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

2022 年 11 月

CC:2022
改訂第 1 版

CCMB-2022-11-002

令和 5 年 9 月 翻訳第 1.0 版
独立行政法人情報処理推進機構
セキュリティセンター
セキュリティ技術評価部

目次

IPA まえがき

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 CC:2022 Revision 1

November 2022 CCMB-2022-11-002

まえがき

本バージョンは、2017 年に CC v3.1 改訂第 5 版として発行されて以来、最初の大幅改訂となる「情報技術セキュリティ評価のためのコモンクライテリア」（CC:2022）である。

歴史的に、CC 標準は共通評価方法（CEM）とともに、IT セキュリティ分野におけるコモンクライテリア認証書の承認に関する協定（CCRA）の参加国によって開発・維持され、その後、ISO（国際標準化機構）及び IEC（国際電気標準会議）が維持する標準として公表されてきた。しかし、CC:2022 と CEM:2022 は、まず ISO/IEC 標準として開発され、その後、CCRA により CC と CEM の新バージョンとして発行されたものである。CC:2022 の ISO 版は ISO/IEC 15408-1:2022～15408-5:2022 として 5 パートで発行され、CEM:2022 の ISO 版は ISO/IEC 18045:2022 として 1 パートで発行されている。

CC:2022 は、以下のパートから構成されている。

— 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

— パート4（新規）：評価方法及び評価アクティビティの仕様のための枠組み

— パート5（新規）：セキュリティ要件の定義済みパッケージ

CC:2022 は、CC v3.1 が発行されて以来用いられてきた標準の新しい使用方法を、正式に規定することを目的としている。CC v3.1 が発行されて以来、新しい保証パラダイムが開発され、附属書や補遺として標準に追加されてきた。これには、評価が適合主張の範囲を超えることを禁止する完全適合の概念や、個々のセキュリティ機能を評価するために、評価アクティビティを使用して、機能に特化した保証や客観性のあるガイドラインを提供するという概念が含まれる。また、標準の前回の大幅な改訂以降、重要性が増した機能要件の形式化も含まれている。CC:2022 の発行は、これらの開発を標準そのものに完全に統合する。

CC:2022 には、新しい ISO/IEC 15408:2022 標準の編集中に提供されたパート 4 とパート 5 が CC の新しいオリジナルパートとして含まれていることを強調する価値がある。これらは、旧版 CC v3.1 R5 を大幅に強化する。パート 5 は、CC v.3.1 改訂第 5 版のパート 3 の関連する節に基づいている。

CC:2022 は、次のような具体的な変更点を取り入れている。

— 文書が再構成され、新たなパートが追加された。

  — パート4：評価方法及び評価アクティビティの仕様の方法を定義している。

  — パート5：事前に定義された保証パッケージを列挙したもので、このバージョンで新たに導入されたものもある。

— 以下の技術的な変更が導入された。

  — 用語が見直され、更新された。

— 新しい機能要件及び新しい保証要件が導入された。

— 完全適合の種別が導入された。

— 低保証のプロテクションプロファイル(PP)が削除され、直接根拠PPが導入された。

— マルチ保証評価が導入された。

— 保証の統合が導入された。

CCの全てのパートはCommon Criteria Portal (www.commoncriteriaportal.org)で見ることができる。

本書で使用されている商標は、利用者の便宜を図るための参考情報であり、推奨を意味するものではない。

法定通知

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は、以下に示す政府機関が貢献した。ISO/IEC とともに、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 2022 パート 1 からパート 5（「CC:2022」と呼ぶ）の著作権の共同保有者として、これらの政府機関はここに、ISO/IEC 15408 及びその派生版（それらの国での採用を含む）の改訂版において ISO/IEC に CC:2022 を複製する非排他的許可を与える。ただし、CC:2022 を適切な方法で使用、複製、配布、翻訳、変更する権利は、これらの政府機関が保有する。ISO/IEC はその見返りとして、前述の政府機関に対し、成果物である CC:2022 パート 1 からパート 5 を、彼らが適切と考えるライセンスで使用することを許可する。前述の政府機関は、文書の一部分の修正や再利用を含め、文書の利用者がテキストを再利用することを常に支援しており、今後もこの方針に従う予定である。

オーストラリア	The Australian Signals Directorate
カナダ	Communications Security Establishment
フランス	Agence Nationale de la Sécurité des Systèmes d'Information
ドイツ	Bundesamt für 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
ニュージーランド	Government Communications Security Bureau
韓国	National Security Research Institute
スペイン	Ministerio de Asuntos Económicos y Transformación Digital and Centro Criptológico Nacional
スウェーデン	FMV, Swedish Defence Materiel Administration
英国	National Cyber Security Centre
米国	The National Security Agency and the National Institute of Standards and Technology

序説

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)、PPモジュール、機能パッケージ又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(SFR)又はコンポーネント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、PPモジュール、機能パッケージ又は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、又は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。

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を取り扱うことを目的とするSFRを表すことを可能にする。

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5.2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、以下のようにこの文書を利用する。

a) 消費者は、PP、PPモジュール、機能パッケージ又は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又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、これらの要件に適合する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。

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、PPモジュール、機能パッケージ又は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、及び全ての依存性が考慮され、満たされていることを検証する。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る。

注：この文書では、用語を他のテキストと区別するために、ボールドやイタリック体を使用している場合がある。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。この表記では、全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又は変更されたとき、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又は拡張操作も、ボールドで強調表示される。

イタリック体の使用は、正確な意味を持つテキストであることを示す。セキュリティ保証要件では、この表記は評価に関連する特別な動詞に使用される。

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

1　適用範囲

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。

2 規定の参照

本文中では、以下の文書を、その内容の一部又は全部が本書の要件となるように参照している。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。

情報技術セキュリティ評価のためのコモンクライテリア、CC:2022、改訂第1版、2022年11月 — パート1: 概説と一般モデル

情報技術セキュリティ評価のためのコモンクライテリア、CC:2022、改訂第1版、2022年11月 — パート3: セキュリティ保証コンポーネント

情報技術セキュリティ評価のための共通方法、CEM:2022、改訂第1版、2022年11月 — 評価方法

3 用語と定義

本文書の目的のために、CCパート1、CCパート3、CEM及び以下で使用された用語、定義、及び略語を適用する。

ISO 及び IEC は、標準化で使用するための用語データベースを次のアドレスで管理している。

— ISO Online browsing platform: https://www.iso.org/obp

— IEC Electropedia: https://www.electropedia.org/

3.1
識別情報(identity)
評価対象(TOE)の文脈において、エンティティを一意に識別する表現。

例：そのような表現の例は文字列である。

注1：エンティティは、利用者、プロセス、又はディスクなど多様である。人間の利用者に対して、フルネーム又は略称、又は一意の仮名で表現することが出来る。

注2：エンティティは複数の識別情報を持つことができる。

3.2
TSF間転送(inter TSF transfer)
評価対象(TOE)と他の高信頼IT製品のセキュリティ機能性との間で通信すること。

3.3
内部通信チャネル(internal communication channel)
評価対象(TOE)内部の別々の部分間の通信チャネル。

3.4
TOE内転送(internal TOE transfer)
評価対象(TOE)内部の別々の部分間でデータを通信すること。

3.5
操作(operation)
(CCパート2のコンポーネントでの)
割付、繰返し、詳細化、又は選択により、コンポーネントを改変又は繰り返すこと。

3.6
秘密(secret)
特定の*セキュリティ機能方針(SFP)*(3.8)を実施するため、許可された利用者、及び/又はTOEセキュリティ機能性(TSF)にしか知らせてはならない情報。

3.7
セキュアな状態(secure state)
TOEセキュリティ機能性(TSF)データに一貫性があり、TSFがセキュリティ機能要件(SFR)の正しい実施を継続している状態。

3.8
セキュリティ機能方針(security function policy)
SFP
TOEセキュリティ機能性(TSF)によって実施され、セキュリティ機能要件(SFR)のセットとして表現できる特定のセキュリティのふるまいを記述する規則のセット。

3.9
TOE資源(TOE resource)
評価対象(TOE)内において使用可能又は消費可能なもの。

3.10
TOE範囲外転送(transfer outside of the TOE)
評価対象(TOE)セキュリティ機能性(TSF)の制御下にないエンティティに対してTSFが仲介するデータの通信。

3.11
高信頼チャネル(trusted channel)
評価対象(TOE)セキュリティ機能性(TSF)と他の高信頼IT製品が、必要な信頼をもって通信することができる手段。

3.12
高信頼パス(trusted path)
利用者と評価対象(TOE)セキュリティ機能性(TSF)が必要な信頼をもって通信する手段。

注1：通信とは、通常、双方の識別と認証の確立、及び整合性が保護された利用者固有のセションの概念を意味する。

注2：外部エンティティが高信頼IT製品である場合、高信頼パスではなく*高信頼チャネル*(3.11)の概念を用いる。

注3：セキュアな通信の物理的側面と論理的な面の両方を、信頼を得るためのメカニズムと考えることができる。

3.13
TSFデータ(TSF data)
セキュリティ機能要件(SFR)実施が依存する評価対象(TOE)の動作[i]のためのデータ。

3.14
利用者データ(user data)
評価対象(TOE)が受信又は生成したデータで、外部のエンティティにとって意味を持つものの、TOEセキュリティ機能性(TSF)の動作[ii]に影響を与えないもの。

注1：この定義は、概念にもよるが、利用者が作成しTSFの動作に実際に影響を及ぼすデータも同様に*TSFデータ*(3.13)とみなすことを前提としている。

4 略語

API	アプリケーションプログラミングインタフェース (application programming interface)
CD	コンパクトディスク (compact disk)
DAC	任意アクセス制御 (discretionary access control)
DRBG	決定論的ランダムビット生成器 (deterministic random bit generator)
EMS	電磁スペクトル (electromagnetic spectrum)
GB	ギガバイト (gigabyte)
GHz	ギガヘルツ (gigahertz)
GUI	グラフィカルユーザインタフェース (graphical user interface)
HSM	ハードウェアセキュリティモジュール (hardware security module)
HTTPS	ハイパーテキストトランスファープロトコルセキュア (hypertext transfer protocol secure)
IOCTL	入出力制御 (input output control)
IP	インターネットプロトコル (internet protocol)
IPsec	IPセキュリティ (IP security (protocol))
LDAP	ライトウェイトディレクトリアクセスプロトコル (lightweight directory access protocol)
MAC	強制アクセス制御 (mandatory access control)
MB	メガバイト (megabyte)
MBps	メガバイト毎秒 (megabytes per second)
OS	オペレーティングシステム (operating system)
OTP	ワンタイムプログラマブル (one-time programmable)
PC	パーソナルコンピュータ (personal computer)
PCI	周辺コンポーネント相互接続 (peripheral component interconnect)
PKI	公開鍵基盤 (public key infrastructure)
PP	プロテクションプロファイル (protection profile)
RAM	ランダムアクセスメモリ (random access memory)
RBG	ランダムビット生成器 (random bit generator)
RNG	乱数生成器 (random number generator)
RPC	リモートプロシージャコール (remote procedure call)
SFP	セキュリティ機能方針 (security function policy)
SFR	セキュリティ機能要件 (security functional requirement)
SSH	セキュアシェル (secure shell)

ST	セキュリティターゲット (security target)
TCP	伝送制御プロトコル (transmission control protocol)
TLS	トランスポートレイヤーセキュリティ (transport layer security)
TOE	評価対象 (target of evaluation)
TSF	TOEセキュリティ機能性 (TOE security functionality)
TSFI	TSFインタフェース (TSF interface)
USB	ユニバーサルシリアルバス (universal serial bus)
VPN	仮想プライベートネットワーク (virtual private network)

5 概要

5.1 一般

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(SFR)は、ITセキュリティの全ての問題に対する最終的な回答ではない。この文書は、市場のニーズを反映した高信頼製品を指定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コンポーネントのセットを提供する。これらのセキュリティ機能コンポーネントは、セキュリティ要件の指定の最新段階のものとして表される。

この文書には、全ての可能なセキュリティ機能コンポーネントが含まれているわけではないが、この文書の提供者が価値を認識し、合意したセキュリティ機能コンポーネントが含まれている。

消費者の理解のしかたとニーズは変化するかもしれないので、CCのこのパートの機能コンポーネントは保守されていく必要があろう。PP、PPモジュール、機能パッケージ及びSTの作成者によっては、この文書の機能コンポーネントがカバーしていないセキュリティニーズを持っていると思われる。そのような場合、PP、PPモジュール、機能パッケージ及びSTの作成者は、この文書から取り出したものでない機能コンポーネント及び要件の使用を考慮することが許されている。拡張性の概念については、CCパート1の8.4で説明する。

5.2 本書の構成

5節では、この文書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。

7章では、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。

附属書Aは、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。

附属書Bは、機能コンポーネントの依存性の完全な相互参照表を提供する。

附属書C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、適切な監査又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なければならない。異なる選択肢が付与される箇所では、選択は、PP、PPモジュール、機能パッケージ及びSTの作成者に委ねられる。

PP、PPモジュール、機能パッケージ及びSTの作成者は、適切な構造、規則、及びガイダンスとしてパート1を参照しなければならない、特に:

a) パート1の3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7節では、セキュリティ機能コンポーネントを用いてSFRを指定する方法について説明している。

c) パート1の8節では、セキュリティ機能コンポーネントの構成方法と適用可能な操作について説明している。

d) パート1の附属書Aでは、セキュリティ機能パッケージの構造に関する更なる情報を提供している。

e) パート1の附属書Bでは、PPの構造に関する更なる情報を提供している。

f) パート1の附属書Cでは、PPモジュール及びPP構成の構造に関する更なる情報を提供している。

g) パート1の附属書Dでは、STの構造に関する更なる情報を提供している。

6 機能要件のパラダイム

この節では、この文書のセキュリティ機能コンポーネント及びSFRの導出で使用するパラダイムについて記述する。

この文書は、TOEを説明するSFRの仕様に対して使用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評価は、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。

SFRには、TOEが実施する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SFPは、サブジェクト、オブジェクト、資源又は情報、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する。全てのSFPはTOEセキュリティ機能性(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。

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TSFと呼ぶ。TSFは、セキュリティの実施のために直接的又は間接的に依存するTOEの全てのハードウェア、ソフトウェア、及びファームウェアから構成される。

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。又は、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。

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。

TOEインタフェースは、特定のTOEに範囲を限定するか、又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、又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、又はその方針の特性が不明であるため、TOE範囲外転送と呼ばれる。

対話型(マンマシンインタフェース)又はプログラム型(アプリケーションプログラミングインタフェース(API))のいずれであっても、TSF仲介資源へのアクセス又は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。

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。

例1

TOE装置の一例として、ワークステーションがある。

利用者とTSF間の対話の期間は、利用者セションと呼ばれる。利用者セションの確立は各種の考慮事項に基づいて制御できる。

例2

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、又は合計)。

この文書では、利用者が操作を行うために必要な権利及び/又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又は操作のセットを実行できることを示す。

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3

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。

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。

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全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又は情報の格納先となるコンテナである。

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

   例4：UNIXプロセス。

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

例5：クライアント/サーバアーキテクチャに見られるような機能。

c) TOE自体の一部として動作するサブジェクト

例6：利用者の代わりに動作しないプロセス。

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。

情報を格納し、又は受け取り、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。

例7：サブジェクトの例として、プロセス間通信が挙げられる。

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。

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、又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。

TOEのデータは、利用者データ又は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。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。

例8

利用者データ：

— 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：

— 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、又は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。

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管理する規則のセットで使用される。

情報フロー制御SFPを実装するメカニズムは、制御の範囲内のサブジェクトと情報の属性、及び情報に対するサブジェクトの操作を管理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、又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。

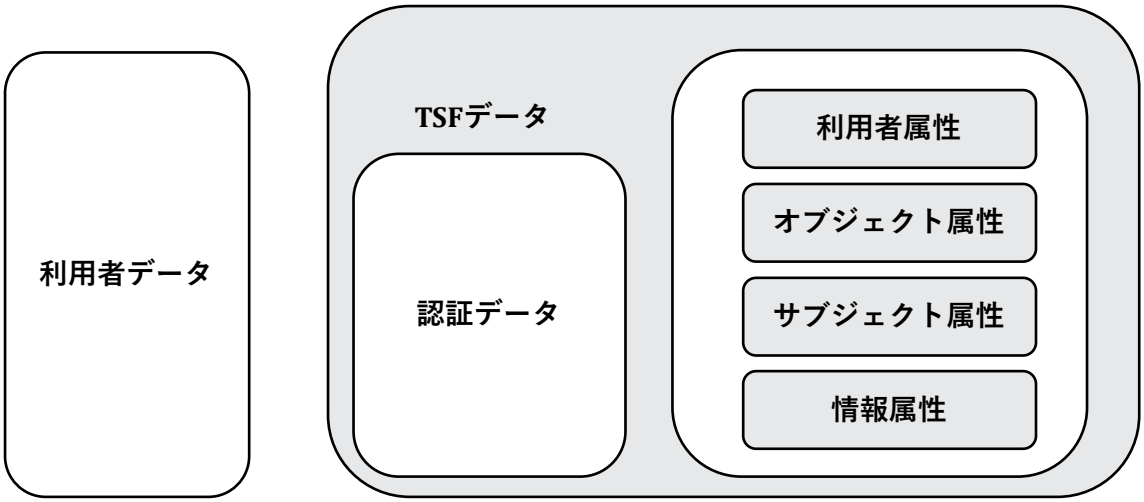


図 1 — 利用者データと TSF データとの関係

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。

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、認証データの全ての形式を秘密に保持する必要はない。生体認証装置の場合は、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。

例9

生体認証装置の例としては指紋読取装置及び網膜スキャナが含まれる

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。

そこで、全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、全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の区分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。

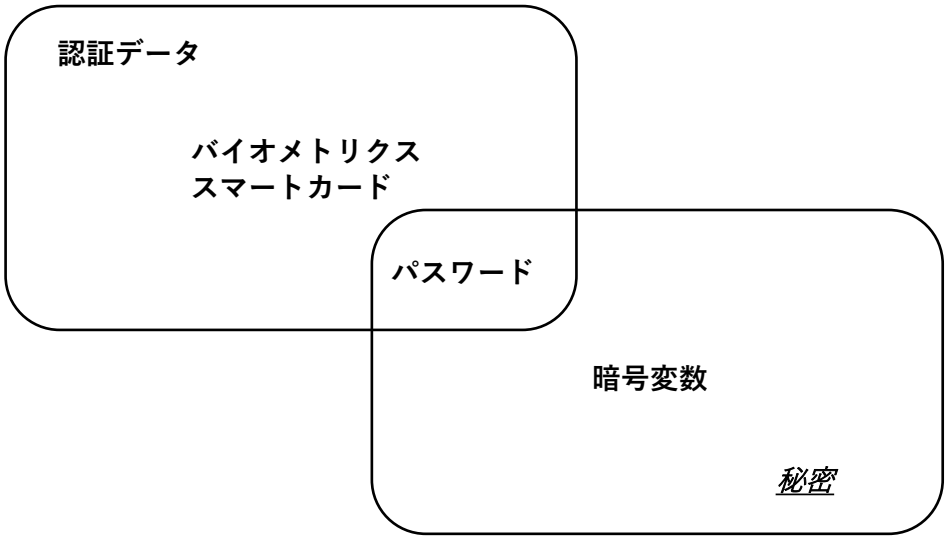


図 2 — 「認証データ」と「秘密」との関係

7 セキュリティ機能コンポーネント

7.1概要

7.1.1 一般

この章では、この文書の機能要件の内容と表現を定義し、PP、PPモジュール、機能パッケージ又はSTに含まれる新しい拡張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。CCパート1の8節にあるように、機能要件は、クラス、ファミリ、コンポーネント及びエレメントで表される。

7.1.2 クラスの構造

7.1.2.1 一般

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。

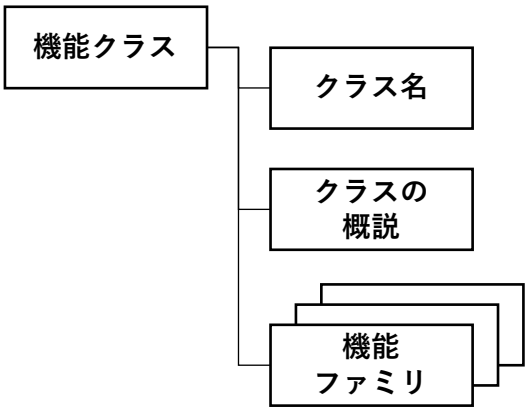


図 3 — 機能クラス構造

注：機能クラスには、1つ以上の機能ファミリが含まれる。

7.1.2.2 クラス名

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。

7.1.2.3 クラスの概説

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又は方法を表す。機能クラスの定義では、要件の指定における形式的な分類方法は反映されない。

クラスの概説には、7.2に説明するように、このクラスのファミリと各ファミリのコンポーネントの階層を記述した図が用意されている。

7.1.3 ファミリ構造

7.1.3.1 一般

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。

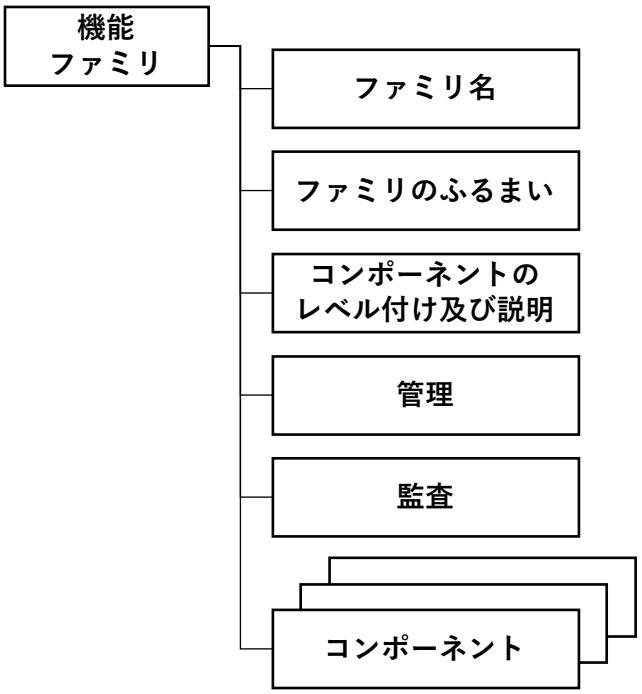


図 4 — 機能ファミリ構造

7.1.3.2 ファミリ名

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、セキュリティコンポーネントの主な参照名を提供する。

7.1.3.3 ファミリのふるまい

ファミリのふるまいの節は、機能ファミリについての叙述的記述を提供するものであり、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から派生したSFR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全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ST、PP、PPモジュール及びセキュリティ機能パッケージの作成者に向けられたものである。

7.1.3.4 コンポーネントのレベル付け及び説明

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ST、PP、PPモジュール及びセキュリティ機能パッケージに含めることができる。コンポーネントのレベル付け及び説明の節の目的は、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。

機能ファミリは使用可能なコンポーネントとこれらの論理的根拠を記述している。コンポーネントの詳細は、各コンポーネントの中に含まれる。

機能ファミリ内でのコンポーネント間の関係は、階層関係になっていることもある。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。

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。

7.1.3.5 管理

管理の節には、ST、PP、PPモジュール及びセキュリティ機能パッケージ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。その節は、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。

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。

7.1.3.6 監査

監査要件の節には、FAUクラスからの要件がST、PP、PPモジュール及びセキュリティ機能パッケージに含まれる場合、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。

監査対象事象の分類は、階層的であることがわかる。

例1

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。

例2

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全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、PPモジュール、機能パッケージ又はSTに含まれる。詳細監査生成が必要な場合は、全ての識別された監査対象事象(「最小」、「基本」及び「詳細」)はPP、PPモジュール、機能パッケージ又はSTに含まれる。

FAUクラスでは、監査に関する規則がさらに詳細に説明されている。

7.1.4 コンポーネント構造

7.1.4.1 一般

図5は、機能コンポーネント構造を示している。

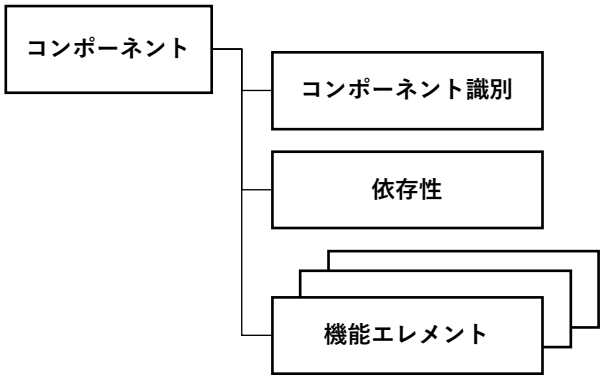


図 5 — 機能コンポーネント構造

7.1.4.2 コンポーネント識別情報

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:

— *一意の名前*。コンポーネントの目的を表す名前。

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

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

7.1.4.3 機能エレメント

エレメントのセットが各コンポーネントに提供される。各エレメントは、個別に定義され、自己完結する。

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つだけ又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、PPモジュール、セキュリティ機能パッケージ又はSTに含めなければならない。

機能エレメント名の一意の短い形式が提供される。

例

エレメント名FDP_IFF.4.2の読み方は以下のとおり。

— 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

7.1.5 依存性

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

各機能コンポーネントは、他の機能コンポーネント及び保証コンポーネントへの依存の完全なリストを提供する。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。このコンポーネントのリストは直接的な依存を提供する、つまり、それは、このコンポーネントがジョブを適切に実行するのに必要となる機能コンポーネントへの単なる参照である。間接的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B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コンポーネントの中から、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、それぞれの機能コンポーネントが、依存性を満たすのに十分である。

例：FDP_UIT.1 データ交換完全性

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又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。

この文書で示されている依存関係は規範的であり、パッケージ、PP又はST内で満たされなければならない。示された依存関係が適用できない状況では、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パッケージ、PP又は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

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。

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、関連する機能又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6は、コンポーネント間に存在する階層関係を見るのに便利である。

機能コンポーネントの記述において、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。

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。

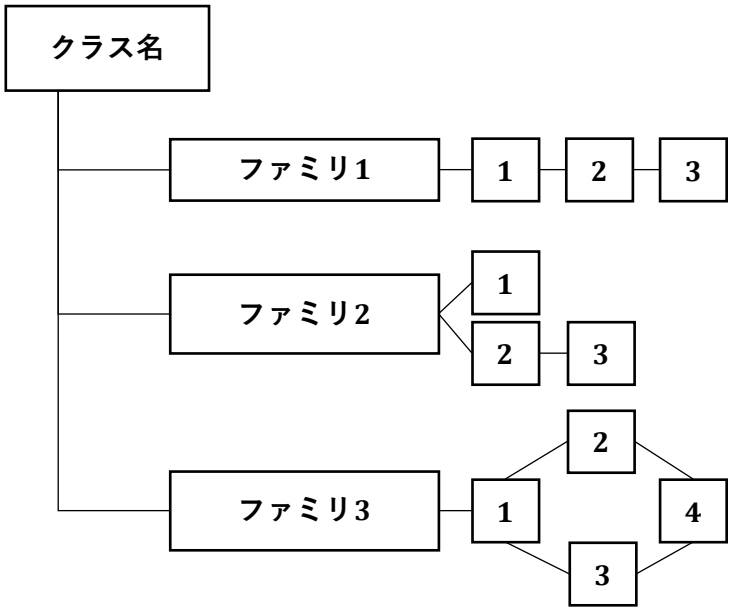


図 6 — サンプルクラスの構成図

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

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

これらの図は、ファミリの文章を補足し、関係の識別を容易にするためのものである。それらは、各コンポーネントにおける階層関係の必須の要求事項である各コンポーネントの「依存性：」の注釈に置き換わるものではない。

8 FAUクラス: セキュリティ監査

8.1クラスの説明

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決定するために検査され得るものである。

図7は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Cは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

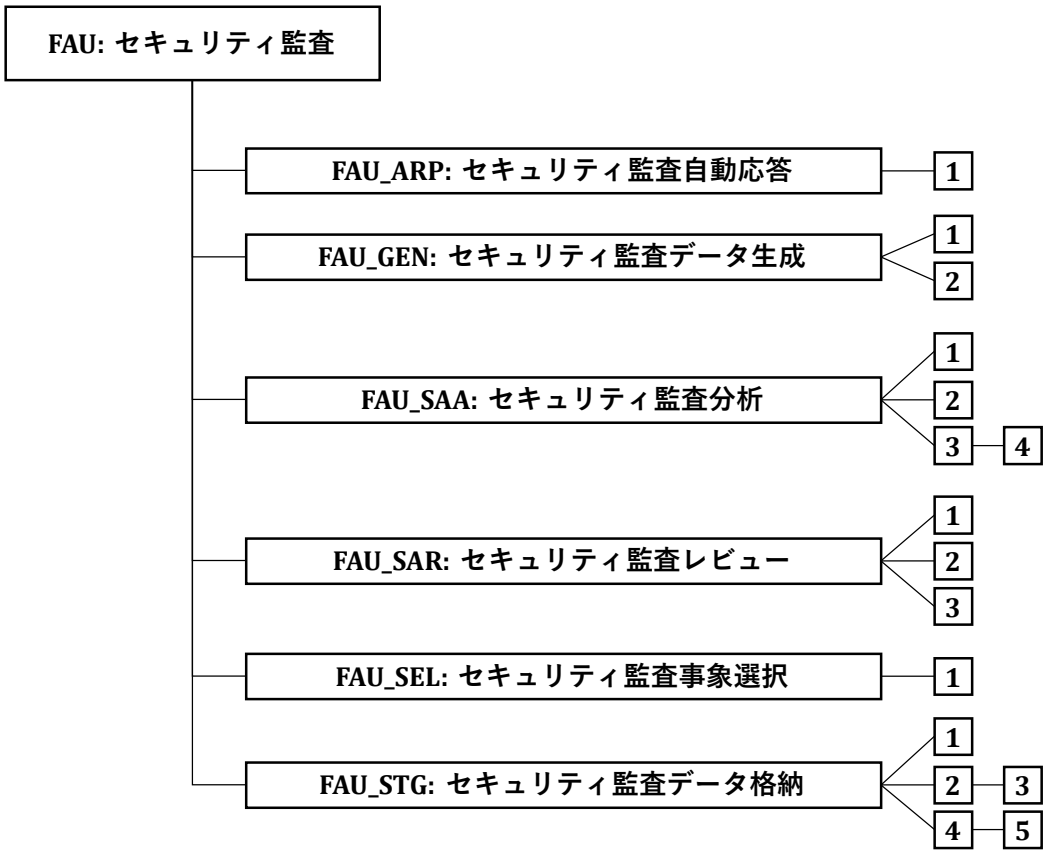


図 7 — FAU: セキュリティ監査クラスの構成

8.2セキュリティ監査自動応答(FAU_ARP)

8.2.1 ファミリのふるまい

このファミリは、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。

8.2.2 コンポーネントのレベル付け及び説明

図8に、本ファミリのコンポーネントのレベル付けを示す。

図 8 — FAU_ARP: コンポーネントのレベル付け

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

8.2.3 FAU_ARP.1の管理

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)。

8.2.4 FAU_ARP.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

8.2.5 FAU_ARP.1 セキュリティアラーム

コンポーネント間の関係

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。

8.3 セキュリティ監査データ生成(FAU_GEN)

8.3.1 ファミリのふるまい

このファミリは、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。

8.3.2 コンポーネントのレベル付け及び説明

図9に、本ファミリのコンポーネントのレベル付けを示す。

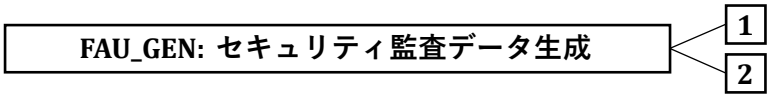


図 9 — FAU_GEN: コンポーネントのレベル付け

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

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

8.3.3 FAU_GEN.1、FAU_GEN.2の管理

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) 予見される管理アクティビティはない。

8.3.4 FAU_GEN.1、FAU_GEN.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

8.3.5 FAU_GEN.1 監査データ生成

コンポーネント間の関係

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データ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*]レベルの全ての監査対象事象。

c) [割付: *その他の個別に定義した監査対象事象*]。

FAU_GEN.1.2

TSFは、各監査データ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) 監査対象事象の日付・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(成功又は失敗)。

b) 各監査対象事象種別に対して、PP、PPモジュール、機能パッケージ又はSTに含まれる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*]。

8.3.6 FAU_GEN.2 利用者識別情報の関連付け

コンポーネント間の関係

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。

8.4 セキュリティ監査分析(FAU_SAA)

8.4.1 ファミリのふるまい

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、侵入検知や、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。

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。

8.4.2 コンポーネントのレベル付け及び説明

図10に、本ファミリのコンポーネントのレベル付けを示す。

図 10 — FAU_SAA: コンポーネントのレベル付け

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

FAU_SAA.2 プロファイル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、プロファイルの対象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。プロファイルの対象グループは、TSFと対話する一人又は複数の個人のグループに対応する。プロファイルの対象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、あるいは収集後のバッチモード分析で実行される。

FAU_SAA.3 単純攻撃の発見において、TSFは、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収集後のバッチモード分析で行える。

FAU_SAA.4 複合攻撃の発見において、TSFは、多段階の侵入シナリオを表現し、かつ検出できなければならない。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ことが知られている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。

8.4.3 FAU_SAA.1の管理

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。

8.4.4 FAU_SAA.2の管理

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) プロファイルの対象グループにおける利用者グループの維持(削除、改変、追加)。

8.4.5 FAU_SAA.3の管理

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)。

8.4.6 FAU_SAA.4の管理

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)。

8.4.7 FAU_SAA.1、FAU_SAA.2、FAU_SAA.3、FAU_SAA.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 全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。

8.4.8 FAU_SAA.1 侵害の可能性の分析

コンポーネント間の関係

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*]の累積、あるいは組み合わせたもの。

b) [割付: *その他の規則*]。

8.4.9 FAU_SAA.2 プロファイルに基づく異常検出

コンポーネント間の関係

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: *プロファイルの対象グループ*]のメンバ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、そのアクティビティ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なければならない。ここで疑惑率とは、利用者の現在のアクティビティが、プロファイル中に表現された確立された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: *異常なアクティビティがTSFにより報告される条件*]

8.4.10 FAU_SAA.3 単純攻撃の発見

コンポーネント間の関係

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次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。

8.4.11 FAU_SAA.4 複合攻撃の発見

コンポーネント間の関係

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、次のような**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**SFR実施の侵害を示している**可能性がある次のような**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.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**又は事象シーケンス**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。

8.5 セキュリティ監査レビュー(FAU_SAR)

8.5.1 ファミリのふるまい

このファミリは、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ツールのための要件を定義している。

8.5.2 コンポーネントのレベル付け及び説明

図11に、本ファミリのコンポーネントのレベル付けを示す。

図 11 — FAU_SAR: コンポーネントのレベル付け

FAU_SAR.1 監査レビューは、監査データからの情報読み出し能力を提供する。

FAU_SAR.2 限定監査レビューは、FAU_SAR.1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。

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。

8.5.3 FAU_SAR.1の管理

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)。

8.5.4 FAU_SAR.2、FAU_SAR.3の管理

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) 予見される管理アクティビティはない。

8.5.5 FAU_SAR.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

8.5.6 FAU_SAR.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

8.5.7 FAU_SAR.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

8.5.8 FAU_SAR.1 監査レビュー

コンポーネント間の関係

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*]を監査データ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、利用者がその情報を解釈するのに適した形式で監査データを提供しなければならない。

8.5.9 FAU_SAR.2 限定監査レビュー

コンポーネント間の関係

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、全ての利用者に監査データへの読み出しアクセスを禁止しなければならない。

8.5.10 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/又は並べ替え方法*]を適用する能力を提供しなければならない。

8.6 セキュリティ監査事象選択(FAU_SEL)

8.6.1 ファミリのふるまい

このファミリは、全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。

8.6.2 コンポーネントのレベル付け及び説明

図12に、本ファミリのコンポーネントのレベル付けを示す。

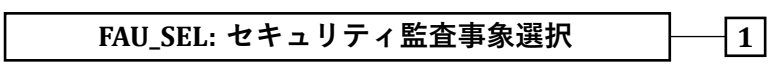


図 12 — FAU_SEL: コンポーネントのレベル付け

FAU_SEL.1 選択的監査は、PP、PPモジュール、機能パッケージ又はSTの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全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。

8.6.3 FAU_SEL.1の管理

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) 監査データを閲覧/改変する権限の維持。

8.6.4 FAU_SEL.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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、監査構成への全ての改変。

8.6.5 FAU_SEL.1 選択的監査

コンポーネント間の関係

下位階層：	なし
依存性：	FAU_GEN.1 監査データ作成 FMT_MTD.1 TSFデータ管理

FAU_SEL.1.1

TSFは以下のような属性に基づいて、全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*]。

8.7 セキュリティ監査データ格納(FAU_STG)

8.7.1 ファミリのふるまい

このファミリは、セキュアな監査証跡の生成及び維持を可能にするためのTSFの要件を定義している。格納された監査データとは、選択を通じて(一時記憶域に)読み出された監査データではなく、監査証跡内のデータを示す。

8.7.2 コンポーネントのレベル付け及び説明

図13に、本ファミリのコンポーネントのレベル付けを示す。

図13 — FAU_STG: コンポーネントのレベル付け

FAU_STG.1 監査データ格納場所は、監査データの格納場所を特定することを要求する。

FAU_STG.2 保護された監査データ格納は、監査データを保護することを要求する。監査証跡は、不当な削除及び/又は改変から保護されることになる。

FAU_STG.3 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。

FAU_STG.4 監査データ損失の恐れ発生時のアクションは、格納された監査データが閾値を超えたときにとられるアクションを特定する。

FAU_STG.5 監査データの損失防止は、監査データ格納が満杯になった場合に取るべきアクションを規定する。

8.7.3 FAU_STG.1の管理

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) 遠隔の監査データ格納場所の維持。

8.7.4 FAU_STG.2の管理

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) 予見される管理アクティビティはない。

8.7.5 FAU_STG.3の管理

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) 監査データ格納機能を制御するパラメタの維持。

8.7.6 FAU_STG.4の管理

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) 監査データ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)。

8.7.7 FAU_STG.5の管理

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) 監査データ格納失敗時にとられるアクションの維持(削除、改変、追加)。

8.7.8 FAU_STG.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 遠隔の監査データ格納場所の変更。

8.7.9 FAU_STG.2、FAU_STG.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

8.7.10 FAU_STG.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

8.7.11 FAU_STG.5の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 監査データ格納失敗によってとられるアクション。

8.7.12 FAU_STG.1 監査データ格納場所

コンポーネント間の関係

下位階層：	なし
依存性：	FAU_GEN.1 監査データ生成 FTP_ITC.1 TSF間高信頼チャネル

FAU_STG.1.1

TSFは、[選択: *TOE自身*、*外部のITエンティティ(FTP_ITCに従った高信頼チャネルを使用して生成された監査データを送信する)*、*[割付: その他の格納場所]*]に生成された監査データを格納できなければならない。

8.7.13 FAU_STG.2 保護された監査データ格納

コンポーネント間の関係

下位階層：	なし
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データ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データへの不正な改変を[選択: *防止*、*検出: から1つのみ選択*]できなければならない。

8.7.14 FAU_STG.3 監査データ可用性の保証

コンポーネント間の関係

下位階層：	FAU_STG.2 保護された監査データ格納
依存性：	FAU_GEN.1 監査データ生成

FAU_STG.3.1

TSFは、監査証跡に格納された監査データを不正な削除から保護しなければならない。

FAU_STG.3.2

TSFは、監査証跡に格納された監査データへの不正な改変を[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.3.3

TSFは、[選択: *監査データ格納の領域枯渇*、*失敗*、*攻撃*]という状況が生じた場合、[割付: *救済する監査データの数値尺度*]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。

8.7.15 FAU_STG.4 監査データ消失の恐れ発生時のアクション

コンポーネント間の関係

下位階層：	なし
依存性：	FAU_STG.2 保護された監査データ格納

FAU_STG.4.1

TSFは、監査データ格納が[割付: ***事前に定義された限界***]を**超えた**場合、[割付: ***監査データ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。

8.7.16 FAU_STG.5 監査データ損失の防止

コンポーネント間の関係

下位階層：	FAU_STG.4 監査データ消失の恐れ発生時のアクション
依存性：	FAU_STG.2 保護された監査データ格納 FAU_GEN.1 監査データ生成

FAU_STG.5.1

TSFは、監査データ格納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*]及び[割付: *監査格納失敗及びその他の条件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 FCOクラス: 通信

9.1クラスの説明

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14は、このクラスの構成を示す。

図14は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Dは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

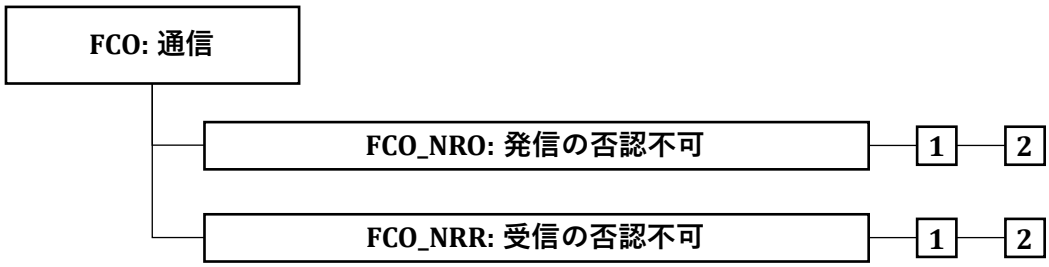


図14 — FCO: 通信クラスの構成

9.2発信の否認不可(FCO_NRO)

9.2.1 ファミリのふるまい

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

9.2.2 コンポーネントのレベル付け及び説明

図15に、本ファミリのコンポーネントのレベル付けを示す。

図15 — FCO_NRO: コンポーネントのレベル付け

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

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

9.2.3 FCO_NRO.1、FCO_NRO.2の管理

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。

9.2.4 FCO_NRO.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

9.2.5 FCO_NRO.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

9.2.6 FCO_NRO.1 発信の選択的証明

コンポーネント間の関係

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_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。

9.2.7 FCO_NRO.2 発信の強制的証明

コンポーネント間の関係

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_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。

9.3 受信の否認不可(FCO_NRR)

9.3.1 ファミリのふるまい

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

9.3.2 コンポーネントのレベル付け及び説明

図16に、本ファミリのコンポーネントのレベル付けを示す。

図16 — FCO_NRR: コンポーネントのレベル付け

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

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

9.3.3 FCO_NRR.1、FCO_NRR.2の管理

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、発信者属性及び第三者の証拠の受信者に対する変更の管理。

9.3.4 FCO_NRR.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

9.3.5 FCO_NRR.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

9.3.6 FCO_NRR.1 受信の選択的証明

コンポーネント間の関係

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。

9.3.7 FCO_NRR.2 受信の強制的証明

コンポーネント間の関係

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*]に対する受信の証拠の**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、情報の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 FCSクラス: 暗号サポート

10.1 クラスの説明

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/又はソフトウェアにおいて行われる。

FCS: 暗号サポートクラスは4つのファミリで構成される。

図17は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Eは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

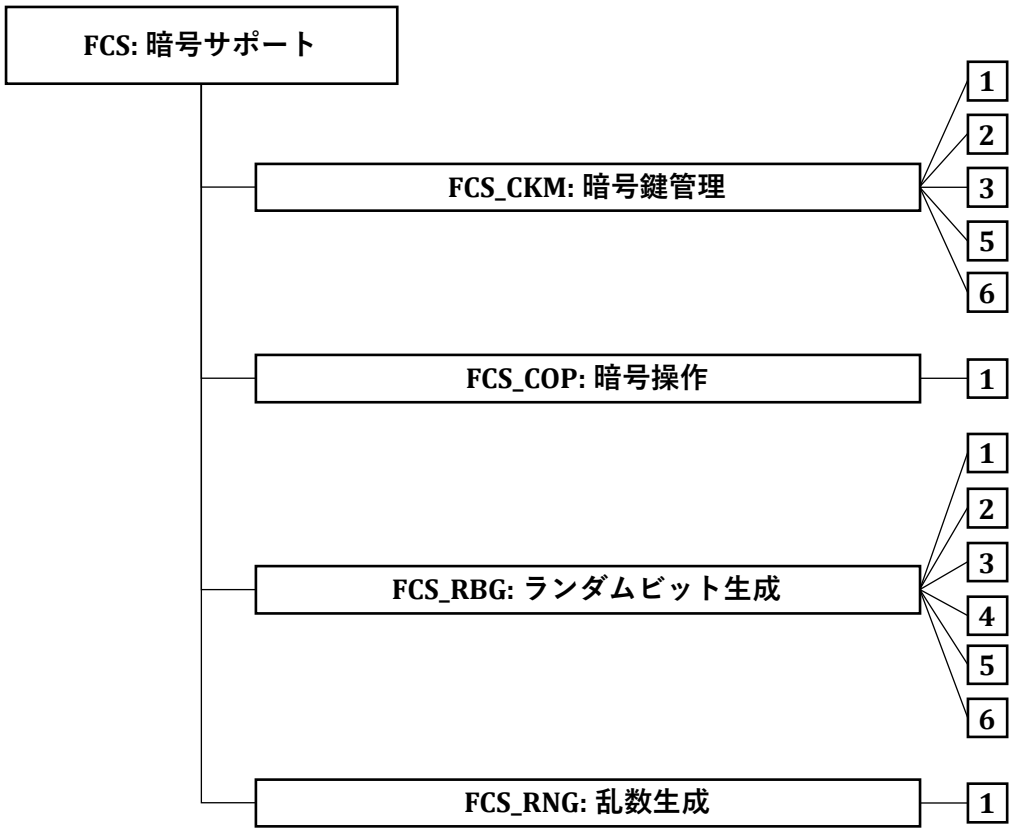


図17 — FCS: 暗号サポートクラスの構成

10.2 暗号鍵管理(FCS_CKM)

10.2.1 ファミリのふるまい

暗号鍵は、そのライフサイクルを通して管理されなければならない。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とし、その結果として以下のアクティビティに対する要件を定義する。

— 暗号鍵生成

— 暗号鍵配付

— 暗号鍵アクセス

— 暗号鍵導出

— 暗号鍵破棄のタイミング及びイベント

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。

10.2.2 コンポーネントのレベル付け及び説明

図18に、本ファミリのコンポーネントのレベル付けを示す。

図18 — FCS_CKM: コンポーネントのレベル付け

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

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

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

FCS_CKM.5 暗号鍵導出は、鍵導出のための方法、標準及びパラメタを特定することを要求する。

FCS_CKM.6 暗号鍵破棄のタイミング及びイベントは、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。

注：本書の旧版ではFCS_CKM.4を規定していたが、本版では非推奨としている。本書の異なる版を適用する際の一貫性を保つため、コンポーネント番号は再使用されていない。

10.2.3 FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.5、FCS_CKM.6の管理

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) 予見される管理アクティビティはない。

10.2.4 FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.5、FCS_CKM.6の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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を除くオブジェクトの値。

10.2.5 FCS_CKM.1 暗号鍵生成

コンポーネント間の関係

下位階層：	なし
依存性：	[FCS_CKM.2 暗号鍵配付、又はFCS_CKM.5 暗号鍵導出、又は FCS_COP.1 暗号操作] FCS_CKM.3 暗号鍵アクセス [FCS_RBG.1 ランダムビット生成(RBG)、又は FCS_RNG.1 乱数生成] FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_CKM.1.1

TSFは、次の[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。

10.2.6 FCS_CKM.2 暗号鍵配付

コンポーネント間の関係

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のインポート、 又は 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、又は FCS_CKM.1 暗号鍵生成、又は FCS_CKM.5 暗号鍵導出] FCS_CKM.3 暗号鍵アクセス

FCS_CKM.2.1

TSFは、次の[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。

10.2.7 FCS_CKM.3 暗号鍵アクセス

コンポーネント間の関係

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のインポート、 又は 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、又は FCS_CKM.1 暗号鍵生成、又は FCS_CKM.5 暗号鍵導出]

FCS_CKM.3.1

TSFは、次の[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。

10.2.8 FCS_CKM.4 暗号鍵破棄

このコンポーネントは非推奨である。代わりにFCS_CKM.6 暗号鍵破棄のタイミング及びイベントを参照すること。

10.2.9 FCS_CKM.5 暗号鍵導出

コンポーネント間の関係

下位階層：	なし
依存性：	[FCS_CKM.2 暗号鍵配付、又は FCS_COP.1 暗号操作] FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_CKM.5.1

TSFは、次の[割付: *標準のリスト*]に合致する、指定された暗号鍵導出アルゴリズム[割付: *暗号鍵導出アルゴリズム*]と指定された暗号鍵長[割付: *鍵長のリスト*]に従って、[割付: *入力パラメタ*]から暗号鍵[割付: *鍵の種別*]を導出しなければならない。

注：このコンポーネントの使用に関する情報については、E.2.6を参照。

10.2.10 FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

コンポーネント間の関係

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のインポート、 又は 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、又は FCS_CKM.1 暗号鍵生成]

FCS_CKM.6.1

TSFは、[選択: *不要、[割付: 鍵又は鍵材料の破棄に関するその他の状況]*]になった場合、[割付: *暗号鍵(鍵材料を含む)のリスト*]を破棄しなければならない。

FCS_CKM.6.2

TSFは、次の[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、FCS_CKM.6.1で指定した暗号鍵及び鍵材料を破棄しなければならない。

10.3 暗号操作(FCS_COP)

10.3.1 ファミリのふるまい

暗号操作が正しく機能するためには、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なければならない。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。

典型的な暗号操作は、データの暗号化及び/又は復号、ディジタル署名の生成及び/又は検証、完全性のための暗号的チェックサムの生成及び/又は検証、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/又は復号、暗号鍵交換などである。

10.3.2 コンポーネントのレベル付け及び説明

図19に、本ファミリのコンポーネントのレベル付けを示す。

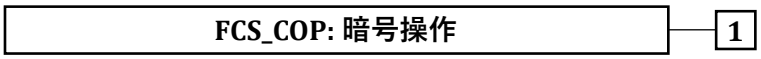


図19 — FCS_COP: コンポーネントのレベル付け

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

10.3.3 FCS_COP.1の管理

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) 予見される管理アクティビティはない。

10.3.4 FCS_COP.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 全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。

10.3.5 FCS_COP.1 暗号操作

コンポーネント間の関係

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のインポート、又は 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、又は FCS_CKM.1 暗号鍵生成、又は FCS_CKM.5 暗号鍵導出] FCS_CKM.3 暗号鍵アクセス

FCS_COP.1.1

TSFは、次の[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。

10.4 ランダムビット生成(FCS_RBG)

10.4.1 ファミリのふるまい

このファミリのコンポーネントは、ランダムビット/乱数の生成の要件を扱う。

10.4.2 コンポーネントのレベル付け及び説明

図20に、本ファミリのコンポーネントのレベル付けを示す。

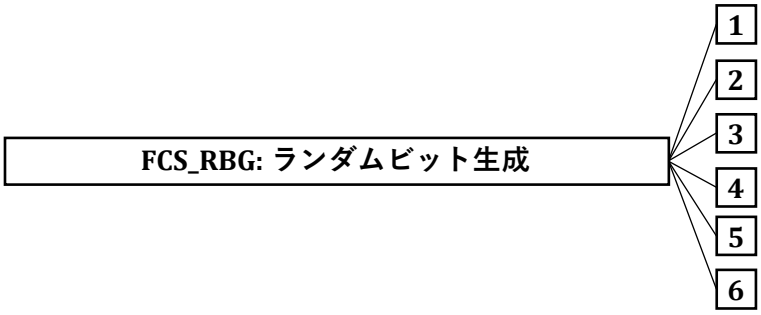


図20 — FCS_RBG: コンポーネントのレベル付け

FCS_RBG.1 ランダムビット生成(RBG)は、選択された標準に従ってランダムビット生成を実行することを要求する。また、初期シードに内部ノイズ源、外部ノイズ源のどちらを使用するか、またRBGの状態がいつ、どのように更新されるかを特定する。

FCS_RBG.2 ランダムビット生成(外部シード)は、外部(TOEの外部)のエントロピー源によるシードの要件を示す。

FCS_RBG.3 ランダムビット生成(内部シード - 単一ソース)は、単一のTSFエントロピー源を使用したシードの要件を示す。

FCS_RBG.4 ランダムビット生成(内部シード - 複数ソース)は、複数のTSFエントロピー源を使用したシードの要件を示す。

FCS_RBG.5 ランダムビット生成(ノイズ源の結合)は、複数のエントロピー源(複数の内部ソース、内部及び外部ソース)を結合するための要件を示す。

FCS_RBG.6 ランダムビット生成サービスは、他のエンティティへのサービスとして、外部インタフェースを介して乱数を供給することを要求する。

10.4.3 FCS_RBG.1、FCS_RBG.2、FCS_RBG.3、FCS_RBG.4、FCS_RBG.5、FCS_RBG.6の管理

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) 予見される管理アクティビティはない。

10.4.4 FCS_RBG.1、FCS_RBG.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: ランダム化処理の失敗、初期化又は再シード(技術でサポートされている場合)の失敗

10.4.5 FCS_RBG.3、FCS_RBG.4、FCS_RBG.5、FCS_RBG.6の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

10.4.6 FCS_RBG.1 ランダムビット生成(RBG)

コンポーネント間の関係

下位階層：	なし
依存性：	[FCS_RBG.2 ランダムビット生成(外部シード)、又は FCS_RBG.3 ランダムビット生成(内部シード - 単一ソース)] FPT_FLS.1 セキュアな状態を保持する障害 FPT_TST.1 TSF自己テスト

FCS_RBG.1.1

TSFは、シードによる初期化後、[割付: *標準のリスト*]に従って[割付: *RBGアルゴリズム*]を用いた決定論的ランダムビット生成サービスを実行しなければならない。

FCS_RBG.1.2

TSF は、[選択: *TSFノイズ源[割付: ノイズ源の名前]*、シード用TSFインタフェース]を初期シードに使用しなければならない。

FCS_RBG.1.3

TSFは、以下の状況で、[割付: *標準のリスト*]に従い、[選択: *TSFノイズ源[割付: ノイズ源の名前]*、シード用TSFインタフェース]を使用した[選択: *再シード*、*インスタンス化の解除と再インスタンス化*]によって、RBGの状態を更新しなければならない。[選択:

— ***更新なし***

— ***要求されたとき***

— ***条件を満たしたとき: [割付: 条件]***

— ***[割付: 時間]経過後*]**

10.4.7 FCS_RBG.2 ランダムビット生成(外部シード)

コンポーネント間の関係

下位階層：	なし
依存性：	FCS_RBG.1 ランダムビット生成(RBG)

FCS_RBG.2.1

TSFは、シードの目的で、TSFインタフェースから[割付: *0より大きい最小入力長*]の最小入力を受け入れることができなければならない。

10.4.8 FCS_RBG.3 ランダムビット生成(内部シード — 単一ソース)

コンポーネント間の関係

下位階層：	なし
依存性：	FCS_RBG.1 ランダムビット生成(RBG)

FCS_RBG.3.1

TSF は、少なくとも[割付: *ビット数*]ビットの最小エントロピーを持つ、[選択: *ソフトウェアベースのTSFノイズ源*、*ハードウェアベースのTSFノイズ源*: *から1つのみ選択*]である[割付: *ノイズ源の名前*]を用いて、RBGをシードすることができなければならない。

10.4.9 FCS_RBG.4 ランダムビット生成(内部シード — 複数ソース)

コンポーネント間の関係

下位階層：	なし
依存性：	FCS_RBG.1 ランダムビット生成(RBG) FCS_RBG.5 ランダムビット生成(ノイズ源の結合)

FCS_RBG.4.1

TSF は、**[選択: *[割付: 数]個のソフトウェアベースのTSFノイズ源*、*[割付: 数]個のハードウェアベースのTSFノイズ源*]**を用いてRBGをシードすることができなければならない。

10.4.10 FCS_RBG.5 ランダムビット生成(ノイズ源の結合)

コンポーネント間の関係

下位階層：	なし
依存性：	FCS_RBG.1 ランダムビット生成(RBG) [FCS_RBG.2 ランダムビット生成(外部シード)、又は FCS_RBG.3 ランダムビット生成(内部シード - 単一ソース)、又は FCS_RBG.4 ランダムビット生成(内部シード - 複数ソース)]

FCS_RBG.5.1

TSFは、[割付: *標準のリスト*]で定義される導出関数へ入力するエントロピーを生成するため、[選択: *TSFノイズ源からの出力*、*シード用TSFインタフェースからの入力*]を[割付: *結合操作*]し、少なくとも[割付: *ビット数*]ビットの最小エントロピーをもたらさなければならない。

10.4.11 FCS_RBG.6 ランダムビット生成サービス

コンポーネント間の関係

下位階層：	なし
依存性：	FCS_RBG.1 ランダムビット生成(RBG)

FCS_RBG.6.1

TSF は、FCS_RBG.1ランダムビット生成(RBG)に規定されるRBG出力をTOE 外のエンティティがサービスとして利用できるよう、[選択: *ハードウェア*、*ソフトウェア*、*[割付: その他のインタフェース種別]*]インタフェースを提供しなければならない。

10.5 乱数生成(FCS_RNG)

10.5.1 ファミリのふるまい

このファミリは、暗号に使用することを目的とした乱数生成に関する品質要件を定義している。

10.5.2 コンポーネントのレベル付け及び説明

図21に、本ファミリのコンポーネントのレベル付けを示す。

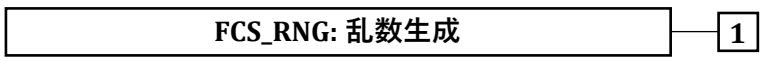


図21 — FCS_RNG: コンポーネントのレベル付け

FCS_RNG.1 乱数生成は、乱数が定義された品質尺度を満たすことを要求する。

10.5.3 FCS_RNG.1の管理

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) 予見される管理アクティビティはない。

10.5.4 FCS_RNG.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

10.5.5 FCS_RNG.1 乱数生成

コンポーネント間の関係

下位階層： なし

依存性： なし

FCS_RNG.1.1

TSFは、[割付: *セキュリティ能力のリスト*]を実装する[選択: *物理的*、*非物理的な真性*、*決定論的*、*ハイブリッド物理的*、*ハイブリッド決定論的*]乱数生成器を提供しなければならない。

FCS_RNG.1.2

TSFは、[割付: *定義された品質尺度*]を満たす[選択: *ビット*、*ビットのオクテット*、*数値[割付: 数値の形式]*]を提供しなければならない。

11 FDPクラス: 利用者データ保護

11.1 クラスの説明

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。

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) 利用者データ保護のセキュリティ機能方針(SFP):

— アクセス制御方針(FDP_ACC)

— 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、PPモジュール、機能パッケージ又はSTの作成者は、利用者データ保護のSFP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」を割付又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)

— 情報保持制御(FDP_IRC)

— 残存情報保護(FDP_RIP)

— ロールバック(FDP_ROL)

— 蓄積データ機密性(FDP_SDC)

— 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)

— 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22は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Fは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

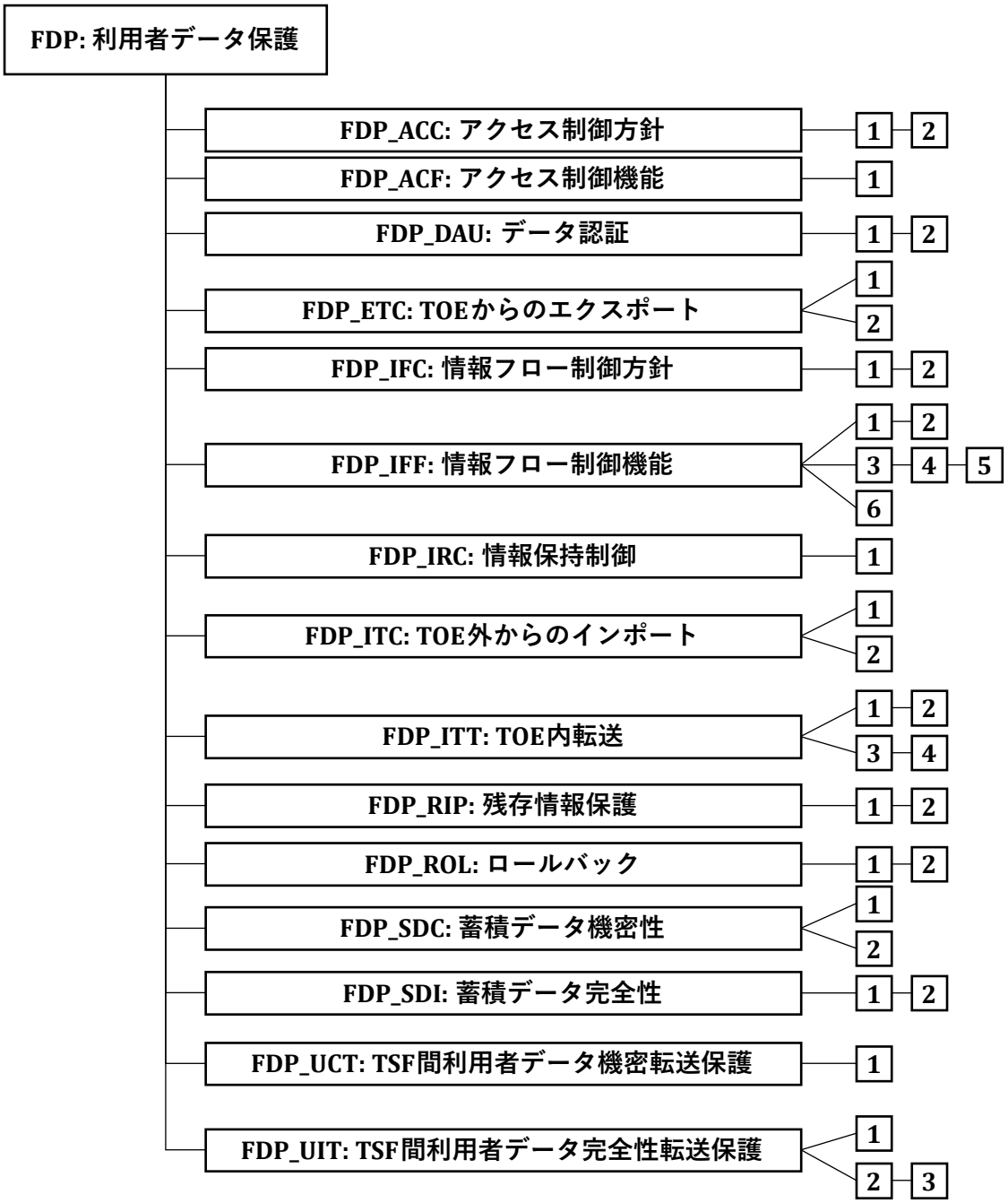


図22 — FDP: 利用者データ保護クラスの構成

11.2 アクセス制御方針(FDP_ACC)

11.2.1 ファミリのふるまい

このファミリは、アクセス制御SFPを(名前で)識別し、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」の割付又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。

11.2.2 コンポーネントのレベル付け及び説明

図23に、本ファミリのコンポーネントのレベル付けを示す。

図23 — FDP_ACC: コンポーネントのレベル付け

FDP_ACC.1 サブセットアクセス制御は、識別された各アクセス制御SFPが、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、適切なものであることを要求する。

FDP_ACC.2 完全アクセス制御は、識別された各アクセス制御SFPが、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全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全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。

11.2.3 FDP_ACC.1、FDP_ACC.2の管理

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) 予見される管理アクティビティはない。

11.2.4 FDP_ACC.1、FDP_ACC.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

11.2.5 FDP_ACC.1 サブセットアクセス制御

コンポーネント間の関係

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。

11.2.6 FDP_ACC.2 完全アクセス制御

コンポーネント間の関係

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: *サブジェクト及びオブジェクトのリスト*]及びSFPで扱われるサブジェクトとオブジェクト間の**全ての**操作に対して[割付: *アクセス制御SFP*]を実施しなければならない。

FDP_ACC.2.2

TSFは、TSFによって制御されるあらゆるサブジェクトとTSFによって制御されるあらゆるオブジェクト間の全ての操作がアクセス制御SFPで扱われることを保証しなければならない。

11.3 アクセス制御機能(FDP_ACF)

11.3.1 ファミリのふるまい

このファミリは、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。

11.3.2 コンポーネントのレベル付け及び説明

図24に、本ファミリのコンポーネントのレベル付けを示す。

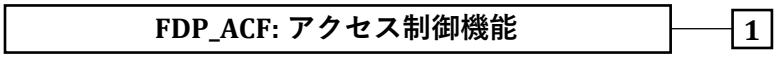


図24 — FDP_ACF: コンポーネントのレベル付け

このファミリは、セキュリティ属性の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、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_ACF.1 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又は拒否することができる。

11.3.3 FDP_ACF.1の管理

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) 明示的なアクセス又は拒否に基づく決定に使われる属性の管理。

11.3.4 FDP_ACF.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての要求。

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。

11.3.5 FDP_ACF.1 セキュリティ属性によるアクセス制御

コンポーネント間の関係

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、次の[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、又は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。

11.4 データ認証(FDP_DAU)

11.4.1 ファミリのふるまい

データ認証は、あるエンティティが情報の真正性についての責任を持つことを許可する。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。

11.4.2 コンポーネントのレベル付け及び説明

図25に、本ファミリのコンポーネントのレベル付けを示す。

図25 — FDP_DAU: コンポーネントのレベル付け

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

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

11.4.3 FDP_DAU.1、FDP_DAU.2の管理

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。

11.4.4 FDP_DAU.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

11.4.5 FDP_DAU.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

11.4.6 FDP_DAU.1 基本データ認証

コンポーネント間の関係

下位階層：	なし
依存性：	なし

FDP_DAU.1.1

TSFは、[割付: *オブジェクト又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。

11.4.7 FDP_DAU.2 保証人識別付きデータ認証

コンポーネント間の関係

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: *オブジェクト又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。

11.5 TOEからのエクスポート(FDP_ETC)

11.5.1 ファミリのふるまい

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。

11.5.2 コンポーネントのレベル付け及び説明

図26に、本ファミリのコンポーネントのレベル付けを示す。

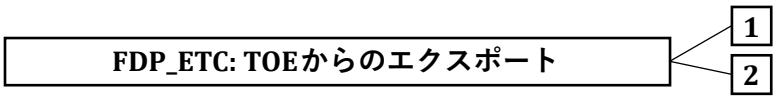


図26 — FDP_ETC: コンポーネントのレベル付け

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

FDP_ETC.2 セキュリティ属性付き利用者データのエクスポートは、セキュリティ属性とエクスポートされる利用者データを正確かつ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。

11.5.3 FDP_ETC.1の管理

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) 予見される管理アクティビティはない。

11.5.4 FDP_ETC.2の管理

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。

11.5.5 FDP_ETC.1、FDP_ETC.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

11.5.6 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

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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/又は情報フロー制御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。

11.5.7 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

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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/又は情報フロー制御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、エクス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、利用者データの所有者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_ETC.2.5

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。

11.6 情報フロー制御方針(FDP_IFC)

11.6.1 ファミリのふるまい

このファミリは、情報フロー制御SFPを(名前によって)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やり取りさせる操作。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」の割付又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。

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。

11.6.2 コンポーネントのレベル付け及び説明

図27に、本ファミリのコンポーネントのレベル付けを示す。

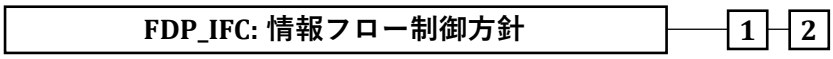


図27 — FDP_IFC: コンポーネントのレベル付け

FDP_IFC.1 サブセット情報フロー制御は、識別された各情報フロー制御SFPが、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、適切なものであることを要求する。

FDP_IFC.2 完全情報フロー制御は、識別された各情報フロー制御SFPが、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全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全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。

11.6.3 FDP_IFC.1、FDP_IFC.2の管理

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) 予見される管理アクティビティはない。

11.6.4 FDP_IFC.1、FDP_IFC.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

11.6.5 FDP_IFC.1 サブセット情報フロー制御

コンポーネント間の関係

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: *サブジェクト、情報、及びSFPで扱われる制御されたサブジェクトとやり取りする制御された情報の流れを引き起こす操作のリスト*]に対して[割付: *情報フロー制御SFP*]を実施しなければならない。

11.6.6 FDP_IFC.2 完全情報フロー制御

コンポーネント間の関係

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: *サブジェクト及び情報のリスト*]及びSFPで扱われるサブジェクトとやり取りする情報の流れを引き起こす**全ての**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のあらゆるサブジェクトとやり取りする、TOEのあらゆる情報の流れを引き起こす全ての操作が、情報フロー制御SFPで扱われることを保証しなければならない。

11.7 情報フロー制御機能(FDP_IFF)

11.7.1 ファミリのふるまい

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、その発生を制限又は防止するために、特別の機能が必要である。

11.7.2 コンポーネントのレベル付け及び説明

図28に、本ファミリのコンポーネントのレベル付けを示す。

図28 — FDP_IFF: コンポーネントのレベル付け

FDP_IFF.1 単純セキュリティ属性は、情報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。

FDP_IFF.2 階層的セキュリティ属性は、SFRのセットにおける全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。

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

FDP_IFF.4不正情報フローの部分的排除は、SFPがいくらか(必ずしも全てではない)の不正情報フローの排除を扱うことを要求する。

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

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

11.7.3 FDP_IFF.1、FDP_IFF.2の管理

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。

11.7.4 FDP_IFF.3、FDP_IFF.4、FDP_IFF.5の管理

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) 予見される管理アクティビティはない。

11.7.5 FDP_IFF.6の管理

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。

11.7.6 FDP_IFF.1、FDP_IFF.2、FDP_IFF.5の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての決定。

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: 方針目標に基づいて流れた、情報の特定のサブセット。

11.7.7 FDP_IFF.3、FDP_IFF.4、FDP_IFF.6の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての決定。

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: 方針目標に基づいて流れた、情報の特定のサブセット。

f) 詳細: 推定最大容量が特定した値を超える、識別された不正情報フローチャネルの利用。

11.7.8 FDP_IFF.1 単純セキュリティ属性

コンポーネント間の関係

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する、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、次の規則、[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、次の規則、[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。

11.7.9 FDP_IFF.2 階層的セキュリティ属性

コンポーネント間の関係

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しなければならない、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、次の規則、[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、次の規則、[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、あらゆる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以下の関係を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又はセキュリティ属性が比較不能であるかどうかを決定する順序付け機能が存在する。

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又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。

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又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。

11.7.10 FDP_IFF.3 制限付き不正情報フロー

コンポーネント間の関係

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: *不正情報フローの種別*]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。

11.7.11 FDP_IFF.4 不正情報フローの部分的排除

コンポーネント間の関係

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: *不正情報フローの種別*]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。

11.7.12 FDP_IFF.5 不正情報フローなし

コンポーネント間の関係

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。

11.7.13 FDP_IFF.6 不正情報フロー監視

コンポーネント間の関係

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。

11.8 情報保持制御(FDP_IRC)

11.8.1 ファミリのふるまい

「情報保持制御」ファミリは、セキュアな情報処理及びストレージアプリケーションにおける基本的なニーズである、TOEがその操作を実行するためにもはや必要としないが、TOEにまだ保存されているデータを安全に管理することに対応する。

ITシステムをデータ保存システムとして捉える歴史的な考え方は、一度入力されたデータがシステムから削除されることはほとんどなく、削除されるのは主にストレージの容量不足によるものだと示唆していた。

しかし、多国間又は高度なセキュリティ環境では、データのシステムへの保存期間と同様に、データの複製を、最小限に抑えることが重要である。また、第三者に悪用されたり、プライバシーを脅かすと思われる機密データの保持を、利用者がIT製品に求めないことも考えられる。FDP_IRCは、不要になったデータのコピーを全て削除することで、製品が安全であることを利用者が確信するのに役立つかもしれない。

FDP_RIP「残存情報保護」ファミリはこの問題の一面に対処するが、不要になったデータの管理に関する明確な要件が欠落している。

もちろん、データによってはより長い期間、より多くの操作のためシステムに必要とされる可能性があるため、競合する要件が発生する可能性がある。この問題に対する解決策としては、以下が考えられる。

— TOEに格納された情報オブジェクトをアクセスからより良く保護する。

— 保護された情報が必要となるたびに、利用者に再要求する。

情報保持制御は、TOEの運用に必要でなくなったデータがTOEによって削除されることを保証する。このファミリのコンポーネントは、PP、PPモジュール、機能パッケージ又はSTの作成者に、単純な処理と複雑な処理の両方を含むTOEの操作と、それらの操作の対象である、TOEに保持されない情報オブジェクトを特定することを要求する。

また、TOEは、そのような保存された情報オブジェクトを追跡し、不要になったオンラインとオフラインの両方の情報オブジェクトを削除することが要求される。

このファミリは、TOEの操作における特定のアクティビティのために要求される情報オブジェクトに関する要件のみを設定し、一般的なデータ収集に関する要件は設定しない。TOEに保存される一般利用者データの収集、保存、処理、開示及び消去を制御する方針は、別の場所で詳述され、それらはPP、PPモジュール、機能パッケージ又はSTの範囲ではなく、環境目標及び組織方針の領域である。

複数の操作が保護オブジェクトの存在を必要とする場合、必要とされるオブジェクトを参照する全ての操作は、そのオブジェクトを削除する前に終了しなければならない。

11.8.2 コンポーネントのレベル付け及び説明

図29に、本ファミリのコンポーネントのレベル付けを示す。

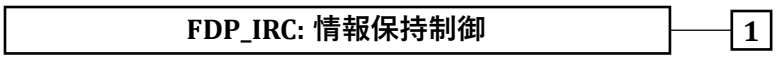


図29 — FDP_IRC: コンポーネントのレベル付け

FDP_IRC.1 情報保持制御は、TOE内の定義されたオブジェクトのセットのコピーが、TOEの運用に厳密に必要でなくなった場合、削除されることをTSFが保証し、オブジェクトを必要とする操作を特定し定義することを要求する。

11.8.3 FDP_IRC.1の管理

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) 予見される管理アクティビティはない。

11.8.4 FDP_IRC.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

11.8.5 FDP_IRC.1 情報保持制御

コンポーネント間の関係

下位階層： なし

依存性： なし

FDP_IRC.1.1

TSFは、[割付: *操作のリスト*]に必要な[割付: *オブジェクトのリスト*]について、選択されたオブジェクトが選択された操作の終了時に速やかにTOEから不可逆的かつ追跡不可能に削除されるように、[割付: *情報消去方針*]を実施しなければならない。

FDP_IRC.1.2

TSFは、[割付: *オブジェクトのリスト*]に、解放後、不可逆的かつ追跡不可能な削除の前にアクセスできないことを保証しなければならない。

11.9 TOE外からのインポート(FDP_ITC)

11.9.1 ファミリのふるまい

このファミリは、利用者データが適切なセキュリティ属性を持ち、かつ適切に保護されるように、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。

11.9.2 コンポーネントのレベル付け及び説明

図30に、本ファミリのコンポーネントのレベル付けを示す。

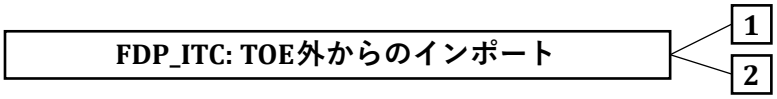


図30 — FDP_ITC: コンポーネントのレベル付け

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。

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。

11.9.3 FDP_ITC.1、FDP_ITC.2の管理

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。

11.9.4 FDP_ITC.1、FDP_ITC.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

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。

11.9.5 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

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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制御下の利用者データをTOE外部からインポートするとき、[割付: *アクセス制御SFP及び/又は情報フロー制御SFP*]を実施しなければならない。

FDP_ITC.1.2

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

FDP_ITC.1.3

TSFは、SFP制御下の利用者データをTOE外部から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。

11.9.6 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

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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、又は 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制御下の利用者データをTOE外部からインポートするとき、[割付: *アクセス制御SFP及び/又は情報フロー制御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、SFP制御下の利用者データをTOE外部から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。

11.10 TOE内転送(FDP_ITT)

11.10.1 ファミリのふるまい

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外部とやり取りするデータのTSF仲介転送に対応する。

11.10.2 コンポーネントのレベル付け及び説明

図31に、本ファミリのコンポーネントのレベル付けを示す。

図31 — FDP_ITT: コンポーネントのレベル付け

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

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

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

FDP_ITT.4 属性に基づく完全性監視は、SFP関連属性によって完全性監視の形態を変えられるようにすることで、3番目のコンポーネントを拡張する。

11.10.3 FDP_ITT.1、FDP_ITT.2の管理

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部分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。

11.10.4 FDP_ITT.3、FDP_ITT.4の管理

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。

11.10.5 FDP_ITT.1、FDP_ITT.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

11.10.6 FDP_ITT.3、FDP_ITT.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

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。

11.10.7 FDP_ITT.1 基本内部転送保護

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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部分間を転送される場合、その[選択: *暴露*、*改変*、*使用不能*]を防ぐための[割付: *アクセス制御SFP及び/又は情報フロー制御SFP*]を実施しなければならない。

11.10.8 FDP_ITT.2 属性による転送分離

コンポーネント間の関係

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、又は 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部分間を転送される場合、その[選択: *暴露*、*改変*、*使用不能*]を防ぐための[割付: *アクセス制御SFP及び/又は情報フロー制御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部分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:

11.10.9 FDP_ITT.3 完全性監視

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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、次の誤り: [割付: *完全性誤り*]について、TOEの物理的に分離された部分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/又は情報フロー制御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。

11.10.10 FDP_ITT.4 属性に基づく完全性監視

コンポーネント間の関係

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、又は 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、**次の属性: [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**、次の誤り: [割付: *完全性誤り*]について、TOEの物理的に分離された部分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/又は情報フロー制御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。

11.11 残存情報保護(FDP_RIP)

11.11.1 ファミリのふるまい

このファミリは、資源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に、資源に含まれるいかなるデータも利用できない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資源に含まれるが、TSF制御資源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。

11.11.2 コンポーネントのレベル付け及び説明

図32に、本ファミリのコンポーネントのレベル付けを示す。

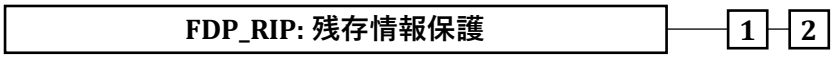


図32 — FDP_RIP: コンポーネントのレベル付け

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

FDP_RIP.2 全残存情報保護は、全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

11.11.3 FDP_RIP.1、FDP_RIP.2の管理

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。

11.11.4 FDP_RIP.1、FDP_RIP.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

11.11.5 FDP_RIP.1 サブセット情報保護

コンポーネント間の関係

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。

11.11.6 FDP_RIP.2 全残存情報保護

コンポーネント間の関係

下位階層：	FDP_RIP.1 サブセット情報保護
依存性：	なし

FDP_RIP.2.1

TSFは、**全ての**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。

11.12 ロールバック (FDP_ROL)

11.12.1 ファミリのふるまい

ロールバック操作とは、直前の操作、又は期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、操作又は一連の操作の結果を元に戻す機能を提供する。

11.12.2 コンポーネントのレベル付け及び説明

図33に、本ファミリのコンポーネントのレベル付けを示す。

図33 — FDP_ROL: コンポーネントのレベル付け

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

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

11.12.3 FDP_ROL.1、FDP_ROL.2の管理

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制限は、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。

11.12.4 FDP_ROL.1、FDP_ROL.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 全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全ての試み。

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全ての試み。

11.12.5 FDP_ROL.1 基本ロールバック

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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/又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/ 又は情報フロー制御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制限*]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。

11.12.6 FDP_ROL.2 高度ロールバック

コンポーネント間の関係

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、又は 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**全ての操作**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/又は情報フロー制御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制限*]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。

11.13 蓄積データ機密性(FDP_SDC)

11.13.1 ファミリのふるまい

このファミリは、TSFによって保護されるメモリ領域内に格納されている間の利用者データ機密性の保護に対応する要件を提供する。TSFは、特定のインタフェースのみを通じてメモリ内のデータへのアクセスを提供し、これらのインタフェースをバイパスした情報の漏洩を防止する。このファミリは、メモリに格納されている間、利用者データを完全性誤りから保護する蓄積データ完全性(FDP_SDI)ファミリを補完するものである。

11.13.2 コンポーネントのレベル付け及び説明

図34に、本ファミリのコンポーネントのレベル付けを示す。

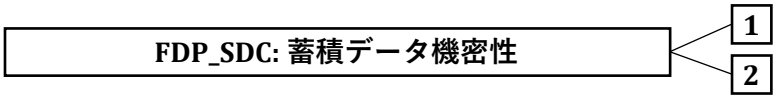


図34 — FDP_SDC: コンポーネントのレベル付け

FDP_SDC.1 蓄積データ機密性は、TSFが指定されたメモリ領域内の利用者データの情報の機密性を保護することを要求する。

FDP_SDC.2 専用方法による蓄積データ機密性は、TSF が、機密性保護の専用方法を特定することにつながるデータ特性に従って、利用者データの機密性を保護することを要求する。

11.13.3 FDP_SDC.1、FDP_SDC.2の管理

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) 予見される管理アクティビティはない。

11.13.4 FDP_SDC.1、FDP_SDC.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

11.13.5 FDP_SDC.1 蓄積データ機密性

コンポーネント間の関係

下位階層： なし

依存性： なし

FDP_SDC.1.1

TSFは、[選択: *全ての利用者データ*、*次の利用者データ[割付: 利用者データのリスト]*]が[選択: *一時的なメモリ*、*永続的なメモリ*、*任意のメモリ*]に保存されている間、その機密性を保証しなければならない。

11.13.6 FDP_SDC.2 専用方法による蓄積データ機密性

コンポーネント間の関係

下位階層： なし

依存性： FCS_COP.1 暗号操作

FDP_SDC.2.1

TSFは、[選択: *全ての利用者データ*、*次の利用者データ[割付: 利用者データのリスト]*]がTSFの管理下で保存されている間、[割付: *データ特性*]に従って、その機密性を保証しなければならない。

FDP_SDC.2.2

TSFは、FDP_SDC.2.1 で特定された利用者データの機密性を、利用者の介入なしに保証しなければならない。

11.14 蓄積データ完全性(FDP_SDI)

11.14.1 ファミリのふるまい

このファミリは、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、メモリ又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。

11.14.2 コンポーネントのレベル付け及び説明

図35に、本ファミリのコンポーネントのレベル付けを示す。

図35 — FDP_SDI: コンポーネントのレベル付け

FDP_SDI.1 蓄積データ完全性監視は、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。

FDP_SDI.2 蓄積データ完全性監視及びアクションは、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、最初のコンポーネントに追加能力を加える。

11.14.3 FDP_SDI.1の管理

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) 予見される管理アクティビティはない。

11.14.4 FDP_SDI.2の管理

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。

11.14.5 FDP_SDI.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み(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。

11.14.6 FDP_SDI.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み(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。

11.14.7 FDP_SDI.1 蓄積データ完全性監視

コンポーネント間の関係

下位階層：	なし
依存性：	なし

FDP_SDI.1.1

TSFは、全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。

11.14.8 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、全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*]を行なわなければならない。

11.15 TSF間利用者データ機密転送保護(FDP_UCT)

11.15.1 ファミリのふるまい

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。

11.15.2 コンポーネントのレベル付け及び説明

図36に、本ファミリのコンポーネントのレベル付けを示す。

図36 — FDP_UCT: コンポーネントのレベル付け

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

11.15.3 FDP_UCT.1の管理

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) 予見される管理アクティビティはない。

11.15.4 FDP_UCT.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

11.15.5 FDP_UCT.1 基本データ交換機密性

コンポーネント間の関係

下位階層：	なし
依存性：	[FTP_ITC.1 TSF間高信頼チャネル、又は FTP_TRP.1 高信頼パス] [FDP_ACC.1 サブセットアクセス制御、又は 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/又は情報フロー制御SFP*]を実施しなければならない。

11.16 TSF間利用者データ完全性転送保護(FDP_UIT)

11.16.1 ファミリのふるまい

このファミリは、TOEと他の高信頼IT製品間で転送中の利用者データの完全性を提供し、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。

11.16.2 コンポーネントのレベル付け及び説明

図37に、本ファミリのコンポーネントのレベル付けを示す。

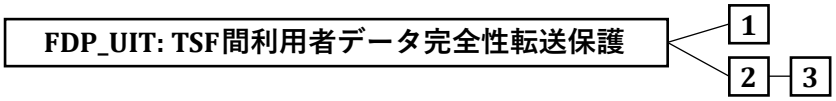


図37 — FDP_UIT: コンポーネントのレベル付け

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

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

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

11.16.3 FDP_UIT.1、FDP_UIT.2、FDP_UIT.3の管理

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) 予見される管理アクティビティはない。

11.16.4 FDP_UIT.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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/又は影響。

11.16.5 FDP_UIT.2、FDP_UIT.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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/又は影響。

11.16.6 FDP_UIT.1 データ交換完全性

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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、又は 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/又は情報フロー制御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決定できなければならない。

11.16.7 FDP_UIT.2 発信側データ交換回復

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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、又は 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/又は情報フロー制御SFP*]を実施しなければならない。

11.16.8 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、又は 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、又は 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/又は情報フロー制御SFP*]を実施しなければならない。

12 FIAクラス: 識別と認証

12.1 クラスの説明

このクラスのファミリは、主張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。

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38は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Gは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

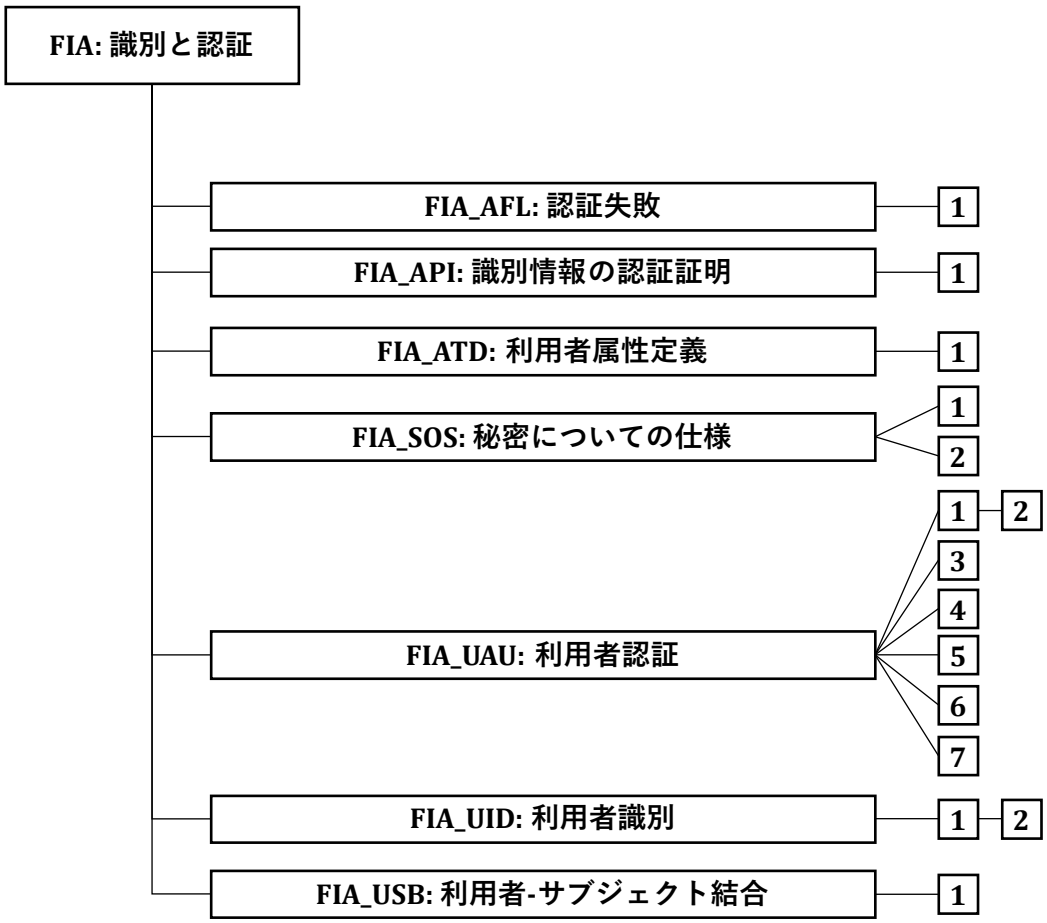


図38 — FIA: 識別と認証クラスの構成

12.2 認証失敗(FIA_AFL)

12.2.1 ファミリのふるまい

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。

12.2.2 コンポーネントのレベル付け及び説明

図39に、本ファミリのコンポーネントのレベル付けを示す。

図39 — FIA_AFL: コンポーネントのレベル付け

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。

12.2.3 FIA_AFL.1の管理

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。

12.2.4 FIA_AFL.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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、もし適切であれば、正常状態への復帰。

12.2.5 FIA_AFL.1 認証失敗時の取り扱い

コンポーネント間の関係

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。

12.3 識別情報の認証証明(FIA_API)

12.3.1 ファミリのふるまい

このファミリは、TOEの識別情報を証明するためにTOEが提供する機能を定義し、TOEのIT環境における外部エンティティによるTOEの検証を可能にする。

12.3.2 コンポーネントのレベル付け及び説明

図40に、本ファミリのコンポーネントのレベル付けを示す。

図40 — FIA_API: コンポーネントのレベル付け

FIA_API.1 識別情報の認証証明は、外部エンティティにTOEの識別情報の証明を提供する。

12.3.3 FIA_API.1の管理

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) 主張された識別情報を証明するために使用される認証情報の管理。

12.3.4 FIA_API.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

12.3.5 FIA_API.1 識別情報の認証証明

コンポーネント間の関係

下位階層： なし

依存性： なし

FIA_API.1.1

TSFは、外部エンティティに次の特性[割付: *特性のリスト*]を含めることにより、[割付: *エンティティ*]の識別情報を証明する[割付: *認証メカニズム*]を提供しなければならない。

12.4 利用者属性定義(FIA_ATD)

12.4.1 ファミリのふるまい

全ての許可利用者は、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。

12.4.2 コンポーネントのレベル付け及び説明

図41に、本ファミリのコンポーネントのレベル付けを示す。

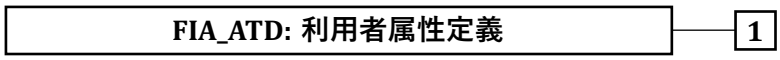


図41 — FIA_ATD: コンポーネントのレベル付け

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

12.4.3 FIA_ATD.1の管理

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。

12.4.4 FIA_ATD.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

12.4.5 FIA_ATD.1 利用者属性定義

コンポーネント間の関係

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*]

12.5 秘密についての仕様(FIA_SOS)

12.5.1 ファミリのふるまい

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

12.5.2 コンポーネントのレベル付け及び説明

図42に、本ファミリのコンポーネントのレベル付けを示す。

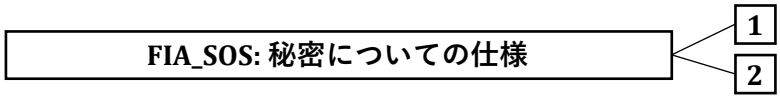


図42 — FIA_SOS: コンポーネントのレベル付け

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

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

12.5.3 FIA_SOS.1の管理

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。

12.5.4 FIA_SOS.2の管理

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。

12.5.5 FIA_SOS.1、FIA_SOS.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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又は受け入れ。

c) 詳細: 定義された品質尺度に対する変更の識別。

12.5.6 FIA_SOS.1 秘密の検証

コンポーネント間の関係

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。

12.5.7 FIA_SOS.2 TSF秘密生成

コンポーネント間の関係

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。

12.6 利用者認証(FIA_UAU)

12.6.1 ファミリのふるまい

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く、要求された属性も定義する。

12.6.2 コンポーネントのレベル付け及び説明

図43に、本ファミリのコンポーネントのレベル付けを示す。

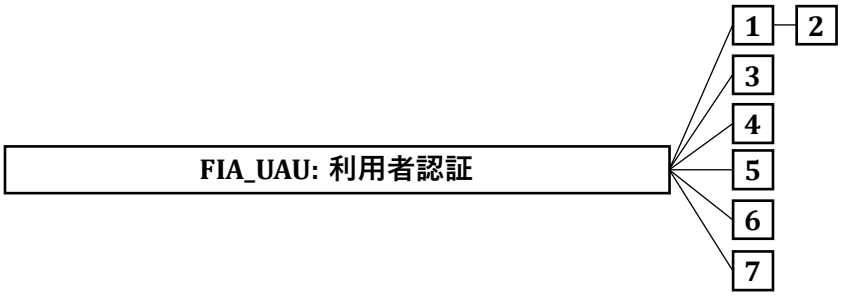


図43 — FIA_UAU: コンポーネントのレベル付け

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

FIA_UAU.2 アクション前の利用者認証は、TSFが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。

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

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

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

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

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

12.6.3 FIA_UAU.1の管理

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。

12.6.4 FIA_UAU.2の管理

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。

12.6.5 FIA_UAU.3、FIA_UAU.4、FIA_UAU.7の管理

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) 予見される管理アクティビティはない。

12.6.6 FIA_UAU.5の管理

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。

12.6.7 FIA_UAU.6の管理

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。

12.6.8 FIA_UAU.7の管理

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) 予見される管理アクティビティはない。[iii]

12.6.9 FIA_UAU.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 認証メカニズムの全ての使用。

c) 詳細: 利用者認証以前に行われた全てのTSF仲介アクション。

12.6.10 FIA_UAU.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 認証メカニズムの全ての使用。

12.6.11 FIA_UAU.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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、直ちにとられた全ての手段とチェックの結果。

12.6.12 FIA_UAU.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

12.6.13 FIA_UAU.5の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

12.6.14 FIA_UAU.6の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 全ての再認証試行。

12.6.15 FIA_UAU.7の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。[iv]

12.6.16 FIA_UAU.1 認証のタイミング

コンポーネント間の関係

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_UAU.1.2

TSFは、その利用者を代行する他の全ての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。

12.6.17 FIA_UAU.2 アクション前の利用者認証

コンポーネント間の関係

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全ての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。

12.6.18 FIA_UAU.3 偽造されない認証

コンポーネント間の関係

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。

12.6.19 FIA_UAU.4 単一使用認証メカニズム

コンポーネント間の関係

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。

12.6.20 FIA_UAU.5 複数の認証メカニズム

コンポーネント間の関係

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。

12.6.21 FIA_UAU.6 再認証

コンポーネント間の関係

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。

12.6.22 FIA_UAU.7 保護された認証フィードバック

コンポーネント間の関係

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。

12.7 利用者識別(FIA_UID)

12.7.1 ファミリのふるまい

このファミリは、利用者が自分自身を識別することが要求されなけれ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全てのアクションの前に行われる。

12.7.2 コンポーネントのレベル付け及び説明

図44に、本ファミリのコンポーネントのレベル付けを示す。

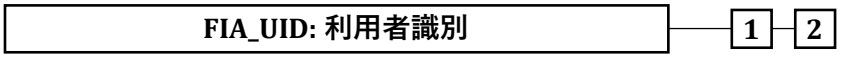


図44 — FIA_UID: コンポーネントのレベル付け

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

FIA_UID.2 アクション前の利用者識別は、TSFが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。

12.7.3 FIA_UID.1の管理

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。

12.7.4 FIA_UID.2の管理

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。

12.7.5 FIA_UID.1、FIA_UID.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての使用。

12.7.6 FIA_UID.1 識別のタイミング

コンポーネント間の関係

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全ての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。

12.7.7 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全ての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。

12.8 利用者-サブジェクト結合(FIA_USB)

12.8.1 ファミリのふるまい

認証された利用者は、TOEを使用するため、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、(全体又は一部が)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。

12.8.2 コンポーネントのレベル付け及び説明

図45に、本ファミリのコンポーネントのレベル付けを示す。

図45 — FIA_USB: コンポーネントのレベル付け

FIA_USB.1 利用者-サブジェクト結合は、利用者のセキュリティ属性と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。

12.8.3 FIA_USB.1の管理

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。

12.8.4 FIA_USB.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

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。

12.8.5 FIA_USB.1 利用者-サブジェクト結合

コンポーネント間の関係

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、利用者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の最初の関連付けについて、以下の規則を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、利用者を代行して動作するサブジェクトに関連付けられた利用者セキュリティ属性の変更を管理する以下の規則を実施しなければならない。 : [割付: *属性の変更の規則*]

13 FMTクラス: セキュリティ管理

13.1 クラスの説明

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。能力の分離のような、異なる管理の役割とこれらの相互の影響を特定することができる。

このクラスは以下の目的を持つ:

a) TSFデータの管理

b) セキュリティ属性の管理

c) TSFの機能の管理

d) セキュリティ役割の定義。

図46は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Hは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

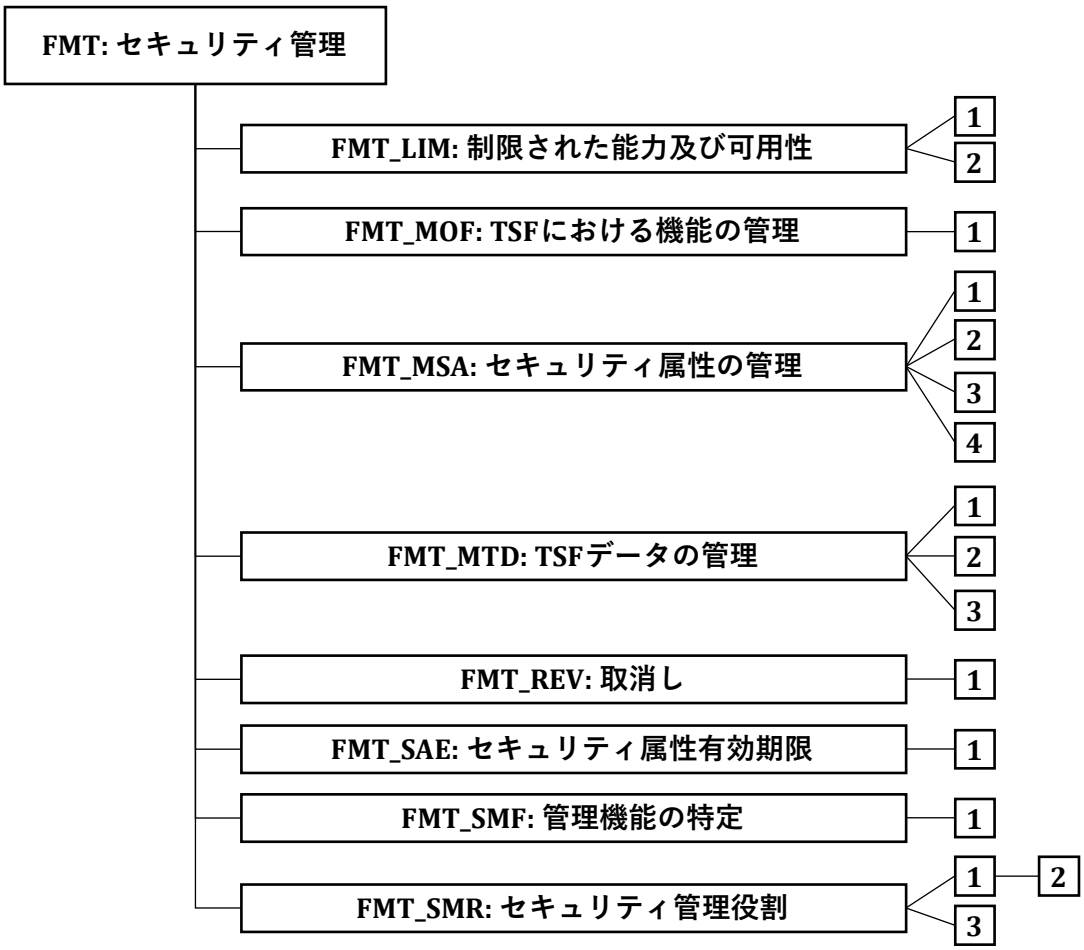


図46 — FMT: セキュリティ管理クラスの構成

13.2 制限された能力及び可用性(FMT_LIM)

13.2.1 ファミリのふるまい

このファミリは、機能の能力及び可用性を複合的に制限することを要求する。

注：FDP_ACFが機能へのアクセスを制限するのに対し、このファミリの「限定された能力」コンポーネントは、機能そのものを特定の方法で設計することを要求する。

13.2.2 コンポーネントのレベル付け及び説明

図47に、本ファミリのコンポーネントのレベル付けを示す。

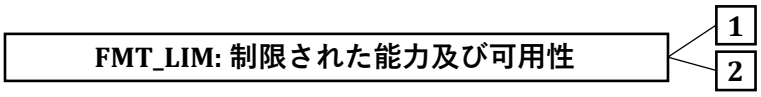


図47 — FMT_LIM: コンポーネントのレベル付け

FMT_LIM.1 制限された能力は、TSF がその真の目的に必要な能力(アクションの実行、情報の収集)だけを提供するように構築されていることを要求する。

FMT_LIM.2 制限された可用性は、TSFが機能の使用を制限することを要求する(制限された能力(FMT_LIM.1)を参照)。これは、例えば、TOEのライフサイクルの特定のフェーズで機能を削除又は無効にすることで達成できる。

13.2.3 FMT_LIM.1、FMT_LIM.2の管理

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) 予見される管理アクティビティはない。

13.2.4 FMT_LIM.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

13.2.5 FMT_LIM.1 制限された能力

コンポーネント間の関係

下位階層： なし

依存性： FMT_LIM.2 制限された可用性

FMT_LIM.1.1

TSFは、「制限された可用性(FMT_LIM.2)」と合わせて、以下の方針が実施されるように、その能力を制限しなければならない。[割付: *制限される能力及び可用性の方針*]

13.2.6 FMT_LIM.2 制限された可用性

コンポーネント間の関係

下位階層： なし

依存性： FMT_LIM.1 制限された能力

FMT_LIM.2.1

TSFは、「制限された能力(FMT_LIM.1)」と合わせて、以下の方針が実施されるように、その可用性を制限するように設計されなければならない。[割付: *制限される能力及び可用性の方針*]

13.3 TSFにおける機能の管理(FMT_MOF)

13.3.1 ファミリのふるまい

このファミリは、許可利用者がTSFにおける機能の管理を統括できるようにする。

13.3.2 コンポーネントのレベル付け及び説明

図48に、本ファミリのコンポーネントのレベル付けを示す。

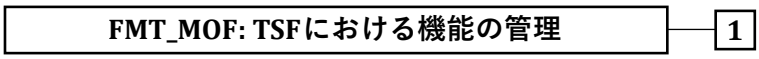


図48 — FMT_MOF: コンポーネントのレベル付け

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

13.3.3 FMT_MOF.1の管理

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。

13.3.4 FMT_MOF.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての改変。

13.3.5 FMT_MOF.1 セキュリティ機能のふるまいの管理

コンポーネント間の関係

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、を無効にする、を有効にする、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。

13.4 セキュリティ属性の管理(FMT_MSA)

13.4.1 ファミリのふるまい

このファミリは、許可利用者がセキュリティ属性の管理を統括することを許可する。この管理には、セキュリティ属性を見たり改変したりする機能が含まれる。

13.4.2 コンポーネントのレベル付け及び説明

図49に、本ファミリのコンポーネントのレベル付けを示す。

図49 — FMT_MSA: コンポーネントのレベル付け

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

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

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

FMT_MSA.4 セキュリティ属性値継承は、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／方針を特定することを認める。

13.4.3 FMT_MSA.1の管理

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。

13.4.4 FMT_MSA.2の管理

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。

13.4.5 FMT_MSA.3の管理

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。

13.4.6 FMT_MSA.4の管理

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。

13.4.7 FMT_MSA.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全て。

13.4.8 FMT_MSA.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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、拒否された値全て。

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全て。

13.4.9 FMT_MSA.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全て。

13.4.10 FMT_MSA.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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/又は変更されたセキュリティ属性の値。

13.4.11 FMT_MSA.1 セキュリティ属性の管理

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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。

13.4.12 FMT_MSA.2 セキュアなセキュリティ属性

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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。

13.4.13 FMT_MSA.3 静的属性初期化

コンポーネント間の関係

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。

13.4.14 FMT_MSA.4 セキュリティ属性値継承

コンポーネント間の関係

下位階層：	なし
依存性：	[FDP_ACC.1 サブセットアクセス制御、又は 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*]

13.5 TSFデータの管理(FMT_MTD)

13.5.1 ファミリのふるまい

このファミリは、許可利用者(役割)がTSFデータの管理を統括することを許可する。

13.5.2 コンポーネントのレベル付け及び説明

図50に、本ファミリのコンポーネントのレベル付けを示す。

図50 — FMT_MTD: コンポーネントのレベル付け

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

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

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

13.5.3 FMT_MTD.1の管理

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。

13.5.4 FMT_MTD.2の管理

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。

13.5.5 FMT_MTD.3の管理

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) 予見される管理アクティビティはない。

13.5.6 FMT_MTD.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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データの値の全ての改変。

13.5.7 FMT_MTD.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての改変。

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全ての改変。

13.5.8 FMT_MTD.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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データの全ての拒否された値。

13.5.9 FMT_MTD.1 TSFデータの管理

コンポーネント間の関係

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。

13.5.10 FMT_MTD.2 TSFデータにおける限界値の管理

コンポーネント間の関係

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なければならない。 : [割付: *とられるアクション*]

13.5.11 FMT_MTD.3 セキュアなTSFデータ

コンポーネント間の関係

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。

13.6 取消し(FMT_REV)

13.6.1 ファミリのふるまい

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。

13.6.2 コンポーネントのレベル付け及び説明

図51に、本ファミリのコンポーネントのレベル付けを示す。

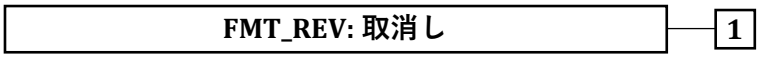


図51 — FMT_REV: コンポーネントのレベル付け

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

13.6.3 FMT_REV.1の管理

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。

13.6.4 FMT_REV.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

13.6.5 FMT_REV.1 取消し

コンポーネント間の関係

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。

FMT_REV.1.2

TSFは、規則[割付: *取消し規則の仕様*]を実施しなければならない。

13.7 セキュリティ属性有効期限(FMT_SAE)

13.7.1 ファミリのふるまい

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

13.7.2 コンポーネントのレベル付け及び説明

図52に、本ファミリのコンポーネントのレベル付けを示す。

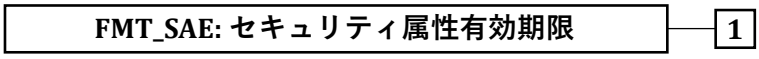


図52 — FMT_SAE: コンポーネントのレベル付け

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

13.7.3 FMT_SAE.1の管理

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。

13.7.4 FMT_SAE.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

13.7.5 FMT_SAE.1 時限付き許可

コンポーネント間の関係

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の経過後、[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。

13.8 管理機能の特定(FMT_SMF)

13.8.1 ファミリのふるまい

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。

13.8.2 コンポーネントのレベル付け及び説明

図53に、本ファミリのコンポーネントのレベル付けを示す。

図53 — FMT_SMF: コンポーネントのレベル付け

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。

13.8.3 FMT_SMF.1の管理

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) 予見される管理アクティビティはない。

13.8.4 FMT_SMF.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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

13.8.5 FMT_SMF.1 管理機能の特定

コンポーネント間の関係

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*]

13.9 セキュリティ管理役割(FMT_SMR)

13.9.1 ファミリのふるまい

このファミリは、利用者への異なる役割の割り当てを制御することを意図している。セキュリティ管理に関するこれらの役割の能力は、このクラスの他のファミリで記述される。

13.9.2 コンポーネントのレベル付け及び説明

図54に、本ファミリのコンポーネントのレベル付けを示す。

図54 — FMT_SMR: コンポーネントのレベル付け

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

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

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

13.9.3 FMT_SMR.1の管理

以下のアクションはFMT_SMR.1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。

13.9.4 FMT_SMR.2の管理

以下のアクションはFMT_SMR.2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。

b) 役割が満たさなければならない条件を管理すること。

13.9.5 FMT_SMR.3の管理

以下のアクションはFMT_SMR.3における管理機能と考えられる:

a) 予見される管理アクティビティはない。

13.9.6 FMT_SMR.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 役割の権限の使用全て。

13.9.7 FMT_SMR.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 役割の権限の使用全て。

13.9.8 FMT_SMR.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

13.9.9 FMT_SMR.1 セキュリティの役割

コンポーネント間の関係

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。

13.9.10 FMT_SMR.2 セキュリティ役割における制限

コンポーネント間の関係

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。

13.9.11 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 FPRクラス: プライバシー

14.1 クラスの説明

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55は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Iは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

図55 — FPR: プライバシークラスの構成

14.2 匿名性(FPR_ANO)

14.2.1 ファミリのふるまい

このファミリは、利用者が利用者の識別情報を暴露することなく、資源やサービスを使用できることを保証する。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。

14.2.2 コンポーネントのレベル付け及び説明

図56に、本ファミリのコンポーネントのレベル付けを示す。

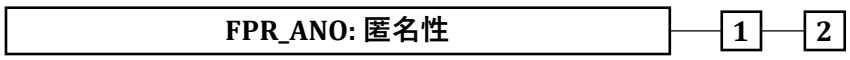


図56 — FPR_ANO: コンポーネントのレベル付け

FPR_ANO.1 匿名性は、あるサブジェクト又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決定できないことを要求する。

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

14.2.3 FPR_ANO.1、FPR_ANO.2の管理

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) 予見される管理アクティビティはない。

14.2.4 FPR_ANO.1、FPR_ANO.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

14.2.5 FPR_ANO.1 匿名性

コンポーネント間の関係

下位階層： なし

依存性： なし

FPR_ANO.1.1

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

14.2.6 FPR_ANO.2 情報を請求しない匿名性

コンポーネント間の関係

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/又はサブジェクトのセット*]が、[割付: *サブジェクト及び/又は操作及び/又はオブジェクトのリスト*]に結合された実利用者名を決定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。

14.3 偽名性(FPR_PSE)

14.3.1 ファミリのふるまい

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

14.3.2 コンポーネントのレベル付け及び説明

図57に、本ファミリのコンポーネントのレベル付けを示す。

図57 — FPR_PSE: コンポーネントのレベル付け

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

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

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

14.3.3 FPR_PSE.1、FPR_PSE.2、FPR_PSE.3の管理

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) 予見される管理アクティビティはない。

14.3.4 FPR_PSE.1、FPR_PSE.2、FPR_PSE.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

14.3.5 FPR_PSE.1 偽名性

コンポーネント間の関係

下位階層： なし

依存性： なし

FPR_PSE.1.1

TSFは、[割付: *利用者及び/又はサブジェクトのセット*]が、[割付: *サブジェクト及び/又は操作及び/又はオブジェクトのリスト*]に結合された実利用者名を決定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。

14.3.6 FPR_PSE.2 可逆偽名性

コンポーネント間の関係

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/又はサブジェクトのセット*]が、[割付: *サブジェクト及び/又は操作及び/又はオブジェクトのリスト*]に結合された実利用者名を決定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、次の[割付: *条件のリスト*]のもとでだけ、[選択: *許可利用者*、*[割付: 高信頼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決定する能力を提供しなければならない。

14.3.7 FPR_PSE.3 別名偽名性

コンポーネント間の関係

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/又はサブジェクトのセット*]が、[割付: *サブジェクト及び/又は操作及び/又はオブジェクトのリスト*]に結合された実利用者名を決定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、次の[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。

14.4 リンク不能性(FPR_UNL)

14.4.1 ファミリのふるまい

このファミリは、選択されたエンティティが、外部エンティティがバックトレースできないようにリンクできることを保証する。

14.4.2 コンポーネントのレベル付け及び説明

図58に、本ファミリのコンポーネントのレベル付けを示す。

図58 — FPR_UNL: コンポーネントのレベル付け

FPR_UNL.1 操作のリンク不能性は、同じ利用者がシステム内である特定の操作の原因になっているかどうか、又は操作が何らかの形で関連しているかどうかを、利用者及び/又はサブジェクトが決定できないことを要求する。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、それによって情報を取得できないことを保証する。

14.4.3 FPR_UNL.1の管理

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。

14.4.4 FPR_UNL.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

14.4.5 FPR_UNL.1 操作のリンク不能性

コンポーネント間の関係

下位階層： なし

依存性： なし

FPR_UNL.1.1

TSFは、[割付: *エンティティ及び/又は操作のリスト*]が[選択: *同じ利用者によって実行された、次のように関係する[割付: 関係のリスト]*]かどうかを[割付: *エンティティ及び/又は操作のセット*]が決定できないことを保証しなければならない。

注：このSFRは、1つのエンティティが実行した個々の操作のセットだけを対象にしているわけではない。このSFRが対象とするのは、複数のエンティティによる相互に関連する一連の操作である。この一連の操作はトランザクションとして包含されることがある。

14.5 観察不能性(FPR_UNO)

14.5.1 ファミリのふるまい

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

14.5.2 コンポーネントのレベル付け及び説明

図59に、本ファミリのコンポーネントのレベル付けを示す。

図59 — FPR_UNO: コンポーネントのレベル付け

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

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

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

FPR_UNO.4 許可利用者観察可能性は、資源及び/又はサービスの利用を観察する権限を、一人又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。

14.5.3 FPR_UNO.1、FPR_UNO.2の管理

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。

14.5.4 FPR_UNO.3の管理

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) 予見される管理アクティビティはない。

14.5.5 FPR_UNO.4の管理

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。

14.5.6 FPR_UNO.1、FPR_UNO.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

14.5.7 FPR_UNO.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

14.5.8 FPR_UNO.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 利用者又はサブジェクトによる資源又はサービスの使用の観察。

14.5.9 FPR_UNO.1 観察不能性

コンポーネント間の関係

下位階層： なし

依存性： なし

FPR_UNO.1.1

TSFは、[割付: *利用者及び/又はサブジェクトのリスト*]が[割付: *保護された利用者及び/又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。

14.5.10 FPR_UNO.2 観察不能性に影響を与える情報の配置

コンポーネント間の関係

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/又はサブジェクトのリスト*]が[割付: *保護された利用者及び/又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の異なる部分に[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*]。

14.5.11 FPR_UNO.3 情報を請求しない観察不能性

コンポーネント間の関係

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: *プライバシー関連情報*]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。

14.5.12 FPR_UNO.4 許可利用者観察可能性

コンポーネント間の関係

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/又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 FPTクラス: TSFの保護

15.1 クラスの説明

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。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が、これらは同じメカニズムを使って実装されていることもあり得る。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。

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60は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Jは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

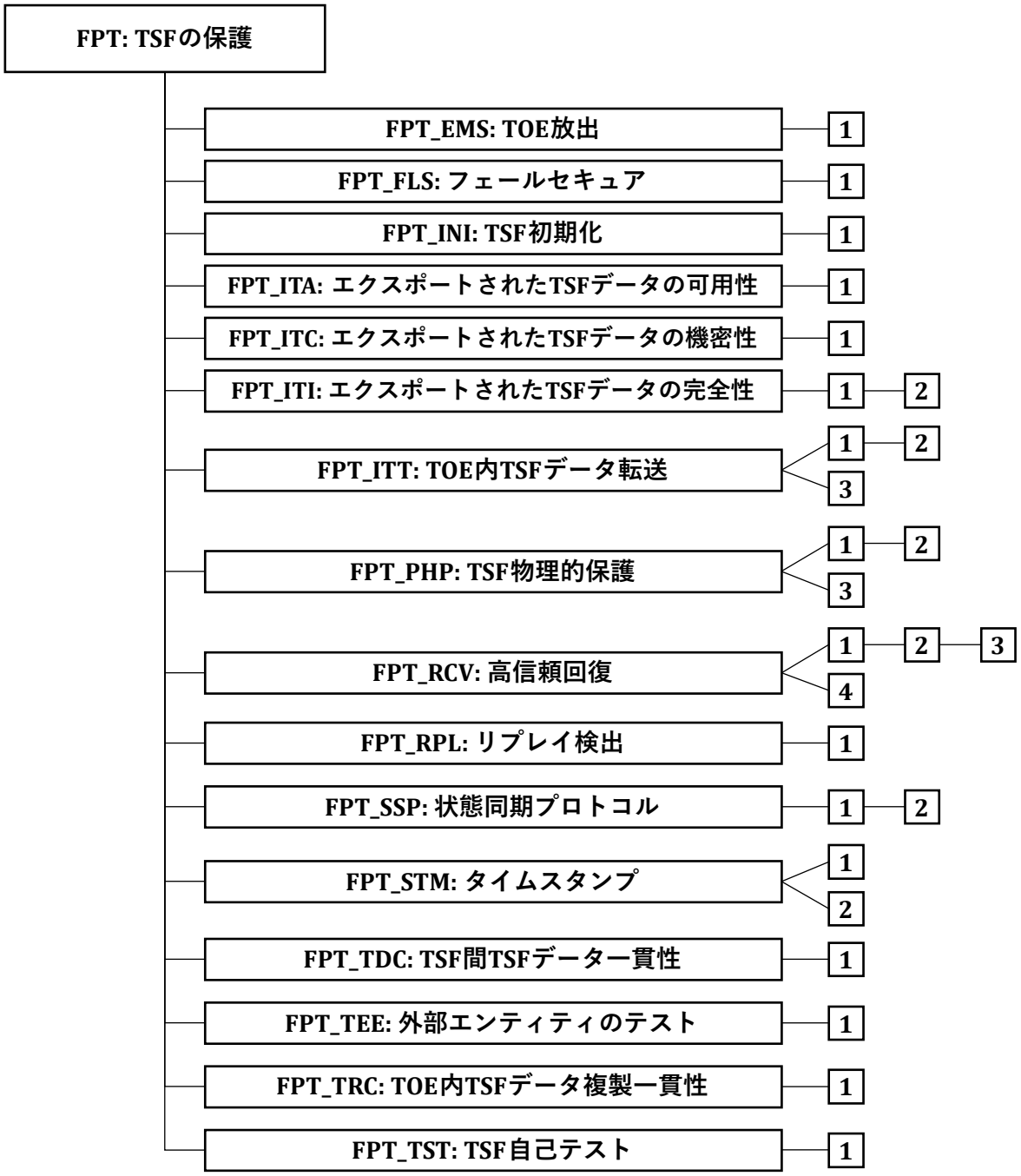


図60 — FPT: TSFの保護クラスの構成

15.2 TOE放出(FPT_EMS)

15.2.1 ファミリのふるまい

FPT(TSFの保護)クラスのFPT_EMS(TOE放出)ファミリは、放出に基づく情報の漏洩に関連するTOEのIT分野のSFRを記述する。

TOEが、TOE及びTOEが処理する秘密データに対する攻撃を防ぐ必要があり、その攻撃がTOEの動作中に外部から観察可能な現象に基づく場合、様々な種類のTSFデータ及び利用者データと同様に、TOEの様々な種類の放出及びインタフェースに対応することができる。

例

TOE及びTOEが処理する秘密データに対するこのような攻撃の例としては、単純電力解析(SPA)、差分電力解析(DPA)、単純電磁解析(SEMA)、差分電磁解析(DEMA)、タイミング攻撃、パディングオラクル攻撃、キャッシュミス攻撃などが挙げられる。

このファミリは、この文書の他のコンポーネントで直接扱われていない、感知できる放出の制限のための機能要件を記述する。

15.2.2 コンポーネントのレベル付け及び説明

図61に、本ファミリのコンポーネントのレベル付けを示す。

図61 — FPT_EMS: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_EMS.1 TSF及び利用者データの放出で構成され、TOEが感知できる放出を軽減するための要件を定義している。

15.2.3 FPT_EMS.1の管理

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) 予見される管理アクティビティはない。

15.2.4 FPT_EMS.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

15.2.5 FPT_EMS.1 TSF及び利用者データの放出

コンポーネント間の関係

下位階層： なし

依存性： なし

FPT_EMS.1.1

TSFは、表1に特定されるTSFデータ及び利用者データへのアクセスを可能にするような量の放出を、その攻撃対象領域に放出しないことを保証しなければならない。

表 1 — FPT_EMS.1.1 表

ID	放出	攻撃対象領域	TSFデータ	利用者データ
1	**[割付:** ***放出の種別のリスト*****]**	**[割付:** ***攻撃対象領域の種別のリスト*****]**	**[割付:** ***TSFデータの種別のリスト*****]**	**[割付:** ***利用者データの種別のリスト*****]**
…	…	…	…	…

15.3 フェールセキュア(FPT_FLS)

15.3.1 ファミリのふるまい

このファミリの要件は、TSF中の識別された障害のカテゴリの事象において、TOEがそのSFRを常に実施することを保証する。

15.3.2 コンポーネントのレベル付け及び説明

図62に、本ファミリのコンポーネントのレベル付けを示す。

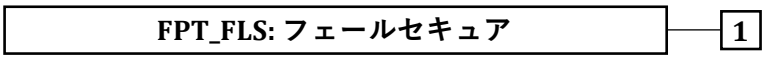


図62 — FPT_FLS: コンポーネントのレベル付け

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。

15.3.3 FPT_FLS.1の管理

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) 予見される管理アクティビティはない。

15.3.4 FPT_FLS.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.3.5 FPT_FLS.1 セキュアな状態を保持する障害

コンポーネント間の関係

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*]。

15.4 TSF初期化(FPT_INI)

15.4.1 ファミリのふるまい

このファミリは、正確でセキュアな運用状態での初期化を保証するTOEの専用機能によるTSFの初期化に関する機能要件を記述する。

15.4.2 コンポーネントのレベル付け及び説明

図63に、本ファミリのコンポーネントのレベル付けを示す。

図63 — FPT_INI: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_INI.1 だけで構成されている。このコンポーネントは、電源投入時にTSFをセキュアな状態にするTSF初期化機能を提供することをTOEに要求する。

15.4.3 FPT_INI.1の管理

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) 予見される管理アクティビティはない。

15.4.4 FPT_INI.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

15.4.5 FPT_INI.1 TSF初期化

コンポーネント間の関係

下位階層： なし

依存性： なし

FPT_INI.1.1

TOEは、完全性と真正性のために自己保護された初期化機能を提供しなければならない。

FPT_INI.1.2

TOE初期化機能は、表2に規定するように、TSFをセキュアな初期状態を確立する直前に、特定の要素に対し特定の特性が保持されることを保証しなければならない。

表 2 — FPT_INI.1.2 表

ID	特性	要素
1	**[割付:** ***特性、例えば真正性、完全性、正しいバージョン*****]**	**[割付:** ***TSF/利用者のファームウェア、ソフトウェア又はデータのリスト*****]**
…	…	…

FPT_INI.1.3

TOE初期化機能は、TOEが[選択: ***停止、[選択: 機能性の制限、エラー状態の通知、[割付: アクションのリスト]]*****]を実施して初期化を正常に完了]するように、初期化中のエラー及び故障を検出し対応しなければならない。**

FPT_INI.1.4

TOE初期化機能は、初期化処理の間、[割付: ***定義された方法*****]においてのみTSFと相互作用しなければならない。**

15.5 エクスポートされたTSFデータの可用性(FPT_ITA)

15.5.1 ファミリのふるまい

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。

15.5.2 コンポーネントのレベル付け及び説明

図64に、本ファミリのコンポーネントのレベル付けを示す。

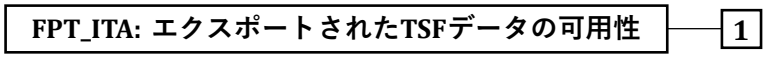


図64 — FPT_ITA: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_ITA.1 定義された可用性尺度以内のTSF間可用性だけから成る。このコンポーネントは、識別された見込みの度合いに対し、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。

15.5.3 FPT_ITA.1の管理

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製品で使用可能なTSFデータの種別のリストの管理。

15.5.4 FPT_ITA.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.5.5 FPT_ITA.1 定義された可用性尺度内のTSF間可用性

コンポーネント間の関係

下位階層： なし

依存性： なし

FPT_ITA.1.1

TSFは、与えられた次の条件[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。

15.6 エクスポートされたTSFデータの機密性(FPT_ITC)

15.6.1 ファミリのふるまい

このファミリは、TSFと他の高信頼IT製品間の送信中のTSFデータの、不正な暴露からの保護に対する規則を定義する。

15.6.2 コンポーネントのレベル付け及び説明

図65に、本ファミリのコンポーネントのレベル付けを示す。

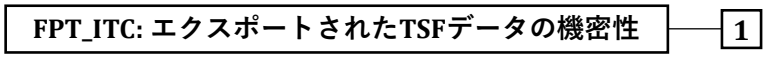


図65 — FPT_ITC: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_ITC.1 送信中のTSF間機密性だけから成り、これは、TSFと他の高信頼IT製品間で送信されるデータが、転送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。

15.6.3 FPT_ITC.1の管理

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) 予見される管理アクティビティはない。

15.6.4 FPT_ITC.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

15.6.5 FPT_ITC.1 送信中のTSF間機密性

コンポーネント間の関係

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製品に送信される全ての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。

15.7 エクスポートされたTSFデータの完全性(FPT_ITI)

15.7.1 ファミリのふるまい

このファミリは、TSFと他の高信頼IT製品間で送信中の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。

15.7.2 コンポーネントのレベル付け及び説明

図66に、本ファミリのコンポーネントのレベル付けを示す。

図66 — FPT_ITI: コンポーネントのレベル付け

FPT_ITI.1 TSF間改変の検出は、他の高信頼IT製品が使用されるメカニズムを認識していることを前提に、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。

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。

15.7.3 FPT_ITI.1の管理

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) 予見される管理アクティビティはない。

15.7.4 FPT_ITI.2の管理

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場合にTSFが訂正を試みる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場合にTSFがとるアクションの種別の管理。

15.7.5 FPT_ITI.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 送信されたTSFデータの改変の検出。

b) 基本: 送信されたTSFデータの改変の検出においてとられるアクション。

15.7.6 FPT_ITI.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 送信されたTSFデータの改変の検出。

b) 基本: 送信された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。

15.7.7 FPT_ITI.1 TSF間改変の検出

コンポーネント間の関係

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製品間で送信中の全ての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製品間で送信される全ての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。

15.7.8 FPT_ITI.2 TSF間改変の検出と訂正

コンポーネント間の関係

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製品間で送信中の全ての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製品間で送信される全ての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製品間で送信される全ての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。

15.8 TOE内TSFデータ転送(FPT_ITT)

15.8.1 ファミリのふるまい

このファミリは、TSFデータが内部チャネルを介してTOEの分離した部分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。

15.8.2 コンポーネントのレベル付け及び説明

図67に、本ファミリのコンポーネントのレベル付けを示す。

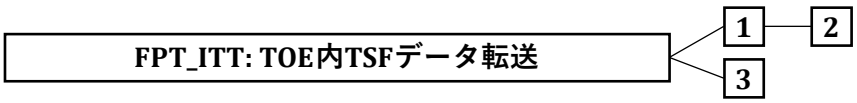


図67 — FPT_ITT: コンポーネントのレベル付け

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

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

FPT_ITT.3 TSFデータ完全性監視は、TOEの分離した部分間で送信される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。

15.8.3 FPT_ITT.1の管理

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が保護すべき改変の種別の管理。

b) TSFの異なる部分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。

15.8.4 FPT_ITT.2の管理

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が保護すべき改変の種別の管理。

b) TSFの異なる部分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。

15.8.5 FPT_ITT.3の管理

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が保護すべき改変の種別の管理。

b) TSFの異なる部分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。

15.8.6 FPT_ITT.1、FPT_ITT.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

15.8.7 FPT_ITT.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.8.8 FPT_ITT.1 基本TSF内データ転送保護

コンポーネント間の関係

下位階層：	なし
依存性：	なし

FPT_ITT.1.1

TSFは、TSFデータがTOEの異なる部分間で送信される場合、TSFデータを[選択: *暴露*、*改変*]から保護しなければならない。

15.8.9 FPT_ITT.2 TSFデータ転送分離

コンポーネント間の関係

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の異なる部分間で送信される場合、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の異なる部分間で送信される場合、利用者データをTSFデータから分離しなければならない。

15.8.10 FPT_ITT.3 TSFデータ完全性監視

コンポーネント間の関係

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の異なる部分間で送信されるTSFデータに対し、[選択: *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*、*[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なければならない。 : [割付: *とられるアクションを指定*]

15.9 TSF物理的保護(FPT_PHP)

15.9.1 ファミリのふるまい

TSF物理的保護コンポーネントは、TSFに対する許可されない物理的アクセスの制限、及びTSFの許可されない物理的改変又は置換の抑止及び抵抗に関係する。

このファミリのコンポーネントの要件は、物理的な改ざんと干渉からTSFが保護されることを保証する。これらのコンポーネントの要件を満たすことは、結果として、TSFがパッケージ化され、かつ、物理的改ざんを検出可能な、あるいは物理的改ざんへの抵抗が強制されるような形で使われることになる。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。

15.9.2 コンポーネントのレベル付け及び説明

図68に、本ファミリのコンポーネントのレベル付けを示す。

図68 — FPT_PHP: コンポーネントのレベル付け

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

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

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

15.9.3 FPT_PHP.1の管理

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又は役割の管理。

15.9.4 FPT_PHP.2の管理

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又は役割の管理。

b) 指定された利用者又は役割に、侵入について通知すべき装置のリストの管理。

15.9.5 FPT_PHP.3の管理

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。

15.9.6 FPT_PHP.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.9.7 FPT_PHP.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.9.8 FPT_PHP.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

15.9.9 FPT_PHP.1 物理的攻撃の受動的検出

コンポーネント間の関係

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。

15.9.10 FPT_PHP.2 物理的攻撃の通知

コンポーネント間の関係

下位階層：	FPT_PHP.1 物理的攻撃の受動的検出
依存性：	FMT_LIM.1 制限された能力

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の装置又はTSFのエレメントに物理的改ざんが生じたとき、[割付: *指示された利用者又は役割*]に通知しなければならない。

15.9.11 FPT_PHP.3 物理的攻撃への抵抗

コンポーネント間の関係

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。

15.10 高信頼回復(FPT_RCV)

15.10.1 ファミリのふるまい

このファミリの要件は、保護の弱体化なくTOEが立ち上がることを決定できること、かつ操作の中断後、保護の弱体化なく回復できることを保証する。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定するからである。

15.10.2 コンポーネントのレベル付け及び説明

図69に、本ファミリのコンポーネントのレベル付けを示す。

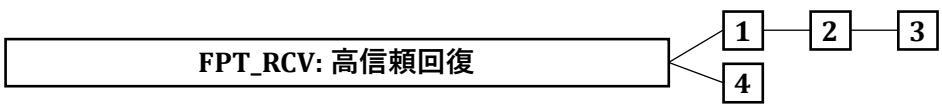


図69 — FPT_RCV: コンポーネントのレベル付け

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

FPT_RCV.2 自動回復は、少なくともサービス中断の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。

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

FPT_RCV.4 機能回復は、特別な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。

15.10.3 FPT_RCV.1の管理

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復元能力に誰がアクセスできるかの管理。

15.10.4 FPT_RCV.2、FPT_RCV.3の管理

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復元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。

15.10.5 FPT_RCV.4の管理

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) 予見される管理アクティビティはない。

15.10.6 FPT_RCV.1、FPT_RCV.2、FPT_RCV.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 障害又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: 障害又はサービス中断の種別。

15.10.7 FPT_RCV.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.10.8 FPT_RCV.1 手動回復

コンポーネント間の関係

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。

15.10.9 FPT_RCV.2 自動回復

コンポーネント間の関係

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。

15.10.10 FPT_RCV.3 過度の損失のない自動回復

コンポーネント間の関係

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

障害又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データ又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。

15.10.11 FPT_RCV.4 機能回復

コンポーネント間の関係

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。

15.11 リプレイ検出(FPT_RPL)

15.11.1 ファミリのふるまい

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。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。

15.11.2 コンポーネントのレベル付け及び説明

図70に、本ファミリのコンポーネントのレベル付けを示す。

図70 — FPT_RPL: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_RPL.1 リプレイ検出だけからなり、これは、識別されたエンティティのリプレイをTSFが検出できなければならないことを要求する。

15.11.3 FPT_RPL.1の管理

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) リプレイを検出する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。

15.11.4 FPT_RPL.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 特定のアクションに基づいてとられるアクション。

15.11.5 FPT_RPL.1 リプレイ検出

コンポーネント間の関係

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。

15.12 状態同期プロトコル(FPT_SSP)

15.12.1 ファミリのふるまい

分散TOEは、TOEの部分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。

状態同期プロトコル(FPT_SSP)は、この高信頼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つの分散した部分が、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。

15.12.2 コンポーネントのレベル付け及び説明

図71に、本ファミリのコンポーネントのレベル付けを示す。

図71 — FPT_SSP: コンポーネントのレベル付け

FPT_SSP.1 単純な高信頼確認応答は、データ受信による単純な確認応答だけを要求する。

FPT_SSP.2 相互の高信頼確認応答は、データ交換の相互の確認応答を要求する。

15.12.3 FPT_SSP.1、FPT_SSP.2の管理

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) 予見される管理アクティビティはない。

15.12.4 FPT_SSP.1、FPT_SSP.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 予期されたときの確認応答受信失敗。

15.12.5 FPT_SSP.1 単純な高信頼確認応答

コンポーネント間の関係

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の他の部分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確認応答をしなければならない。

15.12.6 FPT_SSP.2 相互の高信頼確認応答

コンポーネント間の関係

下位階層：	FPT_SSP.1 単純な高信頼確認応答
依存性：	FPT_ITT.1 基本TSF内データ転送保護

FPT_SSP.2.1

TSFは、TSFの他の部分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確認応答をしなければならない。

FPT_SSP.2.2

TSFは、TSFの関連する部分が、確認応答を使って、異なる部分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。

15.13 タイムスタンプ(FPT_STM)

15.13.1 ファミリのふるまい

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。

15.13.2 コンポーネントのレベル付け及び説明

図72に、本ファミリのコンポーネントのレベル付けを示す。[v]

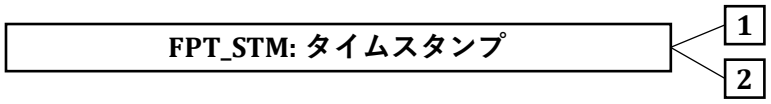


図72 — FPT_STM: コンポーネントのレベル付け

FPT_STM.1 高信頼タイムスタンプは、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。

FPT_STM.2 タイムソースは、タイムスタンプに使用されるタイムソースの記述を要求する。

15.13.3 FPT_STM.1の管理

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。

15.13.4 FPT_STM.2の管理

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) セキュリティ方針に基づき許可された利用者による時刻の設定

15.13.5 FPT_STM.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.13.6 FPT_STM.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 時間の不連続な変更。

b) 詳細: タイムソースの変更。

15.13.7 FPT_STM.1 高信頼タイムスタンプ

コンポーネント間の関係

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。

15.13.8 FPT_STM.2 タイムソース

コンポーネント間の関係

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

FPT_STM.2.1

TSFは、[割付: *セキュリティ方針によって許可された利用者*]が[選択: *時刻を設定する*、*別のタイムソースを設定する*]ことを許可しなければならない。

15.14 TSF間TSFデータ一貫性(FPT_TDC)

15.14.1 ファミリのふるまい

分散環境において、TOEはTSFデータを他の高信頼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。

15.14.2 コンポーネントのレベル付け及び説明

図73に、本ファミリのコンポーネントのレベル付けを示す。

図73 — FPT_TDC: コンポーネントのレベル付け

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

15.14.3 FPT_TDC.1の管理

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) 予見される管理アクティビティはない。

15.14.4 FPT_TDC.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又はSTに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: TSFデータ一貫性メカニズムの成功した使用。

b) 基本: TSFデータ一貫性メカニズムの使用。

c) 基本: どのTSFデータが解釈されたかの識別。

d) 基本: 改変されたTSFデータの検出。

15.14.5 FPT_TDC.1 TSF間基本TSFデータ一貫性

コンポーネント間の関係

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。

15.15 外部エンティティのテスト(FPT_TEE)

15.15.1 ファミリのふるまい

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対してテストを実行するための要件を定義する。

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。

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。

15.15.2 コンポーネントのレベル付け及び説明

図74に、本ファミリのコンポーネントのレベル付けを示す。

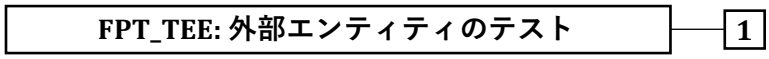


図74 — FPT_TEE: コンポーネントのレベル付け

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

15.15.3 FPT_TEE.1の管理

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、一定間隔、又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。

15.15.4 FPT_TEE.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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

15.15.5 FPT_TEE.1 外部エンティティのテスト

コンポーネント間の関係

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。

15.16 15.13 TOE内TSFデータ複製一貫性(FPT_TRC)

15.16.1 ファミリのふるまい

このファミリの要件は、TSFデータがTOE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の部分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一部が切断されると、一部分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。

15.16.2 コンポーネントのレベル付け及び説明

図75に、本ファミリのコンポーネントのレベル付けを示す。

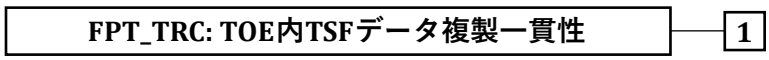


図75 — FPT_TRC: コンポーネントのレベル付け

このファミリは、1つのコンポーネント、FPT_TRC.1 TSF内一貫性だけからなり、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。

15.16.3 FPT_TRC.1の管理

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) 予見される管理アクティビティはない。

15.16.4 FPT_TRC.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

15.16.5 FPT_TRC.1 TSF内一貫性

コンポーネント間の関係

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の部分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の部分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。

15.17 TSF自己テスト(FPT_TST)

15.17.1 ファミリのふるまい

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の重要な部分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。

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)を必ずしも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実行コード又は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しも防げるとは限らないので、これらのチェックが実行される必要がある。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/又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。

15.17.2 コンポーネントのレベル付け及び説明

図76に、本ファミリのコンポーネントのレベル付けを示す。

図76 — FPT_TST: コンポーネントのレベル付け

FPT_TST.1 TSF自己テストは、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。

15.17.3 FPT_TST.1の管理

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、一定間隔、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。

15.17.4 FPT_TST.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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自己テストの完了及びそのテストの失敗。

b) 基本: TSF自己テストの実行とテストの結果。

15.17.5 FPT_TST.1 TSF自己テスト

コンポーネント間の関係

下位階層：	なし
依存性：	なし

FPT_TST.1.1

TSFは、[選択: *[割付: TSFの一部]*、*TSF*]の正常動作を実証するために、[選択: *初期立ち上げ中*、*通常運用中定期的に*、*許可利用者の要求時に*、*条件[割付: 自己テストが作動すべき条件]*下で]以下の自己テストのスイートを実行しなければならない。:[割付: *TSFが実行する自己テストのリスト*]

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 FRUクラス: 資源利用

16.1 クラスの説明

このクラスは、処理能力及び/又は格納容量など、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77は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Kは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

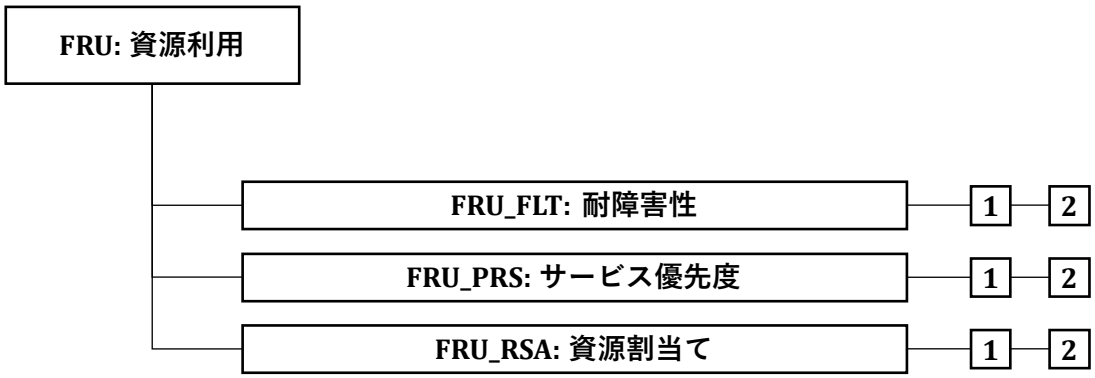


図77 — FRU: 資源利用クラスの構成

16.2 耐障害性(FRU_FLT)

16.2.1 ファミリのふるまい

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

16.2.2 コンポーネントのレベル付け及び説明

図78に、本ファミリのコンポーネントのレベル付けを示す。

図78 — FRU_FLT: コンポーネントのレベル付け

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

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

16.2.3 FRU_FLT.1、FRU_FLT.2の管理

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) 予見される管理アクティビティはない。

16.2.4 FRU_FLT.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全てのTOE機能。

16.2.5 FRU_FLT.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

16.2.6 FRU_FLT.1 機能削減された耐障害性

コンポーネント間の関係

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、次の障害[割付: *障害の種別のリスト*]が生じたとき、[割付: *TOE能力のリスト*]の動作を保証しなければならない。

16.2.7 FRU_FLT.2 制限付き耐障害性

コンポーネント間の関係

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、次の障害[割付: *障害の種別のリスト*]が生じたとき、**全てのTOE能力**の動作を保証しなければならない。

16.3 サービス優先度(FRU_PRS)

16.3.1 ファミリのふるまい

このファミリの要件は、低優先度アクティビティによって引き起こされる過度の干渉や遅延を受けることなく、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。

16.3.2 コンポーネントのレベル付け及び説明

図79に、本ファミリのコンポーネントのレベル付けを示す。

図79 — FRU_PRS: コンポーネントのレベル付け

FRU_PRS.1 制限付きサービス優先度は、サブジェクトによる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。

FRU_PRS.2 完全サービス優先度は、サブジェクトによるTSFの制御下にある全ての資源の利用に対して優先度を提供する。

16.3.3 FRU_PRS.1、FRU_PRS.2の管理

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。

16.3.4 FRU_PRS.1、FRU_PRS.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

16.3.5 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なければならないことを保証しなければならない。

16.3.6 FRU_PRS.2 完全サービス優先度

コンポーネント間の関係

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、**全ての共用可能資源**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なければならないことを保証しなければならない。

16.4 資源割当て(FRU_RSA)

16.4.1 ファミリのふるまい

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

16.4.2 コンポーネントのレベル付け及び説明

図80に、本ファミリのコンポーネントのレベル付けを示す。

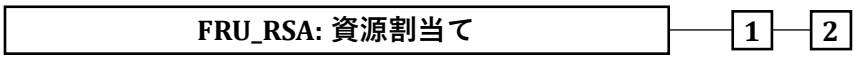


図80 — FRU_RSA: コンポーネントのレベル付け

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

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

16.4.3 FRU_RSA.1の管理

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/又は個々の利用者及び/又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。

16.4.4 FRU_RSA.2の管理

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/又は個々の利用者及び/又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。

16.4.5 FRU_RSA.1、FRU_RSA.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

16.4.6 FRU_RSA.1 最大割当て

コンポーネント間の関係

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*、*特定した期間*]使用できる、次の資源[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。

16.4.7 FRU_RSA.2 最小及び最大割当て

コンポーネント間の関係

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*、*特定した期間*]使用できる、次の資源[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*、*特定した期間*]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 FTAクラス: TOEアクセス

17.1 クラスの説明

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81は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Lは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

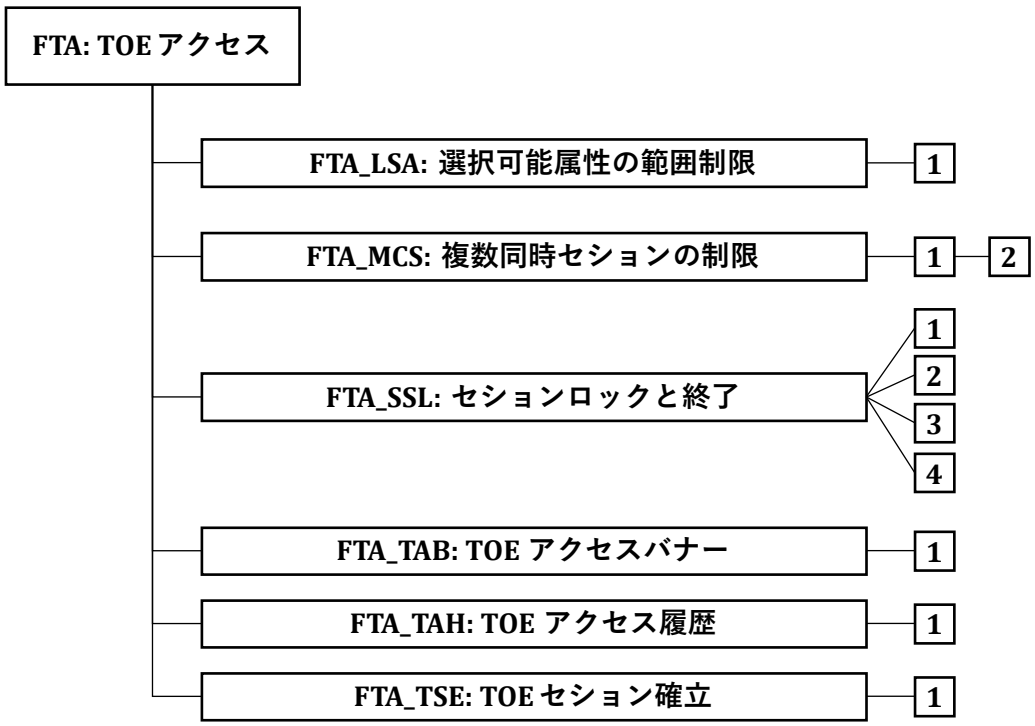


図81 — FTA: TOEアクセスクラスの構成

17.2 選択可能属性の範囲制限(FTA_LSA)

17.2.1 ファミリのふるまい

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

17.2.2 コンポーネントのレベル付け及び説明

図82に、本ファミリのコンポーネントのレベル付けを示す。

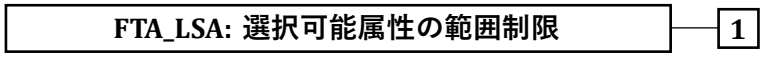


図82 — FTA_LSA: コンポーネントのレベル付け

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

17.2.3 FTA_LSA.1の管理

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。

17.2.4 FTA_LSA.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての失敗した試み。

b) 基本: セションセキュリティ属性の選択における全ての試み。

c) 詳細: 各セションセキュリティ属性の値の取得。

17.2.5 FTA_LSA.1 選択可能属性の範囲制限

コンポーネント間の関係

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。

17.3 複数同時セションの制限(FTA_MCS)

17.3.1 ファミリのふるまい

このファミリは、同一利用者に属する同時セションの数に対する制限を設ける要件を定義する。

17.3.2 コンポーネントのレベル付け及び説明

図83に、本ファミリのコンポーネントのレベル付けを示す。

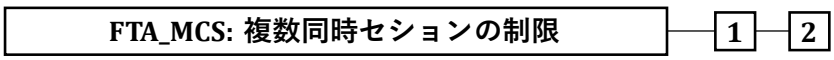


図83 — FTA_MCS: コンポーネントのレベル付け

FTA_MCS.1 複数同時セションの基本制限は、TSFの全ての利用者に適用する制限を提供する。

FTA_MCS.2 複数同時セションの利用者属性ごと制限は、関連したセキュリティ属性に基づく同時セション数の制限を特定する能力を要求することによって、FTA_MCS.1複数同時セションの基本制限を拡張する。

17.3.3 FTA_MCS.1の管理

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。

17.3.4 FTA_MCS.2の管理

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) 管理者による同時利用者セションの最大許可数を制御する規則の管理。

17.3.5 FTA_MCS.1、FTA_MCS.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

17.3.6 FTA_MCS.1 複数同時セションの基本制限

コンポーネント間の関係

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。

17.3.7 FTA_MCS.2 複数同時セションの利用者属性ごと制限

コンポーネント間の関係

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。

17.4 セションロックと終了(FTA_SSL)

17.4.1 ファミリのふるまい

このファミリは、TSF起動及び利用者起動の、対話セションのロック、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。

17.4.2 コンポーネントのレベル付け及び説明

図84に、本ファミリのコンポーネントのレベル付けを示す。

図84 — FTA_SSL: コンポーネントのレベル付け

FTA_SSL.1 TSF起動セションロックは、利用者が非アクティブである特定した時間後の、対話セションのシステム起動のロックを含む。

FTA_SSL.2 利用者起動ロックは、利用者が、利用者自身の対話セションをロック及びロック解除するための能力を提供する。

FTA_SSL.3 TSF起動による終了は、利用者が非アクティブである特定した時間後に、TSFがセションを終了させるための要件を提供する。

FTA_SSL.4 利用者起動による終了は、利用者が、利用者自身の対話セションを終了させる能力を提供する。

17.4.3 FTA_SSL.1の管理

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が発生するまでの、利用者が非アクティブである時間の特定。

b) ロックアウトが発生するまでの、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事象の管理。

17.4.4 FTA_SSL.2の管理

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事象の管理。

17.4.5 FTA_SSL.3の管理

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対話セションを終了させるまでの、利用者が非アクティブである時間の特定。

b) 対話セションを終了させるまでの、利用者が非アクティブであるデフォルト時間の特定。

17.4.6 FTA_SSL.4の管理

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) 予見される管理アクティビティはない。

17.4.7 FTA_SSL.1、FTA_SSL.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

17.4.8 FTA_SSL.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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。

17.4.9 FTA_SSL.4の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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

17.4.10 FTA_SSL.1 TSF起動セションロック

コンポーネント間の関係

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無効にする。

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。

17.4.11 FTA_SSL.2 利用者起動ロック

コンポーネント間の関係

下位階層：	なし
依存性：	FIA_UID.1 識別のタイミング

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無効にする。

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。

17.4.12 FTA_SSL.3 TSF起動による終了

コンポーネント間の関係

下位階層：	なし
依存性：	FMT_SMR.1 セキュリティの役割

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。

17.4.13 FTA_SSL.4 利用者起動による終了

コンポーネント間の関係

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。

17.5 TOEアクセスバナー(FTA_TAB)

17.5.1 ファミリのふるまい

このファミリは、利用者に対し、TOEの適切な利用に関する、設定可能な勧告的警告メッセージを表示する要件を定義する。

17.5.2 コンポーネントのレベル付け及び説明

図85に、本ファミリのコンポーネントのレベル付けを示す。

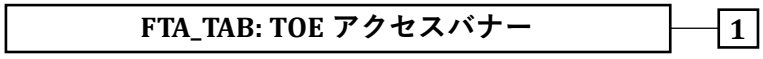


図85 — FTA_TAB: コンポーネントのレベル付け

FTA_TAB.1 デフォルトTOEアクセスバナーは、TOEアクセスバナーに対する要件を提供する。このバナーは、セションの確立のための対話に先立って表示される。

17.5.3 FTA_TAB.1の管理

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。

17.5.4 FTA_TAB.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

17.5.5 FTA_TAB.1 デフォルトTOEアクセスバナー

コンポーネント間の関係

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、[選択: *TSF*、*TOEプラットフォーム*]は、[割付: *メッセージの記述*]メッセージを表示しなければならない。

17.6 TOEアクセス履歴(FTA_TAH)

17.6.1 ファミリのふるまい

このファミリは、セション確立の成功時に、利用者のアカウントにアクセスした成功及び不成功の試みの履歴を、TSFが利用者に対して表示するための要件を定義する。

17.6.2 コンポーネントのレベル付け及び説明

図86に、本ファミリのコンポーネントのレベル付けを示す。

図86 — FTA_TAH: コンポーネントのレベル付け

FTA_TAH.1 TOEアクセス履歴は、セションを確立するための以前の試みに関連する情報をTOEが表示するための要件を提供する。

17.6.3 FTA_TAH.1の管理

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) 予見される管理アクティビティはない。

17.6.4 FTA_TAH.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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) 予見される監査対象事象はない。

17.6.5 FTA_TAH.1 TOEアクセス履歴

コンポーネント間の関係

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。

17.7 TOEセション確立(FTA_TSE)

17.7.1 ファミリのふるまい

このファミリは、TOEとセションを確立するための利用者許可を拒否する要件を定義する。

17.7.2 コンポーネントのレベル付け及び説明

図87に、本ファミリのコンポーネントのレベル付けを示す。

図87 — FTA_TSE: コンポーネントのレベル付け

FTA_TSE.1 TOEセション確立は、属性に基づき、利用者のTOEへのアクセスを拒否する要件を提供する。

17.7.3 FTA_TSE.1の管理

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。

17.7.4 FTA_TSE.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

c) 詳細: 選択されたアクセスパラメタの値の取得。

17.7.5 FTA_TSE.1 TOEセション確立

コンポーネント間の関係

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 FTPクラス: 高信頼パス/チャネル

18.1 クラスの説明

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/又はTSFによって(そのコンポーネントに対して適切に)開始されることができる。

— 通信パスは、利用者が正しいTSFと通信しているということと、TSFが正しい利用者と通信しているということの(そのコンポーネントに対して適切に)保証を提供する能力を持つ。

このパラダイムにおいて、高信頼チャネルは、チャネルのどちらの側からでも開始することができる通信チャネルであり、チャネルの両端の識別情報に関して、否認不可の性質を提供する。

高信頼パスは、利用者が、TSFとの保証された直接対話を通して機能を実行する手段を提供する。高信頼パスは、通常、最初の識別及び/又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。

高信頼チャネル及びパスを提供するために一般的に使用されている通信プロトコルの使用を記述するファミリも与えられている。

図88は、このクラス、ファミリ及びコンポーネントの構成を示す。エレメントは図に示されていない。

附属書Mは、本クラスに関する解説を提供しており、本クラスで識別されるコンポーネントを使用する際に参照するべきである。

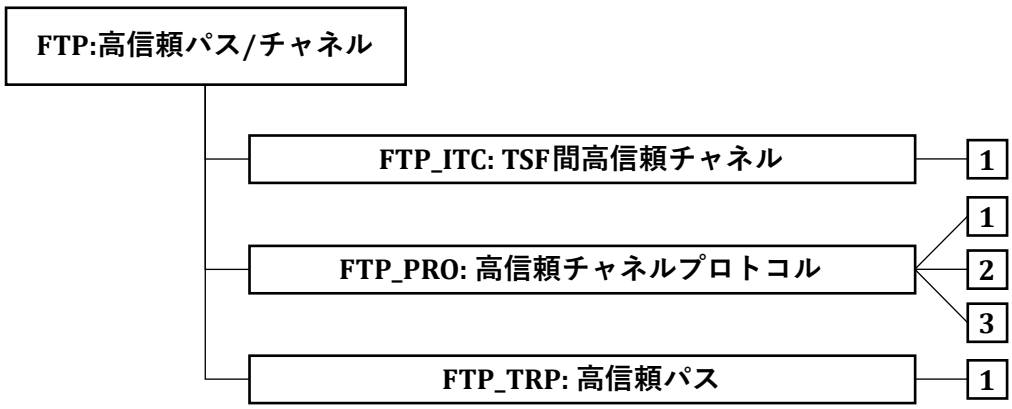


図88 — FTP: 高信頼パス/チャネルクラスの構成

18.2 TSF間高信頼チャネル(FTP_ITC)

18.2.1 ファミリのふるまい

このファミリは、セキュリティ上の重要な操作のために、TSFと他の高信頼IT製品間に高信頼チャネルを生成するための要件を定義する。このファミリのコンポーネントを、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、常に含めることができる。

18.2.2 コンポーネントのレベル付け及び説明

図89に、本ファミリのコンポーネントのレベル付けを示す。

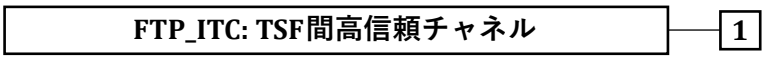


図89 — FTP_ITC: コンポーネントのレベル付け

FTP_ITC.1 TSF間高信頼チャネルは、TSFが、それ自身と他の高信頼IT製品間に高信頼通信チャネルを提供することを要求する。

18.2.3 FTP_ITC.1の管理

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。

18.2.4 FTP_ITC.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての使用の試み。

d) 基本: 全ての高信頼チャネル機能の開始者とターゲットの識別。

18.2.5 FTP_ITC.1 TSF間高信頼チャネル

コンポーネント間の関係

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。

18.3 高信頼チャネルプロトコル(FTP_PRO)

18.3.1 ファミリのふるまい

このファミリは、高信頼チャネルを確立し、TSFデータ又は利用者データを安全に転送するために高信頼チャネルを使用するための要件を定義する。

18.3.2 コンポーネントのレベル付け及び説明

図90に、本ファミリのコンポーネントのレベル付けを示す。

図90 — FTP_PRO: コンポーネントのレベル付け

FTP_PRO.1 高信頼チャネルプロトコルは、定義されたプロトコルに従って通信が確立されることを要求する。

FTP_PRO.2 高信頼チャネル確立は、相手との間で鍵が安全に確立されることを要求する。

FTP_PRO.3 高信頼チャネルのデータ保護は、転送中のデータが保護されることを要求する。

18.3.3 FTP_PRO.1の管理

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) 高信頼チャネルに必要なプロトコルの構成

b) 高信頼チャネルを使用するための認証情報の構成

c) 高信頼チャネルの初期化及び終了の条件の構成

18.3.4 FTP_PRO.2の管理

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) 共有する秘密に関するパラメタの構成

b) 暗号鍵導出のためのパラメタの構成

18.3.5 FTP_PRO.3の管理

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) 高信頼チャネルで使用される暗号化メカニズム及び完全性メカニズムの構成

18.3.6 FTP_PRO.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: 高信頼チャネル確立の失敗。

b) 最小: 失敗した高信頼チャネル確立の開始者とターゲットの識別。

c) 基本: 高信頼チャネルの全ての使用の試み。

d) 基本: 全ての高信頼チャネル試行の開始者とターゲットの識別。

その他の事象は、使用される特定のプロトコルに従って考慮されるべきである。

18.3.7 FTP_PRO.2の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: チャネル確立時の認証失敗

b) 基本: 全ての認証試行。

18.3.8 FTP_PRO.3の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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: FTP_PRO.3.2 のチャネル特性の検証試行時の失敗

18.3.9 FTP_PRO.1 高信頼チャネルプロトコル

コンポーネント間の関係

下位階層：	なし
依存性：	FTP_PRO.2 高信頼チャネル確立 FTP_PRO.3 高信頼チャネルのデータ保護

FTP_PRO.1.1

TSFは、[割付: *定義済みのプロトコル上の役割*]として動作する[割付: *高信頼チャネルプロトコル*]を、[割付: *標準のリスト*]に従って実装しなければならない。

FTP_PRO.1.2

TSFは、[割付: *高信頼チャネルの目的*]のために、[割付: *標準のリスト*]に従い、高信頼チャネルの使用を強制しなければならない。

FTP_PRO.1.3

TSFは、[選択: *自分自身*、*その相手*]が高信頼チャネルを経由して通信を開始することを許可しなければならない。

FTP_PRO.1.4

TSFは、高信頼チャネルに対して以下の規則を実施しなければならない。[割付: *高信頼チャネル及び/又はそのプロトコルの操作と使用を管理する規則*]

FTP_PRO.1.5

TSFは、以下の静的プロトコルオプションを実施しなければならない。 : **[**割付: *オプションの一覧と、それぞれが定義されている標準への参照***]**

FTP_PRO.1.6

TSFは、以下のプロトコル構成のいずれかを、その相手とネゴシエートしなければならない。 : **[**割付: *構成のリストと、それぞれが定義された標準への参照***]**

18.3.10 FTP_PRO.2 高信頼チャネル確立

コンポーネント間の関係

下位階層：	なし
依存性：	FTP_PRO.1 高信頼チャネルプロトコル [FCS_CKM.1 暗号鍵生成、又は FCS_CKM.2 暗号鍵配布] FCS_CKM.5 暗号鍵導出 FCS_COP.1 暗号操作

FTP_PRO.2.1

TSFは、以下のメカニズムの一つを使用し、相手との間で共有秘密を確立しなければならない。 : **[**割付: *鍵確立メカニズムのリスト***]**

FTP_PRO.2.2

TSFは、次のメカニズム**[**割付: *認証メカニズムのリスト***]**の一つを使用し、次の規則**[**割付: *認証を行うための規則のリスト***]**に従って、**[**選択: *その相手*、*その相手に対し自身***]**を認証しなければならない。

FTP_PRO.2.3

TSFは、**[**割付: *鍵導出関数***]**を使用して、共有秘密から以下の暗号鍵を導出しなければならない。 : **[**割付: *暗号鍵のリスト***]**

18.3.11 FTP_PRO.3 高信頼チャネルのデータ保護

コンポーネント間の関係

下位階層：	なし
依存性：	FTP_PRO.1 高信頼チャネルプロトコル FTP_PRO.2 高信頼チャネル確立 FCS_COP.1 暗号操作

FTP_PRO.3.1

TSFは、以下のメカニズムの一つを使用し、転送中のデータを不正な開示から保護しなければならない。 : **[**割付: *暗号化メカニズムのリスト***]**

FTP_PRO.3.2

TSFは、以下のメカニズムの一つを使用し、**[**選択: *改変*、*削除*、*挿入*、*リプレイ*、***[****割付: その他****]]**から転送中のデータを保護しなければならない。 : **[**割付: *完全性保護メカニズムのリスト***]**

18.4 高信頼パス(FTP_TRP)

18.4.1 ファミリのふるまい

このファミリは、利用者とTSF間に高信頼通信を確立し維持するための要件を定義する。高信頼パスは、どのようなセキュリティ関連の対話に対しても要求されるかも知れない。高信頼パス交換は、TSFとの対話の間に利用者によって開始されることもあり、高信頼パスを介してTSFが利用者との通信を確立することもある。

18.4.2 コンポーネントのレベル付け及び説明

図91に、本ファミリのコンポーネントのレベル付けを示す。

図91 — FTP_TRP: コンポーネントのレベル付け

FTP_TRP.1 高信頼パスは、PP、PPモジュール、機能パッケージ又はSTの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/又はTSFは、高信頼パスを開始する能力を持つことができる。

18.4.3 FTP_TRP.1の管理

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。

18.4.4 FTP_TRP.1の監査

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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、全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: 高信頼パス機能の全ての使用の試み。

d) 基本: もし得られれば、全ての高信頼パス呼出に関係する利用者の識別情報。

18.4.5 FTP_TRP.1 高信頼パス

コンポーネント間の関係

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: 他のタイプの完全性*、*又は機密性侵害]*]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
(参考)

セキュリティ機能要件(SFR) 適用上の注釈の構成

A.1 一般

この附属書は、この文書で定義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、この文書の本文と同様である。

A.2 注釈の構造

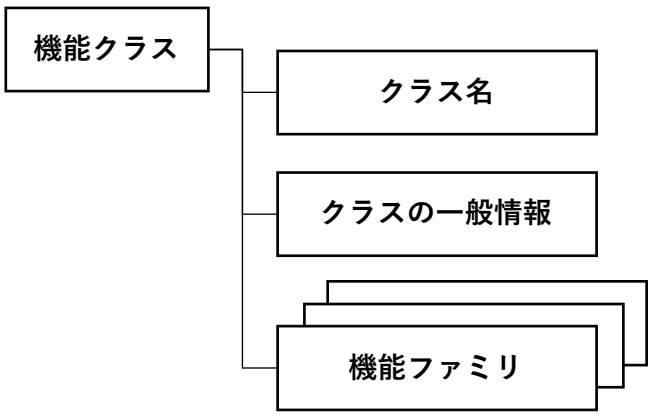
A.2.1 一般

この文書における機能要件に関係する注釈の内容と表現は、以下のように定義される。

A.2.2 クラスの構造

A.2.2.1 一般

図A.1は、この附属書における機能クラス構造を表している。



図A.1 — 機能クラス構造

注：機能クラスの中には、複数の機能ファミリを含むものがある。

A.2.2.2 クラス名

これは、この文書の規定部分で定義されたクラスの一意の名前である。

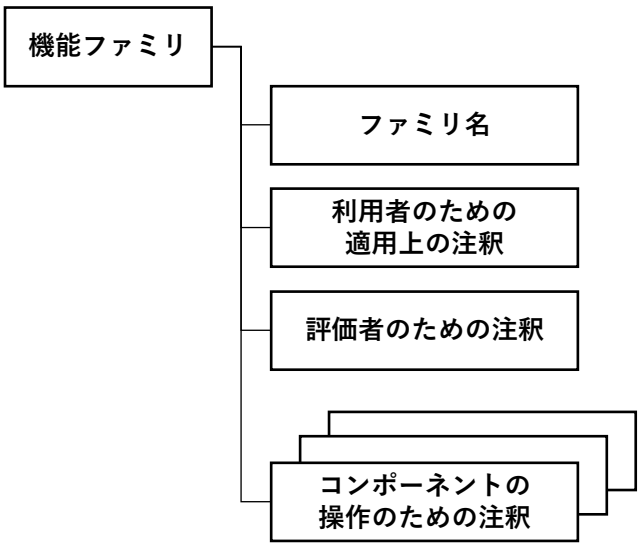
A.2.2.3 クラスの概説

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.2.3 ファミリ構造

A.2.3.1 一般

図A.2は、適用上の注釈のために、図形式で機能ファミリ構造を表したものである。



図A.2 — 適用上の注釈のための機能ファミリ構造

A.2.3.2 ファミリ名

これは、この文書の規定部分で定義されたファミリの一意の名前である。

A.2.3.3 利用者のための適用上の注釈

利用者のための注釈には、そのファミリの潜在的な利用者、つまりPP、PPモジュール、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。

注：付属書では、PP、PPモジュール、機能パッケージ又はSTの作成者という用語には、PP又はSTの作成に使用される文書の作成者が含まれ、これにはPPモジュールや機能パッケージも含まれる。

A.2.3.4 評価者のための注釈

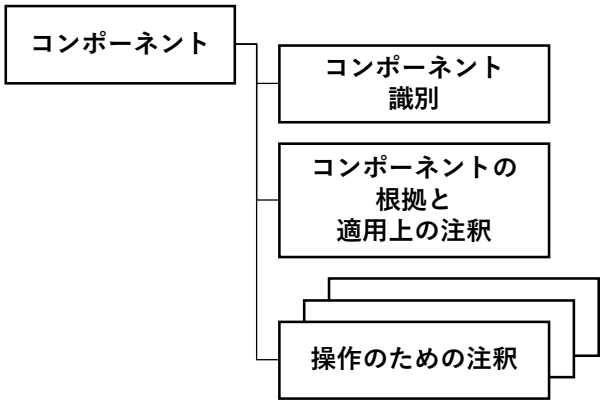
評価者のための注釈には、そのファミリのコンポーネントへの適合を主張するTOEの開発者及び評価者が関心を持つ情報が書かれる。書かれたものは参考情報であり、TOEを評価するうえで特別な注意が必要となるかもしれない様々な領域をカバーできる。これは、評価者にとって特別な関心ごとである注意や警告はもちろん、意味の明確化と要件を解釈するための方法の詳細化を含めることができる。

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.2.4 コンポーネント構造

A.2.4.1 一般

図A.3は、適用上の注釈のための機能コンポーネント構造を表す。



図A.3 — 機能コンポーネント構造

A.2.4.2 コンポーネント識別情報

これは、この文書の規定部分で定義されたコンポーネントの一意の名前である。

A.2.4.3 コンポーネントの根拠と適用上の注釈

コンポーネントに関係する、あらゆる特定の情報がコンポーネントの根拠と適用上の注釈に記載される。

コンポーネントの根拠には、特定のコンポーネントのレベルの一般的なステートメントを詳細化する情報が含まれており、レベル固有の拡充が必要な場合に使用される。

適用上の注釈は、特定のコンポーネントについて説明的に条件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.2.3節に記述した、利用者のための注釈、及び/又は評価者のための注釈に付随させることができる。適用上の注釈は、依存関係の性質を説明するために使用されることがある。

コンポーネントの根拠と適用上の注釈は、適切な場合にだけ記述される。

A.2.4.4 操作に関する注意

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。

許可された操作の項は、適切な場合にだけ記述される。

附属書B
(参考)

セキュリティ機能コンポーネントの依存性の表

B.1 依存性の表

表B.1～表B.11に、機能コンポーネント間の、階層的、直接的、間接的及びオプション的な依存関係を示す。

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、階層構造になっているか(「H」で表示)、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)、あるいはオプション的に要求されるか(「O」で表示)を示す。オプションの要件のセットは、O1やO2のように、添え字でグループ分けして表示される。

セキュリティ保証要件について依存関係が示されている場合、CCパート3を参照しなければならない。

注：選択されたオプションの要件によっては、いくつかの間接的な依存関係は適用されない。

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。

例

オプション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。

表B.1 — FAU: セキュリティ監査クラスの依存性表

	FAU_GEN.1	FAU_SAA.1	FAU_SAA.3	FAU_SAR.1	FAU_STG.1	FAU_STG.2	FAU_STG.4	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FTP_ITC.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			H										
FAU_SAR.1	X											-	

	FAU_GEN.1	FAU_SAA.1	FAU_SAA.3	FAU_SAR.1	FAU_STG.1	FAU_STG.2	FAU_STG.4	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FTP_ITC.1
FAU_SAR.2	-			X								-	
FAU_SAR.3	-			X								-	
FAU_SEL.1	X							-	X	-	-	-	
FAU_STG.1	X											-	X
FAU_STG.2	X											-	
FAU_STG.3	X					H						-	
FAU_STG.4	-					X						-	
FAU_STG.5	X					X	H					-	

表B.2 — FCO: 通信クラスの依存性表

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

表B.3 — FCS: 暗号サポートクラスの依存性表

	FCS_CKM.1	FCS_CKM.2	FCS_CKM.3	FCS_CKM.5	FCS_CGM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RBG.4	FCS_RBG.5	FCS_RNG.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_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_CKM.1	-	O[1]	X	O[1]	X	O[1]	O[2]	-	-		-	O[2]	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-
FCS_CKM.2	O[1]	-	X	O[1]	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_CKM.3	O[1]	-	-	O[1]	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_CKM.5	-	O[1]	-	-	X	O[1]	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.6	O[1]	-	-	-	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-

セキュリティ機能コンポーネントの依存性の表

	FCS_CKM.1	FCS_CKM.2	FCS_CKM.3	FCS_CKM.5	FCS_CGM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RBG.4	FCS_RBG.5	FCS_RNG.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_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_COP.1	O[2]	-	X	O[2]	-	-	-	-	-			-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_RBG.1							-	O[1]	O[1]		-													X	X			
FCS_RBG.2							X	-	-	-	-													-	-			
FCS_RBG.3							X	-	-	-	-													-	-			
FCS_RBG.4							X	-	-	-	X													-	-			
FCS_RBG.5							X	O[1]	O[1]	O[1]	-													-	-			
FCS_RBG.6							X	-	-	-	-													-	-			
FCS_RNG.1																												

表B.4 — FDP: 利用者データ保護クラスの依存性表

	FCS_CKM.1	FCS_CKM.3	FCS_CKM.5	FCS_CKM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_IFF.3	FDP_IFF.4	FDP_ITC.1	FDP_ITC.2	FDP_ITT.1	FDP_ITT.2	FDP_ITT.3	FDP_RIP.1	FDP_ROL.1	FDP_SDI.1	FDP_UIT.1	FDP_UIT.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ACC.1										-	X	-	-													-	-	-	-	-					
FDP_ACC.2										H	X	-	-													-	-	-	-	-					
FDP_ACF.1										X	-	-	-													-	-	X	-	-					
FDP_DAU.1																																		
FDP_DAU.2										H																X									
FDP_ETC.1										O[1]	-	O[1]	-													-	-	-	-	-					
FDP_ETC.2										O[1]	-	O[1]	-													-	-	-	-	-					
FDP_IFC.1										-	-	-	X													-	-	-	-	-					
FDP_IFC.2										-	-	H	X													-	-	-	-	-					
FDP_IFF.1										-	-	X	-													-	-	X	-	-					
FDP_IFF.2										-	-	X	H													-	-	X	-	-					
FDP_IFF.3										-	-	X	-													-	-	-	-	-					
FDP_IFF.4										-	-	X	-	H												-	-	-	-	-					
FDP_IFF.5										-	-	X	-		H											-	-	-	-	-					
FDP_IFF.6										-	-	X	-													-	-	-	-	-					
FDP_IRC.1																																		
FDP_ITC.1										O[1]	-	O[1]	-													-	-	X	-	-					
FDP_ITC.2										O[1]	-	O[1]	-													-	-	-	-	-			X	O[2]	O[2]

	FCS_CKM.1	FCS_CKM.3	FCS_CKM.5	FCS_CKM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_IFF.3	FDP_IFF.4	FDP_ITC.1	FDP_ITC.2	FDP_ITT.1	FDP_ITT.2	FDP_ITT.3	FDP_RIP.1	FDP_ROL.1	FDP_SDI.1	FDP_UIT.1	FDP_UIT.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ITT.1										O[1]	-	O[1]	-													-	-	-	-	-					
FDP_ITT.2										O[1]	-	O[1]	-					H								-	-	-	-	-					
FDP_ITT.3										O[1]	-	O[1]	-					X								-	-	-	-	-					
FDP_ITT.4										O[1]	-	O[1]	-						X	H						-	-	-	-	-					
FDP_RIP.1																																			
FDP_RIP.2																					H														
FDP_ROL.1										O[1]	-	O[1]	-													-	-	-	-	-					
FDP_ROL.2										O[1]	-	O[1]	-									H				-	-	-	-	-					
FDP_SDC.1																																			
FDP_SDC.2	-	-	-	-	X	-	-	-	-	-	-	-	-			-	-								-	-	-	-	-	-	-	-	-	-	-
FDP_SDI.1																																			
FDP_SDI.2																							H												
FDP_UCT.1										O[2]	-	O[2]	-													-	-	-	-	-				O[1]	O[1]
FDP_UIT.1										O[2]	-	O[2]	-													-	-	-	-	-				O[1]	O[1]
FDP_UIT.2										O[1]	-	O[1]	-											O[2]		-	-	-	-	-				O[2]	-
FDP_UIT.3										O[1]	-	O[1]	-											O[2]	H	-	-	-	-	-				O[2]	-

表B.5 — FIA: 識別と認証クラスの依存性表

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_AFL.1		X	-
FIA_API.1			
FIA_ATD.1			
FIA_SOS.1			
FIA_SOS.2			
FIA_UAU.1			X
FIA_UAU.2		H	X
FIA_UAU.3			
FIA_UAU.4			
FIA_UAU.5			
FIA_UAU.6			
FIA_UAU.7		X	-
FIA_UID.1			
FIA_UID.2			H
FIA_USB.1	X		

表B.6 — FMT: セキュリティ管理クラスの依存性表

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

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_SAE.1					-							X	X
FMT_SMF.1													
FMT_SMR.1					X								
FMT_SMR.2					X							H	
FMT_SMR.3					-							X	

表B.7 — FPR: プライバシークラスの依存性表

	FIA_UID.1	FPR_ANO.1	FPR_PSE.1	FPR_UNO.1
FPR_ANO.1				
FPR_ANO.2		H		
FPR_PSE.1				
FPR_PSE.2	X		H	
FPR_PSE.3			H	
FPR_UNL.1				
FPR_UNO.1				
FPR_UNO.2				H
FPR_UNO.3				X
FPR_UNO.4				

表B.8 — FPT: TSF保護クラスの依存性表

	AGD_OPE.1	ADV_FSP.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_SMF.1	FMT_SMR.1	FPT_ITI.1	FPT_ITT.1	FTP_PHP.1	FPT_RCV.1	FPT_RCV.2	FPT_SSP.1	FPT_STM.1
FPT_EMS.1														
FPT_FLS.1														
FPT_INI.1														
FPT_ITA.1														
FPT_ITC.1														

	AGD_OPE.1	ADV_FSP.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_SMF.1	FMT_SMR.1	FPT_ITI.1	FPT_ITT.1	FTP_PHP.1	FPT_RCV.1	FPT_RCV.2	FPT_SSP.1	FPT_STM.1
FPT_ITI.1														
FPT_ITI.2								H						
FPT_ITT.1														
FPT_ITT.2									H					
FPT_ITT.3									X					
FPT_PHP.1														
FPT_PHP.2				X	-					H				
FPT_PHP.3														
FPT_RCV.1	X	-												
FPT_RCV.2	X	-									H			
FPT_RCV.3	X	-										H		
FPT_RCV.4														
FPT_RPL.1														
FPT_SSP.1									X					
FPT_SSP.2									X				H	
FPT_STM.1														
FPT_STM.2			-				X							X
FPT_TDC.1														
FPT_TEE.1														
FPT_TRC.1									X					
FPT_TST.1														

注：AGD及びADVクラスとその依存関係はCCパート3に記載されている。

表B.9 — FRU: 資源利用クラスの依存性表

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

	FPT_FLS.1	FRU_FLT.1	FRU_PRS.1	FRU_RSA.1
FRU_PRS.1				
FRU_PRS.2			H	
FRU_RSA.1				
FRU_RSA.2				H

表B.10 — FTA: TOEアクセスクラスの依存性表

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

表B.11 — FTP: 高信頼パス/チャネルクラスの依存性表

	FCS_CKM.1	FCS_CKM.2	FCS_CKM.3	FCS_CKM.5	FCS_CKM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RNG.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_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1	FTP_PRO.1	FTP_PRO.2	FTP_PRO.3
FTP_ITC.1																													
FTP_PRO.1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		X	X
FTP_PRO.2	O[1]	O[1]	-	X	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X		
FTP_PRO.3	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	
FTP_TRP.1																													

附属書C
(規定)

FAUクラス：セキュリティ監査 — 適用上の注釈

C.1 一般

C.1.1 監査要件に関する一般情報

CC監査ファミリは、PP、PPモジュール、機能パッケージ又はSTの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、直接的であれ、間接的であれ、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。

例1

直接的なフォーマットの例は、人間が読めるフォーマットで監査証跡を保存することである。

間接的なフォーマットの例は、監査分類整理ツールを使うことである。

セキュリティ監査要件の作成時、PP、PPモジュール、機能パッケージ又はSTの作成者は、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2

セキュリティ関連の事象を全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監査機能。

C.1.2 分散環境での監査要件

ネットワーク及びその他の大規模システムに対する監査要件の実装は、スタンドアロンシステムで必要とされるものと大きく異なることがある。システムがより大きく、より複雑かつアクティブになるほど、収集するものの解釈が(あるいは、格納することすら)難しくなるので、どの監査データを集めるか、それをどう管理する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、記録のセットあるいは「証跡」という従来の概念は、多数の恣意的な事象が同時に発生するグローバルな非同期ネットワークには必ずしも適用できない。

また、分散TOEの異なるホストやサーバは、異なる命名方針や値を持つかもしれない。さらに、監査レビューのためのシンボリック名は、冗長さと「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。

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、通常、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)が必要である。

最後に、許可利用者による権限の悪用は、管理者のアクションに関連する監査データのローカルな格納を体系的に避けることによって対処することができる。

C.2 セキュリティ監査自動応答(FAU_ARP)

C.2.1 利用者のための適用上の注釈

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、警報又はTSFアクション(自動応答)の要件を含めることができる。

例

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。

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る場合、「セキュリティ侵害の可能性」と定義される。

C.2.2 FAU_ARP.1 セキュリティアラーム

C.2.2.1 コンポーネントの根拠と適用上の注釈

警報の事象において、1つ以上の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。

これらのアクションは、許可利用者に警報を通知したり、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、あるいは許可利用者が修正アクションを取るためのオプションを提示することが含まれる。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

C.2.2.2 操作

FAU_ARP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

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、このリストでは、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)

C.3.1 一般

C.3.1.1 利用者のための適用上の注釈

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が生成しなければならない監査事象を特定するための要件を含む。

このファミリは、監査サポートを要求する全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、PPモジュール、機能パッケージ又はSTの作成者がPP、PPモジュール、機能パッケージ又はSTを組み立てる際、監査領域に書かれた事項がこれらのコンポーネントの変数を完成させるのに使われる。このように、ある機能領域に対して何が監査され得るかの詳細は、その機能領域においてローカライズされる。

監査対象事象のリストは、全面的にPP、PPモジュール、機能パッケージ又は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全てPP、PPモジュール、機能パッケージ又は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、PPモジュール、機能パッケージ又はSTの作成者に提供する。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:

例1

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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全ての試み。

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を除き、属性の新しい値は保存されるべきである。

注：機密属性データ項目には、パスワードや暗号鍵が含まれる。

選択した機能コンポーネントごとに、そのコンポーネントで指定されている監査対象事象は、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。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。

監査対象事象の分類(最小、基本、詳細)は、この順序で階層的であることに注意しなければならない。

これは以下のことを意味する:

— 例えば、「最小監査生成」が必要とされる場合、「最小」で識別される全ての監査対象事象は、適切な割付操作を使用してPP、PPモジュール、機能パッケージ又はSTに含まれるべきである。

— 例えば、「基本監査生成」が必要とされる場合、「最小」又は「基本」のどちらかに識別される全ての監査対象事象は、適切な割付操作を使用してPP、PPモジュール、機能パッケージ又は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な場合は、全ての識別された監査対象事象(「最小」、「基本」及び「詳細」)をPP、PPモジュール、機能パッケージ又はSTに含めるべきである。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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2

例えば、他のPP、PPモジュール、機能パッケージ又は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、PPモジュール、機能パッケージ又はSTは「最小」監査機能だけを要求することがある。

監査対象事象を生成する機能性は、PP、PPモジュール、機能パッケージ又はSTにおいて、機能要件として特定されるべきである。

例3

以下は、各PP、PPモジュール、機能パッケージ又はSTの機能コンポーネント内で監査対象と定義できる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又は取消し

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/又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、USBメモリ)

C.3.1.2 評価者のための注釈

FAU_GEN.1.1は、FPT_STM.1タイムスタンプ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、PP、PPモジュール、機能パッケージ又はSTの作成者によって、この依存性の削除を正当化し得る。

C.3.2 FAU_GEN.1 監査データ生成

C.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、監査記録が生成されるべき監査対象事象及び監査記録の中で提供される情報を識別するための要件を定義する。

FAU_GEN.1監査データ生成自体は、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に使用できる。これは、PP、PPモジュール、機能パッケージ又は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なければならない場合は、FAU_GEN.2利用者識別情報の関連付けをFAU_GEN.1に追加して使用することができる。

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されていない。したがって、無効なログインの場合は、主張された利用者識別情報を記録すべきである。それは記録された識別情報が認証されていない場合を示すかどうかも考慮すべきである。

C.3.2.2 操作

FAU_GEN.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、PP、PPモジュール、機能パッケージ又は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」、又は「指定なし」のうちの1つである。

FAU_GEN.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FAU_GEN.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、PP、PPモジュール、機能パッケージ又は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、又は「なし」のどちらかの割付をすべきである。

C.3.3 FAU_GEN.2 利用者識別情報の関連付け

C.3.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、個々の利用者識別情報のレベルに対して監査対象事象の内容をどこまでとるべきかの要件に対応する。このコンポーネントは、FAU_GEN.1監査データ生成に追加する形で使われるべきである。

監査とプライバシー要件の間には、潜在的な対立が存在する。監査の目的のためには、誰がアクションを実行したのかを知ることが望ましいかもしれない。利用者は、彼/彼女のアクションを自分だけにとどめて、他人(例えば、求人側)に識別されたくないかもしれない。また、利用者識別情報を保護すべきであることが組織のセキュリティ方針で要求されているかもしれない。このような場合、監査とプライバシーに対するセキュリティ対策方針は互いに矛盾することがある。そのため、もしこの要件が選択され、かつプライバシーが重要であるならば、利用者の偽名性のコンポーネントを含めることを考慮すべきである。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。

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は主張された利用者識別情報を記録すべきである。それは記録された識別情報が認証されていない場合を示すものとして考慮すべきである。

C.3.3.2 操作

このコンポーネントに対して特定の操作は存在しない。

C.4 セキュリティ監査分析(FAU_SAA)

C.4.1 利用者のための適用上の注釈

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、侵入検知や、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ができる。

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。

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。

C.4.2 FAU_SAA.1 侵害の可能性の分析

C.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、その発生又は累積発生がSFR実施の侵害の可能性を示す監査対象事象のセットと、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。

C.4.2.2 操作

FAU_SAA.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、その発生又は累積発生が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。

FAU_SAA.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、ある期間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。

例

期間：1日の時間帯、存続時間など。

C.4.3 FAU_SAA.2 プロファイルに基づく異常検出

C.4.3.1 コンポーネントの根拠と適用上の注釈

*プロファイル*とは、利用者及び/又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確立される。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は、*プロファイル尺度*と呼ばれる。

例1

使用パターン：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。

プロファイル尺度：資源の量、事象カウンタ、タイマ。

各プロファイルは、*プロファイルの対象グループ*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)、あるいは類似した対象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。プロファイルの対象グループは、TSFと対話する一人又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確立するのに使われる。以下は、プロファイルの対象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又はグループアカウント**: 同一のグループIDを所有するか、又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

プロファイルの対象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、確立した使用パターンに対して、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。

異常検出ツールをどこまで精巧にするかは、主に、PP、PPモジュール、機能パッケージ又はSTが要求するプロファイルの対象グループの数と、要求されるプロファイル尺度の複雑さによって、決定される。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又は分析されるべきかを、具体的に列挙すべきである。また、そのアクティビティに関連するどのような情報が使用プロファイルの構築に必要なのかを、具体的に識別すべきである。

FAU_SAA.2プロファイルに基づく異常検出は、TSFがシステム利用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、プロファイルの対象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、使用状況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、PPモジュール、機能パッケージ又はSTの作成者によって定義されるということが重要である。

例2

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できる。

異常なアクティビティは、非異常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ヶ月前には異常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異常でなくなることも(その逆も)ある。もしプロファイル更新アルゴリズムに異常なアクティビティが入らないようにしてしまうと、TSFは、このような概念のものを捕らえることができなくなろう。

許可利用者が疑惑率の重大性を理解できるよう、管理上の告知が提供されるべきである。

PP、PPモジュール、機能パッケージ又はSTの作成者は、疑惑率をどのように解釈するか、及び異常な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。

C.4.3.2 操作

FAU_SAA.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、プロファイルの対象グループを特定すべきである。1つのPP、PPモジュール、機能パッケージ又はSTは、複数のプロファイル対象グループを含むことができる。

FAU_SAA.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFによって異常な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異常なアクティビティの種別に基づいてもよい。

C.4.4 FAU_SAA.3 単純攻撃の発見

C.4.4.1 コンポーネントの根拠と適用上の注釈

実際のところ、セキュリティ侵害が切迫していることを分析ツールが確信を持って検出できることは、よくても稀でしかない。しかしながら、重要であるために、常に単独で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。

例1

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。

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、PPモジュール、機能パッケージ又はSTの作成者が定義する割付に大きく依存しよう。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、その事象が特徴的事象に対応づけされるかどうかを決定するために、その事象に関係するどのような情報が必要なのかを、具体的に識別すべきである。

許可利用者が、事象の重要性及びとり得る適切な対応を理解できるような管理上の通知が提供されるべきである。

システムのアクティビティを監視する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知ツールがすでに開発されていることを踏まえて行われたものである。

例2

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。

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知コンポーネントを開発することができる。

C.4.4.2 操作

FAU_SAA.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、他の全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。

FAU_SAA.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PP

モジュール、機能パッケージ又はSTの作成者は、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.4.5 FAU_SAA.4 複合攻撃の発見

C.4.5.1 コンポーネントの根拠と適用上の注釈

実際のところ、セキュリティ侵害が切迫していることを分析ツールが確信を持って検出できることは、よくても稀でしかない。しかしながら、重要であるために、常に単独で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。

例1

そのような事象の例として、鍵となるTSFセキュリティデータファイル(例えばパスワードファイル)の削除や、管理特権を取得しようとするリモート利用者といったアクティビティがあげられる。

これらの事象は、その他のシステムアクティビティと区分され、その発生が侵入アクティビティを示唆している、特徴的事象と呼ばれる。事象シーケンスとは、侵入アクティビティを示しているかもしれない、順序付けられた特徴的事象のセットである。

与えられるツールの複雑さは、特徴的事象及び事象シーケンスの基本セットの識別においてPP、PPモジュール、機能パッケージ又はSTの作成者が定義する割付に大きく依存しよう。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、その事象が特徴的事象に対応づけされるかどうかを決定するために、その事象に関係するどのような情報が必要なのかを、具体的に識別すべきである。

許可利用者が、事象の重要性及びとり得る適切な対応を理解できるような管理上の通知が提供されるべきである。

システムのアクティビティを監視する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知ツールがすでに開発されていることを踏まえて行われたものである。

例2

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。

そのため、PP、PPモジュール、機能パッケージ又はSTの作成者は、システムアクティビティを監視するのに使用する入力データの種別を特定することによって、レベル付けをする必要がある。

FAU_SAA.4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知コンポーネントを開発することができる。

C.4.5.2 操作

FAU_SAA.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、その発生が既知の侵入シナリオを表すシステム事象のシーケンスリストの基本セットを識別すべきである。これらの事象シーケンスは、既知の侵入シナリオを表す。システム事象が実行されると

きにそれらが既知の侵入事象シーケンスに結合(対応づけ)できるよう、シーケンスの中に表わされる各事象は、監視されるシステム事象に対応付けられるべきである。

FAU_SAA.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、他の全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。

FAU_SAA.4.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、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)

C.5.1 利用者のための適用上の注釈

セキュリティ監査レビューファミリは、監査情報のレビューに関連する要件を定義する。

以下の機能は、格納前あるいは格納後の監査選択を許可すべきである:

例

監査情報のレビューに関連する要件の例として、次のような選択的にレビューする能力がある。

— 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又は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全て、あるいは

— 特定のSFR属性に関連付けられるアクション

各監査レビューの区別は機能性に基づく。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、and/or)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。

C.5.2 FAU_SAR.1 監査レビュー

C.5.2.1 コンポーネントの根拠と適用上の注釈

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。

このコンポーネントは、利用者及び/又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も用いられる。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。

表示可能な監査記録の内容を特定することができる。

C.5.2.2 操作

FAU_SAR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、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。

FAU_SAR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

その例として、「全て」、「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全ての情報」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。「全て」又は「全ての監査情報」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。

C.5.3 FAU_SAR.2 限定監査レビュー

C.5.3.1 コンポーネントの根拠と適用上の注釈

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。

C.5.3.2 操作

このコンポーネントに対して特定の操作は存在しない。

C.5.4 FAU_SAR.3 選択可能監査レビュー

C.5.4.1 コンポーネントの根拠と適用上の注釈

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、「and」あるいは「or」)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能力を提供すべきである。

例

監査データを扱う手段には、並べ替えやフィルタリングが含まれる。

C.5.4.2 操作

FAU_SAR.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFから監査データの選択、及び/又は、並べ替えの能力が必要かどうかを指定すべきである。

FAU_SAR.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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/又は場所」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)

C.6.1 利用者のための適用上の注釈

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。

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。

C.6.2 FAU_SEL.1 選択的監査

C.6.2.1 コンポーネントの根拠と適用上の注釈

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。

個々の利用者識別情報の存在は、このコンポーネントでは想定されない。これは、TOEとして、ルータのような利用者についての認識を持たないかもしれないものを認める。

分散環境に対しては、監査されるべき事象の選択基準として、ホスト識別情報を使用することができる。

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

C.6.2.2 操作

FAU_SEL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、監査の選択性が基づく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。

FAU_SEL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、監査の選択性が基づくあらゆる追加属性を特定すべきである。監査の選択性が基づく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 セキュリティ監査データ格納(FAU_STG)

C.7.1 FAU_STG.1 監査データ格納場所

C.7.1.1 コンポーネントの根拠と適用上の注釈

分散環境において、監査証跡の場所は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、PPモジュール、機能パッケージ又はSTの作成者は、監査記録を監査証跡に格納する前に、その記録の発信者の認証、あるいは記録の発信元の否認不可を要求することができる。

TSFは、許可されない削除や改変から監査証跡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。

FAU_STG.1.1は、FTP_ITC.1 TSF間高信頼チャネルに依存している。「外部のITエンティティ(FTP_ITCに従った高信頼チャネルを使用して生成された監査データを送信する)」が選択されない場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、それがなぜ選択されないかを説明する根拠を提供することにより依存性を満たすことができる。

C.7.1.2 操作

FAU_STG.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、監査データの保存場所を選択するべきである。監査データは、TOE自体に保存されるか、高信頼チャネルを使用して外部エンティティに送信されるか、又は他の保存オプションを割付で特定することができる。

もし、PP、PPモジュール、機能パッケージ又はSTの作成者が、監査データの、追加又は代替の保存場所を指定する必要がある場合、この要件は、FAU_STG.1.1 で選択内の割付を使用して特定できる。

C.7.2 FAU_STG.2 保護された監査データ格納

C.7.2.1 コンポーネントの根拠と適用上の注釈

分散環境において、監査証跡の場所は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、PPモジュール、機能パッケージ又はSTの作成者は、監査記録を監査証跡に格納する前に、その記録の発信者の認証、あるいは記録の発信元の否認不可を要求することができる。

TSFは、許可されない削除や改変から監査証跡に格納された監査データを保護する。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。

C.7.2.2 操作

FAU_STG.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、監査証跡に格納された監査データに対する改変を、TSFが防止しなければならないかあるいは検出だけをしなければならない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。

C.7.3 FAU_STG.3 監査データ可用性の保証

C.7.3.1 コンポーネントの根拠と適用上の注釈

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

分散環境において、監査証跡の場所は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、PPモジュール、機能パッケージ又はSTの作成者は、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。

C.7.3.2 操作

FAU_STG.3.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

数値尺度の例として、100,000件の監査記録を格納できることを示す「100,000」などがある。

FAU_STG.3.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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なけれ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。

C.7.4 FAU_STG.5[vi] 監査データ損失の防止

C.7.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、監査証跡が一杯になった場合のTOEのふるまいを特定する: 監査記録が無視される、あるいは監査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。

C.7.4.2 操作

FAU_STG.5.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FAU_STG.5.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

C.7.5 FAU_STG.4[vii] 監査データ消失の恐れ発生時のアクション

C.7.5.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、事前に定義してある所定の限界値を監査証跡が超えた場合にとられるアクションを要求する。

C.7.5.2 操作

FAU_STG.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、あらかじめ定義された限界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、PPモジュール、機能パッケージ又はSTの作成者は、この限界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。

例

許可利用者に限界値を定義させる場合、割付は、例えば「許可利用者が限界値を設定する」のように書ける。

FAU_STG.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

附属書D
(規定)

FCOクラス：通信 — 適用上の注釈

D.1 一般

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。

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、又は事前に定義された一連の属性種別を含めることもできる。

「受信証明(proof of receipt)」及び「発信証明(proof of origin)」という用語は、文献ではよく使われている。しかし、「証明(proof)」という用語は、正式には数学上の理論的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。

D.2 発信の否認不可(FCO_NRO)

D.2.1 利用者のための適用上の注釈

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。

例1

発信の証拠としては、ディジタル署名がある。

もし情報又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、発信の証拠の検証が失敗するかもしれない。そのため、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTに含めることを考慮すべきである。

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及び/又は他のサブジェクトである。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である。

例2

発信の証拠を要求するサブジェクト：受信者あるいは調停者などの第三者。

証拠の提供先となるサブジェクト：公証人

PP、PPモジュール、機能パッケージ又はSTの作成者は、証拠の有効性を検証するのに満たさなければならない条件を特定しなければならない。

例3

特定される条件の例は、証拠の検証は24時間以内にされなければならない、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。

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、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、このクラスを含めるのが適切かどうか、あるいは伝送サービスプロバイダの識別情報あるいはホストの識別情報が使用されるべきかどうかを考慮しなければならない。

利用者の識別情報に加えて(あるいはその代わりに)、PP、PPモジュール、機能パッケージ又はSTの作成者は、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4

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(発信時刻)を提供するようカスタマイズすることができる。

D.2.2 FCO_NRO.1 発信の選択的証明

D.2.2.1 利用者のための適用上の注釈

このコンポーネントには、ユーザー適用上の注釈は指定されていない。

D.2.2.2 操作

FCO_NRO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、発信機能の証拠の対象となる情報の種別を記入すべきである。

例1

情報の種別の例として、「電子メールメッセージ」がある。

FCO_NRO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例2

第三者とは、調停者、裁判官、法的機関がなり得る。

FCO_NRO.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、情報にリンクしなければならない属性のリストを記入すべきである。

例3

属性には、発信者識別情報、発信時刻、発信場所が含まれる。

FCO_NRO.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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4

制限の例としては、「証拠は24時間の範囲内でだけ検証できる」がある。

「直ちに」や「無制限」を割り付けることは許される。

FCO_NRO.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

D.2.3 FCO_NRO.2 発信の強制的証明

D.2.3.1 利用者のための適用上の注釈

このコンポーネントには、ユーザー適用上の注釈は指定されていない。

D.2.3.2 操作

FCO_NRO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、発信機能の証拠の対象となる情報の種別を記入すべきである。

例1：電子メールメッセージ。

FCO_NRO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRO.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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2：証拠は24時間の範囲内でだけ検証できる。

「直ちに」や「無制限」を割り付けることは許される。

FCO_NRO.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例3：第三者とは、調停者、裁判官、法的機関がなり得る。

D.3 受信の否認不可(FCO_NRR)

D.3.1 利用者のための適用上の注釈

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。

例1：受信の例としてはディジタル署名がある。

情報が受信されたという証拠の提供は、必ずしも情報が読まれた、あるいは理解されたことを意味せず、単に配信されたことを示すことに注意すべきである。

もし情報又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、元の情報に関する受信の証拠の検証が失敗するかもしれない。そのため、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTに含めることを考慮すべきである。

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、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、発信の証拠の提供先となる受信者及び/又は他のサブジェクトである。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。

例2：受信者又はサブジェクトは公証人でありうる。

PP、PPモジュール、機能パッケージ又はSTの作成者は、証拠の有効性を検証するのに満たさなければならない条件を特定しなければならない。

例3

特定される条件の例は、証拠の検証は24時間以内にされなければならない、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。

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、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、このクラスを含めるのが適切かどうか、あるいは伝送サービスプロバイダの識別情報あるいはホストの識別情報が使用されるべきかどうかを考慮しなければならない。

利用者識別情報に加えて(あるいはその代わりに)、PP、PPモジュール、機能パッケージ又はSTの作成者は、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4：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(受信時刻)を提供するようカスタマイズすることができる。

D.3.2 FCO_NRR.1 受信の選択的証明

D.3.2.1 利用者のための適用上の注釈

このコンポーネントには、ユーザー適用上の注釈は指定されていない。

D.3.2.2 操作

FCO_NRR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、受信機能の証拠の対象となる、例えば電子メールメッセージなどの、情報の種別を記入すべきである。

FCO_NRR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：第三者とは、調停者、裁判官、法的機関がなり得る。

FCO_NRR.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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できるなど。「直ちに」や「無制限」を割り付けることは許される。

FCO_NRR.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

D.3.3 FCO_NRR.2 受信の強制的証明

D.3.3.1 利用者のための適用上の注釈

このコンポーネントには、ユーザー適用上の注釈は指定されていない。

D.3.3.2 操作

FCO_NRR.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、受信機能の証拠の対象となる情報の種別を記入すべきである。

例1：電子メールメッセージ。

FCO_NRR.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、情報にリンクしなければならない属性のリストを記入すべきである。

例2：受信者識別情報、受信時刻、受信場所。

FCO_NRR.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FCO_NRR.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。「直ちに」や「無制限」を割り付けることは許される。

例3：証拠は24時間の範囲内でだけ検証できる。

FCO_NRR.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、法的機関がなり得る。

附属書E
(規定)

FCSクラス：暗号サポート ― 適用上の注釈

E.1 一般

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。これらには次のものが含まれるが、必ずしもこれだけに限定されない。

― 識別と認証

― 否認不可

― 高信頼パス

― 高信頼チャネル

― 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/又はソフトウェアにおいて行われる。

FCS: 暗号サポートクラスは、暗号鍵管理(FCS_CKM)、暗号操作(FCS_COP)、ランダムビット生成(FCS_RBG)及び乱数生成(FCS_RNG)の4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し、ランダムビット生成(FCS_RBG)ファミリはランダムビット生成に関する要件を提供し、乱数生成(FCS_RNG)は乱数が定められた品質尺度を満たすかの保証に関連する。

TOEで実装する暗号鍵生成方法ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者は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。

TOEで実装する暗号鍵配付方法ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者は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。

TOEで実装する暗号鍵アクセス方法ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者はFCS_CKM.3暗号鍵アクセスを選択すべきである。

TOEで実装する暗号鍵導出方法ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者はFCS_CKM.5暗号鍵導出のコンポーネントを選択すべきである。

TOEで実装する暗号鍵破棄方法ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者はFCS_CKM.6暗号鍵破棄のタイミング及びイベントのコンポーネントを選択すべきである。

TOEで実行する暗号操作(ディジタル署名、データ暗号化、鍵交換、セキュアハッシュなど)ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者はFCS_COP.1暗号操作のコンポーネントを選択すべきである。

TOEで実装する決定論的ランダムビット生成サービスごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者はFCS_RBG.1ランダムビット生成(RBG)のコンポーネントを選択すべきである。

TOEが使用する外部シード源ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RBG.2ランダムビット生成(外部シード)コンポーネントを選択すべきである。

TOEが使用する(単一の)内部シード源ごとに、もしあれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RBG.3ランダムビット生成(内部シード - 単一ソース)コンポーネントを選択すべきである。

(複数の)内部シード源が特定される場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RBG.4ランダムビット生成(内部シード - 複数ソース)コンポーネントを選択すべきである。

TOEがエントロピー源を結合する場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RBG.5ランダムビット生成(ノイズ源の結合)コンポーネントを特定すべきである。

TOEが実装するランダムビット生成サービスごとに、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RBG.6ランダムビット生成サービスコンポーネントを特定すべきである。

TOEが実装する乱数生成サービスごとに、PP、PPモジュール、機能パッケージ又はSTの作成者は、FCS_RNG.1乱数生成コンポーネントを特定すべきである。

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なけれ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の暗号機能性についての保証が消費者によって求められるときに使用されるべきである。

E.2 暗号鍵管理(FCS_CKM)

E.2.1 利用者のための適用上の注釈

暗号鍵は、その寿命全体を通して管理される必要がある。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)、鍵の生成又は導出、配付、登録、格納、アクセス及び破棄がある。

例1

— バックアップ

— エスクロー

— アーカイブ

— 回復

TOEは全ての鍵のライフサイクルの段階に常に関与するとは限らないので、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2：TOEは、暗号鍵の生成と配付だけを行うかもしれない。

このファミリは、暗号鍵のライフサイクルをサポートすることを意図し、その結果として以下のアクティビティに対する要件を定義する。

— 暗号鍵生成

— 暗号鍵導出

— 暗号鍵配付

— 暗号鍵アクセス

— 暗号鍵破棄

このファミリは、暗号鍵の管理に対する機能要件が存在する場合は、必ず含まれるべきである。

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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)全ての機密上の重要情報を除き、暗号鍵及びパラメタの値を含むことができる。

典型的に、暗号鍵を生成するために乱数が使われる。この場合、FIA_SOS.2 TSF秘密生成コンポーネントの代わりに、FCS_CKM.1暗号鍵生成が使用されるべきである。暗号鍵生成以外の目的で乱数生成が要求される場合、FIA_SOS.2 TSF秘密生成コンポーネントが使用されるべきである。

E.2.2 評価者のための注釈

評価者は、FCS_CKM.5 で特定される標準の使用に関する情報として、CCパート1のB.4を参照するべきである。

FCS_CKM.5はFCS_CKM.6に依存する。この依存性は(1)鍵導出鍵の破棄及び(2)導出された鍵の破棄の2方面の依存関係として理解されるべきである。評価者は、2方面の依存関係を満たさなければならないことを念頭に置き、鍵の機密性を保持するために破棄されるべき中間値(鍵の確立からの値など)も考慮すべきである。

E.2.3 FCS_CKM.1 暗号鍵生成

E.2.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、暗号鍵長と暗号鍵の生成に使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。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。

例：方法の例として、アルゴリズムがある。

E.2.3.2 操作

FCS_CKM.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、使用する暗号鍵生成アルゴリズムを特定すべきである。

FCS_CKM.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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目的に適切であるべきである。

FCS_CKM.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

E.2.4 FCS_CKM.2 暗号鍵配付

E.2.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、暗号鍵を配付するのに使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。PP、PPモジュール、機能パッケージ又はSTにおける標準の使用については、CCパート1を参照すること。

E.2.4.2 操作

FCS_CKM.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、使用する暗号鍵の配付方法を規定すべきである。

FCS_CKM.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

E.2.5 FCS_CKM.3 暗号鍵アクセス

E.2.5.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEの外部における暗号鍵の使用(バックアップ、アーカイブ、エスクロー、回復など)に関する要件を特定することを目的としており、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。

FCS_CKM.3 暗号鍵アクセスは、暗号鍵のアクセス制御の要件の特定を目的としていない。

E.2.5.2 操作

FCS_CKM.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、使用する暗号鍵アクセスの種別を特定すべきである。

例：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、暗号鍵回復がある(ただし、これらに限定されない)。

FCS_CKM.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、使用する暗号鍵に対するアクセス方法を特定すべきである。

FCS_CKM.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

E.2.6 FCS_CKM.5 暗号鍵導出

E.2.6.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、特定された種別の鍵の鍵導出に関連する方法とパラメタの仕様を要求するものである。

FCS_CKM.5はFCS_CKM.6に依存する。この依存性は(1)鍵導出鍵の破棄及び(2)導出された鍵の破棄の2方面の依存関係として理解されるべきである。PP、PPモジュール、機能パッケージ又はSTの作成者は、2方面の依存関係を満たさなければならないことを念頭に置き、鍵の機密性を保持するために破棄されるべき中間値(鍵の確立からの値など)も考慮すべきである。

E.2.6.2 操作

このコンポーネントに対して特定の操作は存在しない。

E.2.7 FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

E.2.7.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、暗号鍵長と暗号鍵の生成に使用する方法を特定することを要求するが、これは、割り付けられた標準に準拠することでよい。

暗号鍵及び鍵材料の破棄の目的は、それらの危殆化に関連する脅威を考慮して、それらの回復を防止することである。

注1：鍵材料には、暗号鍵関係を確立し維持するために必要な鍵及び初期化ベクトルが含まれる。

注2：DRBGが暗号鍵又は鍵材料の生成に使用され、PP/ST作成者がDRBGの状態を保護し、この状態を知ることで鍵又は鍵材料が危殆化する可能性を回避したい場合、PP/ST作成者はFCS_CKM.6.1の割付にDRBGのエントロピー入力、シード入力、DRBGの内部状態を含める。インスタンス化解除操作を使用したDRBGの状態の破棄については、FCS_RBG.1も参照。

E.2.7.2 操作

FCS_CKM.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、特定の状況下で破棄されるべき暗号鍵及び鍵材料のリストを提供する。

FCS_CKM.6.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、暗号鍵の破棄方法と、それを規定する標準を提供する。

FCS_CKM.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、鍵又は鍵材料の破棄の状況を選択する。

E.3 暗号操作(FCS_COP)

E.3.1 利用者のための適用上の注釈

暗号操作は、それに関連付けられた操作の暗号モードを持つことができる。そのような場合は、暗号モードが特定されなければならない。

例

操作の暗号モードの例として、暗号ブロック連鎖、出力フィードバックモード、電子コードブックモード、及び暗号フィードバックモードがある。

暗号操作は、1つ又は複数の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、以下の場合によっては、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/又は暗号鍵長の使用

c) そこで操作されるデータの種別及び/又は機密上の重要性

セキュリティ監査データ生成(FAU_GEN)がPP、PPモジュール、機能パッケージ又は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/又は検証、完全性及び/又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/又は復号、暗号鍵暗号化及び/又は復号、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、サブジェクト役割及びそのサブジェクトに関連する利用者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。

暗号操作を特定する場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、特定した暗号操作が選択された保証要件に対して適切であると確信するために、またTOEの技術種別、環境及び使用事例を考慮して、相当な注意を払うべきである。

注：場合によっては、認証機関は暗号操作の選択に関して方針を適用することができる(CEM A.6 nを参照)。

E.3.2 FCS_COP.1 暗号操作

E.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、使用される暗号アルゴリズムと鍵長が、割り付けられた標準に基づくことができる特定の暗号操作を実行することを要求する。

FCS_RBG.1又はFCS_RNG.1への依存性は、内部で乱数を生成する暗号アルゴリズム操作に必要である。

例1：DSA署名生成、ECDSA署名生成、RSASSA-PSS署名生成

決定論的な暗号アルゴリズム操作では、FCS_RBG.1又はFCS_RNG.1への依存性は必要ない場合がある。

例2：ECBモードでのAES暗号化/復号

E.3.2.2 操作

FCS_COP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又は検証、完

全性及び/又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/又は復号、暗号鍵暗号化及び/又は復号、暗号鍵交換及び乱数生成を含む。暗号操作は、利用者データ又はTSFデータに対して実行できる。

FCS_COP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、使用する暗号アルゴリズムを特定すべきである。

例：典型的な暗号アルゴリズムの例には、DES、RAS、IDEAが含まれるが、それらだけに限定されない。

FCS_COP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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目的に適切であるべきである。

FCS_COP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、識別された暗号操作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、これらには、国際、国内、業界、あるいは組織の標準が含まれるかもしれない。

E.4 ランダムビット生成(FCS_RBG)

E.4.1 利用者のための適用上の注釈

ランダムビットの生成方法を特定する場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、その仕様が選択された保証要件に適切であることを確信するために、TOEの技術種別、環境及び使用事例を考慮して、相当な注意を払うべきである。

注：場合によっては、認証機関は、ランダムビット生成器の選択に関してポリシーを適用できる。(CEM A.6 nを参照)

E.4.2 FCS_RBG.1 ランダムビット生成(RBG)

E.4.2.1 コンポーネントの根拠と適用上の注釈

FCS_RBG.1 については、これらの依存性は常に満たされなければならない。

CCパート1の8.3 c)では、依存性が満たされない場合に正当化を提供することが認められているが、このコンポーネントでは許可されない。

リシードは、RBGの状態を更新するための典型的なメカニズムである。リシードが実行不可能な場合、TSFは、不十分な品質の出力を生成するよりむしろ、RBGのインスタンス化を解除するべきである。

「インスタンス化の解除」は、RBGの内部状態がもはや使用不可能になることを意味する。

状況「更新なし」は、RBGをリシード又はインスタンス化解除できない場合にのみ選択されなければならない。

状況「要求されたとき」は、TOEの内部であろうとTSFI(APIコールなど)として提示されていようと、RBGのリシード又はインスタンス化の解除をトリガーするインタフェースがあることを示す。

状況「条件を満たしたとき」は、PP/ST作成者がリシードのためのアプリケーション固有の条件を指定することを可能にする。

標準のリストには、リシードの間隔、及びインスタンス化の解除とリシードの手順が指定されなければならない。この割付は、状況が「更新なし」であれば「なし」とする。

RBGのヘルステストは、FPT_TST.1で特定される。

注：TOEがDRBGの状態を保護する必要があり、この状態を知ることでその出力から得られる鍵又は鍵材料が危殆化する可能性を回避する場合、PP/ST作成者はFCS_CKM.6.1のインスタンスにDRBGのエントロピー入力、シード入力、DRBGの内部状態を割付に含めることになる。これは、FCS_RBG.1.3 の最後の選択において、「リシード」と「再インスタンス化」のどちらも適用されない場合(したがって、異なる破棄方法を指定する必要がある場合)に特に当てはまる。

E.4.2.2 操作

この説明に対して特定の要件は存在しない。

E.4.3 FCS_RBG.2 ランダムビット生成(外部シード)

E.4.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントでは、エントロピーノイズ源を得るためのインタフェースを複数回使用して入力を行うことができる。例えば、入力長が128ビットの場合、256ビットを得るために2回使用することができる。この場合、DRBGは1回しかインスタンス化できないため、128ビットをDRBGに提供せず、関数が128ビットを2回集め、256ビットのエントロピーノイズ源をDRBGに提供する。

このコンポーネントにおいて、シードの品質に関する要件は記述されない。この点に関する要件を定義し、外部ソースがその要件を満たすことを保証するのは、運用環境の責任である。

PP、PPモジュール、機能パッケージ又はSTの作成者向けの概説のガイダンスでは、RBGに関するあらゆる関連情報(例えば内部状態)の漏洩と同様に、外部ノイズ源からの値の改変及び暴露からの保護についても言及すべきである。

E.4.3.2 操作

この説明に対して特定の要件は存在しない。

E.4.4 FCS_RBG.3 ランダムビット生成(内部シード — 単一ソース)

E.4.4.1 コンポーネントの根拠と適用上の注釈

PP、PPモジュール、機能パッケージ又はSTの作成者は、複数の内部ノイズ源を使用したい場合、TSFが使用する各ノイズ源に対してこの要件を繰返し適用する。

ハードウェアベースのノイズ源は、リングオシレータ、ダイオード、熱雑音など、ノイズの発生を主な機能とするソースである。これらのハードウェアソースからノイズを収集するためにソフトウェアが使用されるが、これらはソフトウェアベースではない。ソフトウェアベースのノイズ源とは、他の主要な機能を持つソースで、ノイズはその通常動作の副産物である。ソフトウェアベースのノイズ源の例としては、利用者やシステムベースのイベント、イベントタイマからの最下位ビットの読み出しなどがある。

ハードウェアベースのノイズ源は、確率的にモデル化されることがあり、その場合、エントロピーの量はよく理解されている。ソフトウェアベースのノイズ源は、通常、あまりよく理解されていないため、より保守的なアプローチをとり、要件よりも多くのビットを収集し、圧縮関数を実行して最終出力を導出することになる。ソフトウェアベースのノイズ源は、多くの場合、エントロピー推定器に依存する。

E.4.4.2 操作

この説明に対して特定の要件は存在しない。

E.4.5 FCS_RBG.4 ランダムビット生成(内部シード — 複数ソース)

E.4.5.1 コンポーネントの根拠と適用上の注釈

最小エントロピーは、FCS_RBG.3.1のソース/繰返しごとに定義される。結果として得られる最小エントロピーは、FCS_RBG.4.1の依存性であるFCS_RBG.5.1によってカバーされる。

E.4.6 FCS_RBG.6 ランダムビット生成サービス

E.4.6.1 コンポーネントの根拠と適用上の注釈

インタフェース種別の特定は、評価アクティビティを開発する上で重要であり、外部インスタンスがTOEにRBGサービスを要求する際の重要な情報である。

E.4.6.2 操作

その他のインタフェース種別は、ネットワークインタフェース上のサービスとすることができる。

例：イーサネット、無線

E.5 乱数生成(FCS_RNG)

E.5.1 利用者のための適用上の注釈

乱数の生成方法を特定する場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、その仕様が選択された保証要件に適切であることを確信するために、TOEの技術種別、環境及び使用事例を考慮して、相当な注意を払うべきである。

注：場合によっては、認証機関は、ランダムビット生成器の選択に関してポリシーを適用できる。(CEM A.6 nを参照)

E.5.2 FCS_RNG.1 乱数生成

E.5.2.1 コンポーネントの根拠と適用上の注釈

STの作成者は、エレメントFCS_RNG.1.1及びFCS_RNG_1.2において、乱数の暗号応用に適した未完了の操作を実行しなければならない。STの作成者は、TOEの乱数生成器が提供するセキュリティ能力の仕様のための選択を実行しなければならない。

注：FCS_RNG の一部の利用者には、「The National Institute of Standards and Technology (NIST) Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015」及び「NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018」が役立つと考えられる。

乱数生成器の評価は、認められた方法に従わなければならない。

例：認められた方法の例として、Bundesamt für Sicherheit in der Informationstechnik(BSI)が発行するAIS31が挙げられる。

E.5.2.2 操作

FCS_RNG.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、セキュリティ能力のリストを特定するべきである。

例1

セキュリティ能力の例には、以下のものが含まれる。

— RNGが起動した直後にエントロピー源の全故障を検出する全故障テスト。全故障を検出した場合、乱数は出力されない。

— RNGの動作中にエントロピー源の全故障が発生した場合、RNGは、[選択: *エントロピー源の全故障後に生成されたいくつかの生の乱数に依存する全ての内部乱数の出力を防止する*、*内部状態のエントロピーが主張する出力エントロピーを保証する限りDRG.2クラスの後処理アルゴリズムを用いて内部乱数を生成する*]。

— (i)RNGが起動した直後及び(ii)RNGが動作している間、生の乱数列の許容できない統計的欠陥を検出するオンラインテスト。TSFは、電源投入時のオンラインテストが正常に終了する前、又は欠陥が検出された場合、乱数を出力してはならない。

— 乱数の許容できない弱点をすぐに検出するために有効であるオンラインテスト手続き

— 乱数列の品質をチェックするオンラインテスト手続き。これは、[選択: *外部から*、*一定間隔で*、*継続的に*、*特定された内部イベントに応じて*]トリガーされる。オンラインテストは、生の乱数の統計的特性の許容できない欠陥を許容期間内に検出するのに適している。

— ノイズ源の故障や深刻な劣化が検出可能であること

— 故障中の出力を防止する、エントロピー源の連続テスト又はその他のメカニズム

注1：PP、PPモジュール又は機能パッケージの場合、FCS_RNG.1.1は、以下のような、より限定的な表現で完成することができる。

— 割付: 追加セキュリティ能力のリスト

FCS_RNG.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、品質尺度に関して適切な選択をするべきである。

例2

品質尺度の例としては、以下のようなものがある。

— テスト手順A[割付: *追加の標準テストスイート*]が、内部乱数と理想的なRNGの出力シーケンスとを判別できない

注2：追加の標準統計テストスイートの割付は、空でもよい。

— 内部ランダムビットあたりの平均シャノンエントロピーが0.998を超える

— 各出力ビットが他の全ての出力ビットから独立している

注3：PP、PPモジュール又は機能パッケージの場合、FCS_RNG.1.2は、次のようなより限定的な表現で完了することができる。

— [選択:

— フルエントロピー出力

— [割付: *出力の偏り及びエントロピー率*]

注4：「品質尺度」は、質的尺度と量的尺度の両方を含むことができる。

例3

ハイブリッド決定論的RNGの場合、以下はその一例である。

「FCS_RNG.1.1/HD

TSFは、NIST Special Publication 800-90Aに定義された[選択: *CTR_DRBG*、*Hash_DRBG*、*HMAC_DRBG*]を実装するハイブリッド決定論的乱数生成器を提供しなければならない。

FCS_RNG.1.2/HD

TSFは、[割付: *セキュリティビット*]を満たす[選択: *ビット*、*ビットのオクテット*、*数値[割付: 数値の形式]*]を提供しなければならない。」

附属書F
(規定)

FDPクラス：利用者データ保護 — 適用上の注釈

F.1 一般

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。

このクラスには、従来の必須アクセス制御: Mandatory Access Control (MAC)あるいは従来の裁量アクセス制御: Discretionary Access Control (DAC)に対する明示的な要件は含まない。ただし、そのような要件は、このクラスからのコンポーネントを使って構成することができる。

FDP: 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、PPモジュール、機能パッケージ又は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。

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/又は「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、PPモジュール、機能パッケージ又はSTの作成者の抽出化のレベルに依存する。

アクセス制御方針とは、情報コンテナに対するアクセスを制御する方針である。属性は、そのコンテナの属性を表す。情報がいったんコンテナから外部に出ると、アクセス者はその情報を改変することが自由になり、その情報を、異なる属性を持つ異なるコンテナに書き込むこともできる。一方、情報フロー方針では、コンテナと独立した情報へのアクセスを制御する。情報の属性は、コンテナの属性と関連付けられていることがある(あるいは、マルチレベルデータベースの場合のように、そうでないこともある)が、情報が動くとそれと一緒に移動する。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。

このクラスは、普通に想像されるような、ITアクセス方針の完全な分類学を意図するものではない。ここに含まれる方針は、単に、実システムについての一般に知られている経験から得られる、要件特定のための基礎となるような方針である。ここでの定義には入らない、他の意向に沿った形式があってもよい。

例1

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(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又は拡張として扱うこともできる。

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2

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。

SFRのセットは、多数の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。全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。

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、PPモジュール、機能パッケージ又はSTを作成する場合、以下の情報が、クラスのどこを見るか、何を選択するかのガイダンスを提供する。

FDP: 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、PPモジュール、機能パッケージ又はSTの作成者は、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。

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全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、PPモジュール、機能パッケージ又はSTの中でそのコンポーネントを複数回具現化することができる。

このファミリからコンポーネントを選択する鍵は、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、全てのアクセス制御方針と全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」の割付又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。

以下のステップは、PP、PPモジュール、機能パッケージ又は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全て実行する。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(「全てのファイル」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)ファミリからの全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、いくつか又は全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全てを識別する。

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全て識別する。

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全てと、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全て識別する。

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全て識別する。

k) TSF間利用者データ機密転送保護(FDP_UCT)又は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。

F.2 アクセス制御方針(FDP_ACC)

F.2.1 利用者のための適用上の注釈

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。

このファミリのコンポーネントは、従来の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する。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」の割付又は選択を必要とする操作を持つ、他の機能コンポーネント全体において使用されることを想定している。

アクセス制御SFPは、サブジェクト、オブジェクト、及び操作という3点セットをカバーする。そのため、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。

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。

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。

このファミリは、PP、PPモジュール、機能パッケージ又はSTの作成者に様々な方針を特定する能力を提供する。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、PPモジュール、機能パッケージ又は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、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.2.2 FDP_ACC.1 サブセットアクセス制御

F.2.2.1 コンポーネントの根拠と適用上の注釈

オブジェクト及びサブジェクトという言葉は、TOEの中の一般的な要素を指す。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では、これらの一般的な用語(サブジェクト、オブジェクト)は詳細化されなければならない。

例：ファイル、レジスタ、ポート、デーモン、オープンコール。

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。

F.2.2.2 操作

FDP_ACC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFによって実施される、一意に名前付けされたアクセス制御SFPを特定すべきである。

FDP_ACC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.2.3 FDP_ACC.2 完全アクセス制御

F.2.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、オブジェクトに対する全ての可能な操作(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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.2.3.2 操作

FDP_ACC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFによって実施される、一意に名前付けされたアクセス制御SFPを特定すべきである。

FDP_ACC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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全ての操作はそのSFPでカバーされる。

F.3 アクセス制御機能(FDP_ACF)

F.3.1 利用者のための適用上の注釈

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。

このファミリは、PP、PPモジュール、機能パッケージ又はSTの作成者に、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。

例1

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、PPモジュール、機能パッケージ又はSTの作成者に、一般的なアクセス制御規則に対する例外を提供する規則を記述できるようにする。そのような例外では、オブジェクトに対するアクセスを、明示的に許可したり拒否したりする。

二人制御、操作の順序規則、あるいは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。

受け入れられる各種のアクセス制御機能性は、このファミリで特定できる。

例2

— 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

F.3.2 FDP_ACF.1 セキュリティ属性によるアクセス制御

F.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、サブジェクト及びオブジェクトに関連したセキュリティ属性に基づいてアクセス制御を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、PPモジュール、機能パッケージ又はSTの作成者が、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。

例

PP、PPモジュール、機能パッケージ又はSTの作成者が割り付けることができる属性の例は次のとおりである。

— 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、又はオブジェクトに関連付けられる。このような属性の例としては、サブジェクトの作成に使用されるプログラムイメージの名前や、そのプログラムイメージに割り付けられるセキュリティ属性などがある。

— 時間属性は、その日のある時間内、その週のある曜日間、又はある暦年内に許可されるアクセスを特定するのに使うことができる。

— 場所属性は、その場所が、操作を要求する場所と操作が実行される場所のいずれか、あるいは両方であるかを特定できる。これは、TSFの論理インタフェースを端末の場所やCPUの場所といった場所に変換する内部表に基づいて可能になる。

— グルーピング属性は、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。

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、又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、又は許可は、利用者、サブジェクト(利用者又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。

F.3.2.2 操作

FDP_ACF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_ACF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又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1

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、時刻、場所、ACL、あるいはPP、PPモジュール、機能パッケージ又はSTの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、それに関連する全ての属性を、サブジェクトに関係付ける有用な方法を提供できる。言い換えれば、各役割は、属性の名前付きグループに関連させられる。

FDP_ACF.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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や小さく分割したアクセス制御機能を特定することができる。

例2

— 一般的なアクセス制御機能：典型的な許可ビット

— 小さく分割したアクセス制御機能：アクセス制御リスト(ACL)

FDP_ACF.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例3

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に基づくものである。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、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

FDP_ACF.1.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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に基づくものである。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、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

F.4 データ認証(FDP_DAU)

F.4.1 利用者のための適用上の注釈

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。

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。

注：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。

F.4.2 FDP_DAU.1 基本データ認証

F.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、情報内容の有効性あるいは真正性の検証に使用され得る、確定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によって満たすことができる。

例：暗号チェックサム、指紋、メッセージダイジェスト。

F.4.2.2 操作

FDP_DAU.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれに対してデータ認証の証拠を生成できなければならないオブジェクト又は情報種別のリストを特定すべきである。

FDP_DAU.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.4.3 FDP_DAU.2 保証人識別付きデータ認証

F.4.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、追加的に、真正性の保証を提供する利用者の識別情報を検証できることを要求する。

例：高信頼第三者

F.4.3.2 操作

FDP_DAU.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれに対してデータ認証の証拠を生成できなければならないオブジェクト又は情報種別のリストを特定すべきである。

FDP_DAU.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.5 TOEからのエクスポート(FDP_ETC)

F.5.1 利用者のための適用上の注釈

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。

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。

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。

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。

複数のSFP(アクセス制御及び/又は情報フロー制御)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。

F.5.2 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

F.5.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、セキュリティ属性のエクスポートなしの利用者データのTSF仲介エクスポートを特定するのに使われる。

F.5.2.2 操作

FDP_ETC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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及び/又は情報フロー制御SFP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。

F.5.3 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

F.5.3.1 コンポーネントの根拠と適用上の注釈

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。その一つは、利用者データとセキュリティ属性を物理的に関連付ける方法である。

例：同一の外部メディア上に置く。

別の方法として、セキュア署名などの暗号技術を使って、属性と利用者データを関連付ける方法がある。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され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開始されることを確実にするために使用できる。

F.5.3.2 操作

FDP_ETC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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や情報フロー制御SFP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.2.5において、PP、PPモジュール、機能パッケージ又はSTの作成者は、追加のエクスポート制御規則を全て、あるいは追加の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/又は情報フローSFPに加えて、TSFによって実施される。

F.6 情報フロー制御方針(FDP_IFC)

F.6.1 利用者のための適用上の注釈

このファミリは、情報フロー制御SFPの識別をカバーし、かつ各々に対して、SFPの制御範囲を特定する。

このファミリのコンポーネントは、TOE内に見られる従来のMAC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とやり取りする制御された情報の流れ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」の割付又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。

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。

各SFPは三点セット: サブジェクト、情報、及びサブジェクトとやり取りする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。この場合、望まれるITセキュリティ機能を、それらのセキュリティ対策方針をサポートするものとして特定できる。

2番目のコンポーネント(FDP_IFC.2完全情報フロー制御)では、各情報フロー制御SFPは、そのSFPのカバーするサブジェクトとやり取りするそのSFPのカバーする情報の流れを生じさせる可能性のある全ての操作をカバーする。さらに、全ての情報フローは、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、用いられる全てのSFPは、フローが生じる前にこのフローを許可しなければならない。

情報フロー制御SFPは、完全に定義された操作のセットをカバーする。SFPのカバー範囲は、いくつかの情報フローに関しては「完全」かもしれず、あるいはその情報フローに影響を与えるいくつかの操作だけに対応するものかもしれない。

アクセス制御SFPは、情報を入れたオブジェクトへのアクセスを制御する。情報フロー制御SFPは、コンテナと独立した、情報に対するアクセスを制御する。その情報の属性は、コンテナの属性と関係付けられていることもあるが(あるいは、マルチレベルデータベースの場合のようにそうでないこともある)、情報が流れるときにそれと一緒にある。明示的な権限がない場合、アクセス者はその情報の属性を変更することができない。

情報のフロー及び操作は、複数のレベルで表現することができる。STの場合、情報のフロー及び操作は、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。

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、PPモジュール、機能パッケージ又は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。

F.6.2 FDP_IFC.1 サブセット情報フロー制御

F.6.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、情報フロー制御方針が、TOE内で可能な操作のサブセットに適用されることを要求する。

F.6.2.2 操作

FDP_IFC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが実施する一意に名前付けされた情報フロー制御SFPを特定すべきである。

FDP_IFC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト、情報、及びSFPがカバーする制御されたサブジェクトとやり取りする制御された情報の流れを生じさせる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、PPモジュール、機能パッケージ又はSTの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：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にさらに特定化したオブジェクトなどのデータを参照することができる。もし、特定された情報がアクセス制御方針の対象であるオブジェクト内に含まれる場合は、特定された情報がそのオブジェクトへ又はオブジェクト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.6.3 FDP_IFC.2 完全情報フロー制御

F.6.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、SFPに含まれるサブジェクトとやり取りする情報の流れを生じさせる全ての可能な操作を要求する。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.6.3.2 操作

FDP_IFC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが実施する一意に名前付けされた情報フロー制御SFPを特定すべきである。

FDP_IFC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。サブジェクトとやり取りする情報の流れを生じさせる全ての操作は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、PPモジュール、機能パッケージ又はSTの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：リストは利用者、マシン、プロセスを特定することができる。

情報は、電子メール、ネットワークプロトコル、あるいはアクセス制御方針において特定されたものと同様、さらに特定化したオブジェクトなどのデータを参照することができる。もし、特定された情報がアクセス制御方針の対象であるオブジェクト内に含まれる場合は、特定された情報がそのオブジェクトへ又はオブジェクト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.7 情報フロー制御機能(FDP_IFF)

F.7.1 利用者のための適用上の注釈

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。

信頼できないソフトウェアを考えると、暴露や改変に対する強力な保護を実現するために、情報フローにおける制御が必要になる。アクセス制御だけでは不十分なのは、それがコンテナに対するアクセスを制御するだけだからである。中に入れた情報が、制御なしでシステム全体を流れるのを許してしまう。

このファミリでは、「不正情報フローの種別」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、PPモジュール、機能パッケージ又はSTの作成者のニーズを反映した改善された分類を指すこともできる。

このコンポーネントの柔軟性は、FDP_IFF.1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の全部又は一部について、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、PPモジュール、機能パッケージ又はSTの作成者は、特権方針の組み込みを考慮すべきである。

F.7.2 FDP_IFF.1 単純セキュリティ属性

F.7.2.1 コンポーネントの根拠と適用上の注釈

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。

このコンポーネントは、セキュリティ属性をどのように割り付けるかの詳細(すなわち利用者対プロセス)を特定しない。必要に応じて、追加方針及び機能要件の特定を認めるような割付を持たせることで、方針における柔軟性を提供する。

このコンポーネントはまた、情報フロー制御機能がセキュリティ属性に基づいて情報フローを明示的に許可及び拒否できる要件を規定する。これは、このコンポーネントで定義した基本方針に対する例外をカバーする特権方針の実現に使用することができる。

F.7.2.2 操作

FDP_IFF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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1

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レベル、サブジェクトの取扱許可レベル、情報の機密レベルがある。

セキュリティ属性の種別は、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。

FDP_IFF.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、操作ごとに、サブジェクトと情報セキュリティ属性の間で保持する、TSFが実施するセキュリティ属性に基づく関係を特定すべきである。

FDP_IFF.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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として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全ての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。追加の規則が全くないなら、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」を指定するべきである。

FDP_IFF.1.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例2

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に基づくものがある。

このような能力が不要な場合、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

FDP_IFF.1.5において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.1.5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に基づくものがある。このような能力が不要な場合、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

F.7.3 FDP_IFF.2 階層的セキュリティ属性

F.7.3.1 コンポーネントの根拠と適用上の注釈

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。

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。

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。

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、PPモジュール、機能パッケージ又はSTの作成者は、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可能性がある。

F.7.3.2 操作

FDP_IFF.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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レベル、サブジェクトの取扱許可レベル、情報の機密レベルなどがある。セキュリティ属性の各種別の最小数種別は、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。

FDP_IFF.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、操作ごとに、サブジェクトと情報セキュリティ属性の間で保持する、TSFが実施するセキュリティ属性に基づく関係を特定すべきである。これらの関係は、セキュリティ属性間の順序に基づくべきである。

FDP_IFF.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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として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全ての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。

例1

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、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。追加の規則が全くないなら、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」を指定するべきである。

FDP_IFF.2.4において、PP、PPモジュール、機能パッケージ又はSTの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.2.4に含められている。

例2

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に基づくものがある。

このような能力が不要な場合、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

FDP_IFF.2.5において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.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に基づくものがある。このような能力が不要な場合、PP、PPモジュール、機能パッケージ又はSTの作成者は「なし」と特定すべきである。

F.7.4 FDP_IFF.3 制限付き不正情報フロー

F.7.4.1 コンポーネントの根拠と適用上の注釈

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

特定された不正情報フローに対して、ある最大容量が提供されるべきである。加えて、PP、PPモジュール、機能パッケージ又はSTの作成者は、不正情報フローが監査されなければならないかどうかを特定することができる。

F.7.4.2 操作

FDP_IFF.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、全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。

F.7.5 FDP_IFF.4 不正情報フローの部分的排除

F.7.5.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、不正情報フローの制御を要求する全てのSFPが、いくつかの(全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に使用されるべきである。

F.7.5.2 操作

FDP_IFF.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、全ての識別された不正情報フローに対して許可された最大容量を特定すべきである。

FDP_IFF.4.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.7.6 FDP_IFF.5 不正情報フローなし

F.7.6.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、不正情報フローの制御を要求するSFPが、全ての不正情報フローの排除を要求するときに使用されるべきである。しかしながら、全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、PPモジュール、機能パッケージ又はSTの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、全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が、多くの実際のアプリケーションで示されている。

F.7.6.2 操作

FDP_IFF.5.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.7.7 FDP_IFF.6 不正情報フロー監視

F.7.7.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、特定した容量を超える不正情報フローの使用を監視する能力をTSFが提供することが求められるときに使用されるべきである。そのようなフローを監査するこ

とが求められる場合、このコンポーネントは、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。

F.7.7.2 操作

FDP_IFF.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_IFF.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

注：ここで、制御対象のサブジェクトは、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の両方を指す。

F.8 情報保持制御(FDP_IRC)

F.8.1 利用者のための適用上の注釈

FDP_IRCが要求するオブジェクトの排除の大きな側面は、コンテナとしてのオブジェクト内に格納された情報を指す一方で、オブジェクトに関連付けられるかもしれない全ての属性(メタデータの意味もある)も含まれる。

この面で、FDP_IRCの焦点は、FDP_IFFやFDP_IFCのようなアクセス制御や情報フロー制御方針に関連する他のコンポーネントとは異なっている。さらに重要なことは、ここでのオブジェクトは常に、これらのオブジェクトに対して実行される選択されたアクティビティのコンテキストで考慮されることです。残存情報保護(FDP_RIP)とは対照的に、FDP_IRCはオブジェクトをあらゆるアクセスや情報フローから除外し、一連のアクティビティで不要になった時点で不可逆的かつ追跡不可能に削除する。

どのオブジェクトを考慮すべきかが完全には明確でない場合もあるが、具体的なテストを可能にするために、遅くともPP、PPモジュール、機能パッケージ又はSTの作成者によってオブジェクトのリストが割付されることが不可欠である。いかなる場合でも、オブジェクトのリストは、構造化された分析から導かれなければならない。

F.8.2 FDP_IRC.1 情報保持制御

F.8.2.1 コンポーネントの根拠と適用上の注釈

FDP_IRC.1に定義される情報消去方針は、割付オブジェクトに含まれる全ての情報を、情報が主要コンテンツであるか、何らかの種類の属性であるかにかかわらず、誤用から保護する役割を果たす。この方針は、オブジェクトとアクティビティの組み合わせを対象とする。方針の適用範囲は、1つ以上のアクティビティに関連する全てのオブジェクトに関して「完全」である場合もあれば、1つ以上のアクティビティに関連するオブジェクトの一部のみを対象とする場合もある。

FDP_IRC.1における「速やかに」という用語は、特に、オブジェクトが以前のようにはアクセスできないということを保証する方法で終了させなければならないということを意味する。

F.8.2.2 操作

FDP_IRC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFによって実施される、一意に名前付けされた情報消去方針を特定すべきである。

FDP_IRC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それぞれのアクティビティのリストに必要なオブジェクトのリスト、例えば、「全てのメッセージオブジェクト」を特定すべきである。

FDP_IRC.1.1では、PP、PPモジュール、機能パッケージ又はSTの作成者は、情報消去方針が関係するアクティビティのリスト、例えば、「メッセージの受信、メッセージの暗号処理、メッセージの送信など、メッセージを渡すことに関連する全てのアクティビティ」を特定すべきである。

FDP_IRC.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それぞれのアクティビティのリストに必要とされるオブジェクトのリストを特定すべきである。この割付は、FDP_IRC.1.1における割付オブジェクトと同一でなければならない。

F.9 TOE外からのインポート(FDP_ITC)

F.9.1 利用者のための適用上の注釈

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に、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。

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。

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。

例1

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、テープ、スキャナ、ビデオ、あるいはオーディオ信号)から、セキュリティ属性を含めずに、及びその内容を示すために媒体に物理的な印をつけずに、利用者データをインポートすること。

b) セキュリティ属性を含めて媒体から利用者データをインポートし、そのオブジェクトのセキュリティ属性が適切であることを検証すること。

c) 利用者データとセキュリティ属性の関係を保護するための暗号封印技術を使用して、セキュリティ属性を含めて媒体から利用者データをインポートすること。

このファミリは、利用者データをインポートしてよいかどうかの決定には関係しない。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。

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。

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、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。

例2：暗号チェックサム

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。

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。

これらのインポート要件は、ITの制限及び組織のセキュリティ方針に依存して、人間の介在あり、あるいはなしでTSFによって扱われるかもしれない。例えば、利用者データが「機密」チャネル上で受信される場合は、オブジェクトのセキュリティ属性は「機密」に設定される。

複数のSFP(アクセス制御及び/又は情報フロー制御)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。

F.9.2 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

F.9.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者データに関連付けられた信頼できる(あるいは何でも)セキュリティ属性を持たない利用者データのインポートを特定するのに使用される。この機能は、インポートされた利用者データのセキュリティ属性がTSFの中で初期化されることを要求する。PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.9.2.2 操作

FDP_ITC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又は情報フロー制御SFPを特定すべきである。この機能がインポートする利用者データは、これらのSFPの割付によって範囲が決められる。

FDP_ITC.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、全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/又は情報フロー制御SFPに追加されて、TSFによって実施される。

F.9.3 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

F.9.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、信頼できるセキュリティ属性が関連付けられた利用者データのインポートを特定するのに用いられる。この機能は、インポート媒体上でオブジェクトと正確か

つ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、PPモジュール、機能パッケージ又はSTの作成者は、インポートのための規則を特定することもできる。

F.9.3.2 操作

FDP_ITC.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又は情報フロー制御SFPを特定すべきである。この機能がインポートする利用者データは、これらのSFPの割付によって範囲が決められる。

FDP_ITC.2.5において、PP、PPモジュール、機能パッケージ又はSTの作成者は、全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/又は情報フロー制御SFPに追加して、TSFによって実施される。

F.10 TOE内転送(FDP_ITT)

F.10.1 利用者のための適用上の注釈

このファミリは、内部チャネルを介してTOEの部分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。

このファミリの要件は、TOE内で転送中の利用者データにとって望ましいセキュリティをPP、PPモジュール、機能パッケージ又はSTの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、又は可用性の損失に対する保護であってもよい。

このファミリが適用すべき物理的分離の度合いの決定は、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の部分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。

複数のSFP(アクセス制御及び/又は情報フロー制御)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。

F.10.2 FDP_ITT.1 基本内部転送保護

F.10.2.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈はない。

F.10.2.2 操作

FDP_ITT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、転送される情報をカバーするアクセス制御SFP及び/又は情報フロー制御SFPを特定すべきである。

FDP_ITT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、使用不能である。

F.10.3 FDP_ITT.2 属性による転送分離

F.10.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、例えば、各種の取扱許可レベルを備えた情報に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。

転送時のデータの分離を達成する方法の1つは、論理的又は物理的な分離チャネルを使用することである。

F.10.3.2 操作

FDP_ITT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、転送される情報をカバーするアクセス制御SFP及び/又は情報フロー制御SFPを特定すべきである。

FDP_ITT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、使用不能である。

FDP_ITT.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEの物理的に分離された部分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TSFが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。

F.10.4 FDP_ITT.3 完全性監視

F.10.4.1 コンポーネントの根拠と適用上の注釈

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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、検出されなければならない誤りの種別を特定しなければならない。PP、PPモジュール、機能パッケージ又はSTの作成者は、次の点を考慮すべきである: データの改変、データの置換、データの回復不能な順序変更、データのリプレイ、不完全なデータ、その他の完全性誤り。

PP、PPモジュール、機能パッケージ又はSTの作成者は、障害検出時にTSFがとるべきアクションを特定しなければならない。

例

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

F.10.4.2 操作

FDP_ITT.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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及び/又は情報フロー制御SFPを特定すべきである。

FDP_ITT.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データの転送において監視される、発生可能性のある完全性誤りの種別を特定すべきである。

FDP_ITT.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

TSFは利用者データの再発行を要求すべきである。FDP_ITT.3.1で特定したSFPは、TSFによってとられるアクションとして実施される。

F.10.5 FDP_ITT.4 属性に基づく完全性監視

F.10.5.1 コンポーネントの根拠と適用上の注釈

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、PPモジュール、機能パッケージ又はSTの作成者が、完全性誤りの検出においてとられるアクションを特定することを認める。

例1

このコンポーネントは、異なる完全性誤り検出と、異なる完全性レベルでの情報に対するアクションを提供するのに使用できる。

PP、PPモジュール、機能パッケージ又はSTの作成者は、検出されなければならない誤りの種別を特定しなければならない。PP、PPモジュール、機能パッケージ又はSTの作成者は、次の点を考慮すべきである: データの改変、データの置換、データの回復不能な順序変更、データのリプレイ、不完全なデータ、その他の完全性誤り。

PP、PPモジュール、機能パッケージ又はSTの作成者は、完全性誤り監視を必要とする属性(及び関連する転送チャネル)を特定すべきである。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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2

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。

F.10.5.2 操作

FDP_ITT.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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及び/又は情報フロー制御SFPを特定すべきである。

FDP_ITT.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データの転送において監視される、発生可能性のある完全性誤りの種別を特定すべきである。

FDP_ITT.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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決定するために使用される。このエレメントは、FDP_ITT.2属性による転送分離に直接関係する。

FDP_ITT.4.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.11 残存情報保護(FDP_RIP)

F.11.1利用者のための適用上の注釈

残存情報保護は、TSF-制御された資源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、割当て解除前に資源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により扱われることを保証する。

TOEは通常、オブジェクトから資源を割当て解除する可能性や、オブジェクトにそれらの資源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。それら資源全体ではないが部分的には、以前使った資源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、それらの資源に対し、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資源の解放や、割当て解除とそれに続く別のオブジェクトへの資源の再割当てというTSFの暗黙的アクションにも同様に適用される。

例

明示的な要求の例としては、ファイルの削除や切捨て、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。

オブジェクト再利用の要件はオブジェクトに属する資源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資源やオブジェクトに関する全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。

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(又はその逆)、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。

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。

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、PPモジュール、機能パッケージ又はSTの作成者は、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。

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。

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。

このファミリは、アクセス制御SFP又は情報フロー制御SFPの中で特定されたオブジェクトに対して、PP、PPモジュール、機能パッケージ又はSTの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。

F.11.2 FDP_RIP.1 サブセット情報保護

F.11.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEにおけるオブジェクトのサブセットに対して、それらのオブジェクトに割当てられた、あるいはそれらのオブジェクトから割当て解除された資源中に、利用可能な残存情報が存在しないことをTSFが保証することを要求する。

F.11.2.2 操作

FDP_RIP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FDP_RIP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.11.3 FDP_RIP.2 全残存情報保護

F.11.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEにおける全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。

F.11.3.2 操作

FDP_RIP.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.12 ロールバック(FDP_ROL)

F.12.1 利用者のための適用上の注釈

このファミリは、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といった利用者の必要性など、明確に定義された有効な状態に戻る必要性に対応する。

このファミリは、利用者が最後のアクションのセットを元に戻した後で、明確に定義された有効な状態に戻ること、あるいは分散データベースにおいて、全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ことを補助することを意図している。

資源の割当てをオブジェクトから解除した時点での内容の利用不可を残存情報保護(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。

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1

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。

例2

バックアップ。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。

F.12.2 FDP_ROL.1 基本ロールバック

F.12.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者又はサブジェクトが、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。

F.12.2.2 操作

FDP_ROL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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及び/又は情報フロー制御SFPを特定すべきである。これは、特定されたSFPを回避するのにロールバックが使用されないことを確実にするために必要である。

FDP_ROL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、ロールバックし得る操作のリストを特定すべきである。

FDP_ROL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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/又はリストを特定すべきである。

FDP_ROL.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、あらかじめ定義した期間として特定できる。

例

過去2分以内に実行された操作は元に戻すことができる。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.12.3 FDP_ROL.2 高度ロールバック

F.12.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、全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。

F.12.3.2 操作

FDP_ROL.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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及び/又は情報フロー制御SFPを特定すべきである。これは、特定されたSFPを回避するのにロールバックが使用されないことを確実にするために必要である。

FDP_ROL.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、ロールバック方針の対象となるオブジェクトのリストを特定すべきである。

FDP_ROL.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、あらかじめ定義した期間として特定できる。

例

過去2分以内に実行された操作は元に戻すことができる。

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.13 蓄積データ機密性(FDP_SDC)

F.13.1 利用者のための適用上の注釈

このファミリは、TSFによって保護されるメモリ領域内に格納されている間の利用者データの機密性の保護に対応する要件を提供する。TSFは、指定されたインタフェースを通じてのみメモリ内のデータへのアクセスを提供し、これらのインタフェースをバイパスした情報の漏洩を防止する。TSFは、メモリに格納されている間、利用者データを完全性エラーから保護する蓄積データ完全性(FDP_SDI)ファミリを補完するものである。

F.13.2 評価者のための注釈

実際には、FCS_COP.1への依存性は、PP、PPモジュール、機能パッケージ又はSTの作成者が、一部の特殊なケースでは、暗号に代わる方法が使用されることを説明する根拠を提供することにより、満たすことができる。

F.13.3 FDP_SDC.1 蓄積データ機密性

F.13.3.1 コンポーネントの根拠と適用上の注釈

FDP_SDC.1 蓄積データ機密性において、PP、PPモジュール、機能パッケージ又はSTの作成者は、どの利用者データを保護するか、どのメモリ種別で利用者データを保護することを要求するかを特定する。2番目の選択では、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データが保護されるメモリの種別を提供する。

F.13.3.2 操作

FDP_SDC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、「全ての利用者データ」を選択するか、その次の割付を使用して利用者データのリストを提供しなければならない。2番目の選択において、PP、PPモジュール、機能パッケージ又はSTの作成者は、一時的なメモリ、永続的なメモリ又は任意のメモリのいずれかを指定できる。「任意のメモリ」には、一時的(揮発性)メモリと永続的(不揮発性)メモリの両方が含まれる。

FDP_SDC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、メモリで保護されるべき利用者データのリストを提供する。

F.13.4 FDP_SDC.2 専用方法による蓄積データ機密性

F.13.4.1 コンポーネントの根拠と適用上の注釈

FDP_SDC.2 専用方法による蓄積データ機密性は、PP、PPモジュール、機能パッケージ又はSTの作成者が、様々なデータ特性を用いて利用者データのリストを詳細化できるようにすることで、FDP_SDC.1.1のエレメントを詳細化している。

F.13.4.2 操作

選択操作と最初の割付操作は、FDP_SDC.1と同様である。

2番目の割付では、PP、PPモジュール、機能パッケージ又はSTの作成者は、データ特性を提供する。データ特性には、データ長(閾値より短いか長いか)、データ型(バイナリ、テキスト、画像、音声、映像)、データ表現(バイナリ、ベクトル、文字、フレーム)などの項目を含めることができる。

F.14 蓄積データ完全性(FDP_SDI)

F.14.1 利用者のための適用上の注釈

このファミリは、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。

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。

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。

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。

F.14.2 FDP_SDI.1 蓄積データ完全性監視

F.14.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、完全性誤りに対して、媒体に格納されたデータを監視する。PP、PPモジュール、機能パッケージ又はSTの作成者は、監視の基礎として使われる、様々な種類の利用者データ属性を特定できる。

F.14.2.2 操作

FDP_SDI.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが検出する完全性誤りを特定すべきである。

FDP_SDI.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.14.3 FDP_SDI.2 蓄積データ完全性監視及びアクション

F.14.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、完全性誤りに対して、媒体に格納されたデータを監視する。PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.14.3.2 操作

FDP_SDI.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが検出する完全性誤りを特定すべきである。

FDP_SDI.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.15 TSF間利用者データ機密転送保護(FDP_UCT)

F.15.1 利用者のための適用上の注釈

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。

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。

F.15.2 FDP_UCT.1 基本データ交換機密性

F.15.2.1 コンポーネントの根拠と適用上の注釈

アクセス制御又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又は受信することが要求される。

F.15.2.2 操作

FDP_UCT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データの交換時に実施されるアクセス制御SFP及び/又は情報フロー制御SFP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。

FDP_UCT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.16 TSF間利用者データ完全性転送保護(FDP_UIT)

F.16.1 利用者のための適用上の注釈

このファミリは、TSFと他の高信頼IT製品間で転送される利用者データの完全性を提供し、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。

このファミリは、転送中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。

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。

F.16.2 FDP_UIT.1 データ交換完全性

F.16.2.1 コンポーネントの根拠と適用上の注釈

アクセス制御又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又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。

F.16.2.2 操作

FDP_UIT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、送信データ又は受信データに対して実施されるアクセス制御SFP及び/又は情報フロー制御SFP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。

FDP_UIT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、オブジェクトを送信又は受信するTSFにこのエレメントを適用するかどうかを特定すべきである。

FDP_UIT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、データが改変、削除、挿入、あるいはリプレイから保護されるべきかどうかを特定すべきである。

FDP_UIT.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.16.3 FDP_UIT.2 発信側データ交換回復

F.16.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、もし必要ならば、他の高信頼IT製品の助けを借りて、識別された伝送誤りのセットから回復する能力を提供する。他の高信頼IT製品は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

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。

F.16.3.2 操作

FDP_UIT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データの回復時に実施するアクセス制御SFP及び/又は情報フロー制御SFPを特定すべきである。特定した方針は、どのデータが回復され得るか、どのようにして回復され得るかを決定するために実施される。

FDP_UIT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

F.16.4 FDP_UIT.3 着信側データ交換回復

F.16.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、識別された伝送誤りのセットから回復するための能力を提供する。このタスクは、発信源の高信頼IT製品の助けを借りずになされる。

例

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。

F.16.4.2 操作

FDP_UIT.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者データの回復時に実施するアクセス制御SFP及び/又は情報フロー制御SFPを特定すべきである。特定した方針は、どのデータが回復され得るか、どのようにして回復され得るかを決定するために実施される。

FDP_UIT.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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
(規定)

FIAクラス：識別と認証 — 適用上の注釈

G.1 一般

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。

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。

例：セキュリティ属性は、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を含む。

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。

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。

身元確認の認証(FIA_API)ファミリは、TOEのIT環境において、TOEの識別情報を証明し、外部エンティティによって検証されるために、TOEが提供する機能の定義に対応する。

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。

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。

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。

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。

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。

G.2 認証失敗(FIA_AFL)

G.2.1 利用者のための適用上の注釈

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。

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。

G.2.2 FIA_AFL.1 認証失敗時の取り扱い

G.2.2.1 コンポーネントの根拠と適用上の注釈

PP、PPモジュール、機能パッケージ又はSTの作成者は、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開発者又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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、認証に失敗した際にTSFがとらなければならないアクションのリストを特定できる。また、PP、PPモジュール、機能パッケージ又はSTの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る。

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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

これらのアクションの例は、以下のとおり。

— 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)

G.2.2.2 操作

FIA_AFL.1認証失敗時の取り扱いにおいて、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FIA_AFL.1認証失敗時の取り扱いにおいて、PP、PPモジュール、機能パッケージ又はSTの作成者は認証事象を特定すべきである。

例

認証事象の例は、以下のとおり。

— 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

— 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

— 直前の10分間における不成功認証試行

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。

FIA_AFL.1認証失敗時の取り扱いにおいて、正の整数の割付が選択された場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、その値に達するか上回ったときに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。

FIA_AFL.1認証失敗時の取り扱いにおいて、管理者設定可能な正の整数が選択された場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FIA_AFL.1.2で、PP、PPモジュール、機能パッケージ又はSTの作成者は、定義された不成功の認証試行の回数に達するか、上回ったかのどちらを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。

FIA_AFL.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、選択のとおり、閾値に達するか上回っ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、手段、及び適用可能な場合はその手段の存続時間(あるいはその手段が終了される条件)を特定すべきである。

G.3 識別情報の認証証明(FIA_API)

G.3.1 利用者のための適用上の注釈

FIAクラスの他のファミリは、TOEが行う利用者の識別情報の認証検証のみを記述し、利用者が自身の識別情報を証明する機能については記述していない。FIA_APIファミリは、TOEが自身の識別情報を証明するための機能を特定することができる。

G.3.2 FIA_API.1 識別情報の認証証明

G.3.2.1 コンポーネントの根拠と適用上の注釈

FIA_API.1 識別情報の認証証明は、TOEの識別情報を外部エンティティに証明するために使用する認証メカニズムを特定することができる。

G.3.2.2 操作

3番目の割付[viii]は、PP、PPモジュール、機能パッケージ又はSTの作成者が、使用する認証メカニズムを特定する場合である。

例

このような認証方法の例としては、「Triple-DESに基づく認証メカニズム」や「TR-03110に基づくチップ認証プロトコル」などがある。

2番目の割付は、PP、PPモジュール、機能パッケージ又はSTの作成者が、識別情報がどのエンティティに関連づけられるかを特定できるようにする。

最初の割付は、特性のリストを提供するために使用される。特性のリストには、役割や資格情報を含めることができる。

G.4 利用者属性定義(FIA_ATD)

G.4.1 利用者のための適用上の注釈

全ての許可利用者は、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。

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。

G.4.2 FIA_ATD.1 利用者属性定義

G.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者のレベルで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で割り付けられ、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このリスト内のセキュリティ属性を変更しても、他の全ての利用者のセキュリティ属性に影響を与えるべきではない。

セキュリティ属性が利用者のグループに属する場合(グループに対する能力リストなど)、利用者は、対応するグループへの参照を(セキュリティ属性として)持つ必要があろう。

G.4.2.2 操作

FIA_ATD.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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.5 秘密についての仕様(FIA_SOS)

G.5.1 利用者のための適用上の注釈

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。

例1

このようなメカニズムの例には、利用者が作るパスワードの自動的チェック、あるいは自動化されたパスワード生成などがある。

秘密は、TOEの外部で生成できる。

例2

TOEの外部で生成された秘密の例には、利用者によって選択され、TOEに導入された秘密がある。

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/又は以前に使われていない、に沿っていることを保証するために使用できる。

秘密は、TOEによって生成することもできる。そのような場合、FIA_SOS.2 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。

秘密には、利用者が所有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。

G.5.2 FIA_SOS.1 秘密の検証

G.5.2.1 コンポーネントの根拠と適用上の注釈

秘密は、利用者が生成できる。このコンポーネントは、利用者が生成した秘密が、ある品質尺度を満たすことが検証できることを保証する。

G.5.2.2 操作

FIA_SOS.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、秘密が満たさなけれ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。

例

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/又は受容できる秘密が満たさなければならない空間サイズである。

G.5.3 FIA_SOS.2 TSF秘密生成

G.5.3.1 コンポーネントの根拠と適用上の注釈

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。

疑似乱数生成器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(シード)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シードの数が、生成しなければならない秘密の最小個数と少なくとも同じである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。

G.5.3.2 操作

FIA_SOS.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、秘密が満たさなけれ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。

例1

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/又は受容できる秘密が満たさなければならない空間サイズである。

FIA_SOS.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSF生成の秘密が使われなければならないTSF機能のリストを提供しなければならない。

例2：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.6 利用者認証(FIA_UAU)

G.6.1 利用者のための適用上の注釈

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く、要求された属性を定義する。

G.6.2 FIA_UAU.1 認証のタイミング

G.6.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者の主張する識別情報が認証される前に、利用者を代行してTSFによって実行されることのできるTSF仲介アクションをPP、PPモジュール、機能パッケージ又はSTの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。リストにない全ての他の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なければならない。

このコンポーネントは、そのアクションが、識別が行われる前に実行され得るかどうかを制御することはできない。それには、適切な割付を施したFIA_UID.1識別のタイミング又は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。

G.6.2.2 操作

FIA_UAU.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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。

G.6.3 FIA_UAU.2 アクション前の利用者認証

G.6.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、全ての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。

G.6.3.2 操作

このコンポーネントでは、操作は指定されていない。

G.6.4 FIA_UAU.3 偽造されない認証

G.6.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、認証データの保護を提供するメカニズムに対する要件に対応する。他の利用者から複製された、あるいは何らかの方法で組み立てられた認証データは、検出及び/又は拒否されるべきである。これらのメカニズムは、TSFによって認証された利用者が、実際に彼らがそう主張する者であることの信用性を提供する。

このコンポーネントは、共有不能な認証データ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。

G.6.4.2 操作

FIA_UAU.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが、認証データの偽造を検出するか、防止するか、あるいは検出及び防止するかを特定すべきである。

FIA_UAU.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが、認証データの複製を検出するか、防止するか、あるいは検出及び防止するかを特定すべきである。

G.6.5 FIA_UAU.4 単一使用認証メカニズム

G.6.5.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、単一使用認証データに基づく認証メカニズムに対する要件に対応する。単一使用認証データとは、利用者が持つかあるいは知っているものとすることができるが、利用者自身についてのものであってはならない。

例

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/又は秘密のルックアップテーブルからの乱数などがある。

PP、PPモジュール、機能パッケージ又はSTの作成者は、この要件が適用される認証メカニズムを特定できる。

G.6.5.2 操作

FIA_UAU.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、「全ての認証メカニズム」とすることができる。

例

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。

G.6.6 FIA_UAU.5 複数の認証メカニズム

G.6.6.1 コンポーネントの根拠と適用上の注釈

このコンポーネントを使用すれば、TOE内で使用される複数の認証メカニズムに対する要件の特定ができる。各々の個別のメカニズムに対して、各メカニズムに適用するために、FIA:識別と認証クラスから適用すべき要件が選択される。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。

FMTクラス中の管理機能は、認証が成功したかどうかを決定する規則に加え、認証メカニズムのセットに対する維持能力を提供する。

TOEと対話する匿名利用者を認めるために、認証メカニズム「なし」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必要がある。

G.6.6.2 操作

FIA_UAU.5.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用可能な認証メカニズムを特定すべきである。

例1

そのようなリストは、「なし、パスワードメカニズム、生体認証(網膜スキャン)、S/Keyメカニズム」である。

FIA_UAU.5.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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なければならないことを意味している。

例2

そのような規則のリストの一例: 「利用者が特別な権限を有していれば、パスワードメカニズム及び生体認証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。その他全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なければならない」。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例3

規則の一例: 「利用者は常にトークンを用いて認証されなければならない。管理者は、併用されなければならない追加の認証メカニズムを特定できる」。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

G.6.7 FIA_UAU.6 再認証

G.6.7.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、定義された時点における利用者の再認証の潜在的な必要性に対応する。これらは、再認証に対する非TSFエンティティからの要求だけでなく、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。

例：サーバーアプリケーションは、TSFがサービスを提供しているクライアントを再認証するよう要求する。

G.6.7.2 操作

FIA_UAU.6.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、再認証を要求する条件のリストを特定すべきである。このリストには、特定された利用者非アクティブ状態経過期間、アクティブなセキュリティ属性の利用者変更要求、あるいはセキュリティ上重要な機能をTSFが実行することの利用者要求などが含まれる。

PP、PPモジュール、機能パッケージ又はSTの作成者は、再認証が行われる、及び詳細が許可管理者に委ねられる境界を与えることができる。

例

「利用者は常に少なくとも1日に1回再認証されなければならない。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指定ができる」。

G.6.8 FIA_UAU.7 保護された認証フィードバック

G.6.8.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者に提供される認証プロセスにおけるフィードバックに対応する。あるシステムでは、フィードバックは何文字がタイプされたかを示しても文字自体は示さないように構成され、別のシステムでは、その情報すら不適切かもしれない。

このコンポーネントは、認証データがそのまま利用者に返されないことを要求する。ワークステーションの環境では、各パスワードの文字ごとに、元の文字ではなく、代用文字を表示することができる。

例：スター「＊」文字

G.6.8.2 操作

FIA_UAU.7 保護された認証フィードバックにおいて、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

フィードバックの割付は、「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は、「認証に失敗した認証メカニズム」とすることができる。

G.7 利用者識別(FIA_UID)

G.7.1 利用者のための適用上の注釈

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全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。

G.7.2 FIA_UID.1識別のタイミング

G.7.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者が識別されるときの要件を述べる。PP、PPモジュール、機能パッケージ又はSTの作成者は、識別が行われる前に実行する特定のアクションを示すことができる。

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。

G.7.2.2 操作

FIA_UID.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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。

G.7.3 FIA_UID.2 アクション前の利用者識別

G.7.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントにおいて利用者が識別される。利用者は、識別される前は、全てのアクションの実行をTSFから許可されない。

G.7.3.2 操作

このコンポーネントでは、操作は指定されていない。

G.8 利用者-サブジェクト結合(FIA_USB)

G.8.1 利用者のための適用上の注釈

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、(全体又は一部が)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。

G.8.2 FIA_USB.1 利用者-サブジェクト結合

G.8.2.1 コンポーネントの根拠と適用上の注釈

これは、あるタスクを実行するために、サブジェクトを発生あるいは活性化させた利用者を代行して、そのサブジェクトが動作することを意図したものである。

そのため、サブジェクトが生成されたとき、そのサブジェクトは、その生成を起動した利用者を代行して動作する。匿名性が使われる場合、サブジェクトはそれでも利用者を代行して動作するが、利用者の識別情報は知られない。特殊な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。

例：利用者の例は、サーバプロセスである。

G.8.2.2 操作

FIA_USB.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FIA_USB.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、又は「なし」を特定すべきである。

FIA_USB.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者を代行して動作するサブジェクトに関連付けられた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、又は「なし」を特定すべきである。

附属書H
(規定)

FMTクラス：セキュリティ管理 ― 適用上の注釈

H.1 一般

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。

TOEが物理的に分離された複数の部分で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の部分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。

FMT_LIMファミリは、TSF機能の能力や可用性を制限する方針を指定することを可能にする要件を提供する。これは、PP、PPモジュール、機能パッケージ又はSTの作成者が、最小特権や攻撃対象領域の最小化などの設計原則を強制する必要がある場合に有用である。

注：これら、及び他のアーキテクチャと設計原則、ならびに適切な評価については、ISO/IEC TS 19249で議論されている。

H.2 制限された能力及び可用性(FMT_LIM)

H.2.1 利用者のための適用上の注釈

機能要件FMT_LIM.1及びFMT_LIM.2は、方針を実施するために、共に保護を提供する2種類のメカニズム(能力の制限及び可用性の制限)が存在することを前提としている。また、これは以下のことを可能とする。

a) TSFは利用者環境において製品に制限なく提供されるが、その機能は非常に限られているため、方針が実施される。又は、

b) TSFは高機能に設計されているが、利用者環境においては製品から削除又は無効化される。

両要件の組み合わせにより、方針を実施しなければならない。

H.2.2 FMT_LIM.1 制限された能力

H.2.2.1 コンポーネントの根拠と適用上の注釈

例

限定された能力の例として、JTAGインタフェースの有効化があり、有効又は無効のいずれかを選択することができる。

H.2.2.2 操作

FMT_LIM.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、制限された能力の方針を特定するべきである。

H.2.3 FMT_LIM.2 制限された可用性

H.2.3.1 コンポーネントの根拠と適用上の注釈

例

制限された可用性の例として、JTAGインタフェースの有効化があり、TOEを運用する前に有効化又は無効化することができる。

H.2.3.2 操作

FMT_LIM.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、制限された可用性の方針を特定するべきである。

H.3 TSFにおける機能の管理(FMT_MOF)

H.3.1 利用者のための適用上の注釈

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、説明責任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の定義と更新、あるいは監査システム制御の定義と更新、利用者ごとの方針属性の定義と更新、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である。

   例1

   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の識別子、利用者アカウント、システム入力パラメタ。

   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、監査報告生成。

   利用者ごとの方針属性：取扱許可。

b) 可用性の制御に関する管理機能。

   例2：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3：TOE構成、手動回復、TOEセキュリティ修正のインストール(もしあれば)、ハードウェアの修復及び再設置。

d) TOE資源の日常的な制御及び維持に関する管理機能。

   例4：周辺装置の有効化と無効化、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。

これらの機能は、PP又は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。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、PPモジュール、機能パッケージ又はSTの作成者の責任である。

TSFに、管理者が制御できる機能を含められる。

例5

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/又は認証メカニズムを修正可能にすることができる。

H.3.2 FMT_MOF.1 セキュリティ機能のふるまいの管理

H.3.2.1 コンポーネントの根拠と適用上の注釈

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無効にする又は有効にする、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。

例

セキュリティ機能のふるまい修正には、認証メカニズムの変更がある。

H.3.2.2 操作

FMT_MOF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、役割が、セキュリティ機能について、ふるまいを決定するか、無効にするか、有効にするか、ふるまいを改変するか、を選択すべきである。

FMT_MOF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、識別された役割が修正することのできる機能を特定すべきである。例として、監査及び時間決定などがある。

FMT_MOF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.4 セキュリティ属性の管理(FMT_MSA)

H.4.1 利用者のための適用上の注釈

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。

セキュリティ属性は、TSFのふるまいに影響を与える。

例

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、役割又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／規則のセット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。

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/又は潜在的に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。

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受け入れられる全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。

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。

H.4.2 FMT_MSA.1 セキュリティ属性の管理

H.4.2.1 コンポーネントの根拠と適用上の注釈

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。

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。初期値は、パラメタの具現化(作成)時に与えられ、デフォルト値を上書きする。

H.4.2.2 操作

FMT_MSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、そのセキュリティ属性が適用可能なアクセス制御SFP又は情報フロー制御SFPをリストすべきである。

FMT_MSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、その役割が、デフォルト値変更、問い合わせ、セキュリティ属性の改変、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。

FMT_MSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、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。

例1

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、サービスレベルの優先度、アクセス制御リスト、デフォルトアクセス権などがある。

FMT_MSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_MSA.1.1において、もし選択されれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例2：そのような操作の例は「作成」である。

H.4.3 FMT_MSA.2 セキュアなセキュリティ属性

H.4.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、セキュリティ属性に割り付けることのできる値の要件を含む。割り付けられる値は、TOEがセキュアな状態を保持するようなものであるべきである。

「セキュア」が何を意味するかの定義は、このコンポーネントでは回答されず、TOEの開発、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。

H.4.3.2 操作

FMT_MSA.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

H.4.4 FMT_MSA.3 静的属性初期化

H.4.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFが、関連するオブジェクトのセキュリティ属性にデフォルト値を提供することを要求し、それは、初期値によって上書きされることができる。もし生成時に許可を特定できるメカニズムが存在するならば、新しいオブジェクトに対して、作成時に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。

H.4.4.2 操作

FMT_MSA.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、そのセキュリティ属性が適用可能なアクセス制御SFP又は情報フロー制御SFPをリストすべきである。

FMT_MSA.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_MSA.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者がその他の特性を選択した場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、デフォルト値が要求する特性を特定すべきである。

FMT_MSA.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

H.4.5 FMT_MSA.4 セキュリティ属性値継承

H.4.5.1 コンポーネントの根拠と適用上の注釈

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。

H.4.5.2 操作

FMT_MSA.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、特定のセキュリティ属性により継承される値を管理する規則を、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

もし新しいファイル又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.5 TSFデータの管理(FMT_MTD)

H.5.1 利用者のための適用上の注釈

このコンポーネントは、TSFデータの管理における要件を課すものである。

例：TSFデータの例は、現在時刻と監査証跡である。

このファミリは、誰が監査証跡を読み出し、削除、又は作成できるかを特定することを認める。

H.5.2 FMT_MTD.1 TSFデータの管理

H.5.2.1 コンポーネントの根拠と適用上の注釈

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。

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。初期値は、パラメタの具現化(作成)時に与えられ、デフォルト値を上書きする。

H.5.2.2 操作

FMT_MTD.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、その役割が、デフォルト値変更、問い合わせ、あるいはTSFデータの改変、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、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_MTD.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、デフォルト値が管理され得ることを特定することが可能である。

FMT_MTD.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_MTD.1.1において、もし選択されれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：そのような操作の一例は、「作成する」である。

H.5.3 FMT_MTD.2 TSFデータにおける限界値の管理

H.5.3.1 コンポーネントの根拠と適用上の注釈

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。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。

H.5.3.2 操作

FMT_MTD.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、限界値を持つことのできるTSFデータ[ix]を特定すべきである。そのようなTSFデータの一例は、ログインした利用者の数である。

FMT_MTD.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFデータの限界値を修正することが許される役割[x]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_MTD.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

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。

H.5.4 FMT_MTD.3 セキュアなTSFデータ

H.5.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFデータに割り付けることのできる値における要件をカバーする。割り付けられる値は、TOEがセキュアな状態を保持するようなものであるべきである。

「セキュア」が何を意味するかの定義は、このコンポーネントでは回答されず、TOEの開発、及びその結果としてのガイダンスの情報に委ねられる。

H.5.4.2 操作

FMT_MTD.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.6 取消し(FMT_REV)

H.6.1 利用者のための適用上の注釈

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。

H.6.2 FMT_REV.1 取消し

H.6.2.1 コンポーネントの根拠と適用上の注釈

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、全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。

H.6.2.2 操作

FMT_REV.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、関連するオブジェクト／サブジェクト／利用者／他の資源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。

FMT_REV.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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によって提供されなければならないかどうかを特定すべきである。

FMT_REV.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_REV.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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によって提供されなければならないかどうかを特定すべきである。

FMT_REV.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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「全ての新しいサブジェクト作成に対して」などがある。

H.7 セキュリティ属性有効期限(FMT_SAE)

H.7.1 利用者のための適用上の注釈

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、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。

例：証明書の例としては、ANSI X509のような鍵認証書がある。

H.7.2 FMT_SAE.1 時限付き許可

H.7.2.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

H.7.2.2 操作

FMT_SAE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：そのような属性の一例は、利用者のセキュリティ取扱許可である。

FMT_SAE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FMT_SAE.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、各セキュリティ属性の有効期限が切れ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、有効期限が切れたとき、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、PPモジュール、機能パッケージ又は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.8 管理機能の特定(FMT_SMF)

H.8.1 利用者のための適用上の注釈

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、又はセキュリティ機能管理のうちのいずれかである

H.8.2 FMT_SMF.1 管理機能の特定

H.8.2.1 コンポーネントの根拠と適用上の注釈

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。

PP、PPモジュール、機能パッケージ又は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、PPモジュール、機能パッケージ又は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。

H.8.2.2 操作

FMT_SMF.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、セキュリティ属性管理、TSFデータ管理、又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.9 セキュリティ管理役割(FMT_SMR)

H.9.1 利用者のための適用上の注釈

このファミリは、利用者が、彼らに割り付けられた機能上の責任外のアクションをとることでその権限を悪用することから生じる損害の公算を低減する。また、TSFをセキュアに管理するには不適切なメカニズムが提供されるという脅威にも対応する。

このファミリは、利用者が特定のセキュリティ関連管理機能の使用を許可されているかどうかを識別するための情報が維持されることを要求する。

ある管理アクションは利用者によって実行でき、あるものは組織内の指定された人間だけが実行できる。このファミリは、所有者、監査者、管理者、日常管理といった様々な役割の定義を認める。

このファミリで使用される役割は、セキュリティ関連の役割である。各役割は、広範な一連の能力を含むか、又は単一の権限であることができる。このファミリは、役割を定義する。役割の能力は、制限された能力及び可用性(FMT_LIM)、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。

例1

能力のセット：UNIXのroot。

単一の権限：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

ある役割の種別は互いに排他的であることがある。

例2

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、管理者(役割)用に確保されている利用者の削除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。

H.9.2 FMT_SMR.1 セキュリティの役割

H.9.2.1 コンポーネントの根拠と適用上の注釈

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。

H.9.2.2 操作

FMT_SMR.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、システムによって認識される役割を特定すべきである。これらは、セキュリティに関して利用者がとり得る役割である。

例：役割の例には、所有者、監査者、管理者がある。

H.9.3 FMT_SMR.2 セキュリティ役割における制限

H.9.3.1 コンポーネントの根拠と適用上の注釈

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。

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。

H.9.3.2 操作

FMT_SMR.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、システムによって認識される役割を特定すべきである。これらは、セキュリティに関して利用者がとり得る役割である。

例1：役割の例には、所有者、監査者、管理者がある。

FMT_SMR.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、役割の割付を管理する条件を特定すべきである。

例2

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なければならない」。

H.9.4 FMT_SMR.3 負わせる役割

H.9.4.1 コンポーネントの根拠と適用上の注釈

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なければならないことを特定する。

H.9.4.2 操作

FMT_SMR.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それを負わせるために明示的な要求を必要とする役割を特定すべきである。

例：役割の例には、所有者、監査者、管理者がある。

附属書I
(規定)

FPRクラス：プライバシー ― 適用上の注釈

I.1 一般

このクラスは、システムの操作における十分な制御を維持するために、可能な限りシステムに柔軟性を持たせる一方、利用者のプライバシーの必要性を満たすために課すことができる要件を記述する。

このクラスのコンポーネントでは、許可利用者は要求されたセキュリティ機能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1

例えば、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

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2

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(おそらく匿名性や偽名性のため)、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、PPモジュール、機能パッケージ又はSTに監査要件を含めることは可能であり、そこでは、特定のセキュリティ関連事象が発生したという事実の方が、誰がそれに対して責任があるかを知るよりも重要となる。

追加情報がFAU: 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。

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3：監査の要件がある場合。

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。

全てのファミリは、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4

TSFが電子メッセージやデータベース中の利用者名を隠すことは期待されていない。

このクラスの全てのファミリは、操作によって範囲を決め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、PPモジュール、機能パッケージ又はSTの作成者が明らかにできるようにする。

例5

匿名性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/又はサブジェクトが決定できないことを保証する」。

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。

注：CCに基づいて記述されたISO/IEC TS 19608に読者の関心事項が記載されている。ISO/IEC TS 19608:

— 個人を特定できる情報(PII)を保護するためにCCパート2からSFRを選択し、特定すること。

— プライバシーとSFRの両方を協調して定義するための手順。

— ISO/IEC 29100で定義されたプライバシー原則に基づく、CCパート2に記述されたパラダイムを通じた、拡張コンポーネントとしてのプライバシー機能要件の開発。

I.2 匿名性(FPR_ANO)

I.2.1 利用者のための適用上の注釈

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又はサービスを使用できることを保証する。

このファミリの意図は、利用者又はサブジェクトが、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、PPモジュール、機能パッケージ又はSTの作成者に提供する。

したがって、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又はその識別情報の参照さえも決定できない。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。

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。

「決定する(determine)」の解釈は、その語の意味を最も広義にとるべきである。

コンポーネントのレベル付け及び説明は、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取得することが認められる。しかしながら、許可利用者が利用者の識別情報を決定する能力を持つことが可能であるという特別な要件があるわけではない。究極のプライバシーのため、どのアクションを実行する誰についてもその識別情報を見ることができないということを言うために、このコンポーネントが使われよう。

提供される全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、PPモジュール、機能パッケージ又はSTの作成者が全てのサブジェクト/操作に対応したい場合は、「全てのサブジェクト及び全ての操作」という語が提供されよう。

次のような機能を含むアプリケーションがあり得る: 公のデータベースに機密性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。

例

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は、プロバイダ、システムオペレータ、通信相手、及び利用者を含み、彼らは悪意を持つ部品(例えばマルウェア)をこっそりとシステムに持ち込む。これらの利用者は全て、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。

I.2.2 FPR_ANO.1 匿名性

I.2.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者の識別情報が暴露から保護されることを保証する。しかしながら、特定の許可利用者が、あるアクションを実行したのは誰かを決定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。

I.2.2.2 操作

FPR_ANO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのセットを特定すべきである。例えば、PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。

例1

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_ANO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト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/又は操作、及び/又はオブジェクトのリストを識別すべきである。

例2：オブジェクトの例は「投票アプリケーション」である。

I.2.3 FPR_ANO.2 情報を請求しない匿名性

I.2.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFが利用者の識別情報を知ることを許可されないことを保証する。

I.2.3.2 操作

FPR_ANO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのセットを特定すべきである。

例1

例えば、PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護する。

例2

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_ANO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト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/又は操作、及び/又はオブジェクトのリストを識別すべきである。

例3

「投票アプリケーション」

FPR_ANO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、例えば「職務記述書へのアクセス」など、匿名性要件の対象となるサービスのリストを識別すべきである。

FPR_ANO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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のリストを識別すべきである。

I.3 偽名性(FPR_PSE)

I.3.1 利用者のための適用上の注釈

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又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。

偽名性は、いくつかの点で匿名性に似ている。偽名性と匿性名の両方とも利用者の識別情報を保護するが、偽名性においては、責任を明確にするため、あるいは他の目的のために、利用者識別情報への参照が維持される。

コンポーネントFPR_PSE.1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。

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1

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取得される必要がある。PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

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2

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、PPモジュール、機能パッケージ又はSTの作成者は、参照が適合しなければならない規則を特定するために、FPR_PSE.3別名偽名性を一緒に使いたいと思うかもしれない。

上述の構成概念を使い、利用者識別情報が保護されること、及び、条件として特定すれば、ディジタルマネーが二度使われた場合に利用者識別情報を追跡する要件が存在することを特定するFPR_PSE.2可逆偽名性を使って、ディジタルマネーが作成できる。利用者が正直者であればその利用者の識別情報は保護され、利用者が不正行為を行おうとすればその利用者の識別情報を追跡することができる。

別の種類のシステムとして、ディジタルクレジットカードがあげられよう。そこでは利用者は、現金が引き落とされる口座を示す偽名を提供する。このような場合、例えば、FPR_PSE.3別名偽名性を使うことができる。このコンポーネントは、利用者識別情報が保護されること、さらに、利用者は、自分が提供した金額(条件にそう特定されていれば)に対して割り付けられた値だけを入手することを特定する。

より厳格なコンポーネントが、識別と認証や監査のような他の要件と組み合わせられない場合があるということを理解すべきである。「識別情報を決定する(determine the identity)」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決定することはできず、利用者やサブジェクトが入手可能な、将来において利用者の識別情報を公開してしまいかねない情報をTSFが記録することもない。

その意図は、TSFは、利用者の識別情報を危うくする情報を一切明らかにしないということである。

例3

利用者を代行するサブジェクトの識別情報。

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。

例4

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。

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は、プロバイダ、システムオペレータ、通信相手、及び利用者を含み、彼らは悪意を持つ部品(マルウェアを含む)をこっそりとシステムに持ち込む。これらの攻撃者は全て、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。

I.3.2 FPR_PSE.1 偽名性

I.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、他の利用者に対する識別情報の暴露に対する利用者保護を提供する。利用者は、そのアクションに対して責任を保持する。

I.3.2.2　操作

FPR_PSE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供しなければならない利用者及び/又はサブジェクトのセットを特定すべきである。

例1

例えば、PP、PPモジュール、機能パッケージ又はSTの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/又はサブジェクトに関しても保護する。

例2

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト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/又は操作、及び/又はオブジェクトのリストを識別すべきである。

例3：求人情報に対するアクセス。

注意：「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。

FPR_PSE.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが提供できる別名の数(1つ又は複数)を識別すべきである。

FPR_PSE.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

I.3.3　FPR_PSE.2 可逆偽名性

I.3.3.1　コンポーネントの根拠と適用上の注釈

このコンポーネントにおいて、TSFは、特定の条件下で、与えられた参照に関連する利用者識別情報が決定できることを保証しなければならない。

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決定できる。

例

電子キャッシュ環境におけるそのような条件:「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決定できる能力を公証人に提供しなければならない」。

I.3.3.2 操作

FPR_PSE.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのセットを特定すべきである。

例1

PP/ST作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。例えば、利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト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/又は操作、及び/又はオブジェクトのリストを識別すべきである。

例2

「求人情報に対するアクセス」

注意：「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。

FPR_PSE.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが提供できる別名の数(1つ又は複数)を識別すべきである。

FPR_PSE.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.2.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、許可利用者及び/又は高信頼サブジェクトが実際の利用者名を決定できるかどうかを選択すべきである。

FPR_PSE.2.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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決定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、時刻のような条件か、あるいは裁判所の命令のような行政的なものがある。

FPR_PSE.2.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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のリストを識別すべきである。

例3

公証人あるいは特別の許可利用者。

I.3.4 FPR_PSE.3 別名偽名性

I.3.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントにおいて、TSFは、提供された参照がある構造規則を満たすこと、それによって、セキュアでない可能性のあるサブジェクトによっても、セキュアな方法で使用されることができることを保証する。

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。

I.3.4.2 操作

FPR_PSE.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのセットを特定すべきである。

例1

PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。

例2

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_PSE.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、サブジェクト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/又は操作、及び/又はオブジェクトのリストを識別すべきである。

例3

「求人情報に対するアクセス」

注意：「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。

FPR_PSE.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが提供できる別名の数(1つ又は複数)を識別すべきである。

FPR_PSE.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.3.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_PSE.3.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSF生成の、あるいは利用者生成の別名が適合すべき尺度を識別すべきである。

FPR_PSE.3.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.4 リンク不能性(FPR_UNL)

I.4.1 利用者のための適用上の注釈

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。

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1

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決定することができる。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。

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なければならないということを暗に示すことになる。さもなければ、これらの情報は、複数の操作をリンクするために使われるかもしれない。

リンク不能性は、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2

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、PPモジュール、機能パッケージ又はSTの作成者は、対抗しなければならない、どのような種類の関係が存在するかを特定できる。

対象となるアプリケーションは、利用者の識別情報を暴露しかねない使用パターンを作成することなしに、1つの偽名を何度も使用させる能力を含むことがある。

例3

敵対的なサブジェクト及び利用者の可能性を持つものは、プロバイダ、システムオペレータ、通信相手、及び利用者を含み、彼らは悪意を持つ部品(例えばマルウェア)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。これらの攻撃者は全て、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。

例4

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呼び出しである。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。

I.4.2 FPR_UNL.1 リンク不能性

I.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者がシステム内の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。

I.4.2.2 操作

FPR_UNL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのセットを特定すべきである。

例1

PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。

例2

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、リンク不能性の要件の対象になるべき操作のリスト、を識別すべきである。

例3：「電子メールの送信」

FPR_UNL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPR_UNL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それに対抗して保護されるべき関係のリストを識別すべきである。

例4：「同じIPアドレスからの発信」

I.5 観察不能性(FPR_UNO)

I.5.1 利用者のための適用上の注釈

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。

観察不能性は、これまでのファミリ、匿名性、偽名性、及びリンク不能性と異なる方向から利用者識別情報を取り上げる。この場合の意図は、利用者の識別情報を隠すよりも、資源あるいはサービスの使用を隠すことである。

多くの技法が、観察不能性を実現するために適用できる。

例

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、Bluetooth、WiFiや近距離無線通信帯域(NFC)を含む、インターネットや無線など)、利用者は、その情報を誰が実際に受信

し、使用したかを決定できない。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。

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なければならない。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、一人又は複数の許可利用者に、資源の使用状況を見る能力を提供する。

このファミリは、「TOEの部分」という概念を使用する。これは、TOEの任意の部分であって、TOE内の他の部分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。

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。

I.5.2 FPR_UNO.1 観察不能性

I.5.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、機能あるいは資源の使用を非許可利用者が観察できないことを要求する。

I.5.2.2 操作

FPR_UNO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのリストを特定すべきである。

例1

PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。

例2

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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を観察できなくなる。

例3

オブジェクトに対する読み取りや書き込み。

FPR_UNO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例4

特定のメールサーバあるいはftpサイト。

FPR_UNO.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、その観察不能性情報が保護される利用者及び/又はサブジェクトのセットを特定すべきである。

例5：「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」。

I.5.3 FPR_UNO.2 観察不能性に影響を与える情報の配置

I.5.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、特定された利用者あるいはサブジェクトが、機能あるいは資源の使用を観察できないことを要求する。さらに、このコンポーネントは、攻撃者がTOE内のどの部分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の複数の部分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。

例1

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つの識別された部分でだけ利用できるものでなければならず、TOEのこの部分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。

例2

もっと複雑な例が、ある「投票アルゴリズム」に見られる。TOEのいくつかの部分がそのサービスに関与するが、TOEの個々の部分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が決定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)。

I.5.3.2 操作

FPR_UNO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがそれらに対して保護を提供する利用者及び/又はサブジェクトのリストを特定すべきである。例えば、PP、PPモジュール、機能パッケージ又はSTの作成者が単一の利用者あるいはサブジェクト役割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/又はサブジェクトに関しても保護しなければならない。

例1

利用者のセットとは、同じ役割の元で操作を行える、あるいは全員が同一のプロセスを使用できる利用者のグループが該当する。

FPR_UNO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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を観察できなくなる。

例2：オブジェクトに対する読み取りや書き込み。

FPR_UNO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、観察不能性要件によってカバーされるオブジェクトのリストを識別すべきである。一例は、特定のメールサーバあるいはftpサイトである。

FPR_UNO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、その観察不能性情報が保護される利用者及び/又はサブジェクトのセットを特定すべきである。

例3：「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」。

FPR_UNO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例4：このような情報として、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含まれる。

FPR_UNO.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例5

このような条件の例としては次のようなものがある。

— 「情報は、TOEの単一の分離した部分だけに置かれねばならず、TOEのこの部分の外部に伝達されてはならない」

— 「情報は、TOEの単一の分離した部分だけに存在しなければならず、TOEの別の部分に定期的に移動されなければならない」

— 「情報は、TOEのどの5つの分離した部分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の異なる部分間に分散されなければならない」

I.5.4 FPR_UNO.3 情報を請求しない観察不能性

I.5.4.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、特定のサービスが提供されるときに、TSFが、観察不能性を損なうかもしれない情報を取得しようと試みないことを要求するために使用される。そのために、TSFは、観察不能性を危うくするために使われるかもしれないどのような情報も求めることはない(つまり、他のエンティティから取得しようと試みない)。

I.5.4.2 操作

FPR_UNO.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、観察不能性要件の対象となるサービスのリストを識別すべきである。

例1：「職務記述書へのアクセス」。

FPR_UNO.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、特定されたサービスの提供時に、そのサブジェクトからプライバシー関連情報を保護すべきサブジェクトのリストを識別すべきである。

FPR_UNO.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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2

プライバシー関連情報の例として、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。

I.5.5 FPR_UNO.4 許可利用者観察可能性

I.5.5.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、資源利用を調べる権限を持つ一人又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。

I.5.5.2 操作

FPR_UNO.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、資源利用を観察する能力をTSFが提供する許可利用者のセットを特定すべきである。例えば、許可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許可利用者のグループが該当する。

FPR_UNO.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、許可利用者が観察できなければならない資源及び/又はサービスを特定すべきである。

附属書J
(規定)

FPTクラス：TSFの保護 — 適用上の注釈

J.1 一般

このクラスは、TSFを構成するメカニズムの完全性と管理、及び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。

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。

FPT: TSFの保護クラスにおけるファミリの全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) TOE放出(FPT_EMS)、これは、放出によるTOEからの情報漏洩の可能性に対応する。

b) 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。

c) TSF初期化(FPT_INI)、これは、TOEの正しくセキュアな運用状態への初期化に対応する。

d) TOE内TSFデータ転送(FPT_ITT)、これは、TOEの物理的に分離した部分間で伝送されるときのTSFデータの保護に対応する。

e) TSF物理的保護(FPT_PHP)、これは、TSFを構成するTOEの部分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。

f) 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。

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

h) 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の異なる部分間の状態の同期に対応する。

i) 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。

j) 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。

k) 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。

J.2 TOE放出(FPT_EMS)

J.2.1 利用者のための適用上の注釈

このファミリは、TOEに保存され使用されるデータに対する攻撃が、TOEの外部から観測可能な物理現象に基づくものである場合に、TOEがその攻撃を防止又は軽減できるための要件を定義する。

例

このような攻撃の例として、TOEの電磁放射の解析、単純電力解析(SPA)、差分電力解析(DPA)、タイミング攻撃などがある。

FPT_EMS.1.1 放出の制限は、TOEに、TSFデータ又は利用者データへのアクセスを可能にする感知できる放出物を放出しないよう要求する。

J.2.2 FPT_EMS.1 TOE放出

J.2.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントを特定するには、攻撃対象領域と組み合わされた任意の放出に関連するTSFデータ及び/又は利用者データの任意の組み合わせの関係表現が要求される。データ、放出、攻撃対象領域は類型化することができる。

FPT_EMS.1.1 放出の制限のエレメントの一部として含まれる**FPT_EMS.1.1の表**は、PP、PPモジュール、機能パッケージ又はSTの作成者が完成させなければならない。各行は「識別子」を用いて識別され、PP、PPモジュール、機能パッケージ又はSTの作成者が、放出、インタフェース、TSFデータ及び利用者データの様々な異なる組み合わせに対するTOEの放出防止の要件を特定できるように、SFRの完成に必要な一連の割付を提供する。

作成者が全ての種類の放出及び攻撃対象領域等を一行に入力することは想定されていない。

例

放出の種類には、音波や電磁波が含まれる。

インタフェースの種類には、ICの境界面、電子部品が含まれる。

J.2.2.2 操作

このコンポーネントに対して特定の操作は存在しない。

J.3 フェールセキュア(FPT_FLS)

J.3.1 利用者のための適用上の注釈

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。

J.3.2 FPT_FLS.1 セキュアな状態を保持する障害

J.3.2.1 コンポーネントの根拠と適用上の注釈

「セキュアな状態」という用語は、TSFデータに一貫性があり、TSFがSFRの正しい実施を継続している状態を指す。

セキュアな状態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、全ての状況でそれが可能なわけではない。PP、PPモジュール、機能パッケージ又はSTの作成者は、監査が望まれ、かつ実行可能な状況を特定すべきである。

TSFにおける障害には、「ハード」障害が含まれることがあり、これは機器の不調を示すもので、TSFのメンテナンス、サービス、あるいは修復が必要かもしれない。TSFにおける障害には、回復可能な「ソフト」障害も含まれることがあり、これは、TSFの初期化あるいはリセットだけを必要とするかもしれない。

J.3.2.2 操作

FPT_FLS.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.4 TSF初期化(FPT_INI)

J.4.1 利用者のための適用上の注釈

このファミリは、TSFの初期化に関する機能要件を定義する。TOEの専用機能は、TSFの初期化が正しくセキュアな運用状態になることを保証する。これは、起動時に変更不可能なメモリに格納され実行されるコード/データ、不変のルートオブトラスト、及びバージョンや識別子などその他のワンタイムプログラマブル(OTP)値をカバーすることができる。

J.4.2 FPT_INI.1 TSF初期化

J.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントでは、例えば、起動時に変更不可能なメモリに格納され実行されるコード/データ、不変のルートオブトラスト、及びバージョンや識別子などのその他のOTP値をカバーする。

J.4.2.2 操作

FPT_INI.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、エレメント内の割付表形式を使用して、特性とそれらが適用される要素を列挙しなければならない。

例

特性には、真正性、完全性、正しいバージョンなどが含まれ、特性が適用される要素には、TSF又は利用者のファームウェア、ソフトウェア又はデータなどが含まれる。

作成者が1行に全ての特性と要素を入力することは想定されていない。

FPT_INI.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、初期化中にエラーやその他の障害が発生した場合のTOE初期化機能の動作を、選択と割付を用いて記述する。

FPT_INI.1.4において、PP、PPモジュール、機能パッケージ又はSTの作成者は、割付を使用して、TOE初期化機能がTSFと相互作用するための方法を記述する。

J.5エクスポートされたTSFデータの可用性(FPT_ITA)

J.5.1 利用者のための適用上の注釈

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。

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した状況で使用される。TSFは、そのサイトにおいての処置を講じられるだけで、他方の高信頼IT製品のTSFに対しては責任を持つことができない。

もし、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。

J.5.2 FPT_ITA.1 定義された可用性尺度内のTSF間可用性

J.5.2.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

J.5.2.2 操作

FPT_ITA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、可用性尺度の対象となるTSFデータの種別を特定すべきである。

FPT_ITA.1.1において、PP、PPモジュール、機能パッケージ又はSTは、適用可能なTSFデータに対する可用性尺度を特定すべきである。

FPT_ITA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、可用性が保証されなければならない条件を特定すべきである。

例：TOEと他の高信頼IT製品間に接続がなければならない。

J.6エクスポートされたTSFデータの機密性(FPT_ITC)

J.6.1 利用者のための適用上の注釈

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。

例

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。

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した状況で使用される。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。

J.6.2 評価者のための注釈

送信中のTSFデータの機密性は、そのような情報を暴露から保護するために必要である。

例

機密性を提供できるような実装としては、スペクトラム拡散技術はいうまでもなく、暗号アルゴリズムの使用も含まれる。

J.6.3 FPT_ITC.1 送信中のTSF間機密性

J.6.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFデータをTSFから他の高信頼IT製品へ送信する際に、機密性に関する要件を特定する必要がある場合に使用される。

J.6.3.2 操作

このコンポーネントでは、操作は指定されていない。

J.7 エクスポートされたTSFデータの完全性(FPT_ITI)

J.7.1 利用者のための適用上の注釈

J.7.1.1 一般

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。

例

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。

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した状況で使用される。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決定できないので、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。

J.7.1.2 評価者のための注釈

FPT_ITI.2では、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。

J.7.2 FPT_ITI.1 TSF間改変の検出

J.7.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、いつデータが改変されたかを検出するので十分な状況において使われるべきである。そのような状況の例は、改変が検出された場合に他の高信頼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。

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。

J.7.2.2 操作

FPT_ITI.1.1において、PP、PPモジュール、機能パッケージ又はSTは、検出メカニズムが満たす改変尺度を特定すべきである。この改変尺度は、改変検出の望まれる強度を特定しなければならない。

FPT_ITI.1.2において、PP、PPモジュール、機能パッケージ又はSTは、もしTSFデータの改変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。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。

J.7.3 FPT_ITI.2 TSF間改変の検出と訂正

J.7.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFの重要なデータの改変に対する検出あるいは訂正が必要な状況において使用されるべきである。

改変の検出に望まれる強度は、使用されたアルゴリズムの機能である特定された改変尺度に基づき、その機能は、複数ビットの変化の検出に失敗するかもしれないチェックサム及びパリティメカニズムから、もっと複雑な暗号チェックサムのアプローチまでの幅を持つ。定義する必要のある尺度は、それが抵抗する攻撃、あるいは公の文献で広く知られたメカニズムを参照することができる。

例

参照する攻撃：「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」

広く知られたメカニズム：「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」

改変を訂正するためにとられるアプローチは、誤り訂正チェックサムの形式などを通して行うことができる。

J.7.3.2 操作

FPT_ITI.2.1において、PP、PPモジュール、機能パッケージ又はSTは、検出メカニズムが満たす改変尺度を特定すべきである。この改変尺度は、改変検出の望まれる強度を特定しなければならない。

FPT_ITI.2.2において、PP、PPモジュール、機能パッケージ又はSTは、もしTSFデータの改変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。

例

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.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.8 TOE内TSFデータ転送(FPT_ITT)

J.8.1 利用者のための適用上の注釈

このファミリは、TSFデータが内部チャネルを介してTOEの分離した部分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。

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)の度合いの決定は、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の部分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。

J.8.2 評価者のための注釈

この保護を提供するためにTSFが利用可能な実用的メカニズムの1つは、暗号技術に基づくメカニズムである。

J.8.3 FPT_ITT.1 基本TSF内データ転送保護

J.8.3.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

J.8.3.2 操作

FPT_ITT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

J.8.4 FPT_ITT.2 TSFデータ転送分離

J.8.4.1 コンポーネントの根拠と適用上の注釈

SFP関連属性に基づくTSFデータの分離を達成する方法の1つは、分離した論理又は物理チャネルの使用によるものである。

J.8.4.2 操作

FPT_ITT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

J.8.5 FPT_ITT.3 TSFデータ完全性監視

J.8.5.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

J.8.5.2 操作

FPT_ITT.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFが検出できなければならない改変の望ましい種別を特定すべきである。PP、PPモジュール、機能パッケージ又はSTの作成者は、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、あるいはその他全ての完全性誤りから選択すべきである。

FPT_ITT.3.1において、もしPP、PPモジュール、機能パッケージ又はSTの作成者は、前の段落において注釈された最後の選択を選ぶ場合、作成者は、TSFが検出の能力を持つべきそれらの他の完全性誤りが何であるかについても特定すべきである。

FPT_ITT.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.9 TSF物理的保護(FPT_PHP)

J.9.1 利用者のための適用上の注釈

TSF物理的保護コンポーネントは、TSFに対する許可されない物理的アクセスにおける制約、及び許可されない物理的改変の抑止及び抵抗、あるいはTSFの置換に関係する。

このファミリの要件は、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がどのように応答するかに関する要件も提供する。

例1

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、温度変更、などがある。

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、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)する。つまり、全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。

例2：構造体の例としては、外部シールド、カード、及びチップが含まれる。

これらのコンポーネントに関係しては最小限の監査があるだけだが、これは単に、監査サブシステムとの対話レベルの下で、検出及び警報メカニズムが完全にハードウェアに実装されるかもしれないという可能性のためである。とは言え、PP、PPモジュール、機能パッケージ又はSTの作成者は、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決定するかもしれない。このような場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、監査事象のリストに適切な要件を含めるべきである。

注：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。

例3

ハードウェアベースの検知システムの例として、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)の点灯に基づくものがある。

J.9.2 FPT_PHP.1 物理的攻撃の受動的検出

J.9.2.1 コンポーネントの根拠と適用上の注釈

FPT_PHP.1物理的攻撃の受動的検出は、TOEの一部分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_LIM.1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。もしこれが物理的な検査などの非ITメカニズムでなされる場合は、管理機能は要求されない。

J.9.2.2 操作

このコンポーネントでは、操作は指定されていない。

J.9.3 FPT_PHP.2 物理的攻撃の通知

J.9.3.1 コンポーネントの根拠と適用上の注釈

TOEの一部分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。

J.9.3.2 操作

FPT_PHP.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPT_PHP.2.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又は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_LIM.1ファミリの)によって異なることがある。

J.9.4 FPT_PHP.3 物理的攻撃への抵抗

J.9.4.1 コンポーネントの根拠と適用上の注釈

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。

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。

例：物理的改ざんは、観察、分析、あるいは改変を含む。

J.9.4.2 操作

FPT_PHP.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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

方針の保護の例：

機密性の方針に関して、保護された情報が取得され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。

FPT_PHP.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.10高信頼回復(FPT_RCV)

J.10.1 利用者のための適用上の注釈

J.10.1.1 一般

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が決定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定するからである。

回復コンポーネントは、予想される障害、動作の中断、あるいは立ち上げの発生に対する直接の応答として、TSFのセキュアな状態を再構築し、あるいはセキュアでない状態への移行を防ぐ。

例

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又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、インターネット接続の喪失)。

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)。

注：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。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。

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、又はメンテナンスモードに移るかのどちらか一方を行う。

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。

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。

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。

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。

J.10.1.2 評価者のための注釈

FPT_RCV.1において、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。

FPT_RCV.2において、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。

FPT_RCV.2.1に対して、回復可能な障害及びサービス中断のセットを決定するのは、TSFの開発者の責任である。

自動回復メカニズムの堅牢性が検証されることが想定される。

FPT_RCV.3において、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。

評価者は自動回復メカニズムの堅牢性を検証することが想定される。

J.10.2 FPT_RCV.1 手動回復

J.10.2.1 コンポーネントの根拠と適用上の注釈

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。

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。

J.10.2.2 操作

FPT_RCV.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEがメンテナンスモードに移る、障害又はサービス中断のリストを特定するべきである。

例：停電、監査格納の領域枯渇、あらゆる障害又は中断。

J.10.3 FPT_RCV.2 自動回復

J.10.3.1 コンポーネントの根拠と適用上の注釈

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。

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。

J.10.3.2 操作

FPT_RCV.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEがメンテナンスモードに移る必要がある、障害又はサービス中断のリストを特定するべきである。

例：停電、監査格納の領域枯渇。

FPT_RCV.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それに対して自動回復が可能でなければならない障害又は他の中断のリストを特定しなければならない。

J.10.4 FPT_RCV.3 過度の損失のない自動回復

J.10.4.1 コンポーネントの根拠と適用上の注釈

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。

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、オブジェクトを全て削除し、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。

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。

J.10.4.2 操作

FPT_RCV.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEがメンテナンスモードに移る必要がある、障害又はサービス中断のリストを特定するべきである。

例：停電、監査格納の領域枯渇。

FPT_RCV.3.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、それに対して自動回復が可能である障害又は他の中断のリストを特定すべきである。

FPT_RCV.3.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

J.10.5 FPT_RCV.4 機能回復

J.10.5.1 コンポーネントの根拠と適用上の注釈

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。

J.10.5.2 操作

FPT_RCV.4.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.11リプレイ検出(FPT_RPL)

J.11.1 利用者のための適用上の注釈

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。

J.11.2 FPT_RPL.1 リプレイ検出

J.11.2.1 コンポーネントの根拠と適用上の注釈

ここに含まれるエンティティは、リプレイ検出に関連する可能性があるものである。

例：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。

J.11.2.2 操作

FPT_RPL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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。

FPT_RPL.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.12状態同期プロトコル(FPT_SSP)

J.12.1 利用者のための適用上の注釈

分散TOEは、TOEの部分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。

状態同期プロトコル(FPT_SSP)は、高信頼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つの分散した部分(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。

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。

例1

暗号鍵失効が一例であり、そこでは、失効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応答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失効が行われないのか。

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。PP、PPモジュール、機能パッケージ又はSTの作成者は、そのような場合、他の要件を表すべきである。

例2：警報を発生する、事象を監査する。

J.12.2 FPT_SSP.1 単純な高信頼確認応答

J.12.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントでは、TSFは、要求されたときにTSFの他の部分に確認応答を与える。この確認応答は、分散TOEの1つの部分が、分散TOEの別の部分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。

J.12.2.2 操作

このコンポーネントに対して特定の操作は存在しない。

J.12.3 FPT_SSP.2 相互の高信頼確認応答

J.12.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントにおいて、TSFがデータ送信の受信に対する確認応答を提供できることに加え、TSFは、TSFの他の部分からの、確認応答に対する確認応答の要求に応じる。

例

ローカルTSFがTSFのリモート部分にデータを送信する。TSFのリモート部分は、そのデータの正常受信に確認応答し、送信TSFに対して確認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の両方の部分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.12.3.2 操作

このコンポーネントに対して特定の操作は存在しない。

J.13タイムスタンプ(FPT_STM)

J.13.1 利用者のための適用上の注釈

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。

「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、PPモジュール、機能パッケージ又はSTの作成者の責任である。

J.13.2 FPT_STM.1 高信頼タイムスタンプ

J.13.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントが使えそうなものとして、セキュリティ属性の有効期限に対してはもちろん、監査目的のための高信頼タイムスタンプの提供というものがある。

J.13.2.2 操作

このコンポーネントに対して特定の操作は存在しない。

J.14TSF間TSFデータ一貫性(FPT_TDC)

J.14.1 利用者のための適用上の注釈

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データを交換する必要があるかもしれない。

例：データに関連したSFP属性、監査情報、識別情報。

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。

このファミリのコンポーネントは、TOEのTSFと他の高信頼IT製品の間でTSFデータを送信するとき、TSFデータの一貫性に対する自動化されたサポートのための要件を提供する。全面的に手続き的な方法でセキュリティ属性の一貫性を作り出せるという可能性もあるが、それらは、ここでは提供されない。

このファミリは、FDP_ETC及びFDP_ITCと異なっており、それは、これら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。

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、転送中の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。

J.14.2 FPT_TDC.1 TSF間基本TSFデータ一貫性

J.14.2.1 コンポーネントの根拠と適用上の注釈

TSFは、特定された機能によって使われあるいは関係し、かつ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

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。

J.14.2.2 操作

FPT_TDC.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPT_TDC.1.2において、PP、PPモジュール、機能パッケージ又はSTは、TSFによって適用されるべき解釈規則のリストを割り付けるべきである。

J.15外部エンティティのテスト(FPT_TEE)

J.15.1 利用者のための適用上の注釈

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/又は、ハードウェアの組み合わせが含まれる。

例

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)

注：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。

J.15.2 評価者のための注釈

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全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において、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、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。

J.15.3 FPT_TEE.1 外部エンティティのテスト

J.15.3.1 コンポーネントの根拠と適用上の注釈

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。

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。

PP、PPモジュール、機能パッケージ又は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。

J.15.3.2 操作

FPT_TEE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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なければならない。

FPT_TEE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例1

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。

FPT_TEE.1.1において、PP、PPモジュール、機能パッケージ又は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。

例2

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。

FPT_TEE.1.2において、PP、PPモジュール、機能パッケージ又は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3

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.16TOE内TSFデータ複製一貫性(FPT_TRC)

J.16.1 利用者のための適用上の注釈

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の部分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が内部的にTOEの部分のネットワークとして構成されている場合、一部分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。

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、PPモジュール、機能パッケージ又はSTに必要であれば、それは、詳細化によって特定することができる。

ある状態を同期させることは不可能かもしれず、あるいはそのような同期のコストが高すぎるかもしれない。

例：この状況の例は、通信チャネルと暗号鍵失効である。

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。

J.16.2 FPT_TRC.1 TSF内一貫性

J.16.2.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

J.16.2.2 操作

FPT_TRC.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.17TSF自己テスト(FPT_TST)

J.17.1 利用者のための適用上の注釈

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

例としては、実施機能に対するインタフェースや、TOEの重要な部分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、定期的に、許可利用者の要求時に、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。

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)を必ずしも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実行コード又は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しも防げるとは限らないので、これらのチェックが実行される。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/又は物理的保護に起因する、TSFの悪意の破壊のために生じ得る。

加えて、適切な条件でこのコンポーネントを使用することは、メンテナンスアクティビティの結果として、不適切な、あるいは損害を与えるTSF変更が動作中のTOEに適用されるのを防ぐのに役立つかもしれない。

「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。

J.17.2 評価者のための注釈

FPT_TST.1 TSF自己テストにおいて、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。

J.17.3 FPT_TST.1 TSFテスト

J.17.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、テスト機能を呼び出し、かつTSFデータと実行コードの完全性をチェックする能力を要求することによって、TSFの動作の重要な機能をテストすることに対するサポートを提供する。

J.17.3.2 操作

FPT_TST.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFがTSFテストをするときを特定すべきである。初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、他の条件で。また、最後の選択肢において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPT_TST.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、自己テストが、全ての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。

FPT_TST.1.1において、もし選択されれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、自己テストが行われるべき条件を特定すべきである。

FPT_TST.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPT_TST.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、データの完全性の検証が、全ての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。

FPT_TST.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

FPT_TST.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFの完全性の検証が、全ての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。

FPT_TST.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

注：FCS_RBG.1が選択された場合、FCS_RBG.1で選択された標準はTSFが実行する自己テストスイートを要求することができる。PP、PPモジュール、機能パッケージ又はSTの作成者は、標準の全部又は参照された特定の部分のみを満たすように、選択された各標準を検討する(CCパート1、B.4及びD.5を参照)。

附属書K
(規定)

FRUクラス：資源利用 ― 適用上の注釈

K.1 一般

このクラスは、処理能力及び/又は格納容量など、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。

K.2 耐障害性(FRU_FLT)

K.2.1 利用者のための適用上の注釈

このファミリは、障害の発生時でも能力を利用可能にする要件を規定する。

例1：このような障害の例には、停電、ハードウェアの障害、又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は指定された能力を維持する。

例2

PP、PPモジュール、機能パッケージ又はSTの作成者は、原子力発電所で使用されるTOEが、停電又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。

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。

耐障害性を提供するメカニズムは、能動的又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)。

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。

K.2.2 FRU_FLT.1 機能削減された耐障害性

K.2.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、システムの障害後、それにもかかわらずTOEがどの能力を提供するかを特定しようとするものである。全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。

例

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。

K.2.2.2 操作

FRU_FLT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、特定された障害の間及びその後にTOEが維持するTOE能力のリストを特定すべきである。

FRU_FLT.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEが明示的に保護されなけれ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.2.3 FRU_FLT.2 制限付き耐障害性

K.2.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、どのような障害の種別にTOEが抵抗するかを特定しようとするものである。全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。

例

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。

K.2.3.2 操作

FRU_FLT.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TOEが明示的に保護されなけれ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.3 サービス優先度(FRU_PRS)

K.3.1 利用者のための適用上の注釈

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。

このファミリは、いくつかの資源の種別に適用できる。

例：処理容量及び通信チャネル容量。

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。

監査要件は、拒絶に対する全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。

K.3.2 FRU_PRS.1 制限付きサービス優先度

K.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、サブジェクトに対する優先度と、この優先度が使用される資源を定義する。もしサブジェクトが、サービス優先度要件によって制御される資源に対してアクションをとろうと試みる場合、そのアクセス及び/又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.3.2.2 操作

FRU_PRS.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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：プロセス、ディスク領域、メモリ、帯域幅などの資源

K.3.3 FRU_PRS.2 完全サービス優先度

K.3.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、サブジェクトに対する優先度を定義する。TSF制御下の全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/又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.3.3.2 操作

このコンポーネントでは、操作は指定されていない。

K.4 資源割当て(FRU_RSA)

K.4.1 利用者のための適用上の注釈

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。

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量の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。

例1

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/又はサイズを制限するオブジェクト割当てを提供する。

— TSFの制御下にある事前に割り付けられた資源ユニットの、割当て/割当て解除を制御する。

一般に、これらの機能は、利用者及び資源に割り付けられた属性の使用を通して実現される。

これらのコンポーネントの目的は、利用者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。

例2：単一の利用者が利用可能な全ての空間を割り当てるべきではない。

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悪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3：メインメモリあるいはCPUサイクル。

その実施例においては、このコンポーネントは、資源割当てがサブジェクトのレベルにあることを認める。

このファミリは、資源自体の使用においてではなく、資源の割当てにおける要件を課する。そのため、監査要件も、資源の使用についてではなく、資源の割当てについて適用する。

K.4.2 FRU_RSA.1 最大割当て

K.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEにおける共有可能資源の特定されたセットだけに適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、割当てを利用者に関連付けること、TOEに適用できる場合には利用者あるいはサブジェクトのグループに割り付けることを認める。

K.4.2.2 操作

FRU_RSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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：制御される資源の例としては、プロセス、ディスク領域、メモリ、帯域幅がある。

もしTSF制御下の全ての資源が含まれる必要があれば、「全てのTSF資源」という語を特定することができる。

FRU_RSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、最大割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

K.4.3 FRU_RSA.2 最小及び最大割当て

K.4.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEにおける共有可能資源の特定されたセットに適用される、割当てメカニズムに対する要件を提供する。この要件は、ある利用者に関連付けられる割当てが、TOEに適用できる範囲で、利用者あるいはサブジェクトのグループに割り付けられることを認める。

K.4.3.2 操作

FRU_RSA.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

もしTSF制御下の全ての資源が含まれる必要があれば、「全てのTSF資源」という語を特定することができる。

FRU_RSA.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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る。

もしTSF制御下の全ての資源が含まれる必要があれば、「全てのTSF資源」という語を特定することができる。

例：制御される資源の例としては、プロセス、ディスク領域、メモリ、帯域幅がある。

FRU_RSA.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、最大割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、最小割当てを、個々の利用者、定義された利用者グループ、あるいはサブジェクト、あるいはこれらの任意の組み合わせに適用するかどうかを選択すべきである。

FRU_RSA.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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
(規定)

FTAクラス：TOEアクセス ― 適用上の注釈

L.1 一般

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つ又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機能要件を特定する。

利用者セションは、識別/認証の時点、あるいは、もし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全てのサブジェクト(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。

L.2 選択可能属性の範囲制限(FTA_LSA)

L.2.1 利用者のための適用上の注釈

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/又は時間。

例1: 時刻、曜日。

このファミリは、PP、PPモジュール、機能パッケージ又はSTの作成者が、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2

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。

例3

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:

— 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)。

— 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。

— 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。

L.2.2 FTA_LSA.1 選択可能属性の範囲制限

L.2.2.1 コンポーネントの根拠と適用上の注釈

コンポーネントの根拠や適用上の注釈は提供されていない。

L.2.2.2 操作

FTA_LSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例1：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。

FTA_LSA.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例2

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.3 複数同時セションの制限(FTA_MCS)

L.3.1 利用者のための適用上の注釈

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。

L.3.2 FTA_MCS.1 複数同時セションの基本制限

L.3.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TOEの資源を効果的に使用するために、システムがセションの数を制限することを認める。

L.3.2.2 操作

FTA_MCS.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.3.3 FTA_MCS.2 複数同時セションの利用者属性ごと制限

L.3.3.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者が行使できる同時セションの数に対し、課すべき制約を増やすことを認めることによって、FTA_MCS.1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。

L.3.3.2 操作

FTA_MCS.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例

規則の例は、「同時セションの最大数は、利用者の秘密区分レベルが『秘密』の場合は1、その他は5とする」である。

FTA_MCS.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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.4 セションロックと終了(FTA_SSL)

L.4.1 利用者のための適用上の注釈

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。

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、PPモジュール、機能パッケージ又はSTの作成者によって特定された事象が起こらなければならない。

利用者は、もしある特定の期間、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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、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なければならない。

L.4.2 FTA_SSL.1 TSF起動セションロック

L.4.2.1 コンポーネントの根拠と適用上の注釈

FTA_SSL.1 TSF起動セションロックは、TSFが特定した期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。

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)。

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、PPモジュール、機能パッケージ又はSTの作成者が特定することを認める。これらの事象は、端末、利用者又は時間に関連する場合がある。

例

事象の例を以下に示す:

— 端末関連：セションのロックを解除するキーストロークの固定したセット

— 利用者関連：再認証

— 時間関連：15分後

L.4.2.2 操作

FTA_SSL.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、PPモジュール、機能パッケージ又はSTの作成者は、その時間間隔の特定を許可管理者あるいは利用者に任せることを、割付によって特定することができる。FMTクラスにおける管理機能は、この時間をデフォルト値にし、それを修正する能力を特定できる。

FTA_SSL.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。

例：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。

L.4.3 FTA_SSL.2 利用者起動ロック

L.4.3.1 コンポーネントの根拠と適用上の注釈

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なけれ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。

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)。

L.4.3.2 操作

FTA_SSL.2.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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しなければならない。

例：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。

L.4.4 FTA_SSL.3 TSF起動による終了

L.4.4.1 コンポーネントの根拠と適用上の注釈

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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者が彼/彼女のアクティビティを終了した後も、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。

例：利用者がアクティビティを終了した後も、セションが継続している例としては、バックグラウンド処理がある。

L.4.4.2 操作

FTA_SSL.3.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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。要求があれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、その間隔の特定を許可管理者あるいは利用者に任せることを、割付によって特定することができる。FMTクラスにおける管理機能は、この時間をデフォルト値にし、それを修正する能力を特定できる。

L.4.5 FTA_SSL.4 利用者起動による終了

L.4.5.1 コンポーネントの根拠と適用上の注釈

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。

PP、PPモジュール、機能パッケージ又はSTの作成者は、利用者が彼/彼女のアクティビティを終了した後も、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。

例：利用者がアクティビティを終了した後も、セションが継続している例としては、バックグラウンド処理がある。

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.4.5.2 操作

このコンポーネントでは、操作は指定されていない。

L.5 TOEアクセスバナー(FTA_TAB)

L.5.1 利用者のための適用上の注釈

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。

L.5.2 FTA_TAB.1 デフォルトTOEアクセスバナー

L.5.2.1 コンポーネントの根拠と適用上の注釈

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、PPモジュール、機能パッケージ又はSTの作成者は、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.5.2.2 操作

このコンポーネントでは、操作は指定されていない。

L.6 TOEアクセス履歴(FTA_TAH)

L.6.1 利用者のための適用上の注釈

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。

L.6.2 FTA_TAH.1 TOEアクセス履歴

L.6.2.1 コンポーネントの根拠と適用上の注釈

このファミリは、その利用者アカウントの悪用の可能性を示す情報を許可利用者に提供できる。

このコンポーネントは、利用者が情報を提示されることを要求する。利用者は、情報をレビューできるべきであるが、それを強制はされない。

例：利用者は、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。

L.6.2.2 操作

FTA_TAH.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、及び/又は場所がある。

FTA_TAH.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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、及び/又は場所がある。

例

アクセスの方法：ftp

場所：端末50

L.7 TOEセション確立(FTA_TSE)

L.7.1 利用者のための適用上の注釈

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、時間の範囲、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。

例1

セキュリティ属性：識別情報、取扱許可レベル、完全性レベル、役割における資格。

時間の範囲：時刻、曜日、カレンダの日付。

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、PPモジュール、機能パッケージ又はSTの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。

例2

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が利用できる環境で使用するのに最適である。

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

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。

c) 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、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。

L.7.2 FTA_TSE.1 TOEセション確立

L.7.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントには、コンポーネントの根拠や適用上の注釈は提供されていない。

L.7.2.2 操作

FTA_TSE.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、セション確立を制限するために使うことができる属性を特定すべきである。

例

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、telnet)など。

附属書M
(規定)

FTPクラス：高信頼パス/チャネル ― 適用上の注釈

M.1 一般

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。

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。

M.2 TSF間高信頼チャネル(FTP_ITC)

M.2.1 利用者のための適用上の注釈

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。

例

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。

M.2.2 FTP_ITC.1 TSF間高信頼チャネル

M.2.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、TSFと他の高信頼IT製品間に高信頼通信チャネルが要求されるときに、使用される。

M.2.2.2 操作

FTP_ITC.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、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なければならないかどうかを特定しなければならない。

FTP_ITC.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼チャネルを必要とする機能を特定すべきである。

例

これらの機能の例には、利用者、サブジェクト、及び/又はオブジェクトのセキュリティ属性の転送、及びTSFデータの一貫性の保証がある。

M.3 高信頼チャネルプロトコル(FTP_PRO)

M.3.1 利用者のための適用上の注釈

このファミリは、TSFと他の高信頼IT製品間に張られデータ転送を保護するための、高信頼チャネル接続の作成のための規則を定義する。FTP_ITCやFTP_TRPとは対照的に、FTP_PROは、チャネルに使用されるプロトコルのセキュリティの詳細に関するもので、多数の別々のSFRに分割することができるプロトコルの特性に焦点を当てる。FTP_PROは、他のSFR(FCS_COP.1など)に記述されている暗号機能にリンクすることができるプロトコル内のメカニズムを強調することで、PP、PPモジュール、機能パッケージ又はSTの明確性を向上させることができる。

FTP_PROのコンポーネントは階層化されていないが、機密性及び完全性保護機能など、高信頼チャネルのさまざまな側面を個別に特定するために一緒に使用されることを意図している。

共有秘密の確立のセキュリティに関するメカニズムは、FTP_PRO.2自体に記述されているメカニズムの一部となるため、FTP_PRO.2からFTP_PRO.3への依存性はない。

高信頼チャネルプロトコルで使用される暗号操作の一部がTOEの外部で実行される場合、FTP_PRO.2及び/又はFTP_PRO.3はPP、PPモジュール、機能パッケージ又はSTから省略することができ、ST作成者は、FTP_PROコンポーネントの間で満たされない依存性の理由を提示する必要があるだろう。

チャネルごとにSFRを完成させる必要がある場合、関連するFTP_PROコンポーネントの別々の繰返しを使用することができる。一般的に、それぞれの個別の繰返しは、依存性の根拠となる3つのコンポーネントを全て含む必要がある。

M.3.2 FTP_PRO.1 高信頼チャネルプロトコル

M.3.2.1 コンポーネントの根拠と適用上の注釈

FTP_PROの操作の完了時に使用される値が、異なるSFRエレメント間の依存性を持つ場合、SFRのインスタンス化で明確にする必要がある。

例

列が選択と割付を表し、行が値の有効な組み合わせを定義する表を与えることができる。

M.3.2.2 操作

FTP_PRO.1.1において、選択された場合、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼チャネルプロトコル及び定義済みのプロトコル上の役割を特定しなければならない。

例1

「定義済みのプロトコル上の役割」の例としては、「クライアント」又は「サーバ」(TLS)、「イニシエータ」又は「レスポンダ」(IKEv2/IPsec)、「トラストセンター」(ZigBee)又は「鍵配布センター」(Kerberos)などが挙げられる。

FTP_PRO.1.2において、最初の割付は、監査サーバとの通信に高信頼チャネルを使用することを義務付けるなど、TOEが高信頼チャネルを使用する必要がある場合の規則を示すことを

目的としている。この割付は、TOEにチャネルの特定の使用が義務付けられていない場合、「指定なし」(2番目の割付でも「指定なし」)という値を取ることができる。

FTP_PRO.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼チャネルの確立を開始することを許可されるエンティティを選択することができる。

FTP_PRO.1.5では、割付はプロトコルの実装に関連する規則を記載することを意図している。規則が不要な場合、又はSFRの他のエレメントで参照される標準に関連規則が含まれ、SFRが使用されるコンテキストで特定の評価者のチェックが必要ない場合は、「指定なし」の値を取ることができる。

例2：規則には、最大パケットサイズや鍵更新間隔が含まれる。

FTP_PRO.1.6において、割付は、プロトコルを定義する標準と比較してTOEが提供するオプションを狭めることを意図している場合、プロトコルのネゴシエーション可能な側面に関連する規則を記載することを意図している。

例3：許容可能な古いプロトコルのバージョンの特定

割付は、規則が要求されない場合、値「指定なし」を取ることができる。割付がリストで完了する場合、そのリストでは許可される唯一の構成が指定され、それ以外の構成はSFRの違反となる。このエレメントは、例えば、リストの各項目の後に「(サポート必須)」を付けて必須構成を列挙し、標準で許可された他の構成が許可されることを示す最終要素を含めることによって、TOEがこれらの構成を使用することを制限せずに、必須のサポート構成を特定するために使用することができる。

M.3.3 FTP_PRO.2 高信頼チャネル確立

M.3.3.1 コンポーネントの根拠と適用上の注釈

FTP_PRO.2において、「認証を実行するための規則のリスト」を使用して、認証メカニズムに利用可能なパラメタを制限することができる。

例

交換する認証データに識別子の代替ソースがある場合、識別子のフォーマット(FQDN又はIPアドレス、ワイルドカードの使用など)又は優先順位について規則を記述することができる。

M.3.3.2 操作

FTP_PRO.2.2において、認証の方向を示す選択肢を選択すべきである

FTP_PRO.2.1において、PP、PPモジュール、機能パッケージ又はSTの作成者が、鍵確立メカニズムのリストを提供する。

FTP_PRO.2.2において、割付は、認証時に使用される認証メカニズムのリストと、認証時に使用されるルールのリストを提供することを含む。

M.3.4 FTP_PRO.3 高信頼チャネルのデータ保護

M.3.4.1 コンポーネントの根拠と適用上の注釈

FTP_PRO.3コンポーネントは、高信頼チャネルを介して転送されるデータの保護(機密性、完全性)に対応する。

M.3.4.2 操作

PP、PPモジュール、機能パッケージ又はSTの作成者は、TSFによって軽減される攻撃を選択する。

PP、PPモジュール、機能パッケージ又はSTの作成者は、暗号化及び完全性保護メカニズムのリストを指定することで、割付を完了させる。

例

完全性保護メカニズムの例としては、システムファイルやシステムディレクトリに対するその内容やファイルシステム上のパーミッションの保護、コードインジェクションに対するプロセスの保護、未署名のカーネル拡張に対する保護が含まれる。

M.4 高信頼パス(FTP_TRP)

M.4.1 利用者のための適用上の注釈

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。

M.4.2 FTP_TRP.1 高信頼パス

M.4.2.1 コンポーネントの根拠と適用上の注釈

このコンポーネントは、利用者とTSF間に高信頼通信が要求されるときに、最初の認証目的だけのためか、あるいは追加の特定された利用者操作のために使用される。

M.4.2.2 操作

FTP_TRP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼パスをリモート及び/又はローカル利用者へ伸ばすかどうかを特定する。

FTP_TRP.1.1において、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼パスが、改変、暴露、及び/又は、他のタイプの完全性や機密性侵害から、データを保護しなければならないかどうかを特定する。

FTP_TRP.1.1において、もし選択されれば、PP、PPモジュール、機能パッケージ又は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る。

FTP_TRP.1.2において、PP、PPモジュール、機能パッケージ又はSTの作成者は、TSF、ローカル利用者、及び/又はリモート利用者が、高信頼パスを起動できるかどうかを特定する。

FTP_TRP.1.3において、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼パスを、最初の利用者認証のために、及び/又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る。

FTP_TRP.1.3において、もし選択されれば、PP、PPモジュール、機能パッケージ又はSTの作成者は、高信頼パスが要求される他のサービスがあれば、それを識別する。

参考文献

[1] ISO/IEC TS 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications*

[2] ISO/IEC TS 19608, *Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*

[3] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[4] THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[5] THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI), AIS31

---

[i] 【訳注】原文の 3.13 の operation には 3.5 への参照があるが、3.5 の operation は CC パート 2 のコンポーネントの操作を意味し、3.13 で用いられている operation とは意味が異なる。

[ii] 【訳注】原文の 3.14 の operation には 3.5 への参照があるが、3.5 の operation は CC パート 2 のコンポーネントの操作を意味し、3.14 で用いられている operation とは意味が異なる。

[iii] 【訳注】原文では"the management of the rules for authentication."とあるが、内容がコンポーネントと関連していない。また、「FIA_UAU.7 の管理」は 12.6.5 にも記載がある。

[iv] 【訳注】原文では"a) well-formedness of rules regarding the semantics of rule-set; b) basic: verification of enforceability of rules."とあるが、内容がコンポーネントと関連していない。コンポーネントの内容は CC v3.1 改訂第 5 版から変更が無いため、コンポーネントの監査についても CC v3.1 改訂第 5 版と同様としている。

[v] 【訳注】図 72(及び図 60)について、原文では FPT_STM.2 が FPT_STM.1 の上位のコンポーネントであるかのような図となっているが、15.13.8 の FPT_STM.2 の説明のとおり階層関係は無い。

[vi] 【訳注】原文では FAU_STG.4 となっているが、内容は FAU_STG.5 のもの。

[vii] 【訳注】原文では FAU_STG.5 となっているが、内容は FAU_STG.4 のもの。

[viii] 【訳注】G.3.2.2 について、原文と本書ではコンポーネントの操作の記載順が異なるため、原文の"The first assignment"が「3 番目の割付」となっている。

[ix] 【訳注】原文では"specify the TSF data that can have limits, and the value of those limits"と、TSF データの他にその限界値についての割付に関する言及があるが、13.5.10 の FMT_MTD.2.1 には限界値そのものの割付操作はない。

[x] 【訳注】原文では"specify the roles that are allowed to modify the limits on the TSF data and the actions to be taken"と、役割の他にアクションの割付に関する言及があるが、13.5.10 の FMT_MTD.2.1 にはアクションの割付操作はない。