならない秘密の最小個数に等しいことを保証するように、パラメタの選択が行わねばならない。

操作

割付:

FIA_SOS.2.1において、PP/ST作成者は、定義された品質尺度を提供すべきである。品質尺度仕様は、実行されるべき品質チェックの記述といった単純なものでよく、あるいは、秘密が満たさねばならない品質尺度を定義した、政府公表の標準の参照といった公式のものでもよい。品質尺度の例は、受容できる秘密の英数字構造の記述、及び/または受容できる秘密が満たさねばならない空間サイズである。

FIA_SOS.2.2において、PP/ST作成者は、TSF生成の秘密が使われねばならないTSF機能のリストを提供すべきである。そのような機能の例に、パスワードに基づく認証メカニズムがある。

G.4　利用者認証(FIA_UAU)

このファミリは、TSFがサポートする利用者認証メカニズムの種別を定義する。このファミリは、利用者認証メカニズムが基づかねばならない、要求された属性を定義する。

FIA_UAU.1　認証のタイミング

利用者のための適用上の注釈

このコンポーネントは、利用者の主張する識別情報が認証される前に、利用者を代行してTSFによって実行されることのできるTSF調停アクションをPP/ST作成者が定義することを要求する。TSF調停アクションは、認証される前に利用者が自分自身を不正確に識別することに対しては、セキュリティ上の懸念を持つべきでない。リストにないすべての他のTSF調停アクションに対し、TSFが利用者を代行してそのアクションを実行できるようになる前に利用者は認証されねばならない。

このコンポーネントは、そのアクションが、識別が行われる前に実行され得るかどうかを制御することはできない。それには、適切な割付を施したFIA_UID.1及びFIA_UID.2のどちらかの使用が必要である。

操作

割付:

FIA_UAU.1.1において、PP/ST作成者は、利用者の主張する識別情報が認証される前に、利用者を代行してTSFによって実行されることのできるTSF調停アクションのリストを特定すべきである。このリストを空とすることはできない。適切なアクションが存在しない場合は、コンポーネントFIA_UAU.2が代わりに使用されるべきである。そのようなアクションの例には、ログイン手続きにおけるヘルプの要求などがある。

FIA_UAU.2　アクション前の利用者認証

利用者のための適用上の注釈

このコンポーネントは、すべてのTSF調停アクションが利用者を代行して行われるようになる前に、その利用者が識別されることを要求する。

FIA_UAU.3　偽造されない認証

利用者のための適用上の注釈

このコンポーネントは、認証データの保護を提供するメカニズムに対する要件に対応する。

他の利用者から複製された、あるいは何らかの方法で組み立てられた認証データは、検出されるべき、及び/または拒否されるべきである。これらのメカニズムは、TSFによって認証された利用者が、実際に彼らがそう主張する者であることの信用性を提供する。

このコンポーネントは、共有不能な認証データ(生物的尺度など)に基づく認証メカニズムと一緒の場合だけに有用かもしれない。TSFは、TSFの制御外でのパスワードの共有を検出したり防止したりすることは不可能である。

操作

選択:

FIA_UAU.3.1において、PP/ST作成者は、TSFが、認証データが偽造されたことを検出する、防止する、あるいは検出及び防止する、のいずれかを特定すべきである。

FIA_UAU.3.2において、PP/ST作成者は、TSFが、認証データが複製されたことを検出する、防止する、あるいは検出及び防止する、のいずれかを特定すべきである。

FIA_UAU.4　単一使用認証メカニズム

利用者のための適用上の注釈

このコンポーネントは、単一使用認証データに基づく認証メカニズムに対する要件に対応する。単一使用認証データとは、利用者が持つかあるいは知っているものとすることができるが、利用者自身についてのものであってはならない。単一使用認証データの例として、単一使用パスワード、暗号化されたタイムスタンプ、及び/または秘密のルックアップテーブルからの乱数などがある。

PP/ST作成者は、この要件が適用される認証メカニズム(一つまたは複数)を特定できる。

操作

割付:

FIA_UAU.4.1において、PP/ST作成者は、この要件が適用される認証メカニズムのリストを特定すべきである。この割付は、「すべての認証メカニズム」とすることができる。この割付の一例は、「外部ネットワーク上の人を認証するために用いられる認証メカニズム」である。

FIA_UAU.5　複数の認証メカニズム

利用者のための適用上の注釈

このコンポーネントを使用すれば、TOE内で使用される複数の認証メカニズムに対する

要件の特定ができる。各々の個別のメカニズムに対して、各メカニズムに適用するために、FIAクラスから適用すべき要件が選択されねばならない。認証メカニズムのさまざまな用途に対するさまざまな要件を反映するために、同一のコンポーネントを複数回選択することが可能である。

FMTクラス中の管理機能は、認証が成功したかどうかを判断する規則に加え、認証メカニズムのセットに対する維持能力を提供できる。

システム上に匿名利用者を認めるために、「なし」認証メカニズムを併用できる。そのようなアクセスの使用は、FIA_UAU.5.2の規則で明確に説明されるべきである。

操作

割付:

FIA_UAU.5.1において、PP/ST作成者は、利用可能な認証メカニズムを特定すべきである。そのようなリストの一例は、「なし、パスワードメカニズム、生物的尺度(網膜スキャン)、S/鍵メカニズム」である。

FIA_UAU.5.2において、PP/ST作成者は、認証メカニズムがどのように認証を提供するか、いつ使われるかを記述する規則を特定すべきである。これは、各状況に対して、利用者を認証するために使われるメカニズムのセットが記述されねばならないことを意味している。そのような規則のリストの一例: 「利用者が格別の特権を有していれば、パスワードメカニズム及び生物的尺度メカニズムの両方が使用されねばならず、両方が成功した場合だけ成功となる; その他すべての利用者に対しては、パスワードメカニズムが使用されねばならない。」

PP/ST作成者は、許可管理者が特定の規則を定めることができる境界を与えることができる。規則の一例: 「利用者は常にトークンを用いて認証されねばならない; 管理者は、併用されねばならない付加認証メカニズムを特定できる。」PP/ST作成者は、どの境界も特定せず、認証メカニズムとその規則を完全に許可管理者に委ねてもかまわない。

FIA_UAU.6　**再認証**

利用者のための適用上の注釈

このコンポーネントは、定義された時点における利用者の再認証の潜在的な必要性に対応する。これらは、再認証に対する非TSFエンティティからの要求(例えば、サービス提供先のクライアントの再認証をTSFに要求するサーバアプリケーション)だけでなく、利用者がTSFに対してセキュリティに関連するアクションの実行を要求することを含められる。

操作

割付:

FIA_UAU.6.1において、PP/ST作成者は、再認証を要求する条件のリストを特定すべきである。このリストには、特定された利用者非アクティブ状態経過期間、アクティブなセキュリティ属性の利用者変更要求、あるいはセキュリティ上重要な機能をTSFが実行することの利用者要求などが含まれる。

PP/ST作成者は、再認証が行われるべき、及び詳細が許可管理者に委ねられるべき境界を与えることができる。そのような規則の一例: 「利用者は常に少なくとも1日に1回再認証されねばならない; 管理者は、10分ごとに1回を超えない範囲で、再認証をより多く行うべきと特定できる。」

FIA_UAU.7　保護された認証フィードバック

利用者のための適用上の注釈

このコンポーネントは、利用者に提供される認証プロセスにおけるフィードバックに対応する。あるシステムでは、フィードバックは何文字がタイプされたかを示しても文字自体は示さないように構成され、別のシステムでは、その情報すら不適切かもしれない。

このコンポーネントは、認証データがそのまま利用者に返されないことを要求する。ワークステーションの環境では、各パスワードの文字ごとに、元の文字ではなく、「ダミー」(例えばスター)を表示することができる。

操作

割付:

FIA_UAU.7.1において、PP/ST作成者は、利用者に提供される、認証プロセスに関連したフィードバックを特定すべきである。フィードバックの割付の一例は、「タイプされた文字の個数」。フィードバックの他の種別として、「認証に失敗した認証メカニズム」。

G.5　利用者識別(FIA_UID)

このファミリは、利用者が、TSFに調停され、かつ利用者識別を要求するすべての他のアクションを実行する前に、自分自身を識別することが要求される条件を定義する。

FIA_UID.1　識別のタイミング

利用者のための適用上の注釈

このコンポーネントは、利用者が識別されるときの要件を述べる。PP/ST作成者は、識別が行われる前に実行可能な特定のアクションを示すことができる。

FIA_UID.1を使用する場合、FIA_UID.1で言及されたTSF調停アクションは、FIA_UAU.1にも現れるべきである。

操作

割付:

FIA_UID.1.1において、PP/ST作成者は、利用者が自分自身を識別しなければならない前に、利用者を代行してTSFによって実行できるTSF調停アクションのリストを特定すべきである。このリストを空とすることはできない。適切なアクションがない場合は、代わりにコンポーネントFIA_UID.2が使用されるべきである。そのようなアクションの一例は、ログイン手続きにおけるヘルプの要求である。

FIA_UID.2　アクション前の利用者識別

利用者のための適用上の注釈

このコンポーネントにおいて利用者が識別される。利用者は、識別される前は、すべてのアクションの実行をTSFから許可されない。

G.6　利用者・サブジェクト結合(FIA_USB)

認証された利用者は、TOEを使用するため、典型的にサブジェクトを活性化する。利用者のセキュリティ属性は、(全体または一部が)このサブジェクトに関連付けられる。このファミリは、利用者のセキュリティ属性とその利用者を代行して動作するサブジェクトとの関連付けを作成し、維持する要件を定義する。

FIA_USB.1　利用者サブジェクトの結合

利用者のための適用上の注釈

「を代行して動作する」という語句は、以前の基準において論争点であったことが判明している。これは、あるタスクを実行するためにあるサブジェクトを存在せしめるようにした、あるいは活性化されるようにした利用者を代行してそのサブジェクトが動作する、ということを意図したものである。そのため、サブジェクトが生成されたとき、そのサブジェクトは、その生成を起動した利用者を代行して動作する。匿名性が使われる場合、サブジェクトはそれでも利用者を代行して動作するが、利用者の識別情報は知られない。特殊なカテゴリは、複数の利用者にサービスするサブジェクト(例えばサーバプロセス)である。そのような場合、そのサブジェクトを生成した利用者が「所有者」と見なされる。

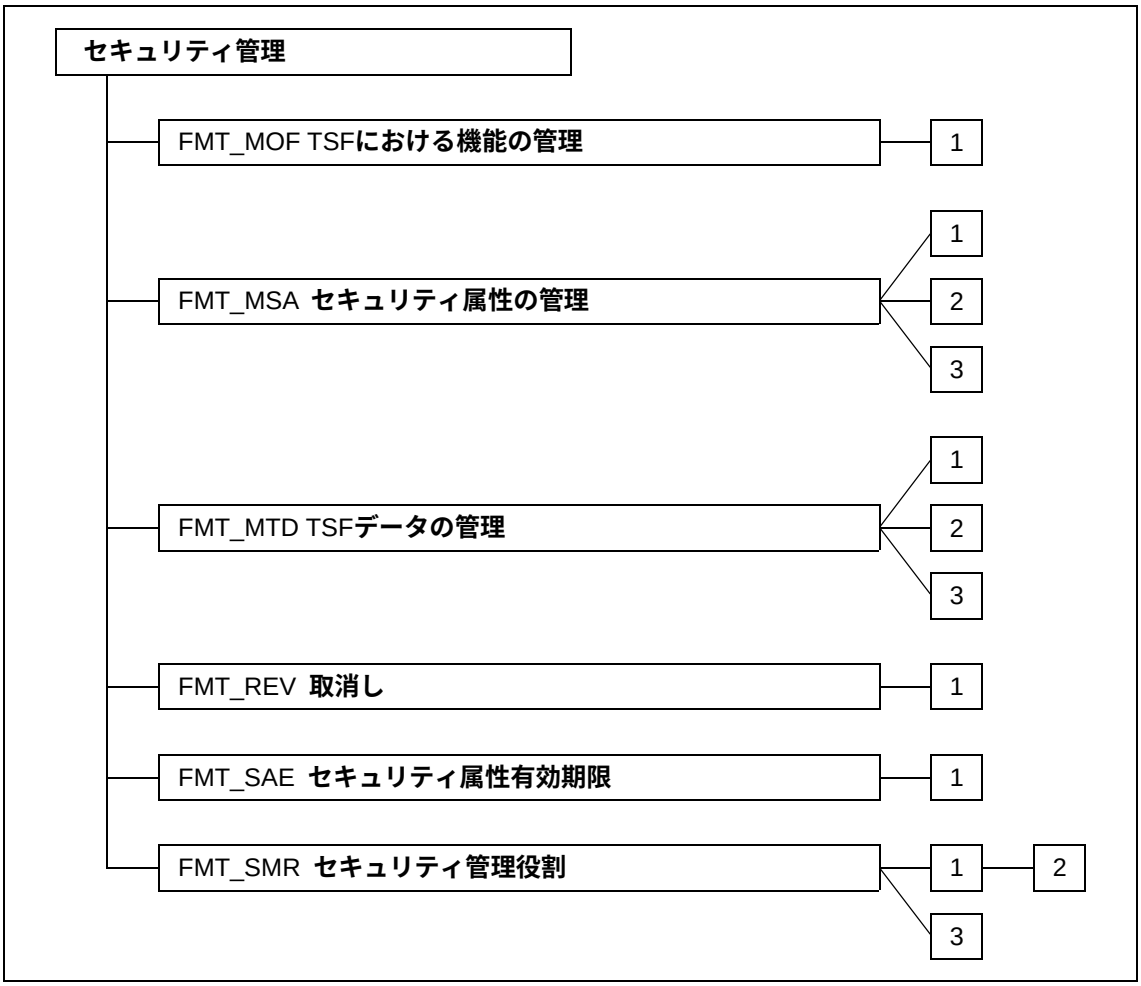
附属書H

(参考)

セキュリティ管理(FMT)

このクラスは、TSFのいくつかの側面の管理を特定する: セキュリティ属性、TSFデータ、及びTSFにおける機能。能力の分離など、さまざまな管理役割及びそれらの相互作用も特定できる。

分散システムを形成する物理的に分離された複数のパートでTOEが構成される環境では、セキュリティ属性・TSFデータ・機能修正の伝搬に関するタイミングの問題が非常に複雑になり、とりわけ、TOEのパート間で情報が複製される必要のある場合はそうである。FMT_REV.1 取消しやFMT_SAE.1 時間付き許可のようなコンポーネントを選択する場合、ふるまいが阻害される恐れがあるところでは、このようなことが熟慮されるべきである。このような状況では、FPT_TRCからのコンポーネントを使うのが当を得ている。



図H.1 - **セキュリティ管理クラスのコンポーネント構成**

H.1　TSFにおける機能の管理(FMT_MOF)

TSFの管理機能は、許可利用者に、TOEのセキュアな操作のセットアップと制御を可能にする。これらの管理機能は典型的に、多くの異なるカテゴリに入れられる。

a) TOEが実施するアクセス制御、アカウント及び認証制御に関係する管理機能。例えば、利用者セキュリティ特性(利用者名に関連付けられた一意な識別子、利用者アカウント、システム入力パラメタなど)の定義と更新、あるいは監査システム制御(監査事象の選択、監査証跡の管理、監査証跡分析、及び監査報告生成など)の定義と更新、利用者ごとの方針属性(取扱許可など)の定義と更新、既知のシステムアクセス制御ラベルの定義、及び利用者グループの制御と管理など。

b) 可用性の制御に関する管理機能。例えば、可用性パラメタや資源割当ての定義及び更新。

c) 設置及び設定全般に関する管理機能。例えば、TOE設定、手動回復、TOEセキュリティフィックスの設置(もしあれば)、ハードウェアの修復及び再設置など。

d) TOE資源の日常的な制御及び維持に関する管理機能。例えば、周辺装置の活性化/不活性化、リムーバブル格納媒体のマウント、利用者及びシステムオブジェクトのバックアップ及び回復など。

これらの機能は、PPまたはSTに含まれるファミリに基づいて、TOE中に存在する必要があることに注意。セキュアなやり方でシステムを管理するために適切な機能が提供されことを保証するのは、PP/ST作成者の責任である。

TSFに、管理者が制御できる機能を含められる。例えば、監査機能をスイッチオフでき、時間同期を切り替え可能にでき、及び/または認証メカニズムを修正可能にすることができる。

FMT_MOF.1　セキュリティ機能のふるまいの管理

このコンポーネントは、識別された役割にTSFのセキュリティ機能の管理を認める。これは、セキュリティ機能の現在のステータスの取得、セキュリティ機能の非活性化/活性化、あるいはセキュリティ機能のふるまいの修正を伴うかもしれない。セキュリティ機能のふるまい修正例には、認証メカニズムの変更がある。

操作

選択:

FMT_MOF.1.1において、PP/ST作成者は、セキュリティ機能に対する非活性化、

活性化、及び/またはふるまいの修正を行うことを、役割が決定できるかどうかを選択すべきである。

割付:

FMT_MOF.1.1において、PP/ST作成者は、識別された役割が修正することのできる機能を特定すべきである。例として、監査及び時間決定などがある。

FMT_MOF.1.1において、PP/ST作成者は、TSFにおける機能の修正が許される役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

H.2　セキュリティ属性の管理(FMT_MSA)

このファミリは、セキュリティ属性の管理における要件を定義する。

利用者、サブジェクト、及びオブジェクトは、TSFのふるまいに影響を与えるセキュリティ属性に関連付けられる。そのようなセキュリティ属性の例としては、利用者が所属するグループ、彼/彼女に想定される役割、プロセス(サブジェクト)の優先度、役割または利用者に属する権限などがある。これらのセキュリティ属性は、利用者、サブジェクト、あるいは特定の許可利用者(この管理に対する権限が明示的に付与された利用者)によって管理される必要があるかもしれない。

利用者に権限を割り付ける権限は、それ自体がセキュリティ属性であり、及び/または潜在的にFMT_MSA.1による管理の対象になるということに注意が要る。

FMT_MSA.2は、セキュリティ属性の妥当とみなされるすべての組み合わせがセキュアな状態の範囲内にあることを保証するのに使用できる。「セキュア」が何を意味するかの定義は、TOEガイダンス及びTSPモデルに委ねられている。セキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を開発者が提供すれば、FMT_MSA.2のADV_SPM.1への依存性が論証される。

実際の例では、サブジェクト、オブジェクト、あるいはは利用者アカウントが作成されることがある。関連するセキュリティ属性に対して明示的な値がない場合、デフォルト値を使用する必要がある。FMT_MSA.1は、これらデフォルト値が管理できることを特定するために使える。

FMT_MSA.1　セキュリティ属性の管理

このコンポーネントは、ある役割を果たしている利用者に、識別されたセキュリティ属性を管理することを認める。利用者は、コンポーネントFMT_SMR.1内で役割が割り付けられる。

パラメタのデフォルト値は、パラメタが特定の値を割り付けられずに具現化されたときに取る値である。パラメタの具現化(作成)時に初期値が与えられ、デフォルト値を上書きする。

操作

割付:

FMT_MSA.1.1において、PP/ST作成者は、そのセキュリティ属性が適用可能なアクセス制御SFPまたは情報フロー制御SFPをリストすべきである。

選択:

FMT_MSA.1.1において、PP/ST作成者は、識別されたセキュリティ属性に適用

することのできる操作を特定すべきである。PP/ST作成者は、その役割が、デフォルト変更、問合せ、セキュリティ属性の修正、セキュリティ属性の全削除、あるいはそれら自体の操作の定義を行えることを特定できる。

割付:

FMT_MSA.1.1において、もし選択されれば、PP/ST作成者は、その役割が、他のどの操作を実行できるかを特定すべきである。そのような操作の一例は、「作成する」である。

FMT_MSA.1.1において、PP/ST作成者は、識別された役割よって操作され得るセキュリティ属性を特定すべきである。PP/ST作成者は、デフォルトアクセス権のようなデフォルト値が管理され得ることを特定することが可能である。これらセキュリティ属性の例としては、利用者の取扱許可、サービスの優先度、アクセス制御リスト、デフォルトアクセス権などがある。

FMT_MSA.1.1において、PP/ST作成者は、そのセキュリティ属性において操作が許される役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

FMT_MSA.2　セキュアなセキュリティ属性

このコンポーネントは、セキュリティ属性に割り付けることのできる値の要件を含む。割り付けられる値は、TOEがセキュアな状態を保持するようなものであるべきである。

「セキュア」が何を意味するかの定義は、このコンポーネントでは回答されず、TOEの開発(特に、ADV_SPM.1 非形式的TOEセキュリティ方針モデル)、及びその結果としてのガイダンスの情報に委ねられる。一例をあげれば、利用者アカウントを作成する場合はありふれたものでないパスワードを持つべきである、のようになる。

FMT_MSA.3　静的属性初期化

利用者のための適用上の注釈

このコンポーネントは、TSFが、関連するオブジェクトのセキュリティ属性にデフォルト値を提供することを要求し、それは、初期値によって上書きされることができる。もし生成時に許可を特定できるメカニズムが存在するならば、新しいオブジェクトに対して、作成時にさまざまなセキュリティ属性を持たせることも可能にできる。

操作

割付:

FMT_MSA.3.1において、PP/ST作成者は、そのセキュリティ属性が適用可能なアクセス制御SFPまたは情報フロー制御SFPをリストすべきである。

選択:

FMT_MSA.3.1において、PP/ST作成者は、アクセス制御属性のデフォルト特性が、制限的、許可的、あるいはその他の特性のいずれになるのかを選択すべきである。その他の特性の場合、PP/ST作成者は、これを特定の特性に詳細化すべきである。

割付:

FMT_MSA.3.2において、PP/ST作成者は、セキュリティ属性の値を修正することが許された役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

H.3　TSF**データの管理**(FMT_MTD)

このコンポーネントは、TSFデータの管理における要件を課すものである。TSFデータの例は、現在時刻と監査証跡である。それで、このファミリは、だれが監査証跡を読み出し、削除、または作成できるかを特定することを認める。

FMT_MTD.1　TSF**データの管理**

このコンポーネントは、ある役割を持つ利用者が、TSFデータの値を管理することを認める。利用者は、コンポーネントFMT_SMR.1内の役割に割り付けられる。

パラメタのデフォルト値は、パラメタが特定の値を割り付けられずに具現化されたときに取る値である。パラメタの具現化(作成)時に初期値が与えられ、デフォルト値を上書きする。

操作

選択:

FMT_MTD.1.1において、PP/ST作成者は、識別されたTSFデータに適用することのできる操作を特定すべきである。PP/ST作成者は、その役割が、デフォルト変更、問合せ、あるいはTSFデータの修正、あるいはTSFデータの全削除を行えることを特定できる。もし必要ならば、PP/ST作成者はどのような種別の操作でも特定できる。「TSFデータを消去する」の意味を判りやすく言うと、TSFデータの内容が除去されるが、エンティティそれ自身はシステムの中に残るということである。

割付:

FMT_MTD.1.1において、もし選択されれば、、PP/ST作成者は、その役割が、他のどの操作を実行できるかを特定すべきである。そのような操作の一例は、「作成する」である。

FMT_MTD.1.1において、PP/ST作成者は、識別された役割よって操作され得るTSFデータを特定すべきである。PP/ST作成者は、デフォルト値が管理され得ることを特定することが可能である。

FMT_MTD.1.1において、PP/ST作成者は、そのTSFデータにおいて操作が許される役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

FMT_MTD.2　TSF**データにおける限界値の管理**

このコンポーネントは、TSFデータの限界値と、その限界値を超えた場合にとられるアクションを特定する。例えば、このコンポーネントは、監査証跡のサイズの限界値が定義さ

れること、及びこれらの制限を超えたときにとられるアクションの特定を認める。

操作

割付:

FMT_MTD.2.1において、PP/ST作成者は、限界値を持つことのできるTSFデータとそれらの限界値を特定すべきである。そのようなTSFデータの一例は、ログインした利用者の数である。

FMT_MTD.2.1において、PP/ST作成者は、TSFデータの限界値を修正することが許される役割、及びとられるアクションを特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

FMT_MTD.2.2において、PP/ST作成者は、特定したTSFデータにおける特定した限界値を超えた場合にとられるアクションを特定すべきである。そのようなTSFアクションの一例は、許可利用者が通知を受け、監査記録が生成される、である。

FMT_MTD.3　セキュアなTSFデータ

このコンポーネントは、TSFデータに割り付けることのできる値における要件をカバーする。割り付けられる値は、TOEがセキュアな状態を保持するようなものであるべきである。

「セキュア」が何を意味するかの定義は、このコンポーネントでは回答されず、TOEの開発(特に、ADV_SPM.1 非形式的TOEセキュリティ方針モデル)、及びその結果としてのガイダンスの情報に委ねられる。セキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を開発者が提供すれば、FMT_MSA.2のADV_SPM.1への依存性が論証される。

H.4　**取消し**(FMT_REV)

このファミリは、TOE内のさまざまなエンティティに対するセキュリティ属性の取消しに対応する。

FMT_REV.1　**取消し**

このコンポーネントは、権限の取消しにおける要件を特定する。これは、取消しの規則の特定を要求する。例を以下に示す:

a)　利用者の次回ログイン時に取消しが行われる;

b)　次回のファイルオープン試行時に取消しが行われる;

c)　固定時間内に取消しが行われる。これは、すべての開かれた接続が x 分ごとに再評価されることを意味するかもしれない。

操作

選択:

FMT_REV.1.1において、PP/ST作成者は、利用者、サブジェクト、オブジェクト、あるいはその他の資源からセキュリティ属性を取り消す能力が、TSFによって提供されねばならないかどうかを特定すべきである。最後の選択肢が選ばれる場合、PP/ST作成者は、その資源を定義する詳細化操作を使用するべきである。

割付:

FMT_REV.1.1において、PP/ST作成者は、TSFにおける機能を修正することが許される役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

FMT_REV.1.2において、PP/ST作成者は、取消し規則を特定すべきである。これらの規則の例には、「関係付けられた資源の次回操作の前に」、あるいは「すべての新しいサブジェクト作成に対して」などがある。

H.5　セキュリティ属性有効期限(FMT_SAE)

このファミリは、セキュリティ属性の有効性に対して時間制限を実施する能力に対応する。このファミリは、アクセス制御属性、識別と認証属性、認証書(例えばANSI X509のような鍵認証書)、監査属性等々に対する有効期限の特定に適用することができる。

FMT_SAE.1　時限付き許可

操作

割付:

FMT_SAE.1.1において、PP/ST作成者は、有効期限がサポートされるべきセキュリティ属性のリストを特定すべきである。そのような属性の一例は、利用者のセキュリティ取扱許可である。

FMT_SAE.1.1において、PP/ST作成者は、TSFにおけるセキュリティ属性を修正することが許される役割を特定すべきである。対象となる役割は、FMT_SMR.1で特定される。

FMT_SAE.1.2において、PP/ST作成者は、各セキュリティ属性が有効期限になったときにとられるアクションのリストを特定すべきである。一例は、有効期限となったとき、利用者のセキュリティ取扱許可が、TOEにおける最低限の取扱許可レベルにセットされるというものである。PP/STによって即時取消しが必要とされる場合は、「即時取消し」アクションが特定されるべきである。

H.6　セキュリティ管理役割(FMT_SMR)

このファミリは、利用者が、彼らに割り付けられた機能上の責任外のアクションをとることでその権限を悪用することから生じる損害の公算を低減する。また、TSFをセキュアに管理するには不適切なメカニズムが提供されるという脅威にも対応する。

このファミリは、利用者が特定のセキュリティ関連管理機能の使用を許可されているかどうかを識別するための情報が維持されることを要求する。

ある管理アクションは利用者によって実行でき、あるものは組織内の指定された人間だけが実行できる。このファミリは、所有者、監査者、管理者、日常管理といったさまざまな役割の定義を認める。

このファミリで使用される役割は、セキュリティ関連の役割である。各役割は、広範囲にわたる能力のセット(例えば、UNIXにおけるルート)を範囲とすることもでき、あるいは単一の権限(例えば、ヘルプファイルのような単一のオブジェクトを読む権限)とすることもできる。このファミリは、役割を定義する。役割の能力は、FMT_MOF、FMT_MSA、及びFMT_MTDで定義される。

ある役割の種別は互いに排他的であることがある。例えば、日常管理は、利用者の定義及び活性化が可能かもしれないが、利用者の削除(管理者(役割)用に留保されている)はできないかもしれない。このクラスは、二人制御のような方針を特定することを認める。

FMT_SMR.1　セキュリティ役割

このコンポーネントは、TSFが認識すべきさまざまな役割を特定する。システムは、しばしば、エンティティの所有者、管理者及び他の利用者を区別する。

操作

割付:

FMT_SMR.1.1において、PP/ST作成者は、システムによって認識される役割を特定すべきである。これらは、セキュリティに関して利用者がとり得る役割である。例: 所有者、監査者、管理者。

FMT_SMR.2　セキュリティ役割における制限

このコンポーネントは、TSFが認識すべきさまざまな役割、及びそれらの役割がどのように管理され得るかの条件を特定する。システムは、しばしば、エンティティの所有者、管理者及び他の利用者を区別する。

それらの役割における条件は、いつ利用者がその役割を負えるかの制約はもちろん、さまざまな役割間の相互関係も特定する。

操作

割付:

FMT_SMR.2.1において、PP/ST作成者は、システムによって認識される役割を特定すべきである。これらは、セキュリティに関して利用者がとり得る役割である。例: 所有者、監査者、管理者。

FMT_SMR.2.3において、PP/ST作成者は、役割の割付を運営する条件を特定すべきである。これらの条件の例: 「一つのアカウントは、監査者及び管理者の役割の両方を持てない」、あるいは「アシスタントの役割を持つ利用者は、所有者の役割も持たねばならない」。

FMT_SMR.3　負わせる役割

このコンポーネントは、特定の役割を負わせるために明示的な要求を与えねばならないことを特定する。

操作

割付:

FMT_SMR.3.1において、PP/ST作成者は、それを負わせるために明示的な要求を必要とする役割を特定すべきである。例: 監査者及び管理者。

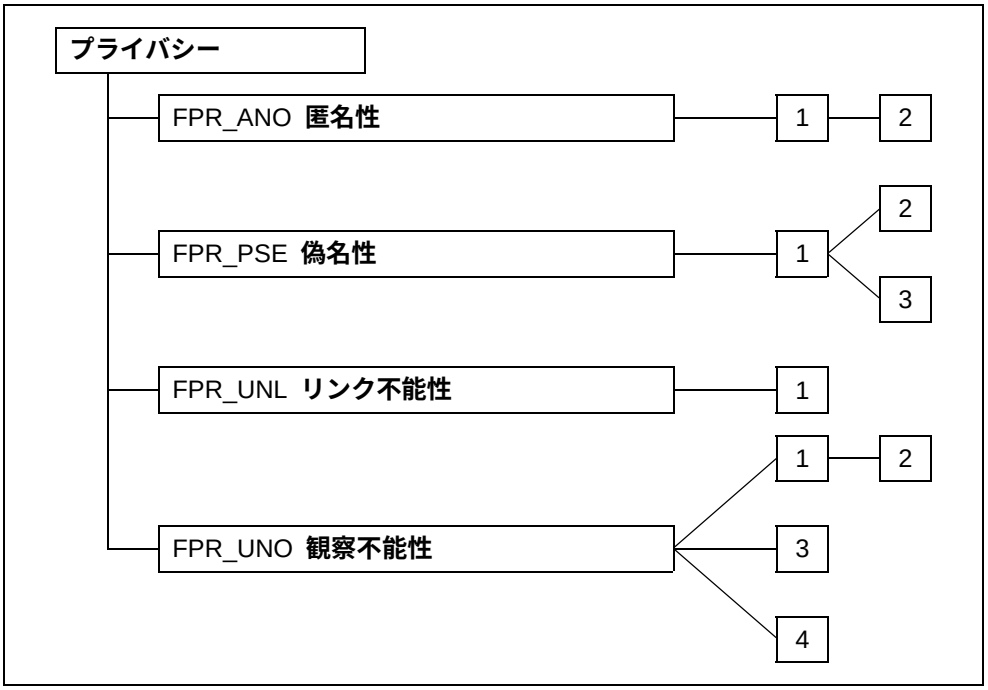
附属書I

(参考)

プライバシー(FPR)

このクラスは、システムの操作における十分な制御を維持するために、可能な限りシステムに柔軟性を持たせる一方、利用者のプライバシーの必要性を満たすために課すことができる要件を記述する。

このクラスのコンポーネントでは、許可利用者は要求されたセキュリティ機能によってカバーされるかどうかに関しての柔軟性がある。例えば、PP/ST作成者は、適切に許可された利用者に対しては、利用者全般のプライバシーの保護を要求しないことが適切であると考えるかもしれない。



図I.1 - プライバシークラスのコンポーネント構成

このクラスは、他のクラス(監査、アクセス制御、高信頼パス、否認不可などに関するもの)と共に、望ましいプライバシーのふるまいを特定するための柔軟性を提供する。一方、このクラスの要件は、FIAやFAUのような他のクラスのコンポーネントの使用における制限を強いることがある。例えば、許可利用者が利用者識別情報を見ることが許されない場合(例えば、匿名性や偽名性)、個々の利用者に、彼らの実行するプライバシー要件によってカバーされたセキュリティ関連アクションについての責任を持たせることは、明らかに不可能となろう。しかしながら、PP/STに監査要件を含めることは可能であり、そこでは、

特定のセキュリティ関連事象が発生したという事実の方が、誰がそれに対して責任があるかを知るよりも重要となる。

追加情報がFAUクラスにおける適用上の注釈で提供されており、そこでは、監査の文脈における「識別情報」の定義が、利用者の識別が可能な別名やその他の情報でもよいことを説明している。

このクラスは4つのファミリを記述する: 匿名性、偽名性、リンク不能性、観察不能性。匿名性、偽名性、及びリンク不能性は、複雑な相互関係を持つ。そのため、ファミリを選択するとき、その選択は識別された脅威に依存すべきである。ある種別のプライバシー脅威に対しては、偽名性の方が匿名性よりも適切になろう(例えば、監査のための要件がある場合)。加えて、ある種別のプライバシー脅威は、いくつかのファミリからのコンポーネントの組み合わせによって対抗するのが最善である。

すべてのファミリは、利用者が、利用者自身の識別情報を開示するアクションを明示的に実行しないことを前提にしている。例えば、TSFが電子メッセージやデータベース中の利用者名を隠すことは期待されていない。

このクラスのすべてのファミリは、操作によって範囲を決めることのできるコンポーネントを持つ。これらの操作は、TSFが抵抗しなければならない協同した利用者/サブジェクトを、PP/ST作成者が明らかにできるようにする。匿名性の実例に次のようなものがある: 「TSFは、遠隔コンサルティングアプリケーションに結びつけられた利用者識別情報を、利用者及び/またはサブジェクトが判断できないことを保証しなければならない」。

TSFは、個々の利用者だけでなく、情報を得ようとする協同した利用者に対しても、この保護を提供すべきことに注意が必要である。このクラスが提供する保護の強度は、パート1附属書B及び附属書Cで詳述された機能強度として記述されるべきである。

I.1 匿名性(FPR_ANO)

匿名性は、その利用者識別情報を開示することなく、サブジェクトが資源またはサービスを使用できることを保証する。

利用者のための注釈

このファミリの意図は、利用者またはサブジェクトが、その利用者識別情報を利用者、サブジェクト、あるいはオブジェクトのような他者に公開することなしにアクションがとれることを特定することである。このファミリは、あるアクションを実行している者の識別情報を見ることができない利用者のセットを識別する手段をPP/ST作成者に提供する。

そのため、サブジェクトが匿名性を使用してアクションを実行すると、他のサブジェクトはそのそのサブジェクトを用いている利用者の識別情報を判断できず、その識別情報の参照すら行えない。匿名性の焦点は、サブジェクトの識別情報の保護ではなく、利用者の識別情報の保護である; そのため、サブジェクトの識別情報は、開示から保護されない。

サブジェクトの識別情報は他のサブジェクトや利用者に公開されないが、TSFは利用者識別情報の取得を明示的には禁止されていない。TSFが利用者の識別情報を知ることを許されない場合には、FPR_ANO.2を用いることができる。その場合には、TSFは、利用者情報を要求すべきでない。

「判断する(determine)」の解釈は、その語の意味を最も広義にとるべきである。PP/ST作成者は、どれくらいの厳密さが適用されるべきかを示すのに、機能強度を使用したいと考えるかもしれない。

コンポーネントのレベル付けは、利用者と許可利用者を区別する。許可利用者はしばしばこのコンポーネントから除外され、そのために、利用者の識別情報を読み出すことが認められる。しかしながら、許可利用者が利用者の識別情報を判断する能力を持つことが可能でなければならないという特別な要件があるわけではない。究極のプライバシーのため、どのアクションを実行する誰についてもその識別情報を見ることができないということを言うために、このコンポーネントが使われよう。

提供されるすべてのサービスにおいて匿名性を提供するシステムもあれば、あるサブジェクト/操作に対して匿名性を提供するシステムもある。この柔軟性を提供するために、要件の範囲を定義するところに操作を含める。もしPP/ST作成者がすべてのサブジェクト/操作に対応したい場合は、「すべてのサブジェクト及びすべての操作」という語が提供されよう。

次のような機能を含むアプリケーションがあり得る: 公のデータベースに秘密的な性格を持つ問い合わせをする、電子投票に対応する、匿名の支払いや寄付をする。

敵対的な利用者あるいはサブジェクトの可能性を持つものの例は、プロバイダ、システムオペレータ、通信相手、及び利用者であり、彼らは悪意を持つ部品(例えばトロイの木馬)

をこっそりとシステムに持ち込む。これらの利用者はすべて、使用パターン(どの利用者がどのサービスを使ったかなど)を調査し、その情報を悪用することができる。

FPR_ANO.1 **匿名性**

利用者のための適用上の注釈

このコンポーネントは、利用者の識別情報が暴露から保護されることを保証する。しかしながら、特定の許可利用者が、あるアクションを実行したのは誰かを判断できるという実現例もあり得る。このコンポーネントは、限定された、あるいは全面的なプライバシー方針を手に入れるための柔軟性を与える。

操作

割付:

FPR_ANO.1.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのセットを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_ANO.1.1において、PP/ST作成者は、サブジェクト(例えば「投票アプリケーション」)の実際の利用者の名前が保護されるべきサブジェクト、及び/または操作、及び/またはオブジェクトのリストを識別すべきである。

FPR_ANO.2 **情報を請求しない匿名性**

利用者のための適用上の注釈

このコンポーネントは、TSFが利用者の識別情報を知ることを許可されないことを保証する。

操作

割付:

FPR_ANO.2.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのセットを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が

同一のプロセスを使用できる利用者のグループが該当する。

FPR_ANO.2.1において、PP/ST作成者は、サブジェクト(例えば「投票アプリケーション」)の実際の利用者の名前が保護されるべきサブジェクト、及び/または操作、及び/またはオブジェクトのリストを識別すべきである。

FPR_ANO.2.2において、PP/ST作成者は、匿名性要件の対象となるサービス(例えば「業務内容説明へのアクセス」)のリストを識別すべきである。

FPR_ANO.2.2に対して、PP/ST作成者は、特定されたサービスの提供時に、そのサブジェクト(単数形)の実際の利用者名をそれらから保護すべきサブジェクト(複数形)、のリストを識別すべきである。

I.2 **偽名性**(FPR_PSE)

偽名性は、利用者が、その識別情報を開示することなく資源またはサービスを利用でき、しかもその利用に対して責任を持ち得ることを保証する。利用者は、TSFが保持している参照(別名)に直接関連付けられることによって、あるいはアカウント番号のように処理目的に対して使用される別名を提供することによって、責任を持ち得るようになる。

利用者のための注釈

偽名性は、いくつかの点で匿名性に似ている。偽名性と匿性名の両方とも利用者の識別情報を保護するが、偽名性においては、責任を明確にするため、あるいは他の目的のために、利用者識別情報への参照が維持される。

コンポーネントFPR_PSE.1は、利用者の識別情報に対する参照の要件を特定しない。参照における要件を特定する目的に対しては、二つの要件のセット: FPR_PSE.2及びFPR_PSE.3が与えられる。

参照を使用するためには、元の利用者の識別子を取得できる必要がある。例えば、ディジタルキャッシュの環境では、一つの小切手が複数回発行されたとき(つまり、詐欺行為)、その利用者の識別情報を追跡できると都合がよい。一般に、特定の条件において、利用者の識別情報が検索される必要がある。PP/ST作成者は、可逆偽名性(FPR_PSE.2)を使って、それらのサービスを記述しようとするかもしれない。

参照のもう一つの使い方は、利用者の別名としてである。例えば、識別されたくない利用者は、資源の利用に対して課金されるべきアカウントを提供することができる。そのような場合、利用者の識別情報への参照とはその利用者に対する別名のことであり、他の利用者あるいはサブジェクトは、その利用者の識別情報を取得することなくそれぞれの機能(例えば、システムの使用における統計的操作)を実行するために、その別名を利用できる。この場合、PP/ST作成者は、参照が適合しなければならない規則を特定するために、FPR_PSE.3 別名偽名性を一緒に使いたいと思うかもしれない。

上述の構成概念を使い、利用者識別情報が保護されること、及び、条件として特定すれば、ディジタルマネーが二度使われた場合に利用者識別情報を追跡する要件が存在することを特定するFPR_PSE.2 可逆偽名性を使って、ディジタルマネーが作成できる。利用者が正直者であればその利用者の識別情報は保護され; 利用者が不正行為を行おうとすればその利用者の識別情報を追跡することができる。

別の種類のシステムとして、ディジタルクレジットカードがあげられよう。そこでは利用者は、現金が引き落とされる口座を示す偽名を提供する。このような場合、例えば、FPR_PSE.3 別名偽名性を使うことができる。このコンポーネントは、利用者識別情報が保護されること、さらに、利用者は、自分が提供した金額(条件にそう特定されていれば)に対して割り付けられた値だけを入手することを特定する。

より厳格なコンポーネントが、識別と認証や監査のような他の要件と組み合わせられない

場合があるということを理解すべきである。「識別情報を判断する」の解釈は、その語の最も広義のものにとるべきである。その情報は操作時にTSFによって提供されることはなく、そのエンティティは操作を行ったサブジェクトあるいはサブジェクトの所有者を判断することはできず、利用者やサブジェクトが入手可能な、将来において利用者の識別情報を公開してしまいかねない情報をTSFが記録することもない。

その意図は、TSFは、利用者の識別情報を危うくする情報、例えば利用者を代行するサブジェクトの識別情報を一切明らかにしないということである。機密上重要と考えられる情報とは、攻撃者が費やすことができる労力に依存するものである。そのため、FPR_PSE 偽名性ファミリは、機能強度要件の対象になる。

応用として考えられるものは、識別情報を開示せず、割増レートの電話サービスに対して呼び出し側に課金する、あるいは電子支払いシステムの匿名利用に対して課金されるようにするものである。

敵対的な利用者あるいはサブジェクトの可能性を持つものの例は、プロバイダ、システムオペレータ、通信相手、及び利用者であり、彼らは悪意を持つ部品(例えばトロイの木馬)をこっそりとシステムに持ち込む。これらの攻撃者はすべて、どの利用者がどのサービスを使ったかを調査でき、この情報を悪用できる。

匿名性サービスに加え、偽名性サービスは、識別なしの許可、特に匿名支払い(「ディジタルキャッシュ」)のための方法を含む。これは、プロバイダが、顧客の匿名性を保ちながらセキュアな方法で支払いを受けることを補助する。

FPR_PSE.1　偽名性

利用者のための適用上の注釈

このコンポーネントは、他の利用者に対する識別情報の暴露に対する利用者保護を提供する。利用者は、そのアクションに対して責任を保持する。

操作

割付:

FPR_PSE.1.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのセットを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.1.1において、PP/ST作成者は、サブジェクト(例えば「求人情報に対するアクセス」)の実際の利用者の名前が保護されるべきサブジェクト、及び/ま

たは操作、及び/またはオブジェクトのリストを識別すべきである。「オブジェクト」は、利用者あるいはサブジェクトに利用者の実際の識別情報を推論させ得るその他のどのような情報も含むことに注意。

FPR_PSE.1.2において、PP/ST作成者は、TSFが提供できる別名の数(一つあるいはそれ以上)を識別すべきである。

FPR_PSE.1.2において、PP/ST作成者は、TSFがある別名を提供できるサブジェクトのリストを識別すべきである。

選択:

FPR_PSE.1.3において、PP/ST作成者は、利用者の別名がTSFによって生成されるのか、あるいはその利用者によって供給されるのかを特定すべきである。

割付:

FPR_PSE.1.3において、PP/ST作成者は、TSF生成の、あるいは利用者生成の別名が適合すべき尺度を識別すべきである。

FPR_PSE.2 **可逆偽名性**

利用者のための適用上の注釈

このコンポーネントにおいて、TSFは、特定の条件下で、与えられた参照に関連する利用者識別情報が判断できることを保証しなければならない。

FPR_PSE.1において、TSFは、利用者識別情報の代わりに別名を提供しなければならない。特定の条件が満たされるとき、その別名が属する利用者識別情報が判断できる。電子キャッシュ環境におけるそのような条件の一例: 「TSFは、一つの小切手が二度発行されたという条件の元でのみ、提供された別名に基づく利用者識別情報を判断できる能力を公証人に提供しなければならない」。

操作

割付:

FPR_PSE.2.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのセットを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.2.1において、PP/ST作成者は、サブジェクト(例えば「求人情報に対

するアクセス」)の実際の利用者の名前が保護されるべきサブジェクト、及び/または操作、及び/またはオブジェクトのリストを識別すべきである。「オブジェクト」は、利用者あるいはサブジェクトに利用者の実際の識別情報を推論させ得る、その他のどのような情報も含むことに注意。

FPR_PSE.2.2において、PP/ST作成者は、TSFが提供できる別名の数(一つあるいはそれ以上)を識別すべきである。

FPR_PSE.2.2において、PP/ST作成者は、TSFがある別名を提供できるサブジェクトのリストを識別すべきである。

選択:

FPR_PSE.2.3において、PP/ST作成者は、利用者の別名がTSFによって生成されるのか、あるいはその利用者によって供給されるのかを特定すべきである。

割付:

FPR_PSE.2.3において、PP/ST作成者は、TSF生成の、あるいは利用者生成の別名が適合すべき尺度を識別すべきである。

選択:

FPR_PSE.2.4において、PP/ST作成者は、許可利用者及び/または高信頼サブジェクトが実際の利用者名判断できるかどうかを選択すべきである。

割付:

FPR_PSE.2.4において、PP/ST作成者は、特定の条件下で実際の利用者名を取得することのできる高信頼サブジェクト、例えば公証人あるいは特別の許可利用者、のリストを識別すべきである。

FPR_PSE.2.4において、PP/ST作成者は、提供された参照に基づいて高信頼サブジェクト及び許可利用者が実際の利用者名を判断できる条件のリストを識別すべきである。これらの条件は、曜日の時間のような条件か、あるいは裁判所の命令のような行政的なものがある。

FPR_PSE.3　別名偽名性

利用者のための適用上の注釈

このコンポーネントにおいて、TSFは、提供された参照がある構造規則を満たすこと、それによって、セキュアでない可能性のあるサブジェクトによっても、セキュアな方法で使用されることができることを保証しなければならない。

もし利用者が、その識別情報を開示することなくディスク資源を使用したい場合、偽名性が使用できる。しかしながら、利用者はシステムにアクセスするたびに、同一の別名を使

用しなければならない。そのような条件は、このコンポーネントで特定することができる。

操作

割付:

FPR_PSE.3.1において、PP/ST作成者は、TSFがそれらに対して保護を提供すべき利用者及び/またはサブジェクトのセットを特定せねばならない。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.3.1において、PP/ST作成者は、サブジェクト(例えば「求人情報に対するアクセス」)の実際の利用者の名前が保護されるべきサブジェクト、及び/または操作、及び/またはオブジェクトのリストを識別すべきである。「オブジェクト」は、利用者あるいはサブジェクトに利用者の実際の識別情報を推論させ得る、その他のどのような情報も含むことに注意。

FPR_PSE.3.2において、PP/ST作成者は、TSFが提供できる別名の数(一つあるいはそれ以上)を識別すべきである。

FPR_PSE.3.2において、PP/ST作成者は、TSFがある別名を提供できるサブジェクトのリストを識別すべきである。

選択:

FPR_PSE.3.3において、PP/ST作成者は、利用者の別名がTSFによって生成されるのか、あるいはその利用者によって供給されるのかを特定すべきである。

割付:

FPR_PSE.3.3において、PP/ST作成者は、TSF生成の、あるいは利用者生成の別名が適合すべき尺度を識別すべきである。

FPR_PSE.3.4において、PP/ST作成者は、実際の利用者名に対して使用される参照が同一でなければならない場合と、異なるものでなければならない場合を示す条件、例えば「利用者が同一のホストにログオンするとき、」利用者はただ一つの別名を使う、のリストを識別すべきである。

I.3 **リンク不能性**(FPR_UNL)

リンク不能性は、利用者が複数の資源あるいはサービスを使用するとき、他人がそれらを一つにリンクできないようにして使用できることを保証する。リンク不能性は、偽名とは異なるものであり、それは、偽名性においても利用者は同様に知られることはないが、異なるアクション間の関係は提供され得るという点である。

利用者のための注釈

リンク不能性の要件は、操作のプロファイリングの使用に対して利用者識別情報を保護することを意図している。例えば、ある電話用のスマートカードが、あるただ一つの番号で用いられるとき、電話会社はそのカードの利用者のふるまいを判断することができる。利用者の電話のプロファイルがわかれば、そのカードは特定の利用者にリンクされ得る。異なるサービスの呼び出し、あるいは資源のアクセス間の関係を隠すことが、この種の情報収集を防ぐことになる。

結果的に、リンク不能性の要件は、ある操作のサブジェクトと利用者識別情報が保護されねばならないということを暗に示すことになる。さもなければ、これらの情報は、複数の操作をリンクするために使われるかもしれない。

リンク不能性は、さまざまな操作が関係付けできないことを要求する。この関係は、いくつかの形態をとり得る。例えば、その操作に関連付けられた利用者、そのアクションを起動した端末、そのアクションが実行された時間など。PP/ST作成者は、対抗せねばならない、どのような種類の関係が存在するかを特定できる。

対象となるアプリケーションは、利用者の識別情報を暴露しかねない使用パターンを作成することなしに、一つの偽名を何度も使用させる能力を含むことがある。

敵対的なサブジェクト及び利用者の可能性を持つものの例は、プロバイダ、システムオペレータ、通信相手、及び利用者であり、彼らは悪意を持つ部品(例えばトロイの木馬)を、彼らが操作はしないがそれについての情報を得ようとするシステムにこっそりと持ち込む。これらの攻撃者はすべて、この情報(例えばどの利用者がどのサービスを使ったかを)を調査・悪用できる。リンク不能性は、一人の顧客のいくつかのアクション間から引き出し得るリンケージから利用者を保護する。一例は、一人の匿名の顧客からさまざまな相手にかけられた一連の電話の呼である。相手の識別情報の組み合わせから、その顧客の識別情報を暴露できるかもしれない。

FPR_UNL.1 **リンク不能性**

利用者のための適用上の注釈

このコンポーネントは、利用者がシステム内のさまざまな操作をリンクできず、そのために情報を取得できないことを保証する。

操作

割付:

FPR_UNL.1.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのセットを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNL.1.1において、PP/ST作成者は、リンク不能性の要件の対象になるべき操作のリスト、例えば「電子メールを送信」、を識別すべきである。

選択:

FPR_UNL.1.1において、PP/ST作成者は、分かりにくくされるべき関係を選択すべきである。この選択は、利用者識別情報あるいは関係の割付が特定されることを認める。

割付:

FPR_UNL.1.1において、PP/ST作成者は、それに対抗して保護されるべき関係のリスト、例えば「同一の端末からの発信」、を識別すべきである。

I.4 観察不能性(FPR_UNO)

観察不能性は、他者、特に第三者が資源あるいはサービスが使用されていることを観察できない状態で、利用者がその資源あるいはサービスを使用できることを保証する。

利用者のための注釈

観察不能性は、これまでのファミリ、匿名性、偽名性、及びリンク不能性と異なる方向から利用者識別情報を取り上げる。この場合の意図は、利用者の識別情報を隠すよりも、資源あるいはサービスの使用を隠すことである。

多くの技術が、観察不能性を実現するために適用できる。観察不能性を提供する技術の例は以下のとおり:

a) 観察不能性に影響を与える情報の配置: 観察不能性関連情報(操作が行われたことを表す情報など)は、TOE内のさまざまな場所に配置できる。その情報は、攻撃者にTOE内のどのパートを攻撃すべきかを知られないよう、TOE内のランダムに選んだ一箇所に配置されることがある。別のシステムでは、もし抜け道を通られても、TOE内の一箇所に利用者のプライバシーを損なうのに十分な情報を持たないよう、その情報を分散させることがある。この技術は、FPR_UNO.2で明示的に対応される。

b) ブロードキャスト: 情報がブロードキャストされる場合(イーサネットやラジオなど)、利用者は、その情報を誰が実際に受信し、使用したかを判断できない。この技術は、その情報に興味を持つことを人に知られるのを恐れる受信者にその情報が届けられる場合(秘密にすべき医療情報など)にとりわけ有効である。

c) 暗号保護とメッセージパディング: メッセージストリームを観察する人は、メッセージが転送されたという事実とメッセージ上の属性から情報を取得するかもしれない。トラフィックパディング、メッセージパディング、及びメッセージストリームの暗号化によって、メッセージの伝送及びその属性を保護できる。

場合によって、利用者は資源の使用を見るべきでないが、許可利用者は、その任務を果たすために、資源の使用を見ることを許可されねばならない。そのような場合、FPR_UNO.4が使用でき、これは、一人または複数の許可利用者に、資源の使用状況を見る能力を提供する。

このファミリは、「TOEのパート」という概念を使用する。これは、TOEの任意のパートであって、TOE内の他のパートから物理的あるいは論理的に分離されたものと考えられる。論理的分離では、FPT_SEPが関係するかもしれない。

通信の観察不能性は、憲法上の権利・組織の方針の実施、あるいは防衛関連の応用のよう

な多くの場面で、重要な要素となろう。

FPR_UNO.1　観察不能性

利用者のための適用上の注釈

このコンポーネントは、機能あるいは資源の使用を非許可利用者が観察できないことを要求する。このコンポーネントに加え、PP/ST作成者は、隠れチャネル分析を一緒に使用したいと思うかもしれない。

操作

割付:

FPR_UNO.1.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのリストを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNO.1.1に対して、PP/ST作成者は、観察不能性要件の対象となる操作のリストを識別すべきである。それによって、他の利用者/サブジェクトは、その特定されたリストでカバーされるオブジェクトにおける操作(オブジェクトに対する読み出しや書き込みなど)を観察できなくなる。

FPR_UNO.1.1において、PP/ST作成者は、観察不能性要件によってカバーされるオブジェクトのリストを識別すべきである。一例は、特定のメールサーバあるいはftpサイトである。

FPR_UNO.1.1において、PP/ST作成者は、その観察不能性情報が保護される利用者及び/またはサブジェクトのセットを特定すべきである。一例は、「インターネットを介してシステムにアクセスする利用者」となろう。

FPR_UNO.2　観察不能性に影響する情報の配置

利用者のための適用上の注釈

このコンポーネントは、特定された利用者あるいはサブジェクトが、機能あるいは資源の使用を観察できないことを要求する。さらに、このコンポーネントは、攻撃者がTOE内のどのパートが標的かを知ることができないように、あるいは彼らがTOE内のあちこちを攻撃する必要があるように、利用者のプライバシーに関係する情報がTOE内に分散されることを特定する。

このコンポーネントの使用例は、一つの機能を提供するために、ランダムに配置された一つのノードの使用である。この場合には、コンポーネントは、プライバシー関連の情報がTOEの一つの識別されたパートでだけ利用できるものでなければならず、TOEのこのパートの外部との通信は行われないということを要求するかもしれない。

もっと複雑な例が、ある「投票アルゴリズム」に見られる。TOEのいくつかのパートがそのサービスに関与するが、TOEの個々のパートは方針に違反することができない。そのため、投票が行われたかどうか、投票がどうなったかをTOEが判断できないような状態で、人は投票することができる(投票が満場一致になったときは別だが)。

このコンポーネントに加え、PP/ST作成者は、隠れチャネル分析を一緒に使用したいと思うかもしれない。

操作

割付:

FPR_UNO.2.1において、PP/ST作成者は、TSFがそれらに対して保護を提供せねばならない利用者及び/またはサブジェクトのリストを特定すべきである。例えば、PP/ST作成者が単一の利用者あるいはサブジェクトを特定したとしても、TSFは、個々の利用者やサブジェクトに対抗して保護を提供するだけでなく、協同する利用者及び/またはサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNO.2.1に対して、PP/ST作成者は、観察不能性要件の対象となる操作のリストを識別すべきである。それによって、他の利用者/サブジェクトは、その特定されたリストでカバーされるオブジェクトにおける操作(オブジェクトに対する読み出しや書き込みなど)を観察できなくなる。

FPR_UNO.2.1において、PP/ST作成者は、観察不能性要件によってカバーされるオブジェクトのリストを識別すべきである。一例は、特定のメールサーバあるいはftpサイトである。

FPR_UNO.2.1において、PP/ST作成者は、その観察不能性情報が保護される利用者及び/またはサブジェクトのセットを特定すべきである。一例は、「インターネットを介してシステムにアクセスする利用者」となろう。

FPR_UNO.2.2において、PP/ST作成者は、どのプライバシー関連の情報が制御された仕方で分散されるべきかを識別すべきである。このような情報の例として、サブジェクトのIPアドレス、オブジェクトのIPアドレス、時間、使用された暗号鍵などがある。

FPR_UNO.2.2において、PP/ST作成者は、情報の散布が守るべき条件を特定すべきである。これらの条件は、各事例のプライバシー関連の情報のライフタイ

ムを通して維持されるべきである。このような条件の例として、「情報は、TOEの単一の分離したパートだけに置かれねばならず、TOEのこのパートの外部に伝達されてはならない」、「情報は、TOEの単一の分離したパートだけに存在しなけらばならず、TOEの別のパートに定期的に移動されねばならない」、「情報は、TOEのどの5つの分離したパートが危殆化してもセキュリティ方針が損なわれることのないよう、TOEの異なる分離したパート間に分散されねばならない」などがある。

FPR_UNO.3　情報を請求しない観察不能性

利用者のための適用上の注釈

このコンポーネントは、特定のサービスが提供されるときに、TSFが、観察不能性を損なうかもしれない情報を取得しようと試みないことを要求するために使用される。そのために、TSFは、観察不能性を危うくするために使われるかもしれないどのような情報も求めることはない(つまり、他のエンティティから取得しようと試みない)。

操作

割付:

FPR_UNO.3.1において、PP/ST作成者は、観察不能性要件の対象となるサービス(例えば「業務内容説明へのアクセス」)のリストを識別すべきである。

FPR_UNO.3.1に対して、PP/ST作成者は、特定されたサービスの提供時に、そのサブジェクトからプライバシー関連情報を保護すべきサブジェクトのリストを識別すべきである。

FPR_UNO.3.1において、PP/ST作成者は、特定されたサブジェクトから保護すべきプライバシー関連情報を特定すべきである。例として、サービスを使用したサブジェクトの識別情報、及びメモリ資源利用のような使用したサービスの量などがある。

FPR_UNO.4　許可利用者観察可能性

利用者のための適用上の注釈

このコンポーネントは、資源利用を調べる権限を持つ一人あるいはそれ以上の許可利用者が存在することを要求するために使用される。このコンポーネントなしでもこの検査は認められるが、必須にはならない。

操作

割付:

FPR_UNO.4.1において、PP/ST作成者は、資源利用を観察する能力をTSFが提供しなければならない許可利用者のセットを特定すべきである。許可利用者のセットとは、例えば、同一の役割の元で操作できる、あるいは全員が同じプロセスを使用できる、許可利用者のグループなどである。

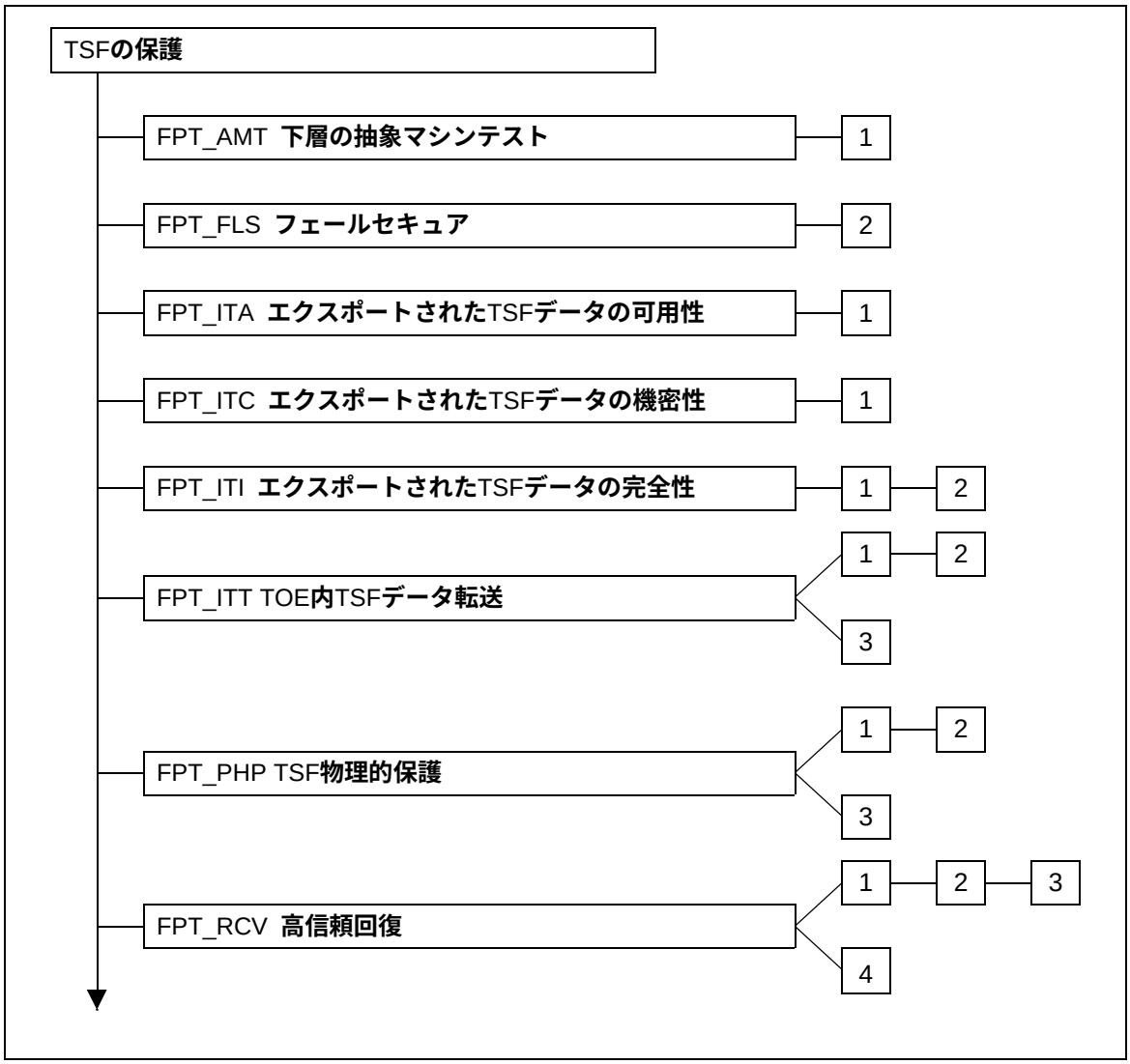
FPR_UNO.4.1において、PP/ST作成者は、許可利用者が観察できねばならない資源及び/またはサービスを特定すべきである。

附属書J

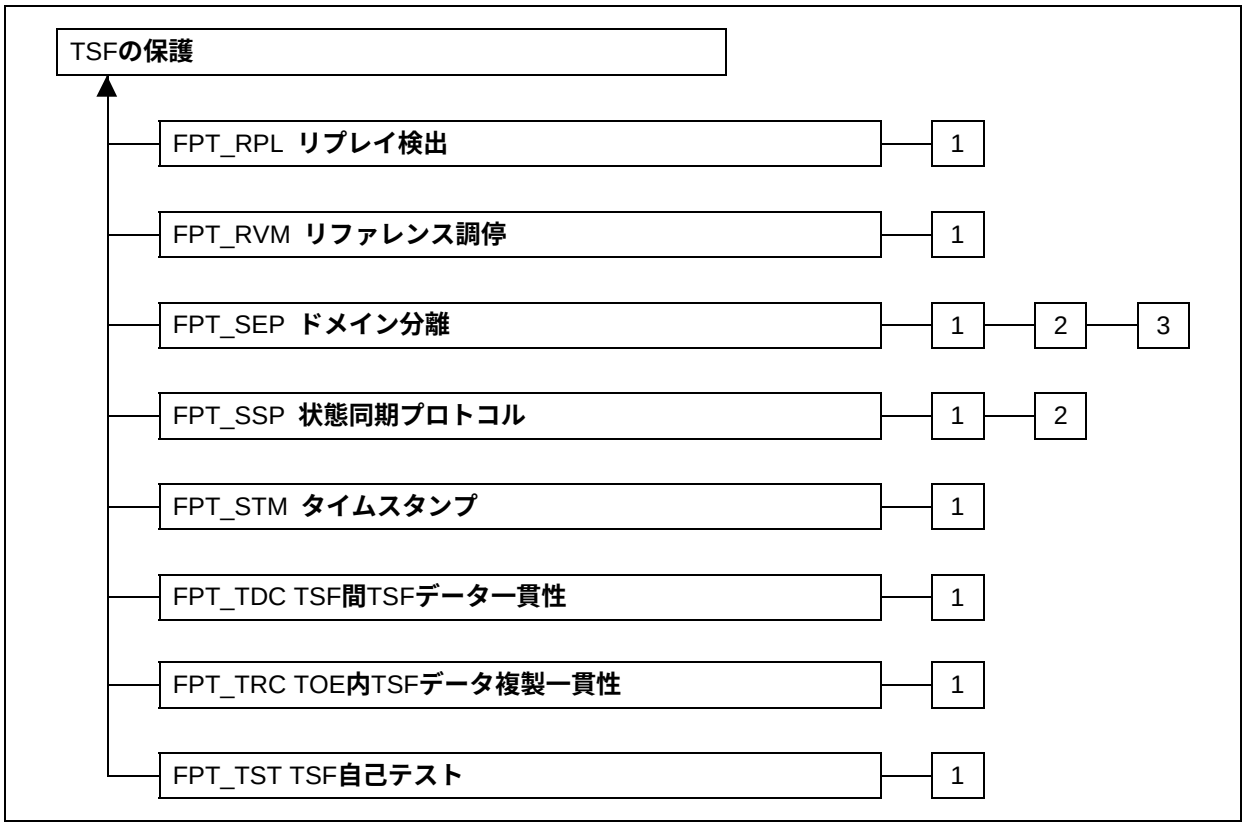
(参考)

TSFの保護(FPT)

このクラスは、TSFを提供するメカニズムの完全性及び管理に関係し(TSP特有のものから独立)、かつTSFデータの完全性に関係する(TSPデータの特有な内容から独立)機能要件のファミリを含む。ある意味で、このクラスの中のファミリは、FDP(利用者データ保護)クラスの中のコンポーネントと重複しているように見えるかもしれず、同じメカニズムを使って実現されることさえあるかもしれない。しかしながら、FDPは利用者データの保護に焦点を当てるが、FPTはTSFデータの保護に焦点を当てる。実際、FPTクラスのコンポーネントは、TOEのSFPを改ざんあるいはバイパスすることができない要件を適用するために必要である。



図J.1 - TSF**の保護クラスのコンポーネント構成**



図J.2 - TSF**の保護クラスのコンポーネント構成(続き)**

このクラスの観点から、TSFを構成する三つの重要な部分がある。

a) TSFの*抽象*マシン、これは、評価を行う特定のTSFが実装される、仮想的または物理的なマシンである。

b) TSFの*実装*、これは、抽象マシン上で動作し、TSPを実施するメカニズムを実装する。

c) TSFの*データ*、これは、TSPの実施を導く管理上のデータベースである。

FPTクラスにおけるファミリのすべてはこれらの領域に関係付けられ、さらに以下のグループに入れられる。

a) FPT_PHP(TSF物理的保護)、これは、TSFを構成するTOEのパートに対する外部攻撃を検出する能力を許可利用者に提供する。

b) FPT_AMT(下位の抽象マシンテスト)とFPT_TST(TSF自己テスト)、これらは、TSFデータと実行可能コードの完全性はもちろん、下位の抽象マシンとTSFの正しい操作を検証する能力を許可利用者に提供する。

c) FPT_SEP(ドメイン分離)とFPT_RVM(リファレンス調停)、これらは、動作中

のTSFを保護し、TSFがバイパスされ得ないことを保証する。これらのファミリの適切なコンポーネントがADV_INT(TSF内部構造)の適切なコンポーネントと組み合わされたとき、TOEは、従来「リファレンスモニタ」と呼ばれていたものを持つと言えるようになる。

d) FPT_RCV(高信頼回復)、FPT_FLS(フェールセキュア)、及びFPT_TRC(TOE内TSFデータ複製一貫性)、これらは、障害発生時と直後のTSFのふるまいに対応する。

e) FPT_ITA(エクスポートされたTSFデータの可用性)、FPT_ITC(エクスポートされたTSFデータの機密性)、FPT_ITI(エクスポートされたTSFデータの完全性)、これらは、TSFとリモート高信頼IT製品間のTSFデータの保護及び可用性に対応する。

f) FPT_ITT(TOE内TSFデータ転送)、これは、TOEの物理的に分離したパート間で伝送されるときのTSFデータの保護に対応する。

g) FPT_RPL(リプレイ検出)、これは、情報及び/または操作のさまざまな種別のリプレイに対応する。

h) FPT_SSP(状態同期プロトコル)、これは、TSFデータに基づく、分散TSFの異なるパート間の状態の同期に対応する。

i) FPT_STM(タイムスタンプ)、これは、信頼できるタイミングに対応する。

j) FPT_TDC(TSF間TSFデータ一貫性)、これは、TSFとリモート高信頼IT製品間で共有するTSFデータの一貫性に対応する。

J.1　下層の抽象マシンテスト(FPT_AMT)

このファミリは、TSFが依存する下層の抽象マシンについて作られたセキュリティ想定事項のTSFのテストに対する要件を定義する。この「抽象」マシンとは、ハードウェア/ファームウェアのプラットフォームかもしれず、仮想マシンとして動作する既知の評価されたハードウェア/ソフトウェアの組み合わせであってもよい。このようなテストの例としては、ハードウェアのページ保護をテストする、受信確認のためにサンプルパケットをネットワーク経由で送信する、仮想マシンインタフェースのふるまいを検証する、などがある。これらのテストは、何らかのメンテナンス状態で、スタートアップ時に、オンラインで、あるいは連続的に、実行することができる。テストの結果としてTOEがとるべきアクションは、FPT_RCVで定義する。

利用者のための注釈

「下層の抽象マシン」という用語は、典型的に、TSFが実装されるハードウェアコンポーネントを指す。しかしながら、下層にあり、既に評価済みのハードウェアとソフトウェアの組み合わでTSFが依存する仮想マシンとして動作するものを指す場合にも、この語句を使用することができる。

抽象マシンのテストは、さまざまな形式をとることができる。

a) **パワーオンテスト。**下層のプラットフォームの正しい動作を保証するテストである。ハードウェア及びファームウェアの場合は、メモリボード、データパス、バス、制御ロジック、プロセッサのレジスタ、通信ポート、コンソールインタフェース、スピーカ、及び周辺装置といったエレメントのテストを含むかもしれない。ソフトウェアエレメント(仮想マシン)の場合は、正しい初期化及びふるまいの検証が含まれよう。

b) **ロード可能性テスト。**許可利用者がロード及び実行させ、あるいは特定の条件で活性化されるテスト。プロセッサコンポーネントのストレステスト(ロジックユニット、計算ユニットなど)及びメモリ制御が含まれる。

評価者のための注釈

下層の抽象マシンのテストは、TSFが依存する下層の抽象マシンのすべての特性をテストするのに十分なものであるべきである。

FPT_AMT.1　抽象マシンテスト実施

利用者のための適用上の注釈

このコンポーネントは、テストの機能を定期的に呼び出す能力を要求することによって、TSFの操作が依存する下層の抽象マシンのセキュリティ想定の定期的テストに対する支援を提供する。

PP/ST作成者は、その機能が、オフライン、オンライン、あるいはメンテナンスモードで利用可能であるべきかどうかを述べるために、要件を詳細化することができる。

評価者のための適用上の注釈

定期的なテストのための機能は、オフラインあるいはメンテナンスモードでのみ利用可能とすることができる。メンテナンス時、制御は、アクセスを許可利用者に制限するために当を得たものであるべきである。

操作

選択:

FPT_AMT.1.1において、PP/ST作成者は、初期立ち上げ時、通常操作中に定期的に、許可利用者の要求に応じて、あるいはその他の条件で、いつTSFが抽象マシンを実行させるかを特定すべきである。最後の選択肢の場合、PP/ST作成者はそれらの条件が何かを詳細化すべきである。PP/ST作成者は、この選択を通して、自己テストが走る頻度を指示する能力を持つ。テストがしばしば走れば、テストがあまり頻繁に走らないときと比べて*、エンド利用者は、TOEが正しく動作しているという、より大きな信頼を持つはずである。しかしながら、自己テストがTOEの通常動作を遅延させることがしばしばあるので、TOEが正しく動作していることの信頼に対する必要性は、TOEの可用性に対する潜在的な影響とバランスをとらねばならない。 ***(*: 原文は "then" だが、 "than"の間違いと思われる。)***

J.2　フェールセキュア(FPT_FLS)

このファミリの要件は、TSFにおいてある種別の障害が発生したときに、TOEがそのTSPを侵害しないことを保証する。

FPT_FLS.1　セキュアな状態を保持する障害

利用者のための適用上の注釈

「セキュアな状態」という用語は、TSFデータに一貫性があり、TSFがTSPの正しい実施を継続している状態を指す。「セキュアな状態」は、TSPモデルで定義される。もし開発者が、セキュアな状態の明確な定義と、なぜそれがセキュアと考えられるべきかの理由を提供すれば、FPT_FLS.1からADV_SPM.1への依存性が論証できる。

セキュアな状態を保持する障害が発生する状況を監査することが望ましいとはいえ、すべての状況でそれが可能なわけではない。PP/ST作成者は、監査が望まれ、かつ実行可能な状況を特定すべきである。

TSFにおける障害には、「ハード」障害が含まれることがあり、これは機器の不調を示すもので、TSFのメンテナンス、サービス、あるいは修復が必要かもしれない。TSFにおける障害には、回復可能な「ソフト」障害も含まれることがあり、これは、TSFの初期化あるいはリセットだけを必要とするかもしれない。

操作

割付:

FPT_FLS.1.1において、PP/ST作成者は、TSFにおいて、TSFが「フェールセキュア」であるべき、つまり、セキュアな状態を保持し、TSPを正しく実施し続けるべき障害の種別をリストすべきである。

J.3　エクスポートされたTSFデータの可用性(FPT_ITA)

このファミリは、TSF及びリモートの高信頼IT製品間を移動するTSFデータの可用性の損失の防止に対する規則を定義する。このデータは、パスワード、鍵、監査データ、あるいはTSF実行コードのようなTSFの機密上重要なデータなどである。

利用者のための適用上の注釈

このファミリは、TSFがTSFデータをリモートの高信頼IT製品に提供している分散システムを背景として使用される。TSFは、そのサイトにおいての処置を講じられるだけで、他方の高信頼IT製品のTSFに対しては責任を持つことができない。

もし、さまざまな種別のTSFデータに対してさまざまの利用可能な尺度が存在する場合は、TSFデータの尺度と種別の一意の組み合わせごとに、このコンポーネントが繰り返されるべきである。

FPT_ITA.1　**定義された可用性尺度内のTSF間可用性**

操作

割付:

FPT_ITA.1.1において、PP/ST作成者は、可用性尺度の対象となるTSFデータの種別を特定すべきである。

FPT_ITA.1.1において、PP/STは、適用可能なTSFデータに対する可用性尺度を特定すべきである。

FPT_ITA.1.1において、PP/ST作成者は、可用性が保証されねばならない条件を特定すべきである。例: TOEとリモートの高信頼IT製品間にコネクションがなければならない。

J.4　エクスポートされたTSFデータの機密性(FPT_ITC)

このファミリは、TSFとリモートの高信頼IT製品間で移動するTSFデータの許可されない暴露からの保護に対する規則を定義する。このデータの例として、パスワード、鍵、監査データ、あるいはTSF実行コードのようなTSFの機密上重要なデータがある。

利用者のための適用上の注釈

このファミリは、TSFがTSFデータをリモートの高信頼IT製品に提供している分散システムを背景として使用される。TSFは、そのサイトにおいての処置を講じられるだけで、他方の高信頼IT製品のTSFに対しては責任を持つことができない。

FPT_ITC.1　**送信中のTSF間機密性**

評価者のための適用上の注釈

送信中のTSFデータの機密性は、そのような情報を暴露から保護するために必要である。機密性を提供できるような実装としては、スプレッドスペクトラム技術はいうまでもなく、暗号アルゴリズムの使用が含まれる。

J.5　エクスポートされたTSFデータの完全性(FPT_ITI)

このファミリは、TSFとリモートの高信頼IT製品間で送信中のTSFデータの、許可されない改変からの保護に対する規則を定義する。このデータの例として、パスワード、鍵、監査データ、あるいはTSF実行コードのようなTSFの機密上重要なデータがある。

利用者のための注釈

このファミリは、TSFがTSFデータをリモートの高信頼IT製品と交換する分散システムの背景において使用される。リモートの高信頼IT製品がそのデータを保護するために使用するメカニズムは前もって判断できないので、リモートの高信頼IT製品における改変、検出、あるいは回復に対応する要件は特定できないことに注意がいる。この理由のために、これらの要件は、リモートの高信頼IT製品が使用できる「TSF提供の能力」という用語で表現される。

FPT_ITI.1　TSF間改変の検出

利用者のための適用上の注釈

このコンポーネントは、いつデータが改変されたかを検出するので十分な状況において使われるべきである。そのような状況の例は、改変が検出された場合にリモートの高信頼IT製品がTOEのTSFにデータの再送を要求できる状況、あるいはそのような種別の要求に応答できる状況である。

改変の検出に望まれる強度は、使用されたアルゴリズムの機能である特定された改変尺度に基づき、その機能は、複数ビットの変化の検出に失敗するかもしれない弱いチェックサム及びパリティメカニズムから、もっと複雑な暗号チェックサムのアプローチまでの幅を持つ。

操作

割付:

FPT_ITI.1.1において、PP/STは、検出メカニズムが満たさねばならない改変尺度を特定すべきである。この改変尺度は、改変検出の望まれる強度を特定しなければならない。

FPT_ITI.1.2において、PP/STは、もしTSFデータの改変が検出されたらとられるべきアクションを特定すべきである。アクションの例: 「そのTSFデータを無視し、送信元の高信頼製品にそのTSFデータの再送を要求する」。

FPT_ITI.2　TSF間改変の検出と訂正

利用者のための適用上の注釈

このコンポーネントは、TSFの機密上重要なデータの改変に対する検出あるいは訂正が必

要な状況において使用されるべきである。

改変の検出に望まれる強度は、使用されたアルゴリズムの機能である特定された改変尺度に基づき、その機能は、複数ビットの変化の検出に失敗するかもしれないチェックサム及びパリティメカニズムから、もっと複雑な暗号チェックサムのアプローチまでの幅を持つ。定義する必要のある尺度は、それが抵抗する攻撃(例えば、1000個のランダムなメッセージのから一つだけを受け入れる)、あるいは公の文献で広く知られたメカニズム(例えば、強度はセキュアハッシュアルゴリズムが提供する強度に準じなければならない)を参照することができる。

改変を訂正するためにとられるアプローチは、誤り是正チェックサムの様式などを通して行われよう。

評価者のための注釈

この要件を満たす手段として、暗号機能あるいは何らかのチェックサムの様式の使用を必要とするものが考えられる。

操作

割付:

FPT_ITI.1.1において、PP/STは、検出メカニズムが満たさねばならない改変尺度を特定すべきである。この改変尺度は、改変検出の望まれる強度を特定しなければならない。

FPT_ITI.1.2において、PP/STは、もしTSFデータの改変が検出されたらとられるべきアクションを特定すべきである。アクションの例: 「そのTSFデータを無視し、送信元の高信頼製品にそのTSFデータの再送を要求する」。

FPT_ITI.2.3において、PP/ST作成者は、TSFがその改変から回復する能力を持つべき改変の種別を定義すべきである。

J.6　TOE内TSFデータ転送(FPT_ITT)

このファミリは、TSFデータが内部チャネルを介してTOEの分離したパート間を転送されるとき、そのTSFデータの保護に対応する要件を提供する。

利用者のための注釈

このファミリの適用を有効なものにする分離(すなわち、物理的あるいは論理的)の度合いの判断は、意図する使用環境に依存する。敵対的環境では、システムバスあるいはプロセス間通信チャネルだけで分離したTOEのパート間の転送から生じる危険があるかもしれない。もっと穏やかな環境では、従来のネットワーク媒体を使って転送が行える。

評価者のための注釈

この保護を提供するためにTSFが利用可能な実用的メカニズムの一つは、暗号技術に基づくものである。

FPT_ITT.1　**基本TSF内データ転送保護**

操作

選択:

FPT_ITT.1.1において、PP/ST作成者は、選択候補(暴露、改変)から提供されるべき望ましい保護の種別を特定すべきである。

FPT_ITT.2　**TSFデータ転送分離**

利用者のための適用上の注釈

SFP関連属性に基づくTSFデータの分離を達成する方法の一つは、分離した論理または物理チャネルの使用によるものである。

操作

選択:

FPT_ITT.2.1*において、PP/ST作成者は、選択候補(暴露、改変)から提供されるべき望ましい保護の種別を特定すべきである。 *(原文では "FPT_ITT.1.1" となっているが、明らかに "2.1" の間違いである。)*

FPT_ITT.3　**TSFデータ完全性監視**

操作

選択:

FPT_ITT.3.1において、PP/ST作成者は、TSFが検出できねばならない改変の望ましい種別を特定すべきである。PP/ST作成者は、以下から選択すべきである:

データの改変、データの置換、データの順序変更、データの削除、あるいはその他すべての完全性誤り。

割付:

FPT_ITT.3.1において、もしPP/ST作成者は、前の段落において注釈された最後の選択を選ぶ場合、作成者は、TSFが検出の能力を持つべきそれらの他の完全性誤りが何であるかについても特定すべきである。

FPT_ITT.3.2において、PP/ST作成者は、完全性誤りが識別されたときにとられるアクションを特定すべきである。

J.7　TSF物理的保護(FPT_PHP)

TSF物理的保護コンポーネントは、TSFに対する許可されない物理的アクセスにおける制約、及び許可されない物理的改変の抑止及び抵抗、あるいはTSFの置換に関係する。

このファミリにおける要件は、TSFが物理的な改ざん及び干渉から保護されることを保証する。それらのコンポーネントの要件を満たすことは、物理的な改ざんが検出可能であるような、あるいは定義されたワークファクタに基づき物理的改ざんに対する抵抗が計測可能であるような仕方で、TSFがパッケージ化され使用されることになる。物理的な損害を防げない環境では、これらのコンポーネントなしではTSFの保護機能は有効性を失う。このコンポーネントは、また、物理的な改ざんの試みに対してTSFがどのように応答しなければならないかに関する要件も提供する。

物理的改ざんのシナリオの例として、機械的な攻撃、放射線、温度を変える、などがある。

利用者のための注釈

許可利用者が物理的な改ざんの検出に利用できる機能は、オフラインあるいはメンテナンスモードでだけ利用できるものであってよい。そのようなモードの場合は、アクセスを許可利用者に制限するよう、適切な制御がなされるべきである。そのようなモードの場合は、TSFが「動作可能」でないかもしれないので、許可利用者のアクセスに対する通常の処理を提供できないかもしれない。TOEの物理的な実装は、いくつかの構造体から構成されよう: 例えば、外部シールド、カード、及びチップ。この「エレメント」のセットは、全体として、TSFを物理的な改ざんから保護(保護、通知、及び抵抗)しなければならない。すべてのデバイスがこれらの特質を提供しなければならないわけではなく、全体として、完全な物理的構成となるべきである。

これらのコンポーネントに関係しては最小限の監査があるだけだが、これは単に、監査サブシステムとの対話レベルの下で、検出及び警報メカニズムが完全にハードウェアに実装されるかもしれないという可能性のためである(例えば、許可利用者がボタンを押したときに回路が切断されるものとすれば、回路の切断と発光ダイオード(LED)の点灯に基づくハードウェアベースの検出システム)。とは言え、PP/ST作成者は、特別の脅威が予期される環境に対して、物理的な改ざんを監査する必要があると判断するかもしれない。このような場合、PP/ST作成者は、監査事象のリストに適切な要件を含めるべきである。これらの要件を含めることは、ハードウェア設計とソフトウェアに対するそれのインタフェースに、密接な係わり合いを持つかもしれないことに注意。

FPT_PHP.1　**物理的攻撃の受動的検出**

利用者のための適用上の注釈

FPT_PHP.1は、TOEのパートに対する許可されない物理的な改ざんの脅威が手続き的方法では対抗できないときに使用されるべきである。それは、TSFに対する検出されない物理的改ざんの脅威に対応する。典型的に、許可利用者は、改ざんが行われたかどうかを検

証するための機能を与えられる。文字通り、このコンポーネントは、単にTSFに改ざんを検出する能力を提供するだけである。FMT_MOF.1に対する依存性は、誰がその能力を使用できるようにするか、及び彼らがどのようにその能力を使用できるようにするかを特定するために要求される。もしこの機能が非ITメカニズム(物理的な検査など)で実現される場合は、FMT_MOF.1に対する依存性が満たされないことが正当化されよう。

FPT_PHP.2　**物理的攻撃の通知**

利用者のための適用上の注釈

TOEのパートに対する許可されない物理的改ざんからの脅威が手続き的方法によって対抗されず、指示された個々人に物理的改ざんを通知することが要求されるとき、FPT_PHP.2が使用されるべきである。これは、TSFエレメントに対する物理的改ざんが検出されたとしても、それが通知されないかもしれないという脅威に対応する。

操作

割付:

FPT_PHP.2.3に対して、PP/ST作成者は、物理的改ざんのアクティブな検出が要求されるTSFデバイス/エレメントのリストを提供すべきである。

FPT_PHP.2.3において、PP/ST作成者は、改ざんが検出されたときに通知されるべき利用者あるいは役割を指示すべきである。利用者あるいは役割の種別は、PP/STに含まれる個々のセキュリティ管理コンポーネント(FMT_MOF.1ファミリの)に依存して異なってよい。

FPT_PHP.3　**物理的攻撃への抵抗**

改ざんの形態によっては、TSFは改ざんを検出するだけでなく、実際にそれに抵抗する、あるいは攻撃者の行為の進行を妨げることが必要になる。

利用者のための適用上の注釈

このコンポーネントは、TSFデバイスあるいはTSFエレメントが、TSFデバイスの内部、あるいはTSFエレメント自体の物理的改ざん(例えば、観察、分析、あるいは改変)が脅威となる環境で動作することが予期される場合に使用されるべきである。

操作

割付:

FPT_PHP.3.1に対して、PP/ST作成者は、TSFがそれの物理的改ざんに抵抗すべきTSFデバイス/エレメントのリストについて、改ざんのシナリオを特定すべきである。このリストは、デバイスの技術上の制限及び関係する物理的露出などを十分に考慮したTSFの物理的デバイス及びエレメントの定義されたサブセットに適用できる。このようなサブセット化は、明確に定義され正当化され

るべきである。さらに、TSFは、物理的改ざんに自動的に応答すべきである。自動的応答は、そのデバイスの方針が保持されるべきものである; 例えば、機密性の方針に関して、保護された情報が読み出せないようデバイスを物理的に非活性化するというものが相当する。

FPT_PHP.3.1において、PP/ST作成者は、すでに識別されたシナリオにおける、TSFが物理的改ざんに抵抗すべきTSFデバイス/エレメントのリストを特定すべきである。

J.8　高信頼回復(FPT_RCV)

このファミリの要件は、TOEが保護の危殆化なしに立ち上げられること、及び動作の中断後に保護の危殆化なしに回復できることをTSFが判断できることを保証する。このファミリが重要なのは、TSFの立ち上げ状態が、それに続く状態の保護を決めるからである。

回復コンポーネントは、予想される障害、動作の中断、あるいは立ち上げの発生に対する直接の応答として、TSFのセキュアな状態を再構築し、あるいはセキュアでない状態への移行を防ぐ。一般的に予期しなければならない障害には、次のようなものがある。

a) 常にシステムクラッシュにつながる阻止できないアクション障害(例えば、重要なシステムテーブルの継続的矛盾、ハードウェアあるいはファームウェアの一時的障害、電源障害、プロセッサ障害、通信障害によって発生するTSFコード内の制御されない転送)。

b) TSFオブジェクトを表す媒体の一部または全部をアクセス不能にし、あるいは壊す媒体障害(例えば、パリティ誤り、ディスクヘッドのクラッシュ、位置ずれしたディスクヘッドが引き起こす継続的な読み出し/書き込み障害、磨耗した磁気コーティング、ディスク表面のゴミ)

c) 間違った管理上のアクション、あるいはタイムリな管理上のアクションの欠如によって引き起こされる動作の中断(例えば、電源オフによる予期しないシャットダウン、重要な資源の枯渇の無視、設置された設定が不適切)

回復は、全体あるいは部分的障害シナリオのどちらからのものでもよいことに注意。全体障害は、一体構造のオペレーティングシステムで発生し得るが、分散環境ではあまり起きることはない。そのような環境では、サブシステムが障害になるかもしれないが、他の部分は動作可能のままである。さらに、重要なコンポーネントは冗長であるかもしれず(ディスクのミラーリング、代替ルート)、かつチェックポイントが利用可能かもしれない。そのため、回復とは、セキュアな状態への回復と表現される。

このファミリはメンテナンスモードを識別する。このメンテナンスモードでは、通常の動作が不可能であるか、あるいは厳しく制限されるであろうが、それは、そうしないと、セキュアでない状況が生じ得るからである。典型的には、許可利用者だけがこのモードへのアクセスを許されるべきであるが、誰がこのモードにアクセスできるかの実際の詳細は、FMTセキュリティ管理クラスの機能である。もしFMTが、誰がこのモードをアクセスできるかについて何の制御もしないとすれば、TOEがそのような状態になった場合に、どの利用者でもシステムの回復を許可されることが受け入れられることになる。しかしながら、利用者がシステムを修復することは、TSPが侵害されるような方法でTOEを設定する機会を持つことになるので、実際には、これはたぶん望ましくないであろう。

動作時の例外条件を検出するよう設計されたメカニズムは、FPT_TST(TSF自己テスト)、FPT_FLS(フェールセキュア)、及び「ソフトウェアの安全性」の概念に対応する、他の

領域の管轄である。

利用者のための注釈

このファミリ全体で、「セキュアな状態」という語句が使用される。これは、TOEが、一貫したTSFデータ及び正しく方針を実施できるTSFを持つ状態を指す。この状態は、クリーンなシステムの初期「ブート」であってもよく、あるいは、何らかのチェックポイント状態でもよい。「セキュアな状態」は、TSPモデルで定義する。開発者が、セキュアな状態の明確な定義と、なぜそれがセキュアとみなされるべきかの理由を提供すれば、FPT_FLS.1からADV_SPM.1への依存性を論証することができる。

FPT_RCV.1　**手動回復**

高信頼回復ファミリの階層構成において、手動の介入だけを要求する回復は、無人操作方式のシステムの使用を排除することになり、最も好ましくない。

利用者のための適用上の注釈

このコンポーネントは、セキュアな状態へ無人で回復することを要求しないTOEにおける使用を意図したものである。このコンポーネントの要件は、障害あるいは他の中断からの回復後、有人のTOEがセキュアでない状態に戻ることから生じる保護の危殆化の脅威を低減する。

評価者のための適用上の注釈

高信頼回復に対して許可利用者が利用できる機能が、メンテナンスモードでだけ利用可能であることは許容できる。制御は、メンテナンスモード時に、アクセスを許可利用者に制限するのに適切なものであるべきである。

FPT_RCV.2　**自動回復**

自動回復は、マシンが無人操作方式で動作するのを認めるので、手動回復よりも便利であると考えられる。

利用者のための適用上の注釈

コンポーネントFPT_RCV.2は、障害あるいはサービス中断からの自動化された回復方法が少なくとも一つ存在することを要求することによって、FPT_RCV.1の特質のカバレジを拡張する。これは、障害あるいは他の中断からの回復後、無人のTOEがセキュアでない状態に戻ることから生じる保護の危殆化の脅威に対応する。

評価者のための適用上の注釈

高信頼回復に対して許可利用者が利用できる機能が、メンテナンスモードでだけ利用可能であることは許容できる。制御は、メンテナンスモード時に、アクセスを許可利用者に制限するのに適切なものであるべきである。

FPT_RCV.2.1に対して、回復可能な障害及びサービス中断のセットを決定するのは、

TSFの開発者の責任である。

自動回復メカニズムの堅牢性が検証されることが前提とされる。

操作

割付:

FPT_RCV.2.2に対して、PP/ST作成者は、それに対して自動回復が可能でなければならない障害及び他の中断のリストを特定すべきである。

FPT_RCV.3　**過度の損失のない自動回復**

自動回復は、手動回復よりも便利であると考えられるが、実際の多数のオブジェクトを失う危険を招く。オブジェクトの過度の損失を防ぐことは、回復作業のために付加的な効用を提供する。

利用者のための適用上の注釈

コンポーネントFPT_RCV.3は、TSC内のTSFデータあるいはオブジェクトの過度の損失がないことを要求することで、FPT_RCV.2の特質のカバレジを拡張する。FPT_RCV.2では、自動回復メカニズムは、おそらく、オブジェクトをすべて削除し、既知のセキュアな状態にTSFを戻すことで回復できよう。この種の荒っぽい自動回復は、FPT_RCV.3では除外される。

このコンポーネントは、TSC内のTSFデータあるいはオブジェクトの大きな損失を伴う障害あるいは他の中断からの回復後、無人のTOEがセキュアでない状態に戻ることから生じる保護の危殆化の脅威に対応する。

評価者のための適用上の注釈

高信頼回復に対して許可利用者が利用できる機能が、メンテナンスモードでだけ利用可能であることは許容できる。制御は、メンテナンスモード時に、アクセスを許可利用者に制限するのに適切なものであるべきである。

自動回復メカニズムの堅牢性が検証されることが想定される。

操作

割付:

FPT_RCV.3.2に対して、PP/ST作成者は、それに対して自動回復が可能でなければならない障害及び他の中断のリストを特定すべきである。

FPT_RCV.3.3に対して、PP/ST作成者は、許容し得る、TSFデータあるいはオブジェクトの損失量を数値化したものを提供すべきである。

FPT_RCV.4　**機能回復**

機能回復は、TSF内で障害が発生したとしても、TSF内の所定のSFが成功裏に完了するか、あるいはセキュアな状態に回復することを要求する。

操作

割付:

FPT_RCV.4.1において、PP/ST作成者は、SF及び障害シナリオのリストを特定すべきである。識別されたどの障害シナリオが発生した場合でも、特定されたSFは、成功裏に完了するか、あるいは一貫しかつセキュアな状態に回復しなければならない。

J.9 **リプレイ検出**(FPT_RPL)

このファミリは、さまざまな種別のエンティティに対するリプレイの検出と、それに続く訂正のためのアクションに対応する。

FPT_RPL.1 **リプレイ検出**

利用者のための適用上の注釈

ここに含まれるエンティティには、例えば、メッセージ、サービス要求、サービス応答、あるいはセションなどがある。

操作

割付:

FPT_RPL.1.1において、PP/ST作成者は、それに対するリプレイの検出が可能であるべき、識別されたエンティティのリストを提供すべきである。そのようなエンティティの例として、メッセージ、サービス要求、サービス応答、及び利用者セションなどがある。

FPT_RPL.1.2において、PP/ST作成者は、リプレイの検出時にTSFによってとられるべきアクションのリストを特定すべきである。とられ得るアクションのセットとして可能性があるもの: リプレイされたエンティティを無視する、識別された発信源にエンティティの確認を要求する、リプレイされたエンティティを発信したサブジェクトを終了する。

J.10 **リファレンス調停**(FPT_RVM)

このファミリのコンポーネントは、従来のリファレンスモニタの「常に呼び出された」側面に対応する。これらのコンポーネントの目標は、TSCに関して、そのSFPによって制御されるオブジェクトに対し、そのSFPのなんらかあるいはすべてに関して信頼できないサブジェクトが呼び出す方針の実施を要求するすべてのアクションが、そのSFPに対するTSFによって確認されることを保証することである。SFPを実施するTSFの部分がFPT_SEP(ドメイン分離)及びADV_INT(TSF内部機能)の適切なコンポーネントの要件も満たすならば*、TSFのその部分は、そのSFPに対する「リファレンスモニタ」を提供する。 (*: *原文では接続詞の"than"が使われているが、"then"の間違いと思われる。*)

リファレンスモニタは、TSPの実施に対して責任を持つTSFのその部分である。それは、次の3つの特性を持つ:

a) 信頼できないサブジェクトはその動作に干渉できない; すなわち、それは改ざん不可である。これは、FPT_SEPファミリのコンポーネントによって対応される。

b) 信頼できないサブジェクトはそのチェックをバイパスできない; すなわち、それは常に呼び出されている。これは、FPT_RVMファミリのコンポーネントによって対応される。

c) それは分析するには十分に単純であり、ふるまいはあらかじめ知られている(すなわち、その設計は概念的に単純)。これは、ADV_INTファミリのコンポーネントで対応される。

このコンポーネントは、「TSFは、TSC内の各々かつすべての機能が進行を許可される前に、TSP実施機能が呼び出され成功することを保証する」と述べている。どのようなシステムにおいても(分散型であってもそうでなくても)、TSPの実施に責任を持つ機能の数は有限である。この要件の中に、セキュリティを取り扱うために単一の機能が呼び出されることを必須とし、あるいは規定するものはない。むしろ、複数の機能がリファレンスモニタの役割を満たすことを許しており、TSPの実施に責任を持つそれらの集合が、単純に、集合的に、リファレンスモニタと呼ばれる。しかしながら、これは、「リファレンスモニタ」を単純なものに保つという目標によって、バランスされねばならない。

SFPのある部分、あるいはすべてに関して信頼できないサブジェクトによって要求されるすべての実施可能アクション(例えば、オブジェクトへのアクセス)について、それが成功する前にTSFによって確認された場合、かつその場合だけ、そのSFPを実現するTSFは、許可されない機能に対する有効な保護を提供する。もし実施可能アクションが不正確に実施され、あるいはバイパスされた場合は、SFPの実施全体が危殆化する。「信頼できない」サブジェクトは、さまざまの許可されない方法でSFPをバイパスできよう(例えば、あるサブジェクトあるいはオブジェクトに対するアクセスチェックを回避、アプリケーションによって保護されるという想定のオブジェクトに対するチェックをバイパス、意図

する寿命を超えてアクセス権を保持、監査されるアクションの監査をバイパス、あるいは認証をバイパス)。「信頼できないサブジェクト」という用語は、実施される特定のSFPのどれか、あるいはすべてに関して信頼できないサブジェクトを指す。あるサブジェクトは、一つのSFPに関しては信頼でき、別のSFPに関しては信頼できないかもしれない。

FPT_RVM.1　TSPの非バイパス性

利用者のための適用上の注釈

リファレンスモニタに相当するものを得るため、このコンポーネントは、FPT_SEP.2(SFPドメイン分離)、あるいはFPT_SEP.3(完全リファレンスモニタ)、及びADV_INT.3(複雑さの最小化)と一緒に使用されねばならない。さらに、完全なリファレンス調停が要求されれば、FDPクラス 利用者データ保護のコンポーネントが、すべてのオブジェクトをカバーしなければならない。

J.11　ドメイン分離(FPT_SEP)

このファミリのコンポーネントは、少なくとも一つのセキュリティドメインがTSF自身の実行のために利用可能で、かつ、信頼できないサブジェクトによる外部の干渉及び改ざん(例えば、TSFコードあるいはデータ構造の改変による)からTSFが保護されることを保証する。このファミリの要件を満たすことは、TSFを自己防衛的にする。これは、信頼できないサブジェクトがTSFを改変したり損害を与えることができないことを意味する。

このファミリは、以下を要求する:

a) TSFのセキュリティドメイン(「保護ドメイン」)の資源、及びそのドメインの外部にあるサブジェクト及び制約を受けないエンティティの資源は、保護ドメインの外部にあるエンティティが保護ドメインの内部にあるデータ構造あるいはコードを観察あるいは改変できないように分離される。

b) ドメイン間のサブジェクトの転送は、保護ドメインへの自由な出入りができないよう制御される。

c) 保護ドメインにアドレスで渡される利用者あるいはアプリケーションパラメタは、保護ドメインのアドレス空間について確認され、かつ、値で渡されるそれは、保護ドメインが予期する値について確認される。

d) 各サブジェクトの各セキュリティドメインは、TSFによって制御される共有を除き、各々異なる。

利用者のための注釈

このファミリは、TSFが破壊されていないことの確信が要求される場合には、いつでも必要となる。

リファレンスモニタに相当するものを得るため、このファミリのコンポーネントFPT_SEP.2(SFPドメイン分離)、あるいはFPT_SEP.3(完全リファレンスモニタ)が、FPT_RVM.1(TSPの非バイパス性)、及びADV_INT.3(複雑さの最小化)と一緒に使用されねばならない。さらに、完全なリファレンス調停が要求されれば、FDPクラス 利用者データ保護のコンポーネントが、すべてのオブジェクトをカバーしなければならない。

FPT_SEP.1　TSFドメイン分離

TSFのための分離した保護ドメインなしでは、TSFが、信頼できないサブジェクトによるどんな改ざん攻撃の対象にもなっていないという保証はあり得ない。そのような攻撃は、TSFコード及び/またはTSFデータ構造の改変を伴うかもしれない。

FPT_SEP.2　SFPドメイン分離

TSFが提供する最も重要な機能は、そのSFPの実施である。設計を単純にし、重要なSFPがリファレンスモニタ(RM)の性質(特に、改ざん不可であること)を現す公算を大きくする

ため、それらは、TSFの残りの部分から区別されたドメインになければならない。

評価者のための適用上の注釈

階層型設計におけるリファレンスモニタはSFPの機能を超える機能を提供してもよい、とすることが可能である。これは、階層型ソフトウェア設計の実用的な性質から生じる。目標は、非SFP関連機能を最小化することであるべきである。

リファレンスモニタにとって、含まれるすべてのSFPに対して、複数のリファレンスモニタドメイン(各々が一つあるいは複数のSFPを実施する)を持つのはもちろん、単一の区別されたリファレンスモニタドメイン内に置かれることが許容されることに注意。もしSFPに対して複数のリファレンスモニタドメインが存在する場合、それらは、互いに対等であることも、階層的な関係であることも許容される。

FPT_SEP.2.1について、「TSFの分離できない部分」という用語は、TSFにおける、FPT_SEP.2.3によってカバーされない機能からなるTSFの部分を指す。

操作

割付:

FPT_SEP.2.3に対して、PP/ST作成者は、一つの分離したドメインを持つべきTSPにおけるアクセス制御及び/または情報フロー制御SFPを特定すべきである。

FPT_SEP.3　完全リファレンスモニタ

TSFが提供する最も重要な機能は、そのSFPの実施である。このコンポーネントは、すべてのアクセス制御及び/または情報フロー制御SFPが、TSFの残りの部分と区別されるドメインにおいて実施されるのを要求するということで、先行するコンポーネントの意図を踏まえたものである。これは、さらに設計を単純化し、リファレンスモニタ(RM)の特性(特に、改ざん不可であること)がTSF中に見られる公算を大きくする。

評価者のための適用上の注釈

階層型設計におけるリファレンスモニタはSFPの機能を超える機能を提供してもよい、とすることが可能である。これは、階層型ソフトウェア設計の実用的な性質から生じる。目標は、非SFP関連機能を最小化することであるべきである。

リファレンスモニタにとって、含まれるすべてのSFPに対して、複数のリファレンスモニタドメイン(各々が一つあるいは複数のSFPを実施する)を持つのはもちろん、単一の区別されたリファレンスモニタドメイン内に置かれることが許容されることに注意。もしSFPに対して複数のリファレンスモニタドメインが存在する場合、それらは、互いに対等であることも、階層的な関係であることも許容される。

J.12　状態同期プロトコル(FPT_SSP)

分散システムは、システムのパート間において状態の相違が生じる可能性及び通信の遅延によって、一体構造のシステムに比べて複雑さが増大するかもしれない。ほとんどの場合、分散機能間の状態の同期は、単純なアクションではなく、交換プロトコルを用いる。これらのプロトコルの分散環境に悪意が存在する場合、より複雑な防御プロトコルが要求される。

FPT_SSPは、TSFのある機密上重要なセキュリティ機能に対して、高信頼プロトコルを使用する要件を制定する。FPT_SSPは、TOEの二つの分散したパート(例えばホスト)が、セキュリティ関連のアクション後に、それらの同期した状態を持つことを保証する。

利用者のための注釈

ある状態は同期できないかもしれず、あるいは、実用上、トランザクションコスト高すぎるかもしれない; 暗号鍵廃棄が一例であり、そこでは、廃棄アクションが起動された後の状態を知ることができない。アクションはとられたが確認を送ることができないのか、あるいは敵対的な通信相手によってメッセージが無視され廃棄が行われないのか。不確定性は、分散システムに固有のものである。不確定性と状態同期は関係しており、同じ解決方法が適用できるかもしれない。不確定な状態に対する設計を行うのは無駄である; PP/ST作成者は、そのような場合、他の要件(例えば、警報を発生する、事象を監査する)を表すべきである。

FPT_SSP.1　単純信頼肯定応答

利用者のための適用上の注釈

このコンポーネントでは、TSFは、要求されたときにTSFの他のパートに肯定応答を与えねばならない。この肯定応答は、分散TOEの一つのパートが、分散TOEの別のパートから改変されていない送信を正常に受信したことを示すべきである。

FPT_SSP.2　相互信頼肯定応答

利用者のための適用上の注釈

このコンポーネントにおいて、TSFがデータ送信の受信に対する肯定応答を提供できることに加え、TSFは、TSFの他のパートからの、肯定応答に対する肯定応答の要求に応じられなければならない。

例えば、ローカルTSFがTSFのリモートパートにデータを送信する。TSFのリモートパートは、そのデータの正常受信に肯定応答し、送信TSFに対して肯定応答を受信したことを確認することを要求する。このメカニズムは、データ送信に関与したTSFの両方のパートが送信が正常に完了したこと知るという、付加的な確証を提供する。

J.13　**タイムスタンプ**(FPT_STM)

このファミリは、TOE内の高信頼タイムスタンプ機能に対する要件に対応する。

利用者のための注釈

「高信頼タイムスタンプ」という用語の意味を明確にすること、及び信頼の受入れを決定する責任がどこにあるかを示すことは、PP/ST作成者の責任である。

FPT_STM.1　**高信頼タイムスタンプ**

利用者のための適用上の注釈

このコンポーネントが使えそうなものとして、セキュリティ属性の有効期限に対してはもちろん、監査目的のための高信頼タイムスタンプの提供というものがある。

J.14　TSF間TSFデーター貫性(FPT_TDC)

分散あるいは複合システム環境において、TOEは他の高信頼IT製品とTSFデータ(例えば、データに関連したSFP属性、監査情報、識別情報)を交換する必要があるかもしれない。このファミリは、TOEのTSFと、別の高信頼IT製品のTSFとの間で、これら属性の共有及び一貫した解釈のための要件を定義する。

利用者のための注釈

このファミリにおけるコンポーネントは、TOEのTSFと他の高信頼IT製品の間でTSFデータを送信するとき、TSFデータの一貫性に対する自動化されたサポートのための要件を提供する。全面的に手続き的な方法でセキュリティ属性の一貫性を作り出せるという可能性もあるが、それらは、ここでは提供されない。

このファミリは、FDP_ETC及びFDP_ITCと異なっており、それは、これら二つのファミリが、TSFとそのインポート/エクスポート媒体間のセキュリティ属性の問題解決だけに関与しているためである。

TSFデータの完全性に関心が置かれるのであれば、FPT_ITIファミリから要件を選択すべきである。これらのコンポーネントは、通過するTSFデータの改変をTSFが検出かつ訂正できる要件を特定する。

FPT_TDC.1　TSF間基本TSFデーター貫性

利用者のための適用上の注釈

TSFは、特定された機能によって使われあるいは関係し、かつ二つあるいはそれ以上の高信頼システム間で共通である、TSFデータの一貫性の維持に責任を持つ。例えば、二つの異なるシステムのTSFデータは、内部的に異なる使われ方をしているかもしれない。TSFデータが受信側高信頼IT製品で適切に使用されるためには(例えば、利用者データにTOEの内部と同じ保護を与えるため)、TOEと他の高信頼IT製品は、TSFデータ交換のための事前に確立されたプロトコルを使わねばならない。

操作

割付:

FPT_TDC.1.1において、PP/ST作成者は、TSFと他の高信頼IT製品の間で共有されるときに、それに対して一貫性のある解釈をする能力をTSFが提供すべき、TSFデータの種別のリストを定義すべきである。

FPT_TDC.1.2において、PP/STは、TSFによって適用されるべき解釈規則のリストを割り付けるべきである。

J.15　TOE内TSFデータ複製一貫性(FPT_TRC)

このファミリの要件は、TSFデータがTOEの内部で複製されるときに、その一貫性を保証するために必要になる。もしTOEのパート間の内部チャネルが動作不能になると、そのようなデータは一貫性をなくすかもしれない。もしTOEの内部がTOEのパートをネットワーク化した形で構成されていると、パートが非活性化されたとき、ネットワーク接続が切れたときなどに、これが発生し得る。

利用者のための注釈

一貫性を保証する方法は、このコンポーネントでは特定されない。トランザクションロギングの形で(適切なトランザクションが、再接続時にサイトへ「ロールバック」される)達成できることがあり; 複製されたデータを同期プロトコルによって更新することもある。もし特定のプロトコルがPP/STに必要であれば、それは、詳細化によって特定することができる。

ある状態を同期させることは不可能かもしれず、あるいはそのような同期のコストが高すぎるかもしれない。この状況の例は、通信チャネルと暗号鍵廃棄である。また、不確定状態も発生するかもしれない; もし特定のふるまいが望ましければ、それは、詳細化によって特定されるべきである。

FPT_TRC.1　TSF内一貫性

操作

割付:

FPT_TRC.1.2において、PP/ST作成者は、TSFデータ複製一貫性に依存するSFのリストを特定すべきである。

J.16　TSF自己テスト(FPT_TST)

このファミリは、期待される正しい動作に関して、TSFを自己テストするための要件を定義する。例は、実施機能に対するインタフェースや、TOEの機能上重要なパートにおけるサンプル算術演算などである。これらのテストは、立ち上げ時・定期的に・許可利用者の要求によって・あるいは他の条件が満たされたときに実行されることができる。自己テストの結果としてTOEによって取られるアクションは、他のファミリで定義される。

このファミリの要件は、TOEの動作(他のファミリで扱われよう)を必ず止めるとは限らないさまざまな障害による、TSF実行コード(すなわちTSFソフトウェア)及びTSFデータの破壊を検出するためにも必要とされる。これらの障害を必ず防げるとは限らないので、これらのチェックが実行されねばならない。このような障害は、ハードウェア・ファームウェア・あるいはソフトウェアの設計における予見できない障害モード、あるいは関連する不注意のために、あるいは不適切な論理的及び/または物理的保護に起因する、TSFの悪意の破壊のために生じ得る。

加えて、適切な条件でこのコンポーネントを使用することは、メンテナンスアクティビティの結果として、不適切な、あるいは損害を与えるTSF変更が動作中のTOEに適用されるのを防ぐのに役立つかもしれない。

利用者のための注釈

「TSFの正しい動作」という用語は、主として、TSFソフトウェアの動作とTSFデータの完全性を指す。TSFソフトウェアが実装される抽象マシンは、FPT_AMTへの依存性を介してテストされる。

FPT_TST.1　TSFテスト

利用者のための適用上の注釈

このコンポーネントは、テスト機能を呼び出し、かつTSFデータと実行コードの完全性をチェックする能力を要求することによって、TSFの動作の重要な機能をテストすることに対するサポートを提供する。

評価者のための適用上の注釈

定期的テストのために許可利用者が利用できる機能について、オフラインあるいはメンテナンスモードでだけ利用可能であることは受容できる。これらのモードのとき、アクセスを許可利用者に限定するために、制御がなされるべきである。

操作

選択:

FPT_TST.1において、PP/ST作成者は、TSFがTSFテストをするときを特定すべきである; 初期立ち上げ時、通常動作中に定期的に、許可利用者の要求に応じ

て、他の条件で。また、最後の選択肢において、PP/ST作成者は、次の割付を通して、それらの条件が何であるかを割り付けるべきである。

割付:

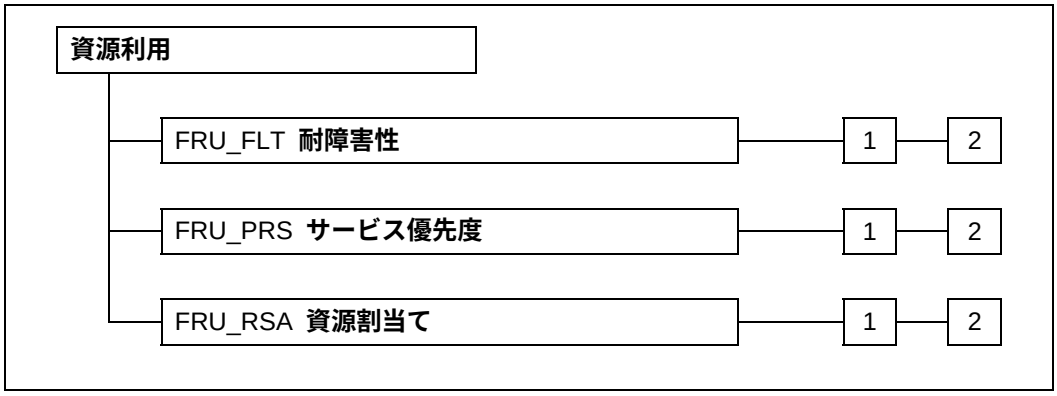
FPT_TST.1.1において、もし選択されれば、、PP/ST作成者は、自己テストが行われるべき条件を特定すべきである。

附属書K

(参考)

資源利用(FRU)

このクラスは、処理能力及び/または格納容量のような、要求される資源の可用性をサポートする三つのファミリを提供する。耐障害性ファミリは、TOEの障害によって引き起こされる、能力の利用不可に対する保護を提供する。サービス優先度ファミリは、資源が、より重要な、あるいは時間制約の厳しいタスクに割当てられ、低優先度のタスクによって専有されないことを保証する。資源割当てファミリは、利用可能な資源の使用における制限を提供し、それによって、利用者が資源を専有することを防ぐ。



図K.1 - 資源利用クラスのコンポーネント構成

K.1　耐障害性(FRU_FLT)

このファミリは、障害時においてさえ能力の利用を可能とする要件を提供する。そのような障害の例は、電源障害、ハードウェア障害、ソフトウェア誤りである。これらの誤りの場合、もしそのように特定されていれば、TOEは特定された能力を維持する。例えば、PP/ST作成者は、核プラントで使用されるTOEは電源障害あるいは通信障害の場合シャットダウン手続き動作を継続する、のように特定することができる。

利用者のための注釈

TOEは、もしTSPが実施された場合だけにその正しい動作を継続できるので、システムは障害のあともセキュアな状態のままである、という要件が存在する。この能力は、FPT_FLS.1によって提供される。

耐障害性をサポートするためのメカニズムは、能動的でも受動的でもよい。能動的メカニズムの場合、誤り発生時に活性化される特定の機能がある。例えば、火災警報は能動的メカニズムである: TSFは、火災を検出し、バックアップシステムに切り替えるようなアクションをとることができる。受動的方式の場合、TOEのアーキテクチャは誤りを処理できる能力を持つ。例えば、複数プロセッサによる多数決方式の使用は、受動的な解である; 一つのプロセッサの障害はTOEの動作を混乱させない(とはいえ、訂正を認めるために、検出されることは必要である)。

このファミリにとって、障害が偶発的なものか(浸水あるいは間違った装置の引き抜きなど)、あるいは意図的なものか(専有など)は、問題でない。

FRU_FLT.1　**機能削減された耐障害性**

利用者のための適用上の注釈

このコンポーネントは、システムの障害後、それにもかかわらずTOEがどの能力を提供するかを特定しようとするものである。すべての特定された障害を記述することは困難なので、障害のカテゴリを特定することができる。一般的な障害の例は、コンピュータ室の浸水、短期間の電源断、CPUあるいはホストの故障、ソフトウェア障害、あるいはバッファオーバフローである。

操作

割付:

FRU_FLT.1.1において、PP/ST作成者は、特定された障害の間及びその後にTOEが維持するTOE能力のリストを特定すべきである。

FRU_FLT.1.1において、PP/ST作成者は、TOEが明示的に保護されねばならない障害の種別のリストを特定すべきである。もしこのリストの障害が起きた場合、TOEはその動作を継続できる。

FRU_FLT.2　**制限付き耐障害性**

利用者のための適用上の注釈

このコンポーネントは、どのような障害の種別にTOEが抵抗しなければならないかを特定しようとするものである。すべての特定された障害を記述することは困難なので、障害のカテゴリを特定することができる。一般的な障害の例は、コンピュータ室の浸水、短期間の電源断、CPUあるいはホストの故障、ソフトウェア障害、あるいはバッファオーバフローである。

操作

割付:

FRU_FLT.2.1において、PP/ST作成者は、TOEが明示的に保護されねばならない障害の種別のリストを特定すべきである。もしこのリストの障害が起きた場合、TOEはその動作を継続できる。

K.2 サービス優先度(FRU_PRS)

このファミリの要件は、低優先度アクティビティに起因する干渉や遅延を受けることなく、TSC内の高優先度アクティビティがいつでも遂行されるように、利用者及びサブジェクトによるTSC内資源の使用をTSFが制御することを認める。つまり、時間制約の厳しいタスクは、あまり時間制約が厳しくないタスクによって遅延されることはない。

このファミリは、例えば処理容量及び通信チャネル容量など、いくつかの資源の種別に適用できる。

サービス優先度メカニズムは、受動的でも能動的でもよい。受動的サービス優先度システムでは、二つの待ち状態のアプリケーション間の選択をすることになったとき、高優先度を持つタスクを選択する。受動的サービス優先度メカニズムを使用している場合、低優先度のタスクが走っているときは、高優先度のタスクはそれに割り込めない。能動的サービス優先度メカニズムを使用している場合は、低優先度タスクが高優先度の新しいタスクによって割り込まれることがある。

利用者のための注釈

監査要件は、拒絶に対するすべての理由は監査されるべきと述べている。動作が拒絶はされないが遅延されることについての議論は、開発者に任されている。

FRU_PRS.1 **制限付きサービス優先度**

利用者のための適用上の注釈

このコンポーネントは、サブジェクトに対する優先度と、この優先度が使用される資源を定義する。もしサブジェクトが、サービス優先度要件によって制御される資源に対してアクションをとろうと試みる場合、そのアクセス及び/またはアクセスの時間は、サブジェクトの優先度、現在動作中のサブジェクトの優先度、及びまだ待ち行列中のサブジェクトの優先度に依存する。

操作

割付:

FRU_PRS.1.2において、PP/ST作成者は、TSFがサービス優先度を実施する、制御された資源のリストを特定すべきである(例えば、プロセス、ディスク空間、メモリ、帯域幅などの資源)。

FRU_PRS.2 完**全サービス優先度**

利用者のための適用上の注釈

このコンポーネントは、サブジェクトに対する優先度を定義する。TSC内のすべての共有可能な資源は、サービス優先度メカニズムの対象となる。もしサブジェクトが、共有可

能なTSC資源に対してアクションをとろうと試みる場合、そのアクセス及び/またはアクセスの時間は、サブジェクトの優先度、現在動作中のサブジェクトの優先度、及びまだ待ち行列中のサブジェクトの優先度に依存する。

K.3　資源割当て(FRU_RSA)

このファミリの要件は、利用者やサブジェクトによるTSC内の資源の使用をTSFが制御することを認め、他の利用者やサブジェクトによる資源専有の手段によって、許可されないサービス拒否が起きないようにする。

利用者のための注釈

資源割当て規則は、特定の利用者あるいはサブジェクトのために割り当てられる、資源空間あるいは時間の総量における制限を定義する割当ての作成あるいは他の手段を許可する。これらの規則は、例えば次のようなものである:

- 特定の利用者が割当てることのできるオブジェクトの数及び/またはサイズを制限するオブジェクト割当てを提供する。
- TSFの制御下にある事前に割り付けられた資源ユニットの、割当て/割当て解除を制御する。

一般に、これらの機能は、利用者及び資源に割り付けられた属性の使用を通して実現される。

これらのコンポーネントの目的は、利用者(例えば、単一の利用者が利用可能なすべての空間を割り当てるべきでない)及びサブジェクトの間に、一定量の公平さを保証することである。資源割当てはしばしばサブジェクトの寿命期間を超えて続き(すなわち、ファイルは、しばしばそれを生成したアプリケーションよりも永く存在する)、かつ同一利用者によるサブジェクトの複数の具現化が他の利用者にあまりネガティブな影響を与えるべきでないので、このコンポーネントは、割当て制限が利用者に関係することを認める。ある状況において、資源はサブジェクトによって割当てられる(例えば、メインメモリあるいはCPUサイクル)。その実施例においては、このコンポーネントは、資源割当てがサブジェクトのレベルにあることを認める。

このファミリは、資源自体の使用においてではなく、資源の割当てにおける要件を課する。そのため、監査要件も、資源の使用についてではなく、資源の割当てについて適合する。

FRU_RSA.1　最大割当て

利用者のための適用上の注釈

このコンポーネントは、TOEにおける共有可能資源の特定されたセットだけに適合する割当てメカニズムに対する要件を提供する。この要件は、利用者に関連付けられる割当てが、TOEに適用できる範囲で、利用者あるいはサブジェクトのグループに割り付けられるのを認めることもある。

操作

割付:

FRU_RSA.1.1において、PP/ST作成者は、最大資源割当て制限が要求される制御された資源のリストを特定すべきである(例えば、プロセス、ディスク空間、メモリ、帯域幅)。もしTSC内のすべての資源が含まれる必要があれば、「すべてのTSC資源」という語を特定することができる。

選択:

FRU_RSA.1.1において、PP/ST作成者は、最大割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.1.1において、PP/ST作成者は、最大割当てが、任意の与えられた時間(同時に)、あるいは特定の時間間隔に適用されるかどうかを選択すべきである。

FRU_RSA.2 **最小及び最大割当て**

利用者のための適用上の注釈

このコンポーネントは、TOEにおける共有可能資源の特定されたセットに適用される、割当てメカニズムに対する要件を提供する。この要件は、ある利用者に関連付けられる割当てが、TOEに適用できる範囲で、利用者あるいはサブジェクトのグループに割り付けられることを認める。

操作

割付:

FRU_RSA.2.1において、PP/ST作成者は、最大及び**最小**資源割当て制限が要求される制御された資源のリストを特定すべきである(例えば、プロセス、ディスク空間、メモリ、帯域幅)。もしTSC内のすべての資源が含まれる必要があれば、「すべてのTSC資源」という語を特定することができる。

選択:

FRU_RSA.2.1において、PP/ST作成者は、最大割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.2.1において、PP/ST作成者は、最大割当てが、任意の与えられた時間(同時に)、あるいは特定の時間間隔に適用されるかどうかを選択すべきである。

割付:

FRU_RSA.2.2において、PP/ST作成者は、最小割当て制限がセットされる必要がある制御された資源を特定すべきである(例えば、プロセス、ディスク空間、メモリ、帯域幅)。もしTSCにおけるすべての資源が含まれる必要があれば、「すべてのTSC資源」という語を特定することができる。

選択:

FRU_RSA.2.2において、PP/ST作成者は、最小割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.2.2において、PP/ST作成者は、最小割当てが、任意の与えられた時間(同時に)、あるいは特定の時間間隔に適用されるかどうかを選択すべきである。

附属書L

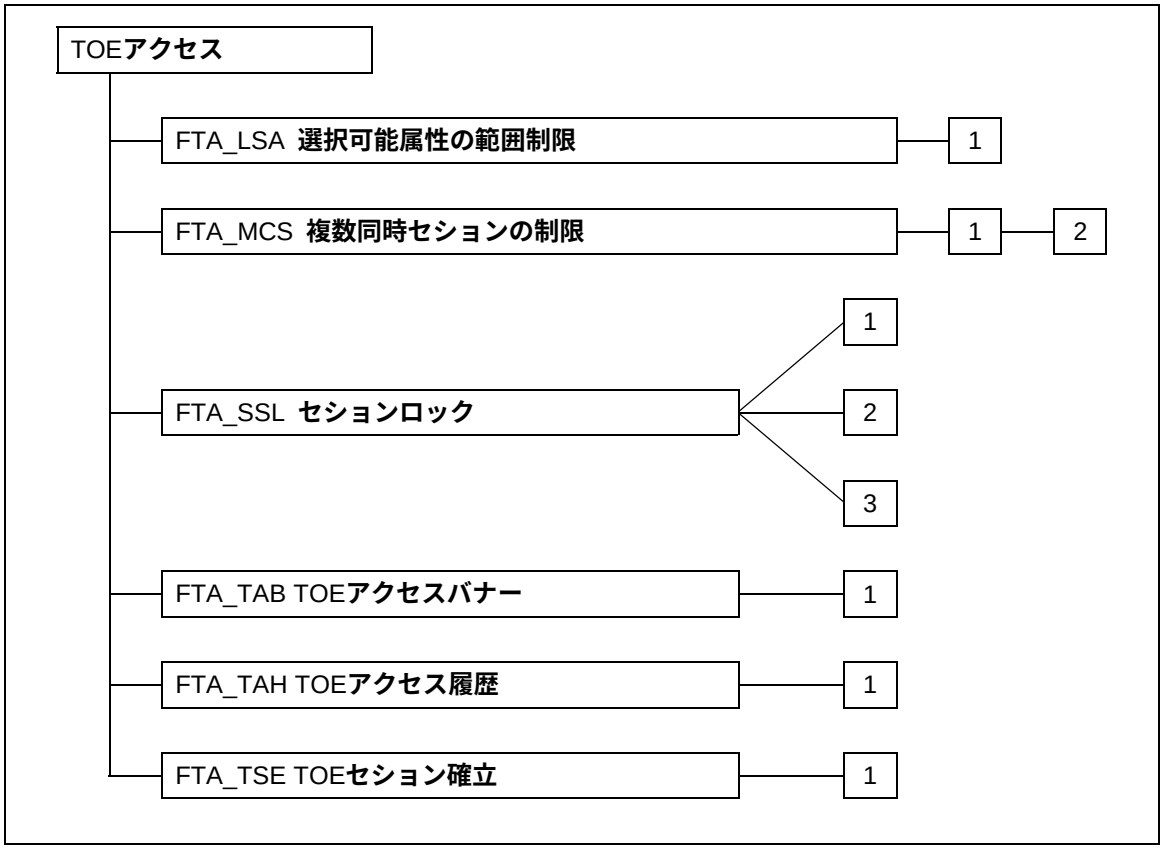
(参考)

TOEアクセス(FTA)

利用者セションの確立は、典型的に、TOEにおいて利用者の代わりに動作を行う一つあるいはそれ以上のサブジェクトを作成することからなる。セション確立手続きの最後で、提供されたTOEアクセス要件が満たされ、作成されたサブジェクトは、識別と認証機能によって決定された属性を伝える。このファミリは、利用者セションの確立を制御するための機能要件を特定する。

利用者セションは、識別/認証の時点、あるいは、もし更に適切であれば、利用者とシステム間の対話の開始で始まり、そのセションに関係するすべてのサブジェクト(資源及び属性)が割当て解除された瞬間までの期間として定義される。

図L.1は、TOEアクセスクラスのコンポーネント構成を示す。



図L.1 - TOE**アクセスクラスのコンポーネント構成**

L.1 選択可能属性の範囲制限(FTA_LSA)

このファミリは、利用者が選択できるセションセキュリティ属性、及び以下に基づいて利用者が結合できるサブジェクトを制限する要件を定義する: アクセス方法; アクセスの場所あるいはポート; 及び/または時間(例えば、時刻、曜日)。

利用者のための注釈

このファミリは、PP/ST作成者が、環境条件に基づいて、許可利用者のセキュリティ属性のドメインにおける制限を課すための、TSFに対する要件を特定できる能力を提供する。例えば、ある利用者は、通常勤務時間中は「秘密セション」を確立することが許されるかもしれないが、その時間帯外では、同じ利用者が「非区分セション」の確立だけに制約されるかもしれない。選択可能属性のドメインに関連する制約の識別は、選択操作を使用することで達成できる。これらの制約は、属性一つずつに適用することができる。制約を複数の属性に対して特定する必要があるときは、このコンポーネントを各属性ごとに複製しなくてはならない。セションセキュリティ属性を制限するのに使える属性の例は:

a) アクセスの方法は、どのような種別の環境で利用者が操作するかを特定するために使用できる(例えば、ファイル転送プロトコル、端末、vtam)。

b) アクセスの場所は、利用者のアクセスの場所あるいはポートに基づいて、利用者の選択可能属性のドメインを制約するために使用できる。この能力は、ダイヤルアップ設備あるいはネットワーク設備が利用できる環境で使用するのに最適である。

c) アクセスの時間は、利用者の選択可能属性のドメインを制約するために使用できる。例えば、範囲は、時刻、曜日、あるいはカレンダの日付に基づくことができる。この制約は、適切な監視あるいは適切な手続き的手段がきちんと行われない時間に発生し得る利用者アクションに対して、何らかの動作上の保護を提供する。

FTA_LSA.1 **選択可能属性の範囲制限**

操作

割付:

FTA_LSA.1.1において、PP/ST作成者は、制約を設けるべきセションセキュリティ属性のセットを特定すべきである。これらのセションセキュリティ属性の例は、利用者の取扱許可レベル、廉直性レベル、役割である。

FTA_LSA.1.1において、PP/ST作成者は、セションセキュリティ属性の範囲を決定するために使用できる属性のセットを特定すべきである。そのような属性の例は、利用者識別情報、発信場所、アクセスの時刻、及びアクセスの方法である。

L.2　複数同時セションの制限(FTA_MCS)

このファミリは、利用者が、同時にいくつのセション(同時セション)を持てるかを定義する。同時セションの数は、各個別利用者ごとに設定できる。

FTA_MCS.1　**複数同時セションの基本制限**

利用者のための適用上の注釈

このコンポーネントは、TOEの資源を効果的に使用するために、システムがセションの数を制限することを認める。

操作

割付:

FTA_MCS.1.2において、PP/ST作成者は、使用される最大同時セションのデフォルト数を特定すべきである。

FTA_MCS.2　**複数同時セションの利用者ごと属性制限**

利用者のための適用上の注釈

このコンポーネントは、利用者が行使できる同時セションの数に対し、課すべき制約を増やすことを認めることによって、FTA_MCS.1に対する追加能力を提供する。これらの制約は、利用者の識別情報あるいは役割の資格など、利用者のセキュリティ情報に関するものについてである。

操作

割付:

FTA_MCS.2.1において、PP/ST作成者は、同時セションの最大数を決定する規則を特定すべきである。規則の例は、「同時セションの最大数は、利用者の秘密区分レベルが『秘密』の場合は1、その他は5とする」である。

FTA_MCS.2.2において、PP/ST作成者は、使用される最大同時セションのデフォルト数を特定すべきである。

L.3　セションロック(FTA_SSL)

このファミリは、TSFに、対話セションのロック及びロック解除の能力(例えばキーボードロック)を提供するための要件を定義する。

利用者がTOEにおけるサブジェクトと直接対話しているとき(対話セション)、もし無人のまま放置されれば、利用者の端末は脆弱になる。このファミリは、特定された不動作の期間後にTSFが端末を非活性化(ロック)しあるいはセションを終了するための、及び、利用者が端末の非活性化(ロック)を起動するための要件を提供する。端末を再動作させるには、利用者再認証のような、PP/ST作成者によって特定された事象が起こらねばならない。

利用者は、もしある時間TOEに何も刺激を与えなかったとすると、非アクティブと見なされる。

PP/ST作成者は、FTP_TRP.1 高信頼パスを含めるべきかどうかを考慮すべきである。その場合、「セションロック」機能は、FTP_TRP.1における操作に含められるべきである。

FTA_SSL.1　TSF起動セションロック

利用者のための適用上の注釈

FTA_SSL.1 TSF起動のセションロックは、TSFに対し、特定した時間後に動作中の利用者セションをロックする能力を提供する。端末のロックは、その先、そのロックされた端末を使っての、存在するアクティブセションとのあらゆる対話をできなくする。

このコンポーネントは、どの事象がセションをロック解除するかをPP/ST作成者が特定することを認める。これらの事象は、端末(例えば、セションをロック解除するキーストロークの固定したセット)、利用者(例えば、再認証)、あるいは時間に関係するかもしれない。

操作

割付:

FTA_SSL.1.1において、PP/ST作成者は、対話セションのロックの引き金となる利用者の非アクティブである間隔を特定すべきである。もし必要であれば、PP/ST作成者は、その時間間隔の特定を許可管理者あるいは利用者に任せることを、割付によって特定することができる。FMTクラスにおける管理機能は、この時間をデフォルト値にし、それを修正する能力を特定できる。

FTA_SSL.1.2において、PP/ST作成者は、セションがロック解除される前に生じるべき事象を特定すべきである。そのような事象の例: 「利用者再認証」あるいは「利用者はロック解除鍵シーケンスを入力」。

FTA_SSL.2　**利用者起動ロック**

利用者のための適用上の注釈

FTA_SSL.2 利用者起動ロックは、許可利用者のために、彼/彼女自身の端末をロック及びロック解除する能力を提供する。これは、アクティブセションを終了させねばならないということなく、アクティブセションのそれ以上の使用を効果的に妨げる能力を、許可利用者に提供する。

操作

割付:

FTA_SSL.2.2において、PP/ST作成者は、セションがロック解除される前に生じるべき事象を特定すべきである。そのような事象の例: 「利用者再認証」あるいは「利用者はロック解除鍵シーケンスを入力」。

FTA_SSL.3　**TSF起動による終了**

利用者のための適用上の注釈

FTA_SSL.3 TSF起動による終了は、ある不動作の時間後、TSFが対話利用者セションを終了させることを要求する。

PP/ST作成者は、利用者が彼/彼女のアクティビティを終了した後も、例えばバックグラウンド処理など、セションが継続しているかもしれないことに注意すべきである。この要件は、利用者が非アクティブである期間後、そのサブジェクトの状態と関係なくこのバックグラウンドサブジェクトを終了させる。

操作

割付:

FTA_SSL.3.1において、PP/ST作成者は、対話セションの終了の引き金を引く、利用者の非アクティブである間隔を特定すべきである。もし必要であれば、PP/ST作成者は、その間隔の特定を許可管理者あるいは利用者に任せることを、割付によって特定することができる。FMTクラスにおける管理機能は、この時間をデフォルト値にし、それを修正する能力を特定できる。

L.4　TOEアクセスバナー(FTA_TAB)

識別と認証に先立ち、TOEアクセス要件は、TOEの適切な使用にふさわしい可能性を持つ利用者に、勧告的警告メッセージを表示する能力を提供する。

FTA_TAB.1　デフォルトTOEアクセスバナー

このコンポーネントは、TOEの許可されない使用に関する勧告的警告が存在することを要求する。PP/ST作成者は、デフォルトバナーを含めるために、要件を詳細化できる。

L.5　TOE**アクセス履歴**(FTA_TAH)

このファミリは、TOEに対する成功したセション確立において、そのアカウントに対する成功しなかったアクセス試行の履歴をTSFが利用者に表示する要件を定義する。この履歴は、識別された利用者による最後の成功したアクセス以来、TOEをアクセスした成功しなかった試行の数だけでなく、TOEに対する最後の成功したアクセスの日付、時刻、アクセスの方法、及びポートを含むことができる。

FTA_TAH.1　TOE**アクセス履歴**

このファミリは、その利用者アカウントの悪用の可能性を示す情報を許可利用者に提供できる。

このコンポーネントは、利用者が情報を提示されることを要求する。利用者は、情報をレビューできるべきであるが、それを強制はされない。もし利用者が望むのであれば、例えば、この情報を無視し、他のプロセスを開始するようなスクリプトを作成してもよい。

操作

選択:

FTA_TAH.1.1において、PP/ST作成者は、利用者インタフェースで示される、最後の成功したセション確立のセキュリティ属性を選択すべきである。項目: 日付、時刻、アクセスの方法(ftpなど)、及び/または場所(例えば、端末50)。

FTA_TAH.1.2において、PP/ST作成者は、利用者インタフェースで示される、最後の成功しなかったセション確立のセキュリティ属性を選択すべきである。項目: 日付、時刻、アクセスの方法(ftpなど)、及び/または場所(例えば、端末50)。

L.6 TOEセション確立(FTA_TSE)

このファミリは、アクセスの場所あるいはポート、利用者のセキュリティ属性(例えば、識別情報、取扱許可レベル、廉直性レベル、役割における資格)、時間の幅(例えば、時刻、曜日、カレンダの日付)、あるいはパラメタの組み合わせなどの属性に基づいて、TOEとセションを確立する利用者許可を拒否するための要件を定義する。

利用者のための注釈

このファミリは、許可利用者がTOEとセションを確立する能力における制約を課するためのTOEに対する要件をPP/ST作成者が特定する能力を提供する。関連する制約の識別は、選択操作を使用して達成できる。セション確立制約を特定するために使用できる属性の例:

a) アクセスの場所は、利用者のアクセスの場所あるいはポートに基づき、利用者がTOEとアクティブセションを確立する能力を制約するために使用できる。この能力は、ダイヤルアップ設備あるいはネットワーク設備を利用できる環境において特に有用である。

b) 利用者のセキュリティ属性は、TOEとアクティブセションを確立する利用者の能力において制約を課すために使用できる。例えば、これらの属性は、以下のどれかに基づいて、セション確立を拒否する能力を提供する。

- 利用者の識別情報;

- 利用者の取扱許可レベル;

- 利用者の廉直性レベル; 及び

- 利用者の役割における資格

この能力は、TOEアクセスチェックが実行されるのと異なる場所で許可あるいはログインが行われるかもしれない状況に、特に関連する。

a) アクセスの時間は、時間帯に基づいて、利用者がTOEとアクティブセションを確立する能力を制約するために使用できる。例えば、その幅は、時刻、曜日、またはカレンダの日付に基づくかもしれない。この制約は、適切な監視あるいは適切な手続き手段が存在しないかもしれないときに生じ得るアクションに対して、何らかの動作上の保護を提供する。

FTA_TSE.1　TOE**セション確立**

操作

割付:

FTA_TSE.1.1において、PP/ST作成者は、セション確立を限定するために使うことができる属性を特定すべきである。使える属性の例は、利用者識別情報、発信場所(例えば、リモート端末不可)、アクセスの時間(例えば、勤務時間外)、あるいはアクセスの方法(例えば、Xウィンドウ)など。

附属書M

(参考)

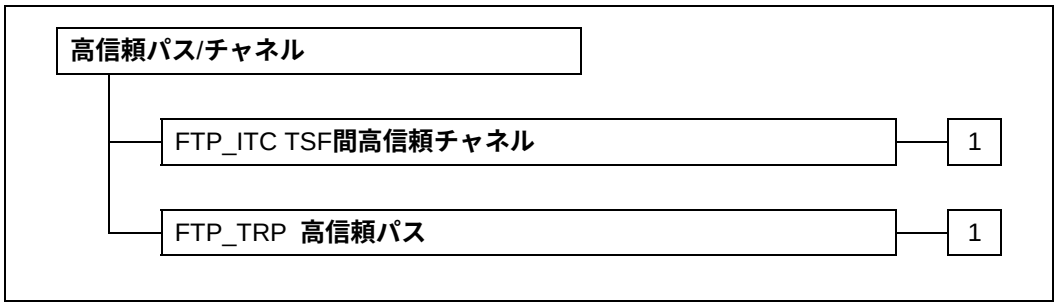
高信頼パス/チャネル(FTP)

利用者は、しばしば、TSFとの直接対話を通して機能を実行する必要がある。高信頼パスは、TSFが呼び出されたときはいつでも、利用者が直接それと通信しているという信頼を提供する。高信頼パスを介した利用者の応答は、信頼できないアプリケーションが利用者の応答を傍受あるいは改変できないことを保証する。同様に、高信頼チャネルは、TSFとリモートIT製品間のセキュアな通信に対する一つのアプローチである。

パート2、4ページ、図1.2は、TOEあるいはTOEのネットワーク内で生じ得るさまざまな通信の種別(すなわち、TOE内転送、TSF間転送、及びTSF制御外のインポート/エクスポート)、及びさまざまな形態の高信頼パス及びチャネルの間の関係を図示している。

信頼できないアプリケーションが使われる環境では、高信頼パスが存在しないと、責任あるいはアクセス制御の不履行が許されてしまうかもしれない。これらのアプリケーションは、パスワードなど利用者のプライベート情報を横取りし、他の利用者になりすますためにそれを使用することができる。その結果、あらゆるシステムアクションに対する責任を、信頼を持って、責任を負うべきエンティティに割り付けることができない。また、これらのアプリケーションは、何も疑っていない利用者のディスプレイに誤りのある情報を出力することができ、結果として、それにつながる利用者アクションが誤りのあるものになるかもしれず、かつセキュリティ違反を導くかもしれない。

図M.1は、高信頼パス/チャネルクラスのコンポーネント構成を示している。



図M.1 - 高信頼パス/チャネルクラスのコンポーネント構成

M.1　TSF**間高信頼チャネル**(FTP_ITC)

このファミリは、TSFと他の高信頼IT製品間に張られ製品間でセキュリティ上重要な動作を実行するための、高信頼チャネル接続の作成のための規則を定義する。そのようなセキュリティ上重要な動作の例に、監査データの収集機能を持つ高信頼製品からのデータの転送によって、TSF認証データベースの更新を行うというものがある。

FTP_ITC.1　TSF**間高信頼チャネル**

利用者のための適用上の注釈

このコンポーネントは、TSFと他の高信頼IT製品間に高信頼通信チャネルが要求されるときに、使用されるべきである。

操作

選択:

FTP_ITC.1.2において、PP/ST作成者は、ローカルTSF、リモート高信頼IT製品、あるいは両方が、高信頼チャネルを起動する能力を持たねばならないかどうかを特定しなければならない。

割付:

FTP_ITC.1.3において、PP/ST作成者は、高信頼チャネルを必要とする機能を特定すべきである。これらの機能の例には、利用者、サブジェクト、及び/またはオブジェクトのセキュリティ属性、及びTSFデータの一貫性の保証がある。

M.2　高信頼パス(FTP_TRP)

このファミリは、利用者及びTSFへ/からの高信頼通信を確立及び維持する要件を定義する。高信頼パスは、あらゆるセキュリティ関連の対話のために要求されることができる。高信頼パス交換は、TSFとの対話時に利用者によって起動でき、あるいはTSFが高信頼パスを介した利用者との通信を確立することができる。

FTP_TRP.1　高信頼パス

利用者のための適用上の注釈

このコンポーネントは、利用者とTSF間に高信頼通信が要求されるときに、最初の認証目的だけのためか、あるいは追加して特定された利用者操作のために使用されるべきである。

操作

選択:

FTP_TRP.1.1において、PP/ST作成者は、高信頼パスをリモート及び/またはローカル利用者へ伸ばさねばならないかどうかを特定すべきである。

FTP_TRP.1.2において、PP/ST作成者は、TSF、ローカル利用者、及び/またはリモート利用者が、高信頼パスを起動できるべきかどうかを特定すべきである。

FTP_TRP.1.3において、PP/ST作成者は、高信頼パスを、最初の利用者認証のために、及び/または他の特定されたサービスのために使うべきかどうかを特定すべきである。

割付:

FTP_TRP.1.3において、もし選択されれば、PP/ST作成者は、高信頼パスが要求される他のサービスがあれば、それを識別すべきである。