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

正式な文書は、以下の URL よりダウンロード可能です。

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

# 汎用オペレーティングシステム
# プロテクションプロファイル


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

バージョン 3.9

第 1 部：一般モデル、セキュリティ課題定義、セキュリティ機能要件及びセキュリティ保証要件

平成 25 年 11 月 12 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

# 目次

1 プロテクションプロファイル概論 ..... 6
1.1 プロテクションプロファイルの参照情報 ..... 6
1.2 TOE 概要 ..... 7
1.2.1 TOE の種類 ..... 8
1.2.2 TOE をサポートするハードウェア／ソフトウェア／ファームウェア ..... 8
1.3 プロテクションプロファイルの構造 ..... 9
1.4 用語 ..... 9
1.4.1 利用者 ..... 9
1.4.2 グループ ..... 10
1.4.3 サブジェクト ..... 11
1.4.4 リソース ..... 12
1.4.5 オブジェクト ..... 12
1.4.6 セキュリティ属性 ..... 13
1.4.7 高信頼利用者・サブジェクト ..... 13
1.4.8 セキュリティ方針 ..... 14
1.4.9 ストレージオブジェクトの種類 ..... 14
1.5 参照情報 ..... 14
2 OSPP フレームワーク ..... 15
2.1 ST が提供すべき必須情報 ..... 15
2.1.1 適合主張 ..... 15
2.1.2 OSPP 拡張パッケージ参照を伴う SFR 参照 ..... 15
2.2 OSPP 拡張パッケージによって提供される必須情報 ..... 16
2.2.1 拡張パッケージの識別上方 ..... 16
2.2.2 拡張パッケージの作成ルール ..... 16
2.2.3 OSPP 拡張パッケージの仕様 ..... 16
2.3 OSPP 基本部に制限される仕様 ..... 16
3 OSPP 基本部の概論 ..... 18
3.1 TOE 概要 ..... 18
3.1.1 監査 ..... 18
3.1.2 利用者データ保護 ..... 19
3.1.3 識別と認証 ..... 21
3.1.4 セキュリティメカニズムの管理 ..... 23
3.1.5 高信頼チャネル ..... 24
3.2 高信頼システム間の協調 ..... 25
3.3 TOE 境界 ..... 27
4 適合主張 ..... 29
4.1 CC パート 2 及び 3 への適合 ..... 29
4.2 他のプロテクションプロファイルへの適合 ..... 29
4.3 適合記述 ..... 29
4.4 OSPP 拡張パッケージに必要とされる適合 ..... 29
5 セキュリティ課題定義 ..... 30
5.1 脅威 ..... 30
5.1.1 資産 ..... 30
5.1.2 脅威エージェント ..... 30
5.1.3 TOE によって対抗される脅威 ..... 31
5.2 組織のセキュリティ方針 ..... 31

5.3 前提条件 ..... 32
5.3.1 物理的側面 ..... 32
5.3.2 人的側面 ..... 32
5.3.3 手続的側面 ..... 32
5.3.4 接続性の側面 ..... 32
6 セキュリティ対策方針 ..... 33
6.1 TOE のセキュリティ対策方針 ..... 33
6.2 運用環境のセキュリティ対策方針 ..... 34
6.3 セキュリティ対策方針の根拠 ..... 35
6.3.1 セキュリティ対策方針のカバレージ ..... 35
6.3.2 セキュリティ対策方針の十分性 ..... 36
7 拡張コンポーネントの定義 ..... 41
7.1 FIA_PK_EXT.1 公開鍵ベースの認証 ..... 41
7.1.1 コンポーネントのレベル付け ..... 41
7.1.2 管理 ..... 41
7.1.3 監査 ..... 41
7.1.4 FIA_PK_EXT.1 公開鍵ベースの認証 ..... 41
7.1.5 根拠 ..... 41
7.2 FMT_SMF_RMT.1 リモート管理機能 ..... 41
7.2.1 コンポーネントのレベル付け ..... 41
7.2.2 管理 ..... 41
7.2.3 監査 ..... 42
7.2.4 FMT_SMF_RMT.1 リモート管理機能 ..... 42
7.2.5 根拠 ..... 42
8 セキュリティ要件 ..... 43
8.1 セキュリティ機能要件 ..... 43
8.1.1 クラス：セキュリティ監査（FAU） ..... 43
8.1.2 クラス：利用者データ保護 (FDP) ..... 48
8.1.3 クラス：識別及び認証 (FIA) ..... 54
8.1.4 クラス：セキュリティ管理 (FMT) ..... 60
8.1.5 クラス：TSF の保護（FPT） ..... 65
8.1.6 クラス：TOE アクセス（FTA） ..... 65
8.1.7 クラス：高信頼パス／チャネル（FTP） ..... 67
8.2 セキュリティ機能要件の根拠 ..... 69
8.2.1 要件の内部的な一貫性 ..... 69
8.2.2 セキュリティ要件のカバレージ ..... 70
8.2.3 セキュリティ要件の依存性分析 ..... 73
8.3 セキュリティ保証要件 ..... 74
8.4 セキュリティ保証要件の根拠 ..... 75
9 略語集 ..... 77

# 表の目次

表 1：TOE のセキュリティ対策方針のカバレージ ..... 35
表 2：TOE 環境のセキュリティ対策方針のカバレージ ..... 35
表 3：TOE 脅威の十分性 ..... 37
表 4：セキュリティ方針の十分性 ..... 38
表 5：前提条件の十分性 ..... 40
表 6：監査対象事象の最小集合と、事象特有の情報 ..... 45
表 7：セキュリティ機能要件のカバレージ ..... 71
表 8：セキュリティ機能要件の根拠 ..... 73
表 9：セキュリティ機能要件の依存性分析 ..... 74
表 10：セキュリティ保証要件 ..... 75
表 11：セキュリティ保証要件の依存性分析 ..... 75

# 図の目次

図 1：TOE インスタンスの種類とその境界 ..... 28

# 改版履歴

| バージョン | 日付 | 作成者 | 変更点 |
|---|---|---|---|
| 3.0 | 2012-03-15 | Helmut Kurth, atsec | 整合化作業のための変更 |
| 3.1 | 2012-03-21 | Helmut Kurth, atsec | BSI からのコメントに対応 |
| 3.2 | 2012-04-11 | Helmut Kurth, atsec | マイクロソフト及び最近の電話会社からのコメントに対応 |
| 3.3 | 2012-04-16 | Helmut Kurth, atsec | 追加コメントに対応 |
| 3.3a | 2012-05-05 | Helmut Kurth, atsec | BSI との契約への対応を完了 |
| 3.3b | 2012-07-17 | Helmut Kurth, atsec | 受領したコメントから SFR を更新 |
| 3.4 | 2012-08-03 | Helmut Kurth, atsec | 受領したコメントから更新。大規模コミュニティへ配布される最初のバージョン |
| 3.5 | 2012-08-07 | Helmut Kurth, atsec | 配布前の最後の更新 |
| 3.6 | 2012-08-17 | OSPP TC | 最終更新 |
| 3.7 | 2012-09-07 | OSPP TC | FTP_ITC.1 に関する軽微な変更 |
| 3.8 | 2012-12-03 | Gerald Krummeck, atsec | OSPP TC での合意により保証要件を追加。未解決の依存性の根拠を追加<br>将来の拡張パッケージに関する文言を更新 |
| 3.9 | 2012-03-06 | OSPP TC | 公開へ向けた最後の更新<br>• PP を DRAFT とマーク<br>• CC V3.1 R4 を参照<br>• X.509 に加えて公開鍵（SSH）を許容するため、FIA_X509_EXT を FIA_PK_EXT に変更<br>• FTP_ITC.1 : 強制される暗号スイートとオプションの暗号スイートのリストを再構成<br>• 軽微な編集上の変更 |

# 1 プロテクションプロファイル概論

本文書は、ネットワーク環境において運用可能な汎用オペレーティングシステムに提供が期待されるセキュリティ機能を定義するものである。また、本プロテクションプロファイルへのオペレーティングシステムの適合性を評価する際に用いられる最小セットを定義する一連の保証コンポーネントも提供する。本 PP の第 2 部では、評価中に実施が求められる一般的アプローチ及び保証アクティビティを定義し、これによって言明された保証コンポーネントを詳細化する。

他の大部分のプロテクションプロファイルとは異なり、汎用オペレーティングシステムプロテクションプロファイル（OSPP）は「基本」部と、一連の（オプションの）「拡張パッケージ」から構成されている。この構成は、汎用オペレーティングシステムが幅広い範囲のさまざまな機能を提供する可能性があることから、さまざまな運用環境やさまざまな運用要件へ最大限順応するために選択された。このドラフト版の整合化された OSPP においては、拡張パッケージはまだ利用できない。

汎用オペレーティングシステムは、組織内の多数のシステムによって使用される集中型サービスを提供する環境で運用される場合が多い。モダンな汎用オペレーティングシステムには、例えば認証サーバ、ディレクトリサーバ、証明書サービス、あるいは監査ログサーバなどのセキュリティ機能を実装するために、集中型サービスを利用できる能力を提供することが期待される。大部分のモダンな汎用オペレーティングシステムは集中型セキュリティサービスなどの機能を実装しているが、さらにこれらのサービスのサーバとして機能できてもよい。「拡張パッケージ」の候補となるためには、集中型セキュリティサービスのサーバとして機能する能力を持たなくてはならない（must）。

他の高信頼 IT システムと協調してセキュリティサービスを提供することは、集中型サービスに限られたものではなく、ピアツーピア関係によって実現することもできる。例としては、例えばスマートカードなどのトークンの提示を利用者に求めることによって、人間の利用者を認証する機能が挙げられる。このシナリオでは、利用者は PIN を用いてスマートカードに対する認証を行い、そしてスマートカードは、例えば利用者の証明書を提示して、証明書中の公開鍵と関連付けられた個別鍵を持っていることをオペレーティングシステムに保証することによって、その利用者をオペレーティングシステムに対して認証する。

この「基本」文書に規定されたセキュリティ機能要件は、オペレーティングシステムがその環境中の他の IT システムからのオンラインサポートを受けずに提供する必要がある機能を規定する。運用環境のサポートに依存する機能については、拡張パッケージまたは ST 固有の拡張に任される。

本プロテクションプロファイルに適合するオペレーティングシステムは、それらが機能しているプラットフォーム（ハードウェア、デバイス、及びファームウェア）が、物理的な攻撃及び不正操作から保護された環境で運用されることが前提とされている。さらに、すべての管理アクティビティが十分な知識を持った信頼できる利用者によって実施されることが前提とされている。

## 1.1 プロテクションプロファイルの参照情報

PP のタイトル：汎用オペレーティングシステムのプロテクションプロファイル

PP のバージョン： 3.9

公開日：2012-12-06

作成者：OSPP 技術コミュニティ

CC のバージョン：3.1 リビジョン 4

キーワード：オペレーティングシステム、汎用オペレーティングシステム

## 1.2 TOE 概要

OSPP では、マルチユーザ及びマルチタスキング環境を提供する汎用オペレーティングシステムを取り扱う。

汎用オペレーティングシステムの（セキュリティの観点から見た）主な目的は、オペレーティングシステムの外部インタフェースによって提供される機能を用いるエンティティへ定義されたオブジェクト、リソース及びサービスを提供すること、及びオブジェクトへのアクセス、リソースの利用、及びサービスの利用に関して定義された方針を強制することである。最低でも、本プロテクションプロファイルの対象となるオペレーティングシステムは、オペレーティングシステム「上」で実行されるプログラムへのインタフェース、及び外部エンティティへのインタフェースをエクスポートする。これには、ネットワークインタフェースに加えて、外部エンティティのデータやアクションをオペレーティングシステムへ「トランスポート」するために用いられるデバイス（例えば、キーボードやマウス）へのインタフェースが含まれる。さらに、オペレーティングシステムはその機能を提供するために基盤となるハードウェア及びソフトウェアを利用する。これには、外部エンティティに接続されていないデバイスを利用して、このエンティティが直接そのデバイスのふるまいに影響を与えられるようにすること（例えば、ハードディスクやディスプレイ）が含まれる。

本プロテクションプロファイルに適合するオペレーティングシステムは、データセンタ内のサーバシステムとしても、また 1 人以上の人間の利用者によって直接使われるクライアントシステムとしても、運用することができる。本プロテクションプロファイルに適合するオペレーティングシステムは一部の基本的なネットワークサービスを提供し利用することができなくてはならないことが義務付けられる一方で、またそのようなシステムは全くネットワークに接続されておらず、ネットワークサービスがインアクティブな環境において起動されるかもしれない。本プロテクションプロファイルに適合するオペレーティングシステムは、利用者の識別、アクセス制御、管理及び監査を行うための基本的なセキュリティ機能を提供しなくてはならないことが義務付けられる。

TOE は利用者へサービスを直接提供するか、あるいはネットワークを利用するアプリケーションのプラットフォームとして働き、また 1 つ以上の暗号保護されたネットワークプロトコルを用いて、または専用の物理的に分離したネットワークリンクのサポートによって、保護された通信をサポートすることになる。保護された通信をサポートするため、TOE は少なくとも TCP/IP ネットワークプロトコルファミリを実装しなくてはならないが、本 PP においては IP のバージョンに関しては何も言明しない。

OSPP は、良好に管理されたエンタープライズ環境において動作する汎用オペレーティングシステムを対象としている。これは主にサーバを対象としているが、運用環境が 4 章に定義されるセキュリティ課題と、ST 中で主張される任意の OSPP 拡張パッケージの定義するセキュリティ課題を満たしているならば、デスクトップクライアントも対象となる。これらのセキュリティ課題には、エンタープライズまたは政府環境に見られるが個人利用者の管理するホーム環境においては通常見られない、システムの専門的な管理と物理攻撃に対する基本的な保護に関する要件が含まれる。エンタープライズまたは政府環境には、モバイルシステムやホームオフィス向けの設定も含まれるかもしれないが、これらの環境を本 PP 中のセキュリティ課題定義に適合させるようなメカニズムを TOE が実装している場合に限られる。OSPP は、特定のサーバオペレーティングシステムまたはクライアントオペレーティングシステムへ適用される主張または言明は行わない。拡張パッケージの有無にかかわらず、OSPP 基本部のセキュリティ課題定義において定義された要件をオペレーティングシステムが満たしているならば、そのオペレーティングシステムは本プロテクションプロファイルへの適合性を主張することができる。

### 1.2.1 TOE の種類

本 PP において定義される要件は、汎用オペレーティングシステムへ適用可能なものでなくてはならない（shall）。

OSPP は、汎用オペレーティングシステムによって提供されるべき要件の規定に関するフレームワークを提供しなくてはならない（shall）。

### 1.2.2 TOE をサポートするハードウェア／ソフトウェア／ファームウェア

OSPP が対象とするオペレーティングシステムは、その基盤となるプラットフォームに依存しており、そのプロットフォームは通常、ハードウェア（プロセッサ、メモリ、各種デバイス）及びファームウェアから構成される。場合によっては、論理的パーティション化を提供する分離したソフトウェアレイヤまたは仮想化レイヤの上で、オペレーティングシステムが実行されているかもしれない。そのような仮想化によって、ハードウェアの全部または一部が、TOE にとってトランスペアレントな方法で、または TOE に仮想化レイヤへの専用インタフェースを利用させることによって、エミュレートされる。いずれの場合でも、基盤となるプラットフォームへのインタフェースは、オペレーティングシステムがどのように基盤となるプラットフォームの機能を利用するかの分析を可能とするために定義され、記述されなくてはならない（must）。

少なくとも、信頼できないサブジェクトがオペレーティングシステムの機能に干渉したり、あるいはその保護機能をバイパスしたりしないようにオペレーティングシステムが自分自身を保護するために利用できる機能を、基盤となるプラットフォームは提供しなくてはならない（must）。これには、オペレーティングシステムに以下を可能とする機能が必要とされる。

- □ メインメモリの領域を、信頼できないサブジェクトからアクセスされないように保護する。
- □ デバイスを、信頼できないサブジェクトから（オペレーティングシステムによって仲介されるアクセス以外に）直接アクセスされないように保護する。
- □ 基盤となるプラットフォームの他の任意の機能を、オペレーティングシステムのセキュリティ方針に違反するような方法で信頼できないサブジェクトから利用されないように保護する。

本プロテクションプロファイルは、基盤となるプラットフォームがこれらの義務的な保護機能を実装する方法については定義しない。

少なくとも、要求される保護機能の全部または一部をバイパスできるようなオペレーティングシステムソフトウェアのすべての部分は、TOE の境界よりも内側に存在する。多くのオペレーティングシステムは、メモリやプロセッサの状態及び各種デバイスを構成するために基盤となるハードウェアを操作する特権を持つ「カーネル」と、一連の「高信頼サブジェクト」から構築され、これらの高信頼サブジェクトにはオペレーティングシステム全体が強制する必要のあるセキュリティ方針の全部または一部に違反することを許可する特権がカーネルによって割り当てられている。そのような高信頼サブジェクトもまた、TSF の一部とみなされなくてはならない（must）。

評価の対象となる TSF は、有用なセキュリティ機能を追加する OSPP 拡張パッケージによって、要件追加されてもよい。

本プロテクションプロファイルの観点からは、基盤となるプラットフォームは IT 環境中に位置づけられる。このことは、適合 ST が基盤となるプラットフォームの全部または一部を含めることによって、異なる TOE 境界を定めることを妨げるものではない。例えば、ST 作成者は仮想化レイヤを TOE に含めるが、それでも基盤となるハードウェアは含めないように判断してもよい。

## 1.3 プロテクションプロファイルの構造

この文書は、以下のような構造をしている。

- □ 1 章では、OSPP の概論と TOE の概要を説明する。このセクションは、TOE の使用ならびに OSPP 基本部の導入部中及び各 OSPP 拡張パッケージ中の主要なセキュリティ機能によって拡張されていることに注意されたい。この章に見られる記述は基本部に加えて、OSPP の拡張パッケージにも適用される。
- □ 2 章では、基本部と拡張パッケージとの分割を含め、OSPP フレームワークを定義し規定する。ここではまた、OSPP や拡張パッケージ文書から導出される ST へ、OSPP 基本部またはその他の OSPP 拡張パッケージとの関連付けを可能とするため、追加されるべき義務的な情報も定義される。
- □ 3 章には、OSPP 基本部の概論が含まれる。このセクションは、CC パート 1 から導出された OSPP のプロテクションプロファイル構造から始まる。
- □ 4 章は、OSPP への適合主張を規定する。
- □ 5 章には、セキュリティ課題定義が含まれる。
- □ 6 章では、対策方針が定義される。
- □ 7 章には、拡張コンポーネントの定義が含まれる。
- □ 8 章には、セキュリティ要件の定義と根拠が含まれる。

この構造は、OSPP 基本部に加えて、一般的な OSPP の制約もこの文書に規定されることを意味している。追加 OSPP 拡張パッケージは、3 章以降に見られる構造に非常によく似た構造を持つ、別の文書中で定義される。

## 1.4 用語

以下のセクションでは、汎用オペレーティングシステムプロテクションプロファイル（OSPP）に使われる用語を定義する。

### 1.4.1 利用者

コモンクライテリアに定義されているように、利用者は TOE と対話する外部エンティティである。そのような外部エンティティには、他の IT システムだけではなく、人間の利用者も含まれる。

利用者は、匿名（すなわち、オペレーティングシステムは利用者の識別情報を知らない）であるか、識別情報と関連付けられるかのどちらかである。オペレーティングシステムによって強制されるセキュリティ方針によって異なる利用者が区別される場合には常に、オペレーティングシステムは利用者の識別情報が正しいことを確認しなくてはならない（must）。

オペレーティングシステムが異なる種類の利用者をサポートすることは非常によく行われる。これらの異なる種類の利用者は、異なるセットのインタフェースの利用が許可されたり、異なるセキュリティ属性を有したり、異なる方法で識別及び認証されたり、そしてセキュリティ方針の異なるルールを適用されたりする。例えば、「利用者」としての IT システムは、定義されたネットワークサービスを介した接続のみが許可されたり、デジタル証明書を利用したチャレンジレスポンスプロトコルを用いて認証されたり、そしてファイルシステムオブジェクトへの直接アクセスが許可されなかったりするかもしれない。一方では、「人間の利用者」はシステムコールインタフェースの使用が（それらに束縛されたサブジェクトを介して）許可されたり、利用者 ID／パスワードの組み合わせを（そして最終的には何らかの他の認証メカニズムを）用いて認証されたり、そしてファイルシステムオブジェクトへの直接アクセス（利用者の代理として起動されるサブジェクトを介して）が、それらのオブジェクトへの任意アクセス制御方針のルールにしたがって許可されるかもしれない。

利用者は、ローカルに定義し管理することもできる。この場合には、オペレーティングシステムは有効な利用者のリストを彼らのセキュリティ属性と共に保持しなくてはならず（must）、またこれらの利用者がどのように管理されるかを定義する方針を持たなくてはならない（must）。

多くの場合、オペレーティングシステムはローカルには定義されず管理されない利用者が、オペレーティングシステムへ接続してサービスを要求することも許可している。このような場合には、オペレーティングシステムは別の高信頼 IT システムに、以下の確認を委ねることになる。

- □ その利用者が依然として利用者コミュニティの有効なメンバであり、失効していない。
- □ リモートの高信頼エンティティからオペレーティングシステムへ渡される利用者のセキュリティ属性が、依然として有効である。利用者のセキュリティ属性は、デジタル証明書の中に入った形で TOE へ渡される可能性があることに注意されたい。この場合、そのデジタル証明書を発行した認証局が、たとえこのエンティティへ TOE が全く直接接続できない場合であっても、リモートの高信頼エンティティとなる。

この基本プロテクションプロファイルに規定された要件は、ローカルに定義された利用者に適用されることに注意されたい。したがって、本プロテクションプロファイルに適合するオペレーティングシステムは、TOE 環境のサポートなしで利用者をローカルに定義し管理する機能を**持たなくてはならない**（must）。オペレーティングシステムには、リモートで定義され管理される利用者を取り扱う機能が**あってもよい**。その機能はセキュリティターゲットに含まれる追加 SFR 中に表現されるか、あるいはそのような機能を定義する拡張パッケージへの適合を主張することによって表現する必要がある（have to）。

### 1.4.2 グループ

グループは、グループ識別子によって参照可能な利用者のセットを定義する。利用者と同様に、グループは TOE それ自身が管理してもよいし、あるいはリモートの高信頼エンティティが管理してもよい。グループの管理には、以下が含まれる。

- □ グループそのものの定義。
- □ グループのメンバシップの管理。
- □ グループのセキュリティ属性（例えば、グループのメンバへ与えられる特権及びアクセス権）の管理。
- □ 利用者とグループのセキュリティ属性またはアクセス権が競合する可能性がある場合（例えば、利用者及びグループのセキュリティ属性として同一のセキュリティ属性が存在したり、アクセス権が利用者だけでなくグループにも割り当てられたりする場合）、それらがどのように評価されるかの定義。
- □ 利用者が複数のグループのメンバになり得る場合、グループのセキュリティ属性またはグループのアクセス権がどのように評価されるかを定義するルール。
- □ 利用者が持つことのできる「アクティブ」なグループメンバシップを定義するルール（利用者が 2 つ以上のグループのメンバになり得る場合、TOE のセキュリティ方針のルールを評価する際に考慮されるグループの数が、TOE のセキュリティ方針によって制限されるかもしれない）

グループは、ある役割に必要とされるセキュリティ属性やアクセス権をグループに割り当て、それからその特定の役割を期待される利用者をそのグループへ割り当てることによって、役割を定義するために使われることが多い。あるいは、オペレーティングシステムは利用者に割り当てられる単一のセキュリティ属性として役割を実装することもでき、その場合このセキュリティ属性がこの役割によって利用者へ割り当てられる特権の固定的または構成可能なセットを定義することになる。

### 1.4.3 サブジェクト

サブジェクトは、システムにおけるアクティブなエンティティである。プログラムの実行に関して、OSPP 適合オペレーティングシステムは、オペレーティングシステム「上」で実行される別個のアクティブなエンティティを、オペレーティングシステムが一意に識別可能な別個の「サブジェクト」として識別し、分離することができなくてはならない（must）。これによってオペレーティングシステムは、定義された方針のルールを強制することによって、サブジェクトからのオブジェクトへのアクセスやリソースの割り当て、そしてオペレーティングシステムサービスの利用をコントロールできるようになる。OSPP に適合したオペレーティングシステムのアーキテクチャは、そのようなサブジェクトがいかなる方針ルールへの違反や、あるいは方針ルールを強制するオペレーティングシステム内でのコントロールのバイパスを防止しなくてはならない（must）。

オペレーティングシステムは、方針ルールの一部または全部が強制されない「高信頼サブジェクト」を承認することもできる。そのような「高信頼サブジェクト」は、評価された構成の一部である場合、TSF の一部でなくてはならない（must）。そのような「高信頼サブジェクト」は、信頼されない利用者へセキュリティ方針のルールに違反する方法を提供してはならない（must not）。

本プロテクションプロファイルでは、オペレーティングシステムが作成するサブジェクトをどのように実装し、分離し、そしてコントロールするのかを規定しない。この側面はセキュリティターゲット中で説明されなくてはならず、またセキュリティアーキテクチャ保証コンポーネントについて提供される証拠資料の中で、さらに詳述されなくてはならない（must）。

本プロテクションプロファイルに適合するオペレーティングシステムは、特定の外部エンティティ（「利用者」）をサブジェクトへ「束縛（bind）」できなくてはならない（must）。利用者へ束縛されたサブジェクトは、利用者の代理として動作する。オペレーティングシステムによって強制されるセキュリティ方針ルールは「利用者のセキュリティ属性」によって定義されることが多いため、オペレーティングシステムがサブジェクトを利用者へ「束縛」する場合、オペレーティングシステムは利用者の代理として動作するサブジェクトのセキュリティ属性がどのように導出されるのかを定義するルールを持たなくてはならない（must）。最も単純な場合には、利用者のセキュリティ属性がサブジェクトのセキュリティ属性へ、1 対 1 にコピーされる。多くのオペレーティングシステムでは、はるかに複雑なルールが実装されている。例えば、サブジェクトのセキュリティ属性を、利用者のセキュリティ属性や、その利用者がメンバとなっているアクティブなグループのセキュリティ属性、さらにはサブジェクトが起動された環境（これには時間や日付、あるいは利用者が TOE への接続に使用しているポートが含まれるかもしれない）及び TOE の現在の状態から導出する方法を定義するルールを、オペレーティングシステムが持っているかもしれない。本プロテクションプロファイルでは、ユーザ・サブジェクト間の束縛に関するルールは規定しない。したがって、これらのルールは本プロテクションプロファイルへの適合を主張するセキュリティターゲットの中で定義されなくてはならない（must）。

オペレーティングシステムそれ自身が、セキュリティ方針の強制に積極的に関与するサブジェクトや、方針の全部または一部をバイパス可能なサブジェクトを作成し利用するかもしれない、ということに注意されたい。これらのサブジェクトは定義済みの方針を強制するために「高信頼」である必要があり、したがってオペレーティングシステムの TSF の一部である。さらに、作成時には TSF の一部であるが、その後「信頼されない」サブジェクトへ変化する（例えば、利用者をサブジェクトへ束縛するプロセスの一部として）サブジェクトを作成するオペレーティングシステムもある。

サブジェクトは、いかなる利用者にも束縛されていない状態で、オペレーティングシステムによって作成されることもある。例えば、起動時または特定の事象の結果としてオペレ

ーティングシステムによって起動されるデーモンなどである。これらのサブジェクトについて、セキュリティ方針のルールを一貫して強制できるように、オペレーティングシステムはこれらのサブジェクトの特権やアクセス権のアクティブな集合を定義する方針を持たなくてはならない（must）。一部のオペレーティングシステムでは「仮想ユーザ（pseudo-users）」のメカニズムを用いて、どのリアルな利用者にも割り当てられていない識別情報を持つ「ユーザ」の識別情報を持ってサブジェクトが起動されるようにしている。これによってオペレーティングシステムは、利用者管理の機能を使って特権やアクセス権を割り当てることができ、また利用者・サブジェクト間の束縛のルールを使って、これらのサブジェクトの特権やアクセス権のアクティブな集合を確立することができる。仮想ユーザは外部エンティティを表現するものではないので、通常は利用者認証を必要としない。

### 1.4.4 リソース

リソースは、オペレーティングシステムが利用者やサブジェクト、あるいはオブジェクトへ割り当てることができる、論理的エンティティまたは物理的エンティティあるいはその両方の限定されたセットである。リソースの割り当ては TOE が管理しなくてはならない（must）。永続的ストレージのブロックや CPU サイクル、メインメモリ、そしてネットワーク帯域などはリソースの例である。通常リソースは割り当てられるものであり、また再利用可能な場合には後で割り当てが解放されて再利用に備えられる。OSPP 基本部では、リソースに適用される特定の方針の実装や、リソースがサブジェクトや利用者またはオブジェクトへ割り当てられる方法は要求していない。しかし、OSPP 基本部ではすべての再利用可能なリソースが、最後に割り当てられたものとは異なるサブジェクトや利用者またはオブジェクトへ割り当てられる際、再割り当ての際にそのリソースから以前の利用または内容に関する情報が何ら得られないように、再利用に備えなくてはならないと要求している。OSPP 拡張パッケージでは、例えば割り当て解放に際してリソースの内容をクリアするような、さらに制約されたリソース解放メカニズムが定義されてもよい。また OSPP 拡張パッケージでは、例えばクォータ管理やリソース割り当て時の具体的な優先度など、リソース割り当てに関する特定の方針の実装を要求してもよい。

### 1.4.5 オブジェクト

オブジェクトはオペレーティングシステムによって作成されコントロールされるパッシブなエンティティであり、それらのオブジェクトを利用する利用者またはサブジェクトあるいはその両方にサービスを提供する。名前付きオブジェクトは、利用者またはサブジェクトあるいはその両方が特定の種類の名前付きオブジェクトを定義された方法で利用する際に満たさなくてはならない条件を定義するアクセス制御方針強制ルールを実装するオペレーティングシステムによって、取り扱われる。名前付きオブジェクトは、サブジェクトがオブジェクトへのアクセスを試みる際や、オブジェクトのセキュリティ属性やアクセス権が管理される際に、オペレーティングシステムがオブジェクトを識別できるように、識別情報を持たなくてはならない（must）。サブジェクトからアクセス不可能なオブジェクトが存在したり、TOE によってインスタンス化されたりするかもしれない、という点に注意されたい。そのような TOE 内部オブジェクトについては、それらが内部オブジェクトである限り TOE のセキュリティ方針は適用されくてもよい。

OSPP 基本部では、少なくとも 1 つの種類の名前付きオブジェクトが永続的ストレージ中に作成されて保持されなくてはならず、また利用者またはサブジェクトあるいはその両方が以下のことをできるようにしなくてはならないことを要求している。

- □ この種類の新しいオブジェクトの作成
- □ オブジェクトへのデータの書き込み
- □ オブジェクトからのデータの読み取り
- □ オブジェクトの削除

この種類の名前付きオブジェクトに関する他の操作が定義されてもよいが、OSPP 基本部

においては義務的ではない。

この種類の名前付きオブジェクトについて、OSPP 基本部では、利用者またはサブジェクトあるいはその両方がこの種類のオブジェクトに対して定義された 4 つの操作のうちの 1 つを行う際に満たさなくてはならない条件を明確に定義するアクセス制御方針が実装されなくてはならないと要求している。アクセス制御方針が満たさなくてはならない、これ以外の条件が、本文書のこの後で定義される。

オペレーティングシステムには多数の異なる種類の名前付きオブジェクトが実装されているのが普通であり、それぞれの名前付きオブジェクトの種類に対して異なるアクセス制御方針が実装されていてもよい。

### 1.4.6 セキュリティ属性

オペレーティングシステムには、非匿名利用者、サブジェクト、そして名前付きオブジェクトに対してオペレーティングシステムが関連付けるセキュリティ属性が定義されている。これらのセキュリティ属性の一部は、アクセス制御方針のルールの中でオペレーティングシステムによって使われる。一部の属性は、例えば利用者またはサブジェクトに特定の管理アクションの実施が許可されているかどうかの判定など、別の目的に利用されてもよい。

特権は通常、管理タスクを実施する際に必要とされる権限である。セキュリティメカニズムに影響を与える管理アクションは制限されなくてはならない（must）ため、例えばこれらのアクションを実施するサブジェクトの特権など、検証可能な属性に基づいて TOE はこれらの制限を行わなくてはならない（must）。

そのような特権は、例えば UNIX ライクな環境での UID 0 など、具体的に割り当てられる属性であってもよいし、通常はアクセス不可能なデータに対する操作を行うための利用者データまたは TSF データあるいはその両方を含むリソースに関する特定のアクセス制御の設定であってもよい。

さらに特権は、TOE の状態、サブジェクトが代理となっている利用者が TOE へ到達する際に経由しているインタフェース、サブジェクトがそのアクションを実施する時間など、任意のその他のメカニズムに基づいてサブジェクトへも与えられてもよい。

セキュリティ機能仕様によって参照されるすべての特権について、ST 作成者はその特権がどのようにサブジェクトへ割り当てられるかを規定しなくてはならない（must）。

### 1.4.7 高信頼利用者・サブジェクト

一部の利用者は、セキュリティ方針に定義されるルールの一部または全部をバイパスする能力や、セキュリティ方針が依存する TSF データを管理する能力が与えられるような、セキュリティ属性やアクセス権を持っていることがある。これらの利用者は、自分の能力を悪用しないと信頼されている。一部の場合には、例えば利用者が自分の所有するオブジェクトのアクセス制御リストを管理できる場合など、これらの能力は非常に限られているかもしれないことに注意されたい。また、そのような利用者はこの能力を賢明な方法で利用し、例えばシステムの限られた利用者のみがアクセス可能であるべき情報を保存するために自分が使っているストレージオブジェクトへのアクセス権をすべての利用者へ与えるようなことはしないと信頼されている。

高信頼利用者に加えて、オペレーティングシステムには高信頼サブジェクトを持つこともできる。高信頼利用者と同様に、これらはセキュリティ方針に定義されるルールの一部または全部をバイパスする能力や、セキュリティ方針が依存する TSF データを管理する能力を持つサブジェクトである。これらのサブジェクトは、利用者と束縛されていないか、または利用者と束縛されているかのどちらかであり、後者の場合にはこの利用者が高信頼で

ないサブジェクトと束縛されている際にはアクセスを許可されないオブジェクトまたはリソースあるいはその両方へのアクセスが許可される。したがって高信頼サブジェクトには、高信頼でないサブジェクトにはない追加的な能力があり、またそのような能力の使用にはサブジェクト特有の方針が強制されることになる。例としては、利用者に特定の TSF データ（例えば、自分自身のパスワード）の変更を許可するような高信頼サブジェクトが挙げられる。この追加的能力のため、高信頼サブジェクトは TSF の一部となる。

### 1.4.8 セキュリティ方針

オペレーティングシステムの「セキュリティ方針」は、信頼されていないものだけでなく、信頼されているサブジェクト及び利用者がオペレーティングシステムのサービスを要求する際に、オペレーティングシステムが強制するセキュリティに関連したルールのセットである。このセキュリティに関連したルールのセットは、オペレーティングシステムのセキュリティターゲット中で定義される。本プロテクションプロファイルでは、本プロテクションプロファイルに適合するすべてのオペレーティングシステムが強制しなくてはならない（must）そのようなルールの最小セットを定義する。

### 1.4.9 ストレージオブジェクトの種類

本プロテクションプロファイルでは、「永続的ストレージオブジェクト」及び「一時的ストレージオブジェクト」という用語を採用している。以下の定義が適用される。

永続的ストレージオブジェクトは、利用者データまたは TSF データまたは TSF 機能あるいはそれらの任意の組み合わせを保持できるオブジェクトであって、以下の場合にも保存されたデータを保持するものである。

- ☐ TOE の初期化中
- ☐ TOE の再初期化中
- ☐ TOE の電源切断中または電源再投入中

他方、一時的ストレージオブジェクトは、やはり利用者データまたは TSF データまたは TSF 機能あるいはそれらの任意の組み合わせを保持できるオブジェクトではあるが、このデータは永続的ストレージオブジェクトに規定された事象中にそのままの形では保持されないものである。これは、上記の事象後に一時的ストレージオブジェクトが常にクリアまたはゼロ化されることは意味しないことに注意されたい。OSPP 基本部は、一時的ストレージオブジェクトまたはデータを保存可能なリソースが、それらに自動的にデータを失わせるような事象を経由せず再割り当てが実施された際には、再利用に備えなくてはならないと要求している。一時的ストレージオブジェクトまたはリソースが、以前割り当てられていたものと同一のサブジェクトに再割り当てされた際、または以前割り当てられていたサブジェクトと同一のセキュリティ属性を持つ別のサブジェクトに割り当てられた際には、再利用への備えは必要とされない。

## 1.5 参照情報

参照情報が再定義されない限り、本文書だけでなくすべての OSPP 拡張パッケージ文書に下記の参照情報が適用される。

CC Common Criteria for Information Technology Security Evaluation Parts 1 through 3, September 2012, Version 3.1 Revision 4

CEM Common Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4

OSPP-2 General-Purpose Operating System Protection Profile. Part2: General Approach and Assurance Activities for OSPP Evaluations, Version 3.9.

# 2 OSPP フレームワーク

OSPP では、OSPP 基本部に加え、オプションとして ST によって主張できる機能拡張の定義も許可している。それゆえ、OSPP では以下のコンポーネントが定義される。

- □ OSPP 基本部では、OSPP 基本部への適合を主張するすべての汎用オペレーティングシステムが満たすべき適合主張、セキュリティ課題、対策方針、セキュリティ機能要件、及びセキュリティ保証要件を定義する。OSPP 基本部は必須であり、OSPP への適合を主張するすべてのオペレーティングシステムの共通項を定義するものである。
- □ OSPP 拡張パッケージは、OSPP 基本部に加えて実装してもよいメカニズムのセキュリティ課題定義、対策方針、及びセキュリティ機能要件を規定する。通常、OSPP 拡張パッケージは、複数の汎用オペレーティングシステムに望まれる、または実装される拡張機能を定義する。しかし、OSPP 拡張パッケージに規定された機能は、汎用オペレーティングシステムに一般的には見られないものである。OSPP 拡張パッケージはオプションとして、ST を作成する際に OSPP 基本機能へ追加することができる。ST 作成者は、ST を導出する際に OSPP 拡張パッケージのセットから選択してもよい。セキュリティ機能が実用とするには小さすぎる OSPP 拡張パッケージへ断片化されることを避けるため、OSPP 拡張パッケージには 1 つ以上の一般的なセキュリティ課題に対処する機能要件のセットが定義されなくてはならない（shall）。OSPP 拡張パッケージは、OSPP テクニカルコミュニティ、または少なくとも拡張パッケージが用いられるスキームによって承認される必要がある。

OSPP は、拡張可能なフレームワークとして定義される。OSPP 拡張パッケージの現在のセットは、OSPP 拡張パッケージの新たな開発、または更新によって増強することができる。このようなパッケージは後に、再評価及び再認証された OSPP 基本部の一部になるであろう。したがってこのフレームワークでは、汎用オペレーティングシステムの一側面を規定することに興味を抱いている人なら誰でも、OSPP 拡張パッケージを作成し、そして OSPP が管理される場である OSPP フォーラムへそれを付託することが歓迎される。このようなアプローチを取ることにより、常に OSPP 基本部と拡張パッケージの有効なセットが存在し、それらが互いに適合していることになるであろう。他の OSPP 拡張パッケージへの依存性も規定できる。

## 2.1 ST が提供すべき必須情報

下記の情報が、OSPP から導出された ST の一部として提供されなくてはならない（must）。

### 2.1.1 適合主張

OSPP への適合適合を規定する際に ST は、ST が適合しなくてはならない（shall）OSPP 拡張パッケージが存在する場合には、それらを規定しなくてはならない（must）。

また ST は、ST によって主張された OSPP 拡張パッケージが依存する OSPP 拡張パッケージが存在する場合には、それらへの適合を主張しなくてはならない（must）。

### 2.1.2 OSPP 拡張パッケージ参照を伴う SFR 参照

ST の一部として SFR を規定する際には、SFR の直接的な対応付けを容易とするために、特に繰返しを考慮して、OSPP 基本部または OSPP 拡張パッケージの略称への参照がなされなくてはならない（must）。

この要件は、ST が適合性を主張している OSPP 基本部または OSPP 拡張パッケージからの SFR であってカバーされずに残っているものがないことを確実にするように、ST 作成者及び評価者を支援するものである（shall）。

## 2.2 OSPP 拡張パッケージによって提供される必須情報

すべての OSPP 拡張パッケージは、その拡張パッケージが OSPP のフレームワークへ組み込まれるために、下記の情報を提供しなくてはならない（must）。

### 2.2.1 拡張パッケージの識別情報

OSPP 拡張パッケージを識別するために、下記の情報が提供されなくてはならない（must）。

- □ 口語体の英語での拡張パッケージ名
- □ その拡張パッケージへの容易かつ明確な参照を可能とするための、拡張パッケージの略称
- □ 拡張パッケージのバージョン
- □ 拡張パッケージの所有者、すなわち正当な変更を行う担当者

### 2.2.2 拡張パッケージの作成ルール

OSPP 拡張パッケージを他の OSPP 拡張パッケージと組み合わせて使う方法を規定するため、下記の情報が提供されなくてはならない（must）。

- □ 依存する OSPP 拡張パッケージのリストと、それら各パッケージの最低バージョン。
- □ 認められない OSPP 拡張パッケージのリストと、それら各パッケージの最低バージョン。

拡張パッケージは、OSPP 基本部またはそのいかなる部分をも除外してはならない（must not）ことに注意されたい。しかし拡張パッケージが、それぞれの拡張パッケージに要求される OSPP 基本部の最低バージョンを規定することはできる。

既存の拡張パッケージが別のパッケージ（「現行」の拡張パッケージ）を収容するために変更されなくてはならない（must）場合、現行の拡張パッケージの作成者は既存の拡張パッケージの所有者と連絡を取り、必要な変更に関して合意することが要請される。

### 2.2.3 OSPP 拡張パッケージの仕様

OSPP 拡張パッケージには、OSPP 基本部への追加として多くの側面を定義することができる。仕様には、以下の情報が含まれる。

- □ パッケージの概論
- □ 他の OSPP 拡張パッケージへの依存性
- □ セキュリティ課題定義
- □ 対策方針
- □ セキュリティ機能要件
- □ セキュリティ保証要件の詳細化。より高度な、または拡張セキュリティ保証要件の仕様は許可されないことに注意されたい。OSPP 全体が相互承認協定でカバーされることが意図されており、OSPP 基本部はこれを確実にしなくてはならない（shall）。

## 2.3 OSPP 基本部に制限される仕様

OSPP 基本部は、下記の属性を独占的に定義する。

- □ 他のプロテクションプロファイルへの適合主張
- □ 適合の種類（正確適合）
- □ 任意の要件追加を含む、セキュリティ保証要件への適合主張

OSPP 拡張パッケージは、保証コンポーネントへの詳細化を定義してもよい。詳細化には、拡張パッケージ中の SFR へ特に限定して保証要件を満たす方法のガイダンスが提供されてもよい。しかし、OSPP の核心的な要件のひとつは、プロテクションプロファイル及びそのすべてのモジュールを、相互承認協定でカバーし続けることである。したがって、いかなる OSPP 拡張パッケージも SAR を追加したり、SAR のレベルを変更したりしてはならない（shall not）。それは相互承認協定によって線引きされた境界を越えてしまうかもしれないからである。詳細化は SFR 及び SAR に対して許可される操作であり、そのような詳細化もまた、パッケージ中に定義された機能に特有の側面を評価する方法に関して、評価者をガイドするために使用できることに注意されたい。とくに SAR に関しては、詳細化が使用されるべきである（should）。拡張保証コンポーネントは、可能な限り避けるべきである（should）。

# 3 OSPP 基本部の概論

OSPP 基本部では、今日の汎用オペレーティングシステムに見られる基本的な機能が定義される。ここでは、すべての汎用オペレーティングシステムにおいて、提供されなくてはならない（must）機能及びメカニズム、及びすでに実装されているものを規定する。

一般的な監査要件も OSPP 基本部に追加される。この機能は政府機関の利用者にとって必須であり、多くの IT セキュリティ標準に必須とされる基本的なアカウンタビリティ（責任追跡性）要件を満たすために要求されるからである。

TOE は、他の高信頼 IT エンティティと連携してセキュリティ機能を提供してもよい。セキュリティ課題定義では、TOE を利用するために可能な方法として、そのようなシナリオが考慮される。

## 3.1 TOE 概要

このセクションでは、OSPP 基本部への適合を主張する TOE によって提供されるセキュリティ機能の概要を述べる。

本文書に見られるような汎用オペレーティングシステムは、以下の機能を有している。

- 異なる「ユーザ」へサービスを提供する。ユーザは人間の利用者であってもよいし、他の IT システム（本プロテクションプロファイルにおいては「リモート IT エンティティ」と呼ばれる）であってもよい。
- 複数のサブジェクト（通常はプロセスまたはアドレス空間）を同時にサポートし、異なる利用者の代理として動作することを可能とする。また、異なる利用者のために動作するサブジェクトを互いに分離する。
- オペレーティングシステムによって定義された「名前付きオブジェクト」へのアクセスを仲介及び強制し、明確に定義されたルールに基づいてそのようなアクセスを許可または禁止する。
- 外部利用者の識別情報を検証し、そのような利用者にオペレーティングシステムが関連付けたセキュリティ属性に基づいたアクセス制御方針を可能とする。
- 定義された事象を十分なデータと共に記録し、事象の種類、事象が発生した時刻、そして可能であればその事象を引き起こした利用者の識別情報をレビュー者が特定することを可能とする。
- 管理可能なセキュリティ方針の側面を、管理アクティビティを実施できる利用者を限定するルールと共に定義する。
- 自分自身及び自分自身が依存するデータやオブジェクトを、改ざん及びセキュリティ方針のバイパスから保護する。

### 3.1.1 監査

本プロテクションプロファイルに適合するすべてのオペレーティングシステムは、セキュリティに関連するとみなされる事象をそのオペレーティングシステムが記録できるような監査機能を実装しなくてはならない（must）。そのような事象に対してオペレーティングシステムが作成した記録には、少なくとも事象の種類、事象が発生した時刻、その事象を引き起こした利用者またはサブジェクトの識別情報（該当する場合）、及び事象特有の追加データが含まれなくてはならない（must）。事象がある機能の利用要求であれば、その記録にはその機能がどのように使われることが意図されていたか（通常はその機能に渡されたパラメタによって定義される）、及びその機能の結果に関する十分な情報を含んでいることもまた必要とされる。事象がオブジェクトに関して実施された操作に関連する場合には、そのオブジェクトの識別情報が記録に含まれていなくてはならない（must）。

監査記録は、永続的ストレージ中の監査証跡に保存されなくてはならない（must）。あるいは、信頼できる集中型の監査サーバへ送信されてもよいが、利用者が集中型監査ストレージを構成しない場合やそのような監査ストレージが利用できなくなった場合に備えて、オペレーティングシステムはローカル監査ストレージをサポートしなくてはならない（must）。監査証跡に用いられるローカルストレージは、利用者またはサブジェクトによる不正アクセスから保護されなくてはならない（must）。以下を定義する方針が存在しなくてはならない（must）。

- ☐ 監査される実際の事象（監査可能事象の全体リストの中から）
- ☐ 利用者またはサブジェクトが監査されるべき事象を定義可能な場合を定義するルール
- ☐ 利用者またはサブジェクトが監査証跡から監査記録を読み出せる場合を定義するルール
- ☐ 利用者またはサブジェクトが監査証跡を削除または最初期化できる場合を定義するルール

オペレーティングシステムは、ローカルの監査証跡に割り当てられたスペースの量を監視し、スペースが不十分でそれ以上監査記録が保存できないことを検出した際には適切なアクションを取らなくてはならない（must）。

監査生成機能は、完全にローカルに（TSF によって独占的に）提供される。TOE は、以下ができなくてはならない（shall）。

- ☐ セキュリティ関連事象から監査情報を収集する。
- ☐ 監査情報をローカルに保存する機能を提供し、またリモートストレージメカニズムの提供を可能とする（監査データの分析は、ローカルに保存された監査データのみに適用される）
- ☐ 監査証跡がローカルに保存される場合、監査証跡のローカルな分析を提供する。
- ☐ どの監査記録が生成されるかの選択を可能とする。
- ☐ ローカルに保存される場合、 監査証跡の保護を提供する。
- ☐ いかなる監査記録も失われないよう、保護を提供する。

リモート監査処理は、OSPP 拡張パッケージへ移動されていることに注意されたい。さらに、TOE はリモート機能を使って監査データの保存または評価あるいはその両方を行うことができ、また適切な権限を認可された利用者に、さまざまな監査機能のどれが使われるかを定義させることができる。

### 3.1.2 利用者データ保護

以下のセクションで、汎用オペレーティングシステムプロテクションプロファイルの利用者データ保護に関する考慮事項を記述する。

#### 3.1.2.1 任意アクセス制御

任意アクセス制御は、特定の名前付けオブジェクトへのアクセス制御の設定が、任意アクセス制御方針の対象となるすべての利用者／サブジェクトとオブジェクトとの関係へ、個別に定義できることを意味する。

任意アクセス制御をサポートし、意図された利用者へルールセットが適用されるようにするため、TSF は利用者・サブジェクト間の束縛を実施してもよい。このプロセスの間、サブジェクトは特定の利用者と関連付けられ、オペレーティングシステムはサブジェクトのセキュリティ属性を、オペレーティングシステムがそのサブジェクトを束縛した利用者のセキュリティ属性から得る。そのような束縛の後、サブジェクトは利用者の代理者となる。この束縛は、セクション 3.1.3 においてより詳細に説明され、規定される。

単一のオペレーティングシステムに、異なる種類のサブジェクトまたはオブジェクトに対する異なる任意アクセス制御方針を実装してもよい。これらのアクセス制御方針がすべて、単一利用者の粒度にまで細かくアクセス権を規定可能であること、という基本要件を満たす限り、またこれらのアクセス制御方針が総体として、サブジェクト及びオブジェクトの

すべての種類をカバーしている限り、このことは問題とはならない。

任意アクセス制御方針の全体仕様は、以下を含む必要がある。

- □ 方針によってカバーされるオブジェクトの種類
- □ 方針によってカバーされるサブジェクト／利用者の種類
- □ 方針によってカバーされる操作
- □ 特定のサブジェクト／利用者が特定のオブジェクトに関するアクセス制御方針によってカバーされる操作を行うことが許可されているかどうかを判定するために用いられるルール。これには、それらのルールに利用されるサブジェクト／利用者のセキュリティ属性、オブジェクトのセキュリティ属性、及び他の任意の TSF データが含まれる

さらに、下記の側面がカバーされている必要がある。

- □ オブジェクトが作成可能な場合、それを判定するルール
- □ 任意アクセス制御方針中で用いられるオブジェクトのデフォルトセキュリティ属性を判定するルール
- □ 利用者にアクセス権の追加／変更／削除が許可される場合を判定するルール
- □ 方針中で用いられるオブジェクトのセキュリティ属性の変更／追加／削除が利用者に許可される場合を判定するルール
- □ オブジェクトの削除が利用者に許可される場合を判定するルール

アクセス制御方針は、利用者がデータを共有するために利用する可能性のあるすべての種類のオブジェクトに対して存在する必要がある（have to）。これには、永続的オブジェクト（例えばファイル）や、一時的オブジェクト（例えば共有メモリ）が含まれる。ここでの意図は、本プロテクションプロファイルに適合したオペレーティングシステムが、利用者が他の通常利用者と隔離された状態で操作できる（すなわち、オペレーティングシステムの管理者ではないいかなる他のユーザともデータを共有しない）ことと、単一の利用者の粒度にまで共有を細かく定義できることである。この目標を達成するためには、少なくとも 1 種類の永続的オブジェクトに対して、単一の利用者の粒度にまでアクセス権を細かく定義できる、少なくとも 1 つの任意アクセス制御方針が存在しなくてはならない（must）。すべての任意アクセス制御方針に、このレベルの粒度の提供が求められているわけではないことに注意されたい。

特定の状況においては、オブジェクトが別のオブジェクトに包含されてもよい（例えば、単一ファイル中に実装されたファイルシステム）ことに注意されたい。そのような場合には、2 つの異なる、そして互いに競合する可能性のあるアクセス制御方針が、永続的ストレージの同一の部分に対して適用されるかもしれない。オペレーティングシステムが自動的にそのような競合を解決しない場合、2 つのアクセス制御方針が競合しないように適切なアクセス権を設定する方法が、ガイダンスに説明されなくてはならない（must）。

OSPP は ST 作成者に、新たにアクセス制御されるオブジェクトに対するものだけではなく、新たなサブジェクトに対するデフォルトのアクセス権を、（該当する場合には）これらのデフォルトアクセス権の管理方法を定義するルールを含めて、規定することを要求している。

最後に、OSPP は ST 作成者に、利用者またはサブジェクトにアクセス制御ルールの中で用いられる TSF データの管理が許可される前に TOE が強制するルールの規定を要求している。通常、これらのルールは特定の TSF データ（利用者の特権など）に基づくものである。この TSF データが管理可能である場合、適用される管理ルールもまた規定されなくてはならない（must）。TSF データを管理するために満たされなくてはならない（must）条件を（そのアクセス制御ルールに用いられる TSF データを含めて）記述することは、ST 作成者の責任である。

OSPP では、アクセス制御ルール中にローカル及びリモートに保存された TSF データの使用を許可している。

さらに、OSPP では ST 作成者に、他のリモートの高信頼 IT 製品に対するアクセス制御判定を TOE が提供するかどうかの規定を許可している。このオプションを使えば、ST 作成

者はサーバ側にパーミッションストレージを規定することが可能となる。

#### 3.1.2.2 ネットワーク情報フローの制御

TOE は、受信されたネットワークデータのフィルタメカニズムによる取り扱いを定義する情報フロー制御方針を用いて､外部エンティティから TOE へ送られるネットワークデータ、または TOE 内のサブジェクトによって生成され外部エンティティへ送られようとしているネットワークデータをフィルタリングできなくてはならない（shall）。OSPP 基本部の要求するフィルタリング機能は、セクション 3.1.5.1 に記述されたプロトコルに対する静的フィルタルールに限定される。TCP/IP ベースのフィルタリングに関しては、ステートレスな、またはステートフルな、あるいはその両方のパケットフィルタリングがサポートされるかどうかの定義を、OSPP は ST 作成者に許可している。これらのフィルタリングルールは情報フロー方針として定義される。フィルタルールは、ネットワークインタフェースから宛先である TOE 中の「消費者」へネットワークデータが流れるために満たす必要のある条件を規定するからである。

情報フロー制御方針は、ネットワークデータを識別するルール、及びネットワークデータに対して行われる操作を定義する。

TOE は、最初にネットワークデータを識別することによって、次にネットワークデータに関してアクションを行うことによって、ネットワーク情報フロー制御を実施する。ネットワークデータの識別は、ネットワークデータの属性と、例えば、TCP 接続の状態、時間ベースのルール、または IP パケット n 個ごとにマッチするなどの統計的手段に基づくルールなど、TOE がネットワークトラフィックを仲介する際に管理される付加情報に基づいて行うことができる。識別されたネットワークデータに課されるアクションは、データの破棄、データの変更、送信者への通知の送信、あるいはネットワークデータを変更なしに通過させる、など多岐にわたる。

### 3.1.3 識別と認証

識別と認証は､TOE が TOE と対話する利用者の識別情報に必要とされる信頼を置くために要求される。利用者の識別と認証は、利用者の識別情報に基づくセキュリティ方針によって保護されたサービスをオペレーティングシステムが与える際に必要となる。識別と認証に用いられる手法は利用者の種類によって異なってもよく、またオペレーティングシステムは同一の種類の利用者に複数の異なる識別と認証の手法を許可してもよい。本プロテクションプロファイルに適合するオペレーティングシステムは、人間の利用者に関しては利用者 ID／パスワードを、また高信頼チャネルを確立しようとするリモート IT エンティティに関しては暗号トークンに基づいた認証をサポートしなくてはならない（must）。暗号トークンを用いた認証手法はネットワークプロトコルによって定義され、そして本プロテクションプロファイルに適合する TOE は（証明書ベースの認証と共に）SSH､TLS､または IPsec の中から少なくとも 1 つのプロトコルをサポートしなくてはならない（must）。

本プロテクションプロファイルに適合する TOE は､人間及びリモート IT エンティティに関して追加認証手法をサポートしてもよく、その場合それらは認証手法を管理するために必要な管理機能と共にセキュリティターゲットにおいて定義される必要がある。

人間の利用者の識別と認証が成功した後、オペレーティングシステムは認証済み利用者に代わって動作することになる（shall）信頼されないサブジェクトを起動する際にはいつでも、利用者・サブジェクト間の束縛を行う。オペレーティングシステムが他の IT システムに、それらの代理となるサブジェクトを起動することを許可している場合であって、この場合には利用者・サブジェクト間の束縛プロセスが異なる場合には、セキュリティターゲットにはそのようなサブジェクトからサブジェクトのセキュリティ属性を導出するルールを規定する、利用者・サブジェクト間の束縛のセキュリティ機能要件の 2 番目の具体化が含まれる必要がある。

OSPP は、利用者または他の IT システムが、セキュリティ方針によって特定の利用者に限定されているオペレーティングシステムの任意のサービスを利用する前に認証されなくてはならないことを要求する。OSPP 適合システムは、アクセス制御方針によってコントロールされているオブジェクトへ未認証の利用者がアクセスすることを許可してもよい。アクセス制御方針は、未認証の利用者に許可される操作を、そのような「公共」の操作であってオブジェクトを変更しないものに限定できなくてはならない（must）。

オペレーティングシステムは、リモートで認証された利用者に関する情報を含んだメッセージの完全性と真正性をオペレーティングシステムが検証できるような方法で、他の高信頼 IT システムが利用者の識別情報を報告する場合、その利用者を識別され認証されたものとして受け入れてもよい。これは、この基本プロテクションプロファイルに規定される範囲を超える機能となるであろうから、そのような機能を定義する追加 SFR が必要とされるであろう。

またオペレーティングシステムは、他の高信頼 IT システムの助けを借りて利用者を認証してもよい。例えば、他のシステムから認証に使用される情報（例えば、パスワードのハッシュ値）を取得する場合、または利用者から取得した情報を他のシステムへリダイレクトし､リモート高信頼 IT システムが利用者認証を行ってその結果を TOE へ報告する場合など。

OSPP 基本部では、以下の定義によるローカルまたはリモートで行われる識別と認証を許可することにより、TOE は識別と認証を提供しなくてはならない（shall）。

- ローカルの識別と認証は、TOE が利用者の識別情報を確立する操作を行うことを意味する。この定義により、利用者の資格情報を保持する TSF データを、TOE 上またはリモートの高信頼 IT システムのいずれかに、保存することが許可される。しかし、TOE は資格情報を含む TSF データを完全に取得して必要な操作を行うことができなくてはならず、また識別と認証のロジックがローカルに実装されていることをチェックしなくてはならない（must）。利用者が自分の識別情報を定義するトークン（証明書、Kerberos トークンなど）を提供した際には、別のローカルの識別と認証が行われる。TOE は、そのトークンを検証しなくてはならない（must）。
- リモートの識別と認証は、TOE が認証サーバのクライアントであることを意味する。TOE は利用者から提供された識別と認証のデータをサーバへ送付し、送信した資格情報の検証が成功したか失敗したかをサーバへ問い合わせる。次に TOE は、認証サーバによる判定を強制する。
- 公共オブジェクトへのアクセスについて、TOE は未認証の利用者の操作を許可しなくてはならない（shall）（利用者は識別と認証を免除されなくてはならない（shall））。許可される操作と公共オブジェクトは、ST 作成者によって定義されなくてはならない（must）。

例えば、ディレクトリサーバは利用者の資格情報や利用者の資格情報の内部表現を保存するかもしれない。TOE が利用者のパスワードを含めたすべての資格情報を取得でき、利用者に提供された資格情報を保存されたものと突き合わせて検証する操作を行う際には、ローカルの識別と認証が行われる。しかし、例えば TOE が利用者から提供された資格情報を用いて LDAP に束縛された操作を行い､LDAP サーバがその操作を拒否するかどうかを確認するだけの場合には、リモートの識別と認証が行われる。

OSPP は、ローカル、リモート、及びローカルとリモートとを組み合わせた識別と認証を許可している。最後のものは、通常大規模なシステムに見られる。例えば、ローカルの利用者データベースが管理ユーザ ID で定義されており、認証サーバとの接続が切断された際にのみ使用できるようなものである。もうひとつ例を挙げるとすれば、認証サーバの利用者データベースを TOE がキャッシュしており、認証サーバとのリンクが切断された場合にこのデータベースを適用することが考えられる。TOE が同時に複数の認証手法（例えばローカル認証とリモート認証）を許可する場合には、ST 作成者は認証手法が適用される順序

を指定しなくてはならない（shall）。

さらに、OSPP は ST 作成者に、TOE が他のリモート高信頼 IT 製品へ識別と認証を提供するかどうかを規定できるようにしなくてはならない（shall）。このオプションを採用した場合、ST 作成者はサーバ側に資格情報ストレージを規定できる。

資格情報または利用者資格情報の内部表現が TOE 内に保存される際には、TOE は資格情報が管理ユーザまたは正当な利用者によって変更される際に資格情報の品質を確実に保たなくてはならない（shall）。

少なくとも、識別と認証の機能は以下のメカニズムのすべてを提供しなくてはならない（shall）。

- □ 利用者 ID／パスワード（人間の利用者に対して）
- □ ソフトウェアトークンベースの認証（高信頼チャネルを設定しようとするリモート IT エンティティに対して）

識別と認証が成功した後で、TSF は利用者・サブジェクト間の束縛を行ってもよい。そのような束縛は、オペレーティングシステムが利用者の代理として動作するサブジェクトを作成し起動する際に必要とされる。このプロセスによって、外部エンティティ（または利用者）がサブジェクトへ確実に「束縛」されることになる。ST 作成者は、利用者・サブジェクト間の束縛プロセスへ適用されるルールを定義しなくてはならない（must）。これらのルールは、サブジェクトのセキュリティ属性が初期化される方法（通常は利用者のセキュリティ属性から導出される）を定義する。詳細に関しては、セクション 1.4.3 を参照されたい。利用者・サブジェクト間の束縛の間、セキュリティ方針のルールによって用いられるサブジェクトのすべてのセキュリティ属性が確立されなくてはならない（must）。

### 3.1.4 セキュリティメカニズムの管理

TOE は、TOE によって提供されるすべてのセキュリティ機能について管理メカニズムを提供しなくてはならない（must）。

TOE がリモート高信頼 IT システムのサポートも受ける場合には、この管理要件は TOE によって提供される機能の側面のみを対象とする。

セキュリティ機能の側面の管理を行う権限は専用の管理ルールに基づくが、それは特権をベースにしている場合が多い。これらの特権は、管理インタフェースを使用する、または TSF のふるまいを支配するリソースへアクセスする、特定の特権を要求することによって、TOE が明示的に実装できる。また特権は、例えば TSF の全部または一部の構成を保持する構成ファイルまたは構成データベースなど、TSF データへの書き込みアクセスを許可することによって、暗黙的に与えられてもよい。一方では、管理操作が行われる方法を規制するルールは、例えば TSF データを含むストレージオブジェクトへのアクセス、もしくは特定のインタフェースまたはデバイスへのアクセス、システムの状態、またはこれらの側面の任意の組み合わせなどの他の側面に基づいて実施されてもよい。

OSPP 基本部においては、ST 作成者は管理操作が許可されるかどうかを判定するルールだけではなく、管理可能な TSF データも定義しなくてはならない（must）。少なくとも、管理可能な TSF データには以下が含まれなくてはならない（must）。

- □ 利用者及び利用者の管理可能なセキュリティ属性の管理。
- □ 任意アクセス制御方針に用いられるセキュリティ属性の管理。セキュリティ属性の管理によって、単一利用者の粒度にまでアクセスを細かく定義できなくてはならない（must）（アクセス制御方針によって制御されるオブジェクトへのアクセスが許可され

る利用者の種類について）。
- □ 情報フロー制御方針に用いられるセキュリティ属性の管理。
- □ 監査方針の管理。これには、少なくとも監査されるべき事象の選択と、監査証跡が含まれるストレージオブジェクトの管理が含まれる。

OSPP は、特定の実装を強制しない。しかし、TOE は以下にしたがわなくてはならない（must）。

- □ 管理機能をゼロ人、1 人、または 2 人以上の利用者へ割り当てることができること。

ST 作成者は、管理アクティビティが許可されるかどうかを判定するために用いられるルール､及びそれらのルールにおいて用いられる TSF データを規定しなくてはならない（shall）。OSPP は、いかなる方針も、またいかなる特定のルールのセットも、規定しない。それゆえ、ST 作成者はすべての特権を与えられた 1 人の利用者（UNIX の root ユーザなど）を規定することができる。さらに、ST 作成者は階層的な特権や役割ベースの管理など、洗練された管理方針を規定することもできる。

TOE は、これらのセキュリティ機能のローカルな、または集中型の、あるいはその両方の管理ができなくてはならない（shall）。

- □ ローカルな管理は、セキュリティ機能の側面を構成するツールが TOE によって提供されることを意味する。SFR は、TOE データがリモートに保存されるかどうかに関して一切の言明を行わない（上記のローカルの識別と認証に関する議論を参照）。
- □ リモート管理は､セキュリティ機能の管理が TOE によって提供されるのではなく､TOE が管理アクションを強制することを意味する。これは、この基本プロテクションプロファイルに含まれない追加的な SFR を用いて定義される必要のある、オプションの機能となるであろうことに注意されたい。

管理の種類（ローカルかリモートか）に関わらず、構成データはローカルまたはリモートに保存することができる。リモートに保存される場合、構成データがリモート管理システムまたは他のシステムに保存されるかどうかに関しての制約は存在しない。

OSPP では、管理ルール中にローカル及びリモートに保存された TSF データの使用を許可している。

さらに、OSPP では ST 作成者に、他のリモートの高信頼 IT 製品に対する管理判定を TOE が提供するかどうかの規定を許可している。このオプションを採用した場合、ST 作成者はサーバ側での管理操作を規定できる。

### 3.1.5 高信頼チャネル

リモート管理をサポートするため、OSPP ではオペレーティングシステムが高信頼リモートエンティティへの高信頼チャネルを確立する機能を有することを要求している。リモート管理アクティビティは、そのような高信頼チャネルを要求しなくてはならず（shall）、またリモートエンティティの公開鍵ベースの認証を用いる必要もある。

さらに、TOE がセキュリティ方針の強制をサポートするリモート高信頼 IT システムからの入力を必要とする場合、TOE はこのリモート高信頼 IT システムへの高信頼チャネルを確立しなくてはならない（shall）。リモート高信頼 IT システムの関与は、利用者認証またはシンプルなリモートストレージやリモート高信頼 IT システムから TOE へインポートされた TSF データの管理などの機能を提供する、アクティブなサポートを意味する可能性がある。また TOE は、リモート高信頼 IT システムを用いて利用者及び TSF データを保存し、そのデータを TOE、またはそのリモート高信頼 IT システム、あるいは他の高信頼 IT システムが

使えるようにすることもできる。さらに、TOE はリモート高信頼 IT システムへセキュリティ関連のサービスを提供してもよい。これらすべての場合において、TOE と高信頼 IT システムとの間の通信は、真正性 TOE とリモート高信頼 IT システムとの間で交換されるデータが十分に保護されることを確実にし、交換される TSF データの真正性、完全性、及び機密性が確実に保たれるようにしなくてはならない（must）。

したがって多くの場合、オペレーティングシステムは高信頼チャネルを利用して、高信頼チャネルの両エンドポイントの相互認証に加えて、機密性と完全性の保護を提供することになる。またリモート高信頼 IT システムへの高信頼チャネルを確立し維持する機能は、オペレーティングシステムがサブジェクトや利用者へ提供できるサービスでもある。本プロテクションプロファイルへ適合したオペレーティングシステムは、そのような機能をサブジェクトへ提供しなくてはならない（must）。

#### 3.1.5.1 暗号保護されたネットワークプロトコル

TOE は、完全性、機密性、及び真正性が保護された利用者及び TSF データの送信を可能とするネットワークプロトコルの形で、応用暗号サービスを提供しなくてはならない（shall）。

少なくとも、TOE は下記のプロトコルの 1 つを実装しなくてはならない（must）。

- ☐ SSH（このプロトコルのバージョン 1 は認められない）
- ☐ TLS
- ☐ IPSEC – OSPP は、実装が IKE と ESP を提供しなくてはならないことを義務付けている。OSPP が IPSEC を規定する際には AH は要求されていないが、ST 作成者によって追加されてもよい。

詳細については、高信頼チャネルに関する上記のセクションを参照されたい。

さらに TOE は、一般的な暗号サービスを実装してもよく、それを利用者またはサブジェクトが直接利用できるようにしてもよい。これらのサービスはこの基本プロテクションプロファイルの対象ではないが、セキュリティターゲット中の追加 SFR として規定してもよい。また、暗号サービスプロバイダの基本要件は拡張パッケージ中に規定することも意図されている。

OSPP は、上記のプロトコルの基盤となる暗号メカニズムが、異なる OSPP 拡張パッケージで概要説明される他のコンポーネントまたはセキュリティ機能から使用されることを、強制してもいないし禁止してもいない。しかし、他のネットワークメカニズムが他のセキュリティ機能とは独立したそれ自身の暗号メカニズムのインスタンスを実装する場合には、評価者はこれらのインスタンスもまた評価しなくてはならない（must）。

## 3.2 高信頼システム間の協調

現在の IT アーキテクチャにおいては、オペレーティングシステムのみならず IT アプリケーションが、IT 環境全体の中で使用される集中型サーバによって提供されるサービスを利用することは、一般的である。またこれは、本プロテクションプロファイルに定義されるようなセキュリティ機能を実装するオペレーティングシステム機能についてもあてはまる。例としては、利用者のセキュリティ属性を集中管理するためのディレクトリサーバ、集中型の認証サーバ、集中型のアクセスマネージャ、集中型の監査の収集及び評価、さらには集中型のセキュリティ管理機能などが挙げられる。OSPP ではそのような集中型サービスの使用を強制はしないが、一方では OSPP 基本部に適合するオペレーティングシステムが、セキュリティ機能の一部を提供するリモート高信頼 IT システムを用いてセキュリティ機能を実装することを禁止してもいない。それでも、すでに述べたように、OSPP 基本部に適合するオペレーティングシステムは OSPP 基本部に列挙された SFR を満たす機能をローカルに、すなわち IT 環境のサポートなしに、実装**しなくてはならない（must）**。例として、

OSPP 基本部への適合主張を望むオペレーティングシステムは、オプションとして外部ディレクトリサーバに依存する識別と認証サービスまたは利用者管理を提供してもよいのはもちろんであるが、ローカルな利用者認証及び利用者管理もサポートしなくてはならない（must）。

オペレーティングシステムが IT 環境からのサポートを利用する機能を提供する場合であっても、オペレーティングシステムは利用者及びサブジェクトへ要求されるセキュリティ機能へのインタフェースを提供しなくてはならず、またリモート高信頼システムによって提供されるいかなるサービスも正しく呼び出され、そのようなサービスが TOE のセキュリティ方針にしたがって適切に使用される結果となることを確実にしなくてはならないことが要求されている。例えば、オペレーティングシステムがアクセス制御の判断をサポートするためにオプションとして集中型アクセスマネージャを利用できる場合、その TSF はリモートアクセスマネージャのサービスが必要なときに呼び出されること、行われるべきアクセスの判断に関して正しく呼び出されること、さらに TSF がリモートアクセスマネージャの呼び出しから自分に戻ってきた結果を正しく使用することを確実にしなくてはならない（must）。

そのようなリモート高信頼システムを、自身のセキュリティ方針のサポートのために利用する TOE は、セキュリティ方針のどの部分がリモート高信頼 IT 製品の支援を受けて強制されるのかについて、またそのようなリモート高信頼 IT システムの機能に関する前提条件を、そのセキュリティターゲット中に定義しなくてはならない（must）。セキュリティ機能要件の概念を用いてこれらの前提条件を規定することは、必要とはされないが有用かもしれない。これによってそれらの前提条件を、そのようなリモート高信頼 IT システムのセキュリティターゲットに定義されたセキュリティ機能要件へ、容易に関連付けることが可能となる（このシステムもまた評価された製品を用いて実装されている場合）。

またセキュリティサービスをサポートするためリモート高信頼 IT システムを利用する多くのオペレーティングシステムは、そのようなサービスを自分自身でも提供できるようにオペレーティングシステムを構成することを可能としている。これによってシステムインテグレータは、すべて同一のオペレーティングシステム製品を基本とした複数のシステムからなる IT 環境を構築し、これらのシステムの 1 つが集中型サービスを提供するサーバとして動作するように構成し、他のすべてはこのサービスのクライアントとして動作するように構成して、この集中型サービスを利用してその組織のセキュリティ方針の強制を行うようにすることができる。典型的な例としては、利用者のセキュリティ属性を保存及び管理する集中型サービスとしてのディレクトリサーバであって、利用者認証をサポートし利用者・サブジェクト間の束縛に必要とされる利用者のセキュリティ属性を提供するために、特定の IT 環境中のすべてのシステムによって利用されるものが挙げられる。

そのような高信頼 IT システム間の協調は、クライアントサーバ型の関係に必ずしも制約されない。例えば利用者認証プロセスの一部としてスマートカードが使われる、ピアツーピア型の関係であってもよい。さらに、オペレーティングシステムは複数のリモート高信頼 IT システムを使用して単一のセキュリティ機能を提供してもよく、利用者を認証するために、TOE は利用者にスマートカードの提示を要求してもよい。スマートカードは（利用者の代理として）デジタル証明書を提示してもよく、それに対して TOE はチャレンジレスポンスプロトコルを使用して、スマートカードが提示するデジタル証明書と関連付けられた秘密鍵が実際にスマートカードに含まれていることを検証してもよい。さらに、TOE はディレクトリサーバのサービスを使用して、証明書が失効していないことを検証してもよい。また、TOE はスマートカードの認証プロセスに必要とされる暗号操作（スマートカードの提示する証明書を発行した CA のデジタル署名の検証を含む）及びディレクトリサーバの提供する失効リストのデジタル署名を検証するプロセスを行うために、TOE 境界外部の暗号モジュールへのピアツーピア接続を利用してもよい。

## 3.3 TOE 境界

本プロテクションプロファイルでは、TOE 境界を以下のようにみなしている。TOE は、すべての外部エンティティに対して単一のユニットとして動作するシステムである。この定義により、以下の例を用いて単一の TOE インスタンスとその境界を説明する。

- □ 1 つのオペレーティングシステムのインスタンスを収容する単一のマシン、例えば 1 台の物理マシンまたは仮想マシン。
- □ 複数のハードウェアコンポーネントであって、すべてが単一のシステムイメージを実行するもの。すなわち、複数のハードウェアマシンが相互接続され 1 つのオペレーティングシステムのカーネルを実行する NUMA システムなど、1 つのソフトウェアインスタンスがすべてのハードウェアコンポーネントを制御するもの。
- □ 複数のハードウェアコンポーネントであって、それぞれが独自の TOE オペレーティングシステムのインスタンスまたはオペレーティングシステムカーネルを実行するが、どの外部エンティティからも唯一の定義されたパスを持ってこのシステムへアクセスするとともに、これらの複数のシステムが一体となって動作していると「見える」もの。例えば高性能コンピューティグクラスタであって、異なるノードが異なるタスクを割り当てられている（例えば 1 つのノードが計算業務を行い、1 つのノードがディスク空間をホストし、1 つのノードがクラスタのネットワーク接続を確立し、1 つのノードが他のエンティティへのインタフェースを提供する）が、クラスタ全体の機能を提供するためには協調動作しなくてはならないもの。

複数のオペレーティングシステムのインスタンスであって、外部エンティティからこれらのインスタンスが「見える」ものは、複数の TOE インスタンスを形成するとみなされる。特にこれは、クライアントサーバまたはピアツーピア構成であって、各オペレーティングシステムのインスタンスが 1 つの TOE インスタンスを構成するものに当てはまる。例えば、集中型の LDAP サーバが他のオペレーティングシステムのインスタンスへ集中型の識別及び認証インスタンスを提供する場合、LDAP サーバのオペレーティングシステム及び他のオペレーティングシステムのインスタンスは、個別の TOE インスタンスを形成する。同様に、ストレージエリアネットワーク（SAN）または分散ファイルシステムなど、1 以上のリソースを共有する複数のオペレーティングシステムのインスタンスは、個別の TOE インスタンスを構成する。共有リソースが 1 つの TOE に所属するか、どの TOE とも独立したリソースを形成するとみなされるかの判断は、ST 作成者に任されている。

以下の例は、TOE インスタンスの異なる形態を示すものである。青色のボックスはすべて、TOE インスタンスの 1 つの例である。ボックスを結ぶ線は、対話があり得ることを示している。

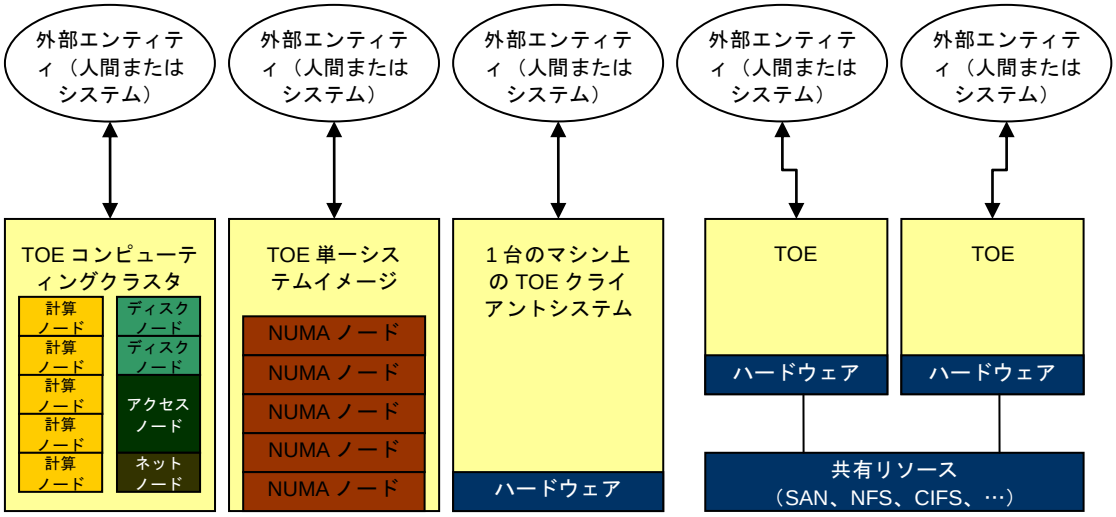


**図 1：TOE インスタンスの種類とその境界**

# 4 適合主張

以下のセクションでは、汎用オペレーティングシステムプロテクションプロファイル（OSPP）の適合主張を記述する。

## 4.1 CC パート 2 及び 3 への適合

OSPP は、CC バージョン 3.1 リビジョン 4 パート 2 拡張及びパート 3 へ適合する。

## 4.2 他のプロテクションプロファイルへの適合

OSPP は、他のいかなるプロテクションプロファイルへの適合も主張しない。

## 4.3 適合記述

OSPP は、ST による正確適合を要求する。

ST 作成者は、複数の OSPP 拡張パッケージへの適合を主張する際、OSPP 基本部及びすべての OSPP 拡張パッケージの ST への統合が正確適合に関して [CC] に規定されたルールに準拠していることを検証しなくてはならないことに注意されたい。ある OSPP 拡張パッケージが、他の OSPP 拡張パッケージと互いに相容れないということもあり得る。OSPP 拡張パッケージの作成者は互換性の評価を行っていなくてはならない（shall）が、その評価の結果がより新しいバージョンの OSPP 拡張パッケージや、あるいは新たに規定された OSPP 拡張パッケージによって無効となっているかもしれないからである。

## 4.4 OSPP 拡張パッケージに必要とされる適合

OSPP 拡張パッケージは、OSPP 基本部の機能を拡張することが許可される。機能を拡張するには、SFR を追加するのみではなく、新たな対応方針及びセキュリティ課題定義への追加が拡張パッケージに規定されてもよい。しかし、これらの拡張パッケージはコモンクライテリアのルール、具体的には [CC] パート 1、附属書 D において正確適合に関して概説されたルールに準拠しなくてはならない（must）。

この要件は、とりわけ以下のことを意味する。

- ☐ OSPP 基本部またはそれに依存する OSPP 拡張パッケージに言明された前提条件は、TOE によってカバーされるべき SFR へ変換される脅威または組織のセキュリティ方針あるいはその両方によって、置き換えられてもよい。
- ☐ OSPP 基本部またはそれに依存する OSPP 拡張パッケージに既に含まれている機能に関しては、前提条件を追加することはできない。そのような前提条件は、TOE によって実装されることが期待される機能を、環境へと移動してしまうかもしれないからである。

# 5 セキュリティ課題定義

OSPP 基本部機能のセキュリティ課題定義は、マルチユーザ、マルチプロセスのシステムとして実装される汎用オペレーティングシステムを定義するものである（shall）。

以下のセクションでは、OSPP 基本部のセキュリティ機能の基礎となる、さまざまな重要な用語、脅威、前提条件及び方針の定義を提供する。

## 5.1 脅威

TOE によって対抗されるべき脅威は、脅威の対象となる資産、脅威エージェント、及び敵対的な動作によって特徴づけられる。

以下の脅威エージェント及び保護資産の定義は、OSPP 基本部と共に、OSPP 拡張パッケージにも、特に断りのない限り適用される。

### 5.1.1 資産

保護されるべき資産は、以下のとおりである。

- 利用者データまたは TSF データ、あるいはその両方の保存のために使われるストレージオブジェクトであって、このデータが以下の操作のいずれからも保護される必要があるもの。
  - 不正な読み取りアクセス
  - 不正な変更
  - オブジェクトの不正な削除
  - 新しいオブジェクトの不正な作成
  - オブジェクト属性の不正な管理
- TSF 機能及びそれに関連付けられた TSF データ
- TSF によって管理されるリソースであって、上記のオブジェクトを保存するために利用されるもの（これらのオブジェクトを管理するために必要とされるメタデータを含む）。

### 5.1.2 脅威エージェント

脅威エージェントは、TOE を攻撃するおそれのある外部エンティティである。脅威エージェントは、下記の基準の 1 つ以上を満たす。

- 資産へアクセスする権限のない外部エンティティが、正当なエンティティへのなりすましによって、または適切な認可なしに TSF サービスの使用を試みることによって、それらへのアクセスを試みるおそれがある。
- 特定の資産へアクセスする権限のある外部エンティティが、それらが利用を許可されているサービスの悪用によって、または異なる外部エンティティへのなりすましによって、権限を持たない他の資産へのアクセスを試みるおそれがある。
- 信頼されないサブジェクトが、それらが利用を許可されているサービスの悪用によって、または異なるサブジェクトへのなりすましによって、権限を持たない資産へのアクセスを試みるおそれがある。

脅威エージェントは典型的に、専門知識、利用可能なリソース、及び動機などのいくつかの要因と、問題となる資産の価値と直接リンクした動機によって特徴づけられる。TOE は、拡張された基本的な攻撃能力を有する攻撃者による、意図的または意図的でない TOE セキュリティの違反に対して保護を行う。

以下の脅威は、OSPP 基本部に適合した TOE によって対処される。本 PP はこれらの脅威と、必要なセキュリティ機能を導出するために必要な組織のセキュリティ方針をカバーする。保証レベルを正当化する脅威や方針は存在しない。選択された評価保証レベルはすでに CC において､保証手段によって対抗される脅威を説明する根拠と共に定義されているため、不必要とみなされる。

### 5.1.3 TOE によって対抗される脅威

T.ACCESS.TSFDATA 脅威エージェントが、必要な認可なしに TOE の機能を用いて TSF データを読み取り、または変更するおそれがある。

T.ACCESS.USERDATA 脅威エージェントが、TOE によって提供される機能を用いて、TOE のセキュリティ方針にしたがって適切に認可されることなく、TOE によって保存、処理、または送信された利用者データへのアクセスを行うおそれがある。

T.ACCESS.TSFFUNC 脅威エージェントが、TSF の保護メカニズムをバイパスすることによって、TSF の機能を利用し、または管理するおそれがある。

T.ACCESS.COMM 脅威エージェントが、TOE と別のリモート高信頼 IT システムとの間の高信頼チャネルを介して転送される暗号保護データへアクセスしたり、受信者によって検出できないような方法で転送中のそのようなデータを変更したり、あるいはリモート高信頼 IT システムになりすましたりするおそれがある。

T.RESTRICT.NETTRAFFIC 脅威エージェントが、情報フロー制御方針に違反してネットワーク通信チャネルを介して TOE 内の受信者へデータパケットを送信するおそれがある。

T.IA.MASQUERADE 脅威エージェントが、利用者データ、TSF データ、または TOE リソースへの不正なアクセスを行うために、TOE そのものや TOE の一部を含めた正当なエンティティになりすますおそれがある。

T.IA.USER 脅威エージェントが、TSF によって識別され認証されることなく、公共オブジェクトを除いた利用者データ、TSF データ、または TOE リソースへのアクセスを行うおそれがある。

T.UNATTENDED_SESSION 脅威エージェントが、放置されたセッションへ不正なアクセスを行うおそれがある。

## 5.2 組織のセキュリティ方針

以下の組織のセキュリティ方針は、PP に適合した TOE によって対処される。

P.ACCOUNTABILITY TOE の利用者は、TOE 内での自分のセキュリティ関連の行動に責任を持たなくてはならない（shall）。

P.USER 権限は、正しく行動を行うことが信頼されている利用者にのみ与えられなくてはならない（shall）。

P.ROLES TSF 機能への管理権限は、信頼できる要員へ与えられ、またそ

の要員の有する管理職務のみをサポートするよう、可能な限り制限されなくてはならない（shall）。

## 5.3 前提条件

以下の特定の条件が、PP に適合した TOE 環境に存在することが前提となる。

### 5.3.1 物理的側面

A.PHYSICAL　IT 環境によって、TOE の保護する IT 資産の価値に対応した、適切な物理的セキュリティが TOE へ提供されることが前提とされる。

### 5.3.2 人的側面

A.MANAGE　TOE のセキュリティ機能は、1 人以上の適格な個人によって管理される。システム管理要員は、不注意であったり、故意に怠慢であったり、あるいは敵対的であったりしてはならず、またガイダンス文書の提供する指示に従い、これを遵守する。

A.AUTHUSER　正当な利用者は、TOE の管理する情報の少なくとも一部へアクセスするために必要な権限を有し、また良性の環境において協力的な態度で行動することが期待される。

A.TRAINEDUSER　利用者は十分に教育され、自分の利用者データに関する完全な制御権を行使することにより、セキュアな IT 環境の内部で何らかのタスク、またはタスクのグループを達成するよう信頼されている。

### 5.3.3 手続的側面

A.DETECT　意図的か、あるいは偶然に、利用者または基盤となるプラットフォームによって引き起こされた、TOE のセキュリティ強制機能またはセキュリティ関連ファイルの何らかの改変または損傷は、管理ユーザによって検出される。

A.PEER.MGT　TSF データまたはサービスを TOE へ提供すること、またはセキュリティ方針の判断の強制において TSF をサポートすることが TSF によって信頼されるすべてのリモート高信頼 IT システムは、同一の管理制御下にあって TOE のものと互換性のあるセキュリティ方針の制限下で動作することが前提となる。

A.PEER.FUNC　TSF データまたはサービスを TOE へ提供すること、またはセキュリティ方針の判断の強制において TSF をサポートすることが TSF によって信頼されるすべてのリモート高信頼 IT システムは、TSF によって用いられる機能を、この機能について定義された前提条件と一貫して正しく実装することが前提となる。

### 5.3.4 接続性の側面

A.CONNECT　リモート高信頼 IT システムとの、及び TSF 自身によって保護されない TSF の物理的に分離した部分間のすべての接続は、物理的または論理的に TOE 環境中で保護されて、送信されるデータの完全性及び機密性が確実に保たれ、そして通信エンドポイントの真正性が確実に保たれる。

適用上の注意：TOE が分離した部分から構成され、またこれらの部分間を通過中の TSF データの保護を確実にするメカニズムを TOE が実装している場合、ST 作成者は FPT_ITT.1 を主張して A.CONNECT を補足または置換することを考慮してもよい。

# 6 セキュリティ対策方針

以下のセクションでは、汎用オペレーティングシステムプロテクションプロファイルのセキュリティ対策方針を記述する。

## 6.1 TOE のセキュリティ対策方針

以下のセキュリティ対策方針が、TOE に定義される。

O.AUDITING TSF は、定義されたセキュリティ関連の事象（通常は TOE の利用者のセキュリティ上重要なアクションが含まれる）を記録できなくてはならない（must）。監査証跡がローカルシステム用に保存されている場合、TSF はこの情報を保護し、正当な利用者へ提示しなくてはならない（must）。セキュリティ関連事象に関して記録された情報には、発生した事象の時刻及び日付と、可能な場合には、その事象を引き起こした利用者の識別情報が含まれていなくてはならず、またセキュリティ違反の試行または IT 資産を危殆化させるかもしれない TOE セキュリティ機能の構成ミスを正当な利用者が検出できるように、十分に詳細でなくてはならない（must）。

O.DISCRETIONARY.ACCESS TSF は、オブジェクトの識別情報に基づいて、名前付きリソースへのサブジェクトまたは利用者あるいはその両方のアクセスを制御しなくてはならない（must）。TSF は、正当な利用者が、各アクセスモードについて、そのアクセスモードでどの利用者／サブジェクトに特定の名前付きオブジェクトへのアクセスが許可されるかを指定できるようにしなくてはならない（must）。

O.NETWORK.FLOW TOE は、そのネットワーク情報フローセキュリティ方針にしたがって、TOE 外部のエンティティと TOE 内部の受信者との間のネットワーク通信を仲介しなくてはならない（shall）。

O.SUBJECT.COM TOE は、その任意アクセス制御方針にしたがって、異なるサブジェクトセキュリティ属性と共に動作するサブジェクト間でオブジェクトまたはリソースの共有が可能な場合には、それを仲介しなくてはならない（shall）。

O.I&A TOE は、正当な利用者にのみ提供されると TOE が定義する任意のアクションを許可する前に、利用者の認証が成功していることを確実にしなくてはならない（must）。

O.MANAGE TSF は、TOE のセキュリティメカニズムを管理する責任を持つ正当な利用者をサポートするために必要なすべての機能及び設備を提供しなくてはならず、そのような管理アクションを専門の利用者に制限することができなくてはならず（must）、またそのような正当な利用者のみが管理機能へアクセスできることを確実にしなくてはならない（must）。

O.TRUSTED_CHANNEL TSF は、転送されたデータの完全性及び機密性を確実にするとともに通信のエンドポイントを認証できる暗号保護されたネットワークプロトコルを用いて正当な利用者が TOE へリモートアクセスすることを許可しなければならない（must）。TSF が複数

の部分に物理的に分離しており、それらが信用できないネットワーク接続上で互いにセキュアな通信を行わなくてはならない場合にも、同一のプロトコルが用いられてもよいことに注意されたい。またこのプロトコルは、リモート高信頼 IT システムのなりすましを防ぐことができなくてはならない（must）。

O.UNATTENDED_SESSION　TOE は、利用者のセッションの一時的な中断を許可するとともに、利用者自身が TSF へ再認証することによってセッションを再開した後にのみ、その中断されたセッションならびに利用者に関連した入力及び出力の継続を許可しなければならない（must）。

## 6.2 運用環境のセキュリティ対策方針

以下の対策方針は、TOE の運用環境によって満たされるべきものである。

OE.ADMIN　TOE の責任者は、適任かつ信頼できる個人であって、TOE 及びそれに含まれる情報のセキュリティを管理できる。

OE.REMOTE　TOE がその方針の強制のサポートをリモート高信頼 IT システムに依存している場合、これらのシステムは TOE によって必要とされる機能を提供し、またこれらの機能に間違った結果を生じさせる可能性のある任意の攻撃から十分に保護される。

OE.INFO_PROTECT　TOE の責任者は、情報が適切に保護されていることを確実にする手順を確立し、実行しなくてはならない（must）。特に、

- □ すべてのネットワーク及び周辺装置の配線は、システムの保持する最も機密性の高いデータの送信が承認されたものでなくてはならない（must）。そのような物理リンクは、送信されるデータの機密性及び完全性への脅威に対して十分に保護されていることが前提となる。
- □ セキュリティ関連のファイル（監査証跡や認証データベースなど）の DAC 保護は、常に正しく設定されていなくてはならない（shall）。
- □ 利用者は TOE の管理するデータの部分へアクセスする権限を持ち、また自分のデータに関する制御権を行使するよう教育される。

OE.INSTALL　TOE の責任者は、セキュアな方法でハードウェア、ソフトウェア、及びファームウェアコンポーネントが配付され、インストールされ、構成されることを確実にする手順を確立し、実行することによって、TOE によって提供されるセキュリティメカニズムをサポートしなくてはならない（must）。

OE.MAINTENANCE　TOE の正当な利用者は、製品の提供する包括的な診断機能が、スケジュールされた予防保全周期で毎回起動されることを確実にしなくてはならない（must）。

OE.PHYSICAL　TOE の責任者は、セキュリティ方針の強制に不可欠な TOE の部分が、IT セキュリティ対策方針を危殆化させるかもしれない物理攻撃から保護されていることを確実にしなくてはならない（must）。この保護は、TOE によって保護される IT 資産の価値

と対応していなくてはならない（must）。

OE.RECOVER TOE の責任者は、システム障害やその他の断絶後に保護（セキュリティ）の危殆化を実現することなく確実に回復するための手続きまたはメカニズムあるいはその両方が提供されることを確実にしなくてはならない（must）。

OE.TRUSTED.IT.SYSTEM リモート高信頼 IT システムは、セキュリティ方針の強制をサポートするために TSF によって要求されるプロトコル及びメカニズムを実装する。

これらのリモート高信頼ITシステムはTOEと同一管理ドメイン下に置かれ、TOE に適用されるものと同一のルール及び方針に基づいて管理され、そして TOE と同様に物理的かつ論理的に保護されている。

## 6.3 セキュリティ対策方針の根拠

以下の表は、セキュリティ対策方針と、脅威、方針、及び前提条件によって定義された環境との対応付けを示すものであり、セキュリティ対策方針のそれぞれが少なくとも 1 つの脅威、前提条件または方針をカバーしていること、及び脅威、前提条件または方針が少なくとも 1 つのセキュリティ対策方針によってカバーされていることを説明している。

### 6.3.1 セキュリティ対策方針のカバレージ

| 対策方針 | SPD カバレージ |
|---|---|
| O.AUDITING | P.ACCOUNTABILITY |
| O.DISCRETIONARY.ACCESS | T.ACCESS.USERDATA, T.ACCESS.TSFDATA |
| O.NETWORK.FLOW | T.RESTRICT.NETTRAFFIC |
| O.SUBJECT.COM | T.ACCESS.USERDATA, T.ACCESS.TSFDATA |
| O.I&A | T.IA.MASQUERADE, T.IA.USER |
| O.MANAGE | P.ACCOUNTABILITY, P.USER, T.ACCESS.TSFFUNC |
| O.TRUSTED_CHANNEL | T.ACCESS.USERDATA, T.ACCESS.TSFDATA, T.ACCESS.TSFFUNC, T.ACCESS.COMM |
| O.UNATTENDED_SESSION | T.UNATTENDED_SESSION |

**表 1：TOE のセキュリティ対策方針のカバレージ**

| 対策方針 | SPD カバレージ |
|---|---|
| OE.ADMIN | A.AUTHUSER, A.MANAGE, A.TRAINEDUSER |
| OE.REMOTE | T.ACCESS.COMM, A.CONNECT |
| OE.INFO_PROTECT | P.USER, A.AUTHUSER, A.TRAINEDUSER, A.PHYSICAL, A.MANAGE |
| OE.INSTALL | A.MANAGE, A.DETECT |
| OE.MAINTENANCE | A.DETECT |
| OE.PHYSICAL | A.PHYSICAL |
| OE.RECOVER | A.MANAGE, A.DETECT |
| OE.TRUSTED.IT.SYSTEM | A.CONNECT, A.PEER.MGT, A.PEER.FUNC |

**表 2：TOE 環境のセキュリティ対策方針のカバレージ**

### 6.3.2 セキュリティ対策方針の十分性

| 脅威 | 対策方針 |
|---|---|
| T.ACCESS.TSFDATA | 適切な権限のない TSF データへのアクセスという脅威は、以下によって低減される。<br><br>☐ O.TRUSTED_CHANNEL が、高信頼 IT システム間を通過する TOE によって管理される TSF データを含むデータに暗号保護された通信チャネルを要求することによって、<br>☐ O.DISCRETIONARY.ACCESS が、TOE に保存された TSF データを含むデータに任意アクセス制御による保護を要求することによって、<br>☐ O.SUBJECT.COM が、TSF にサブジェクト間の通信の仲介を要求することによって。 |
| T.ACCESS.USERDATA | 適切な権限のない利用者データへのアクセスという脅威は、以下によって低減される。<br><br>☐ O.TRUSTED_CHANNEL が、高信頼 IT システム間を通過する TOE によって管理される利用者データを含むデータに暗号保護された通信チャネルを要求することによって、<br>☐ O.DISCRETIONARY.ACCESS が、TOE に保存された利用者データを含むデータに任意アクセス制御による保護を要求することによって、<br>☐ O.SUBJECT.COM が、TSF にサブジェクト間の通信の仲介を要求することによって。 |
| T.ACCESS.TSFFUNC | 適切な権限のない TSF 機能へのアクセスという脅威は、以下によって低減される。<br><br>☐ O.TRUSTED_CHANNEL が､暗号保護された通信チャネルを要求し、外部エンティティからアクセス可能な TSF 機能を制限することによって、<br>☐ O.MANAGE が、正当な利用者のみに管理 TSF 機能が利用できることを要求することによって。 |
| T.ACCESS.COMM | TOE と他のリモート高信頼 IT システムとの間の信頼関係を確立する通信チャネルへのアクセスという脅威は、以下によって低減される。<br><br>☐ O.TRUSTED_CHANNEL が、TOE に自分自身とリモート高信頼 IT システムとの間の高信頼チャネルを実装し、このチャネル上で転送される利用者データ及び TSF データを開示及び検出されない変更から保護すること､及びリモート高信頼 IT システムへのなりすましを防止することによって、<br>☐ OE.REMOTE が、TOE の要求する機能を提供するシステムを、これらの機能に間違った結果を生じさせる可能性のある任意の攻撃から十分に保護することによって。 |

| 脅威 | 対策方針 |
|---|---|
| T.RESTRICT.NETTRAFFIC | ネットワーク通信を介した情報のアクセスまたは他の受信者への情報の送信が、この通信を試行する権限なしに行われるという脅威は、以下によって低減される。<br><br>☐ O.NETWORK.FLOW が TOE に、自分自身とリモートエンティティとの間の通信を、そのセキュリティ方針にしたがって仲介することを要求することによって。 |
| T.IA.MASQUERADE | 利用者データ、TSF データ、または TOE リソースへの不正なアクセスを行うために、正当なエンティティへのなりすましが行われるという脅威は、以下によって低減される。<br><br>☐ O.I&A が、正当な利用者のみに TOE が提供するものと定義された任意のアクションを許可する前に、TOE と対話するすべてのエンティティが適切に識別され認証されることを要求することによって。 |
| T.IA.USER | 識別及び認証が行われることなく、利用者データ、TSF データ、または TOE リソースへアクセスが行われるという脅威は、以下によって低減される。<br><br>☐ O.I&A が、正当な利用者のみに TOE が提供するものと定義された任意のアクションを許可する前に、TOE と対話するすべてのエンティティが適切に識別され認証されることを要求することによって。 |
| T.UNATTENDED_SESSION | 放置されたセッションを利用して保護された TSF の機能、利用者データ、または TSF データへのアクセスを行おうとする攻撃エージェントの脅威は、以下によって低減される。<br><br>☐ O.UNATTENDED_SESSION が、放置されたセッションを権限のない人物による使用から保護できる機能を要求することによって。 |

**表 3：TOE 脅威の十分性**

| セキュリティ方針 | セキュリティ対策方針 |
|---|---|
| P.ACCOUNTABILITY | 利用者に、TOE 内部のセキュリティに関連した自分のアクションに責任を持たせるという方針は、以下によって実現される。<br><br>☐ O.AUDITING が、TOE に監査機能を提供することによって、<br>☐ O.MANAGE が、この機能の管理を許可することによって。 |
| P.USER | 利用者に与えられた信頼と、利用者が実施する権限を与 |

| セキュリティ方針 | セキュリティ対策方針 |
|---|---|
| | えられたアクションとを対応付けるという方針は、以下によって実現される。<br><br>☐ O.MANAGE が、適切な権限を与えられた利用者に TSF の管理を許可することによって、<br>☐ OE.INFO_PROTECT が、利用者が自分のデータを保護するために TOE の保護メカニズムを利用するよう信頼されることを要求することによって。 |

**表 4：セキュリティ方針の十分性**

| 前提条件 | セキュリティ対策方針 |
|---|---|
| A.PHYSICAL | TOE によって保護される IT 資産の価値に対応した適切な物理的セキュリティを TOE へ提供するという、IT 環境に関する前提条件は、以下によってカバーされる。<br><br>☐ OE.INFO_PROTECT が、ネットワーク及び周辺装置の配線の承認を要求することによって、<br>☐ OE.PHYSICAL が、物理的保護を要求することによって。 |
| A.MANAGE | 1 人以上の信頼できる個人によって管理されるという、TOE セキュリティ機能に関する前提条件は、以下によってカバーされる。<br><br>☐ OE.ADMIN が、信頼できる要員が TOE を管理することを要求することによって、<br>☐ OE.INFO_PROTECT が、情報が適切な方法で保護されることを確実にすることを要員に要求することによって、<br>☐ OE.INSTALL が、セキュアな方法で、システムを構成するコンポーネントが配付され、インストールされ、そして構成されることによって TOE の提供するセキュリティメカニズムを確実に支援することを要員に要求することによって、<br>☐ OE.RECOVER が、システム障害やその他の断絶後に保護（セキュリティ）の危殆化を実現することなく確実に回復することを要員に要求することによって。 |
| A.AUTHUSER | TOE の管理する情報の少なくとも一部へアクセスするために必要な権限を有し、また良性の環境において協力的な態度で行動するという、正当な利用者に関する前提条件は、以下によってカバーされる。<br><br>☐ OE.ADMIN が、TOE の責任者が適任かつ信頼できる個人であって、TOE 及びそれに含まれる情報のセキュリティを管理できることを確実にすることによって。<br>☐ OE.INFO_PROTECT が、セキュリティ関連ファイル（監査証跡及び認証データベースなど）の DAC |

| 前提条件 | セキュリティ対策方針 |
|---|---|
| | 保護が常に正しく設定されなくてはならず、TOE の管理するデータの部分へアクセスするためには利用者が認可されていることを要求することによって。 |
| A.TRAINEDUSER | 十分に教育され、自分の利用者データに関する完全な制御権を行使することにより、セキュアな IT 環境の内部で何らかのタスク、またはタスクのグループを達成するよう信頼されているという、利用者に関する前提条件は、以下によってカバーされる。<br><br>☐ OE.ADMIN が、適任の要員が TOE を管理することを要求することによって。<br>☐ OE.INFO_PROTECT が、情報が適切な方法で保護され、利用者が自分のデータに関して管理権を行使するよう教育されることを確実にする手順を、TOE の管理者が確立し実施しなくてはならないことを要求することによって。 |
| A.DETECT | TOE のセキュリティ強制機能またはセキュリティ関連ファイルの何らかの改変または損傷は、管理ユーザによって検出されるという前提条件は、以下によってカバーされる。<br><br>☐ OE.INSTALL が、セキュアな方法で、TOE が配付され、インストールされ、そして構成されることによって TOE の提供するセキュリティメカニズムを確実に支援することを管理ユーザに要求することによって、<br>☐ OE.MAINTENANCE が、診断機能がスケジュールされた予防保全周期で毎回起動され、TOE の正しい動作を検証することを確実にすることを管理ユーザに要求することによって、<br>☐ OE.RECOVER が、システム障害やその他の断絶後に保護（セキュリティ）の危殆化を実現することなく確実に回復するための手続きまたはメカニズムあるいはその両方が提供されることを確実にすることを管理ユーザに要求することによって。 |
| A.PEER.MGT | すべてのリモート高信頼 IT システムが、同一の管理制御下にあって TOE のものと互換性のあるセキュリティ方針の制限下で動作するという前提条件は、以下によってカバーされる。<br><br>☐ OE.TRUSTED.IT.SYSTEM が、これらのリモート高信頼 IT システムは TOE と同一管理ドメイン下に置かれ、そして TOE に適用されるものと同一のルール及び方針に基づいて管理されることを要求することによって。 |
| A.PEER.FUNC | すべてのリモート高信頼 IT システムが、TSF によって用いられる機能を、この機能について定義された前提条 |

| 前提条件 | セキュリティ対策方針 |
|---|---|
| | 件と一貫して正しく実装するという前提条件は、以下によってカバーされる。<br><br>☐ OE.TRUSTED.IT.SYSTEM が、セキュリティ方針の強制をサポートするために TSF によって要求されるプロトコル及びメカニズムをリモート高信頼 IT システムが実装することを要求することによって。 |
| A.CONNECT | リモート高信頼 IT システムとの、及び TSF 自身によって保護されない TSF の物理的に分離した部分間のすべての接続は、物理的または論理的に TOE 環境中で保護されるという前提条件は、以下によってカバーされる。<br><br>☐ OE.REMOTE がリモート高信頼 IT システムに、TOE の要求する機能を提供し、またこれらの機能に間違った結果を生じさせる可能性のある任意の攻撃からの十分な保護を要求することによって、<br>☐ OE.TRUSTED.IT.SYSTEM が、TOE と同等の物理的及び論理的保護を要求することによって。 |

**表 5：前提条件の十分性**

# 7 拡張コンポーネントの定義

## 7.1 FIA_PK_EXT.1 公開鍵ベースの認証

FIA_PK_EXT.1 は、リモート IT システムの認証に用いられる公開鍵暗号方式に関連する SFR である。

### 7.1.1 コンポーネントのレベル付け

FIA_PK_EXT.1 は、[CC] のパート 2 のいかなる他のコンポーネントとも階層をなさない。

### 7.1.2 管理

鍵または証明書の管理は、FMT_MTD.1 の具体化によって対処される必要がある。

### 7.1.3 監査

FIA_PK_EXT.1 に関する監査要件は存在しない。

### 7.1.4 FIA_PK_EXT.1 公開鍵ベースの認証

| | |
|---|---|
| 階層： | なし |
| 依存性： | FMT_MTD.1 TSF データの管理 |
| FIA_PK_EXT.1.1 | TSF は、[選択：[割付：証明書フォーマット標準]、公開鍵暗号方式] を [割付：証明書管理及び証明書有効性確認標準またはその他の鍵管理／鍵検証手法] の定義により、[割付：暗号プロトコル] 接続の認証をサポートするために利用しなくてはならない（shall）。 |
| FIA_PK_EXT.1.2 | TSF は、証明書または公開鍵あるいはその両方を保存し、不正な削除及び改変から保護しなくてはならない（shall）。 |

### 7.1.5 根拠

リモート IT エンティティは、公開鍵暗号方式に基づいて認証されることが多い。この SFR は、公開鍵ベースの認証に用いられる手法と、公開鍵ベースの認証を実施する暗号プロトコルを規定する。デジタル証明書が用いられる場合には、証明書パス検証に用いられる標準も定義される。注意：公開鍵ベースの認証は、選択された暗号プロトコル中で使用される公開鍵ベースの認証の定義に適合していなくてはならない（must）。

## 7.2 FMT_SMF_RMT.1 リモート管理機能

FMT_SMF_RMT.1 は、リモート管理に関連する SFR である。

### 7.2.1 コンポーネントのレベル付け

FMT_SMF_RMT.1[CC] のパート 2 のいかなる他のコンポーネントとも階層をなさない。

### 7.2.2 管理

要件なし

### 7.2.3 監査

FMT_SMF_RMT.1 に特定の監査要件は存在しない。

### 7.2.4 FMT_SMF_RMT.1 リモート管理機能

| | |
|---|---|
| 階層： | なし |
| 依存性： | FTP_ITC.1 TSF 間高信頼チャネル |
| FMT_SMF_RMT.1.1 | TSF は、FTP_ITC.1 に言明される要件にしたがって確立される高信頼チャネルを用いてリモート IT エンティティから管理機能が実行されることも許可しなければならない（shall）。 |

### 7.2.5 根拠

高信頼チャネルを用いたリモート管理機能は、汎用オペレーティングシステムに必要とされる。この機能を用いる管理者は認証される必要があり、これはローカル利用者認証の場合と同様に有効な認証情報の提供を要求することによって、または明確に管理ユーザへ束縛された証明書によって、行われる。

# 8 セキュリティ要件

この章では、TOE に規定される要件を規定する。SFR または SAR の一部として規定できない特定のオプションを OSPP が義務付ける場合には、PP には「ST 作成者への注意」として表現される。ST 作成者は、ST の作成時及び本 PP への適合主張時にこの注記を適用しなくてはならない（must）。

「適用上の注意」と表現された注記は、SFR または SAR の理解を助けるための参考情報である。

本プロテクションプロファイルには、以下の編集操作のスタイルが適用される。

- □ 割付と選択は、ボールド体のフォントで表現される。
- □ 繰返しは、SFR の特定にサフィックスを付加して表現される。
- □ 詳細化は、ボールド及びイタリック体のフォントで表現される。

## 8.1 セキュリティ機能要件

### 8.1.1 クラス：セキュリティ監査（FAU）

#### 8.1.1.1 FAU_GEN.1 監査データの生成

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成することができなくてはならない（shall）。

a) 監査機能の開始と終了、
b) 監査のレベルが**規定されていない**すべての監査対象事象、及び
c) **監査中の事象のセットへのすべての変更、**
d) **すべての利用者認証試行、**
e) **OSPP 基本部に定義されたアクセス制御方針が適用されるオブジェクトへの、すべての拒否されたアクセス、**
f) **アクセス制御方針の対象となるオブジェクトへの明示的なアクセス権の変更、及び**
g) **FAU_GEN.1.2 の表に定義される、その他の具体的に定義された監査対象事象。**

適用上の注意： FAU_GEN.1.1 には、本 PP に適合したすべてのオペレーティングシステムが監査できなくてはならない事象の最小セットを反映するために、部分的に実施される操作が含まれている。OSPP 基本部は正当な管理者に監査されるべき事象を選択する能力を要求しているから、このセットを変更するすべてのアクティビティは監査対象であることが必要とされる。また、すべての利用者認証試行は監査対象でなくてはならないが、実際に監査される事象を認証試行の失敗、特定の種類の利用者の認証試行、特定の認証手法が用いられた際の認証試行、などに正当な管理者が制限することは許可されている。正当な管理者が、TOE が監査可能な事象の集合から実際に監査される事象を定義することを許可するルールは、FAU_SEL.1（または階層的に上位のコンポーネント）において定義されなくてはならない（must）。

オペレーティングシステムが、アクセス制御方針に列挙されたオブジェクトへのアクセス試行の拒否を監査できることも必要とされる。この要件によって、例えば大量のアクセス試行を行

う攻撃など、アクセス権の潜在的な構成ミスを検出するためのアクセス試行の拒否の分析が可能となる。

アクセス権の明示的な変更は、アクセス権変更の明示的な要求によって行われるものである。これらは、例えばトロイの木馬によって行われた場合には、必須のものとなる。

FAU_GEN.1.2 TSF は、少なくとも下記の情報を各監査記録内に記録しなくてはならない（shall）。

a) 事象の日付及び時刻、事象の種類、サブジェクトの識別情報（該当する場合）、及び事象の結果（成功または失敗）、ならびに
**b) セキュリティターゲット中に含まれるすべての管理 SFR について、管理操作を行った／行おうとした利用者の識別情報、管理操作の一部として何が管理されたかの表示及び管理ユーザが何を変更したかの表示、ならびに**
c) すべての監査事象の種類について、*以下の表*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て、

| **SFR** | **事象及び事象特有の情報** |
|---|---|
| FAU_SAR.1 | 事象 : 監査記録へのアクセスのあらゆる試行<br>• 監査記録へアクセスを試みた利用者の識別情報<br>• 成功または失敗 |
| FAU_SEL.1 | 監査されるべき事象の変更のあらゆる試行<br>• 監査されるべき事象の変更を試みた利用者の識別情報<br>• 成功または失敗<br>• 成功の場合 : 監査されるべき事象の集合への変更内容 |
| FDP_ACF.1 | 事象 : SFP によって保護されるオブジェクトへのアクセスのあらゆる試行<br>• SFP によって保護されるオブジェクトへのアクセスを試みた利用者の識別情報。注意 : 利用者の代理として動作していないサブジェクトによって試みられた操作の場合には、サブジェクトの識別情報<br>• 利用者がアクセスを試みたオブジェクトの識別情報<br>• 試みられた操作<br>• 成功または失敗 |
| FDP_IFF.1 | 事象 : 情報フローの拒否<br>• ネットワークインタフェースの識別情報<br>• 情報フローが拒否された理由 |
| FIA_AFL.1 | 事象 : 連続した認証試行失敗の回数の制限超過 |

| SFR | 事象及び事象特有の情報 |
|---|---|
| | • 制限を超過した利用者の識別情報 |
| FIA_UAU.1(HU) | 事象：利用者の認証が成功したことの検証<br>• 利用者の識別情報<br>• 利用者の認証が成功したことを示す表示<br>認証が TOE によって行われる場合には、失敗した認証試行の事象も監査対象とする必要がある。<br>• 提供された利用者の識別情報<br>• 認証が失敗したことを示す表示 |
| FTA_SSL.1 | セッションのロックを解除するための再認証試行<br>• 利用者の識別情報<br>• 再認証の成功または失敗 |
| FTA_SSL.2 | セッションのロックを解除するための再認証試行<br>• 利用者の識別情報<br>• 再認証の成功または失敗 |
| FTP_ITC.1 | 事象：高信頼チャネルの初期化<br>• 通信の相手方の識別情報<br>• チャネルの確立に用いられたプロトコル<br>• チャネル設定の成功または失敗 |

**表 6：監査対象事象の最小集合と、事象特有の情報**

ST 作成者への注意： 規定された監査のレベルは OSPP 基本部に加えて、ST が適合を主張するすべての OSPP 拡張パッケージに定義されたすべての SFR へ適用される。

適用上の注意： 上記 FAU_GEN.1.2 に定義された表は、本プロテクションプロファイルに適合するオペレーティングシステムが監査できなくてはならない事象の最小セットを、時刻及び日付、事象の種類といった一般的な情報に加えて監査記録に含まれる必要のある最小限の情報とともに定義している。事象特有の情報によって、「サブジェクトの識別情報」や「事象の結果」への要件が詳細化される場合が多い。例えば、表のある項目で事象特有の情報として「利用者の識別情報」が規定されている場合、この情報に加えてサブジェクトの識別情報も記録する必要はない。

適用上の注意： サブジェクトの識別情報が利用者・サブジェクト間の束縛プロセスによって確立される場合には、サブジェクトの識別情報は利用者の識別情報と同一かもしれない。この場合、監査記録には 1 つの識別情報のみが含まれる必要がある。この目的は、事象から事象を引き起こした利用者を追跡できるようにするためである。これは、事象が発生した際、サブジェクトの識別情報からサブジェクトが束縛されている利用者を特定することが許

可されない場合には、可能ではないかもしれない。したがって、FAU_GEN.2 をサポートするために、記録されるべき情報として利用者の識別情報が追加されている。

適用上の注意： 監査対象事象と共に記録されるべき結果は、TOE の実装に応じて、バイナリ（成功または失敗）か、あるいはその事象から生じる値のどちらでもよい。例えば、アクセス制御判定機能は、アクセス制御判定の結果に関する情報を監査証跡と共に保存しなくてはならない（shall）。TOE は、単にアクセスが許可されたか拒否されたかよりも多くの判定結果を実装することができ、その場合にはこれらの結果のすべてがアクセス制御チェック事象の結果として記録されなくてはならない（shall）。

適用上の注意： 例えば追加管理アクティビティなどの追加 SFR を含むセキュリティターゲットは、そのような追加 SFR に対する監査要件を、セキュリティターゲット中に上記の表を拡張して規定する必要がある。管理ユーザによって開始されたすべての管理アクティビティに関する一般的なルールとして、事象特有の情報にはその管理操作を行った／行おうとした利用者の識別情報、管理操作の一部として何が管理されたかの表示及び管理ユーザが何を変更したかの表示が含まれる必要がある。管理ユーザが単に管理対象項目の状態を問い合わせるだけの操作は、監査対象である必要はない。

#### 8.1.1.2 FAU_GEN.2 利用者識別情報の関連付け

FAU_GEN.2.1 識別済み利用者の行動に起因する監査事象については、TSF は各監査対象事象をその事象を発生させた利用者の識別情報に関連付けることができなくてはならない（shall）。

#### 8.1.1.3 FAU_SAR.1 監査レビュー

FAU_SAR.1.1 TSF は、**[割付：正当な識別済みの役割、または以下のルールを満たす利用者 [割付:利用者にそのアクティビティの実行が許可される場合を定義するルール]]** へ、監査記録から [割付：監査情報のリスト] を読み出す機能を提供しなくてはならない（shall）。

FAU_SAR.1.2 TSF は、利用者が情報を解釈するのに適した形式で監査記録を提供しなくてはならない（shall）。

ST 作成者への注意： 正当な利用者は、人間の利用者であっても、他の高信頼 IT システムであってもよい。ST 作成者は、利用者に監査証跡情報の読み取りを許可するために満たされなくてはならない条件を定義しなくてはならない（must）。本プロテクションプロファイルに適合するオペレーティングシステムは、監査記録から異なる情報を読み出すために満たす必要のある条件とともに、異なる種類の利用者を定義してもよい。定義済みの人間の利用者に特定の種類の監査記録または監査記録の特定のフィールドの読み取りを許可する一方で、特定の外部システムにすべての監査記録のダウンロードを許可するオペレーティングシステムは、この要件に適合している。

ST 作成者への注意： ST 作成者は、監査記録から情報を読み出すために必要とされる正確な権限を定義する必要がある。これは、この能力が割り当

てられた特定の役割であってもよいし、あるいは利用者に割り当てられなくてはならない 1 つ以上の特権であってもよい。

#### 8.1.1.4 FAU_SAR.2 制約された監査レビュー

FAU_SAR.2.1 TSF は、明示的な読み取りアクセスが与えられている利用者を除いて、すべての利用者に監査記録への読み取りアクセスを禁止しなくてはならない（shall）。

#### 8.1.1.5 FAU_SEL.1 選択的監査

FAU_SEL.1.1 TSF は、以下の属性に基づいて、監査対象事象の集合から監査されるべき事象の集合を選択することができなくてはならない（shall）。

a) **監査事象の種類、**
b) **サブジェクトまたは利用者の識別情報、**
c) **監査事象の結果（成功または失敗）、**
d) **名前付きオブジェクトの識別情報、**
e) **[割付：監査の選択対象となる追加属性のリスト]**。

#### 8.1.1.6 FAU_STG.1 保護された監査証跡ストレージ

FAU_STG.1.1 TSF は、監査証跡内に保存された監査記録を、不正な削除から保護しなくてはならない（shall）。

FAU_STG.1.2 TSF は、監査証跡内の監査記録への不正な改変を [選択、1 つを選択：防止、検出] できなくてはならない（shall）。

適用上の注意： TOE はローカルに監査記録を保存してもよいし、その監査記録を保存しさらに処理するためリモート高信頼 IT システムに渡してもよい。ただしこの場合であっても、TOE は通常、監査記録の一部をバッファするため、またはリモート監査サーバが利用できない場合に時間を稼ぐため、（たぶん揮発性の）キャッシュとして何らかの種類のローカルな監査証跡を必要とするだろう。そのようなローカルな監査証跡は、この SFR に記述されているように保護されなくてはならない（must）。

#### 8.1.1.7 FAU_STG.3 監査データの損失が生じたおそれのある場合のアクション

FAU_STG.3.1 TSF は、監査証跡が [割付：事前に定義された制限] を越えた場合、*または監査記録の損失が生じるかもしれない以下のいずれか [割付：条件のリスト] が検出された場合*、[割付：監査データの損失が生じたおそれのある場合に取るべきアクション] を行わなくてはならない（shall）。

ST 作成者への注意： 監査データの損失につながる可能性のある条件は多数存在する可能性があり、定義済みの閾値に達することはその中のひとつにすぎない。監査データが自動的に別の高信頼 IT システムへ転送される場合、このシステムの通信リンクのいかなる問題も監査データの損失につながるおそれがある。FAU_STG.3.1 は、TSF が検出可能な監査データの損失のおそれのある条件を列挙し、そのような条件が検出された際の TSF の反応を記述することを ST 作成者に要求している。この反応が検出された条件によって異なる場合、ST 作成者は FAU_STG.3.1 の複数回の繰返しを用

いて異なる反応を記述し、それらと TSF によって監査データの損失のおそれが検出される条件とを関連付けなくてはならない（shall）。

ST 作成者への注意： この SFR は、TSF によって保存される監査証跡のみに明示的に限定されてはいない。TOE がリモート高信頼 IT システムの監査証跡を保存する場合、監査証跡ストレージが特定の閾値に達した場合、TOE は TOE へ監査データを送付しているリモート高信頼 IT システムへ通知を送り、この状態に関して知らせることを確実にしなくてはならない（must）。

#### 8.1.1.8 FAU_STG.4 監査データの損失の防止

FAU_STG.4.1 TSF は、監査証跡に空きがなくなった場合、[選択、1 つを選択：「監査事象を無視」、「**[割付：正当な識別済みの役割、または以下のルールを満たす利用者 [割付：利用者にそのアクティビティの実行が許可される場合を定義するルール]** によって行われるものを除いて監査事象を防止」、保存された監査記録で最も古いものを上書き」] し、[割付：監査格納失敗の場合に取られるべきその他のアクション] を行わなくてはならない（shall）。

ST 作成者への注意： この SFR は、TSF によって保存される監査証跡のみに明示的に限定されてはいない。TOE がリモート高信頼 IT システムの監査証跡を保存する場合、監査証跡ストレージに空きがなくなった場合、TOE は TOE へ監査データを送付しているるリモート高信頼 IT システムへ通知を送り、この状態に関して知らせることを確実にしなくてはならない（must）。

### 8.1.2 クラス：利用者データ保護 (FDP)

#### 8.1.2.1 FDP_ACC.1 サブセットアクセス制御

FDP_ACC.1.1 TSF は、以下に関して [割付：アクセス制御 SFP] を強制しなくてはなない（shall）。

a) **[SFP によってカバーされる、利用者の種類、またはサブジェクトの種類、あるいはその両方のリスト]、**
b) **[割付：SFP によってカバーされる名前付きオブジェクトの種類のリスト]、**
c) **[割付：SFP によってカバーされる操作のリスト]。**

ST 作成者への注意： オペレーティングシステムは複数のアクセス制御 SFP を実装するかもしれないので、ここでの意図は FDP_ACC.1、FDP_ACF.1 の複数の具体化及びこれらに関連する管理 SFR が、SFP の対象となる利用者／サブジェクト、オブジェクトの種類、及び操作の面から各アクセス制御 SFP を記述できることであり、また特定の利用者／サブジェクトが SFP の対象となる特定のオブジェクトに関する特定の操作を行うことが許可されているかどうかを判定するために遵守されるルールを、関連する FDP_ACF.1 の具体化が正確に記述できることである。

ST 作成者への注意： オブジェクトに関する操作のリストは、新たなオブジェクトの作成、オブジェクトの破壊、オブジェクトへのすべての種類のアクセス、そしてオブジェクトと関連付けられ保存されている

TSF データに関する操作（例えば、オブジェクト名、オブジェクトと関連付けられたアクセス制御リスト、その他のオブジェクトのセキュリティ属性）をカバーする必要がある。これらの操作の一部が TSF データの管理に関連する SFR でカバーされている場合、これらの操作が記述されている場所を ST 読者が特定できるよう、ST 作成者はそれらの SFR への参照を含めなくてはならない（shall）。

#### 8.1.2.2 FDP_ACF.1 セキュリティ属性に基づいたアクセス制御

FDP_ACF.1.1 TSF は、以下に基づいてオブジェクトへ [割付：アクセス制御 SFP] を強制しなくてはならない（shall）：[割付：示された SFP の下で制御されるサブジェクト*または利用者*及びオブジェクトのリスト、そしてそのそれぞれに対して、SFP に関連したセキュリティ属性、または SFP に関連したセキュリティ属性の名前付きグループ]。

FDP_ACF.1.2 TSF は、以下のルールを強制して、制御されるサブジェクト及び制御されるオブジェクト間での操作が許可されるかどうかを判定しなくてはならない（shall）：[割付：制御されるサブジェクト、*または利用者*、*あるいはその両方*、及び制御されるオブジェクト間でのアクセスを支配するルールであって、制御されるオブジェクトに関する制御された操作を用い、*単一のサブジェクトまたは利用者の粒度にまで細かくアクセスを許可することができるもの*]。

FDP_ACF.1.3 TSF は、以下の追加ルールに基づいて、オブジェクトへのサブジェクトのアクセスを明示的に認可しなくてはならない（shall）：[割付：セキュリティ属性*またはその他の TSF データ*に基づくルールであって、オブジェクトへのサブジェクトのアクセスを明示的に認可するもの]。

FDP_ACF.1.4 TSF は、以下の追加ルールに基づいて、オブジェクトへのサブジェクトのアクセスを明示的に拒否しなくてはならない（shall）：[割付：セキュリティ属性*またはその他の TSF データ*に基づくルールであって、オブジェクトへのサブジェクトのアクセスを明示的に拒否するもの]。

適用上の注意： 永続的ストレージオブジェクト（例えばファイル）に対するアクセス制御 SFP であって、単一の利用者／サブジェクトの粒度にまで細かくアクセス権の仕様を可能にするものが、少なくとも 1 つ存在しなくてはならない（must）。個別の利用者に対してアクセス権を規定できるアクセス制御リストであって、そのアクセス制御リストのエントリの一部ではない利用者またはグループのアクセスをデフォルトで拒否するものは、この条件を満たす実装例である。グループへアクセスを割り当てたり、それ自身が独立して利用者／サブジェクトまたはグループあるいはその両方に割り当て可能な特権へアクセスを束縛したりする追加的な機能は、単一の利用者のレベルにまで細かくアクセスを割り当てられるという条件に違反してはいない。

ST 作成者への注意： アクセス制御方針は非常に複雑となる可能性があるため、オペレーティングシステムは多数の「例外」、例えば一部のアクセス

権を特定の特権へ束縛することを実装しているかもしれない。ルールセット全体があまりに複雑となることを避けるため、ST 作成者はこれらの例外をすべては記載しないと判断するかもしれない。これは、それらの例外が評価された構成には関連しないように TOE を構成し管理する方法を、評価された構成のガイダンスが明確に記述していることを条件として、許可される。例えば、特定の特権を持つ利用者へ自動的に与えられるアクセス権は、評価された構成で動作している際にはこの特権が利用者へ割り当てられてはならないとそのガイダンスが明確に言明していることを条件として、アクセス制御ルールの記述において無視してもよい。

ST 作成者への注意： ST は、FDP_ACC.1 の具体化のそれぞれについて、アクセスを判定するルールに用いられる関連したセキュリティ属性とともにアクセスそれ自身を判定するルールを記述する FDP_ACF.1 によって、FDP_ACF.1 を繰り返さなくてはならない。提供される記述は、読者／評価者がアクセス判定を行う際に用いられる TSF データを特定するとともに、アクセス判定プロセスのモデルを導出できるものでなくてはならない（must）。アクセス判定ルールに用いられる TSF データの特定が必要とされるのは、攻撃者がこの判定プロセスに用いられる TSF に影響を及ぼすことによってアクセス制御判定に影響を及ぼすことが可能な方法を特定するため、この TSF データがどのように導出され管理されるかを評価者が判定する必要があるからである。

#### 8.1.2.3 FDP_IFC.1 サブセット情報フロー制御

FDP_IFC.1.1 TSF は、以下に基づいた**ネットワーク情報フロー制御方針**を強制しなくてはならない（shall）。

a) **発信側エンティティ**：
   i. **未認証の外部 IT エンティティであって、ネットワークデータを TOE のネットワークインタフェースへ送信するもの、**
   ii. **TOE 内部のサブジェクトであって、ネットワークデータを未認証の外部エンティティへ TOE のネットワークインタフェースを介して送信するもの、**

b) **情報**：
   i. **外部 IT エンティティから TOE が受信したネットワークデータ、**
   ii. **TOE 上で実行されているサブジェクトによって TOE へ提供されたネットワークデータであって、TOE の制御するネットワークインタフェースを介して外部 IT エンティティへ送信されることを意図しているもの、**
   iii. **[選択：[割付：SFP の対象となるその他の情報]、なし]、**

c) **操作**：
   i. **未認証の外部 IT エンティティからのネットワークデータの受信、**
   ii. **TOE 内部のサブジェクトによる、未認証の外部 IT エンティティへのネットワークデータの送信。**

適用上の注意： この SFR は FDP_IFF.1 とともに、着信及び発信の両方のネットワークパケットについて、基本的なパケットフィルタリングルールを定義する機能を実装することを TOE に要求している。この要件は最低限、管理者がパケットの検査ルールを定義でき、その結果としてパケットが意図された受信者への送信を許可されるか、それとも破棄されるかの判定が行えるような、TCP/IP、VLAN あるいはその両方のフィルタリング機能を有することである。

適用上の注意： OSPP では、インターネットプロトコルのバージョンを明示的には規定していない。これは、評価された構成において利用可能なインターネットプロトコルのバージョンが、この SFR でカバーされなくてはならないことを意味している。

#### 8.1.2.4 FDP_IFF.1 単純なセキュリティ属性

FDP_IFF.1.1 TSF は、以下の種類のサブジェクト及び情報セキュリティ属性に基づいて、**ネットワーク情報フロー制御方針**を強制しなくてはならない（shall）。

**オブジェクトのセキュリティ属性：それを介して外部 IT エンティティからのネットワークデータが TOE に入る、または送信されることが意図されている論理または物理ネットワークインタフェース、**

**[選択（a または b あるいはその両方）**：

a) **TCP/IP 情報セキュリティ属性**：
   i. **送信元及び送信先 IP アドレス、**
   ii. **送信元及び送信先 TCP ポート番号、**
   iii. **送信元及び送信先 UDP ポート番号、**
   iv. **IP、TCP、UDP、[選択：ICMP、[割付：その他のプロトコル]] のネットワークプロトコル、**
   v. **[選択：[選択：SYN、ACK、[割付：その他の TCP ヘッダフラグ]] の TCP ヘッダフラグ、[割付：その他のネットワークデータ情報セキュリティ属性]、その他のセキュリティ属性なし]、**

b) **レイヤ 2 セキュリティ属性**：
   i. **MAC アドレス、**
   ii. **VLAN 識別子、**
   **iii.** **[選択：[割付：その他のネットワークデータ情報セキュリティ属性]、その他のセキュリティ属性なし]**

**]**。

適用上の注意： 本プロテクションプロファイルに適合する TOE は、異なるネットワークインタフェースに異なるルールセットを適用できる必要はないが、この機能を提供する場合にはデータが受信されたインタフェースまたはデータの送信が意図されたインタフェースは、適用される必要のある正しいルールの集合を選択するために使われるセキュリティ属性として TOE にみなされる必要がある。

適用上の注意： FDP_IFF.1.3 に規定されるネットワークフロー制御の最小要件は、ネットワーク情報フロー制御方針の目的、すなわちここに規定されたセキュリティ属性を用いてネットワークデータを識

別し、少なくとも特定されたネットワークデータを破棄するか、変更されずに TOE を通過させることを定義している。

FDP_IFF.1.2 TSF は、制御されるサブジェクトと制御される情報との間の制御される操作を介した情報フローを、下記のルールが成り立つならば許可しなければならない（shall）。

**外部 IT エンティティからのネットワークデータの受信と、TOE 内部のサブジェクトによる外部 IT エンティティへのネットワークデータの送信の両方について**：

a) **FDP_IFF.1.3 に定義されるセキュリティ属性に応じて定義されたルールの集合が、ネットワークデータが破棄されることを定めている場合、ネットワークデータは TOE によって意図された受信者へ配送されてはならない（shall not）。**
**b) FDP_IFF.1.3 に定義されるセキュリティ属性に応じて定義されたルールの集合が、ネットワークデータが未変更のまま配送されることを定めている場合、ネットワークデータは TOE によって意図された受信者へ未変更のまま配送されなくてはならない（shall）。**
c) **FDP_IFF.1.3 に定義されるセキュリティ属性に応じて定義されたルールのセットが、ネットワークデータの破棄または意図された受信者へのデータの未変更のままの配送以外の別のアクションを定めている場合、TOE はこのアクションを行わなくてはならない（shall）。**

適用上の注意： 外部 IT エンティティから受信されたネットワークデータについては、「意図された受信者」はそのネットワークデータがさらに処理されるために配信されることになっている TOE 内部のプロセスである。これは、利用者の代理として動作しているサブジェクトやその他のサブジェクト（例えばネットワークデーモン）、あるいは TSF の専用部分であるかもしれない。

TOE 内部で生成されたネットワークデータであってリモート IT エンティティへの送付が意図されているものに関しては、「意図された受信者」はフィルタリングルールによって処理される前にネットワークデータ中に指定されていた IP アドレスまたは MAC アドレスのいずれかによって特定されるリモート IT エンティティである。

FDP_IFF.1.3 TSF は、**ルールが発火する場合の識別及びルールが発火した際に取られるべきアクションから構成される以下のルールの遵守**を強制しなくてはならない（shall）：**以下の概念の 1 以上を用いたネットワークデータの識別**：

a) **以下のセキュリティ属性に基づいてマッチする情報セキュリティ属性 [割付：マッチングルールに用いられるセキュリティ属性のリスト]、**
b) **[選択：[割付：TCP コネクションの状態に基づくマッチングルール]、[割付：時間ベースのマッチングルール]、[割付：統計分析マッチングルール]]、[選択：その他のマッチング概念なし、[割付：その他のマッチング概念]]、**

**以下のアクションの 1 つ以上を行う**：

a) **[選択：それ以上の処理を行わずに、送信者へ通知を送信して]、ネットワークデータを破棄する、**
b) **意図された受信者へ TOE によって未変更のままネットワークデータを配送させる、**
c) **[選択：その他のアクションを行わない、[ルールが発火した際に行われるその他のアクション]]**。

ST 作成者への注意： FDP_IFF.1.3 a) は、単純なマッチング（すなわち、セキュリティ属性の値の単純な比較によってネットワークパケットの通過が許可されるか許可されないかが判断される）のルール中に用いられるネットワークプロトコルにおけるセキュリティ属性の定義を、ST 作成者に要求している。FDP_IFF.1.3 b) は、TCP コネクションの状態、時間、または何らかの統計的特性（例えば、特定の送信元からのあまりに多数の同種のネットワークパケット）のいずれかに基づいて、少なくとも 1 つのより複雑なルールのセットを TOE が持つことを要求している。ST 作成者は FDP_IFF.1.3 に、これらの概念の少なくとも 1 つのルールを規定して、どのマッチング概念が使われるかを説明することができ、またネットワークパケットが通過を許可されるかどうかの判定に用いられる TOE によって実装されるその他のマッチング概念をも規定しなくてはならない（shall）。ルールの完全なセットを規定することは、ネットワークインタフェースにおけるテストの期待される結果を判定し、これらを実際に得られた結果と比較する上で重要である。ST 作成者は次に、ルールが「発火」した際に取られる可能性のあるアクションを規定する必要があり、ここでは少なくともネットワークデータの破棄と、未変更のネットワークデータの通過ができなくてはならない（must）。

ST 作成者への注意： 規定されてもよい別のアクションの一例として、おそらくは破棄されるネットワークデータを含めて、アクションのロギングを行うことが挙げられる。これがアクションとして定義される場合、FAU_GEN.1 中の監査されるべき事象のリストは拡張される必要がある。このネットワークフィルタリング関連のロギングが他の監査対象事象の監査メカニズムを使って行われない場合には、ST 作成者は SFR に関連する監査の全体セットが、ネットワークフィルタリング関連の監査機能についてどのように TOE によって対処されるかを記述する必要がある。

FDP_IFF.1.4 TSF は、以下のルールに基づいて情報フローを明示的に認可しなくてはならない（shall）: [割付：ルール、セキュリティ属性に基づいて、情報フローを明示的に認可するルール]。

FDP_IFF.1.5 TSF は、以下のルールに基づいて情報フローを明示的に拒否しなくてはならない（shall）: [割付：ルール、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ルール]。

適用上の注意： OSPP は、TCP/IP ネットワークデータセキュリティ属性のインターネットプロトコルのバージョンを明確には規定していない。これは、評価された構成において利用可能なインターネットプロトコルのバージョンが、この SFR でカバーされなくてはなら

ないことを意味している。

#### 8.1.2.5 FDP_RIP.2 完全な残存情報の保護

FDP_RIP.2.1 TSF は、すべてのオブジェクト、*サブジェクト、またはサブジェクト／オブジェクト関連の TSF データ* [選択：へのリソースの割り当て、からのリソースの割り当て解除] の際に、*そのリソースが別のサブジェクトまたは利用者へ割り当てられるか利用できるようにされる前に*、リソースのあらゆる以前の情報コンテンツが利用できなくなることを確実にしなくてはならない（shall）。

適用上の注意： この SFR の目的は、信頼できないサブジェクトまたは利用者が TSF または利用者データを、別のサブジェクトへ以前割り当てられていたリソースから確実に取得できなくすることである。これにはもちろん、別の利用者に属するファイルに以前割り当てられていたディスクスペース、別の利用者の代理として動作するサブジェクトへ以前割り当てられていたメインメモリが含まれるが、別の利用者の代理として動作するサブジェクトに属するプロセスからのコンテクストスイッチ後のレジスタや、開示に対する保護を必要とする情報の保存に以前使われていた TSF 内部メモリも含まれる。

同一のサブジェクト／利用者または同一のオブジェクトへ再割り当てされたリソースには再利用の準備が必要ないことに注意されたい。これらに含まれている情報は、それを開放する前にサブジェクトまたは利用者から何らかの形でアクセス可能であったためである。

### 8.1.3 クラス：識別及び認証 (FIA)

TOE は、人間の利用者（管理者及び信頼されない利用者）と動作中の IT エンティティとで、異なる種類の識別と認証方式をサポートしなくてはならない（must）。通常 I&A プロセスの一部とみなされる可能性のあるこの要件の一部、特に FTP_ITC.1 TSF 間高信頼チャネルに規定される暗号プロトコルに関連するものは、この PP の別のセクションに規定されている。したがって、マシンレベルでのみ認証が行われる IT エンティティの認証については、X.509v3 証明書を用いる暗号プロトコルを利用して認証が行われる。これは、理解しやすさのために IT エンティティに関する I&A 要件を特定されたプロトコルと共にグループ化するためと、その対応する RFC を一緒にグループ化するために行われた（FPT_ITC.1）。

このセクションの要件は、適合 TOE の I&A 機能の以下の別個の側面をカバーする。

- ☐ 人間の利用者向けの I&A。TOE は、ローカルに TOE と接続する（例えばコンソール）利用者によって、あるいは利用者がリモートから TOE へ接続する（例えば、IT エンティティを介した高信頼チャネル）際に使われるパスワードメカニズムを提供しなくてはならない（must）。すべての利用者は、ST 作成者が FIA_UAU.5 に定義する少なくとも 1 つの利用者認証メカニズムを用いて認証されることが要求される。
- ☐ 資格情報。ここ、及び PP の別のセクションに規定されるプロトコル（FTP_ITC.1）及びメカニズム（FIA_UAU.5）は、I&A プロセスにおいて用いられる異なる資格情報に依存している。 利用者については FIA_UAU.5 に列挙されるパスワードまたはその他のオプションの利用者認証メカニズム、そして高信頼チャネルと FTP_ITC.1 に列挙されるプロトコル（IPsec、TLS、SSH）の 1 つを用いて TOE へ接続する IT エンティティについては証明書である。

#### 8.1.3.1 FIA_AFL.1 認証失敗時の取り扱い

FIA_AFL.1.1 TSF は、*パスワードに基づいた認証手法 [割付：その他の認証手法またはなし]* の認証試行の失敗が、**許容される値の範囲内の管理者によって構成可能な正の整数回** [割付：認証事象のリスト] に関連して発生したことを検出できなくてはならない（shall）。

FIA_AFL.1.2 定義された回数の認証試行の失敗が**満たされた**際、TSF は：[割付：アクションのリスト] を行わなくてはならない（shall）。

適用上の注意： TOE は、異なる種類の利用者に対して異なる認証手法を用いることができ、また認証手法または利用者の種類あるいはその両方に基づいて認証の失敗をどう取り扱うか異なるルールを持つことができる。リモートシステムの認証失敗は通常、人間の利用者の認証試行とは異なる取り扱いをされる。人間の利用者であっても、認証失敗への反応は、利用者 ID／パスワードによる認証と、スマートカードやデジタル証明書による認証とでは異なってもよい。

適用上の注意： 認証試行の不成功は連続している必要はないが、認証事象と関連している必要がある。そのような認証事象は、所与の端末での最後のセッション確立の成功からカウントすることができるだろう。

適用上の注意： アクションのリストは TOE 特有であってもよいが、それに引き続く認証試行によって認証データの取り得る空間の準総当たり検索に基づく攻撃が防止されることを一連のアクションが確実にする必要がある。例えば、不成功の追加認証試行の回数を 1 日につき 1 回に制限するアクションは受容可能であるが、不成功の認証試行のオプションの監査を強制的な監査に変更するだけのアクションは受容できないであろう。

適用上の注意： FIA_AFL.1.1 における最初の割付は単純明快であり、何らかの形式の失敗時の処理が適用される、利用可能な認証手法を列挙することを ST 作成者へ単に要求している。2 番目の割付は、認証試行の失敗が計測される方法に関するものであり、認証手法によって異なるかもしれない。FIA_AFL.1.2 における選択及び割付にも、同じことが言え、認証手法に基づいて異なるアクションが取られるかもしれない。例えば、コンソールからパスワードをローカルに入力する利用者については 3 回失敗するとアカウントがロックされるが、リモートからパスワードを入力する利用者は 3 回失敗してもリモートセッションが終了するだけかもしれない。取られるアクションは、信頼できない利用者と管理ユーザとで異なるかもしれない。これらすべての例は受容可能であり、重要なことは、どの認証手法がカバーされるか、どのような状況下でアクションが行われることになるか、そして行われるアクションは何か、ということに関して要件が明確になっていることである。

#### 8.1.3.2 FIA_ATD.1 利用者属性の定義

FIA_ATD.1.1 TSF は、個別の*人間の*利用者に属するセキュリティ属性の下記のリストを維持管理しなくてはならない（shall）。

a) **利用者識別子**、
b) **グループのメンバシップ**、
c) **利用者のパスワード**、
d) **セキュリティ役割**、
e) **[割付：その他の利用者セキュリティ属性]**。

ST 作成者への注意： 上に列挙された利用者セキュリティ属性は、TOE 環境におけるサポート高信頼システムが利用できない場合であっても、TOE がその SFR を強制できるように TOE それ自身によって維持管理される必要があることに注意されたい。これは、他の高信頼 IT システムのサポートが利用できる環境で動作する TOE が、そのようなサポートを利用することを禁止するものではない。

TOE がリモート高信頼 IT システムによる利用者属性の維持管理を許可し、TOE はバックアップのため（例えば、リモート高信頼 IT システムへの接続が切断された場合に備えて）、またはリモート高信頼 IT システムを補完するためにローカルデータストアを維持管理している場合、ST 作成者はこの SFR を、1 つの繰り返しは TSF によって維持管理されるセキュリティ属性に適用されるもの、もう 1 つはリモート高信頼 IT システムによって維持管理されるセキュリティ属性に適用されるものとして、どのセキュリティ属性がどこに保持されるのかを明確に表明して、繰り返さなくてはならない（shall）。

#### 8.1.3.3 FIA_UAU.1(RITE) 認証のタイミング

FIA_UAU.1.1 TSF は、リモート IT エンティティの代理として

a) **ネットワーク情報フロー制御の対象となる情報フロー（リモート IT エンティティへの）**、

b) **[割付：その他の TSF 仲介アクション]**

が、リモート IT エンティティが認証される前に実行されることを許可しなければならない（shall）。

FIA_UAU.1.2 TSF は、そのリモート IT エンティティの代理としてあらゆるその他の TSF 仲介アクションが許可される前に、それぞれのリモートエンティティの認証成功を要求しなくてはならない（shall）。

適用上の注意： このエレメントは、リモート IT エンティティによって送信され、TOE によって処理されるネットワークトラフィックに適用される。リモート IT エンティティによって送信されるネットワークトラフィックの一部は、その後リモート IT エンティティを認証するために使われる通信チャネルを設定するために用いられる。FTP_ITC.1.3 エレメントは、リモート IT エンティティが認証されていることを必要とする条件が何か（高信頼チャネルを用いて行われるアクション）を ST 作成者が規定する場所である。また、リモート IT エンティティは FDP_IF*コンポーネントに記述されるネットワーク情報フロー制御方針によって許可されるような、認証を必要としないトラフィックを送信してもよい。これらの場合の両方が、FIA_UAU.1.1 エレメントの「a」の部分でカバーされている。ST 中に規定されていることによって、

FDP_IF*要件によってカバーされない、リモート IT エンティティに関する別のアクションを TOE が取るかもしれない。このような場合には、ST 作成者は割付を使ってこれらの機能を規定する。

#### 8.1.3.4 FIA_UAU.1 (HU) 認証のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者の代理として [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（shall）。

FIA_UAU.1.2 TSF は、その利用者の代理としてあらゆるその他の TFS 仲介アクションが許可される前に、それぞれの利用者の認証成功を要求しなくてはならない（shall）。

#### 8.1.3.5 FIA_UAU.5 複数の認証メカニズム

FIA_UAU.5.1 TSF は、以**下の認証メカニズム**を提供して、

a) **利用者名とパスワードに基づいた認証（人間の利用者について）、**
b) **[選択：[割付：その他の認証メカニズムのリスト]、なし]**

利用者認証をサポートしなくてはならない（shall）。

FIA_UAU.5.2 TSF は、いかなる利用者の主張する識別情報も**以下のルール**にしたがって認証しなくてはならない（shall）。

a) **人間の利用者について FIA_UAU.5.1 b に定義される別の認証手法が選択されている場合を除き、利用者名とパスワードに基づいた認証は、TOE による要求により、デフォルトで TSF によって保存される資格情報を用いて実施される。**
b) **パスワードが失効した利用者は [選択：失効したパスワードを正しく入力した後に新たなパスワードの作成が要求される、管理者によってパスワードがリセットされるまでロックアウトされる]。**
c) **[割付：複数の認証メカニズムが認証を提供する方法と、それがどの認証方針に適用されるかを説明したその他のルール]。**

ST 作成者への注意： a) 項は、TOE が利用者名とパスワードに基づく完全な自己充足した識別と認証メカニズムを、OSPP 基本部によって定義される識別と認証メカニズムをサポートするローカルに保存された資格情報を用いて提供することを要求している。それでもなお、ST 作成者はリモートの資格情報ストアを利用する可能性のある追加的な利用者名／パスワードに基づく認証メカニズムを規定することが許可される。そのような場合、ST 作成者は 2 つ（以上）の利用者名／パスワードに基づく認証メカニズム間の関係、例えば優先度の仕様などを特定しなくてはならない（must）。一般的には、複数の認証手法が同一の資格情報について規定された場合、ST 作成者はそれらの間の関係を特定しなくてはならない（must）。

ST 作成者への注意： 認証のルールの何らかの側面が管理可能である場合、ST 作成者

は FMT_MTD.1 の繰り返しを規定してこの管理の側面をカバーしなくてはならない（shall）。

#### 8.1.3.6 FIA_UAU.7 保護された認証フィードバック

FIA_UAU.7.1 TSF は、認証が行われている間に利用者へ**あいまいなフィードバック**のみを提供しなくてはならない（shall）。

適用上の注意： 「フィードバックを与えない」ことは、「あいまいなフィードバック」を与える特定の（より強い）手法とみなされることに注意されたい。

#### 8.1.3.7 FIA_UID.1 識別のタイミング

FIA_UID.1.1 TSF は、利用者が識別される前に利用者の代理として [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（shall）。

FIA_UID.1.2 TSF は、その利用者の代理としてあらゆるその他の TFS 仲介アクションが許可される前に、それぞれの利用者の識別成功を要求しなくてはならない（shall）。

#### 8.1.3.8 FIA_USB.1 利用者・サブジェクト間の束縛

FIA_USB.1.1 TSF は、その*人間の*利用者の代理として動作するサブジェクトに、以下のセキュリティ属性を関連付けなくてはならない（shall）。

a) **利用者の識別情報、**
b) **[割付：アクセス制御方針を強制するため、管理方針を強制するため、または監査要件を満たすために用いられるセキュリティ属性のリスト]**。

適用上の注意： SFR FIA_USB.1 全体を通して、「利用者のセキュリティ属性」という用語が「セキュリティ属性」に詳細化されている。オペレーティングシステムは、サブジェクトが束縛されている利用者のセキュリティ属性から導出されたものではないセキュリティ属性を、サブジェクトへ割り当てるかもしれないからである。

適用上の注意： 役割やグループ、そして特権もまた、それらがセキュリティターゲット中で言及される何らかの SFR を強制するために使われる限り、サブジェクトへ割り当てられる必要がある。TOE は、利用者に割り当て可能な一連の特権として役割を定義することを許可してもよいが、利用者・サブジェクト間の束縛の間に TOE はこれらの役割をその役割を定義する特権へと分解し、別個の特権を割り当てるかもしれない。この場合、「役割」それ自体はサブジェクトが実行中には可視でなくなる。単純化のため、役割を定義する個別の特権を列挙するのではなく、一連のセキュリティ属性をサブジェクトに割り当てられた「役割」としてセキュリティターゲット中で言明することは、いまだに妥当である。これは、役割を定義する一連の特権が管理可能である場合に必要となる。

ST 作成者への注意： ひとつの特定の利用者・サブジェクト間の束縛プロセスにおい

て、利用者の代理として動作するサブジェクトへ規定された属性のサブセットのみを割り当てることは許可される。しかし、複数の種類が実装されている場合には利用者・サブジェクト間の束縛プロセスの種類に応じて規定された割り当てのすべてがTOE によってサポートされ強制されなくてはならず（must）、また TOE によって強制されなくてはならない。これらの種類は、以下の割付に列挙されなくてはならない（must）。

FIA_USB.1.2 TSF は、利用者の代理として動作するサブジェクトのセキュリティ属性の初期の関連付けに関する以下のルールを強制しなくてはならない（shall）: [割付 : 属性の初期の関連付けに関するルール]。

適用上の注意： このルールは、利用者・サブジェクト間の束縛の際に TSF がサブジェクトのセキュリティ属性を特定し選択する方法を定義するものである（shall）。多くの場合、サブジェクトは単に利用者のプロファイルから利用者のセキュリティ属性を継承する。一部のセキュリティ属性に関して、TSF は特定のルールに基づいて利用者のセキュリティ属性がサブジェクトのセキュリティ属性に含まれるかどうかの判断を行ってもよい（例えば、TOE は利用者の持っている役割全体のリストから、アクティブな役割を選択することを利用者に許可してもよい）。その他の、利用者のセキュリティ属性から導出されたサブジェクトのセキュリティ属性は、他の TSF データに基づいて TSF によって決定されてもよい。例えば TSF は、特定の重要な管理特権を、利用者にこの特権が割り当てられているとともに利用者がローカルコンソールなどの特定の接続を介して TOE と接続している場合にのみ、サブジェクトへ割り当てるかもしれない。本プロテクションプロファイルに適合する TOE はそのような複雑なルールの実装を要求されてはいないが、実装している場合には正確に規定される必要がある。

FIA_USB.1.3 TSF は、利用者の代理として動作するサブジェクトに関連付けられたセキュリティ属性の変更を支配する以下のルールを強制しなくてはならない（shall）: [割付 : 属性の変更に関するルール]。

適用上の注意： サブジェクトのセキュリティ属性への変更は、明示的な利用者または管理者のアクションによって許可されてもよいし、特定のアクティビティの結果として自動的に行われてもよい。例えば Unix タイプのシステムでは、実効ユーザ ID とグループ ID が特定の属性を持つプログラムの起動の結果として変化する場合がある。SFR のこの部分は、そのようなルールの定義を意図している。

ST 作成者への注意： 上記の SFR は「人間の」利用者に適用されるが、必ずしもリモート IT エンティティには適用されない。多くのオペレーティングシステムでは、「人間の」利用者に直接束縛されてはいないサブジェクトを実装しているが、2 つの異なる利用者・サブジェクト間の束縛の方法を実装する必要を避けるため、「仮想ユーザ」を定義できるメカニズムを採用している。これは人間の利用者による使用から保護されている（認証情報が関連付けられていない）が、TSF によってのみ利用可能なユーザである。TSF は特定のサブジェクトを起動し、それを「仮想ユーザ」に定義付

けられたセキュリティ属性へ「束縛」することができる。Unix におけるデーモンは、そのようなサブジェクトの典型的な例である。そのような概念を実装する TOE は、(「人間の」利用者について定義されたものと異なる場合）そのような利用者・サブジェクト間の束縛プロセスのルールを記述する FIA_USB.1 の実体化を含む必要がある（has to)。

#### 8.1.3.9 FIA_PK_EXT.1 公開鍵ベースの認証

FIA_PK_EXT.1.1 TSF は、**[割付：RFC5280 または X.509v3 証明書が使われない場合には鍵管理／鍵検証の他の手法]** に定義される **[選択：X.509v3 証明書、公開鍵暗号方式]** を用いて、**[選択：IPsec、TLS、SSH]** 接続の認証をサポートしなくてはならない（shall)。

FIA_PK_EXT.1.2 TSF は、証明書または公開鍵あるいはその両方を保存し、不正な削除及び改変から保護しなくてはならない（shall)。

適用上の注意： FIA_PK_EXT.1.1 については、ST 作成者は管理接続を実装するために使われるプロトコルであって、また公開鍵ベースの認証を用いるものを選択すべきである（should)。X.509v3 証明書が用いられる場合、RFC 5280 に証明書有効性確認と認証パス検証の要件であって、この要件にしたがって TOE が実装しなくてはならないものが定義されていることに注意すべきである（should)。選択されたプロトコルに応じて、追加的なプロトコル特定の証明書関連の要件（及び関連付けられた保証アクティビティ）が規定されてもよい（例えば、IPsec については RFC 4945)。これらの追加的な要件は、そのプロトコルに関連付けられた要件中で規定される。

適用上の注意： FIA_PK_EXT.1.2 は、TSF によって利用され処理される証明書または公開鍵、あるいはその両方に適用される。運用環境内の他のコンポーネント（例えば RADIUS サーバ）によって利用され処理される証明書や公開鍵は、このエレメントによってカバーされることは意図されていない。

適用上の注意： TOE にプリロードされた証明書や公開鍵が含まれる場合、管理者がその使用を「無効化」(例えば、失効、削除）及び有効化できる限り、これは受容可能である。

### 8.1.4 クラス：セキュリティ管理 (FMT)

#### 8.1.4.1 FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1 TSF は、***以下の受容可能なパスワードのルールをそれらの利用者が指定できるようにすることによって、パスワードベースの利用者認証***機能の***ふるまいを変更***できる能力を **[割付：*他の利用者が操作を行うために満たす必要のあるルール*]** に限定しなくてはならない（shall)。

***a) 大文字、小文字、数字、及び特殊文字をパスワード中に使えるようにすること***
***b) 最小限のパスワードの長さを 8 文字以上（少なくとも 15 文字まで）に定めること***
***c) パスワードが少なくとも 1 つの数字と 1 つの特殊文字を含ま***

*なくてはならないと定めること*

*d) 少なくとも 6 個前までのヒストリーによって、同一の利用者が以前使っていたパスワードを拒否すること*

#### 8.1.4.2 FMT_MSA.1 オブジェクトのセキュリティ属性の管理

FMT_MSA.1.1 TSF は、**SFP でカバーされるオブジェクト**のセキュリティ機能の**改変*及び* [選択：デフォルト値変更、問い合わせ、削除、[割付：その他の操作]]** を行う能力を、**そのオブジェクトの所有者及び [割付:他の利用者が操作を行うために満たす必要のあるルール]** に制限する[割付：アクセス制御 SFP] を強制しなくてはならない（shall）。

#### 8.1.4.3 FMT_MSA.3(DAC) 静的な属性の初期化

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**制限的**デフォルト値を与える**[割付:アクセス制御 SFP]**を実施しなければならない（shall）。

FMT_MSA.3.2 TSF は、**[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者がそのアクティビティの実行が許可される場合を定めるルール]]** が、オブジェクトまたは情報が作成される際のデフォルト値に優先する代替的な初期値を規定することを許可しなければならない（shall）。

#### 8.1.4.4 FMT_MSA.3(NI) 静的な属性の初期化

FMT_MSA.3.1 TSF は、**ネットワーク情報フロー制御方針**を強制することによって、[選択、1 つを選択：制約的な、許容的な、[割付：その他のプロパティ]] デフォルト値を、SFP の強制に用いられるセキュリティ属性へ提供しなくてはならない（shall）。

FMT_MSA.3.2 TSF は、**[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者がそのアクティビティの実行が許可される場合を定めるルール]]** が、オブジェクトまたは情報が作成される際のデフォルト値に優先する代替的な初期値を規定することを許可しなければならない（shall）。

#### 8.1.4.5 FMT_MSA.4 セキュリティ属性値の継承

FMT_MSA.4.1 TSF は、以下のルールを用いて*アクセス制御方針のカバーするオブジェクト*のセキュリティ属性の値を設定しなくてはならない（shall）：[割付：セキュリティ属性の値を設定するルール]。

適用上の注意： これらのルールでは、あるアクセス制御方針の対象となる新たなオブジェクトについて、そのセキュリティ属性がどのように初期化されるかを規定する必要がある。これらのルールがオブジェクトの種類によって異なる場合、ST 作成者は FMT_MSA.4 の複数の具体化を用いて、セキュリティ属性を持つすべてのオブジェクトの種類をカバーしなくてはならない（shall）。他のオブジェクトから、またはオブジェクトを作成した利用者／サブジェクトからセキュリティ属性を継承することは、特定の TOE がオブジェクトのセキュリティ属性をどのように初期化するかを決定するためのひとつの方法である。

#### 8.1.4.6 FMT_MTD.1(AE) TSF データの管理

FMT_MTD.1.1 TSF は、**一連の監査事象**の**問い合わせ、変更**を行う能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FAU_SEL.1 に適用される。

#### 8.1.4.7 FMT_MTD.1(AS) TSF データの管理

FMT_MTD.1.1 TSF は、**監査ストレージ**の**クリア、[選択：ストレージの場所の構成、作成、削除、[割付：その他の操作]]** を行う能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FAU_STG.1 に適用される。

#### 8.1.4.8 FMT_MTD.1(AT) TSF データの管理

FMT_MTD.1.1 TSF は、

a) **アクションが行われる際の監査証跡の閾値、**
b) **閾値に達した際のアクション**

を**変更、[選択：追加、削除]** する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FAU_STG.3 に適用される。

#### 8.1.4.9 FMT_MTD.1(AF) TSF データの管理

FMT_MTD.1.1 TSF は、**監査格納失敗した際に取られるアクション**を**変更、[選択：追加、削除]** する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FAU_STG.4 に適用される。

#### 8.1.4.10 FMT_MTD.1(CM) TSF データの管理

FMT_MTD.1.1 TSF は、**リモートエンティティの認証 [選択：[割付：その他のセキュリティ機能]、他のセキュリティ機能なし] に用いられるデジタル証明書または公開鍵**を**インポート、有効化、無効化**する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FTP_ITC.1 に適用される。無効化の能力には、証明書または鍵の削除または失効が含まれるかもしれない。有効化

の側面は、証明書または鍵を正当に使用できるものにすることになる。これらの管理機能は、プリロードされた証明書や公開鍵にも、管理者によってロードされたものにも適用される。

#### 8.1.4.11 FMT_MTD.1(NI) TSF データの管理

FMT_MTD.1.1 TSF は、

a) **ネットワークデータの識別とマッチング、**
b) **識別されたネットワークデータに対して行われるアクション**

**を支配するルールに用いられるセキュリティ属性を定義、問い合わせ、変更、削除、[選択：デフォルト値変更、[割付：その他の操作]]** する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FDP_IFF.1 に適用される。

#### 8.1.4.12 FMT_MTD.1(IAT) TSF データの管理

FMT_MTD.1.1 TSF は、**不成功に終わった認証試行の閾値を変更**する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FIA_AFL.1 に適用される。

#### 8.1.4.13 FMT_MTD.1(IAF) TSF データの管理

FMT_MTD.1.1 TSF は、**認証失敗に陥ったアカウントの認証を再有効化**する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FIA_AFL.1 に適用される。

#### 8.1.4.14 FMT_MTD.1(IAU) TSF データの管理

FMT_MTD.1.1 TSF は、**利用者のセキュリティ属性を初期化、変更、削除**する能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

適用上の注意： この SFR は FIA_ATD.1、FIA_UAU.1、FIA_UID.1 に適用される。

#### 8.1.4.15 FMT_REV.1(OBJ) 失効

FMT_REV.1.1 TSF は、TSF の制御下にある**対応するオブジェクト**と関連付けられた、**SFP によって定義されるオブジェクトのセキュリティ属性**を失効させる能力を **[割付：権限のある識別済みの役割、ま**

**たは以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

FMT_REV.1.2 TSF は、*以下のルール*を強制しなくてはならない（shall）。

a) **オブジェクトと関連付けられたアクセス権は、アクセスチェックが行われる際に強制されなくてはならない（shall）。**
b) **[割付：その他の失効ルールの仕様]。**

#### 8.1.4.16 FMT_REV.1(USR) 失効

FMT_REV.1.1 TSF は、TSF の制御下にある**対応する利用者**と関連付けられた、**SFP によって定義される利用者のセキュリティ属性**を失効させる能力を **[割付：権限のある識別済みの役割、または以下のルールを満たす利用者：[割付：利用者にそのアクティビティの実行が許可される場合を定めるルール]]** に制限しなくてはならない（shall）。

FMT_REV.1.2 TSF は、*以下のルール*を強制しなくてはならない（shall）。

a) **利用者の次回の認証中の次回の利用者-サブジェクト間の束縛プロセスに伴うセキュリティ関連の認証の失効、**
b) **[割付：その他の失効ルールの仕様]。**

#### 8.1.4.17 FMT_SMF_RMT.1 リモート管理機能

FMT_SMF_RMT.1.1 TSF は、FTP_ITC.1 に言明される要件にしたがって確立される高信頼チャネルを用いてリモート IT エンティティから管理機能が実行されることも許可さなくてはならない（shall）。

#### 8.1.4.18 FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSF は、以下の役割を維持管理しなくてはならない（shall）。

a) **正当な管理者、**
b) **通常利用者、**
c) **[割付：その他の管理役割]。**

FMT_SMR.1.2 TSF は、利用者を役割と関連付けることができなくてはならない（shall）。

適用上の注意： TOE が最初に起動する際、TOE の構成に必要な管理機能を実施できる 1 つの役割が存在する必要がある。これが「正当な管理者」とみなされる。TOE には、事前定義された追加的な役割（例えば、特定の管理操作について）があってもよいし、また追加的な役割の動的な定義を許可してもよい。この SFR の意図は事前定義された役割（それらが SFR によって定義されるセキュリティ方針にとって意味がある限り）を規定することであるが、動的に作成されるかもしれないすべての役割を規定するために使うことは、もちろん不可能である。

したがって本プロテクションプロファイルでは、利用者に特定の管理操作を行うことが許可されているかどうかを判定するた

めに方針によって用いられる一般的なルールの仕様を要求している。これらのルールは、利用者が持つ役割に基づいていてもよいが、利用者または利用者が所属するグループに特有の特権や、追加的な TSF データ（例えば、利用者が特定のサブジェクトに束縛されている場合、日時、別の利用者によるアクティビティの承認など）に基づいていてもよい。これらのルールが管理アクティビティを定義された利用者の集合に限定することを許可している限り、またルールが全体として利用者に自分自身の特権を昇格させることを許可していない限り、そのようなルールは受容可能である。ST 作成者には、セキュリティターゲット中にこれらのルールを規定することが要求される。

SFR によって定義されるセキュリティ方針に規定されることを開発者が望んでいるものよりも多くの特権を、特定の TOE がサポートしてもよい。セキュリティターゲット中に用いられない特権については、開発者が何らかの利用者ガイダンスを提供し、セキュリティターゲットに言及されない任意の特権は、TOE を運用する組織の責任においてのみ利用者へ割り当てられることを説明しなくてはならない（shall）。ガイダンス文書全体との関連でそれらが正しく実装されているかは、試験されたり評価の一部として分析されたりしていないからである。

### 8.1.5 クラス：TSF の保護（FPT）

#### 8.1.5.1 FPT_STM.1 高信頼タイムスタンプ

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなくてはならない（shall）。

適用上の注意： TSF は、高信頼タイムスタンプをローカルなハードウェアクロックから取得するか、またはセキュアなネットワーク接続を用いて信頼されたリモートエンティティからタイムスタンプを取得してもよい（そのようなエンティティが利用可能な場合）。ローカルなハードウェアクロックから取得する場合、TSF は、信頼された管理者にローカルタイムの設定または修正を可能とし、それによって TSF がそれ自身のインタフェースを用いてローカルなハードウェアクロックにこれらのアクションを実行させるような管理インタフェースをエクスポートするか、もしくはタイムクロックの設定または変更を可能とするような IT 環境中のハードウェアへの保護されたインタフェースを有する必要がある。例えば、ハードウェアの構成に用いられる専用の管理コンソールを使用してローカルなハードウェアクロックの管理を行うことは許容可能である。

### 8.1.6 クラス：TOE アクセス（FTA）

#### 8.1.6.1 FTA_SSL.1 TSF 主導のセッションのロック

FTA_SSL.1.1 TSF は、[割付：利用者がインアクティブである時間間隔] の後、以下の手段によって、*TSF によって維持管理される人間の利用者との*対話セッションをロックしなくてはならない（shall）。

a) *TSF によって制御される*表示装置の画面の消去または上書きを行い、現在の表示内容を判読不能にすること、
b) セッションのロック解除を除き、利用者のデータアクセス／

*TSF によって制御される*表示装置に関するあらゆるアクティビティを無効とすること。

適用上の注意： FTA_SSL.1.1 b) は、セッションがロックされている間、オペレーティングシステムが利用者の代理として実行しているプロセスの処理を継続することを禁止するものではない。オペレーティングシステムは、セッションがロックされている間、そのようなプロセスからのいかなる出力も表示装置へ表示させないことに加え、セッションのロック解除に必要なものを除き、表示装置に関連付けられた入力装置（例：キーボード及びマウス）からのいかなる入力も受け付けるべきではない（should not）。

FTA_SSL.1.2 TSF は、セッションのロック解除に先立って、以下の事象の発生を必要としなくてはならない（shall）。

a) **[割付：FIA_UAU.5 に規定される許可された方式のリストにある認証方式のリスト] を使用した、セッションを所有する利用者の資格情報の再認証の成功、**
b) **[割付：発生すべきその他の事象]**。

適用上の注意： 最初の割付けの意図は、特定の時間間隔または時間間隔の範囲を管理者が設定できるようにすることである。例えば TOE は、タイムアウト時間を 5 分、15 分、1 時間、またはその間の 1 分刻みで管理者が選択できるようにしてもよい。重要なのは、管理者、またはある種の権限を有する利用者のみに、タイムアウト時間の設定を許可するように TOE が構成できることである。

例えば SSH を用いて、利用者がリモートシステムから TOE に接続することも可能だが、この要件はそのようなセッションには適用されない。

#### 8.1.6.2 FTA_SSL.2 利用者主導のロック

FTA_SSL.2.1 TSF は、以下の手段によって、*TSF によって維持管理される*利用者自身の対話セッションが利用者主導でロックされることを許可しなければならない（shall）。

a) *TSF によって制御される*表示装置の画面の消去または上書きを行い、現在の表示内容を判読不能にすること、
b) セッションのロック解除を除き、利用者のデータアクセス／*TSF によって制御される*表示装置に関するあらゆるアクティビティを無効とすること。

FTA_SSL.2.2 TSF は、セッションのロック解除に先立って、以下の事象の発生を必要としなくてはならない（shall）。

**a) [割付：FIA_UAU.5 に規定される許可された方式のリストにある認証方式のリスト] を使用した、セッションを所有する利用者の資格情報の再認証の成功]、**
**b) [割付：発生すべきその他の事象]。**

適用上の注意： FTA_SSL.1 に関して定義された適用上の注意が、ここでも適用される。

## 8.1.7 クラス：高信頼パス／チャネル（FTP）

### 8.1.7.1 FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 TSF は、自分自身と別の高信頼 IT 製品との間の通信チャネルであって、他の通信チャネルとは論理的に別個であり、そのエンドポイントの保証された識別とチャネルデータの改変~~または~~*及び*開示からの保護を提供するものを、*以下のメカニズムを用い*て提供しなくてはならない（shall）。

**以下を用いた暗号保護された通信チャネル [選択：**

i. **RFC 4251、RFC 4252、RFC 4253、及び RFC 4254 と、そこに定義される以下の暗号スイートの組み合わせによって定義される SSH：**

- **暗号化については 3DES-CBC、AES256-CBC、AES128-CBC、[選択：AES192-CBC、AEAD_AES_128_GCM（RFC 5647 の定義による）、AEAD_AES_256_GCM（RFC 5647 の定義による）、他のアルゴリズムなし]、**
- **完全性については [選択：HMAC_SHA1、HMAC-SHA1-96、HMAC-MD5、HMAC-MD5-96]、**
- **鍵交換については DIFFIE-HELLMAN-GROUP14-SHA1、[選択：DIFFIE-HELLMAN-GROUP1-SHA1、その他のアルゴリズムなし]、**
- **公開鍵暗号化については SSH-DSS、SSH-RSA、[選択：PGP-SIGN-RSA、PGP-SIGN-DSS、その他の公開鍵アルゴリズムなし]。**

ii. **RFC 5246 に定義される TLS であって、X.509 証明書を用い、そこで定義される下記の暗号スイートをサポートするもの：**

- **TLS_RSA_WITH_AES_128_CBC_SHA**
- **TLS_RSA_WITH_AES_256_CBC_SHA**

**[選択：**

- **なし**
- **TLS_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_DH_DSS_WITH_AES_128_CBC_SHA**
- **TLS_DH_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DHE_DSS_WITH_AES_128_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DH_DSS_WITH_AES_256_CBC_SHA**
- **TLS_DH_RSA_WITH_AES_256_CBC_SHA**
- **TLS_DHE_DSS_WITH_AES_256_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
- **TLS_DH_DSS_WITH_AES_128_CBC_SHA256**
- **TLS_DH_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_DHE_DSS_WITH_AES_128_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_DH_DSS_WITH_AES_256_CBC_SHA256**
- **TLS_DH_RSA_WITH_AES_256_CBC_SHA256**

- **TLS_DHE_DSS_WITH_AES_256_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384。**

iii. **RFC 4303 に定義される IPSEC プロトコル ESP であって、以下の暗号アルゴリズムを用いるもの**：

- **ESP 暗号化については AES-CBC-128、AES-CBC-256（両者とも RFC 3602 によって規定される）、[選択 : その他のアルゴリズムなし、Triple-DES、RFC 4106 に定義される AES-GCM-128、RFC 4106 に定義される AES-GCM-256]、**
- **ESP 認証及び認証ヘッダの保護については [選択：HMAC-SHA1-96、AES-XCBC-MAC-96]、**
- **鍵ネゴシエーション及び SA 確立については[選択、少なくとも 1 つを選択：RFC 2407、RFC 2408、RFC 2409、RFC 4109 に定義される IKEv1、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868]; RFC 5996、RFC 4307、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される IKEv2]、**
- **IKE 鍵確立に用いられる DH グループ 14（2048 ビット MODP）、及び [選択：24（2048-bit MODP と 256 ビット POS）、19（256 ビットランダム ECP）、20（384 ビットランダム ECP）、[割付：TOE の実装するその他の DH グループ]、その他の DH グループなし]、**
- **ピア認証については [選択 : DSA、rDSA、ECDSA] アルゴリズム。**

適用上の注意： これらの暗号スイートの仕様については、言及された RFC を参照されたい。

適用上の注意： 上に言及された暗号スイートの 1 つが使われているのではない場合に、TOE が高信頼チャネルの設定を拒否するように構成できることが強制される。この基本 OSPP に適合した TOE は、それでも上に列挙した暗号スイートのサブセットを実装してもよく、また上記のリストに含まれていないが参照されている RFC に列挙されている暗号スイートを実装してもよい。高信頼チャネルが要求された場合、上記の暗号アルゴリズムの組み合わせが用いられることを確実にする機能を提供することだけが必要とされる。その他の暗号スイートは、信頼されないチャネルにのみ用いることができる。

FTP_ITC.1.2 TSF は、[選択：TSF、別の高信頼 IT 製品] の高信頼チャネルを介した通信の開始を許可しなくてはならない（shall）。

FTP_ITC.1.3 TSF は、**ST に規定されるすべてのセキュリティ機能及び [割付：機能のリストまたは高信頼チャネルを必要とするその他の条件]** について、高信頼チャネルを介した通信を開始しなくてはならない（shall）。

## 8.2 セキュリティ機能要件の根拠

このセクションでは、本プロテクションプロファイルに定義されるセキュリティ機能要件の内部的な一貫性及び完全性の根拠を提供する。

### 8.2.1 要件の内部的な一貫性

本プロテクションプロファイルに選択されたコンポーネントの相互サポート及び内部的な一貫性が、このセクションに記述されている。

以下の根拠が、機能要件の内部的な一貫性を例証する。

#### 8.2.1.1 監査

TOE は、一般的な監査メカニズムを実装しなくてはならない（shall）。この監査メカニズムはすべてのセキュリティ関連事象について監査記録を生成しなくてはならず、また正当な利用者は監査される事象を選択できなくてはならない（shall）。正当な利用者には、監査データを読み出し解釈するための手段が提供されなくてはならない（shall）。TOE は監査証跡を保護し、また監査証跡がいっぱいになったり空きがなくなったりした際には適切なアクションが取られることを確実にしなくてはならない（shall）。これはローカルな監査ストレージに適用される。TOE はローカルな監査ストレージを提供しなくてはならない（must）。オプションとして TOE は、監査データがリモート高信頼 IT システムへ転送され、そこで保存されるような構成を許可することができる。

#### 8.2.1.2 利用者データの保護

利用者データは、不正なアクセスから保護される必要がある。これによって TOE は、異なる利用者またはサブジェクト間で利用者データを共有するために使われる可能性のあるすべてのオブジェクトの種類について、アクセス制御方針を実装することが要求される。少なくとも 1 つの種類の永続的オブジェクトについて、アクセス制御方針は単一の利用者のレベルにまで細かくアクセス制御を規定できるようにしなくてはならない（must）。さらに、情報フロー制御方針は意図されたネットワークトラフィックのみが TOE によって許可されることを確実にしなくてはならない。利用者データの保護は、適切な残存情報の保護によってサポートされる。

#### 8.2.1.3 識別及び認証

TOE と対話するエンティティは、適切に識別され認証されなくてはならない（shall）。（TOE のセキュリティ方針によって制御される情報フローを除く。これには適切な識別のみが要求される。）利用者・サブジェクト間の束縛プロセスは、外部エンティティが TSF によって制御される表現を持ち、これによって外部エンティティにセキュリティ方針が強制されることを確実にする。識別と認証をサポートするのは、TOE によって義務付けられるパスワード品質メカニズムである。

#### 8.2.1.4 セキュリティ管理

TOE は、管理機能自身を含め、すべてのセキュリティ機能の管理メカニズムを提供しなくてはならない（shall）。

#### 8.2.1.5 TOE へのアクセス

TOE は、そのサブジェクトを制御する利用者によって、または TOE によって開始されたサブジェクトへの確立されたセッションをロックする機能を提供しなくてはならない（shall）。

#### 8.2.1.6 TOE の保護

TOE は、リモートピアの証明書ベースの認証をサポートする、対称鍵暗号に基づいて暗号

保護されたネットワークプロトコルを提供しなくてはならない（shall）。認証のサポートについては、TOE はプロトコル仕様に定義されるデジタル証明書を用いなくてはならない（shall）。

### 8.2.2 セキュリティ要件のカバレージ

| SFR | 対策方針 |
|---|---|
| FAU_GEN.1 | O.AUDITING |
| FAU_GEN.2 | O.AUDITING |
| FAU_SAR.1 | O.AUDITING |
| FAU_SAR.2 | O.AUDITING |
| FAU_SEL.1 | O.AUDITING |
| FAU_STG.1 | O.AUDITING |
| FAU_STG.3 | O.AUDITING |
| FAU_STG.4 | O.AUDITING |
| FDP_ACC.1 | O.DISCRETIONARY.ACCESS,<br>O.SUBJECT.COM |
| FDP_ACF.1 | O.DISCRETIONARY.ACCESS,<br>O.SUBJECT.COM |
| FDP_IFC.1 | O.NETWORK.FLOW |
| FDP_IFF.1 | O.NETWORK.FLOW |
| FDP_RIP.2 | O.AUDITING<br>O.DISCRETIONARY.ACCESS<br>O.SUBJECT.COM<br>O.NETWORK.FLOW<br>O.I&A |
| FIA_AFL.1 | O.I&A |
| FIA_ATD.1 | O.I&A |
| FIA_UAU.1(RITE) | O.NETWORK.FLOW |
| FIA_UAU.1(HU) | O.I&A |
| FIA_UAU.5 | O.I&A |
| FIA_UAU.7 | O.I&A |
| FIA_UID.1 | O.I&A |
| FIA_USB.1 | O.I&A |
| FIA_PK_EXT.1 | O.TRUSTED_CHANNEL |
| FMT_MOF.1 | O.I&A, O.MANAGE |
| FMT_MSA.1 | O.MANAGE |
| FMT_MSA.3(DAC) | O.MANAGE |
| FMT_MSA.3(NI) | O.MANAGE |
| FMT_MSA.4 | O.MANAGE |
| FMT_MTD.1(AE) | O.MANAGE |
| FMT_MTD.1(AS) | O.MANAGE |
| FMT_MTD.1(AT) | O.MANAGE |
| FMT_MTD.1(AF) | O.MANAGE |
| FMT_MTD.1(CM) | O.MANAGE |
| FMT_MTD.1(NI) | O.MANAGE |
| FMT_MTD.1(IAT) | O.MANAGE |
| FMT_MTD.1(IAF) | O.MANAGE |
| FMT_MTD.1(IAU) | O.MANAGE |
| FMT_REV.1(OBJ) | O.MANAGE |
| FMT_REV.1(USR) | O.MANAGE |
| FMT_SMF_RMT.1 | O.MANAGE |
| FMT_SMR.1 | O.MANAGE |
| FPT_STM.1 | O.AUDITING |
| FTA_SSL.1 | O.I&A |
| FTA_SSL.2 | O.I&A |
| FTP_ITC.1 | O.TRUSTED_CHANNEL |

**表 7：セキュリティ機能要件のカバレージ**

| 対策方針 | カバレージの根拠 |
|---|---|
| O.AUDITING | 監査されるべき事象は [FAU_GEN.1] において定義されており、またその事象を引き起こした利用者の識別情報と関連付けられている [FAU_GEN.2]。正当な利用者には監査記録の読み出し能力が与えられている [FAU_SAR.1] 一方で、他のすべての利用者は監査記録へのアクセスを拒否されている [FAU_SAR.2]。正当な利用者は、どの監査記録が生成されるかを規定する能力を持たなくてはならない（must） [FAU_SEL.1]。TOE は監査ログが改変または削除されることを防止し [FAU_STG.1] 監査ログがリソース不足のため失われないことを確実にする [FAU_STG.3, FAU_STG.4]。監査をサポートするため、TOE は適切なタイムスタンプを維持管理することができる [FPT_STM.1]。<br><br>再利用されたリソースの保護は、どのデータも他の保護されたソースから漏えいしないことを確実にする [FDP_RIP.2]。 |
| O.DISCRETIONARY.ACCESS | TSF は利用者の識別情報に基づいてリソースへのアクセスを制御しなくてはならず、利用者はどのリソースをアクセスして自分のデータを保存したいかを規定することができる。<br><br>アクセス制御方針は、定義された制御の範囲を持たなくてはならない（must） [FDP_ACC.1]。アクセス制御方針のルールは [FDP_ACF.1] によって定義される。<br><br>再利用されたリソースの保護は、どのデータも他の保護されたソースから漏えいしないことを確実にする [FDP_RIP.2]。 |
| O.NETWORK.FLOW | ネットワーク情報フロー制御メカニズムは、異なるエンティティ間に流れる情報を制御する [FDP_IFC.1]。TOE は、情報フローを支配するルールセットを実装する [FDP_IFF.1]。情報フロー制御は未認証のリモート IT エンティティへ強制されるため、認証済みのリモート IT エンティティはネットワーク情報フロー制御方針のルールから除外することができる（FIA_UAU.1(RITE)）。<br><br>再利用されたリソースの保護は、どのデータも他の保護されたソースから漏えいしないことを確実にする [FDP_RIP.2]。 |
| O.SUBJECT.COM | TSF は、利用者の識別情報に基づいて、サブジェクト間の一時的ストレージオブジェクトを用いたデータの交換を制御しなくてはならない（must）。<br><br>アクセス制御方針は、定義された制御の範囲を持たなくてはならない（must） [FDP_ACC.1]。アクセス制御方針のルールは [FDP_ACF.1] によって定義される。<br><br>再利用されたリソースの保護は、どのデータも他の保護さ |

| 対策方針 | カバレージの根拠 |
|---|---|
| | れたソースから漏えいしないことを確実にする [FDP_RIP.2]。 |
| O.I&A | TSF は、正当な利用者のみが TOE 及びそのリソースへのアクセスを行えることを確実にしなくてはならない（must）。TOE へアクセスする権限を持つ正当な利用者は、識別及び認証プロセスを用いなくてはならない（must）[FIA_UID.1, FIA_UAU.1(HU)]。[FIA_UAU.5] に規定されているように、複数の I&A メカニズムは許可される。TOE への正当なアクセスを確実なものとするために、認証データは保護される [FIA_ATD.1, FIA_UAU.7]。また利用者の代理として動作するサブジェクトの適切な認証も、確実に行われる [FIA_USB.1]。認証手法の強度をサポートするため、TOE は不成功に終わった認証試行を特定し反応する能力 [FIA_AFL.1] 及びパスワードのルールを定める能力 [FMT_MOF.1] を有する。さらに、利用者の開始したセッションと TSF の開始したセッションのロック [FTA_SSL.1, FTA_SSL.2] によって、認証された利用者のセッションが保護される。<br><br>再利用されたリソースの保護は、どのデータも他の保護されたソースから漏えいしないことを確実にする [FDP_RIP.2]。 |
| O.MANAGE | TOE は、以下への管理インタフェースを提供する。<br><br>☐ アクセス制御方針 [FMT_MSA.1, FMT_MSA.3(DAC)]、<br>☐ 情報フロー制御方針 [FMT_MSA.3(NI), FMT_MTD.1(NI)]、<br>☐ 監査の側面 [FMT_MTD.1(AE), FMT_MTD.1(AS), FMT_MTD.1(AT), FMT_MTD.1(AF)]、<br>☐ デジタル証明書 [FMT_MTD.1(CM)]、<br>☐ 識別及び認証の側面 [FMT_MTD.1(IAT), FMT_MTD.1(IAF), FMT_MTD.1(IAU)]。<br><br>永続的に保存された利用者データは、階層的または関係的な方法で保存されるが、このことは親オブジェクトからのセキュリティ属性の継承を意味している [FMT_MSA.4]。<br><br>異なる管理側面への権利の管理は、 [FMT_SMR.1] で定義される。<br><br>利用者失効及びオブジェクト属性のインタフェースは、[FMT_REV.1(OBJ) 及び FMT_REV.1(USR)] で提供される。<br><br>パスワードのルールの管理は [FMT_MOF.1] で定義される。リモート管理機能は、[FMT_SMF_RMT.1] に定義されているように提供される必要がある。 |
| O.TRUSTED_CHANNEL | TOE は、リモート高信頼 IT システムと自分自身との間の高信頼チャネルで保護された通信を提供する [FTP_ITC.1]。リモートエンティティに対しては、デジタル証明書が用いられなくてはならない（must） |

| 対策方針 | カバレージの根拠 |
|---|---|
| | [FIA_PK_EXT.1]。 |

**表 8：セキュリティ機能要件の根拠**

### 8.2.3 セキュリティ要件の依存性分析

| SFR | 依存性 | 解決済みか |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | Yes |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | Yes: FAU_GEN.1<br>Yes: FIA_UID.1 |
| FAU_SAR.1 | FAU_GEN.1 | Yes |
| FAU_SAR.2 | FAU_SAR.1 | Yes |
| FAU_SEL.1 | FAU_GEN.1<br>FMT_MTD.1 | Yes: FAU_GEN.1<br>Yes: FMT_MTD.1(AE) |
| FAU_STG.1 | FAU_GEN.1 | Yes |
| FAU_STG.3 | FAU_STG.1 | Yes |
| FAU_STG.4 | FAU_STG.1 | Yes |
| FDP_ACC.1 | FDP_ACF.1 | Yes: FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | Yes: FDP_ACC.1<br>Yes: FMT_MSA.3(DAC) |
| FDP_IFC.1 | FDP_IFF.1 | Yes: FDP_IFF.1 |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | Yes: FDP_IFC.1<br>Yes: FMT_MSA.3(NI) |
| FDP_RIP.2 | N/A | Yes |
| FIA_AFL.1 | FIA_UAU.1 | Yes |
| FIA_ATD.1 | N/A | Yes |
| FIA_UAU.1(RITE) | FIA_UID.1 | Yes |
| FIA_UAU.1(HU) | FIA_UID.1 | Yes |
| FIA_UAU.5 | N/A | Yes |
| FIA_UAU.7 | FIA_UAU.1 | Yes: FIA_UAU.1(HU) |
| FIA_UID.1 | N/A | Yes |
| FIA_USB.1 | FIA_ATD.1 | Yes: FIA_ATD.1 |
| FIA_PK_EXT.1 | FMT_MTD.1 | Yes: FMT_MTD.1(CM) |
| FMT_MOF.1 | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>Yes: FMT_SMF.1 |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>MT_SMR.1<br>FMT_SMF.1 | Yes: FDP_ACC.1<br>Yes: FMT_SMR.1<br>Yes: FMT_SMF.1 |
| FMT_MSA.3(DAC) | FMT_MSA.1 | Yes: FMT_MSA.1 |
| | FMT_SMR.1 | Yes: FMT_SMR.1 |
| FMT_MSA.3(NI) | FMT_MSA.1<br><br>FMT_SMR.1 | NO, but satisfied with FMT_MTD.1(NI)<br>Yes: FMT_SMR.1 |
| FMT_MSA.4 | [FDP_ACC.1 or FDP_IFC.1] | Yes: FDP_ACC.1 |
| FMT_MTD.1(AE) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(AS) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(AT) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(AF) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(CM) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(NI) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_MTD.1(IAT) | FMT_SMR.1 | Yes: FMT_SMR.1 |

| SFR | 依存性 | 解決済みか |
|---|---|---|
| | FMT_SMF.1 | No: FMT_SMF.1 |
| FMT_MTD.1(IAF) | FMT_SMR.1 FMT_SMF.1 | Yes: FMT_SMR.1 No: FMT_SMF.1 |
| FMT_MTD.1(IAU) | FMT_SMR.1<br>FMT_SMF.1 | Yes: FMT_SMR.1<br>No: FMT_SMF.1 |
| FMT_REV.1(OBJ) | FMT_SMR.1 | Yes |
| FMT_REV.1(USR) | FMT_SMR.1 | Yes |
| FMT_SMF_RMT.1 | FTP_ITC.1 | Yes |
| FMT_SMR.1 | FIA_UID.1 | Yes |
| FPT_STM.1 | N/A | Yes |
| FTA_SSL.1 | FIA_UAU.1 | Yes: FIA_AUA.1(HU) |
| FTA_SSL.2 | FIA_UAU.1 | Yes: FIA_AUA.1(HU) |
| FTP_ITC.1 | N/A | Yes |

**表 9：セキュリティ機能要件の依存性分析**

未解決の依存性の根拠：

- ☐ FMT_SMF.1 に基づくいくつかの SFR の依存性は、SFR FMT_SMF.1 がプロテクションプロファイルに含まれないため未解決である。その代わりにプロテクションプロファイルには FMT_MTD.1 の具体的なインスタンスが、別個の管理側面のそれぞれについて含まれており、利用者が管理アクティビティを行うために必要とされる権限を持っているかどうかを判定するために TOE が利用するルールを ST 作成者が的確に規定できるようになっている。
- ☐ FMT_MSA.3(NI) : FMT_MSA.1(NI) が規定されてもよい場所で、FMT_MTD.1(NI) が規定されネットワーク情報フロー制御方針のセキュリティ属性の管理が要求されている。しかし、ネットワーク情報フロー制御方針はセキュリティ属性の管理の際には強制されることを要求されていない。ネットワーク情報フロー制御機能の管理的側面は、ネットワーク情報フロー制御メカニズムによって保護されているわけではないためである。したがって、FMT_MSA.1 は適用されず、FMT_MTD.1(NI) によって置き換えられている。

## 8.3 セキュリティ保証要件

本プロテクションプロファイルには、下記の保証コンポーネントが含まれており、これらは OSPP 第 2 部：「OSPP 評価の一般的アプローチ及び保証アクティビティ」（[OSPP-2]）中の保証アクティビティによって詳細化される。

| SAR | タイトル |
|---|---|
| ASE_INT.1 | ST 概説 |
| ASE_CCL.1 | 適合主張 |
| ASE_SPD.1 | セキュリティ課題定義 |
| ASE_OBJ.2 | セキュリティ対策方針 |
| ASE_ECD.1 | 拡張コンポーネント定義 |
| ASE_REQ.2 | 派生したセキュリティ要件 |
| ASE.TSS.1 | TOE 要約仕様 |
| ADV_ARC.1 | セキュリティアーキテクチャ記述 |
| ADV_FSP.1 | 基本機能仕様 |
| AGD_OPE.1 | 利用者操作ガイダンス |
| AGD_PRE.1 | 準備手続き |
| ALC_CMC.3 | 許可の管理 |
| ALC_CMS.3 | 実装表現の CM 範囲 |
| ALC_DEL.1 | 配付手続き |

| SAR | タイトル |
|---|---|
| ALC_FLR.3 | 系統的な欠陥修正 |
| ALC_LCD.1 | 開発者によるライフサイクルモデルの定義 |
| ATE_COV.2 | カバレージの分析 |
| ATE_DPT.1 | テスト：基本設計 |
| ATE_FUN.1 | 機能テスト |
| ATE_IND.2 | 独立テスト—サンプル |
| AVA_VAN.2 | 脆弱性分析 |

**表 10：セキュリティ保証要件**

## 8.4 セキュリティ保証要件の根拠

| SAR | 依存性 | 解決済みか |
|---|---|---|
| ASE_INT.1 | – | – |
| ASE_CCL.1 | ASE_INT.1 | Yes |
| | ASE_ECD.1 | Yes |
| | ASE_REQ.1 | Yes |
| ASE_SPD.1 | – | – |
| ASE_OBJ.2 | ASE_SPD.1 | Yes |
| ASE_ECD.1 | – | – |
| ASE_REQ.2 | ASE_OBJ.2 | Yes |
| | ASE_ECD.1 | Yes |
| ASE.TSS.1 | ASE_INT.1 | Yes |
| | ASE_REQ.1 | Yes |
| | ADV_FSP.1 | Yes |
| ADV_ARC.1 | ADV_FSP.1 | Yes |
| | ADV_TDS.1 | No |
| ADV_FSP.1 | – | – |
| AGD_OPE.1 | ADV_FSP.1 | Yes |
| AGD_PRE.1 | – | – |
| ALC_CMC.3 | ALC_CMS.1 | Yes |
| | ALC_DVS.1 | No |
| | ALC_LCD.1 | Yes |
| ALC_CMS.3 | – | – |
| ALC_DEL.1 | – | – |
| ALC_FLR.3 | – | – |
| ALC_LCD.1 | – | – |
| ATE_COV.2 | ADV_FSP.2 | No |
| | ATE_FUN.1 | Yes |
| ATE_DPT.1 | ADV_ARC.1 | Yes |
| | ADV_TDS.2 | No |
| | ATE_FUN.1 | Yes |
| ATE_FUN.1 | ATE_COV.1 | Yes |
| ATE_IND.2 | ADV_FSP.2 | No |
| AVA_VAN.2 | AGD_OPE.1 | Yes |
| | AGD_PRE.1 | Yes |
| | ATE_COV.1 | Yes |
| | ATE_FUN.1 | Yes |
| | ADV_ARC.1 | Yes |
| | ADV_FSP.2 | No |
| | ADV_TDS.1 | No |
| | AGD_OPE.1 | Yes |
| | AGD_PRE.1 | Yes |

**表 11：セキュリティ保証要件の依存性分析**

未解決の依存性の根拠：

- ☐ ADV_TDS ファミリのコンポーネントに関する依存性のいくつかが、満たされていない（ADV_ARC.1、ATE_DPT.1、AVA_VAN.2）。ADV_TDS ファミリのコンポーネントはこのマッピングに全く含まれていないが、本ドキュメントに記述された SFR 関連の保証アクティビティの記述からの設計関連の側面は、評価中に考慮する必要がある（have to）。ADV_TDS ファミリのコンポーネントが全く含まれていないのは、これらはいずれも本プロテクションプロファイルに適合した製品の設計評価の側面に必要とされる見方にそぐわないためである。それでも、満たされない依存性のあるコンポーネントの評価アクティビティを実施するために十分な設計情報が提供されていると、本 PP の作成者は確信している。
- ☐ ADV_FSP.2 に関する依存性のいくつかが、満たされていない（ATE_COV.2、ATE_IND.2、AVA_VAN.2）。本プロテクションプロファイルには、ADV_FSP.1 のみが含まれている。しかしここでの意図は、開発者によって提供されるすべての TSFI が、テストケースの開発や期待されるテスト結果の正しい特定、及び脆弱性分析の実施に用いることが可能な程度にまで、記述されることである。したがって、満たされない依存性のあるコンポーネントについて評価アクティビティが実施できるほど十分な情報が TSFI に関して提供されていると、本 PP の作成者は確信している。
- ☐ ALC_CMC.3 の ALC_DVS.1 に対する依存性が満たされていない。しかし、評価者は ALC_CMC.3 に関して開発者が記述した CM プロセスが記述どおりに確立されているかどうかを調査することが期待されている。これは、例えば記述されたプロセスの工程が評価者のオンサイトへの訪問中（例えば、独立テストを行うため）に適用されているかどうかを検証することによって、達成することができる。したがって、本 PP の作成者は ALC_CMC.3 に記述された CM プロセスの存在と適切な適用に関して、評価者が十分な自信を得られるものと確信している。

# 9 略語集

| 略語 | 説明 |
| --- | --- |
| AH | 認証ヘッダ |
| CC | コモンクライテリア |
| DAC | 任意アクセス制御 |
| EAL | 評価保証レベル |
| ESP | カプセル化されたセキュリティペイロード |
| IKE | インターネット鍵交換 |
| IPSEC | IP セキュリティプロトコル |
| MAC | 強制アクセス制御 |
| OSPP | 汎用オペレーティングシステムのプロテクションプロファイル |
| PP | プロテクションプロファイル |
| SAR | セキュリティ保証要件 |
| SFP | セキュリティ機能方針 |
| SFR | セキュリティ機能要件 |
| SSH | セキュアシェル |
| ST | セキュリティターゲット |
| TOE | 評価対象 |
| TLS | トランスポート層セキュリティ |
| TSF | TOE セキュリティ機能 |
| TSFI | TSF インタフェース |
| TSP | TOE セキュリティ方針 |