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: セキュリティ機能コンポーネント

2012 年 9 月

バージョン **3.1**
改訂第 **4** 版

CCMB-2012-09-002

平成 24 年 11 月翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

IPA まえがき

はじめに

本書は、「IT セキュリティ評価及び認証制度」において、「認証機関が公開する評価基準」の規格として公開している Common Criteria(以下、CC という)を翻訳した文書である。

原文

Common Criteria for Information Technology Security Evaluation

Part2: Security functional components Version 3.1 Revision 4
September 2012 CCMB-2012-09-002

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の本バージョン(CC v3.1)は、2005 年に CC v2.3 が公開されて以来、最初の主要な改訂版である。

CC v3.1 は、重複する評価アクティビティを排除し、製品の最終保証にあまり役立たないアクティビティを削減または排除し、誤解を減らすために CC 用語を明確にし、セキュリティ保証が必要である領域に対する評価アクティビティを再構築し焦点を当て、必要に応じて新しい CC 要件を追加することを目的としている。

CC バージョン 3.1 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: セキュリティ機能コンポーネント
- パート 3: セキュリティ保証コンポーネント

商標:

- UNIX は、米国及びその他の諸国の The Open Group の登録商標である。
- Windows は、米国及びその他の諸国の Microsoft Corporation の登録商標である。

法定通知:

以下に示す政府組織は、情報技術セキュリティ評価のためのコモンクライテリアの本バージョンの開発に貢献した。これらの政府組織は、情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1 *のパート 1 から 3(CC* 3.1 *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* 3.1 *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* 3.1 *を使用、複製、配布、翻訳及び改変する権利は、これらの政府組織が保有する。*

オーストラリア/ニュージーランド:	*The Defence Signals Directorate and the Government Communications Security Bureau;*
カナダ:	*Communications Security Establishment;*
フランス:	*Direction Centrale de la Securite des Systemes d'Information;*
ドイツ:	*Bundesamt fur Sicherheit in der Informationstechnik;*
日本:	*独立行政法人情報処理推進機構(Information-technology Promotion Agency);*
オランダ:	*Netherlands National Communications Security Agency;*
スペイン:	*Ministerio de Administraciones Publicas and Centro Criptologico Nacional;*
英国:	*Communications-Electronics Security Group;*
米国:	*The National Security Agency and the National Institute of Standards and Technology*

目次

図一覧

表一覧

1 序説

1 この CC 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)に関して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、利用者が IT との直接の対話(すなわち、入力、出力)により、または IT からの応答により、検出できるセキュリティ特性を記述している。

2 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。

3 パート 2 の対象読者には、セキュアな IT 製品の消費者、開発者、評価者が含まれる。CC パート 1 の 6 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:

a) 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 7 節は、セキュリティ対策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。

b) 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 セキュリティ機能性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。

c) 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すべきである。

2 適用範囲

4 このパートでは、セキュリティ評価のために、セキュリティ機能コンポーネントの必要な構造及び内容を定義している。これには、多くの IT 製品の共通のセキュリティ機能性の要件を満たす機能コンポーネントのカタログが含まれる。

3 規定の参照

5 以下の参照文書は、本文書の適用のために不可欠である。日付の付いている参照資料については、指定した版のみが適用される。日付のない参照資料については、(修正を含む)最新版の参照文書が適用される。

［CC］ 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 4 版、 2012 年 9 月 パート 1: 概説と一般モデル

4 用語と定義、記号と略語

6 本文書の目的のために、CC パート 1 で使用された用語、定義、記号、及び略語を適用する。

5 概要

7 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。

8 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。

9 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、CC パート 1 の附属書 A と B 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)。

5.1 CC パート 2 の構成

10 6 章では、CC 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。

11 7 章では、CC パート 2 機能コンポーネントのカタログを紹介し、8 章から 18 章までは機能クラスを記述している。

12 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を含む機能コンポーネントの潜在的な利用者のために解釈上の情報を提供する。

13 附属書 B から附属書 M までは、機能クラスのための解釈上の情報を提供する。この資料は、適切な操作を適用し、適切な監査または証拠資料情報を選択する方法についての規定の指示とみなさねばならない。助動詞するべきである(should)の使用は、その指示が非常に望ましいことを意味する。しかし他の方法を適切であると正当化することもできる。異なる選択肢が付与される箇所では、選択は、PP/ST 作成者に委ねられる。

14 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 の 2 章を参照すべきである:

a) パート 1 の 4 章では、CC で使用される用語を定義している。

b) パート 1 の附属書 A では、ST の構造を定義している。

c) パート 1 の附属書 B では、PP の構造を定義している。

6 機能要件のパラダイム

15 この章では、パート 2 のセキュリティ機能要件で使用するパラダイムについて記述する。ここで記述する主な概念は、ボールド/イタリックで示す。CC パート 1 の 4 章に定義されている用語を差し替え、または置き換えることは意図していない。

16 このパート 2 は、**評価対象(TOE)**に対して特定できるセキュリティ機能コンポーネントのカタログである。TOE とは、利用者及び管理者のガイダンス文書を伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェアのセットである。TOE には、情報の処理と保存に使用でき、評価対象となる電子記憶媒体(メインメモリ、ディスク領域など)、周辺装置(プリンタなど)、計算能力(CPU 時間など)のような資源が含まれることがある。

17 TOE 評価は、**セキュリティ機能要件(SFR)**の定義済みセットを TOE 資源で確実に実施させることを主な目的としている。SFR は、TOE が資源のアクセス及び使用と、TOE によって制御される情報及びサービスを管理する規則を定義する。

18 SFR には、TOE が実施しなければならない規則を表現する複数の**セキュリティ機能方針(SFP)**を定義することができる。各該当の SFP は、サブジェクト、オブジェクト、資源または情報、及びそれが適用される操作を定義することにより、その**制御範囲**を特定しなければならない。すべての SFP は TSF(以下を参照)によって実装され、TSF のメカニズムが SFR で定義された規則を実施し、必要な機能を提供する。

19 SFR を正しく実施するために要求される TOE の部分は、一括して **TOE セキュリティ機能(TSF)**と呼ぶ。TSF は、セキュリティの実施のため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。

20 TOE は、ハードウェア、ファームウェア、及びソフトウェアを含む一体構造の製品にすることができる。

21 または、内部が複数の個別の部分からなる分散製品にすることもできる。このような TOE の各部分は、TOE の特定のサービスを提供し、**内部通信チャネル**を通じて TOE の他の部分に接続される。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全体にわたることもある。

22 TOE が複数の部分からなる場合、TOE の各部分には独自の TSF の部分を割り当てることができる。TSF の各部分は、内部通信チャネルを通じて、TSF の他の部分と利用者及び TSF のデータを交換する。この対話は、**TOE 内転送**と呼ばれる。この場合、概念上、TSF の個別の部分によって、SFR を実施する複合 TSF が形成される。

23 TOE インタフェースは、特定の TOE に範囲を限定するか、または**外部通信チャネル**を通じて他の IT 製品と対話させることができる。他の IT 製品との外部対話は、次の 2 つの形式をとることがある:

a) 他の「高信頼 IT 製品」の SFR と TOE の SFR の管理を調整し、(個別の評価などによって)他の高信頼IT製品はその SFR を正しく実施していると想定する。この状況での情報の交換は、個々の高信頼製品の TSF 間で生じるため、**TSF 間転送**と呼ばれる。

b) 他の IT 製品を信頼できない場合、このような製品は「信頼できない IT 製品」と呼ばれることがある。その SFR は不明であり、またはその実装に信頼性があるとはみなされない。この状況で TSF が仲介する情報の交換は、他の IT 製品に TSF が存在しない(またはその方針の特性が不明である)ため、**TOE 外への転送**と呼ばれる。

24 対話型(マンマシンインタフェース)またはプログラム型(アプリケーションプログラミングインタフェース)のいずれであっても、TSF 仲介資源へのアクセスまたは TSF からの情報の取得に使用されるインタフェースのセットは、**TSF インタフェース(TSFI)**と呼ばれる。TSFI では、SFR の実施のために備える TOE の機能性の境界を定義する。

25 利用者は、TOE の範囲外である。ただし、SFR で定義された規則に従ったサービスを TOE が実行するよう要求するために、利用者は TSFI を通じて TOE と対話する。CC パート 2 に関係する利用者には、**人間の利用者**と**外部 IT エンティティ**の 2 つのタイプがある。人間の利用者はさらに、TOE 装置(例えばワークステーションなど)を通じて TOE と直接対話する**ローカルの人間の利用者**と、別の IT 製品を通して TOE と間接的に対話する**リモートの人間の利用者**に区別することができる。

26 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、利用者認証、時刻、TOE にアクセスする方法、許可される同時セションの数(利用者あたり、または合計)など、各種の考慮事項に基づいて制御できる。

27 CC の本パートでは、利用者が操作を行うために必要な権利及び/または特権を有することを示すために、「**許可**」という用語を使用する。したがって、「**許可利用者**」という用語は、利用者が SFR によって定義される特定の操作または操作のセットを実行できることを示す。

28 管理者業務の分離を求める要件を表すために、(ファミリ FMT_SMR の)関係するセキュリティ機能コンポーネントは、管理者の**役割**が必要なことを明記している。役割とは、事前に定義される規則のセットで、その役割で操作している利用者と TOE との間に許可された対話を確立する。TOE では、任意の数の役割定義をサポートすることができる。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」などを使用できる。

29 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 SFR を完全かつ正しく実施することである。

30 TOE 資源は、様々な方法で構成し利用することができる。ただし、CC パート 2 では、望ましいセキュリティ特性を特定できるように、資源を明確に区別している。資源から生成できるすべてのエンティティは、次のいずれかの特徴を示す。エンティティが能動的である場合、そのエンティティは TOE 内部で生じるアクションの原因であり、情報に対して操作を実行させる。エンティティが受動的である場合、そのエンティティは情報の発生源または情報の格納先となるコンテナである。

31 オブジェクトに対して操作を実行する TOE の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ことがある:

a) 許可利用者の代わりに動作するサブジェクト(UNIX プロセスなど);

b) 複数の利用者の代わりに処理を実行する特定の機能プロセスとして動作するサブジェクト(クライアント/サーバアーキテクチャに見られる機能など);

c) TOE 自体の一部として動作するサブジェクト(利用者の代わりに動作しないプロセスなど)。

32 CC パート 2 では、上記のタイプのサブジェクトに対する SFR の実施について扱う。

33 情報を格納し、または受け取り、サブジェクトが操作を実行する対象となる TOE の受動的なエンティティは**オブジェクト**と呼ばれる。サブジェクト(能動的なエンティティ)が(プロセス間通信などの)操作の対象である場合、サブジェクトは、オブジェクトの役割を果たすこともある。

34 オブジェクトには、**情報**を格納することができる。この概念は、FDP クラスで扱う情報フロー制御方針を詳述するために必要となる。

35 SFR の規則によって制御される利用者、サブジェクト、情報、オブジェクト、セション、及び資源には、正しい操作のために TOE によって使用される情報を含む特定の**属性**を割り当てることができる。ファイル名のように、情報を提供し、または個々の資源を識別するための使用を目的とする属性と、アクセス制御情報のように、特に SFR を実施するために存在する属性がある。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、CC の本パートの一部で「セキュリティ属性」という用語の省略語として使用する。ただし、属性情報の使用目的にかかわらず、SFR の指示に従って属性を制御する必要がある。

36 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 は、この関係を示している。**利用者データ**は、SFR 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、SFR の要求に応じて決定を下すときに TSF が使用する情報である。**TSF データ**は、SFR が許可している場合は、利用者の影響を受けることがある。TSF データの例には、SFR で定義される規則によって使用される、または TSF とアクセス制御リストエントリの保護のために使用されるセキュリティ属性、認証データ、TSF 内部ステータス変数がある。

37 **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、制御の範囲内の利用者、資源、サブジェクト、オブジェクト、セション、TSF ステータスデータ、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。

38 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、コンテナの属性と関係付けられ、またはコンテナのデータから派生することがあり、TSF によって処理されるときにも情報に伴う。

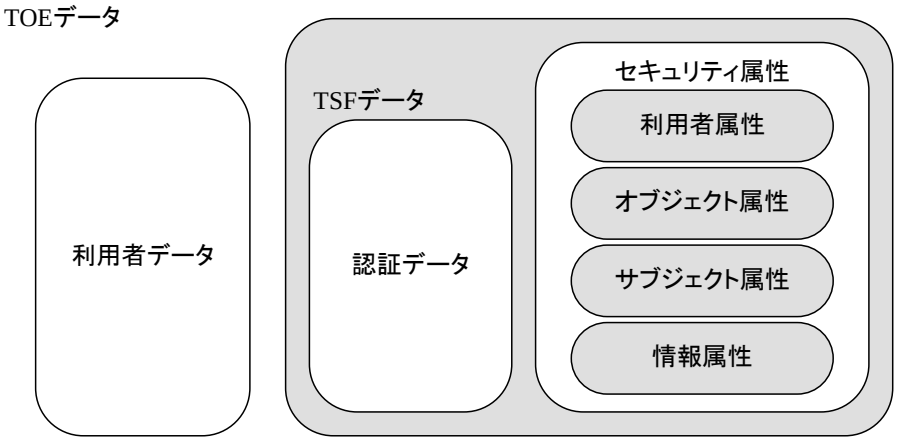


図 1　　利用者データと TSF データとの関係

39　パート 2 が記述する 2 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。

40　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。

41　CC パート2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。

42　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 2 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。

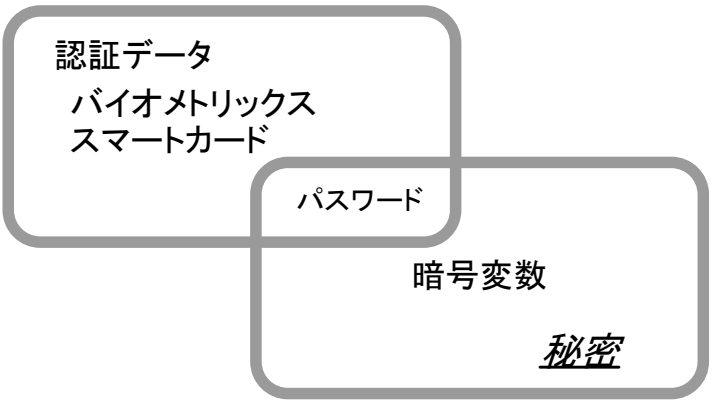


図 2　　「認証データ」と「秘密」との関係

7 セキュリティ機能コンポーネント

7.1 概要

43 この章では、CC の機能要件の内容と表現を定義し、ST に含まれ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。

7.1.1 クラスの構造

44 図 3 は、機能クラス構造を図の形式で示したものである。各機能クラスには、クラス名、クラスの概説、1 つ以上の機能ファミリが含まれる。

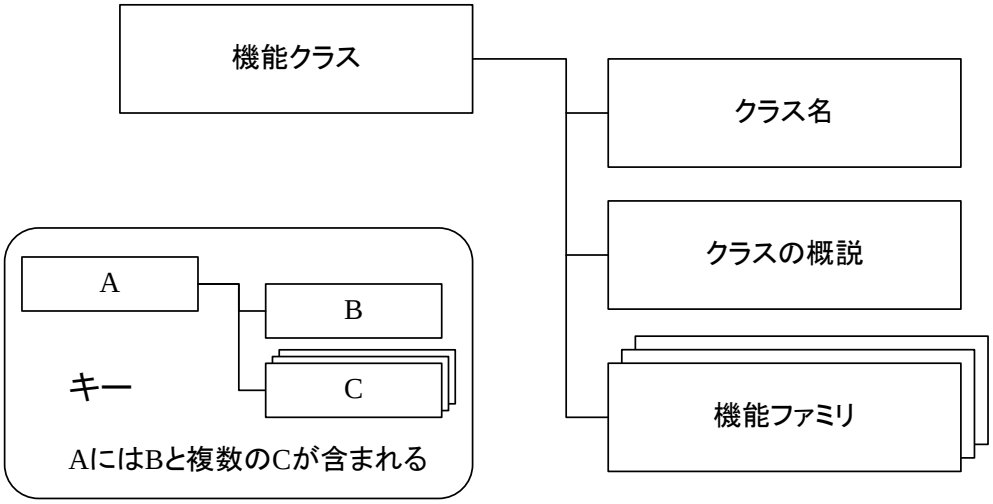


図 3 機能クラス構造

7.1.1.1 クラス名

45 クラス名の節は、機能クラスを識別して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特定するときに使用される。

7.1.1.2 クラスの概説

46 クラスの概説は、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。

47 クラスの概説には、7.2 節に説明するように、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。

7.1.2 ファミリ構造

48 図 4 は、機能ファミリ構造を図の形式で示したものである。

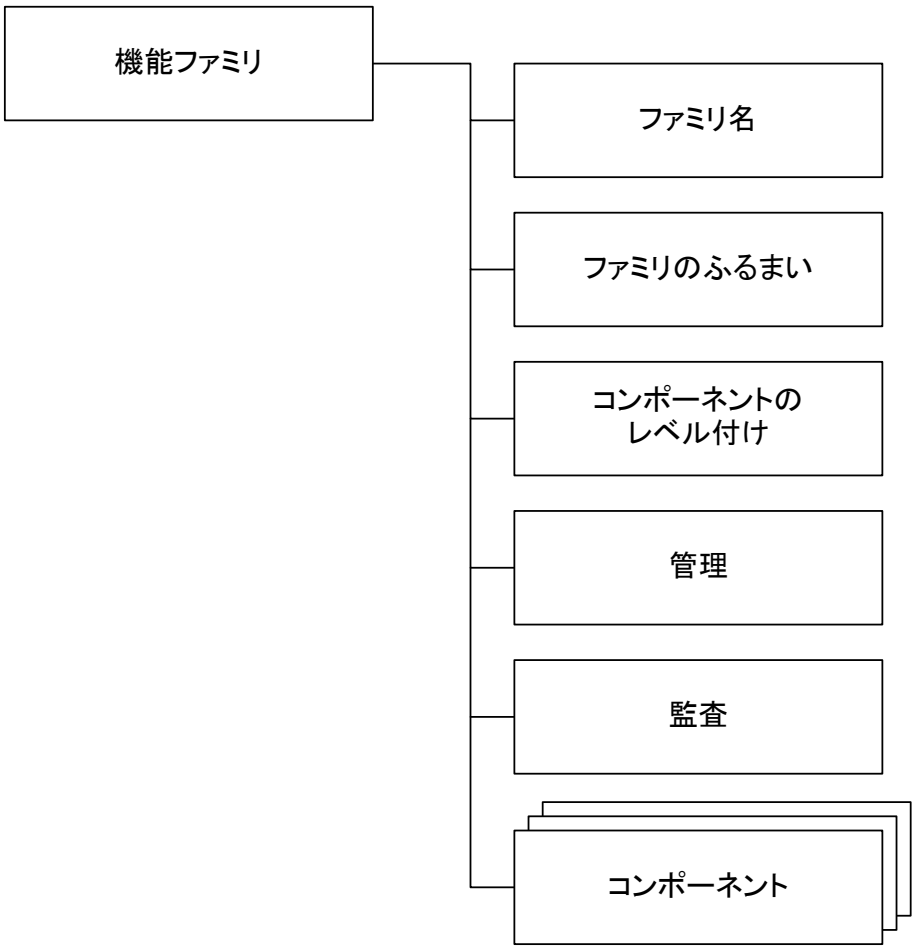


図 4　　機能ファミリ構造

7.1.2.1　　ファミリ名

49　　ファミリ名の節は、機能ファミリを識別して分類するのに必要な分類情報と記述情報を提供する。各機能ファミリ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。

7.1.2.2　　ファミリのふるまい

50　　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。

7.1.2.3 コンポーネントのレベル付け

51 機能ファミリは、1 つ以上のコンポーネントを含む。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。この節の目的は、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。

52 機能ファミリを記述するこの節では、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。

53 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。

54 7.2 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。

7.1.2.4 管理

55 *管理*の章には、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。その章は、管理クラス(FMT)のコンポーネントを参照し、それらのコンポーネントへの操作を介して適用される可能性のある管理アクティビティに関するガイドを提供する。

56 PP/ST 作成者は、示されたコンポーネントを選んでもよく、管理アクティビティについて詳しく述べるために、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。

7.1.2.5 監査

57 *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、セキュリティ監査データ生成(FAU_GEN)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、次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構成値を含む、メカニズムに対して行われたあらゆる構成変更。

58 監査対象事象の分類は、階層的であることに注意すべきである。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、適切な割付操作を使用して 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。

59 FAU クラスでは、セキュリティ監査及び監査に関する規則がさらに詳細に説明されている。

7.1.3 コンポーネント構造

60 図 5 は、機能コンポーネント構造を示している。

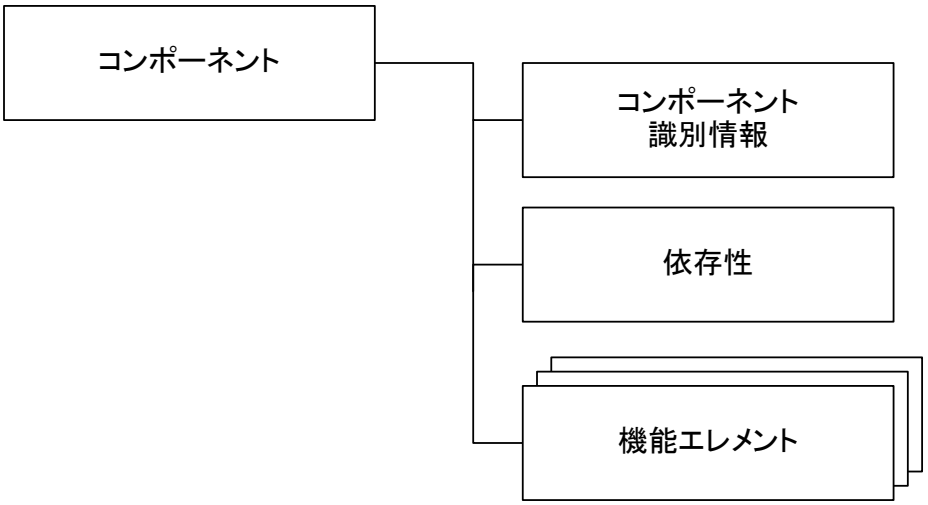


図 5　　機能コンポーネント構造

7.1.3.1　　コンポーネント識別情報

61　　コンポーネント識別情報の節は、コンポーネントを識別、分類、登録及び相互参照するため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:

62　　*一意の名前*。コンポーネントの目的を表す名前。

63　　*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。

64　　*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。

7.1.3.2　　機能エレメント

65　　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。

66　　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。

67　　パッケージや PP、ST を作成するとき、コンポーネントから 1 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。

68　　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。

7.1.3.3 依存性

69 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性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。

70 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。一部のコンポーネントでは、「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ある。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 データ交換完全性を参照)。

71 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ィ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。

72 パート 2 に示されている依存性は規定的なものである。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。

7.2 コンポーネントカタログ

73 CC の本パートにおけるコンポーネントのグループ化は、何らかの形式的な分類方法を反映したものではない。

74 CC 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。各クラスの先頭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。

75 機能コンポーネントの記述において、1 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。

76 各クラスには、図 6 と同様のファミリの階層を記述した図が提供される。図 6 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。

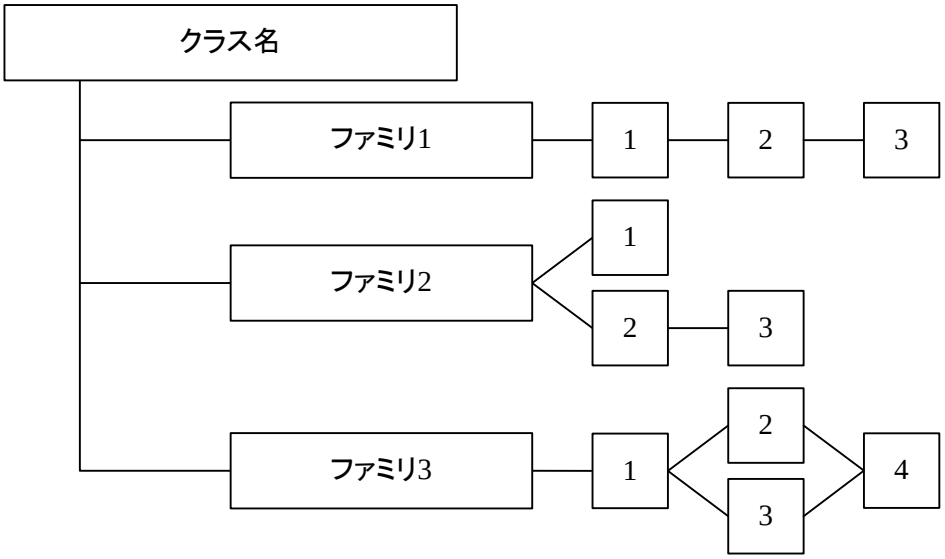


図 6　　サンプルクラスのコンポーネント構成図

77　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。

78　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。

79　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。

7.2.1　コンポーネント変更の強調表示

80　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、要件がボールドで表示される。また、前のコンポーネントを超えて許可される新しい操作または拡張操作も、**ボールド**で強調表示される。

8 クラス FAU: セキュリティ監査

81 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に関する情報の認識、記録、格納、分析（すなわち TSF によって管理されるアクティビティ）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。

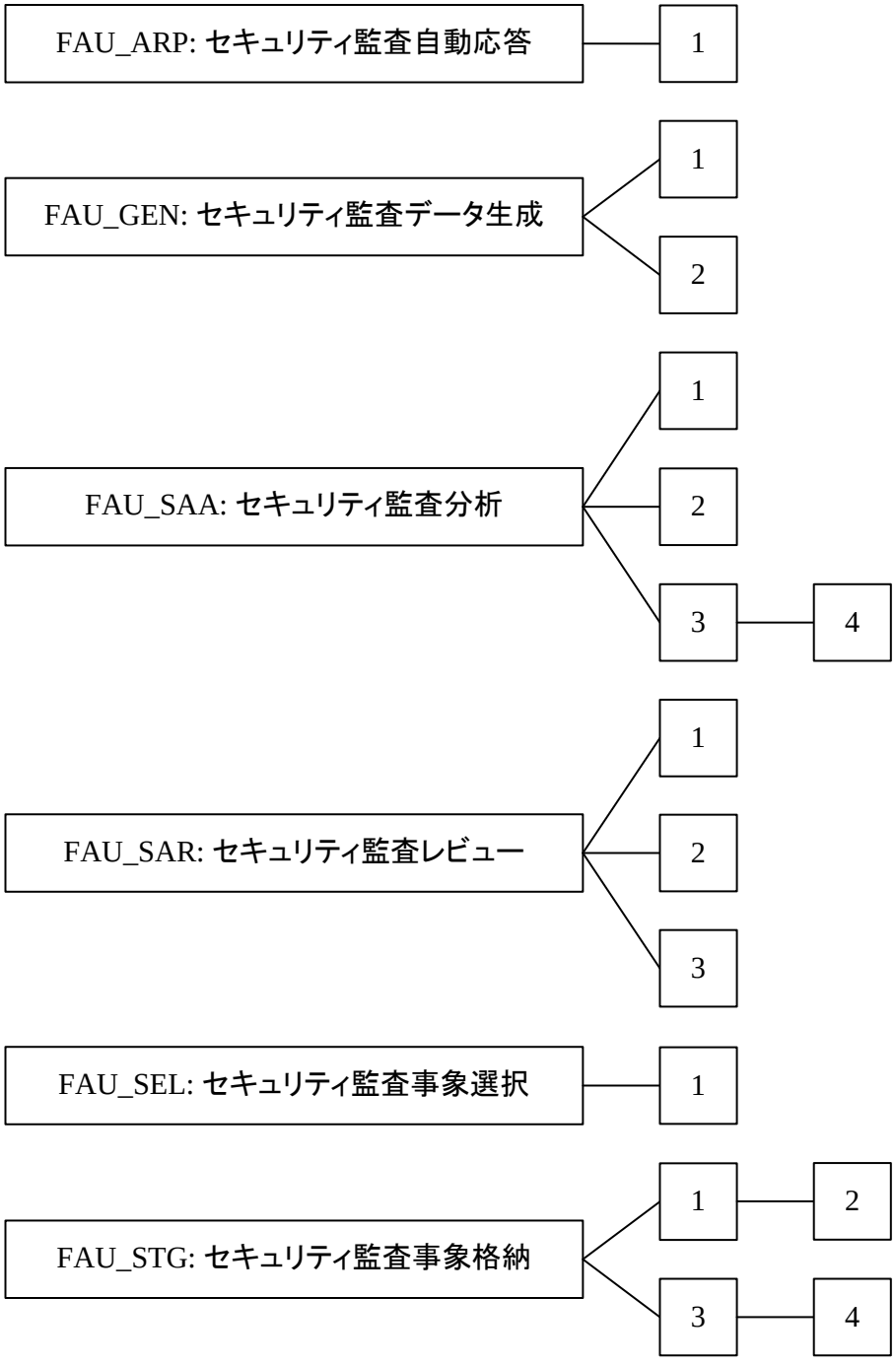


図 7 FAU: セキュリティ監査クラスのコンポーネント構成

8.1 セキュリティ監査自動応答(FAU_ARP)

ファミリのふるまい

82 このファミリでは、潜在的なセキュリティ侵害を示す事象が検出された場合にとられる対応を定義している。

コンポーネントのレベル付け

83 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

84 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) アクションの管理(追加、除去、改変)。

監査: FAU_ARP.1

85 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) 最小: 潜在的な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

依存性: FAU_SAA.1 侵害の可能性の分析

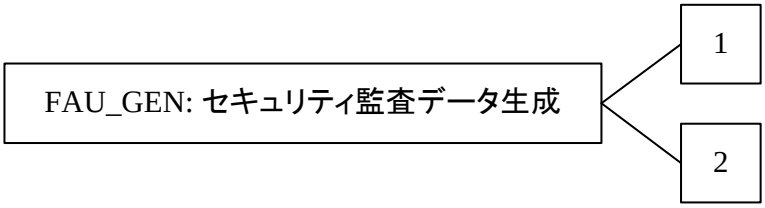
FAU_ARP.1.1 TSF は、セキュリティ侵害の可能性が検出された場合、[割付: *アクションのリスト*]を実行しなければならない。

8.2 セキュリティ監査データ生成(FAU_GEN)

ファミリのふるまい

86 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、様々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



87 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、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。

88 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

89 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

90 予見される監査対象事象はない。

FAU_GEN.1 監査データ生成

下位階層: なし

依存性: FPT_STM.1 高信頼タイムスタンプ

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*: から 1 つのみ選択]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（該当する場合）、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***]** 。

FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

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

FAU_GEN.2.1 識別された利用者のアクションがもたらした監査事象に対し、**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。

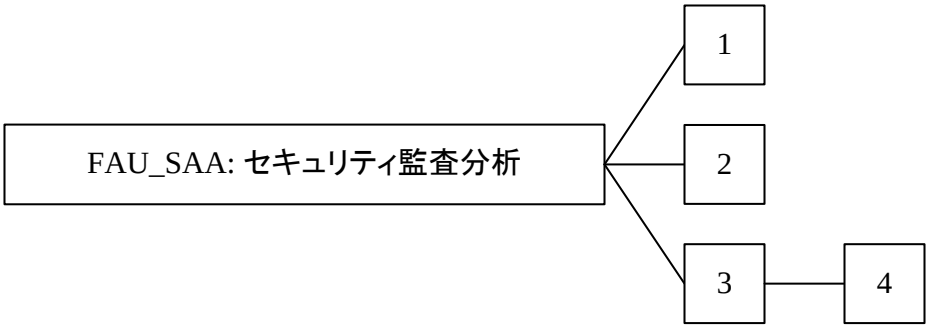
8.3 セキュリティ監査分析(FAU_SAA)

ファミリのふるまい

91 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、潜在的な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。

92 この検出に基づいてとられるアクションは、必要に応じて、セキュリティ監査自動応答(FAU_ARP)ファミリを使用して特定することができる。

コンポーネントのレベル付け



93 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的な閾値検出が要求される。

94 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。ここでプロファイルとは、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た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、1 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、1 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。

95 FAU_SAA.3 単純攻撃の発見において、TSF は、SFR 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なければならない。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。

96 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、かつ検出できなければならない。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、SFR 実施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なければならない。

管理: FAU_SAA.1

97 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) 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

98 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) 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

99 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) 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

100 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) 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

101 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) 最小: すべての分析メカニズムの動作/停止;

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

依存性: FAU_GEN.1 監査データ生成

FAU_SAA.1.1 TSF は、監査事象の監視に規則のセットを適用し、これらの規則に基づき SFR 実施の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、監査された事象を監視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*]の集積、あるいは組み合わせたもの;

b) [割付: *その他の規則*]

FAU_SAA.2 プロファイルに基づく異常検出

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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を超えた場合、SFR 実施の侵害の可能性を通知できなければならない。:[割付: *異例な動作が TSF により報告される条件*]**

FAU_SAA.3 単純攻撃の発見

下位階層: なし

依存性: なし

FAU_SAA.3.1 **TSF** は、SFR 実施の侵害を示している可能性がある以下のような特徴的事象[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.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 SFR 実施の侵害の可能性を示す特徴的事象と合致した場合、SFR 実施の侵害の可能性を通知できなければならない。

FAU_SAA.4 複合攻撃の発見

下位階層: FAU_SAA.3 単純攻撃の発見

依存性: なし

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** SFR 実施の侵害を示している**可能性がある**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。

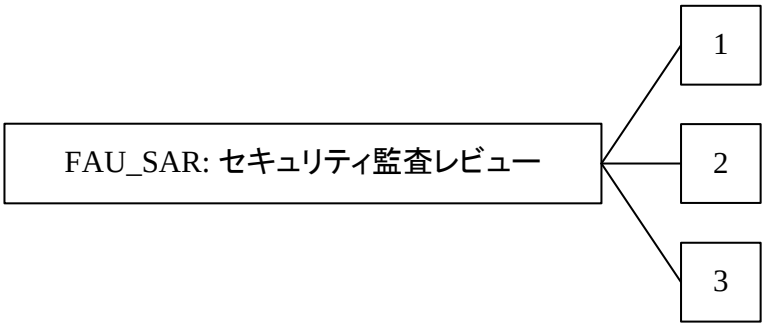
FAU_SAA.4.3 TSF は、システム**アクティビティ**が SFR 実施の侵害の可能性を示す特徴的事象**または事象シーケンス**と合致した場合、SFR 実施の侵害の可能性を通知できなければならない。

8.4 セキュリティ監査レビュー(FAU_SAR)

ファミリのふるまい

102 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べき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



103 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。

104 FAU_SAR.2 限定監査レビューは、FAU_SAR.1 監査レビュー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。

105 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

106 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) 監査記録に対して読み出しアクセス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

107 予見される管理アクティビティはない。

監査: FAU_SAR.1

108 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

109 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

110 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

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

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。**

FAU_SAR.2 限定監査レビュー

下位階層: なし

依存性: FAU_SAR.1 監査レビュー

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。**

FAU_SAR.3 選択可能監査レビュー

下位階層: なし

依存性: FAU_SAR.1 監査レビュー

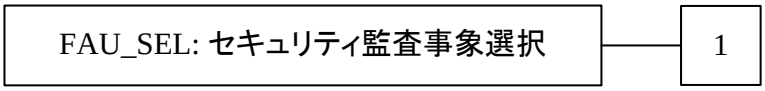
FAU_SAR.3.1 **TSF は、[割付: *論理的な関連の基準*]に基づいて、監査データの[割付: *選択方法、及びまたは 並べ替え方法*]を適用する能力を提供しなければならない。**

8.5 セキュリティ監査事象選択(FAU_SEL)

ファミリのふるまい

111 このファミリでは、すべての監査対象事象のセットから、TOE の動作中に監査される事象のセットを選択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



112 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、FAU_GEN.1 監査データ生成で識別されるすべての監査対象事象のセットから、監査する事象のセットを選択する能力を要求する。

管理: FAU_SEL.1

113 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) 監査事象を閲覧/改変する権限の維持。

監査: FAU_SEL.1

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

FAU_SEL.1 選択的監査

下位階層: なし

依存性: FAU_GEN.1 監査データ生成
FMT_MTD.1 TSF データの管理

FAU_SEL.1.1 TSF は以下のような属性に基づいて、すべての監査対象事象のセットから監査される事象のセットを選択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*]

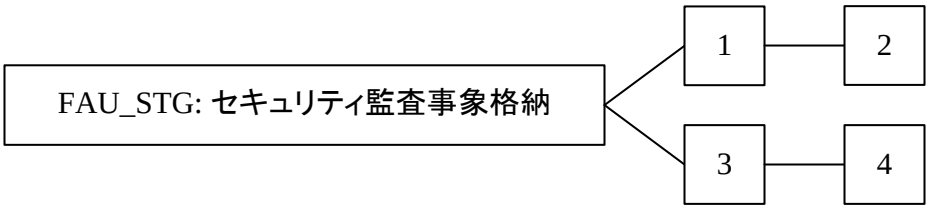
b) [割付: *監査の選択性の基礎となる追加属性リスト*]。

8.6 セキュリティ監査事象格納(FAU_STG)

ファミリのふるまい

115 このファミリでは、セキュアな監査証跡の生成あるいは維持を可能にするための TSF の要件を定義している。格納された監査記録とは、選択を通じて(一時記憶域に)読み出された監査記録ではなく、監査証跡内の記録を示す。

コンポーネントのレベル付け



116 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。

117 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特定する。

118 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特定する。

119 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特定する。

管理: FAU_STG.1

120 予見される管理アクティビティはない。

管理: FAU_STG.2

121 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) 監査格納機能を制御するパラメタの維持。

管理: FAU_STG.3

122 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) 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

123 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) 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

124 予見される監査対象事象はない。

監査: FAU_STG.3

125 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: 閾値を超えたためにとられるアクション。

監査: FAU_STG.4

126 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

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1.1 **TSF は、監査証跡に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、監査証跡に格納された監査記録への不正な改変を[選択: *防止*、*検出*: から1つのみ選択]できなければならない。**

FAU_STG.2 監査データ可用性の保証

下位階層: FAU_STG.1 保護された監査証跡格納

依存性: FAU_GEN.1 監査データ生成

FAU_STG.2.1 TSF は、監査証跡に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、監査証跡に格納された監査記録への不正な改変を[選択: *防止*、*検出*: から1つのみ選択]できなければならない。

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*]の格納された監査記録が維持されることを保証しなければならない。**

FAU_STG.3 監査データ消失の恐れ発生時のアクション

下位階層: なし

依存性: FAU_STG.1 保護された監査証跡格納

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。**

FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が**満杯**になった場合、**[選択: *監査事象の無視*、*特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止*、*最も古くに格納された監査記録への上書き*: から 1 つのみ選択]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*]を行わなければならない。

9 クラス FCO: 通信

127 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 2 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。

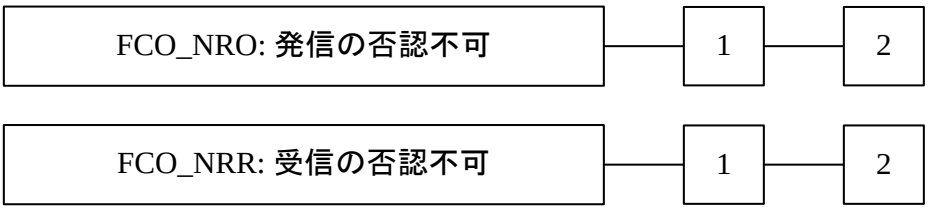


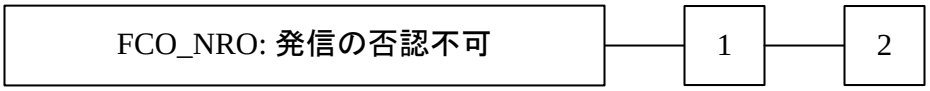
図 8 FCO: 通信クラスのコンポーネント構成

9.1 発信の否認不可(FCO_NRO)

ファミリのふるまい

128 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によって検証され得る。

コンポーネントのレベル付け



129 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。

130 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

131 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

132 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) 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

133 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) 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

依存性: FIA_UID.1 識別のタイミング

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.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。**

FCO_NRO.2 発信の強制的証明

下位階層: FCO_NRO.1 発信の選択的証明

依存性: FIA_UID.1 識別のタイミング

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。

9.2 受信の否認不可(FCO_NRR)

ファミリのふるまい

134 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

135 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。

136 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

137 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、証拠の第三者受信者の変更の管理。

監査: FCO_NRR.1

138 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) 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_NRR.2

139 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) 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_NRR.1　受信の選択的証明

下位階層:　なし

依存性:　FIA_UID.1 識別のタイミング

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.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。**

FCO_NRR.2　受信の強制的証明

下位階層:　FCO_NRR.1 受信の選択的証明

依存性:　FIA_UID.1 識別のタイミング

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**生成を常に実施**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。

10 クラス FCS: 暗号サポート

140 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、暗号機能性を採用することができる。これらは次のもの含む（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。

141 FCS: 暗号サポートクラスは、暗号鍵管理(FCS_CKM)と、暗号操作(FCS_COP)の 2 個のファミリから構成される。暗号鍵管理(FCS_CKM)ファミリは暗号鍵の管理面に対応し、暗号操作(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。

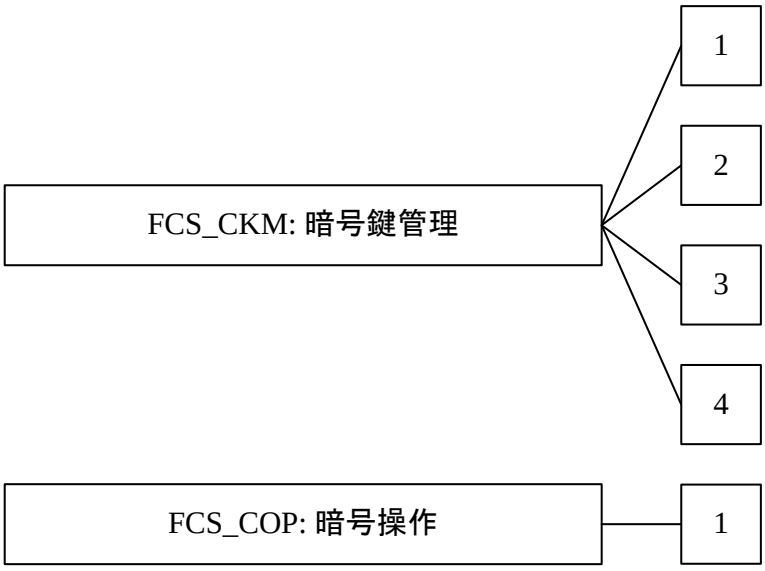


図 9 FCS: 暗号サポートクラスのコンポーネント構成

10.1 暗号鍵管理(FCS_CKM)

ファミリのふるまい

142 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、暗号鍵のライフサイクルをサポートすることを意図し、その結果として暗号鍵生成、暗号鍵配付、暗号鍵アクセス、及び暗号鍵破棄のアクティビティに対する要件を定義する。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。

コンポーネントのレベル付け

143 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。

144 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。

145 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。

146 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

147 予見される管理アクティビティはない

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

148 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) 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

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

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。

FCS_CKM.2　　暗号鍵配付

下位階層: なし

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
FDP_ITC.2 セキュリティ属性を伴う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

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。

FCS_CKM.3　　暗号鍵アクセス

下位階層: なし

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
FDP_ITC.2 セキュリティ属性を伴う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

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。

FCS_CKM.4　　暗号鍵破棄

下位階層: なし

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
FDP_ITC.2 セキュリティ属性を伴う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.4.1　　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。

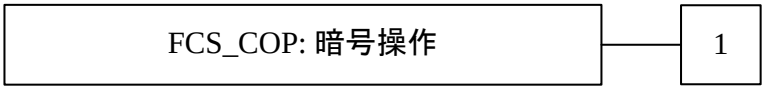
10.2 暗号操作(FCS_COP)

ファミリのふるまい

149 暗号操作が正しく機能するためには、その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るべきである。

150 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



151 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

152 予見される管理アクティビティはない。

監査: FCS_COP.1

153 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) 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

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
FDP_ITC.2 セキュリティ属性を伴う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

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。

11 クラス FDP: 利用者データ保護

154 このクラスには、利用者データの保護に関連する要件を特定するファミリが含まれる。FDP: ユーザデータ保護は、インポート、エクスポート及び保存中にTOE内の利用者データと、利用者データに直接関連するセキュリティ属性を扱う(以下にリストする)4つのファミリのグループに分割される。

155 このクラスのファミリは、次の4つのグループに分けられる:

a) 利用者データ保護におけるセキュリティ機能方針:

- アクセス制御方針(FDP_ACC);及び
- 情報フロー制御方針(FDP_IFC)。

これらのファミリのコンポーネントによって、PP/ST 作成者は、利用者データ保護のセキュリティ機能方針に名前を付け、セキュリティ対策方針に対応するために必要な方針の制御範囲を定義することができる。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の機能性を定義する規則は、アクセス制御機能(FDP_ACF)ファミリ及び情報フロー管理機能(FDP_IFF)ファミリで(それぞれ)定義される。

b) 利用者データ保護の形態:

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

c) オフライン格納、インポート及びエクスポート:

- データ認証(FDP_DAU);
- TOE からのエクスポート(FDP_ETC);
- TOE 外からのインポート(FDP_ITC)。

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

d) TSF 間通信:

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

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。

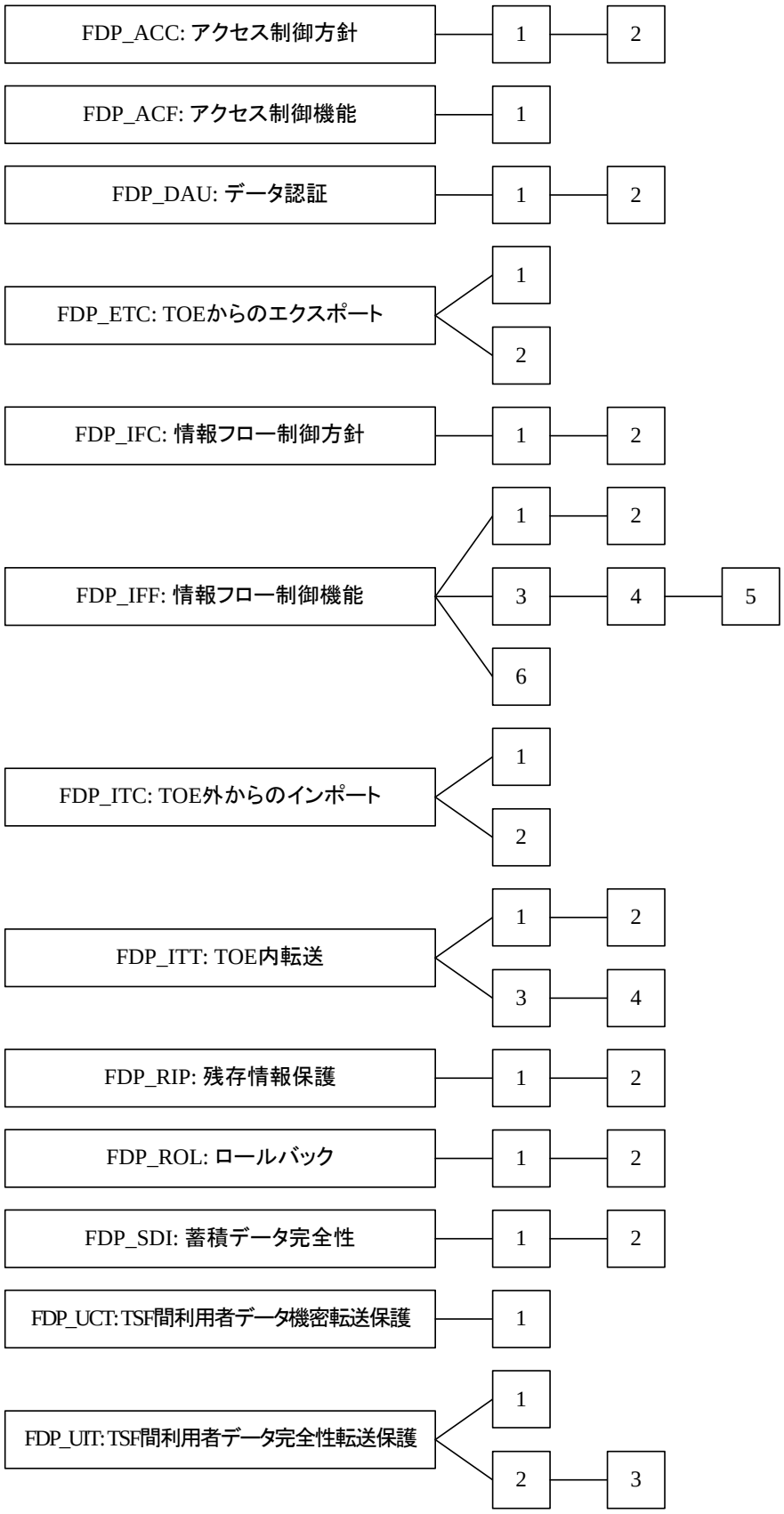


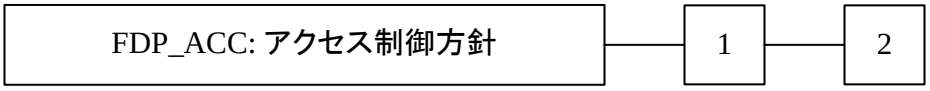
図 10　　FDP: 利用者データ保護クラスのコンポーネント構成

11.1 アクセス制御方針(FDP_ACC)

ファミリのふるまい

156 このファミリは、アクセス制御 SFP を(名前で)識別し、SFP に関連する SFR 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、3 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。本基準では、複数の方針が、各々一意の名前を持って存在することができる。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 1 つずつ繰り返すことで実現できる。アクセス制御 SFP の機能性を定義する規則は、アクセス制御機能(FDP_ACF)及び TOE からのエクスポート(FDP_ETC)のような他のファミリによって定義する。アクセス制御方針(FDP_ACC)で識別したアクセス制御 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。

コンポーネントのレベル付け



157 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。

158 FDP_ACC.2 完全アクセス制御は、識別される各アクセス制御 SFP で、その SFP によってカバーされるサブジェクト及びオブジェクトに対するすべての操作をカバーすることを要求する。さらに、TSF によって保護されるすべてのオブジェクト及び操作が、少なくとも 1 つの識別されたアクセス制御 SFP によってカバーされることを要求する。

管理: FDP_ACC.1、FDP_ACC.2

159 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

160 予見される監査対象事象はない。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

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.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。

FDP_ACC.2 完全アクセス制御

下位階層: FDP_ACC.1 サブセットアクセス制御

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.2.1 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。

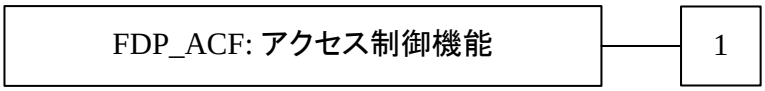
FDP_ACC.2.2 **TSF は、TSF によって制御される任意のサブジェクトと任意のオブジェクト間のすべての操作がアクセス制御 SFP でカバーされることを保証しなければならない。**

11.2 アクセス制御機能(FDP_ACF)

ファミリのふるまい

161 このファミリでは、アクセス制御方針(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。アクセス制御方針(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



162 このファミリは、セキュリティ属性の使用と方針の特性について扱う。このファミリ内のコンポーネントは、アクセス制御方針(FDP_ACC)の指定に従って、SFP を実装する機能の規則を記述するために使用することを目的としている。PP/ST 作成者は、TOE 内の複数の方針を扱うために、このコンポーネントを繰り返すこともできる。

163 FDP_ACF.1 セキュリティ属性によるアクセス制御: セキュリティ属性によるアクセス制御によって、TSF はセキュリティ属性と属性の名前付きグループに基づいてアクセス制御を実施することができる。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許可または拒否することができる。

管理: FDP_ACF.1

164 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) 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

165 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) 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

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

FDP_ACF.1.1 TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]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を決定するために、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、次の追加規則、**[**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許可する規則***]**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許可しなければならない。

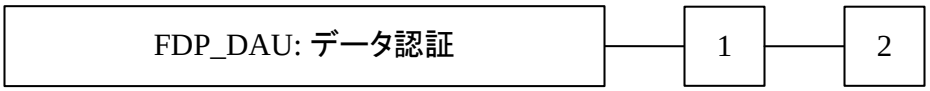
FDP_ACF.1.4 **TSF** は、次の追加規則、**[**割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則***]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

11.3 データ認証(FDP_DAU)

ファミリのふるまい

166 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: セキュリティ監査と異なり、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



167 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。

168 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

169 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) 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設定可能である。

監査: FDP_DAU.1

170 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) 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

171 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) 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

依存性:　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。**

FDP_DAU.2　　保証人識別付きデータ認証

下位階層:　FDP_DAU.1 基本データ認証

依存性:　FIA_UID.1 識別のタイミング

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。

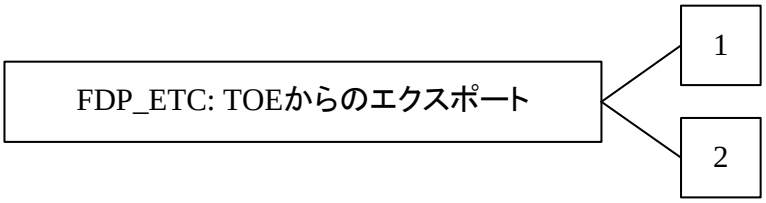
FDP_DAU.2.2　TSF は、示された情報の有効性の証拠**及び証拠を生成した利用者の識別情報**を検証する能力を[割付: *サブジェクトのリスト*]に提供しなければならない。

11.4 TOE からのエクスポート(FDP_ETC)

ファミリのふるまい

172 このファミリは、TOE から利用者データを TSF 仲介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及び保護は、明示的に保持されるか、あるいはエクスポートされた後に無視される。これは、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。

コンポーネントのレベル付け



173 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。

174 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曖昧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

175 予見される管理アクティビティはない。

管理: FDP_ETC.2

176 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) 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

177 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) 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

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_ETC.1.1 **TSF は、SFP 制御下にある利用者データを TOE の外部にエクスポートするとき、[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_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。**

FDP_ETC.2　セキュリティ属性を伴う利用者データのエクスポート

下位階層: なし

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_ETC.2.1 **TSF は、SFP 制御下にある利用者データを TOE の外部にエクスポートするとき、[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_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とも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 TOE 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 TOE からエクスポートされるとき、[割付:** ***追加のエクスポート制御規則*****]の規則を実施しなければならない。**

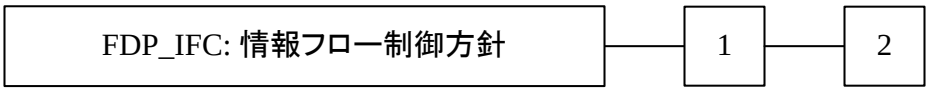
11.5 情報フロー制御方針(FDP_IFC)

ファミリのふるまい

178 このファミリは、情報フロー制御 SFP を(名前によって)識別し、各名前付き情報フロー制御 SFP の制御範囲を定義する。この制御範囲は、3 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情報、及び、方針でカバーされた、制御されたサブジェクトとの間で制御された情報をフローさせる操作。本基準では、複数の方針が、各々一意の名前を持って存在することができる。これは、各々の名前を付けた情報フロー制御方針に対して、このファミリのコンポーネントを 1 つずつ繰り返すことで実現できる。情報フロー制御 SFP の機能性を定義する規則は、情報フロー制御機能(FDP_IFF)及び TOE からのエクスポート(FDP_ETC)のような他のファミリによって定義する。情報フロー制御方針(FDP_IFC)で識別した情報フロー制御 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。

179 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



180 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。

181 FDP_IFC.2 完全情報フロー制御は、識別される各情報フロー制御 SFP で、その SFP によってカバーされるサブジェクト及び情報に対するすべての操作をカバーすることを要求する。さらに、TSF によって制御されるすべての情報フロー及び操作が、少なくとも 1 つの識別された情報フロー制御 SFP によってカバーされることを要求する。

管理: FDP_IFC.1、FDP_IFC.2

182 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

183 予見される監査対象事象はない。

FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 TSF は、[割付: *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サブジェクト、情報及び操作のリスト*]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。

FDP_IFC.2　　完全情報フロー制御

下位階層:　FDP_IFC.1 サブセット情報フロー制御

依存性:　FDP_IFF.1 単純セキュリティ属性

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。

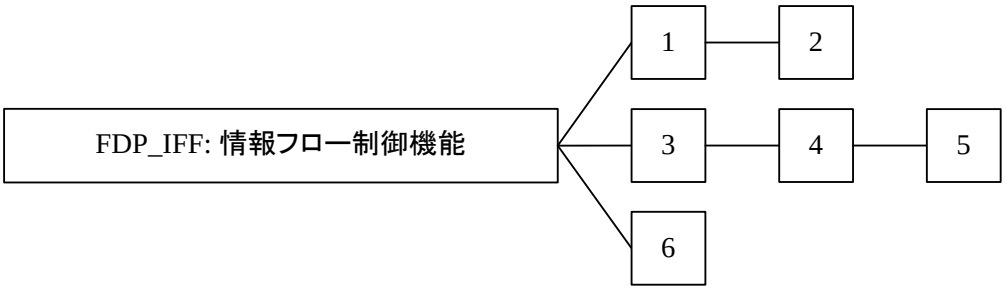
FDP_IFC.2.2　**TSF は、TOE のどのサブジェクトに、またはどのサブジェクトから、TOE の何らかの情報の流れを引き起こすすべての操作が、情報フロー制御 SFP によって扱われることを保証しなければならない。**

11.6 情報フロー制御機能(FDP_IFF)

ファミリのふるまい

184 このファミリは、方針の制御の範囲も特定する情報フロー制御方針(FDP_IFC)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。2 種類の要件から構成され、一方は共通の情報フロー機能問題に対応し、他方は不正な情報フロー(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、情報フロー制御 SFP の残りの部分に直交しているからである。それぞれの性質上、これらは方針の違反につながる情報フロー制御 SFP を回避する。このため、その発生を制限または防止するために、特別の機能が必要である。

コンポーネントのレベル付け



185 FDP_IFF.1 単純セキュリティ属性は、情報のセキュリティ属性、及び情報を流れさせるサブジェクトのセキュリティ属性とその情報の受信者としてふるまうサブジェクトのセキュリティ属性を要求する。これは、機能によって実施しなければならない規則を特定し、機能によってセキュリティ属性を導出する方法を記述する。

186 FDP_IFF.2 階層的セキュリティ属性は、SFR のセットにおけるすべての情報フロー制御 SFP が、(数学で定義される)ラティス(束)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.2.6** はラティス(束)の数学的特性から導かれる。ラティス(束)は、その特性が最初の段落により定義される秩序的な関係にある 1 セットのエレメントで構成され、最小上限が、セットの中でユニークなエレメントで、秩序的関係の中で、ラティス(束)の他のエレメントよりも大きいか同じ、最大下限が、セットの中でユニークなエレメントで、ラティス(束)の他のエレメントより小さいか同じである。

187 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。

188 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。

189 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。

190 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

191 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) 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

192 予見される管理アクティビティはない。

管理: FDP_IFF.6

193 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) 監視機能の有効化及び無効化。

b) 監視の対象となる最大容量の改変。

監査: FDP_IFF.1、FDP_IFF.2、FDP_IFF.5

194 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) 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: 情報フローの実施の決定を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、情報の特定のサブセット(例えば、対象物の劣化の監査)。

監査: FDP_IFF.3、FDP_IFF.4、FDP_IFF.6

195 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) 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

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.1.1 **TSF は、以下のタイプのサブジェクト及び情報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: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性*]**

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、以下の規則、[割付: *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する規則*]に基づいて、情報フローを明示的に許可しなければならない。**

FDP_IFF.1.5 **TSF は、以下の規則、[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]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。**

FDP_IFF.2 階層的セキュリティ属性

下位階層: FDP_IFF.1 単純セキュリティ属性

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.2.1 TSF は、以下のタイプのサブジェクト及び情報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: *示されたSFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性*]

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、以下の規則、[割付: *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する規則*]に基づいて、情報フローを明示的に許可しなければならない。

FDP_IFF.2.5 TSF は、以下の規則、[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]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。

FDP_IFF.2.6 **TSF は、以下の関係を任意の 2 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) **2 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 **2** つの有効なセキュリティ属性を考えたとき、この **2** 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 **2** つの有効なセキュリティ属性を考えたとき、この **2** 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。

FDP_IFF.3 制限付き不正情報フロー

下位階層: なし

依存性: FDP_IFC.1 サブセット情報フロー制御

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。**

FDP_IFF.4 不正情報フローの部分的排除

下位階層: FDP_IFF.3 制限付き不正情報フロー

依存性: FDP_IFC.1 サブセット情報フロー制御

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、[割付: *不正情報フローの種別*]を防止しなければならない。**

FDP_IFF.5 不正情報フローなし

下位階層: FDP_IFF.4 不正情報フローの部分的排除

依存性: FDP_IFC.1 サブセット情報フロー制御

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。

FDP_IFF.6 不正情報フロー監視

下位階層: なし

依存性: FDP_IFC.1 サブセット情報フロー制御

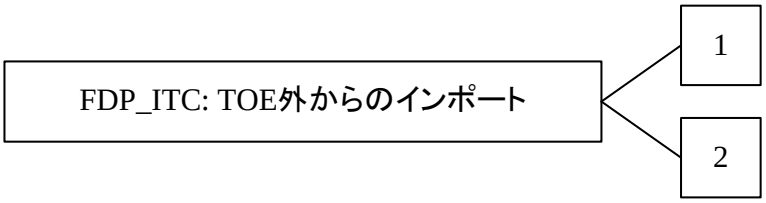
FDP_IFF.6.1 **TSF は、[割付: *不正情報フローの種別*]が[割付: *最大容量*]を超えるのを監視するために[割付: *情報フロー制御 SFP*]を実施しなければならない。**

11.7 TOE 外からのインポート(FDP_ITC)

ファミリのふるまい

196 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 TSF 仲介インポートするためのメカニズムを定義する。これは、インポート時の制限、必要な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るセキュリティ属性の解釈に関係する。

コンポーネントのレベル付け



197 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。

198 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 TOE 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

199 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) 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

200 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) 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

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.1.1　**TSF は、SFP 制御下にある利用者データを TOE の外部からインポートするとき、[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.1.2　**TSF は、TOE 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、TOE 外部から SFP の下で制御される利用者データをインポートするとき、[割付:** ***追加のインポート制御規則*****]の規則を実施しなければならない。**

FDP_ITC.2　セキュリティ属性を伴う利用者データのインポート

下位階層:　なし

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 データ一貫性

FDP_ITC.2.1　**TSF は、SFP 制御下にある利用者データを TOE の外部からインポートするとき、[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_ITC.2.3　**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、TOE 外部から SFP の下で制御される利用者データをインポートするとき、[割付:** ***追加のインポート制御規則*****]の規則を実施しなければならない。**

11.8 TOE 内転送(FDP_ITT)

ファミリのふるまい

201 このファミリは、内部チャネルを介して TOE の分離した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、TSF 間利用者データ機密転送保護(FDP_UCT)及び TSF 間利用者データ完全性転送保護(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 TOE からのエクスポート(FDP_ETC)及び TOE 外からのインポート(FDP_ITC)は、TSF 外へ/からのデータの TSF 仲介転送に対応する。

コンポーネントのレベル付け

202 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。

203 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。

204 FDP_ITT.3 完全性監視は、識別された完全性誤りに対して、TSF 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。

205 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、3 番目のコンポーネントを拡張する。

管理: FDP_ITT.1、FDP_ITT.2

206 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) 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

207 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) 完全性誤り検出時にと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

208 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) 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

209 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) 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: 完全性誤り検出においてとられたアクション。

FDP_ITT.1 基本内部転送保護

下位階層: なし

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.1.1 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 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.2 属性による転送分離

下位階層: FDP_ITT.1 基本内部転送保護

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.2.1 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 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.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、[割付: *分離を要求するセキュリティ属性*]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:

FDP_ITT.3　　完全性監視

下位階層:　なし

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.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 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.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。**

FDP_ITT.4　　属性に基づく完全性監視

下位階層:　FDP_ITT.3 完全性監視

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

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。

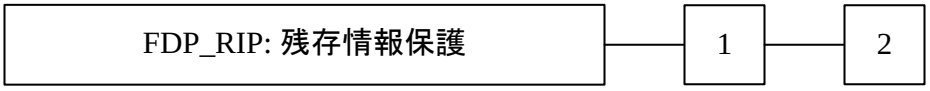
FDP_ITT.4.2　データ完全性誤りの検出において、TSF は[割付: *完全性誤りにおいてとられるアクションを特定*]しなければならない。

11.9 残存情報保護(FDP_RIP)

ファミリのふるまい

210 このファミリは、リソースがあるオブジェクトから割当て解除された場合や、別のオブジェクトに再割当てされた場合は、リソースに含まれるいかなるデータも無効であることを保証する必要性について扱う。このファミリは、論理的に削除された、あるいは解放されたリソースに含まれるが、TSF 制御リソース内にまだ存在するかもしれないデータ、言い換えれば、他のオブジェクトに再割当てされるかもしれないどんなデータに対してもデータの保護を要求する。

コンポーネントのレベル付け



211 FDP_RIP.1 サブセット残存情報保護は、TSF によって制御される定義済み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。

212 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

213 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) 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

214 予見される監査対象事象はない。

FDP_RIP.1 サブセット情報保護

下位階層: なし

依存性: なし

FDP_RIP.1.1 TSF は、[割付: *オブジェクトのリスト*]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。

FDP_RIP.2 全残存情報保護

下位階層: FDP_RIP.1 サブセット残存情報保護

依存性: なし

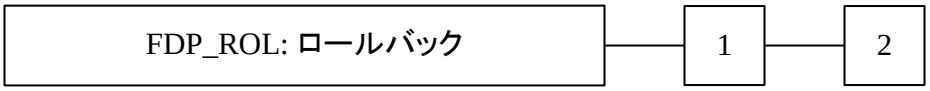
FDP_RIP.2.1 TSF は、**すべての**オブジェクト[選択: *への資源の割当て、からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

11.10 ロールバック(FDP_ROL)

ファミリのふるまい

215 ロールバック操作とは、直前の操作、または時間などの何らかの制限によって境界を指定された一連の操作を元に戻し、以前の定義された状態に戻すことである。ロールバックは、利用者データの完全性を維持したまま、操作または一連の操作の結果を元に戻す機能を提供する。

コンポーネントのレベル付け



216 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。

217 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

218 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) 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

219 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) 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

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.1.1 TSF は、[割付: *情報及び/または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 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_ROL.1.2 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。

FDP_ROL.2　　高度ロールバック

下位階層:　FDP_ROL.1 基本ロールバック

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.2.1　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 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。

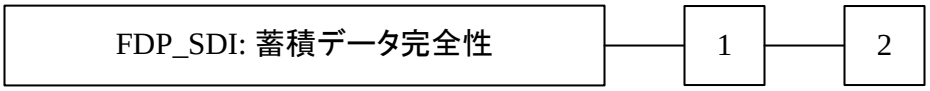
FDP_ROL.2.2　TSF は、[割付: *ロールバックを実行できる境界限界*]内で操作がロールバックされることを許可しなければならない。

11.11 蓄積データ完全性(FDP_SDI)

ファミリのふるまい

220 このファミリでは、TSF によって制御されるコンテナ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。完全性誤りは、メモリまたは記憶装置に格納された利用者データに影響を与えることがある。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 TOE 内転送(FDP_ITT)とは異なるものである。

コンポーネントのレベル付け



221 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、TSF によって制御されるコンテナ内部に蓄積された利用者データを TSF が監視することを要求する。

222 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と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

223 予見される管理アクティビティはない。

管理: FDP_SDI.2

224 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) 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

225 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) 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

226 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) 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

依存性: 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、[割付: *利用者データ属性*]の属性に基づき、TSF によって制御されるコンテナ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。

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 蓄積データ完全性監視

依存性: なし

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、[割付: *利用者データ属性*]の属性に基づき、TSF によって制御されるコンテナ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。

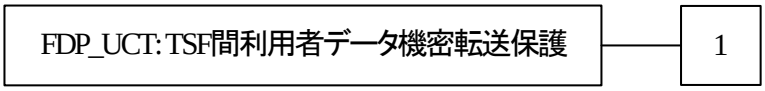
FDP_SDI.2.2 データ完全性誤り検出時に、TSF は[割付: *とられるアクション*]を行なわねばならない。

11.12 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

227 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。

コンポーネントのレベル付け



228 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

229 予見される管理アクティビティはない。

監査: FDP_UCT.1

230 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) 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、不許可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性

下位階層: なし

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]

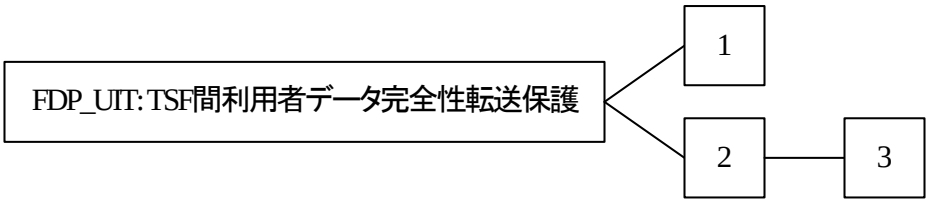
FDP_UCT.1.1 TSF は、不当な暴露から保護した形で利用者データの[選択: *送信*、*受信*]を行うために、[割付: *アクセス制御 SFP 及びまたは情報フロー制御 SFP*]を実施しなければならない。

11.13 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

231 このファミリは、TOE 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様々な方法をサポートする。

コンポーネントのレベル付け



232 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。

233 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。

234 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

235 予見される管理アクティビティはない。

監査: FDP_UIT.1

236 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) 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/または影響。

監査: FDP_UIT.2、FDP_UIT.3

237 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) 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) 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。

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/または影響。

FDP_UIT.1 データ交換完全性

下位階層: なし

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.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*]を行うために、[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_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。

FDP_UIT.2 発信側データ交換回復

下位階層: なし

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、または
FTP_ITC.1 TSF 間高信頼チャネル]

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 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_UIT.3 着信側データ交換回復

下位階層: FDP_UIT.2 発信側データ交換回復

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、または
FTP_ITC.1 TSF 間高信頼チャネル]

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 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。

12 クラス FIA: 識別と認証

238 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。

239 「識別と認証」は、適切なセキュリティ属性(例えば識別情報、グループ、役割、セキュリティあるいは完全性レベル)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。

240 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。

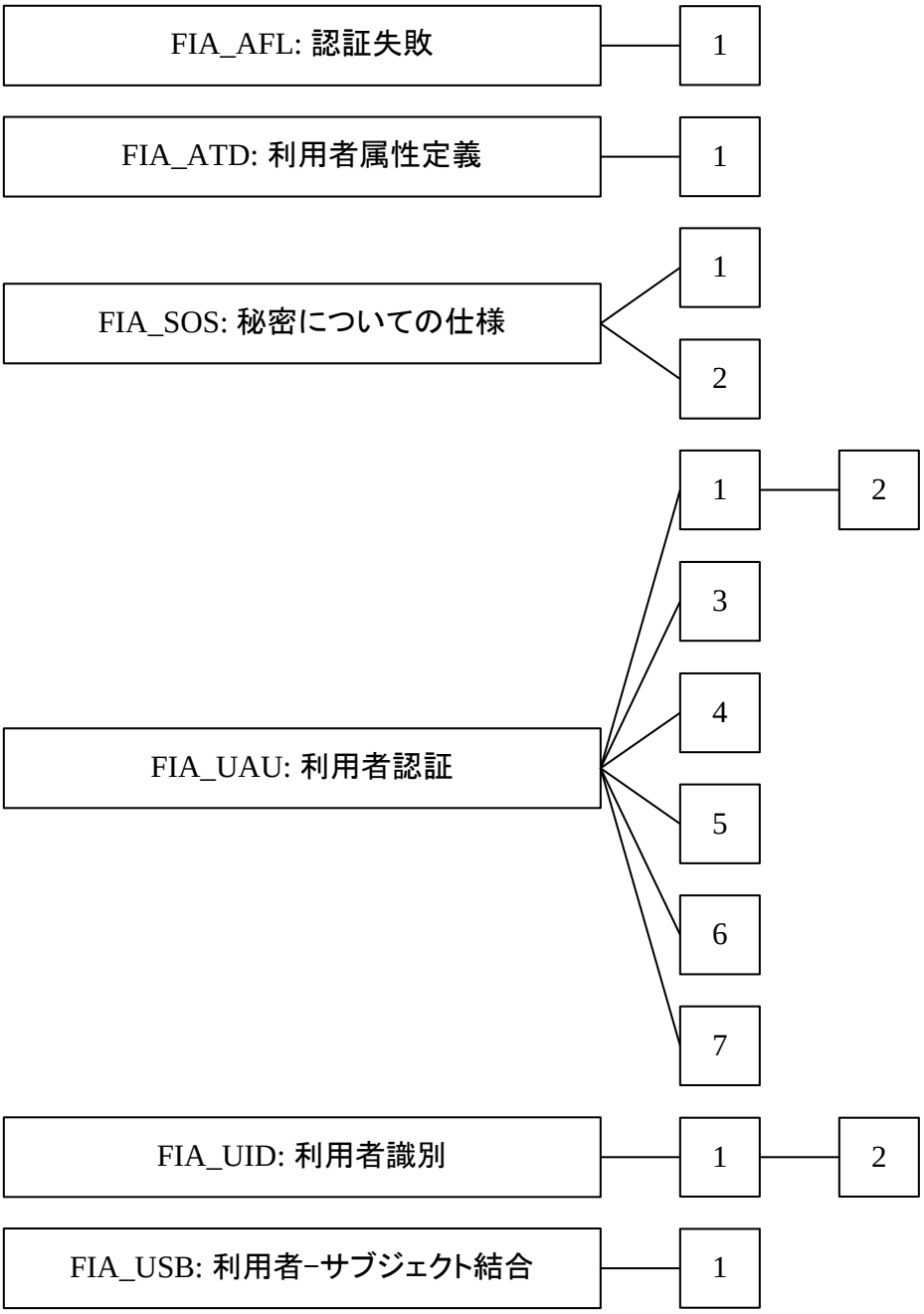


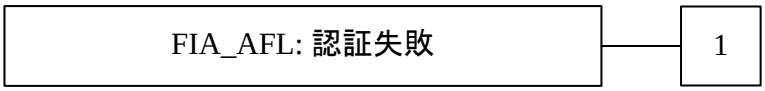
図 11　　FIA: 識別と認証クラスのコンポーネント構成

12.1 認証失敗(FIA_AFL)

ファミリのふるまい

241 このファミリには、不成功の認証試行の回数に関する値、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が含まれる。パラメタは、失敗した認証試行回数及び時間の閾値を含むが、それに限定されない。

コンポーネントのレベル付け



242 FIA_AFL.1 認証失敗時の取り扱いは、利用者の不成功の認証試行が特定した数になった後、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

243 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

244 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) 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

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。

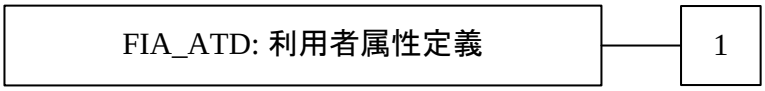
FIA_AFL.1.2 不成功の認証試行が定義した回数[選択:に達する、を上回った]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。

12.2 利用者属性定義(FIA_ATD)

ファミリのふるまい

245 すべての許可利用者は、その利用者の識別情報以外に、SFR 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、セキュリティ上の決定において TSF 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。

コンポーネントのレベル付け



246 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

247 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

248 予見される監査対象事象はない。

FIA_ATD.1 利用者属性定義

下位階層: なし

依存性: なし

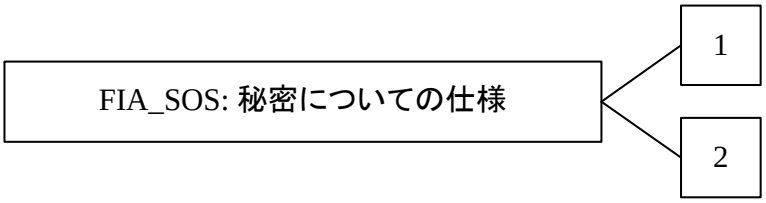
FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]

12.3 秘密についての仕様(FIA_SOS)

ファミリのふるまい

249 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



250 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。

251 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

252 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

253 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

254 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) 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

依存性: 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。

FIA_SOS.2　　TSF 秘密生成

下位階層:　なし

依存性:　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。

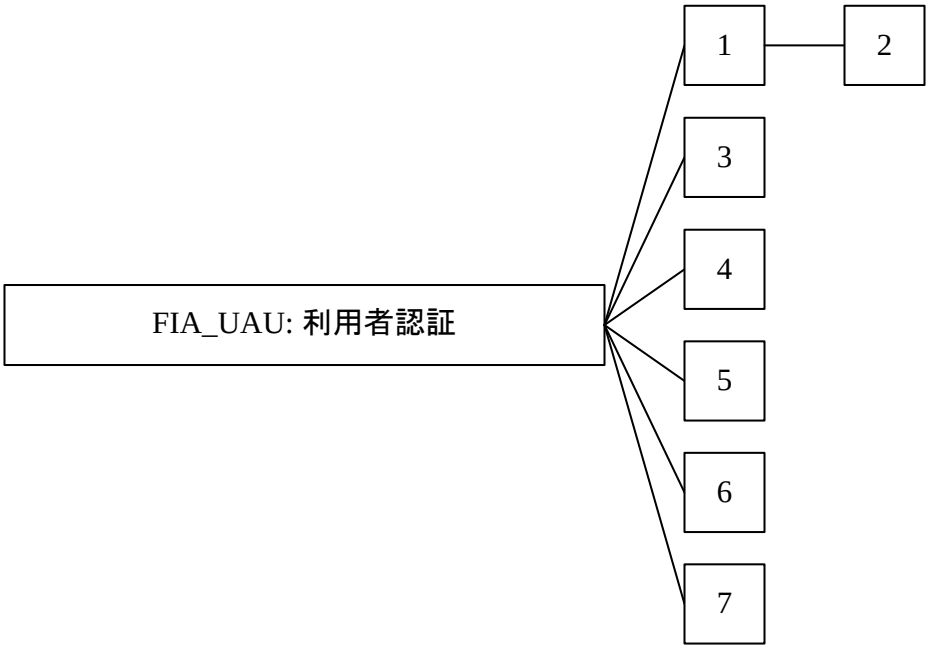
FIA_SOS.2.2　**TSF** は、**[**割付**:** ***TSF*** *機能のリスト***]**に対し、**TSF** 生成の秘密の使用を実施できなければならない。

12.4 利用者認証(FIA_UAU)

ファミリのふるまい

255 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、要求された属性も定義する。

コンポーネントのレベル付け



256 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。

257 FIA_UAU.2 アクション前の利用者認証は、TSF がその他のアクションを許可する前に、利用者の認証を要求する。

258 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。

259 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。

260 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。

261 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。

262 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

263 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) 管理者による認証データの管理;

b) 関係する利用者による認証データの管理;

c) 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

264 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) 管理者による認証データの管理;

b) 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

265 予見される管理アクティビティはない。

管理: FIA_UAU.5

266 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) 認証メカニズムの管理;

b) 認証に対する規則の管理。

管理: FIA_UAU.6

267 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

268 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) 最小: 認証メカニズムの不成功になった使用;

b) 基本: 認証メカニズムのすべての使用;

c) 詳細: 利用者認証以前に行われたすべての TSF 仲介アクション。

監査: FIA_UAU.2

269 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) 最小: 認証メカニズムの不成功になった使用;

b) 基本: 認証メカニズムのすべての使用。

監査: FIA_UAU.3

270 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) 最小: 不正な認証データの検出;

b) 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

271 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) 最小: 認証データを再使用する試み。

監査: FIA_UAU.5

272 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) 最小: 認証の最終決定;

b) 基本: 最終決定でともに用いられた、各々の稼動したメカニズムの結果。

監査: FIA_UAU.6

273 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) 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

274 予見される監査対象事象はない。

FIA_UAU.1 認証のタイミング

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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 仲介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すべての TSF 仲介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。

FIA_UAU.2　　アクション前の利用者認証

下位階層:　FIA_UAU.1 認証のタイミング

依存性:　FIA_UID.1 識別のタイミング

FIA_UAU.2.1　TSF は、その利用者を代行する他の TSF 仲介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。

FIA_UAU.3　　偽造されない認証

下位階層:　なし

依存性:　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*、*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*、*防止*]しなければならない。**

FIA_UAU.4　　単一使用認証メカニズム

下位階層:　なし

依存性:　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。**

FIA_UAU.5　　複数の認証メカニズム

下位階層:　なし

依存性:　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。**

FIA_UAU.6　　再認証

下位階層:　なし

依存性:　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。**

FIA_UAU.7　　保護された認証フィードバック

下位階層:　なし

依存性:　FIA_UAU.1 認証のタイミング

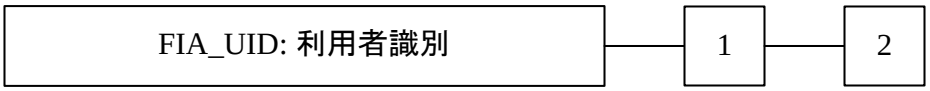
FIA_UAU.7.1　**TSF** は、認証を行っている間、**[割付:** *フィードバックのリスト***]**だけを利用者に提供しなければならない。

12.5 利用者識別(FIA_UID)

ファミリのふるまい

275 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 が仲介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



276 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。

277 FIA_UID.2 アクション前の利用者識別は、TSF がその他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

278 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

279 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、FIA_UID.2

280 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) 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

依存性: 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 仲介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 仲介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。**

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 仲介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。

12.6 利用者-サブジェクト結合(FIA_USB)

ファミリのふるまい

281 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。

コンポーネントのレベル付け

282 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マッピングされるサブジェクト属性との関連付けを管理する規則の仕様を要求する。

管理: FIA_USB.1

283 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。

b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる。

監査: FIA_USB.1

284 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) 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または失敗)。

FIA_USB.1 利用者-サブジェクト結合

下位階層: なし

依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 TSF は、以下の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。: [割付: *利用者セキュリティ属性のリスト*]

FIA_USB.1.2 TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の最初の関連付けの規則*]

FIA_USB.1.3 TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の変更の規則*]

13 クラス FMT: セキュリティ管理

285 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。

286 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。

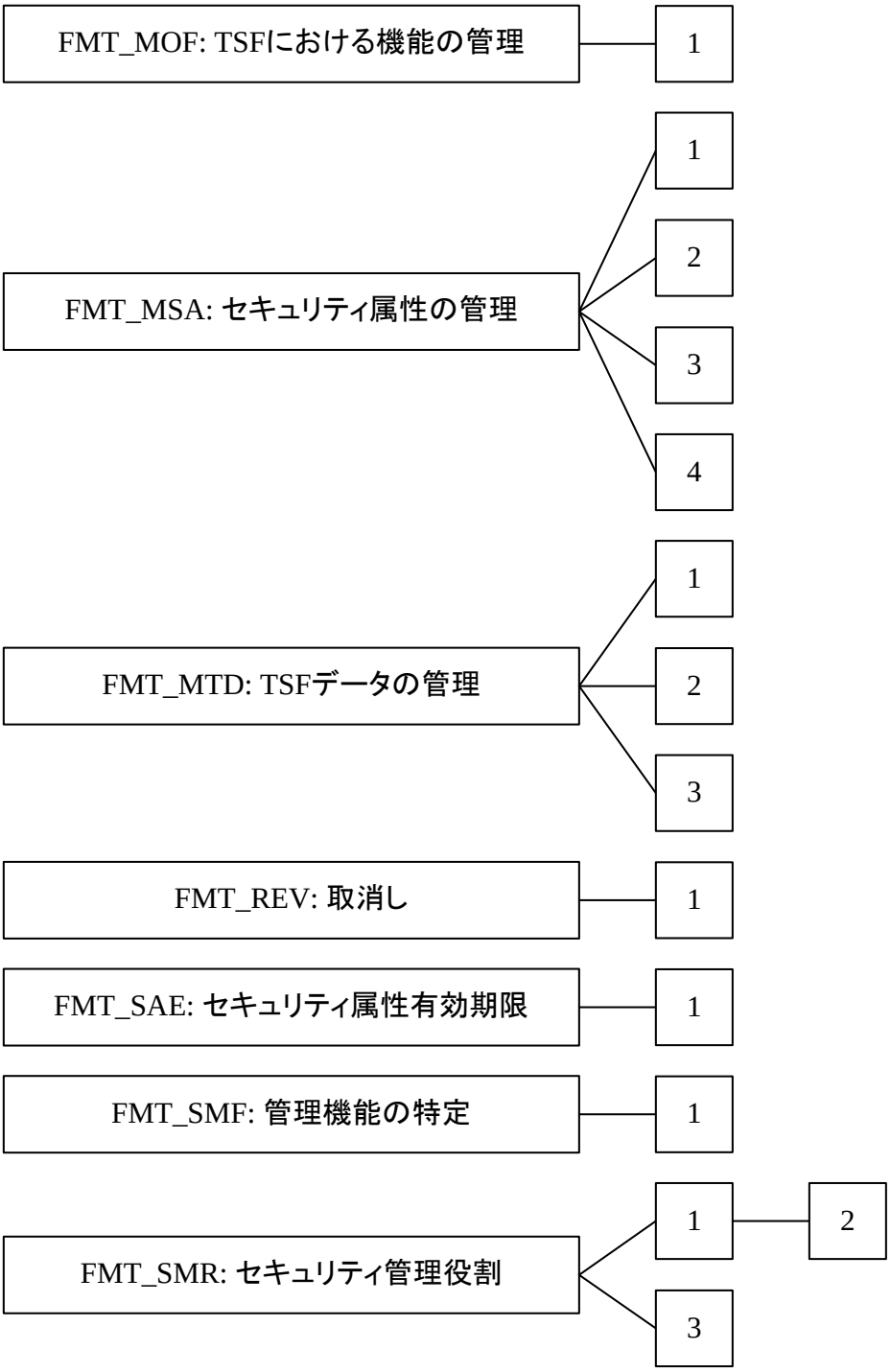


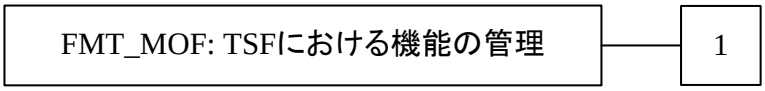
図 12　　FMT: セキュリティ管理クラスのコンポーネント構成

13.1 TSF における機能の管理(FMT_MOF)

ファミリのふるまい

287 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



288 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

289 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) 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

290 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: 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

依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

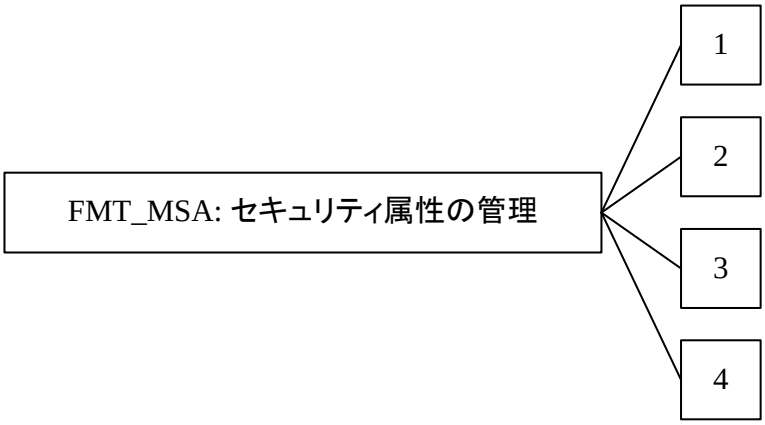
FMT_MOF.1.1 TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。

13.2 セキュリティ属性の管理(FMT_MSA)

ファミリのふるまい

291 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機能が含まれる。

コンポーネントのレベル付け



292 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。

293 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。

294 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。

295 FMT_MSA.4 セキュリティ属性値継承により、セキュリティ属性によって引き継がれる値を決定する規則／方針が詳述される。

管理: FMT_MSA.1

296 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) 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;

b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。

管理: FMT_MSA.2

297 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) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。

管理: FMT_MSA.3

298 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) 初期値を特定し得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;

c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。

管理: FMT_MSA.4

299 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) セキュリティ属性を確立すること、あるいは改変することを許可する役割の特定。

監査: FMT_MSA.1

300 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: セキュリティ属性の値の改変すべて。

監査: FMT_MSA.2

301 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) 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

302 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: 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。

監査: FMT_MSA.4

303 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:セキュリティ属性の変更　場合によっては、古いセキュリティ属性　及び／または変更されたセキュリティ属性の値。

FMT_MSA.1　　セキュリティ属性の管理

下位階層:　なし

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 セキュリティの役割
FMT_SMF.1 管理機能の特定

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[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.2　　セキュアなセキュリティ属性

下位階層:　なし

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.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

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

FMT_MSA.3　　静的属性初期化

下位階層:　なし

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

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に対して[選択: *制限的*、*許可的*、*[割付: その他の特性]*: から 1 つのみ選択]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特定することを許可しなければならない。**

FMT_MSA.4　　セキュリティ属性値継承

下位階層:　なし

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.4.1　**TSF は、セキュリティ属性の値を設定するために、以下の規則を使わなければならない[割付: *セキュリティ属性の値設定のための規則*]**

13.3 TSF データの管理(FMT_MTD)

ファミリのふるまい

304 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、及びその他の TSF 構成パラメタがある。

コンポーネントのレベル付け

305 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。

306 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。

307 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

308 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) 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

309 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) 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

310 予見される管理アクティビティはない。

監査: FMT_MTD.1

311 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: TSF データの値のすべての改変。

監査: FMT_MTD.2

312 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: 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

313 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) 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

依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

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。

FMT_MTD.2 TSF データにおける限界値の管理

下位階層: なし

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

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*]

FMT_MTD.3 セキュアな TSF データ

下位階層: なし

依存性: FMT_MTD.1 TSF データの管理

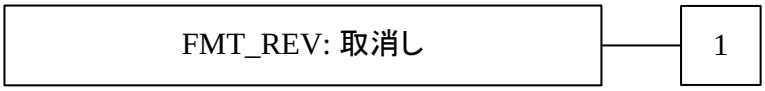
FMT_MTD.3.1 TSF は、[割付: *TSF データのリスト*]としてセキュアな値だけが受け入れられることを保証しなければならない。

13.4 取消し(FMT_REV)

ファミリのふるまい

314 このファミリは、TOE 内の様々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。

コンポーネントのレベル付け



315 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

316 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) 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

317 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) 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

依存性: FMT_SMR.1 セキュリティの役割

FMT_REV.1.1 TSF は、TSF の制御下で、[選択: *利用者*、*サブジェクト*、*オブジェクト*、*[割付: その他追加の資源]*]に関連した[割付: *セキュリティ属性のリスト*]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。

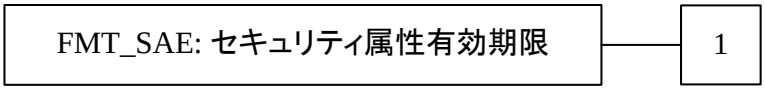
TSF_REV.1.2 TSF は、規則[割付: *取消し規則の詳述*]を実施しなければならない。

13.5 セキュリティ属性有効期限(FMT_SAE)

ファミリのふるまい

318 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



319 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

320 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) 有効期限がサポートされる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

321 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: 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

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

FMT_SAE.1.1 TSF は、[割付: *有効期限がサポートされる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。

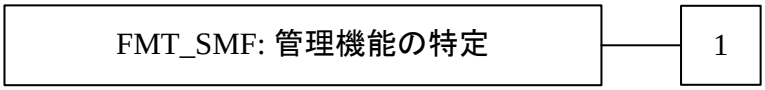
FMT_SAE.1.2 これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、[割付: *各々のセキュリティ属性に対してとられるアクションのリスト*]を行えなければならない。

13.6 管理機能の特定(FMT_SMF)

ファミリのふるまい

322 このファミリは、TOE が管理機能を特定することを可能にする。管理機能は、管理者が TOE のセキュリティに関わる側面を制御するパラメタを定義するための TSFI を提供する。それらは、例えばデータ保護属性、TOE 保護属性、監査属性、及び識別認証属性である。管理機能には、バックアップ及び回復のように、運用者が継続した TOE の運用を保証するために行う機能も含まれる。このファミリは、FMT クラスの他のコンポーネントとともに動作する。FMT: セキュリティ管理クラス: このファミリのコンポーネントは、管理機能を要求し、FMT セキュリティ管理の他のファミリは、これらの管理機能を使用することを制限する。

コンポーネントのレベル付け



323 FMT_SMF.1 管理機能の特定は、TSF が特定の管理機能を提供することを要求する。

管理: FMT_SMF.1

324 予見される管理アクティビティはない。

監査: FMT_SMF.1

325 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) 最小: 管理機能の使用

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]

13.7 セキュリティ管理役割(FMT_SMR)

ファミリのふるまい

326 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

327 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。

328 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。

329 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

330 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) 役割の一部をなす利用者のグループの管理。

管理: FMT_SMR.2

331 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) 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

332 予見される管理アクティビティはない。

監査: FMT_SMR.1

333 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) 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

334 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) 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

335 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) 最小: 役割を負わせる明示的な要求。

FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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付けなければならない。

FMT_SMR.2 セキュリティ役割における制限

下位階層: FMT_SMR.1 セキュリティの役割

依存性: FIA_UID.1 識別のタイミング

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。

FMT_SMR.3 負わせる役割

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMR.3.1 TSF は、[割付: *役割*]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:。

14 クラス FPR: プライバシー

336 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。

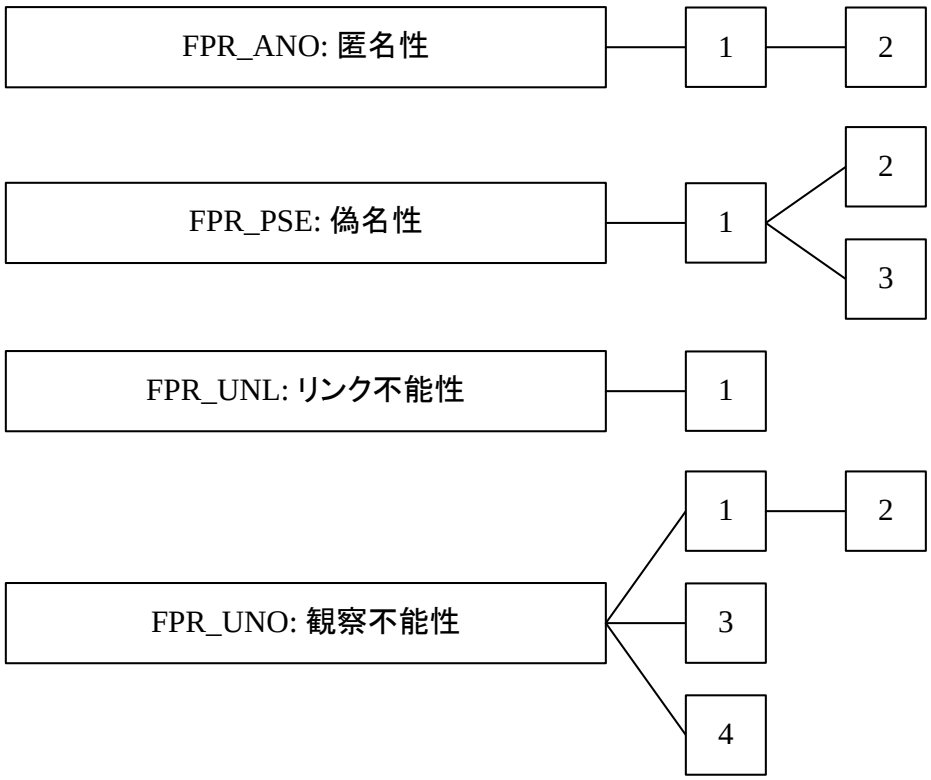


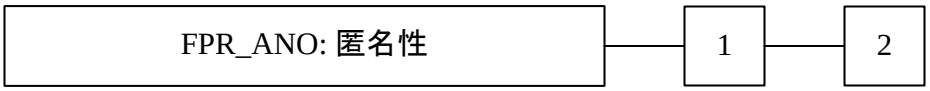
図 13 FPR: プライバシークラスのコンポーネント構成

14.1 匿名性(FPR_ANO)

ファミリのふるまい

337 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ことを保証する。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



338 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。

339 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 匿名性の要件を強化する。

管理: FPR_ANO.1、FPR_ANO.2

340 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

341 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) 最小: 匿名メカニズムの呼出。

FPR_ANO.1 匿名性

下位階層: なし

依存性: 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_ANO.2 情報を請求しない匿名性

下位階層: FPR_ANO.1 匿名性

依存性: なし

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。

14.2 偽名性(FPR_PSE)

ファミリのふるまい

342 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

343 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。

344 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。

345 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

346 予見される管理アクティビティはない。

監査: FPR_PSE.1、FPR_PSE.2、FPR_PSE.3

347 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) 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

依存性: 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*: から 1 つのみ選択]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 可逆偽名性

下位階層: FPR_PSE.1 偽名性

依存性: FIA_UID.1 識別のタイミング

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*: から 1 つのみ選択]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。**

FPR_PSE.3 別名偽名性

下位階層: FPR_PSE.1 偽名性

依存性: なし

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*: から 1 つのみ選択]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。

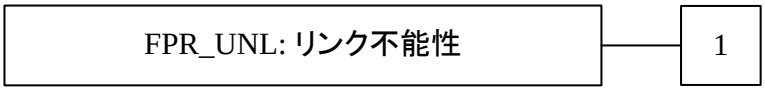
FPR_PSE.3.4 **TSF は、以下の[割付: *条件のリスト*]のもとでは、実利用者名に対して以前に提供された別名と同一の別名を提供しなければならず、そうでない場合は、提供される別名は、以前に提供された別名と無関係でなければならない。**

14.3 リンク不能性(FPR_UNL)

ファミリのふるまい

348 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



349 FPR_UNL.1 リンク不能性は、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

350 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

351 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) 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

依存性: なし

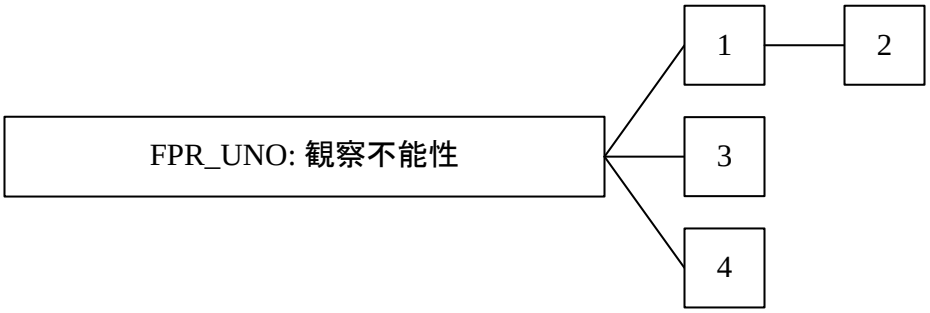
FPR_UNL.1.1 TSF は、[割付: *操作のリスト*]が[選択: *同じ利用者によって実行された、以下のように関係する[割付: 関係のリスト]*]かどうかを[割付: *利用者及びまたはサブジェクトのセット*]が決定できないことを保証しなければならない。

14.4 観察不能性(FPR_UNO)

ファミリのふるまい

352 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



353 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。

354 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。

355 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。

356 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

357 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) 観察不能機能のふるまいの管理。

管理: FPR_UNO.3

358 予見される管理アクティビティはない。

管理: FPR_UNO.4

359 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) 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

360 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) 最小: 観察不能性メカニズムの呼出。

監査: FPR_UNO.3

361 予見される監査対象事象はない。

監査: FPR_UNO.4

362 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) 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

依存性: 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。

FPR_UNO.2 観察不能性に影響を与える情報の配置

下位階層: FPR_UNO.1 観察不能性

依存性: なし

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*]。

FPR_UNO.3 情報を請求しない観察不能性

下位階層: なし

依存性: FPR_UNO.1 観察不能性

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。

FPR_UNO.4 許可利用者観察可能性

下位階層: なし

依存性: 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。

15 クラス FPT: TSF の保護

363 このクラスは、TSF を構成するメカニズムの完全性及び管理に関係し、かつ TSF データの完全性に関係する機能要件のファミリを含む。ある意味で、この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ネントと重複しているように見えるかもしれず、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: 利用者データ保護は、利用者データ保護に焦点を当てているのに対し、FPT: TSF 保護は TSF データ保護に焦点を当てている。実際、FPT: TSF 保護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。

364 このクラスの観点から、TSF に関して、次の 3 つの重要なエレメントがある:

a) TSF の実装、これは SFR を実施するメカニズムを実行し、実装する。

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

c) SFR を実施するために、TSF が相互に影響し得る外部エンティティ。

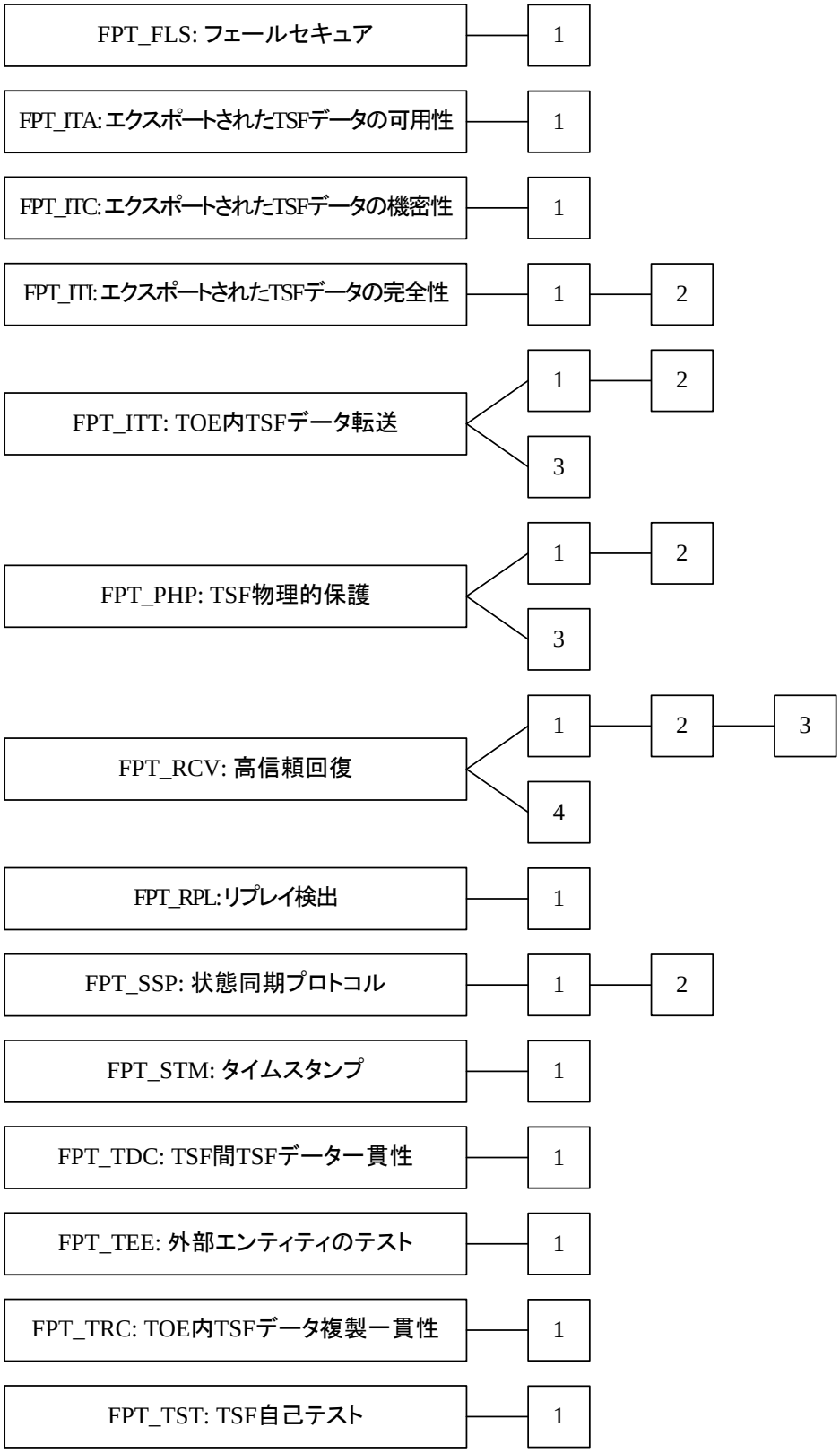


図 14　　FPT: TSF の保護クラスのコンポーネント構成

15.1 フェールセキュア(FPT_FLS)

ファミリのふるまい

365 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 SFR を常に実施することを保証する。

コンポーネントのレベル付け

366 このファミリは 1 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

367 予見される管理アクティビティはない。

監査: FPT_FLS.1

368 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: 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

依存性: 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*]。

15.2 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

369 このファミリは、TSF 及び他の高信頼 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、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

370 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 1 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、他の高信頼 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

371 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) 他の高信頼 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

372 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) 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

依存性: 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、他の高信頼 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。

15.3 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

373 このファミリは、TSF と他の高信頼 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、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

374 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 1 つだけから成り、これは、TSF と他の高信頼 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

375 予見される管理アクティビティはない。

監査: FPT_ITC.1

376 予見される監査対象事象はない。

FPT_ITC.1 送信中の TSF 間機密性

下位階層: なし

依存性: なし

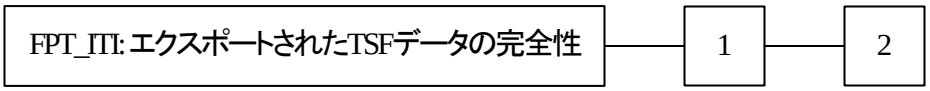
FPT_ITC.1.1 TSF は、TSF から他の高信頼 IT 製品に送信されるすべての TSF データを、送信中の不当な暴露から保護しなければならない。

15.4 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

377 このファミリは、TSF と他の高信頼 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



378 FPT_ITI.1 TSF 間改変の検出は、他の高信頼 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 と他の高信頼 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。

379 FPT_ITI.2 TSF 間改変の検出と訂正は、他の高信頼 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、他の高信頼 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

380 予見される管理アクティビティはない。

管理: FPT_ITI.2

381 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) 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 がとり得るアクションの種別の管理。

監査: FPT_ITI.1

382 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) 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とられるアクション。

監査: FPT_ITI.2

383 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) 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とられるアクション。

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

依存性: なし

FPT_ITI.1.1 **TSF は、以下の尺度の範囲で、TSF と他の高信頼 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 と他の高信頼 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: *とられるアクション*]を実行する能力を提供しなければならない。**

FPT_ITI.2 TSF 間改変の検出と訂正

下位階層: FPT_ITI.1 TSF 間改変の検出

依存性: なし

FPT_ITI.2.1 TSF は、以下の尺度の範囲で、TSF と他の高信頼 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 と他の高信頼 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: *とられるアクション*]を実行する能力を提供しなければならない。

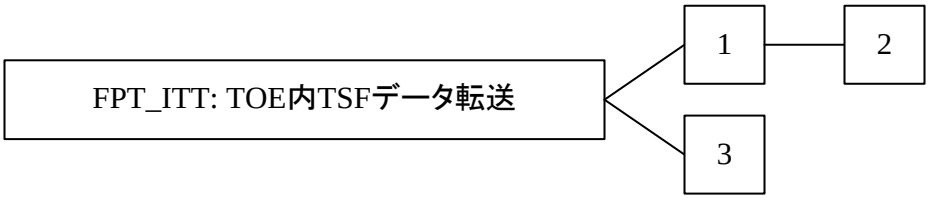
FPT_ITI.2.3 **TSF は、TSF と他の高信頼 IT 製品間で送られるすべての TSF データの[割付: *改変の種別*]を訂正する能力を提供しなければならない。**

15.5 TOE 内 TSF データ転送(FPT_ITT)

ファミリのふるまい

384 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。

コンポーネントのレベル付け



385 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。

386 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。

387 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

388 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) 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

389 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) 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

390 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) 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) TSF が検出を試みるべき TSF データの改変の種別の管理;

d) とられるアクションの管理。

監査: FPT_ITT.1、FPT_ITT.2

391 予見される監査対象事象はない。

監査: FPT_ITT.3

392 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) 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

依存性: なし

FPT_ITT.1.1 TSF は、TSF データが TOE の異なる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 TSF データ転送分離

下位階層: FPT_ITT.1 基本 TSF 内データ転送保護

依存性: なし

FPT_ITT.2.1 TSF は、TSF データが TOE の異なる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 の異なる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。

FPT_ITT.3 TSF データ完全性監視

下位階層: なし

依存性: FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.3.1 TSF は、TOE の異なる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、以下のアクションをとらねばならない。: [割付: *とられるアクションを指定*]

15.6 TSF 物理的保護(FPT_PHP)

ファミリのふるまい

393 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。

394 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。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

395 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。

396 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。

397 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

398 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) 物理的改ざんが生じたかどうかを決定する利用者または役割の管理。

管理: FPT_PHP.2

399 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) 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

400 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) 物理的改ざんに対する自動応答の管理。

監査: FPT_PHP.1

401 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) 最小: IT 手段による検出であれば、侵入の検出。

監査: FPT_PHP.2

402 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) 最小: 侵入の検出。

監査: FPT_PHP.3

403 予見される監査対象事象はない。

FPT_PHP.1 物理的攻撃の受動的検出

下位階層: なし

依存性: なし

FPT_PHP.1.1 TSF は、TSF を弱体化する恐れがある物理的な改ざん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改ざん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 物理的攻撃の通知

下位階層: FPT_PHP.1 物理的攻撃の受動的検出

依存性: FMT_MOF.1 セキュリティ機能のふるまいの管理

FPT_PHP.2.1 TSF は、TSF を弱体化する恐れがある物理的な改ざん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改ざん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改ざんが生じたとき、[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。

FPT_PHP.3 物理的攻撃への抵抗

下位階層: なし

依存性: なし

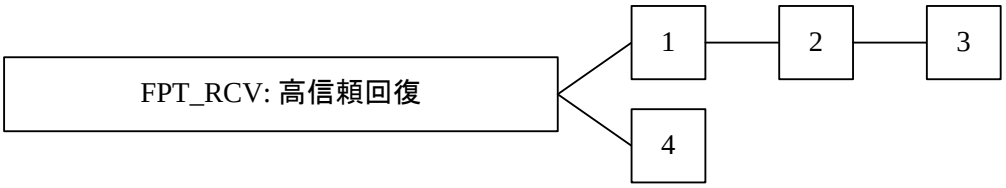
FPT_PHP.3.1 TSF は、SFR が常に実施されるよう自動的に対応することによって、[割付: *TSF 装置/エレメントのリスト*]への[割付: *物理的な改ざんのシナリオ*]に抵抗しなければならない。

15.7 高信頼回復(FPT_RCV)

ファミリのふるまい

404 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。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。

コンポーネントのレベル付け



405 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。

406 FPT_RCV.2 自動回復は、少なくともサービス中断の 1 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。

407 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。

408 FPT_RCV.4 機能回復は、特別な機能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

409 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) 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

410 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) 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

411 予見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

412 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) 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

413 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) 最小: 可能ならば、TSF 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、機能の障害の検出。

FPT_RCV.1 手動回復

下位階層: なし

依存性: AGD_OPE.1 利用者操作ガイダンス

FPT_RCV.1.1 [割付: *障害/サービス中断のリスト*]後、TSF は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 自動回復

下位階層: FPT_RCV.1 手動回復

依存性: AGD_OPE.1 利用者操作ガイダンス

FPT_RCV.2.1 [割付: *障害/サービス中断のリスト*]からの自動回復が不可能な場合、TSF は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。

FPT_RCV.3 過度の損失のない自動回復

下位階層: FPT_RCV.2 自動回復

依存性: AGD_OPE.1 利用者操作ガイダンス

FPT_RCV.3.1 [割付: *障害/サービス中断のリスト*]からの自動回復が不可能な場合、TSF は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、TSF の制御下にある 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。

FPT_RCV.4　　機能回復

下位階層:　なし

依存性:　なし

FPT_RCV.4.1　**TSF** は、**[**割付**:** *機能及び障害シナリオのリスト***]**が、機能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、一貫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。

15.8 リプレイ検出(FPT_RPL)

ファミリのふるまい

414 このファミリは、様々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

415 このファミリは1つだけのコンポーネント、FPT_RPL.1リプレイ検出からなり、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

416 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

417 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: 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

依存性: 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。

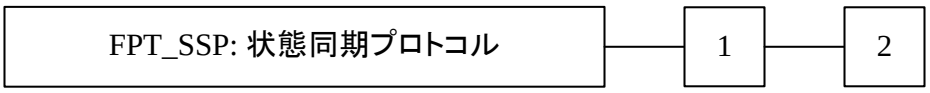
15.9 状態同期プロトコル(FPT_SSP)

ファミリのふるまい

418 分散 TOE は、TOE 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 TOE 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る場合、より複雑な防御プロトコルが要求される。

419 状態同期プロトコル(FPT_SSP)は、この信頼できるプロトコルを使用する TSF のある重要な機能についての要件を制定する。状態同期プロトコル(FPT_SSP)は、TOE の 2 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。

コンポーネントのレベル付け



420 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。

421 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

422 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

423 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) 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

依存性: FPT_ITT.1 基本 TSF 内データ転送保護

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。

FPT_SSP.2 相互信頼肯定応答

下位階層: FPT_SSP.1 単純信頼肯定応答

依存性: FPT_ITT.1 基本 TSF 内データ転送保護

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。

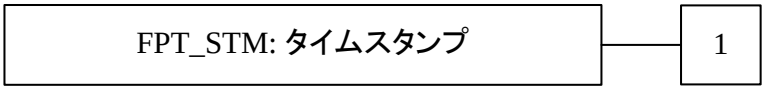
FPT_SSP.2.2 **TSF** は、**TSF** の関連するパーツが、肯定応答を使って、異なるパーツ間で送信されたデータの正確な状態を知ることを保証しなければならない。

15.10 タイムスタンプ(FPT_STM)

ファミリのふるまい

424 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。

コンポーネントのレベル付け



425 このファミリは 1 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なり、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

426 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) 時間の管理。

監査: FPT_STM.1

427 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) 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

依存性: なし

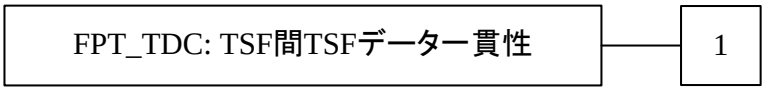
FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

15.11 TSF 間 TSF データー貫性(FPT_TDC)

ファミリのふるまい

428 分散環境において、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



429 FPT_TDC.1 TSF 間基本 TSF データー貫性は、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

430 予見される管理アクティビティはない。

監査: FPT_TDC.1

431 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) 最小: TSF データー貫性メカニズムの成功した使用。

b) 基本: TSF データー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

依存性: 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。

15.12 外部エンティティのテスト(FPT_TEE)

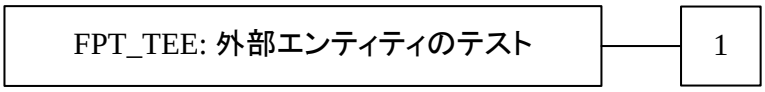
ファミリのふるまい

432 このファミリは TSF がひとつあるいはいくつかの外部エンティティにおいてテストを実行するための要件を定義する。

433 このコンポーネントは人間の利用者に対して適用するものではない。

434 外部エンティティは、TOE 上で稼動するアプリケーション、TOE“の下”で稼動するハードウェアもしくはソフトウェア(プラットフォーム、オペレーティングシステムなど)、TOE に接続されたアプリケーション/ボックス(侵入検知システム、ファイアウォール、ログインサーバ、タイムサーバなど)を含むことができる。

コンポーネントのレベル付け



435 FPT_TEE.1 外部エンティティのテスト、TSF による外部エンティティのテストを提供する。

管理:FPT_TEE.1

436 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) 初期立ち上げ、一定間隔、または特定された条件など、
外部エンティティの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_TEE.1

437 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:外部エンティティのテストの実行とテスト結果

FPT_TEE.1 外部エンティティのテスト

下位階層: なし

依存性: なし

FPT_TEE.1.1 **TSF は、[割付:*外部エンティティの特性のリスト*]の達成をチェックするために、[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、[割付:その他の条件]*]時に、テストスイートを実行しなければならない。**

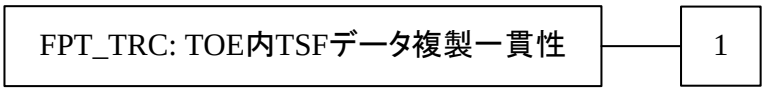
FPT_TEE.1.2 **テストに失敗した場合、TSF は[割付:*アクション*]をとらなければならない。**

15.13 TOE 内 TSF データ複製一貫性(FPT_TRC)

ファミリのふるまい

438 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



439 このファミリはただ 1 つのコンポーネント、FPT_TRC.1 TSF 内一貫性からなり、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

440 予見される管理アクティビティはない。

監査: FPT_TRC.1

441 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) 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

依存性: FPT_ITT.1 基本 TSF 内データ転送保護

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機能のリスト*]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。

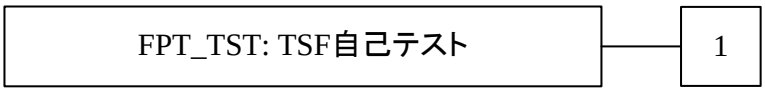
15.14 TSF 自己テスト(FPT_TST)

ファミリのふるまい

442 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。例としては、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 によってとられるアクションは、他のファミリで定義される。

443 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様々な障害による、TSF データ及び TSF 自体 (すなわち TSF 実行コードまたは TSF ハードウェアコンポーネント)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。

コンポーネントのレベル付け



444 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 TSF 自体の完全性を検証する能力を提供する。

管理: FPT_TST.1

445 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) 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

446 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: 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

依存性: なし

FPT_TST.1.1 **TSF** は、**[選択:** ***TSF*****、*****[割付: TSF の一部]*****]**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、**[選択:** ***[割付: TSF データの一部]*****、*****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、**[選択:** ***[割付: TSF の一部]*****、*****TSF*****]**の完全性を検証する能力を提供しなければならない。

16 クラス FRU: 資源利用

447 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 3 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。

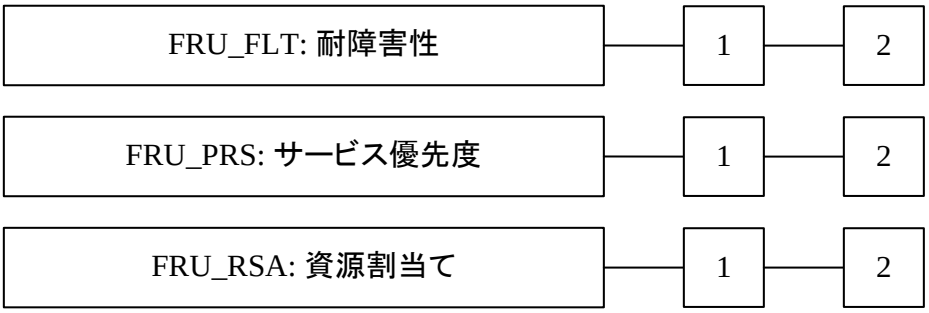


図 15 FRU: 資源利用クラスのコンポーネント構成

16.1 耐障害性(FRU_FLT)

ファミリのふるまい

448 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

449 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。

450 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

451 予見される管理アクティビティはない。

監査: FRU_FLT.1

452 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) 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

453 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) 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

依存性: FPT_FLS.1 セキュアな状態を保持する障害

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。

FRU_FLT.2 制限付き耐障害性

下位階層: FRU_FLT.1 機能削減された耐障害性

依存性: FPT_FLS.1 セキュアな状態を保持する障害

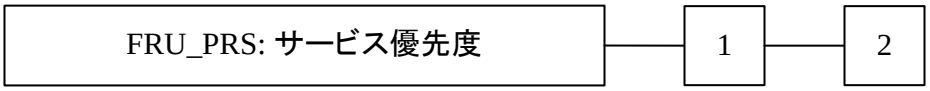
FRU_FLT.2.1 TSF は、以下の障害[割付: *障害の種別のリスト*]が生じたとき、**すべての TOE 機能** (capabilities)の動作を保証しなければならない。

16.2 サービス優先度(FRU_PRS)

ファミリのふるまい

454 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、TSF の制御下にある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 TSF の制御下にある資源利用を 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



455 FRU_PRS.1 制限付きサービス優先度は、サブジェクトによる TSF の制御下にある資源のサブセットの利用に対して優先度を提供する。

456 FRU_PRS.2 完全サービス優先度は、サブジェクトによる TSF の制御下にあるすべての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

457 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) 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

458 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) 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

依存性: 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。

FRU_PRS.2　　完全サービス優先度

下位階層:　FRU_PRS.1 制限付きサービス優先度

依存性:　**なし**

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。

16.3 資源割当て(FRU_RSA)

ファミリのふるまい

459 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

460 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。

461 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

462 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) 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

463 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) 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

464 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) 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

依存性: 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。

FRU_RSA.2 最小及び最大割当て

下位階層: FRU_RSA.1 最大割当て

依存性: なし

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。**

17 クラス FTA: TOE アクセス

465 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。

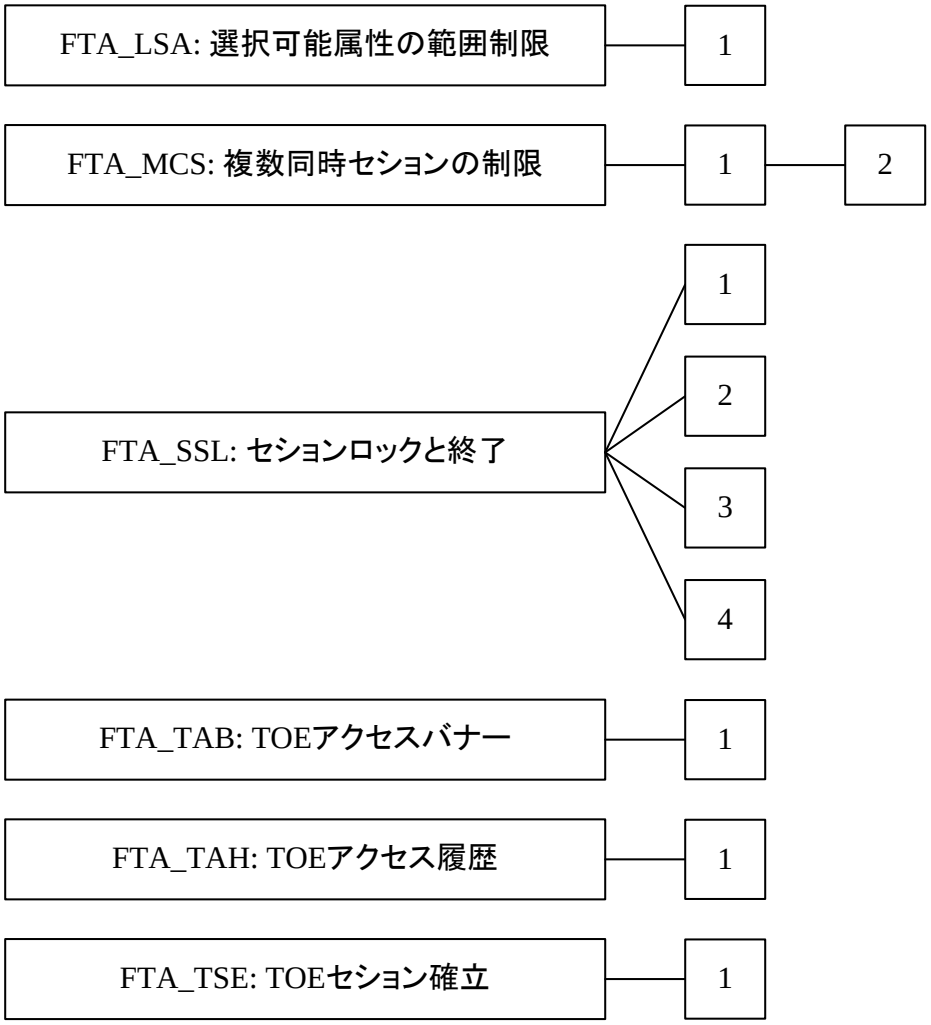


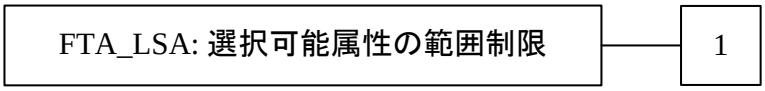
図 16 FTA: TOE アクセスクラスのコンポーネント構成

17.1 選択可能属性の範囲制限(FTA_LSA)

ファミリのふるまい

466 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



467 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

468 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) 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

469 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) 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

依存性: なし

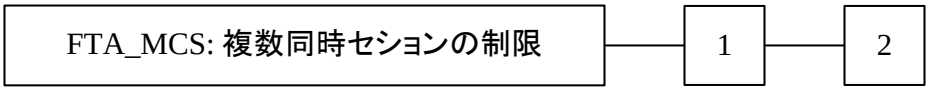
FTA_LSA.1.1 TSF は、[割付: *属性*]に基づき、セションセキュリティ属性[割付: *セションセキュリティ属性*]の範囲を制限しなければならない。

17.2 複数同時セションの制限(FTA_MCS)

ファミリのふるまい

470 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



471 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。

472 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 複数同時セションの基本制限を拡張する。

管理: FTA_MCS.1

473 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) 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

474 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) 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

475 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) 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

依存性: FIA_UID.1 識別のタイミング

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。

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 複数同時セションの基本制限

依存性: FIA_UID.1 識別のタイミング

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。

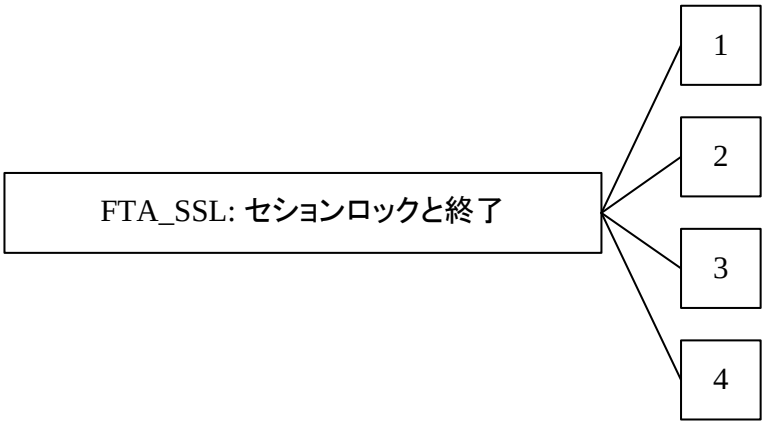
FTA_MCS.2.2 TSF は、デフォルトで、利用者あたり[割付: *デフォルト数*]セションの制限を実施しなければならない。

17.3 セションロックと終了(FTA_SSL)

ファミリのふるまい

476 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、ロック解除、及び終了のための能力を 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



477 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。

478 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。

479 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。

480 FTA_SSL.4 利用者起動による終了は、利用者に対し、利用者自身の対話セションを終了する能力を提供する。

管理: FTA_SSL.1

481 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) 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

482 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) 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

483 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) 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。

管理: FTA_SSL.4

484 予見される管理アクティビティなし

監査: FTA_SSL.1、FTA_SSL.2

485 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) 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

486 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) 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。

監査: FTA_SSL.4

487 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) 最小:利用者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

依存性: FIA_UAU.1 認証のタイミング

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、**[**割付**:** *発生する事象***]**の事象を生じさせることを要求しなければならない。

FTA_SSL.2 利用者起動ロック

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

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、**[**割付**:** *発生する事象***]**の事象を生じさせることを要求しなければならない。

FTA_SSL.3 TSF 起動による終了

下位階層: なし

依存性: 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。

FTA_SSL.4 利用者起動による終了

下位階層: なし

依存性: なし

FTA_SSL.4.1 **TSF** は、利用者自身の対話セションの、利用者起動による終了を許可しなければならない。

17.4 TOE アクセスバナー(FTA_TAB)

ファミリのふるまい

488 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

489 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

490 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) 許可管理者によるバナーの維持。

監査: FTA_TAB.1

491 予見される監査対象事象はない。

FTA_TAB.1 デフォルト TOE アクセスバナー

下位階層: なし

依存性: 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。

17.5 TOE アクセス履歴(FTA_TAH)

ファミリのふるまい

492 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

493 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

494 予見される管理アクティビティはない。

監査: FTA_TAH.1

495 予見される監査対象事象はない。

FTA_TAH.1 TOE アクセス履歴

下位階層: なし

依存性: 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。

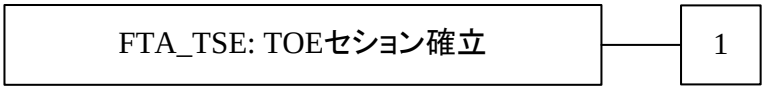
FTA_TAH.1.3 **TSF** は、利用者に情報をレビューする機会を与えることなく利用者インタフェースからアクセス履歴情報を消去してはならない。

17.6 TOE セション確立(FTA_TSE)

ファミリのふるまい

496 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



497 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

498 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) 許可管理者によるセション確立条件の管理。

監査: FTA_TSE.1

499 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) 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

依存性: 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。

18 クラス FTP: 高信頼パス/チャネル

500 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。

501 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。

502 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。

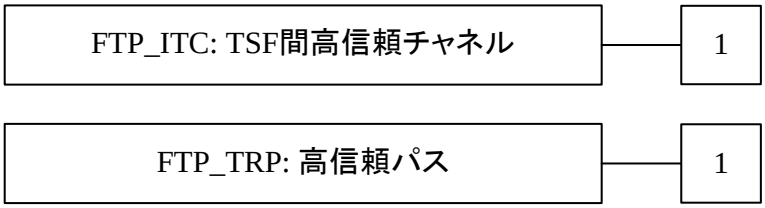


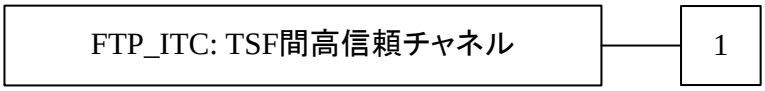
図 17 FTP: 高信頼パス/チャネルクラスのコンポーネント構成

18.1 TSF 間高信頼チャネル(FTP_ITC)

ファミリのふるまい

503 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



504 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

505 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構成。

監査: FTP_ITC.1

506 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) 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

依存性: なし

FTP_ITC.1.1 TSF は、それ自身と他の高信頼 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*、*他の高信頼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。

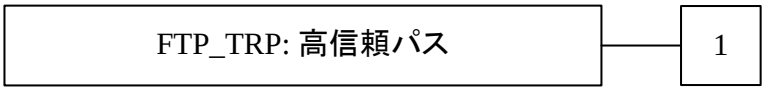
FTP_ITC.1.3 TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

18.2 高信頼パス(FTP_TRP)

ファミリのふるまい

507 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



508 FTP_TRP.1 高信頼パスは、PP/ST 作成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

509 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構成。

監査: FTP_TRP.1

510 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) 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: 高信頼パス機能のすべての使用の試み。

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

依存性: 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と、[選択: *改変*、*暴露*、*[割付: ほかのタイプの完全性、または機密性侵害]*]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。**

附属書A　セキュリティ機能要件適用上の注釈（規定）

511　この附属書は、CC 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追加ガイダンスを載せたもので、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。

A.1　注釈の構造

512　この章は、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　クラスの構造

513　次の図 18 は、この附属書における機能クラス構造を表している。

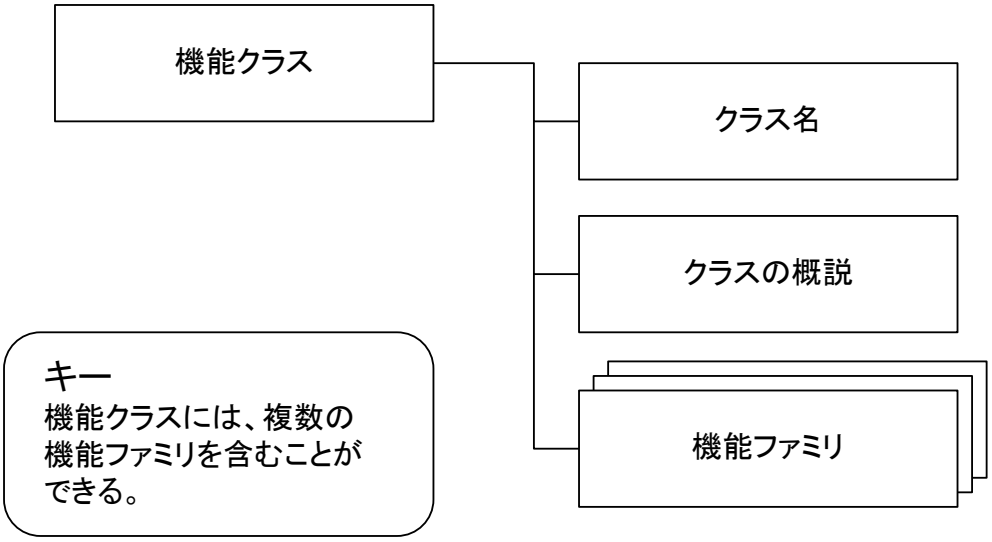


図 18　機能クラス構造

A.1.1.1　クラス名

514　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　クラスの概説

515　この附属書におけるクラスの概説は、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、各クラスの構成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

516 図 19 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。

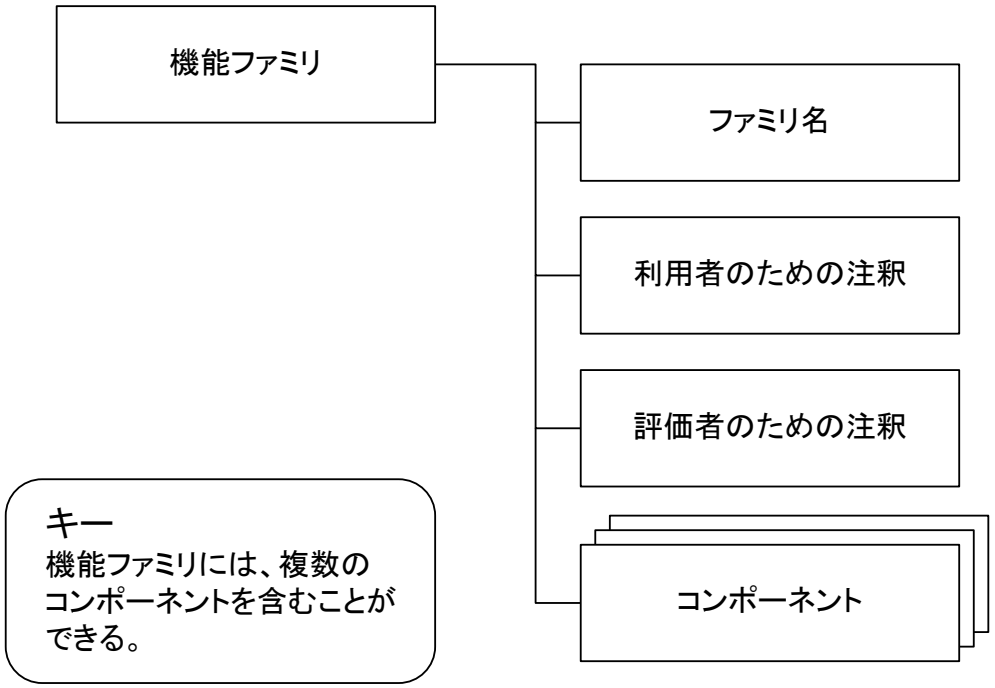


図 19 適用上の注釈のための機能ファミリ構造

A.1.2.1 ファミリ名

517 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

518 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

519 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様々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。

520 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

521 図 20 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。

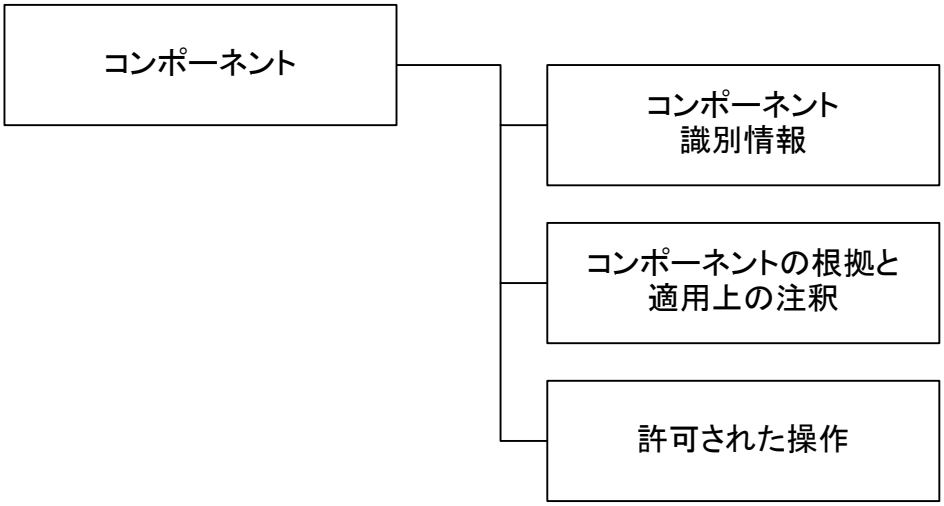


図 20 機能コンポーネント構造

A.1.3.1 コンポーネント識別情報

522 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

523 コンポーネントに関係する、あらゆる特定の情報がこの節に記載される。

- *根拠*は、根拠における一般的なステートメント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)。

524 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.1.3.3 許可された操作

525 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。

526 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 依存性の表

527 次の機能コンポーネントに対する依存性の表は、それぞれの直接的、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 セキュリティ属性なし利用者データのエクスポートで、これは、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のどちらかを要求する。それで、FDP_ACC.1 サブセットアクセス制御が存在すれば、FDP_IFC.1 サブセット情報フロー制御は必要ではなく、その逆もある。文字が表示されていない場合、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。

	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_MTD.1	FMT_SME.1	FMT_SMR.1	FPT_STM.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 1 FAU: セキュリティ監査クラスの依存性

	FIA_UID.1
FCO_NRO.1	X
FCO_NRO.2	X
FCO_NRR.1	X
FCO_NRR.2	X

表 2 FCO: 通信クラスの依存性

	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_ITC.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_CKM.1	-	O	X	O	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.2	O	-	X	-	-	-	-	-	O	O	-	-	-	-	-	-	-	-
FCS_CKM.3	O	-	X	-	-	-	-	-	O	O	-	-	-	-	-	-	-	-
FCS_CKM.4	O	-	-	-	-	-	-	-	O	O	-	-	-	-	-	-	-	-
FCS_COP.1	O	-	X	-	-	-	-	-	O	O	-	-	-	-	-	-	-	-

表 3　　FCS: 暗号サポートクラスの依存性

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
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	-				-	-	-	-	-			
FDP_IFF.4	-	-	X	-				-	-	-	-	-			
FDP_IFF.5	-	-	X	-				-	-	-	-	-			
FDP_IFF.6	-	-	X	-				-	-	-	-	-			
FDP_ITC.1	O	-	O	-				-	-	X	-	-			
FDP_ITC.2	O	-	O	-				-	-	-	-	-	X	O	O
FDP_ITT.1	O	-	O	-				-	-	-	-	-			
FDP_ITT.2	O	-	O	-				-	-	-	-	-			
FDP_ITT.3	O	-	O	-	X			-	-	-	-	-			
FDP_ITT.4	O	-	O	-		X		-	-	-	-	-			
FDP_RIP.1															
FDP_RIP.2															
FDP_ROL.1	O	-	O	-				-	-	-	-	-			
FDP_ROL.2	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	-			O	-	-	-	-	-		O	-
FDP_UIT.3	O	-	O	-			O	-	-	-	-	-		O	-

表 4　　FDP: 利用者データ保護クラスの依存性

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
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 5　　FIA: 識別と認証クラスの依存性

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_MOF.1					-				X	X	
FMT_MSA.1	O	-	O	-	-	-	-		X	X	
FMT_MSA.2	O	-	O	-	-	X	-		-	X	
FMT_MSA.3	-	-	-	-	-	X	-		-	X	
FMT_MSA.4	O	-	O	-	-	-	-		-	-	
FMT_MTD.1					-				X	X	
FMT_MTD.2					-			X	-	X	
FMT_MTD.3					-			X	-	-	
FMT_REV.1					-					X	
FMT_SAE.1					-					X	X
FMT_SMF.1											
FMT_SMR.1					X						
FMT_SMR.2					X						
FMT_SMR.3					-					X	

表 6　　FMT: セキュリティ管理クラスの依存性

	FIA_UID.1	FPR_UNO.1
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		X
FPR_UNO.4		

表 7　　FPR: プライバシークラスの依存性

	AGD_OPE.1	FIA_UID.1	FMT_MOF.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1
FPT_FLS.1						
FPT_ITA.1						
FPT_ITC.1						
FPT_ITI.1						
FPT_ITI.2						
FPT_ITT.1						
FPT_ITT.2						
FPT_ITT.3						X
FPT_PHP.1						
FPT_PHP.2		-	X	-	-	
FPT_PHP.3						
FPT_RCV.1	X					
FPT_RCV.2	X					
FPT_RCV.3	X					
FPT_RCV.4						
FPT_RPL.1						
FPT_SSP.1						X
FPT_SSP.2						X
FPT_STM.1						
FPT_TDC.1						
FPT_TEE.1						
FPT_TRC.1						X
FPT_TST.1						

表 8　　FPT: TSF 保護クラスの依存性

	FPT_FLS.1
FRU_FLT.1	X
FRU_FLT.2	X
FRU_PRS.1	
FRU_PRS.2	
FRU_RSA.1	
FRU_RSA.2	

表 9　FRU: 資源利用クラスの依存性

	FIA_UAU.1	FIA_UID.1
FTA_LSA.1		
FTA_MCS.1		X
FTA_MCS.2		X
FTA_SSL.1	X	-
FTA_SSL.2	X	-
FTA_SSL.3		
FTA_SSL.4		
FTA_TAB.1		
FTA_TAH.1		
FTA_TSE.1		

表 10　FTA: TOE アクセスクラスの依存性

附属書B　機能クラス、ファミリ、及びコンポーネント（規定）

528　以下の附属書 C から M は、CC 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　クラス FAU: セキュリティ監査（規定）

529 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 SFR 実施の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。

530 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)。

C.1 分散環境での監査要件

531 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、時間順のリストあるいは「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。

532 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。

533 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、1 つの多目的監査リポジトリ(その部分が、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。

534 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べきである。

535 図 21 は、このクラスのコンポーネント構成を示す。

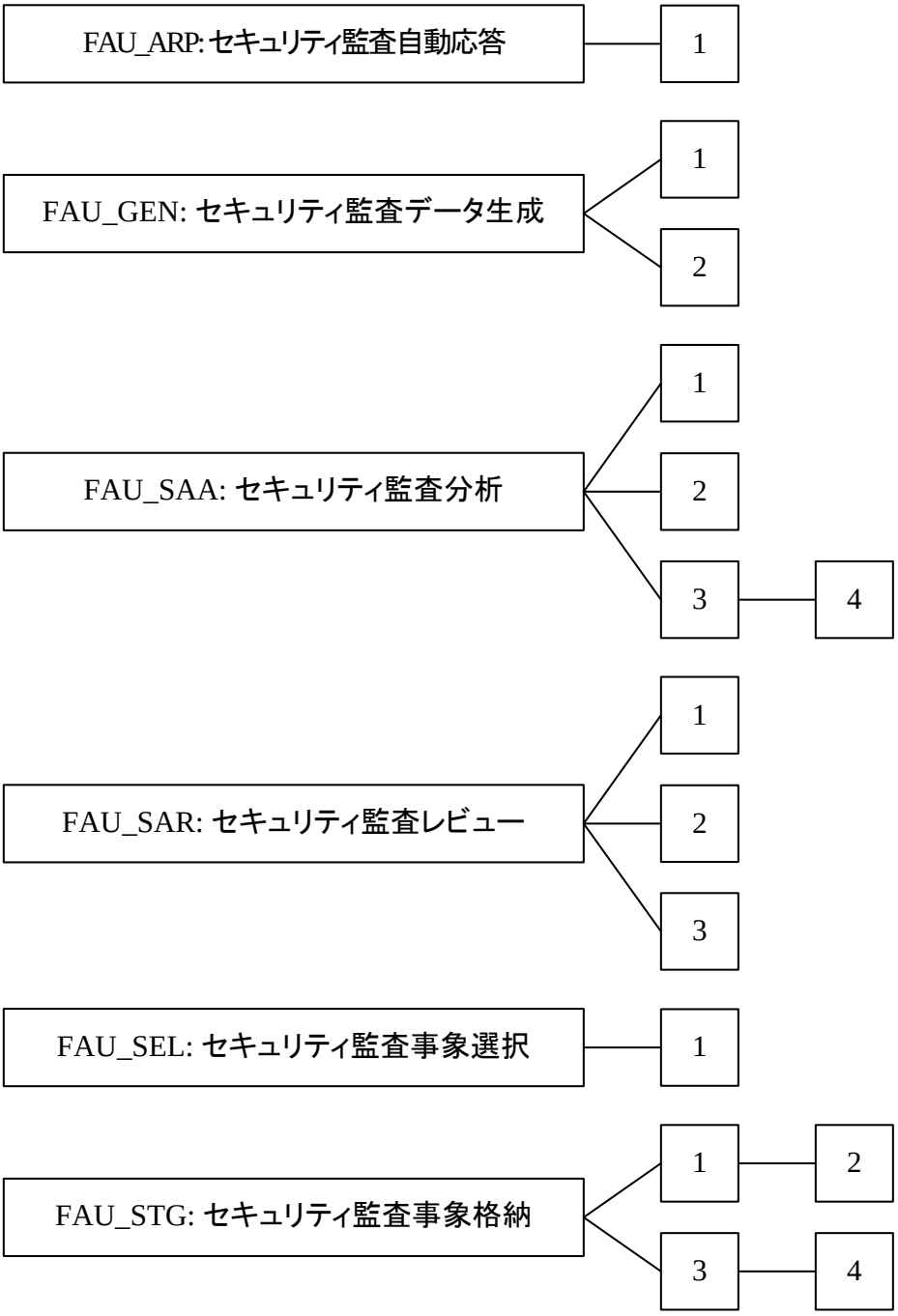


図 21　　FAU: セキュリティ監査クラスのコンポーネント構成

C.2 セキュリティ監査自動応答(FAU_ARP)

利用者のための注釈

536 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。

537 ある監査事象は、もしセキュリティ監査分析(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

538 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:

539 **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。このようなリストの例には、「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」などがある。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.3 セキュリティ監査データ生成(FAU_GEN)

利用者のための注釈

540 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。

541 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が列挙される。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。

542 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 1 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:

543 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) 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。

544 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、セキュリティ監査データ生成(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」がセキュリティ監査データ生成(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。

545 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 に含まれるべきである。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。「詳細監査生成」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 に含まれるべきである。

546 PP/ST 作成者は、所定の監査レベルで要求されている以上の他の監査対象事象を含めることができる。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。

547 監査対象事象を生成する機能性は、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。

548 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) TSF 制御範囲内で、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または取消し;

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ためのアクセス権の使用;

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

549 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。

550 SFR 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 監査データ生成が、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 利用者識別情報の関連付けを追加して使用することができる。

551 サブジェクトが利用者である場合、利用者識別情報はサブジェクト識別情報として記録できる。利用者認証(FIA_UAU)が適用されていない場合、利用者の識別情報はまだ検証することができない。したがって、無効なログインの場合で、主張された利用者識別情報を記録すべきである。記録された識別情報が認証されていない場合でも、示されたと考慮すべきである。

評価者のための注釈

552 タイムスタンプ(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:

553 F**AU_GEN.1.1** において、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」のうちの 1 つである。

割付:

554 F**AU_GEN.1.1** において、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。その割付には、「なし」、あるいは次の事象－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、b)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－などを含むことができる。

555 F**AU_GEN.1.2** において、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、または「なし」のどちらかの割付をすべきである。

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

556 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。

557 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。

558 利用者の識別情報が認証を通じてまだ検証されていない場合、無効なログインの場合で主張された利用者識別情報は、利用者識別情報として記録するべきである。記録された識別情報が認証されていない場合でも、示されたと考慮すべきである。

C.4 セキュリティ監査分析(FAU_SAA)

利用者のための注釈

559 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、潜在的な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。

560 侵害の可能性を検出して TSF が実行するアクションは、セキュリティ監査自動応答(FAU_ARP)コンポーネントで定義される。

561 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、レビューのために許可利用者への配布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

562 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 SFR 実施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:

563 **FAU_SAA.1.2** において、PP/ST 作成者は、その発生または度重なる発生が SFR 実施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。

564 **FAU_SAA.1.2** 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。監査証跡の分析において用いられるべき TSF に関する追加規則が存在しない場合、本割付は、「なし」で完了することができる。

FAU_SAA.2 プロファイルに基づく異常検出

利用者のための適用上の注釈

565 *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/サブジェクトが様々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様々な種別のアクティビティに関して設定される。プロファイルに様々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。

566 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 1 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 1 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 1 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 1 つのプロファイル。

567 1 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。

568 異常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。

569 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。

570 FAU_SAA.2 プロファイルに基づく異常検出は、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、異常検出機構が、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、異常検出機構は、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 ヶ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。

571 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。

572 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セキュリティ監査自動応答(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:

573 **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。1 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。

574 **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

575 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、特徴的事象と呼ばれる。

576 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。

577 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。

578 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。

579 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、あるいは様々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。

580 FAU_SAA.3 単純攻撃の発見のエレメントは、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:

581 **FAU_SAA.3.1** において、PP/ST 作成者は、その発生が SFR 実施の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、SFR 実施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。

582 **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、ど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

583 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、非常に稀である。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。

584 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。

585 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。

586 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。

587 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、あるいは様々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。

588 FAU_SAA.4 複合攻撃の発見のエレメントは、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:

589 **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。

590 **FAU_SAA.4.1** において、PP/ST 作成者は、その発生が SFR 実施の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、SFR 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。

591 **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、ど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.5 セキュリティ監査レビュー(FAU_SAR)

利用者のための注釈

592 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。

593 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 SFR 属性に関連付けられるアクション。

594 各監査レビューの区別は、それが持つ機能性に基づく。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、そのレビュー前に、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監査データのサブセットの選択、監査データの順序付けを行う能力を要求する。

FAU_SAR.1 監査レビュー

根拠

595 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。

利用者のための適用上の注釈

596 このコンポーネントは、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。様々な種別の利用者(人間の利用者、機械の利用者)が存在しており、そのニーズは様々に異なっている可能性がある。

597 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:

598 **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)を必要に応じて含むことができる。

599 **FAU_SAR.1.1** において、PP/ST 作成者は、特定の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。SFR、FAU_SAR.1 を採用する場合、FAU_GEN.1 で初めに特定される監査情報のリストを詳細に繰り返す必要はない。「すべて」または「すべての監査情報」のような用語の使用は、曖昧さをなくし、2 つのセキュリティ要件間で比較分析を不要にするために役立つ。

FAU_SAR.2 限定監査レビュー

利用者のための適用上の注釈

600 このコンポーネントは、FAU_SAR.1 監査レビュー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明示する。

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

601 このコンポーネントは、レビューされる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明示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

割付:

602 **FAU_SAR.3.1** において、PP/ST 作成者は、TSF から監査データの選択、そして/または、順序付けする能力が必要かどうかを指定すべきである。

603 **FAU_SAR.3.1** において、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、場合によっては論理的な関係と共に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/または場所」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場所の 3 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.6 セキュリティ監査事象選択(FAU_SEL)

利用者のための注釈

604 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、セキュリティ監査データ生成(FAU_GEN)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。

605 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

606 このコンポーネントは、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、使用される選択基準と、結果として生じる全監査対象事象の監査サブセットを定義する。

607 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。

608 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。

609 管理機能 FMT_MTD.1 TSF データの管理は、選択を問い合わせあるいは修正する、許可利用者の権利を扱う。

操作

選択:

610 **FAU_SEL.1.1** において、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:

611 **FAU_SEL.1.1** において、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。監査の選択を基本とする追加規則が存在しない場合、本割付は、「なし」で完了することができる。

C.7 セキュリティ監査事象格納(FAU_STG)

利用者のための注釈

612 セキュリティ監査事象格納ファミリは、TOE 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、後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

613 分散環境において、監査証跡は TSF 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。

614 TSF は、許可されない削除や改変から監査証跡に格納された監査記録を保護する。TOE 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:

615 **FAU_STG.1.2** において、PP/ST 作成者は、監査証跡に格納された監査レコードに対する改変を、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。これらの選択肢の 1 つのみを選択することができる。

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

616 PP/ST 作成者は、監査証跡をどの尺度に準拠させるべきなのかを、このコンポーネントで特定することができる。

617 分散環境において、監査証跡は TSF 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:

618 **FAU_STG.2.2** において、PP/ST 作成者は、監査証跡に格納された監査レコードに対する改変を、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。これらの選択肢の 1 つのみを選択することができる。

割付:

619 **FAU_STG.2.3** において、PP/ST 作成者は、格納された監査レコードに関して 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。

選択:

620 **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。この条件は次のいずれかである: 監査格納の領域枯渇、失敗、攻撃。

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

621 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:

622 **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。

623 **FAU_STG.3.1** において、PP/ST 作成者は、閾値を超えたことで切迫した監査格納失敗が示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。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

624 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 TOE をリセットすることすらできなくなるからである。監査格納の領域枯渇の場合では、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:

625 **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。これらの選択肢の 1 つのみを選択することができる。

割付:

626 **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、監査格納失敗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。監査格納失敗の場合においてとられるアクションが存在しない場合、この割付は「なし」で完了できる。

附属書D　クラス FCO: 通信（規定）

627 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。

628 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。

629 「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根拠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。

630 図 22 は、このクラスのコンポーネント構成を示す。

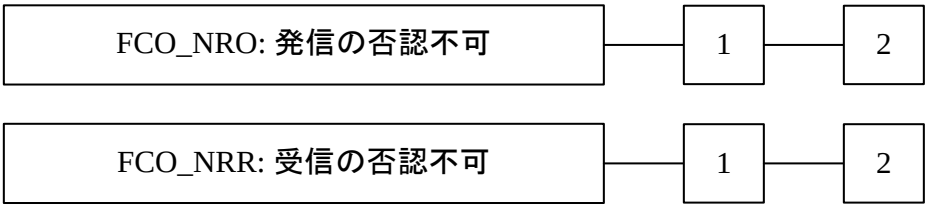


図 22　FCO: 通信クラスのコンポーネント構成

D.1　発信の否認不可(FCO_NRO)

利用者のための注釈

631 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対応付ける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。

632 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。

633 否認不可にはいくつかの役割が関連しており、それぞれの役割は 1 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。

634 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。したがって、これらの条件は、証拠の提供を数年間可能にするなど、法的な要件への否認不可の適応を可能にする。

635 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。

636 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:

637 F**CO_NRO.1.1** において、PP/ST 作成者は、発信機能の証拠に、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:

638 F**CO_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:

639 F**CO_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。

640 F**CO_NRO.1.2** において、PP/ST 作成者は、情報にリンクしなければならない属性、例えば、発信者識別情報、発信時刻、発信場所などのリストを記入すべきである。

641 F**CO_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:

642 F**CO_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:

643 F**CO_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。

644 F**CO_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.2 発信の強制的証明

操作

割付:

645 F**CO_NRO.2.1** において、PP/ST 作成者は、発信機能の証拠に、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。

646 F**CO_NRO.2.2** において、PP/ST 作成者は、情報にリンクしなければならない属性、例えば、発信者識別情報、発信時刻、発信場所などのリストを記入すべきである。

647 F**CO_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:

648 F**CO_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:

649 F**CO_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。

650 F**CO_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。第三者とは、調停者、裁判官、法的機関などがなり得る。

D.2 受信の否認不可(FCO_NRR)

利用者のための注釈

651 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。

652 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。

653 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。

654 否認不可ではいくつかの異なる役割が関連しており、各々は1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(公証人など)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。

655 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ならない、というものである。したがって、これらの条件は、証拠の提供を数年間可能にするなど、法的な要件への否認不可の適応を可能にする。

656 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。

657 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 受信の選択的証明割付

操作

割付:

658 F**CO_NRR.1.1** において、PP/ST 作成者は、受信機能の証拠に、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:

659 F**CO_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:

660 F**CO_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。

661 F**CO_NRR.1.2** において、PP/ST 作成者は、情報にリンクしなければならない属性、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。

662 F**CO_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:

663 F**CO_NRR.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:

664 F**CO_NRR.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。

665 F**CO_NRR.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_NRR.2 受信の強制的証明

操作

割付:

666 F**CO_NRR.2.1** において、PP/ST 作成者は、受信機能の証拠に、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。

667 F**CO_NRR.2.2** において、PP/ST 作成者は、情報にリンクしなければならない属性、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。

668 F**CO_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:

669 F**CO_NRR.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:

670 F**CO_NRR.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。

671 F**CO_NRR.2.3** 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。第三者とは、調停者、裁判官、法的機関などがなり得る。

附属書E　クラス FCS: 暗号サポート
（規定）

672 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、暗号機能性を採用することができる。これらは次のものである(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。

673 FCS: 暗号サポートクラスは、暗号鍵管理(FCS_CKM)と、暗号操作(FCS_COP)の 2 個のファミリから構成される。暗号鍵管理(FCS_CKM)ファミリは暗号鍵の管理面に対応し、暗号操作(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。

674 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 暗号鍵生成のコンポーネントを選択すべきである。

675 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 暗号鍵配付のコンポーネントを選択すべきである。

676 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 暗号鍵アクセスのコンポーネントを選択すべきである。

677 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 暗号鍵破棄のコンポーネントを選択すべきである。

678 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 暗号操作のコンポーネントを選択すべきである。

679 暗号機能性は、FCO クラス: 通信において特定された対策方針を満たすために、かつデータ認証(FDP_DAU)、蓄積データ完全性(FDP_SDI)、TSF 間利用者データ機密転送保護(FDP_UCT)、TSF 間利用者データ完全性転送保護(FDP_UIT)、秘密についての仕様(FIA_SOS)、利用者認証(FIA_UAU)ファミリにおける様々な対策方針を満たすために使用できる。暗号機能性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、暗号機能性が満たさねばならない対策方針を特定する。FCS: 暗号サポートクラスにおける対策方針は、TOE の暗号機能性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。

680 図 23 は、このクラスのコンポーネント構成を示す。

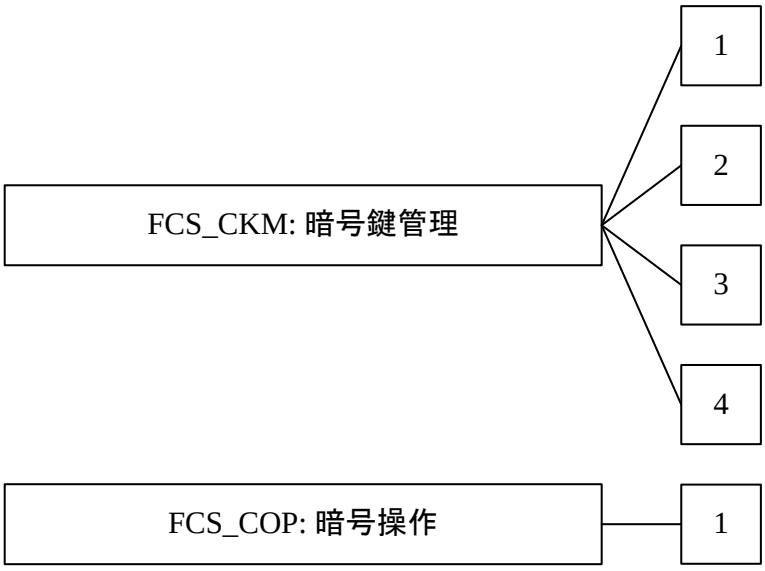


図 23　　FCS: 暗号サポートクラスのコンポーネント構成

E.1　暗号鍵管理(FCS_CKM)

利用者のための注釈

681　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。

682　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、実装される鍵の管理方針に依存する(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)。

683　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、その結果として暗号鍵生成、暗号鍵配付、暗号鍵アクセス、及び暗号鍵破棄のアクティビティに対する要件を定義する。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。

684　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、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。

685　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

686 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することでよい。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 1 つの具体例だけが必要である。鍵長は、様々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:

687 F**CS_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。

688 F**CS_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。

689 F**CS_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、1 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

690 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:

691 F**CS_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。

692 F**CS_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、1 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

693 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:

694 **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)。

695 **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。

696 F**CS_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、1 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

697 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:

698 **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。

699 **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、1 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

700 暗号操作は、それに関連付けられた操作の暗号モード(1 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(1 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。

701 暗号操作は、1 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。暗号操作(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

702 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、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(1 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

703 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(1 つまたは複数)を実行することを要求する。

操作

割付:

704 **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。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。

705 **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。

706 **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。

707 **FCS_COP.1.1** において、PP/ST 作成者は、識別された暗号操作(1 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、1 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　クラス FDP: 利用者データ保護（規定）

708 このクラスには、利用者データの保護に関連する要件を特定するファミリが含まれる。FDP: 利用者データ保護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特定し、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。

709 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。

710 FDP: 利用者データ保護では、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 3 つの目的を適切にカバーしていなければならない。

711 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。

712 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。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。

713 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。

714 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: 利用者データ保護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。

715 最後に、FDP: 利用者データ保護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 単純セキュリティ属性)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。

716 SFR のセットは、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 2 つの方針指向のコンポーネントのアクセス制御方針(FDP_ACC)及び情報フロー制御方針(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 1 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。

717 FDP: 利用者データ保護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。

718 FDP: 利用者データ保護クラスの要件は、SFP を実現する SFR のセット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、SFP 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。

719 コンポーネントを具現化したものは、1 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。

720 このファミリからコンポーネントを選択する鍵は、アクセス制御方針(FDP_ACC)及び情報フロー制御方針(FDP_IFC)という 2 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、明確に定義された TOE セキュリティ対策方針のセットを持つことである。アクセス制御方針(FDP_ACC)と情報フロー制御方針(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性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」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。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 の機能性を定義する規則は、アクセス制御機能(FDP_ACF)ファミリ及び情報フロー管理機能(FDP_IFF)ファミリで(それぞれ)定義される。

721 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) アクセス制御方針(FDP_ACC)と情報フロー制御方針(FDP_IFC)のファミリから実施する方針を識別する。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」のようなステートメントで)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) アクセス制御方針(FDP_ACC)と情報フロー制御方針(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ため、アクセス制御機能(FDP_ACF)ファミリ及び情報フロー制御機能(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ために選択された機能の要件に合致させるべきである。

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、その機能のもとでセキュリティ属性を管理したり、変更したりできるのは誰であるかを特定する。FMT: セキュリティ管理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: セキュリティ管理から適切なコンポーネントを識別する。

f) ロールバック(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) 残存情報保護(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) TOE 外からのインポート(FDP_ITC)及び TOE からのエクスポート(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べきかを識別する。

i) 内部 TOE 転送(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識別する。

j) 蓄積データ完全性(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) TSF 間利用者データ機密転送保護(FDP_UCT)または TSF 間利用者データ完全性転送保護(FDP_UIT)ファミリから適用される TSF 間通信コンポーネントを識別する。

722 図 24 は、このクラスのコンポーネント構成を示す。

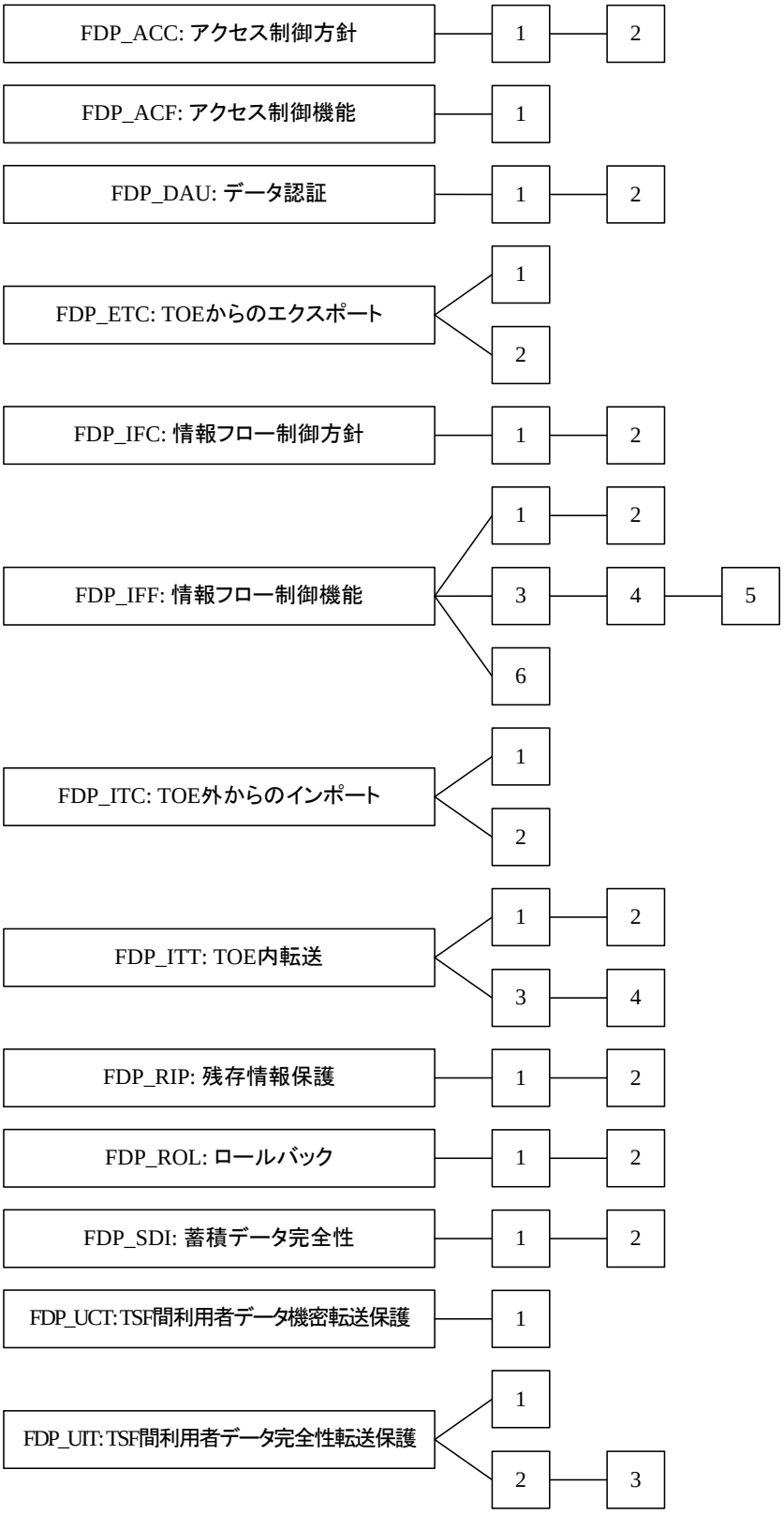


図 24　　FDP: 利用者データ保護クラスのコンポーネント構成

F.1 アクセス制御方針(FDP_ACC)

利用者のための注釈

723 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任意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。

724 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 の(名前による)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 の機能性を定義する規則は、アクセス制御機能(FDP_ACF)及び TOE からのエクスポート(FDP_ETC)のような他のファミリによって定義される。アクセス制御方針(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。

725 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、1 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。

726 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。アクセス制御方針(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: 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。

727 アクセス制御方針(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。

728 このファミリは、PP/ST 作成者に様々な方針を特定させることができる。例えば、1 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 3 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 1 つのサブセットだけをカバーしているとき、TOE は、3 つのアクセス制御 SFP ごとに 1 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 3 つの FDP_ACC.1 サブセットアクセス制御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

729 オブジェクト及びサブジェクトという言葉は、TOE の中のエレメント属性を指す。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 TOE 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。

730 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適切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:

731 **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。

732 **FDP_ACC.1.1** において、PP/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

733 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、1 つのアクセス制御 SFP でカバーされることを要求する。

734 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 1 つのアクセス制御 SFP でカバーされていることを実証しなければならない。

操作

割付:

735 **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。

736 **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)

利用者のための注釈

737 このファミリは、方針の制御の範囲を特定するアクセス制御方針(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。

738 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、アクセスされたオブジェクトが変更されない TOE 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。

739 二人制御、操作の順序規則、あるいは排他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 メカニズムと同様に、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。

740 容認できる各種のアクセス制御機能性は、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

741 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仲介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、アクセス制御仲介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。

742 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。

743 識別情報属性は、仲介に使用するために、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。

744 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。

745 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。

746 グルーピング属性は、1 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、1 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。

747 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:

748 **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、アクセス制御方針(FDP_ACC)からのコンポーネントで定義される。

749 **FDP_ACF.1.1** において、PP/ST 作成者は、各制御されるサブジェクトとオブジェクトに対し、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及び/または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、セキュリティ管理役割(FMT_SMR)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。

750 **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。

751 **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。

752 **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。

F.3 データ認証(FDP_DAU)

利用者のための注釈

753 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。

754 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(発信の否認不可(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 基本データ認証

利用者のための適用上の注釈

755 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一方向ハッシュ関数(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:

756 **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。

757 **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

758 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:

759 **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。

760 **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 TOE からのエクスポート(FDP_ETC)

利用者のための注釈

761 このファミリは、TOE から利用者データを TSF 仲介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た後に無視される。これらのセキュリティ属性の一貫性は、TSF 間 TSF データ一貫性(FPT_TDC)で対応される。

762 TOE からのエクスポート(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。

763 このファミリ、及び対応するインポートファミリ、TOE 外からのインポート(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 TSF 仲介エクスポートと、それに関連するセキュリティ属性に関するものである。

764 ここでは、様々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。両者は互いに関連付けられており、セキュリティ属性は曖昧さなくエクスポートされる利用者データを表す。

765 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_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

766 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 TSF 仲介エクスポートを特定するのに使われる。

操作

割付:

767 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 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 セキュリティ属性を伴う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

768 利用者データは、そのセキュリティ属性と一緒にエクスポートされる。セキュリティ属性は、利用者データと曖昧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。TSF 間高信頼チャネル(FTP_ITC)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、TSF 間 TSF データ一貫性(FPT_TDC)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、高信頼パス(FTP_TRP)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:

769 **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(1 つまたは複数)や情報フロー制御 SFP(1 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。

770 **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)

利用者のための注釈

771 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。

772 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 は、情報フロー制御機能(FDP_IFF)及び TOE からのエクスポート(FDP_ETC)のような他のファミリによって定義する。情報フロー制御方針(FDP_IFC)で名前を付けた情報フロー制御 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、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。

773 これらのコンポーネントはまったく柔軟である。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。

774 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、詳細さのレベルを非常に低くして、オペレーティングシステム内のプロセス単位でサブジェクトを明示的に記述することもあれば、高いレベルで、利用者や入出力チャネルを示す一般的な用語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詳細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方が適切である。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。

775 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、1 つの SFP でカバーされる必要がある。したがって、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、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。

776 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。

777 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。

778 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、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 パケットなど、システムに固有なレベルで特定されることがある。PP の場合、情報のフロー及び操作は、電子メール、データリポジトリ、アクセスの監視などのような種別として表現することができる。

779 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

780 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:

781 **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。

782 **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、様々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。

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

783 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。

784 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:

785 **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。

786 **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、様々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)

利用者のための注釈

787 このファミリは、方針の制御の範囲も特定する情報フロー制御方針(FDP_IFC)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。2 つの「ツリー」から構成され、1 つは共通の情報フロー制御機能問題に対応し、他方は、1 つあるいは複数の情報フロー制御 SFP に関する不正情報フロー(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。

788 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。

789 このファミリでは、「不正情報フローの種別」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。

790 このコンポーネントの柔軟性は、FDP_IFF.1 単純セキュリティ属性及び FDP_IFF.2 階層的セキュリティ属性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

791 このコンポーネントでは、情報におけるセキュリティ属性と、その情報を流れさせるサブジェクトとその情報を受信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。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。

792 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。

793 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:

794 **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、情報フロー制御方針(FDP_IFC)からのコンポーネントにおいて定義される。

795 **FDP_IFF.1.1** において、PP/ST 作成者は、制御されるサブジェクトと情報の各種別に対して、SFP 規則の指定に関連するセキュリティ属性を特定すべきである。例えば、そのようなセキュリティ属性には、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小数種別は、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。

796 **FDP_IFF.1.2** において、PP/ST 作成者は、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。

797 **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。これは、情報とサブジェクトの属性に基づく規則、アクセス操作の結果情報やサブジェクトのセキュリティ属性を自動的に変更する規則、のいずれにも基づかないすべてのSFPの規則を含んでいる。最初の例は特定のタイプの情報のために閾値を制御する SFP の規則である。これはサブジェクトがある特定の回数までのみ、このタイプの情報にアクセスが許可されるような、統計データへのアクセスに基づく規則を持つ情報フローSFP のようなケースが例として挙げられる。2 番目の例は、アクセス操作の結果、どの条件のもとでどのように、サブジェクトやオブジェクトのセキュリティ属性が変化するかを規定しているケースである。ある情報フロー方針は、例えば、特定のセキュリティ属性を持つ情報へのアクセス操作の数を制限するかもしれない。付則が全くないなら、PP／ST 作成者は「なし」を指定するべきである。

798 **FDP_IFF.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、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、前の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.1.4** 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は、特定された SFP がカバーする情報に対し情報フローを生じさせる能力を常時サブジェクトに許可するような、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。

799 **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.1.5** 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は、特定された SFP がカバーする情報に対し、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ような、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

800 このコンポーネントは、名前付き情報フロー制御 SFP が、ラティス(束)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。

801 **FDP_IFF.2.4** 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。

802 **FDP_IFF.2.6** では、ラティス(束)を形成するためのセキュリティ属性のセットに対する要件を表現する。文献により定義され、IT 製品に実装される、いくつもの情報フローポリシーは、ラティス(束)を形成するセキュリティ属性に基づいている。**FDP_IFF.2.6** には、このタイプの情報フローポリシーを記述するため、特に含まれている。

803 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 SFP ごとに 1 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.2.4** のサブ項目に矛盾が生じるかもしれない。

操作

割付:

804 **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、情報フロー制御方針(FDP_IFC)からのコンポーネントにおいて定義される。

805 **FDP_IFF.2.1** において、PP/ST 作成者は、制御されるサブジェクトと情報の各種別に対して、SFP 規則の指定に関連するセキュリティ属性を特定すべきである。例えば、そのようなセキュリティ属性には、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小数種別は、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。

806 **FDP_IFF.2.2** において、PP/ST 作成者は、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。

807 **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。これは、情報とサブジェクトの属性に基づく規則、アクセス操作の結果情報やサブジェクトのセキュリティ属性を自動的に変更する規則、のいずれにも基づかないすべての SFP の規則を含んでいる。最初の例は特定のタイプの情報のために閾値を制御する SFP の規則である。これはサブジェクトがある特定の回数までのみ、このタイプの情報にアクセスが許可されるような、統計データへのアクセスに基づく規則を持つ情報フローSFP のようなケースが例として挙げられる。2 番目の例は、アクセス操作の結果、どの条件のもとでどのように、サブジェクトやオブジェクトのセキュリティ属性が変化するかを規定しているケースである。ある情報フロー方針は、例えば、特定のセキュリティ属性を持つ情報へのアクセス操作の数を制限するかもしれない。付則が全くないなら、PP／ST 作成者は「なし」を指定するべきである。

808 **FDP_IFF.2.4** 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.2.4** 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、すでに特定された 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。

809 F**DP_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.2.5** 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、すでに特定された 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

810 不正情報フローの制御を要求する少なくとも 1 つ以上の SFP がフローの排除を要求しないとき、このコンポーネントが使用されるべきである。

811 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:

812 **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、情報フロー制御方針(FDP_IFC)からのコンポーネントにおいて定義される。

813 **FDP_IFF.3.1** において、PP/ST 作成者は、最大容量制限に従う不正情報フローの種別を特定すべきである。

814 **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

815 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)不正情報フローの排除を要求するとき、このコンポーネントが使用されるべきである。

操作

割付:

816 **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、情報フロー制御方針(FDP_IFC)からのコンポーネントにおいて定義される。

817 **FDP_IFF.4.1** において、PP/ST 作成者は、最大容量制限に従う不正情報フローの種別を特定すべきである。

818 F**DP_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。

819 F**DP_IFF.4.2** において、PP/ST 作成者は、排除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排除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

820 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排除を要求するとき、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排除することが 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性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排除することが期待したとおりの機能性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:

821 **FDP_IFF.5.1** において、PP/ST 作成者は、不正情報フローが排除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、情報フロー制御方針(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

822 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、セキュリティ監査データ生成(FAU_GEN)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:

823 **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、情報フロー制御方針(FDP_IFC)からのコンポーネントにおいて定義される。

824 **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を特定すべきである。

825 **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 TOE 外からのインポート(FDP_ITC)

利用者のための注釈

826 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、TOE の外部から TOE に利用者データを TSF 仲介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、TSF 間 TSF データ一貫性(FPT_TDC)で対応される。

827 TOE 外からのインポート(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。

828 このファミリ及び対応するエクスポートファミリ、TOE からのエクスポート(FDP_ETC)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。

829 ここでは、様々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。

830 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わせるセキュリティ属性の値に関係する。

831 利用者データのインポートに関しては、次の 2 つの可能性がある: 利用者データが、曖昧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。

832 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。

833 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 TSF 仲介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、TOE 外からのインポート(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。TOE からのエクスポート(FDP_ETC)は、その媒体の他端(発生源)に対する責任を持つ。

834 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曖昧さなくインポートされる情報を代表する。

835 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。

836 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

837 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 作成者は、インポートのための規則を特定することもできる。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:

838 **FDP_ITC.1.1** において、PP/ST 作成者は、利用者データが TOE 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。

839 **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 セキュリティ属性を伴う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

840 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曖昧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、TSF 間 TSF データ一貫性(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:

841 **FDP_ITC.2.1** において、PP/ST 作成者は、利用者データが TOE 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。

842 **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ければ「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)

利用者のための注釈

843 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、TSF 間利用者データ機密転送保護(FDP_UCT)及び TSF 間利用者データ完全性転送保護(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 TOE からのエクスポート(FDP_ETC)及び TOE 外からのインポート(FDP_ITC)は、TSF 外へ/からのデータの TSF 仲介転送に対応する。

844 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。

845 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、従来のネットワーク媒体を使って転送が行える。

846 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_ITT.1 基本内部転送保護

操作

割付:

847 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 つまたは複数)を特定すべきである。

選択:

848 **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

849 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様々な形態の保護を提供する場合に使用することができる。

850 転送時のデータの分離を達成する方法の 1 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:

851 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 つまたは複数)を特定すべきである。

選択:

852 **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。

割付:

853 **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

854 このコンポーネントは、FDP_ITT.1 基本内部転送保護あるいは FDP_ITT.2 属性による転送分離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 基本内部転送保護あるいは FDP_ITT.2 属性による転送分離は、データが改変から保護されるような(FDP_ITT.3 完全性監視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。

855 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、次の点を考慮すべきである: データの改変、データの置換、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。

856 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。例えば、利用者データを無視、データを再要求、許可管理者へ通知、他の回線へトラフィック切り替えなどを特定する。

操作

割付:

857 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 つまたは複数)を特定すべきである。

858 F**DP_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。

859 F**DP_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

利用者のための適用上の注釈

860 このコンポーネントは、FDP_ITT.2 属性による転送分離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。

861 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。

862 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、次の点を考慮すべきである: データの改変、データの置換、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。

863 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。

864 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。例えば、利用者データを無視、データを再要求、許可管理者へ通知、他の回線へトラフィック切り替えなどを特定する。

操作

割付:

865 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 つまたは複数)を特定すべきである。

866 **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。

867 **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転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。

868 **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.4.1** 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)

利用者のための注釈

869 残存情報保護は、TSF-制御されたリソースがオブジェクトから割当て解除されたときや他のオブジェクトに再割当てされる前に、リソースに含まれる全部あるいは一部データを再構築することが不可能なやり方で、TSF により割当て解除前に扱われることを保証する。

870 TOE は通常、オブジェクトからリソースを割当て解除する可能性や、オブジェクトにそれらのリソースを再割当てする可能性のある、いくつもの機能をもっている。それらリソース全体ではないが部分的には、以前使ったリソースの重要データを保存するために使用される可能性があり、それらのリソースに対し、FDP_RIP は再利用に対応できるように準備することを求めている。オブジェクトの再利用は、サブジェクトもしくは利用者の明示的な要求によるリソースの解放や、割当て解除とそれに続く別のオブジェクトへのリソースの再割当てという TSF の暗黙的アクションにも同様に適用される。明示的な要求の例としては、ファイルの削除や切捨てや、メインメモリのエリアの解放がある。TSF の暗黙的なアクションの例は、キャッシュ領域の割当て解除と再割当てである。

871 オブジェクト再利用の要件はオブジェクトに属するリソースの内容に関係するが、TSF の他の場所に保存されるかもしれないリソースやオブジェクトに関するすべての情報に関係するわけではない。オブジェクトとしてのファイルのための FDP_RIP 要件を満たす例として、ファイルを構成する全セクターが、再利用に対応できるように準備される必要があることを要求する。

872 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割当て解除とは考えられないかもしれないが、残存情報保護(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。

873 残存情報保護(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、残存情報保護(FDP_RIP)の制御下にある。

874 残存情報保護(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、残存情報保護(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利用者操作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。

875 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残存情報保護(FDP_RIP)が適用される場合、残存情報保護(FDP_RIP)とロールバック(FDP_ROL)で衝突が発生し得る。したがって、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、残存情報保護(FDP_RIP)での「割当て解除」の選択は、ロールバック(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、ロールバック(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り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。

876 利用者が呼び出せる機能ではないため、残存情報保護(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。

877 このファミリは、アクセス制御 SFP(1 つまたは複数)または情報フロー制御 SFP(1 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 サブセット残存情報保護

利用者のための適用上の注釈

878 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:

879 **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:

880 **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

881 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:

882 **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)

利用者のための注釈

883 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。

884 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。

885 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残存情報保護(FDP_RIP)が実施する場合、残存情報保護(FDP_RIP)とロールバック(FDP_ROL)が衝突する。したがって、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、残存情報保護(FDP_RIP)は、ロールバック(FDP_ROL)と併用することはできない。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残存情報保護(FDP_RIP)が実施する場合だけ、残存情報保護(FDP_RIP)はロールバック(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、ロールバック(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。

886 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

887 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:

888 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 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。

889 **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。

890 **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情報及び/またはリストを特定すべきである。

891 **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。ほかに、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

892 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:

893 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 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。

894 **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。

895 **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。ほかに、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)

利用者のための注釈

896 このファミリでは、TSF によって制御されるコンテナ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。

897 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。TSF によって制御される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。

898 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、)情報フロー制御機能(FDP_IFF)あるいはアクセス制御機能(FDP_ACF)ファミリが要求される。

899 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 TOE 内転送(FDP_ITT)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

900 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:

901 **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。

902 **FDP_SDI.1.1** において、PP/ST 作成者は、監視のため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

903 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:

904 **FDP_SDI.2.1** 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。

905 **FDP_SDI.2.1** において、PP/ST 作成者は、監視のため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。

906 **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)

利用者のための注釈

907 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、2 つの端点間の転送中に、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。

908 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。これに対して、エクスポートされた TSF データの機密性(FPT_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

909 アクセス制御または情報フローの方針により、TSF は利用者データの機密性が保護されるような形で利用者データを送信または受信することが要求される。

操作

割付:

910 **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(1 つまたは複数)及び/または情報フロー制御 SFP(1 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:

911 **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)

利用者のための注釈

912 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様々な方法をサポートする。

913 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、エクスポートされた TSF データの完全性(FPT_ITI)は TSF データを扱う。

914 TSF 間利用者データ機密転送保護(FDP_UCT)は利用者データの機密性に対応するので、TSF 間利用者データ完全性転送保護(FDP_UIT)と TSF 間利用者データ機密転送保護(FDP_UCT)は、互いに対をなす。したがって、TSF 間利用者データ完全性転送保護(FDP_UIT)を実現するのと同じメカニズムが、TSF 間利用者データ機密転送保護(FDP_UCT)や TOE 外からのインポート(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

915 アクセス制御または情報フローの方針により、TSF は利用者データの改変が検出されるような形で、利用者データを送信または受信することが要求される。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:

916 **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(1 つまたは複数)や情報フロー制御 SFP(1 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:

917 **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。

918 **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。

919 **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

920 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 TOE の外部にあるので、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:

921 **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(1 つまたは複数)や情報フロー制御 SFP(1 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。

922 **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

923 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:

924 **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(1 つまたは複数)や情報フロー制御 SFP(1 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。

925 **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　クラス FIA: 識別と認証（規定）

926 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曖昧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。

927 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、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。

928 許可利用者の曖昧さのない識別、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。

929 利用者識別(FIA_UID)ファミリは、利用者の識別情報の判断に対応する。

930 利用者認証(FIA_UAU)ファミリは、利用者の識別情報の検証に対応する。

931 認証失敗(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。

932 利用者属性定義(FIA_ATD)ファミリは、SFR の実施時に使用する利用者属性の定義に対応する。

933 利用者-サブジェクトの結合(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。

934 秘密についての仕様(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。

935 図 25 は、このクラスのコンポーネント構成を示す。

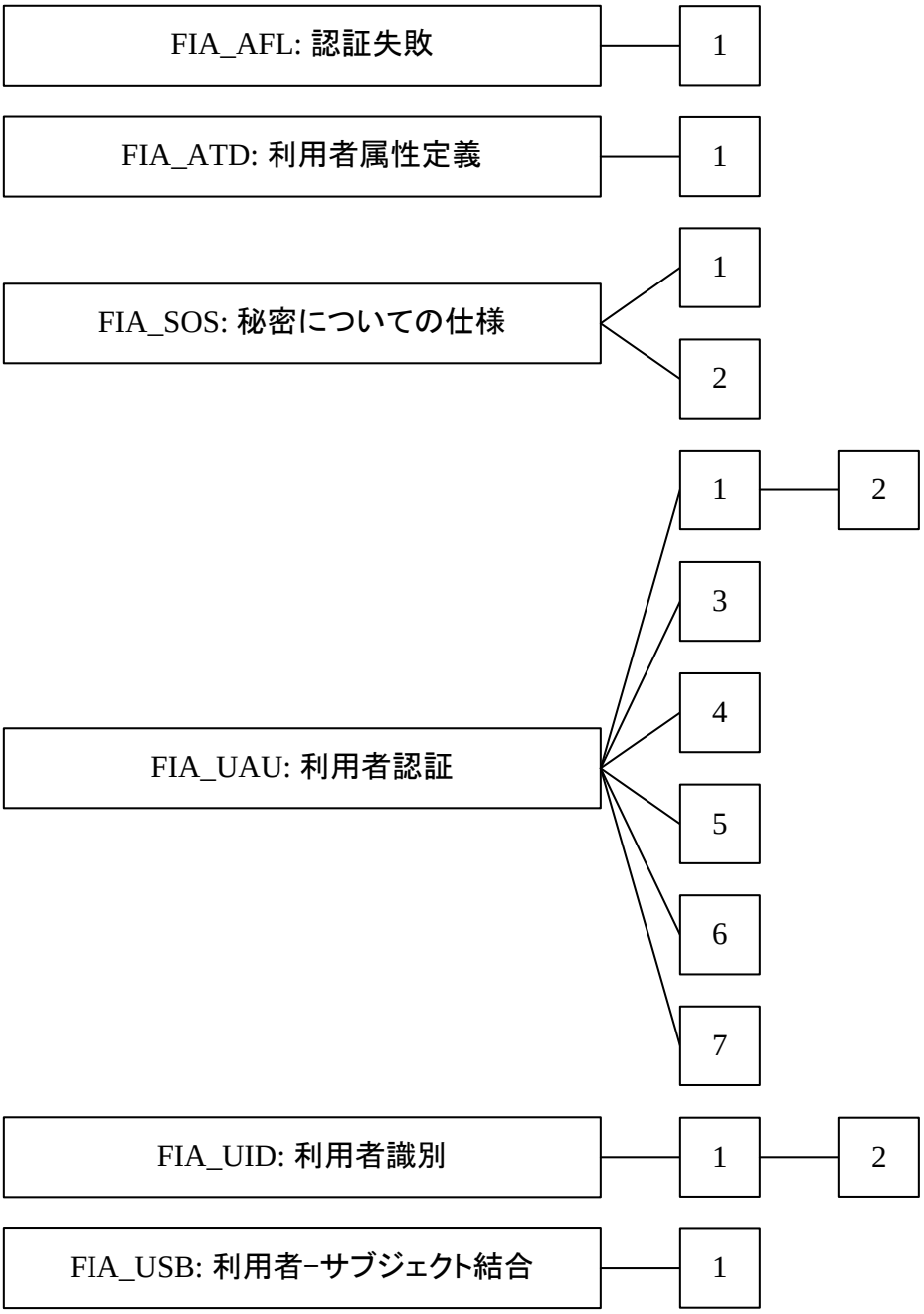


図 25　　FIA: 識別と認証クラスのコンポーネント構成

G.1 認証失敗(FIA_AFL)

利用者のための注釈

936 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閾値を含むが、それに限定されない。

937 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閾値を超えると、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無効にされた場合は、その利用者はシステムにログオンできない。端末が無効にされると、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

938 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、1 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。

939 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、端末の無効化、利用者アカウントの無効化、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。

940 サービス拒否を防ぐため、TOE は通常、無効にできない少なくとも 1 つの利用者アカウントが存在することを保証する。

941 PP/ST 作成者は、利用者セション確立プロセスを再度有効化させたり、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/アカウントを再度有効化させるまで、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、無効時間を倍にする)。

操作

選択:

942 **FIA_AFL.1.1** において、PP/ST 作成者は、正の整数値の割付あるいは許容可能な値を特定する「管理者設定可能な正の整数値」の語句を選択すべきである。

割付:

943 **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 1 つの認証事象が特定されなければならない。

944 **FIA_AFL.1.1** において正の整数の割付が選択された場合、PP/ST 作成者は、その値を満たすか超えたとき事象を引き起こすような不成功認証試行回数のデフォルト値(正の整数)を特定すべきである。

945 **FIA_AFL.1.1** において管理者設定可能な正の整数が選択された場合、PP/ST 作成者は、TOE の管理者が構成できる不成功認証試行回数の許容可能な範囲を特定すべきである。認証試行回数は上限より小さいか等しく、下限より大きいか等しい値とすべきである。

選択:

946 **FIA_AFL.1.2** で、PP/ST 作成者は、定義された不成功の認証試行の数に達するか、上回るかのどちらを TSF によるアクションのトリガーにしなければならないかを選択すべきである。

割付:

947 **FIA_AFL.1.2** において、PP/ST 作成者は、選択のとおり、閾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、端末の無効を徐々に長くする(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無効にし、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)

利用者のための注釈

948 すべての許可利用者は、その利用者の識別情報以外に、SFR 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、セキュリティ上の決定において TSF 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。

949 個々のセキュリティ方針(SFP)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

950 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。

951 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:

952 **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 秘密についての仕様(FIA_SOS)

利用者のための注釈

953 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メカニズム、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。

954 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、TOE に導入される)。そのような場合、FIA_SOS.1 秘密の検証コンポーネントは、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。

955 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 TSF 秘密生成コンポーネントは、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。

956 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: 暗号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

957 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:

958 **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、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 TSF 秘密生成

利用者のための適用上の注釈

959 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。

960 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べきであることを保証するように、パラメタの選択が行われるべきである。

操作

割付:

961 **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。

962 **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)

利用者のための注釈

963 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

964 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 仲介アクションを PP/ST 作成者が定義することを要求する。TSF 仲介アクションは、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 仲介アクションに対し、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。

965 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 識別のタイミングまたは FIA_UID.2 アクション前の利用者識別のどちらかの使用が必要である。

操作

割付:

966 **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 仲介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 アクション前の利用者認証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一例は、ログイン手続きにおけるヘルプの要求である。

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

967 このコンポーネントは、その他の TSF 仲介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、利用者が認証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

968 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。

969 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:

970 **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。

971 **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

972 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。

973 PP/ST 作成者は、この要件が適用される認証メカニズム(1 つまたは複数)を特定できる。

操作

割付:

974 **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

975 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: 識別と認証クラスから適用すべき要件が選択されねばならない。認証メカニズムの様々な用途に対する様々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。

976 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。

977 TOEと対話する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:

978 **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。

979 **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」。

980 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

981 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:

982 **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。

983 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

984 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。

985 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:

986 **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)

利用者のための注釈

987 このファミリは、利用者が、TSF に仲介され、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

988 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。

989 FIA_UID.1 識別のタイミングを使用する場合、FIA_UID.1 識別のタイミングで言及された TSF 仲介アクションは、FIA_UAU.1 認証のタイミングにも現れるべきである。

操作

割付:

990 **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 仲介アクションのリストを特定すべきである。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_UID.2 アクション前の利用者識別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

991 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)

利用者のための注釈

992 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-サブジェクト結合

利用者のための適用上の注釈

993 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。

994 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。特殊なサブジェクトのカテゴリは、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」とみなされる。

操作

割付:

995 **FIA_USB.1.1** において、PP/ST 作成者は、サブジェクトに結合される利用者セキュリティ属性のリストを特定すべきである。

996 **FIA_USB.1.2** において、PP/ST 作成者は、属性がサブジェクトに最初に関連付けられるときに適用する規則、または「なし」を特定すべきである。

997 **FIA_USB.1.3** において、PP/ST 作成者は、利用者に代わって動作するサブジェクトに関連付けられる利用者セキュリティ属性に変更が加えられるときに適用する規則、または「なし」を特定すべきである。

附属書H　クラス FMT: セキュリティ管理（規定）

998　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。能力の分離など、様々な管理役割及びそれらの相互作用も特定できる。

999　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 時限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、TOE 内 TSF データ複製一貫性(FPT_TRC)からのコンポーネントを使うのが当を得ている。

1000　図 26 は、このクラスのコンポーネント構成を示す。

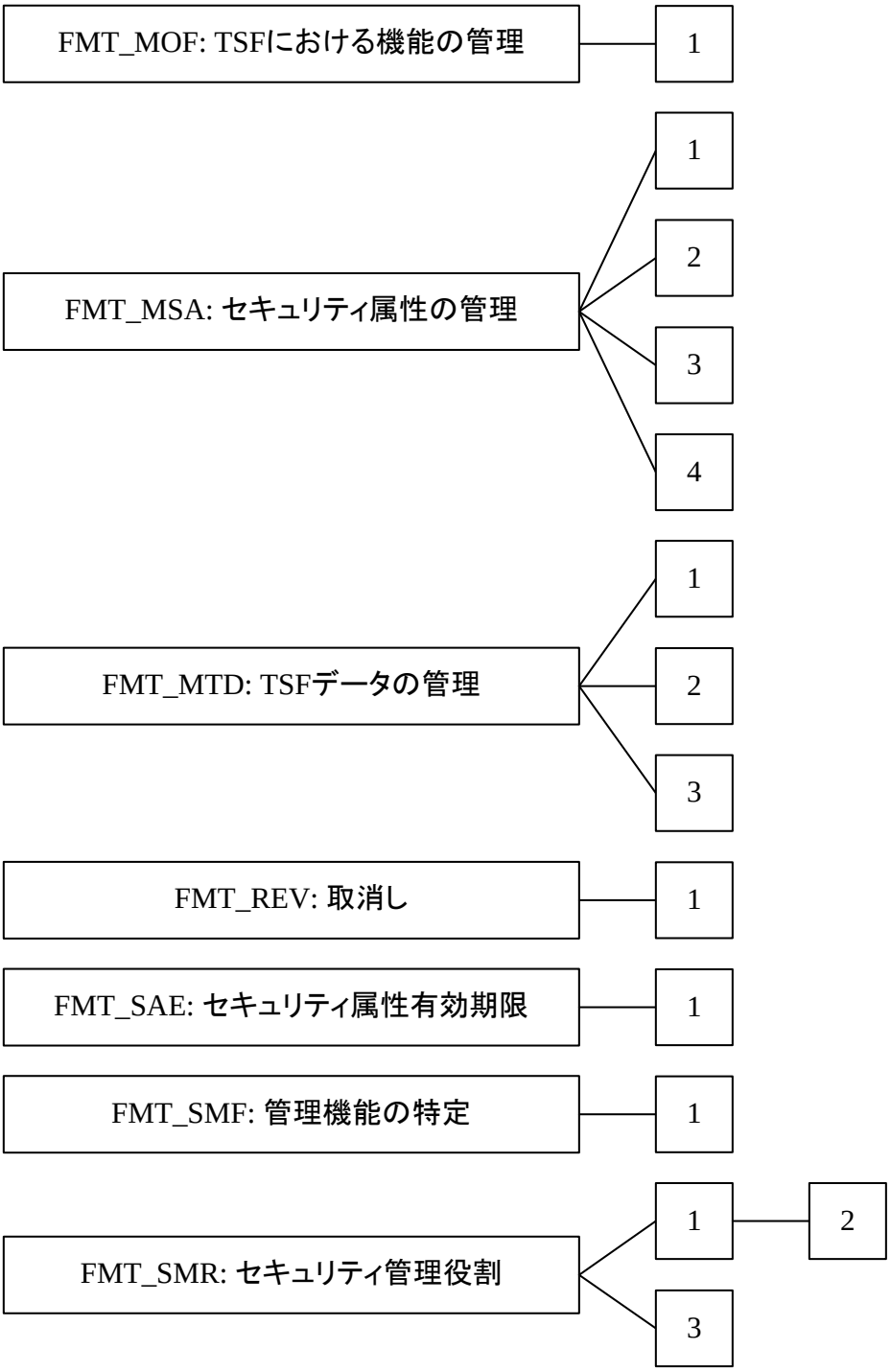


図 26　　FMT: セキュリティ管理クラスのコンポーネント構成

H.1　　TSF における機能の管理(FMT_MOF)

利用者のための注釈

1001　　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) 設置及び構成全般に関する管理機能。例えば、TOE 構成、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、周辺装置を有効/無効にする、リムーバブル格納媒体のマウント、バックアップ及び回復など。

1002 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 TOE 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。

1003 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

利用者のための適用上の注釈

1004 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、セキュリティ機能を停止する/動作させる、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:

1005 **FMT_MOF.1.1** において、PP/ST の作成者は、役割が、セキュリティ機能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、のいずれに決定されるかを選択すべきである。

割付:

1006 **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。

1007 **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 セキュリティ役割で特定される。

H.2 セキュリティ属性の管理(FMT_MSA)

利用者のための注釈

1008 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。

1009 セキュリティ属性は、TSF のふるまいに影響を与える。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、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)あるいは与えられたポリシー／規則によって継承される値によって管理される必要があるかもしれない。

1010 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 セキュリティ属性の管理による管理の対象になるということに注意が要る。

1011 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 ガイダンスに委ねられている。

1012 実際の例では、サブジェクト、オブジェクト、あるい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 セキュリティ属性の管理は、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

利用者のための適用上の注釈

1013 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 セキュリティ役割内で役割が割り付けられる。

1014 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:

1015 **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:

1016 **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、問い合わせ、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:

1017 **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。

1018 **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 セキュリティ役割で特定される。

1019 **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.2 セキュアなセキュリティ属性

利用者のための適用上の注釈

1020 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。

1021 「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、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。

操作

割付:

1022 **FMT_MSA.2.1** において、PP/ST 作成者は、セキュアな値のみが提供されることが要求されるセキュリティ属性のリストを特定すべきである。

FMT_MSA.3 静的属性初期化

利用者のための適用上の注釈

1023 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、作成時に様々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:

1024 **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:

1025 **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。これらの選択肢の 1 つのみを選択することができる。

割付:

1026 **FMT_MSA.3.1** において、PP/ST 作成者がその他の特性を選択した場合、PP/ST 作成者は、デフォルト値が要求する特性を特定すべきである。

1027 **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 セキュリティ役割で特定される。

FMT_MSA.4 セキュリティ属性値継承

利用者のための適用上の注釈

1028 このコンポーネントは、セキュリティ属性が値を継承する規則のセットの詳述と、適用するこれらの規則を満たす条件を要求する。

操作

割付:

1029 **FMT_MSA.4.1** において、PP/ST 作成者は、特定のセキュリティ属性により継承される値を制御する規則を、それらの規則が適用されるための条件を含め特定する。例えば、もし新しいファイルまたはディレクトリが作られるなら(マルチレベルファイルシステムにおいて)、そのラベルは、それが作成されるときに利用者がログインするラベルである。

H.3 TSF データの管理(FMT_MTD)

利用者のための注釈

1030 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、誰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

利用者のための適用上の注釈

1031 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 セキュリティ役割内で役割が割り付けられる。

1032 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:

1033 **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、問い合わせ、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」の意味を分かりやすく言うと、TSF データの内容が除去されるが、TSF データを格納するエンティティは TOE の中に残るということである。

割付:

1034 **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。

1035 **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 セキュリティ役割で特定される。

1036 **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.2 TSF データにおける限界値の管理

利用者のための適用上の注釈

1037 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:

1038 **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。

1039 **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 セキュリティ役割で特定される。

1040 **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

利用者のための適用上の注釈

1041 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。

1042 「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、及びその結果としてのガイダンスの情報に委ねられる。

操作

割付:

1043 **FMT_MTD.3.1** において、PP/ST 作成者は、どのような TSF データがセキュアな値のみを受け入れることを要求するのかを特定すべきである。

H.4 取消し(FMT_REV)

利用者のための注釈

1044 このファミリは、TOE 内の様々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

利用者のための適用上の注釈

1045 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

割付:

1046 **FMT_REV.1.1** において、PP/ST 作成者は、関連するオブジェクト／サブジェクト／利用者／他のリソースに変更があった場合、どのセキュリティ属性が取り消されるのかを特定すべきである。

選択:

1047 **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、あるいはいかなる追加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。

割付:

1048 **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 セキュリティ役割で特定される。

1049 **FMT_REV.1.1** において、PP/ST 作成者は、追加資源が選択された場合、それらの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。

1050 **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)

利用者のための注釈

1051 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:

1052 **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。

1053 **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 セキュリティ役割で特定される。

1054 **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 管理機能の特定(FMT_SMF)

利用者のための注釈

1055 このファミリは、TOE が管理機能を特定することを可能にする。割付を実行する際に、リストされる各セキュリティ管理機能は、セキュリティ属性管理、TSF データ管理、またはセキュリティ機能管理のうちのいずれかである

FMT_SMF.1 管理機能の特定

利用者のための適用上の注釈

1056 このコンポーネントは、提供されるべき管理機能を特定する。

1057 PP/ST の作成者は、このコンポーネントによってリストされるべき管理機能の基礎を得るために、PP/ST に含まれるコンポーネントの「管理」の節を調べるべきである。

操作

割付:

1058 **FMT_SMF.1.1** において、PP/ST の作成者は、セキュリティ属性管理、TSF データ管理、またはセキュリティ機能管理のいずれかである、TSF により提供される管理機能を特定すべきである。

H.7 セキュリティ管理役割(FMT_SMR)

利用者のための注釈

1059 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。

1060 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。

1061 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、日常管理といった様々な役割の定義を認める。

1062 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、TSF における機能の管理(FMT_MOF)、セキュリティ属性の管理(FMT_MSA)、及び TSF データの管理(FMT_MTD)で定義される。

1063 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、利用者の定義及び有効化が可能かもしれないが、利用者の削除(管理者(役割)用に確保されている)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 セキュリティの役割

利用者のための適用上の注釈

1064 このコンポーネントは、TSF が認識すべき様々な役割を特定する。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:

1065 **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。役割の例には、所有者、監査者、管理者などがある。

FMT_SMR.2 セキュリティ役割における制限

利用者のための適用上の注釈

1066 このコンポーネントは、TSF が認識すべき様々な役割、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。

1067 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、様々な役割間の相互関係も特定する。

操作

割付:

1068 **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。役割の例には、所有者、監査者、管理者などがある。

1069 **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:「1 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

利用者のための適用上の注釈

1070 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:

1071 **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。役割の例には、監査者及び管理者などがある。

附属書I クラス FPR: プライバシー（規定）

1072 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。

1073 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性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。

1074 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)とともに、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: 識別と認証や FAU: セキュリティ監査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。

1075 追加情報が FAU: セキュリティ監査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。

1076 このクラスでは、匿名性、偽名性、リンク不能性、及び観察不能性の 4 つのファミリを記述する。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。

1077 すべてのファミリは、利用者が、利用者自身の識別情報を暴露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。

1078 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。匿名性の実例には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」。

1079 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。

1080 図 27 は、このクラスのコンポーネント構成を示す。

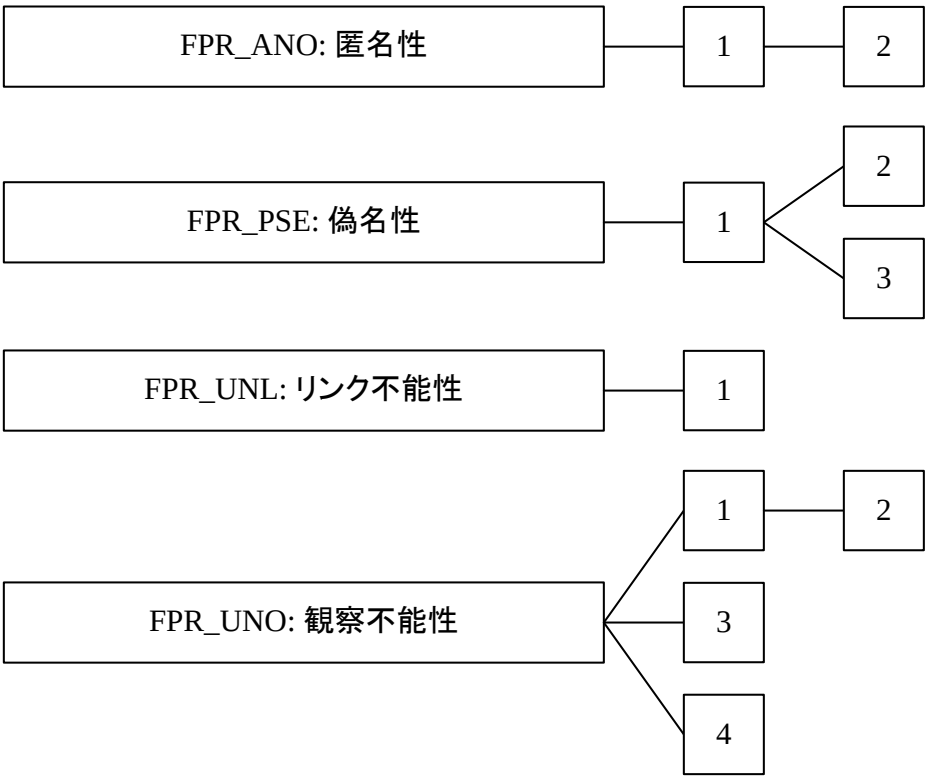


図 27　　FPR: プライバシークラスのコンポーネント構成

I.1　匿名性(FPR_ANO)

利用者のための注釈

1081　匿名性は、その利用者識別情報を暴露することなく、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。

1082　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。

1083　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、暴露から保護されない。

1084　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 情報を請求しない匿名性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。

1085　「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。

1086 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。

1087 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。

1088 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。

1089 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

1090 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:

1091 **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。

1092 **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

1093 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:

1094 **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。

1095 **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。

1096 **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。

1097 **FPR_ANO.2.2** において、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)

利用者のための注釈

1098 偽名性は、利用者が、その識別情報を暴露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。

1099 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。

1100 コンポーネント FPR_PSE.1 偽名性は、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、2 つの要件のセット: FPR_PSE.2 可逆偽名性及び FPR_PSE.3 別名偽名性が提示される。

1101 参照を使用するためには、元の利用者の識別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、1 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、FPR_PSE.2 可逆偽名性を使って、それらのサービスを記述しようとするかもしれない。

1102 参照のもう 1 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。

1103 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。

1104 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。

1105 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。

1106 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。

1107 応用として考えられるものは、識別情報を暴露せず、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。

1108 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

1109 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:

1110 **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。

1111 **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。

1112 **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(1 つまたは複数)を識別すべきである。

1113 **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:

1114 **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。これらの選択肢の 1 つのみを選択することができる。

割付:

1115 **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

1116 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。

1117 FPR_PSE.1 偽名性において、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、1 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:

1118 **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。

1119 **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。

1120 **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(1 つまたは複数)を識別すべきである。

1121 **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:

1122 **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。これらの選択肢の 1 つのみを選択することができる。

割付:

1123 **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:

1124 **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:

1125 **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。

1126 F**PR_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.3 別名偽名性

利用者のための適用上の注釈

1127 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。

1128 もし利用者が、その識別情報を暴露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:

1129 **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。

1130 **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。

1131 **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(1 つまたは複数)を識別すべきである。

1132 **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:

1133 **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。これらの選択肢の 1 つのみを選択することができる。

割付:

1134 **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。

1135 **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 1 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)

利用者のための注釈

1136 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 1 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。

1137 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 1 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分かれば、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。

1138 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。

1139 リンク不能性は、様々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。

1140 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、1 つの偽名を何度も使用させる能力を含むことがある。

1141 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様々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

1142 このコンポーネントは、利用者がシステム内の様々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:

1143 **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。

1144 **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:

1145 **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:

1146 **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)

利用者のための注釈

1147 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。

1148 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。

1149 多くの技法が、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法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 内の様々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。この技法は、FPR_UNO.2 観察不能性に影響を与える情報の配置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。この技法は、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べき場合(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。

1150 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 許可利用者観察可能性が使用でき、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。

1151 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。

1152 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

1153 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。

操作

割付:

1154 **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。

1155 **FPR_UNO.1.1** において、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取りや書き込みなど)を観察できなくなる。

1156 **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。

1157 **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 観察不能性に影響を与える情報の配置

利用者のための適用上の注釈

1158 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。

1159 このコンポーネントの使用例は、1 つの機能を提供するために、ランダムに配置された 1 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 1 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。

1160 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)。

操作

割付:

1161 **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。

1162 **FPR_UNO.2.1** において、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取りや書き込みなど)を観察できなくなる。

1163 **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。

1164 **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。

1165 **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。

1166 **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ればならず、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

1167 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:

1168 **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。

1169 **FPR_UNO.3.1** において、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。

1170 **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

1171 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または複数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レビューは認められるが、必須にはならない。

操作

割付:

1172 **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。

1173 **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　クラス FPT: TSF の保護
（規定）

1174　このクラスは、TSF を構成するメカニズムの完全性及び管理に関係し、かつ TSF データの完全性に関係する機能要件のファミリを含む。ある意味で、この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ネントと重複しているように見えるかもしれず、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: 利用者データ保護は、利用者データ保護に焦点を当てているのに対し、FPT: TSF 保護は TSF データ保護に焦点を当てている。実際、FPT: TSF 保護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。

1175　このクラスの観点から、TSF に関して、次の 3 つの重要なエレメントがある:

a)　TSF の実装、これは SFR を実施するメカニズムを実行し、実装する。

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

c)　SFR を実施するために、TSF が相互に影響し得る外部エンティティ。

1176　FPT: TSF の保護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)　TSF 物理的保護(FPT_PHP)、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)　外部エンティティのテスト(FPT_TEE)と TSF 自己テスト(FPT_TST)、これらは SFR を実施するために、TSF と相互作用する外部エンティティの正しい操作と、TSF データと TSF 自体の完全性を検証する能力を許可利用者に提供する。

c)　高信頼回復(FPT_RCV)、フェールセキュア(FPT_FLS)、及び TOE 内 TSF データ複製一貫性(FPT_TRC)、これらは、障害発生時と直後の TSF のふるまいに対応する。

d)　エクスポートされた TSF データの可用性(FPT_ITA)、エクスポートされた TSF データの機密性(FPT_ITC)、エクスポートされた TSF データの完全性(FPT_ITI)、これらは、TSF と他の高信頼 IT 製品間の TSF データの保護及び可用性に対応する。

e)　TOE 内 TSF データ転送(FPT_ITT)、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。

f)　リプレイ検出(FPT_RPL)、これは、情報及び/または操作の様々な種別のリプレイに対応する。

g)　状態同期プロトコル(FPT_SSP)、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。

h)　タイムスタンプ(FPT_STM)、これは、信頼できるタイミングに対応する。

i)　TSF 間 TSF データ一貫性(FPT_TDC)、これは、TSF と他の高信頼 IT 製品間で共有する TSF データの一貫性に対応する。

1177　図 28 は、このクラスのコンポーネント構成を示す。

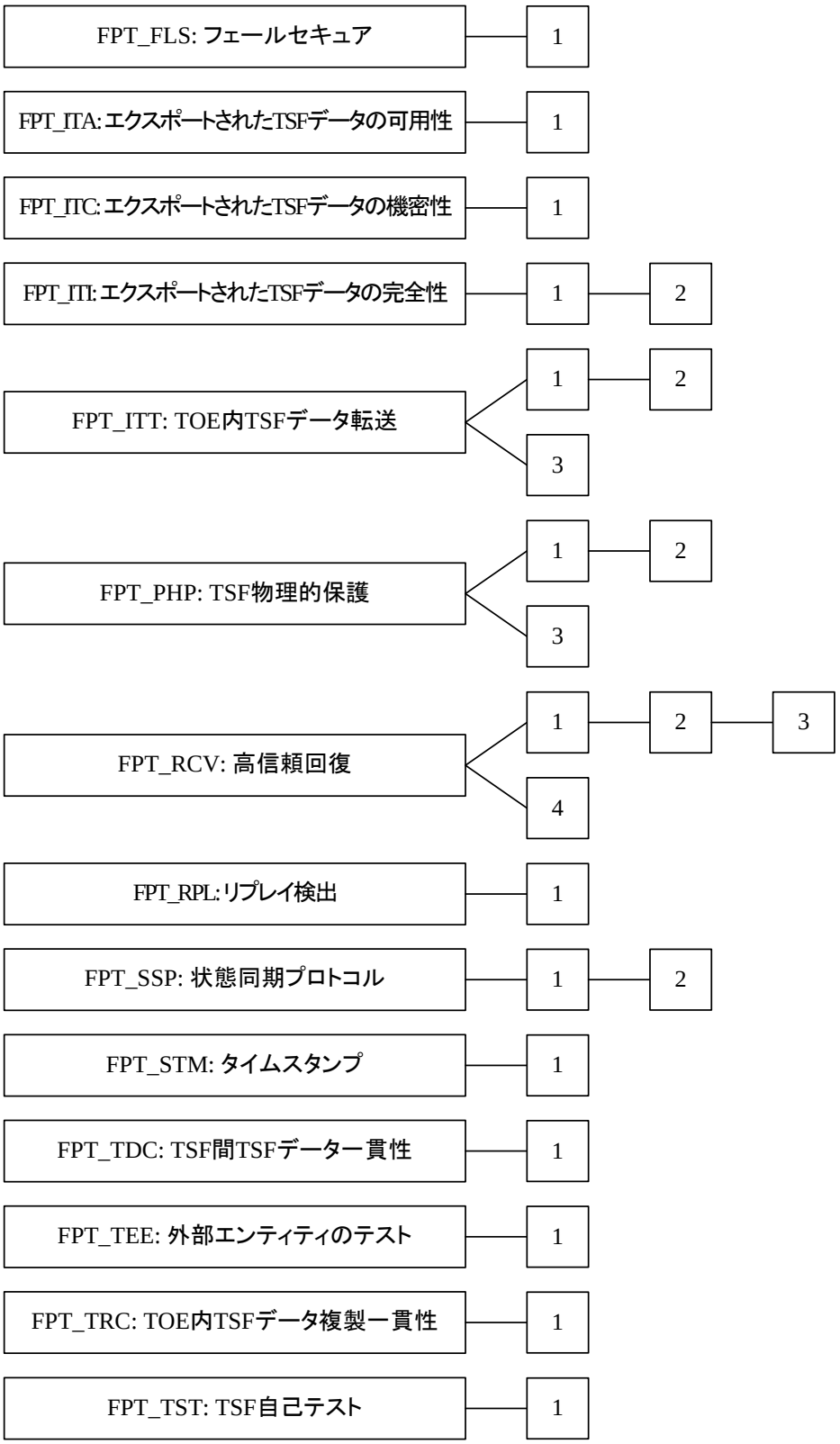


図 28　　FPT: TSF の保護クラスのコンポーネント構成

J.1 フェールセキュア(FPT_FLS)

利用者のための注釈

1178 このファミリの要件は、TSF 中の特定の種別の障害事象において、TOE がその SFR を常に実施することを保証する。

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

1179 「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 SFR の正しい実施を継続している状態を指す。

1180 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。

1181 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:

1182 **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、SFR 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.2 エクスポートされた TSF データの可用性(FPT_ITA)

利用者のための注釈

1183 このファミリは、TSF 及び他の高信頼 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。

1184 このファミリは、TSF が TSF データを他の高信頼 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。

1185 もし、様々な種別の TSF データに対して様々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:

1186 **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。

1187 **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。

1188 **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。例えば、TOE と他の高信頼 IT 製品間に接続がなければならない。

J.3 エクスポートされた TSF データの機密性(FPT_ITC)

利用者のための注釈

1189 このファミリは、TSF と他の高信頼 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。

1190 このファミリは、TSF が TSF データを他の高信頼 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

評価者のための注釈

1191 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.4 エクスポートされた TSF データの完全性(FPT_ITI)

利用者のための注釈

1192 このファミリは、TSF と他の高信頼 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。

1193 このファミリは、TSF が TSF データを他の高信頼 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。他の高信頼 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、他の高信頼 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、他の高信頼 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

1194 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他の高信頼 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。

1195 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:

1196 **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。

1197 **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。アクションの例としては、「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」などがある。

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

1198 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。

1199 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、1,000 個のランダムなメッセージのから 1 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。

1200 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

1201 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:

1202 **FPT_ITI.2.1** 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。

1203 **FPT_ITI.2.2** 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。アクションの例としては、「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」などがある。

1204 **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.5 TOE 内 TSF データ転送(FPT_ITT)

利用者のための注釈

1205 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。

1206 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

1207 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 1 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:

1208 **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

1209 SFP 関連属性に基づく TSF データの分離を達成する方法の 1 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:

1210 **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。

FPT_ITT.3 TSF データ完全性監視

操作

選択:

1211 **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、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から選択すべきである。

割付:

1212 **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。

1213 **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.6 TSF 物理的保護(FPT_PHP)

利用者のための注釈

1214 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。

1215 このファミリにおける要件は、TSF が物理的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。

1216 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。

1217 許可利用者が物理的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、外部シールド、カード、及びチップなど、いくつかの構造体から構成されよう。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。つまり、すべての装置が上記の機能を備える必要はなく、完全な物理的な構造が全体としてこれらの機能を提供するべきである。

1218 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

1219 FPT_PHP.1 物理的攻撃の受動的検出は、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。一般的に、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。文字どおり、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 セキュリティ機能のふるまいの管理における管理機能の特定は、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と考えられるべきである。もしこれが非 IT メカニズム(物理的な検査など)でなされる場合は、管理機能は要求されない。

FPT_PHP.2 物理的攻撃の通知

利用者のための適用上の注釈

1220 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 物理的攻撃の通知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。FMT_MOF.1 セキュリティ機能のふるまいの管理における管理機能の特定は、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と考えられるべきである。

操作

割付:

1221 **FPT_PHP.2.3** において、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 装置/エレメントのリストを提供すべきである。

1222 **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 セキュリティ機能のふるまいの管理ファミリの)によって異なることがある。

FPT_PHP.3 物理的攻撃への抵抗

利用者のための適用上の注釈

1223 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。

1224 このコンポーネントは、TSF 装置あるいは TSF エレメントが、TSF 装置の内部、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:

1225 F**PT_PHP.3.1** において、PP/ST 作成者は、TSF がそれの物理的改ざんに抵抗すべき TSF 装置/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、装置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 の物理的装置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。自動応答は、その装置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装置を物理的に無効にするというものが相当する。

1226 F**PT_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 装置/エレメントのリストを特定すべきである。

J.7 高信頼回復(FPT_RCV)

利用者のための注釈

1227 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。

1228 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取り/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、設置された構成が不適切)。

1229 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。

1230 高信頼回復(FPT_RCV)を選択するとき、考慮しなければならない高信頼回復(FPT_RCV)と TSF 自己テスト(FPT_TST)間の異なる相互作用がある:

a) 高信頼回復の必要性は、TSF 自己テストの結果を通して示すことができる、そこで、自己テストの結果は、TSF がセキュアでない状態であること、そしてセキュアな状態に復帰するのか、あるいはメンテナンスモードに移るのか、が要求されていることを示す。

b) 上述したように、障害は、管理者により識別することができる。管理者は、セキュアな状態に TOE を回復するアクションを行うことができ、またセキュアな状態が達成されたことを確認する TSF 自己テストを起動することができる。あるいは、TSF 自己テストは、回復プロセスを完了するために起動されるかもしれない。

c) 上記の a)及び b)の組み合わせでは、高信頼回復の必要性が、TSF 自己テストの結果を通して示される場合、管理者は TOE がセキュアな状態に回復するアクションを行い、それからセキュアな状態が達成されたことを確認する TSF 自己テストを実施する。

d) 自己テストは、障害/サービスの中断を検出し、次に、自動回復を行うか、またはメンテナンスモードに移るかのどちらか一方を行う。

1231 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: セキュリティ管理の機能である。もし FMT: セキュリティ管理が、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、SFR が侵害されるような方法で TOE を構成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。

1232 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、TSF 自己テスト(FPT_TST)、フェールセキュア(FPT_FLS)、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。これらファミリの 1 つを使用することは、高信頼回復(FPT_RCV)の採用をサポートするために必要であると思われる。これは TOE が、いつ回復が必要とされるか検出することができるように保証することである。

1233 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。

1234 回復の後で、TSF の自己テストを通してセキュアな状態が達成されたことを確認する必要があるかもしれない。しかし、回復がセキュアな状態でのみ達成されるような方法で実行された場合、そうでなければ回復が失敗するような方法で実行された場合、TSF 自己テストのコンポーネントである FPT_TST.1 TSF テストへの依存性は、論証し取り除くことができる。

FPT_RCV.1 手動回復

利用者のための適用上の注釈

1235 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。

1236 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。

評価者のための注釈

1237 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。メンテナンス時に、アクセスを許可利用者に制限するように、制御が適切に行われるべきである。

操作

割付:

1238 **FPT_RCV.1.1** において、PP/ST 作成者は、TOE がメンテナンスモードに移る必要がある、障害/サービス中断(例えば、停電、監査格納の領域枯渇、あらゆる障害または中断)のリストを特定するべきである。

FPT_RCV.2 自動回復

利用者のための適用上の注釈

1239 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。

1240 コンポーネント FPT_RCV.2 自動回復は、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 1 つ存在することを要求することによって、FPT_RCV.1 手動回復の機能範囲を拡張する。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。

評価者のための注釈

1241 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。メンテナンス時に、アクセスを許可利用者に制限するように、制御が適切に行われるべきである。

1242 **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。

1243 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:

1244 **FPT_RCV.2.1** において、PP/ST 作成者は、TOE がメンテナンスモードに移る必要がある、障害/サービス中断(例えば、停電、監査格納の領域枯渇、あらゆる障害または中断)のリストを特定するべきである。

1245 **FPT_RCV.2.2** において、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

利用者のための適用上の注釈

1246 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。

1247 コンポーネント FPT_RCV.3 過度の損失のない自動回復は、TSF 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 自動回復の機能範囲を拡張する。FPT_RCV.2 自動回復では、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 過度の損失のない自動回復では除外される。

1248 このコンポーネントは、TSF 制御下の 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。

評価者のための注釈

1249 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。メンテナンス時に、アクセスを許可利用者に制限するように、制御が適切に行われるべきである。

1250 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:

1251 **FPT_RCV.3.1** において、PP/ST 作成者は、TOE がメンテナンスモードに移る必要がある、障害/サービス中断(例えば、停電、監査格納の領域枯渇、あらゆる障害または中断)のリストを特定するべきである。

1252 **FPT_RCV.3.2** において、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。

1253 **FPT_RCV.3.3** において、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

利用者のための適用上の注釈

1254　機能回復は、TSF 内で障害が発生したとしても、TSF 内の所定の機能が正常に完了すべきか、あるいはセキュアな状態に回復すべきことを要求する。

操作

割付:

1255　**FPT_RCV.4.1** において、PP/ST 作成者は、機能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、特定された機能は、正常に完了するか、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.8　リプレイ検出(FPT_RPL)

利用者のための注釈

1256　このファミリは、様々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

1257　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:

1258　**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。

1259　**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。とられるべきアクションのセットには、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などがある。

J.9　状態同期プロトコル(FPT_SSP)

利用者のための注釈

1260　分散 TOE は、TOE 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 TOE 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。

1261 状態同期プロトコル(FPT_SSP)は、信頼できるプロトコルを使用する TSF のある重要な機能についての要件を制定する。状態同期プロトコル(FPT_SSP)は、TOE の 2 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。

1262 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が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 TOE 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

1263 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 1 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

1264 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。

1265 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 の両方のパートの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.10 タイムスタンプ(FPT_STM)

利用者のための注釈

1266 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。

1267 「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、及び信頼の受け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

1268 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.11 TSF 間 TSF データー貫性(FPT_TDC)

利用者のための注釈

1269 分散あるいは複合環境において、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。

1270 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。

1271 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 2 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。

1272 TSF データの完全性に関心が置かれるのであれば、エクスポートされた TSF データの完全性(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

1273 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 2 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、2 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:

1274 **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 が提供しなければならない、TSF データの種別のリストを定義すべきである。

1275 **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.12 外部エンティティのテスト（FPT_TEE）

利用者のための注釈

1276 このファミリは、TSF によるひとつあるいは複数の外部エンティティのテストに対する要件を規定する。これら外部エンティティは、人間の利用者ではなく、TOE と対話するソフトウェア、及び/または、ハードウェアの組み合わせが含まれる。

1277 実行されるかもしれないテストのタイプに関する例は以下のとおりである。

a)ファイアウォールが存在するか、正しく構成されているかどうかのテスト

b)アプリケーション TOE が稼動するオペレーティングシステムのいくつかの特性のテスト

c)スマートカード OS TOE が稼動する IC のいくつかの特性のテスト(例えば、乱数発生器)

1278 外部エンティティはテスト結果に関し、意図的に、あるいは正常に動作していないため、「うそ」をついているかもしれないことに注意すること。

1279 これらのテストは、あるメンテナンス状態で、始動時、オンラインあるいは継続的に実行できる。テストの結果として TOE によりとられるアクションは、このファミリの中でも定義できる。

評価者のための注釈

1280 外部エンティティのテストは、TSF が依存するそれらの特性のすべてをテストするために、十分であるべきである。

FPT_TEE.1 外部エンティティのテスト

利用者のための適用上の注釈

1281 このコンポーネントは、人間の利用者に適用されることは意図されていない。

1282 このコンポーネントは、定期的にテスト機能を呼び出す能力を要求することによって、TSF の操作が依存する外部エンティティの関連する特性の定期的なテストのサポートを提供する。

1283 PP/ST の作成者は、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。

評価者のための注釈

1284 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。メンテナンス時には、許可利用者のみにアクセスが制限されるように、制御がなされるべきである。

操作

選択:

1285 **FPT_TEE.1.1** において、PP/ST 作成者は、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、あるいはその他の条件で、いつ TSF が外部エンティティのテストを実行させるかを特定すべきである。テストが頻繁に実行されれば、テストがより頻繁に実行されないときと比べて、エンドユーザは、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、外部エンティティのテストが 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。

割付:

1286 **FPT_TEE.1.1** において、PP/ST 作成者は、テストでチェックされる外部エンティティの特性を特定すべきである。これらの特性の例では、TSF の何らかのアクセス制御部分を支援するディレクトリサーバの構成や可用性の特性を含んでもよい。

1287 **FPT_TEE.1.1** において、PP/ST の作成者は、もし、その他の条件が選択されるのであれば、外部エンティティのテストが稼動する頻度を特定すべきである。この、その他の頻度や条件の例としては、利用者が TOE とセションを開始することを要求するたび、テストを実行させるかもしれない。この例では、利用者認証プロセスで、TSF と相互作用する前に、ディレクトリサーバを検査する場合である。

1288 **FPT_TEE.1.2** において、PP/ST の作成者は、テストが失敗したとき、TSF が実行しなければならないアクションを特定すべきである。例えばディレクトリサーバにおけるこれらのアクションの例は、代替可能サーバへの接続か、そうでなければバックアップサーバを探すか、を含んでよい。

J.13 TOE 内 TSF データ複製一貫性(FPT_TRC)

利用者のための注釈

1289 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、パートが無効になったとき、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。

1290 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。

1291 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:

1292 **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機能のリストを特定すべきである。

J.14 TSF 自己テスト(FPT_TST)

利用者のための注釈

1293 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 によってとられるアクションは、他のファミリで定義される。

1294 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様々な障害による、TSF データと TSF 自体(すなわち TSF 実行コードまたは TSF ハードウェアコンポーネント)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。

1295 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。

1296 「TSF の正しい動作」という用語は、主として、TSF の動作と TSF データの完全性を指す。

FPT_TST.1 TSF テスト

利用者のための適用上の注釈

1297 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。

評価者のための注釈

1298 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。これらのモード時に、アクセスを許可利用者に制限するように、制御が適切に行われるべきである。

操作

選択:

1299 **FPT_TST.1.1** 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。

1300 **FPT_TST.1.1** において、PP/ST 作成者は、自己テストが、すべての TSF、あるいは TSF の指定された一部の正しい操作を実証するために行われるかどうか特定するべきである。

割付:

1301 **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。

1302 **FPT_TST.1.1** において、PP/ST 作成者は、選択されている場合、TSF 自己テストが必要となる、TSF の部分のリストを特定するべきである。

選択:

1303 **FPT_TST.1.2** において、PP/ST 作成者は、データの完全性の検証が、すべての TSF データか、あるいは選択されたデータに対してのみか、特定するべきである。

割付:

1304 **FPT_TST.1.2** において、PP/ST 作成者は、選択されている場合、完全性を検証する TSF データのリストを特定するべきである。

選択:

1305 **FPT_TST.1.3** において、PP/ST 作成者は、TSF の完全性の検証が、すべての TSF か、あるいは選択された TSF に対してのみか、特定するべきである。

割付:

1306 **FPT_TST.1.3** において、PP/ST 作成者は、選択されている場合、完全性を検証する TSF のリストを特定するべきである。

附属書K　クラス FRU: 資源利用
(規定)

1307 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 3 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り当てられ、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。

1308 図 29 は、このクラスのコンポーネント構成を示す。

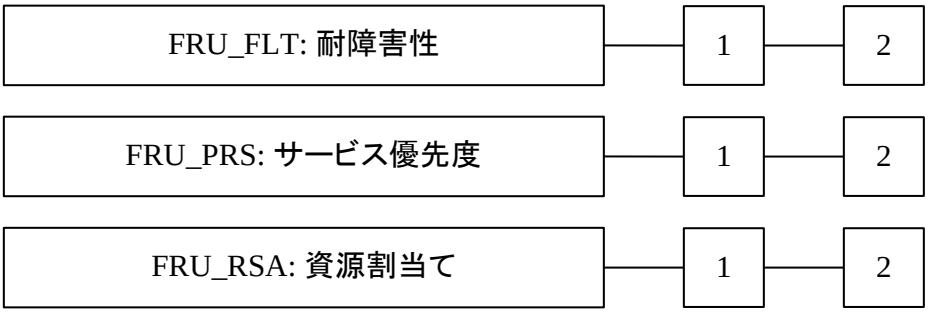


図 29　FRU: 資源利用クラスのコンポーネント構成

K.1　耐障害性(FRU_FLT)

利用者のための注釈

1309 このファミリは、障害の発生時でも機能を利用可能にする要件を規定する。このような障害の例には、停電、ハードウェアの障害、またはソフトウェア誤りなどがある。このような誤りの発生時に、指定されている場合には、TOE は指定された機能を維持する。例えば、PP/ST 作成者は、原子力発電所で使用される TOE が、停電または通信障害が発生した場合に、停止手順の動作を継続することを特定できる。

1310 TOE は、もし SFR 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、システムは障害の後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 セキュアな状態を保持する障害によって提供される。

1311 耐障害性を提供するメカニズムは、能動的または受動的にすることができる。能動的なメカニズムの場合、誤りの発生時にアクティブになる特定の機能が用意される。例えば、火災警報は能動的なメカニズムである。TSF は火災を検出し、バックアップへの動作の切り替えなどの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することができる。例えば、複数プロセッサによる多数決方式の使用は、受動的なソリューションである。1 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、訂正を可能にするために、検出されることは必要である)。

1312 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

1313　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:

1314　**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。

1315　**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

1316　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:

1317　**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)

利用者のための注釈

1318　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干渉や遅延を受けることなく、TSF の制御下にある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 TSF の制御下にある資源利用を TSF が管理することを認める。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。

1319　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。

1320 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、2 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。

1321 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

1322 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:

1323 **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、ディスク領域、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

1324 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。TSF 制御下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 TSF 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)

利用者のための注釈

1325 このファミリの要件は、利用者やサブジェクトによる TSF 制御下の資源の使用を 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。

1326 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:

- 特定の利用者が割り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。

1327 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。

1328 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り当てられる(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。

1329 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用する。

FRU_RSA.1 最大割当て

利用者のための適用上の注釈

1330 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用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:

1331 **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、ディスク領域、メモリ、帯域幅)。もし TSF 制御下のすべての資源が含まれる必要があれば、「すべての TSF 資源」という語を特定することができる。

選択:

1332 **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。

1333 **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

1334 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:

1335 **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を特定すべきである(例えば、プロセス、ディスク領域、メモリ、帯域幅)。もし TSF 制御下のすべての資源が含まれる必要があれば、「すべての TSF 資源」という語を特定することができる。

選択:

1336 **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。

1337 **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:

1338 **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、ディスク領域、メモリ、帯域幅)。もし TSF 制御下のすべての資源が含まれる必要があれば、「すべての TSF 資源」という語を特定することができる。

選択:

1339 **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。

1340 **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　クラス FTA: TOE アクセス
（規定）

1341　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1 つまたは複数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。

1342　利用者セションは、識別/認証の時点、あるいは、もしさらに適切であれば、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。

1343　図 30 は、このクラスのコンポーネント構成を示す。

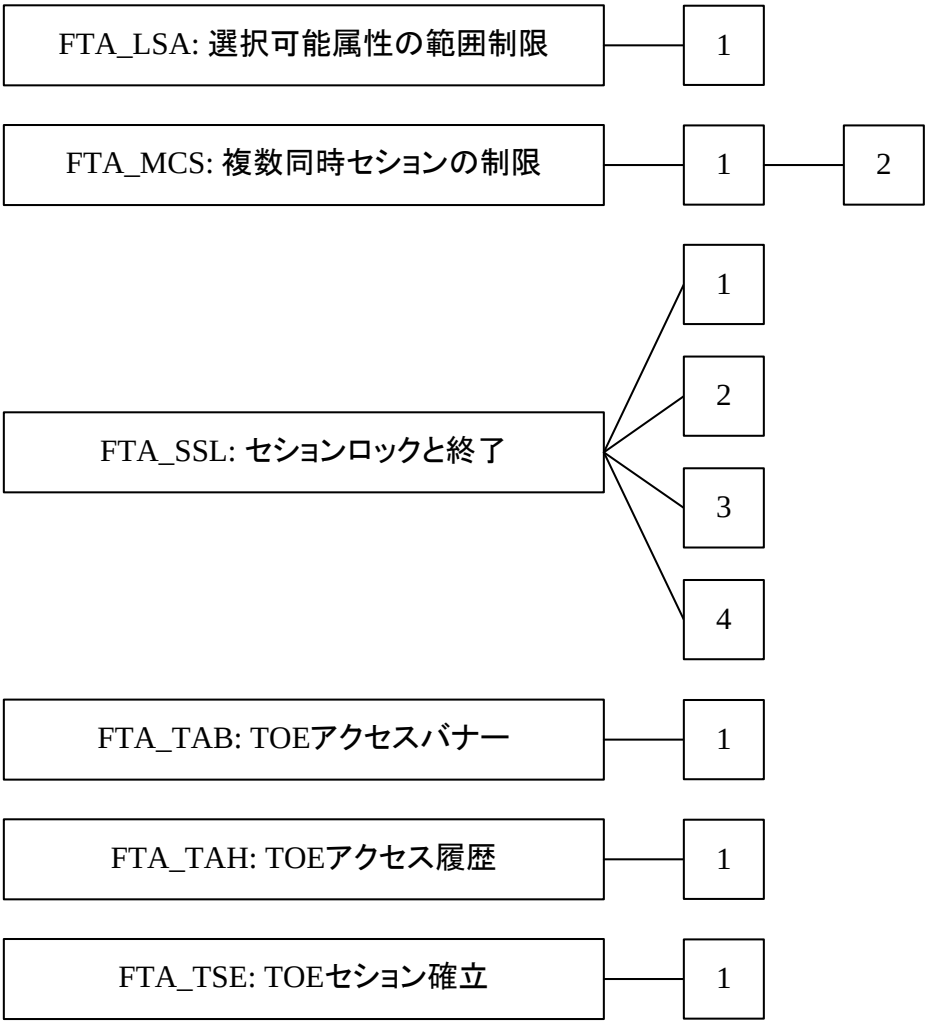


図 30　FTA: TOE アクセスクラスのコンポーネント構成

L.1 選択可能属性の範囲制限(FTA_LSA)

利用者のための注釈

1344 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)。

1345 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「非秘密セション」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1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:

1346 **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、完全性レベル、役割である。

1347 **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)

利用者のための注釈

1348 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

1349 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:

1350 **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属性ごと制限

利用者のための適用上の注釈

1351 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 複数同時セションの基本制限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:

1352 **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。

1353 **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 セションロックと終了(FTA_SSL)

利用者のための注釈

1354 このファミリは、TSF に、対話セションの TSF 起動、利用者起動のロック、及びロック解除、終了の能力を提供するための要件を定義する。

1355 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、特定された非アクティブである期間後に TSF が端末を無効(ロック)にしあるいはセションを終了するための、及び、利用者が端末の無効(ロック)を開始あるいはセションを終了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。

1356 利用者は、もしある特定の時間、TOE に何も刺激を与えなかったとすると、非アクティブとみなされる。

1357 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 高信頼パス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

1358 FTA_SSL.1 TSF 起動セションロックは、TSF が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。

1359 表示装置が上書きされる場合、置換コンテンツは静的である必要はない(つまり、「スクリーンセーバー」は許可される)。

1360 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:

1361 **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。

1362 **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には、「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」などがある。

FTA_SSL.2 利用者起動ロック

利用者のための適用上の注釈

1363 FTA_SSL.2 利用者起動ロックは、許可利用者が彼/彼女自身の対話セション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。

1364 装置が上書きされる場合、置換コンテンツは静的である必要はない(つまり、「スクリーンセーバー」は許可される)。

操作

割付:

1365 **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には、「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」などがある。

FTA_SSL.3 TSF 起動による終了

利用者のための適用上の注釈

1366 FTA_SSL.3 TSF 起動による終了は、非アクティブである期間後、TSF が対話利用者セションを終了させることを要求する。

1367 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:

1368 **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。

FTA_SSL.4 利用者起動による終了

利用者のための適用上の注釈

1369 FTA_SSL.4 利用者起動の終了は、許可利用者に対し、対話セションを終了する能力を与える。

1370 PP/ST の作成者は、セションは利用者がアクティビティを終了した後も、例えばバックグランド処理のように続くかもしれないことに、留意すべきである。この要件は、利用者にこのバックグランドサブジェクトを、サブジェクトの状態によらず終了することを許すだろう。

L.4 TOE アクセスバナー(FTA_TAB)

利用者のための注釈

1371 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

利用者のための適用上の注釈

1372 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)

利用者のための注釈

1373 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

利用者のための適用上の注釈

1374 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。

1375 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:

1376 **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。項目には、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)がある。

1377 **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、最後の失敗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。項目には、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)がある。

L.6 TOE セション確立(FTA_TSE)

利用者のための注釈

1378 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。

1379 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;
- 利用者の完全性レベル;
- 利用者の役割における資格。

1380 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:

1381 **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　クラス FTP: 高信頼パス/チャネル（規定）

1382　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 と他の高信頼 IT 製品間のセキュアな通信に対する 1 つのアプローチである。

1383　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。

1384　図 31 は、このクラスのコンポーネント構成を示す。

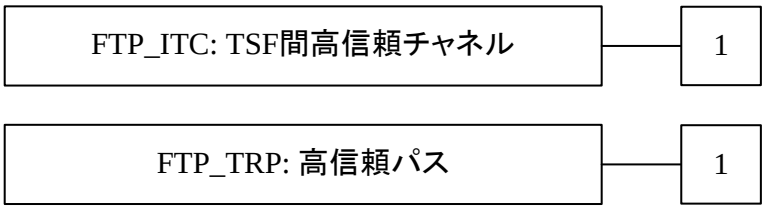


図 31　FTP: 高信頼パス/チャネルクラスのコンポーネント構成

M.1　TSF 間高信頼チャネル(FTP_ITC)

利用者のための注釈

1385　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

1386　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:

1387 **FTP_ITC.1.2** において、PP/ST 作成者は、ローカル TSF、他の高信頼 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:

1388 **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)

利用者のための注釈

1389 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。

FTP_TRP.1 高信頼パス

利用者のための適用上の注釈

1390 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:

1391 **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。

1392 **FTP_TRP.1.1** において、PP/ST の作成者は、高信頼パスが、改ざん、公開、そして/また、他のタイプの完全性、機密性侵害から、データを保護しなければならないかどうかを特定すべきである。

割付:

1393 **FTP_TRP.1.1** において、もし選択されれば、PP/ST の作成者は、高信頼パスがデータを保護しなければならない、その他のタイプの完全性や機密性侵害を識別すべきである。

選択:

1394 **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。

1395 **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:

1396 **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。