MIRACLE LINUX V4.0
/ MIRACLE LINUX V4.0 One
/ MIRACLE LINUX V4.0 x86-64
/ MIRACLE LINUX V4.0 x86-64 One
オペレーティングシステム
セキュリティーターゲット

バージョン： 1.0

発行日： 2007 年 1 月 11 日

作成者： ミラクル・リナックス株式会社

変更履歴

バージョン	日付	修正者	備考
0.10	2006/07/21	寺島、八木	初稿
0.11	2006/07/31	寺島、八木	全面見直し
0.12	2006/08/15	寺島、八木	全面見直し
0.13	2006/08/26	寺島、八木	3 TOE セキュリティ環境 ・ 章構成の変更 4 セキュリティ対策方針 ・ 表現の改善 5 IT セキュリティ要件 ・ 記述方式の修正
0.14	2006/08/30	寺島、八木	5 IT セキュリティ要件 ・ 全面見直し
0.15	2006/09/01	寺島、	2.4 TOE の論理的範囲 ・ 記述の詳細化 8 根拠 ・ 全面見直し
0.16	2006/09/06	寺島、八木	ST 名称の変更 2.3 TOE の物理的範囲 ・ 図 1 を修正 5. IT セキュリティ要件 ・ 全面見直し 6. TOE 要約仕様 ・ 全面見直し
0.17	2006/09/08	寺島、八木	2.3 TOE の物理的範囲 ・ 説明文章を追記 5. IT セキュリティ要件 ・ FDP_ACC.1(b)の修正 ・ FDP_ACF.1(a)の修正 ・ FDP_ACF.1(b)の修正 ・ FMT_MSA.1(a)の修正 ・ FMT_MSA.1(b)の修正 ・ FMT_SMR.1(c)の追加 6. TOE 要約仕様 ・ 全面見直し

			8 根拠 ・ 全面見直し
0.18	2006/09/15	寺島、八木	2.3 TOE の物理的範囲 ・ 図 1 の修正 2.4 TOE の論理的範囲 ・ 監査を追加 5. IT セキュリティ要件 ・ 監査を追加 6. TOE 要約仕様 ・ 監査を追加 8 根拠 ・ 監査を追加
0.19	2006/09/27	寺島、八木	2.3 TOE の利用者役割 ・ 追加 5. IT セキュリティ要件 ・ FMT_MOF.1 を追加 6. TOE 要約仕様 ・ FMT_MOF.1 を追加 8 根拠 ・ FMT_MOF.1 を追加 8.3 TOE セキュリティ機能要件の相互サポート ・ 全面見直し
0.20	2006/10/3	寺島	2.5 TOE の論理的範囲 ・ 監査機能の修正 5 IT セキュリティ要件 ・ FMT_MOF.1(b)を FMT_MOF.1(a)に統合 ・ FMT_MSA.1(b)を削除 ・ FMT_SMF.1 を修正 ・ FMT_SMR.1(c)を削除 6 TOE 要約仕様 ・ 全面見直し 8.2.1 セキュリティ機能要件根拠 ・ 全面見直し 8.2.4 セキュリティ機能要件の依存性根拠 ・ 全面見直し 8.2.5 TOE セキュリティ機能要件の交互サポート ・ 全面見直し 8.2.6 内部一貫性の根拠 ・ 追加 8.3.1 TOE セキュリティ機能の根拠 ・ 全面見直し

0.21	2006/10/6	寺島	1.1 ST 識別 ・ CC 識別の表記を変更 5.1.1 TOE セキュリティ機能要件 ・ 前書きの変更 8.3.1 TOE セキュリティ機能の根拠 ・ FIA_ATD.1 を DAC.1、DAC.2 に変更 ・ FIA_USB.1 に DAC.1、DAC.2 の記述を追加 ・ FMT_SMR.1(a)に AU.3 の記述を追加 ・ FMT_SMR.1(c)から DAC.1 の記述を削除
0.22	2006/10/10	寺島	5.1.1 TOE セキュリティ機能要件 ・ FMT_MTD.1(b)を FMT_MTD.1(a)に統合 ・ FMT_MTD.1(c)を FMT_MTD.(b)に変更 ・ FMT_MTD.1(e)を FMT_MTD.1(d)に統合 ・ FMT_MTD.1(f)を FMT_MTD.1(d)に統合 ・ FMT_MTD.1(d)を FMT_MTD.1(c)に変更 ・ FMT_MSA.1(a)を修正 6.1.2 任意アクセス制御 ・ DAC.2 からグループ ID の記述を削除
0.23	2006/11/1	寺島	5.1.1 TOE セキュリティ機能要件 ・ FAU_GEN.1 のからグループ認証の記述を削除 ・ FAU_GEN.2 の削除 ・ FMT_MSA.3(b)を追加 ・ FMT_MTD.1(a)にグループ管理者を追加 ・ FMT_MTD.1(b)を追加 ・ FMT_MTD.1(e)を追加 ・ FMT_SMF.1 にグループ管理の機能を追加 ・ FMT_SMR.1(d)を追加 ・ FIA_USB.1 を修正 ・ FMT_MTD.1(f)を追加 6.1.1 識別/認証 ・ グループ管理を追加 6.1.2 任意アクセス制御 ・ アトリビュート属性の記述を追加 6.1.3 監査記録の生成 ・ グループ切り替えの記述を削除
0.24	2006/11/30	寺島	全体 ・ アトリビュート属性を ext2/ext3 ファイルシステムのアトリビュートに変更 ・ プロセスへのアクセス制御のサブジェクトを「サブジェクト以外のプロセス」と「サブジェクト以外のプロセスが保持するデータオブジェクト」に分割 2.3 TOE 関連の利用者識別

			・ 所有者の定義を追加 3.2 組織のセキュリティ方針 ・ P_NEED_TO_KNOW.2 を追加 ・ P.LOG_SIZE を追加 3.3 前提条件 ・ A.COOP を削除 4.1 IT セキュリティ対策方針 ・ O.DISCRETIONARY_ACCESS.2 を追加 ・ O.LOG_SIZE を追加 4.2 非 IT セキュリティ対策方針 ・ O.EDUCATION を削除 5.1.1 TOE セキュリティ機能要件 ・ FMT_REV.1 を削除
0.25	2006/12/04	寺島	パスワード入力時のフィードバックの記述を修正
1.0	2007/1/11	寺島	6.3 保証手段 ・ ガイダンス名称を変更

目次

1. ST 概説

1.1. ST 識別

- ST名称　MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One
  MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One
  オペレーティングシステム　セキュリティーターゲット
- STバージョン　1.0
- ST作成日付　2007/1/11
- ST作成者　ミラクル・リナックス株式会社　大石裕司、寺島広大、八木和生
- TOE名称　MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One
  MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One
  オペレーティングシステム
- TOEバージョン　4.0
- 評価保証レベル　EAL1
- CC識別　CCバージョン2.3、ISO/IEC15408: 2005
  Interpretations-0512
- キーワード　オペレーティングシステム、OS、Linux

1.2. ST 概要

本セキュリティターゲットは、MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステムに関するセキュリティ仕様について記述したものである。MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステムは Linux オペレーティングシステムの商用ディストリビューションであり、Intel x86 プラットフォーム上で動作する、マルチユーザ、マルチタスクのオペレーティングシステムである。

TOE は TOE が管理する情報の不正アクセス、改竄、漏洩を防ぐために、個々の利用者を識別/認証する機能、識別/認証された利用者のオブジェクトへのアクセスを制限するアクセス制御機能、各ユーザプロセス間の分離を保証するプロセス分離機能、および利用者を識別/認証する際の監査証跡を記録する監査機能を提供する。

1.3. CC 適合

本書は、以下を満たしている。

- 機能要件: CC バージョン 2.3 パート 2 適合
- 保証要件: CCバージョン2.3 パート3適合
- 補足-0512適用
- EAL1適合
- 本STが適合するPPはない

1.4. 参考資料

本書を作成するにあたり、参考にした資料は以下の通りである。

- 情報セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル
  2005年8月 バージョン2.3 CCMB-2005-08-001
  平成17年12月翻訳第1.0版
  独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
- 情報セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件
  2005年8月 バージョン2.3 CCMB-2005-08-002
  平成17年12月翻訳第1.0版
  独立行政法人情報処理推進機構 セキュリティセンター情報セキュリティ認証室
- 情報セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件
  2005年8月 バージョン2.3 CCMB-2005-08-003
  平成17年12月翻訳第1.0版
  独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
- 補足-0512
  2005年12月 Interpretations-0512
  独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

2. TOE 記述

2.1. 製品種別

本 TOE は、以下の製品の共通部分であるオペレーティングシステム部分である。

- MIRACLE LINUX V4.0
- MIRACLE LINUX V4.0 One
- MIRACLE LINUX V4.0 x86-64
- MIRACLE LINUX V4.0 x86-64 One

2.2. TOE の利用環境

TOE は一般的な Intel x86 互換コンピュータ上で動作可能な、ミッションクリティカル・エンタープライズコンピューティング用途に設計されている。TOE はマルチプロセッサを搭載したコンピュータで動作させることが可能である。

TOE はマシンルームや、データセンター内に設置されたコンピュータにインストールされ、適切に管理されることを想定している。

2.3. TOE 関連の利用者識別

TOE を利用する人間は役割ごとに責任者、管理者、利用者に分類される。責任者は管理者を任命する権限を持ち、管理者は TOE を管理する権限を持つ。利用者は管理者によって TOE へのアクセスを許可される。また、オブジェクトのユーザ ID と一致するユーザを、該当オブジェクトの所有者と呼ぶ。

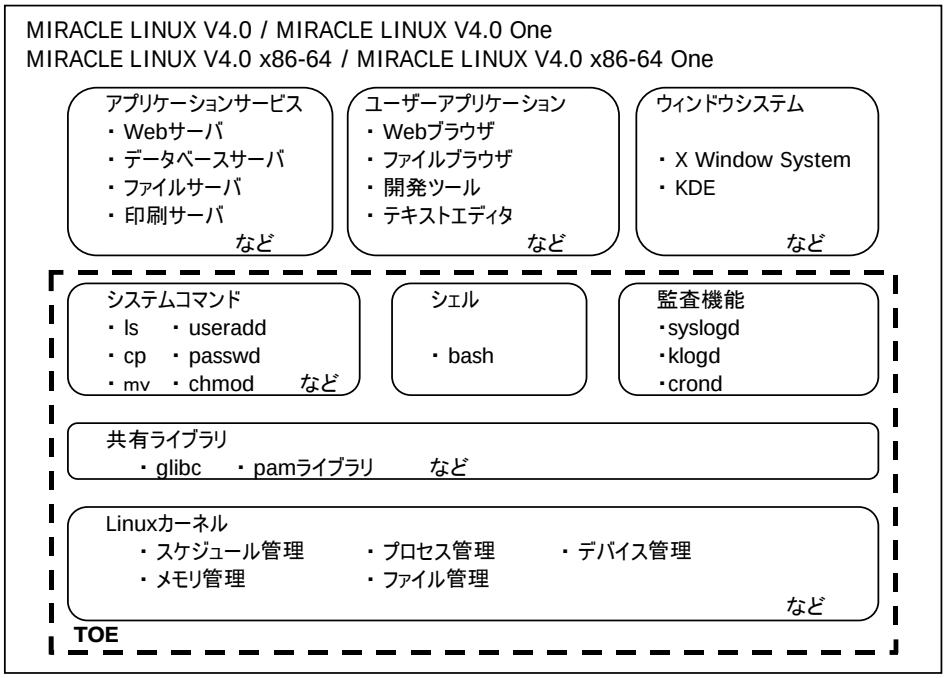
2.4. TOE の物理的範囲

本 TOE は、MIRACLE LINUX V4.0 のオペレーティングシステム部分である。TOE の物理的な範囲を図 1 に示す。

TOE は MIRACLE LINUX V4.0 の Linux カーネル、共有ライブラリ、シェル、システムコマンドである。Linux カーネルはスケジュール管理、メモリ管理、プロセス管理、ファイル管理、デバイス管理、入出力制御などの機能を有し、/boot 下の vmlinuz で始まる名称のファイルである。共有ライブラリは、各種アプリケーションが共通で利用する機能が含まれており、最小インストール時の/lib、/usr/lib 下のファイル全てである。シェルは利用者が対話的にシステムを操作するためのインターフェースおよび機能を有し、システムコマンドを実行するためのプラットフォームを提供する。システムコマンドは、MIRACLE LINUX V4.0 を管

理する上で必要となる基本的なコマンド群であり、キャラクタユーザインタフェース上で利用される。最小インストール時の/bin、/sbin、/usr/bin、/usr/sbin 下の全てのファイルが該当する。MIRACLE LINUX V4.0 には、その他にもウィンドウシステムやアプリケーションサービス、様々なユーザプリケーションが含まれるが、これらは全て MIRACLE LINUX V4.0 オペレーティングシステムの機能ではないため、本 TOE には含めない。

図 1 : TOE の物理的範囲



2.5. TOE の論理的範囲

TOE は Linux オペレーティングシステムの商用ディストリビューションであり、Linux は POSIX 標準に基づいて作成され、GPL ライセンスの元で配布されているオペレーティングシステムである。TOE は IA32、x86-64 アーキテクチャーの CPU を搭載した Intel x86 互換のコンピュータで動作する、マルチユーザ、マルチタスクのオペレーティングシステムである。

TOE は、以下のようにいくつかの層に分けて考えることができる。

- Linux カーネル
- 共有ライブラリ
- シェル
- システムコマンド

TOE は、これらの機能が連携することによって正常に動作する。低位層では、Linux カーネルはアプリケ

ーションプログラムに命令セットを供給し、ハードウェアプラットフォームと対話する。代表的なものとして、スケジュール管理、メモリ管理、プロセス管理、ファイル管理、デバイス管理、入出力管理などの機能を有する。Linux カーネルはカーネルモードと呼ばれるプロセッサーの特権モードで動作し、コンピュータのすべての資源へのフルアクセス権を持つ。

カーネルモードで動作する必要のないアプリケーションは、オペレーティングシステムの機能を直接呼び出すのではなく、共有ライブラリの呼び出しによって必要なオペレーティングシステムのサービスを実行する。UNIX または POSIX のアプリケーションをサポートするために必要な機能はすべて共有ライブラリによって実装されている。

以下に、TOE が持つ各機能の詳細を説明する。

2.5.1. Linux カーネル

2.5.1.1 スケジュール管理

TOE は異なるタスクに CPU 時間を割当てるためのスケジュールサービスを提供する。タスクにはユーザプロセスおよびカーネルプロセスの両方が含まれる。スケジューリングはプロセッサー時間の割当てを管理するだけでなく、カーネルタスクによる共用データへのアクセスが混乱しないことを保証する。スケジュールサービスは、複数のプロセッサーへのタスクの割当ても行う。

2.5.1.2 メモリ管理

メモリ管理サービスは物理メモリにページ、ページグループ、あるいは小さなブロックの割当てを行うために提供され、実行中のプロセスのアドレス空間のマッピングや仮想メモリの割当てを行う。仮想メモリシステムは各プロセスから利用されるアドレス空間の管理を行う。

2.5.1.3 プロセス管理

プロセスは、独自の仮想アドレス空間で動作しているプログラムのことである。プロセスの生成はプログラムの実行とは異なり、プロセスは動作中に新しいプロセスの作成することや、新しいプログラムを既存のプロセス内で実行することができる。

それぞれのプロセスは固有の識別子を持っており、関連するユーザ識別子(ユーザ ID)および 1 つ以上のグループ識別子(グループ ID)がある。これらの識別子は、オブジェクトにアクセスするためのプロセスの権限を決定する。

プロセスが新しいプロセスを作成した場合、作成されたプロセスは元のプロセスの持っている識別子などの特性を継承する。

プロセス間通信は、シグナルおよびセマフォによって実装されており、仮想メモリ空間やオブジェクトを共有している場合に内容の不整合や破壊を防ぐ。

2.5.1.4 ファイル管理

データのストリームの入出力を扱うことができるものは全てファイルである。ファイルには、一般的にファイルと呼ばれるオブジェクトに加えて、ディレクトリ、デバイスドライバおよびネットワーク接続などを含む。個々のファイルの詳細な実装は仮想ファイルシステム(VFS)によって管理される。

2.5.1.5 デバイス管理

Linux のデバイスドライバは全て通常のファイルとして存在し、次の 3 つの種別が存在する。

- ブロックデバイス: 独立した固定サイズブロックのデータへのランダムなアクセスが可能な装置
- キャラクタデバイス: 文字のストリームによってされる装置
- ネットワークデバイス: カーネルのネットワークサブシステムによって使用される。

2.5.2. 共有ライブラリ

共有ライブラリは、他のプログラムにサービスを提供するために使われる特別なプログラムである。共有ライブラリは関数や定数の定義など部品化されたソフトウェアの集合であり、単独のファイルとして実行形式のプログラムとは別に提供される。

2.5.3. シェル

シェルは、プロンプトを出力し、ユーザから入力されたコマンドライン解釈し、与えられた指示をカーネルに命令するためのソフトウェアである。また、システムコマンドを実行するための環境である。

2.5.4. システムコマンド

システムコマンドは、シェル上で動作し、TOE を管理するために必要となるコマンド群である。TOE にはオブジェクトの管理、セキュリティ属性の管理、利用者の管理などを行うために必要なコマンドが含まれ、それらは 1 つのプログラム、またはシェルの機能の一部として提供される。

2.5.5. 監査機能

監査機能は、各利用者が識別/認証を行う際の監査証跡を記録する。監査証跡へのアクセスは管理者のみが行うことができる。

2.6. TOE によって提供されるセキュリティサービス

2.6.1. 識別/認証

全ての利用者はユニークな識別子を割当てられる。TSF は、TSF を介する全ての利用者の行動について、要求した利用者の身元を認証する。認証はパスワードによって行われる。

2.6.2. アクセス制御

アクセス制御はプロセス、ファイルおよびディレクトリ、メモリ上のデータであるオブジェクトに適用される。プロセスのユーザ ID およびグループ ID と、操作対象となるオブジェクトの所有ユーザ ID、所有グループ ID、各パーミッション、ext2/ext3 ファイルシステムのアトリビュートに基づいて制御が実施される。

2.6.3. 監査

監査は、管理者および利用者の認証/識別を逐次記録し、蓄積するための機能である。監査証跡は通常のテキストファイル形式で記録され、管理者のみが読み出し可能である。また、監査証跡は一定のサイズおよび期間でローテーションされる。

2.6.4. プロセスの分離

TSF は、オペレーティングシステムカーネルとユーザプロセス、および各ユーザプロセス間の分離を保証する。

3. TOE セキュリティ環境

3.1. 脅威

TOE および環境が対抗する脅威は存在しない。

3.2. 組織のセキュリティ方針

この章では、TOE が従わなければならない組織のセキュリティ方針を記述する。

3.2.1. P.AUTHORISED_USERS

許可された利用者のみが TOE にアクセス可能である。

3.2.2. P.NEED_TO_KNOW.1

ファイルおよびディレクトリの所有者は、セキュリティ属性を変更することで自身以外の利用者の該当ファイルおよびディレクトリへのアクセスを必要な利用者のみに制限する。

3.2.3. P.NEED_TO_KNOW.2

プロセスへのアクセスは、所有者および管理者のみに制限する。

3.2.4. P.ACCOUNTABILITY

利用者が TOE にアクセスする際の識別/認証を記録する。

3.2.5. P.LOG_SIZE

管理者は、データのあふれによる監査記録の消失を防ぐ設定を行う。

3.3. 前提条件

この章では、TOE を使用する環境において、従わなければならない前提条件を記述する。

3.3.1. A.LOCATE

TOE は、物理的な攻撃から保護されるものとする。

3.3.2. A.MANAGE

TOE の管理者は悪意のある行為を行わず、与えられた権限に対する責務を果たすものとする。

3.3.3. A.PASSWORD

TOE の利用者および管理者のパスワードは推測可能な文字列ではなく、かつ、各利用者および管理者は自身のパスワードを秘匿しなければならない。

4. セキュリティ対策方針

この章では、組織のセキュリティ方針に対するセキュリティ対策方針を記述する。

4.1. IT セキュリティ対策方針

次に組織のセキュリティ方針に対する、IT 環境のセキュリティ対策方針を記述する。

4.1.1. O.AUTHORIZATION

TSF は、許可された利用者のみに TOE へのアクセスを許可しなければならない。

4.1.2. O.DISCRETIONARY_ACCESS.1

TSF はセキュリティ属性に基づき、ファイルおよびディレクトリへのアクセスを制御しなければならない。TSF は、ファイルおよびディレクトリの所有者が、該当ファイルおよびディレクトリのセキュリティ属性を管理することを許可しなければならない

4.1.3. O.DISCRETIONARY_ACCESS.2

TSF はセキュリティ属性に基づき、プロセスへのアクセスを該当プロセスの所有者および管理者のみに制限しなければならない。TSF は、プロセスのセキュリティ属性の管理を管理者のみに制限しなければならない。

4.1.4. O.AUDITING

TSF は、利用者が TOE へアクセスする最初のステップである識別/認証の事象を記録し、管理者にこの情報を提示しなければならない。

4.1.5. O.LOG_SIZE

TSF は、管理者が設定した容量で監査記録を定期的にローテーションしなければならない。

4.2. 非 IT セキュリティ対策方針

次に前提条件に対する、IT 以外の環境のセキュリティ対策方針を記述する。

4.2.1. O.ADMINISTRATOR

TOE の責任者は、悪意を持たない管理者を任命する。

4.2.2. O.PHYSICAL

TOE の責任者は、物理的な攻撃から保護するため、TOE を安全な設備内に設置しなければならない。

4.2.3. O.CREDENTIAL

TOE の管理者は、管理者および許可された利用者のパスワードが安易に推測可能な文字列ではなく、各利用者および管理者は自身のパスワードを秘匿しなければならない。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

この章はセキュリティ対策方針を達成するための、TOE の機能要件を定義する。”詳細化”を行った部分は**ボールド文字と下線**で識別し、”繰り返し”を行った部分は、例えば”(a)” というように括弧とアルファベットサフィックスで識別する。

5.1.1.1 FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1

TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;
b) 監査の[選択: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象;
及び
c) [割付: 上記以外の個別に定義した監査対象事象]。

[選択: 最小、基本、詳細、指定なし: から一つのみ選択]: **指定なし（監査対象事象を表 2 監査対象事象に示す）**

[割付: 上記以外の個別に定義した監査対象事象]: なし

表 2 : 監査対象事象

コンポーネント	監査内容	監査対象事象
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; **基本: 認証メカニズムのすべての使用。**	利用者のログインにあたっての認証の成功および失敗 利用者のログイン中の利用者切り替えにあたっての認証の成功および失敗 管理者のログインにあたっての認証の成功および失敗
FIA_UAU.6	a) 最小: 再認証の失敗; **b) 基本: すべての再認証試行。**	利用者のパスワード変更にあたっての再認証の成功および失敗
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニ	利用者のログインにあたっての識別の成功および失敗

	情報を含む、利用者識別メカニズムの不成功使用; **b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。**	よび失敗 管理者のログインにあたっての識別の成功および失敗

FAU_GEN.1.2

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

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);

及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報]

[割付: その他の監査関連情報]: なし

依存性: FPT_STM.1 高信頼タイムスタンプ

5.1.1.2 FAU_SAR.1 監査レビュー

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

下位階層: なし

FAU_SAR.1.1

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

[割付: 許可利用者]: 管理者

[割付: 監査情報のリスト]: 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)

FAU_SAR.1.2

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

依存性: FAU_GEN.1 監査データ生成

5.1.1.3 FAU_SAR.2 限定監査レビュー

下位階層: なし

FAU_SAR.2.1

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

依存性: FAU_SAR.1 監査レビュー

5.1.1.4 FAU_SAR.3 選択可能監査レビュー

下位階層: なし

FAU_SAR.3.1

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

[割付: 論理的な関連の基準]: 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)

[選択: 検索、分類、並べ替え]: 検索、分類、並べ替え

依存性: FAU_SAR.1 監査レビュー

5.1.1.5 FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1

TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSF は、監査証跡内の格納された監査記録への不正な改変を[選択: 防止、検出: から一つのみ選択]できねばならない。

[選択: 防止、検出: から一つのみ選択]: 防止

依存性: FAU_GEN.1 監査データ生成

5.1.1.6 FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層: なし

FAU_STG.3.1

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

[割付: 事前に定義された限界]: 監査証跡のファイルのサイズ

[割付: 監査格納失敗の恐れ発生時のアクション]: 最も古い監査証跡の削除

依存性: FAU_STG.1 保護された監査証跡格納

5.1.1.7 FDP_ACC.1(a) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1(a)

TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]: 表 3 サブジェクトおよびオブジェクトの操作のリスト

表 3 : サブジェクトおよびオブジェクトの操作のリスト

サブジェクト	オブジェクト	操作のリスト
プロセス	ファイル	・ 読み込み ・ 書き込み/追加書き込み ・ 実行
	ディレクトリ	・ ディレクトリ内のファイルおよびディレクトリの一覧の取得 ・ ディレクトリ内のファイルおよびディレクトリの生成/変更/削除 ・ ディレクトリへの移動

[割付: アクセス制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

5.1.1.8 FDP_ACC.1(b) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1(b)

TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]: 表 4 サブジェクトおよびオブジェクトの操作のリスト

表 4 : サブジェクトおよびオブジェクトの操作のリスト

サブジェクト	オブジェクト	操作のリスト
プロセス	サブジェクト以外のプロセス	・ 停止 ・ 復帰 ・ 削除
	サブジェクト以外のプロセスが保持するデータオブジェクト	・ 読み込み ・ 書き込み

[割付: アクセス制御 SFP]: プロセスへの任意アクセス制御

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

5.1.1.9 FDP_ACF.1(a) セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1(a)

TSF は、以下の[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]: 表 5 サブジェクトおよびオブジェクトのセキュリティ属性

表 5 : サブジェクトおよびオブジェクトのセキュリティ属性

サブジェクト/オブジェクトの区別	サブジェクト/オブジェクト名称	セキュリティ属性
サブジェクト	プロセス	・ ユーザ ID ・ グループ ID

オブジェクト	ファイル	・ ファイルの所有者 ・ ファイルの所有グループ ・ ファイルの所有者のパーミッション ・ ファイルの所有グループのパーミッション ・ ファイルのその他の利用者のパーミッション ・ ext2/ext3 ファイルシステムのファイルのアトリビュート（追加書き込み、変更不可）
オブジェクト	ディレクトリ	・ ディレクトリのスティッキービット ・ ディレクトリの所有者 ・ ディレクトリの所有グループ ・ ディレクトリの所有者のパーミッション ・ ディレクトリの所有グループのパーミッション ・ ディレクトリのその他の利用者のパーミッション ・ ext2/ext3 ファイルシステムのディレクトリのアトリビュート（変更/削除不可、変更不可）

[割付: アクセス制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御

FDP_ACF.1.2(a)

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

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]: 以下の箇条書きで示される規則がすべて適用される。

- プロセスのユーザIDが、該当ファイルまたはディレクトリの所有者と一致する場合、当該ファイルまたはディレクトリの所有者のパーミッションにて設定されている許可される操作が許可される。
- プロセスのグループIDが該当ファイルまたはディレクトリの所有グループと一致する場合、当該ファイルまたはディレクトリの所有グループのパーミッションにて設定されている許可される操作が許可される。
- プロセスのユーザID、グループIDに関わらず、該当ファイルまたはディレクトリのその他の利用者のパーミッションにて設定されている許可される操作が許可される。
- 該当ディレクトリに存在するファイルまたはディレクトリは、該当ディレクトリの所有グループのパーミッション、該当ディレクトリのその他の利用者のパーミッションによって、該当ディレクトリのディレクトリおよびファイルの生成/変更/削除が許可されていたとしても、スティッキービット属性が有効である場合は削除操作が拒否される。
- ext2/ext3ファイルシステムのファイルのアトリビュート（追加書き込み）が有効である場合、該当ファイルのパーミッションによって該当ファイルの書き込み/追加書込み操作が許可されている

IDが管理者であっても、追加書き込み操作だけに限定される。

- ext2/ext3ファイルシステムのディレクトリのアトリビュート（変更/削除不可）が有効である場合、該当ディレクトリのパーミッションによって該当ディレクトリにおけるディレクトリまたはファイルの生成/変更/削除操作が許可されている場合でも生成操作だけに限定される。プロセスのユーザIDが管理者であっても、生成操作だけに限定される。
- ext2/ext3ファイルシステムのファイルのアトリビュート（変更不可）が有効である場合、該当ファイルのパーミッションによって該当ファイルの書き込み/追加書き込み操作が許可されている場合でも、書き込み/追加書き込み操作が拒否される。プロセスのユーザIDが管理者であっても同様に拒否される。
- ext2/ext3ファイルシステムのディレクトリのアトリビュート（変更不可）が有効である場合、該当ディレクトリのパーミッションによって該当ディレクトリの生成/変更/削除操作が許可されている場合でも、生成/変更/削除操作が拒否される。プロセスのユーザIDが管理者であっても同様に拒否される。

FDP_ACF.1.3(a)

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

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]:ユーザ ID が管理者の場合、すべてのファイルおよびディレクトリに対しパーミッションの設定にかかわらずアクセスが可能である。

FDP_ACF.1.4(a)

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

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]:なし
依存性: FDP_ACC.1 サブセットアクセス制御、FMT_MSA.3 静的属性初期化

5.1.1.10 FDP_ACF.1(b) セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1(b)

TSF は、以下の[割付: 示されたSFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、またはSFP 関連セキュリティ属性の名前付けされたグループ]: 表 6 サブジェクトおよびオブジェクトのセキュリティ属性

表 6 : サブジェクトおよびオブジェクトのセキュリティ属性

サブジェクト/オブジェクトの区別	サブジェクト/オブジェクト名称	セキュリティ属性
サブジェクト	プロセス	・ ユーザ ID
オブジェクト	サブジェクト以外のプロセス	・ ユーザ ID
オブジェクト	サブジェクト以外のプロセスが保持するデータオブジェクト	・ ユーザ ID

[割付: アクセス制御 SFP]: プロセスへの任意アクセス制御

FDP_ACF.1.2(b)

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

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]: プロセスはユーザ ID と該当プロセスのユーザ ID を照合する。照合した結果、一致した場合、サブジェクト以外のプロセスの停止、復帰、削除、およびサブジェクト以外のプロセスが保持するデータオブジェクトへの読み込み、書き込みのアクセスを許可する。

FDP_ACF.1.3(b)

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

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]: ユーザ ID が管理者のプロセスはすべてのプロセスおよびすべてのプロセスが保持するデータオブジェクトに対してアクセスが許可される。

FDP_ACF.1.4(b)

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

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]: なし

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

5.1.1.11 FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1

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

[割付:セキュリティ属性のリスト]: ユーザ ID、グループ ID
依存性: なし

5.1.1.12 FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1

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

[割付: 定義された品質尺度]: 管理者が設定する利用者のパスワードポリシー(最小文字数)

依存性: なし

5.1.1.13 FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1

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

依存性: FIA_UID.1 識別のタイミング

5.1.1.14 FIA_UAU.6 再認証

下位階層: なし

FIA_UAU.6.1

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

[割付: 再認証が要求される条件のリスト]: 利用者のパスワード変更
依存性: なし

5.1.1.15 FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1

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

[割付: フィードバックのリスト]: 何も表示されない

依存性: FIA_UAU.1 認証のタイミング

5.1.1.16 FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

5.1.1.17 FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1

TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]: ユーザ ID、グループ ID

FIA_USB.1.2

TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: 属性の最初の関連付けに関する規則]

[割付: 属性の最初の関連付けに関する規則]: 該当プロセスを起動したプロセスのユーザ ID およびグループ ID が関連付けられる。

FIA_USB.1.3

TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: 属性の変更に関する規則]

[割付: 属性の変更に関する規則]:以下の規則がすべて適用される。

- 管理者はプロセスのユーザIDおよびグループIDを変更可能である。
- 利用者はその利用者を代行して動作するプロセスのユーザIDとユーザIDが一致するプロセスに対して、プロセスのグループIDを利用者が所属するグループIDへ変更可能である。
- setuidビット設定が有効であるファイルの実行に伴い起動されるプロセスのユーザ ID は、当該ファイルの所有者に変更される。
- setgidビット設定が有効であるファイルの実行に伴い起動されるプロセスのグループ ID は、当該ファイルの所有グループに変更される。

依存性: FIA_ATD.1 利用者属性定義

5.1.1.18 FMT_MOF.1(a) セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1(a)

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

[割付: 機能のリスト]: 監査データ記録機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]: のふるまいを決定する、を停止する

[割付: 許可された識別された役割]: 管理者

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

5.1.1.19 FMT_MOF.1(b) セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1(b)

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

[割付: 機能のリスト]: 監査データ格納機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]: のふるまいを決定する

[割付: 許可された識別された役割]: 管理者

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

5.1.1.20 FMT_MSA.1(a) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(a)

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

[割付: セキュリティ属性のリスト]: ファイルの所有グループ、ディレクトリの所有グループ、ファイルの所

有者のパーミッション、ディレクトリの所有者のパーミッション、ファイルの所有グループのパーミッション、ディレクトリの所有グループのパーミッション、ファイルのその他の利用者のパーミッション、ディレクトリのその他の利用者のパーミッション
[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]: デフォルト値変更
[割付: 許可された識別された役割]: 管理者
[割付: アクセス制御 SFP、情報フロー制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御

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

5.1.1.21 FMT_MSA.1(b) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(b)

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

[割付: セキュリティ属性のリスト]:ファイルの所有グループ、ディレクトリの所有グループ、ファイルの所有者のパーミッション、ディレクトリの所有者のパーミッション、ファイルの所有グループのパーミッション、ディレクトリの所有グループのパーミッション、ファイルのその他の利用者のパーミッション、ディレクトリのその他の利用者のパーミッション、ディレクトリのスティッキービット
[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]: 改変
[割付: 許可された識別された役割]: 管理者、所有者
[割付: アクセス制御 SFP、情報フロー制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御
依存性: [FDP_ACC.1 サブセットアクセス制御または FDP_IFC.1 サブセット情報フロー制御]、FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

5.1.1.22 FMT_MSA.1(c) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(c)

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

[割付: セキュリティ属性のリスト]: ファイルの所有者、ディレクトリの所有者、ext2/ext3 ファイルシステムのファイルのアトリビュート、ext2/ext3 ファイルシステムのディレクトリのアトリビュート
[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]: 改変
[割付: 許可された識別された役割]: 管理者
[割付: アクセス制御 SFP、情報フロー制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御、プロセスへの任意アクセス制御
依存性: [FDP_ACC.1 サブセットアクセス制御または FDP_IFC.1 サブセット情報フロー制御]、FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

5.1.1.23 FMT_MSA.3(a) 静的属性初期化

下位階層: なし

FMT_MSA.3.1(a)

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（ファイルの所有グループ、ディレクトリの所有グループ、ファイルの所有者のパーミッション、ディレクトリの所有者のパーミッション、ファイルの所有グループのパーミッション、ディレクトリの所有グループのパーミッション、ファイルのその他の利用者のパーミッション、ディレクトリのその他の利用者のパーミッション）**として、[選択: 制限的、許可的: から一つのみ選択、[割付: その他の特性]]デフォルト値を与える[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[選択: 制限的、許可的: から一つのみ選択、[割付: その他の特性]]: [割付: その他の特性]
[割付: その他の特性]: 管理者が設定した値
[割付: アクセス制御 SFP、情報フロー制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御

FMT_MSA.3.2(a)

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

[割付: 許可された識別された役割]: 所有者
依存性: FMT_MSA.1 セキュリティ属性の管理、FMT_SMR.1 セキュリティの役割

5.1.1.24 FMT_MSA.3(b) 静的属性初期化

下位階層: なし

FMT_MSA.3.1(b)

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（所有者、スティッキービット属性、ext2/ext3 ファイルシステムのファイルのアトリビュート、ext2/ext3 ファイルシステムのディレクトリのアトリビュート）**として、[選択: 制限的、許可的: から一つのみ選択、[割付: その他の特性]]デフォルト値を与える[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[選択: 制限的、許可的: から一つのみ選択、[割付: その他の特性]]: [割付: その他の特性]
[割付: その他の特性]:以下の規定値（①ファイルの所有者：ファイルを生成した利用者のユーザ ID、②ディレクトリの所有者：ディレクトリを生成した利用者のユーザ ID、③スティッキービット属性：無効、④ext2/ext3 ファイルシステムのファイルのアトリビュート：無効、④ext2/ext3 ファイルシステムのディレクトリのアトリビュート：無効）
[割付: アクセス制御 SFP、情報フロー制御 SFP]: ファイルおよびディレクトリへの任意アクセス制御

FMT_MSA.3.2(b)

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

[割付: 許可された識別された役割]:なし
依存性: FMT_MSA.1 セキュリティ属性の管理、FMT_SMR.1 セキュリティの役割

5.1.1.25 FMT_MTD.1(a) TSF データの管理

下位階層: なし

FMT_MTD.1.1(a)

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

[割付: TSF データのリスト]: ユーザ ID、グループ ID、グループ管理者
[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: 改変、削除、[割付: その他の操作]
[割付: その他の操作]: 登録
[割付:許可された識別された役割]: 管理者
依存性: FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

5.1.1.26 FMT_MTD.1(b) TSF データの管理

下位階層: なし

FMT_MTD.1.1(b)

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

[割付: TSF データのリスト]: 利用者のパスワード
[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: [割付: その他の操作]
[割付: その他の操作]: 登録
[割付:許可された識別された役割]: 管理者
依存性: FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

5.1.1.27 FMT_MTD.1(c) TSF データの管理

下位階層: なし

FMT_MTD.1.1(c)

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

[割付: TSF データのリスト]: 利用者のパスワード
[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: 改変
[割付:許可された識別された役割]: 管理者、該当利用者
依存性: FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

5.1.1.28 FMT_MTD.1(d) TSF データの管理

下位階層: なし

FMT_MTD.1.1(d)

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

[割付: TSF データのリスト]: 管理者のパスワード、パスワードの最小文字数、日付と時刻
[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: 改変

[割付:許可された識別された役割]: 管理者

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

下位階層: なし

5.1.1.29 FMT_MTD.1(e) TSF データの管理

下位階層: なし

FMT_MTD.1.1(e)

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

[割付: TSF データのリスト]: グループに所属する利用者

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: 改変、削除[割付: その他の操作]

[割付: その他の操作]: 登録

[割付:許可された識別された役割]: 管理者、該当グループ管理者

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

5.1.1.30 FMT_MTD.1(f) TSF データの管理

下位階層: なし

FMT_MTD.1.1(f)

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

[割付: TSF データのリスト]: setuid ビット設定、setgid ビット設定

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]: 改変

[割付:許可された識別された役割]: 管理者、所有者

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

5.1.1.31 FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付: TSF によって提供されるセキュリティ管理機能のリスト]。

[割付: TSF によって提供されるセキュリティ管理機能のリスト]: 次のセキュリティ管理機能のリストを提供する。

- 管理者による監査データ記録機能のふるまいの決定および停止
- 管理者による監査データ格納機能のふるまいの決定
- 管理者によるファイルの所有者のパーミッションのデフォルト値変更
- 管理者によるディレクトリの所有者のパーミッションのデフォルト値変更
- 管理者によるファイルの所有グループのパーミッションのデフォルト値変更
- 管理者によるディレクトリの所有グループのパーミッションのデフォルト値変更
- 管理者によるファイルのその他の利用者のパーミッションのデフォルト値変更
- 管理者によるディレクトリのその他の利用者のパーミッションのデフォルト値変更
- 管理者によるファイルの所有者グループの改変
- 管理者によるディレクトリの所有者グループの改変
- 管理者によるファイルの所有者のパーミッションの改変
- 管理者によるディレクトリの所有者のパーミッションの改変
- 管理者によるファイルの所有グループのパーミッションの改変
- 管理者によるディレクトリの所有グループのパーミッションの改変
- 管理者によるファイルのその他の利用者のパーミッションの改変
- 管理者によるディレクトリのその他の利用者のパーミッションの改変
- 所有者によるファイルの所有者グループの改変
- 管理者によるディレクトリのスティッキービットの改変
- 所有者によるディレクトリの所有者グループの改変
- 所有者によるファイルの所有者のパーミッションの改変
- 所有者によるディレクトリの所有者のパーミッションの改変
- 所有者によるファイルの所有グループのパーミッションの改変
- 所有者によるディレクトリの所有グループのパーミッションの改変
- 所有者によるファイルのその他の利用者のパーミッションの改変
- 所有者によるディレクトリのその他の利用者のパーミッションの改変
- 所有者によるディレクトリのスティッキービットの改変
- 管理者によるファイルの所有者の改変
- 管理者によるディレクトリの所有者の改変
- 管理者によるext2/ext3ファイルシステムのファイルのアトリビュートの改変
- 管理者によるext2/ext3ファイルシステムのディレクトリのアトリビュートの改変

- 管理者によるユーザIDの改変
- 管理者によるユーザIDの削除
- 管理者によるユーザIDの登録
- 管理者によるグループIDの改変
- 管理者によるグループIDの削除
- 管理者によるグループIDの登録
- 管理者によるグループ管理者の改変
- 管理者によるグループ管理者の削除
- 管理者によるグループ管理者の登録
- 管理者によるグループに所属する利用者の改変
- 管理者によるグループに所属する利用者の削除
- 管理者によるグループに所属する利用者の登録
- 該当グループ管理者によるグループに所属する利用者の改変
- 該当グループ管理者によるグループに所属する利用者の削除
- 該当グループ管理者によるグループに所属する利用者の登録
- 管理者による利用者のパスワードの登録
- 管理者による利用者のパスワードの改変
- 該当利用者による利用者のパスワードの改変
- 管理者による管理者のパスワードの改変
- 管理者によるパスワードの有効長改変
- 管理者による日付と時刻の改変
- 所有者によるファイルの setuid ビット設定の改変
- 管理者によるファイルの setuid ビット設定の改変
- 所有者によるファイルの setgid ビット設定の改変
- 管理者によるファイルの setgid ビット設定の改変

依存性: なし

5.1.1.32 FMT_SMR.1(a) セキュリティ役割

下位階層: なし

FMT_SMR.1.1(a)

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

[割付: 許可された識別された役割]: 管理者

FMT_SMR.1.2(a)

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.33 FMT_SMR.1(b) セキュリティ役割

下位階層: なし

FMT_SMR.1.1(b)

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

[割付: 許可された識別された役割]: 該当利用者

FMT_SMR.1.2(b)

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.34 FMT_SMR.1(c) セキュリティ役割

下位階層: なし

FMT_SMR.1.1(c)

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

[割付: 許可された識別された役割]: 所有者

FMT_SMR.1.2(c)

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.35 FMT_SMR.1(d) セキュリティ役割

下位階層: なし

FMT_SMR.1.1(d)

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

[割付: 許可された識別された役割]: 該当グループ管理者

FMT_SMR.1.2(d)

TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.36 FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1

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

依存性: なし

5.1.1.37 FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1

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

FPT_SEP.1.2

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

依存性: なし

5.1.1.38 FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1

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

依存性: なし

5.1.2. 機能強度

本TOE の最小機能強度レベルは、SOF-基本である。確率的、順列的メカニズムを利用するTOE セキュリティ機能要件は、上述の FIA_SOS.1、FIA_UAU.2、FIA_UAU.6 であり、機能強度レベルは SOF-基本である。

5.1.3. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL1 である。保証要件コンポーネントは ACM_CAP.1、ADO_IGS.1、ADV_FSP.1、ADV_RCR.1、AGD_ADM.1、AGD_USR.1、ATE_IND.1 であり、すべての保証要件コンポーネントは CC パート 3 で規定されている EAL1 のコンポーネントを直接使用する。

5.2. IT 環境セキュリティ要件

TOE の IT 環境が満たすべきセキュリティ要件はない。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

6.1.1. 識別/認証

6.1.1.1 識別/認証 (IA.1)

TSF は、利用者および管理者が TOE へアクセスする前に必ず識別/認証を要求する。識別はユーザ ID に基づいて実施され、認証はユーザ ID に対するパスワード認証メカニズムによって実施される。また、パスワード漏洩対策のため、パスワード入力時は画面には入力に対するフィードバックは何も表示しない。

6.1.1.2 識別/認証の管理 (IA.2)

ユーザ ID の登録、削除、改変の操作は管理者のみに制限される。全ての利用者のパスワード登録は管理者のみに制限され、利用者は自身のパスワードのみを改変可能であり、管理者は自身および全ての利用者のパスワードを改変可能である。ただし、利用者が自身のパスワードを改変する際には、パスワード認証メカニズムにより再認証を要求する。パスワードは一定の品質を保つために一定の文字数以上を必要とし、その最小文字数の設定は管理者のみが変更可能である。

6.1.2. 任意アクセス制御

任意アクセス制御は、サブジェクトとオブジェクト間のアクセス制御を規定し、サブジェクトは常にプロセスであるが、オブジェクトは以下の 2 つが存在する。

- ファイルおよびディレクトリ
- プロセス

6.1.2.1 ファイルおよびディレクトリへの任意アクセス制御 (DAC.1)

オブジェクトがファイルおよびディレクトリの場合、ファイルおよびディレクトリは以下のセキュリティ属性を保持する。

＜ファイル＞

- ファイルの所有者
- ファイルの所有グループ

- ファイルの所有者のパーミッション
- ファイルの所有グループのパーミッション
- ファイルのその他の利用者のパーミッション
- ext2/ext3 ファイルシステムのファイルのアトリビュート（追加書き込み、変更不可）

＜ディレクトリ＞

- ディレクトリのスティッキービット
- ディレクトリの所有者
- ディレクトリの所有グループ
- ディレクトリの所有者のパーミッション
- ディレクトリの所有グループのパーミッション
- ディレクトリのその他の利用者のパーミッション
- ext2/ext3 ファイルシステムのディレクトリのアトリビュート（変更/削除不可、変更不可）

プロセスは、セキュリティ属性としてユーザ ID とグループ ID を保持する。これらセキュリティ属性と、上記のオブジェクトのセキュリティ属性に基づき、以下のアクセス制御規則を実施する。

- プロセスのユーザIDが、該当ファイルまたはディレクトリの所有者と一致する場合、当該ファイルまたはディレクトリの所有者のパーミッションにて設定されている許可される操作が許可される。
- プロセスのグループ ID が該当ファイルまたはディレクトリの所有グループと一致する場合、当該ファイルまたはディレクトリの所有グループのパーミッションにて設定されている許可される操作が許可される。
- プロセスのユーザ ID、グループ ID に関わらず、該当ファイルまたはディレクトリのその他の利用者のパーミッションにて設定されている許可される操作が許可される。
- 該当ディレクトリに存在するファイルまたはディレクトリは、該当ディレクトリの所有グループのパーミッション、該当ディレクトリのその他の利用者のパーミッションによって、該当ディレクトリのディレクトリおよびファイルの生成/変更/削除が許可されていたとしても、スティッキービット属性が有効である場合は削除操作が拒否される。
- ext2/ext3 ファイルシステムのファイルのアトリビュート（追加書き込み）が有効である場合、該当ファイルのパーミッションによって該当ファイルの書き込み/追加書込み操作が許可されている場合でも、追加書き込み操作だけに限定される。プロセスのユーザIDが管理者であっても、追加書き込み操作だけに限定される。
- ext2/ext3 ファイルシステムのディレクトリのアトリビュート（変更/削除不可）が有効である場合、該当ディレクトリのパーミッションによって該当ディレクトリにおけるディレクトリまたはファイルの生成/変更/削除操作が許可されている場合でも生成操作だけに限定される。プロセスのユーザ ID が管理者であっても、生成操作だけに限定される。
- ext2/ext3 ファイルシステムのファイルのアトリビュート（変更不可）が有効である場合、該当ファ

イルのパーミッションによって該当ファイルの書き込み/追加書き込み操作が許可されている場合でも、書き込み/追加書き込み操作が拒否される。プロセスのユーザIDが管理者であっても同様に拒否される。

- ext2/ext3ファイルシステムのディレクトリのアトリビュート(変更不可)が有効である場合、該当ディレクトリのパーミッションによって該当ディレクトリの生成/変更/削除操作が許可されている場合でも、生成/変更/削除操作が拒否される。プロセスのユーザIDが管理者であっても同様に拒否される。

ファイルの生成時においては、管理者が設定する以下のセキュリティ属性が付与される。

- ファイルの所有グループ
- ファイルの所有者のパーミッション
- ファイルの所有グループのパーミッション
- ファイルのその他の利用者のパーミッション

上記のセキュリティ属性はファイルを所有することになる所有者が、代替の初期値を設定することができる。

その他のセキュリティ属性は以下に示す値が設定される。

- 所有者: そのファイル、ディレクトリを生成したユーザ
- ext2/ext3 ファイルシステムのアトリビュート: 無効

ディレクトリの生成時において管理者が設定する以下のセキュリティ属性が付与される。

- ディレクトリの所有グループ
- ディレクトリの所有者のパーミッション
- ディレクトリの所有グループのパーミッション
- ディレクトリのその他の利用者のパーミッション

上記のセキュリティ属性はディレクトリを所有することになる所有者が、代替の初期値を設定することができる。

その他のセキュリティ属性は以下に示す値が設定される。

- 所有者: そのファイル、ディレクトリを生成したユーザ
- スティッキービット: 無効
- ext2/ext3 ファイルシステムのアトリビュート: 無効

ファイルにはデバイスファイル、UNIX ドメインソケット、名前付きパイプ、シンボリックリンクなど特殊なものが存在するが、これらは全て通常のファイルと同様の任意アクセス制御に基づいてアクセスが規定されるが、ext2/ext3 ファイルシステムのアトリビュートは保持しない。また、メモリ上のオブジェクトである

IPC オブジェクト(共有メモリ、メッセージキュー、セマフォ)も、ファイルと同様の任意アクセス制御によりアクセスが規定されるが、実行パーミッションのセキュリティ属性は保持しない。

6.1.2.2 プロセスへの任意アクセス制御 (DAC.2)

全てのプロセスは、ユーザ ID を保持する。プロセスから他のプロセスおよびプロセスが保持するデータオブジェクトへのアクセス制御には、ユーザ ID だけが用いられ、サブジェクトのプロセスとオブジェクトのプロセスの関係は次のいずれかとなる。

- サブジェクトのプロセスのユーザ ID とオブジェクトのプロセスまたはプロセスが保持するデータオブジェクトのユーザ ID が一致する。
- サブジェクトのプロセスのユーザIDとオブジェクトのプロセスまたはプロセスが保持するデータオブジェクトのユーザIDが一致しない。

ユーザ ID が一致する場合、サブジェクトのプロセスはサブジェクト以外のプロセスに対して停止、復帰、削除、またはサブジェクト以外のプロセスが保持するデータオブジェクトへの読み込み、書き込みの操作を実行可能である。管理者はユーザ ID の値に依存せず、すべてのプロセスに対して上記操作が実行可能である。

6.1.2.3 セキュリティ属性の管理 (DAC.3)

サブジェクト、オブジェクトともに、プロセスのセキュリティ属性であるユーザ ID およびグループ ID は、そのプロセスを起動した利用者または管理者のユーザ ID、グループ ID が利用される。新しく生成するプロセスが、setuidビット設定が有効であるファイルの実行に伴うものであれば、プロセスのユーザ ID は当該ファイルの所有者に設定変更される。また新しく生成するプロセスが、setgid ビットが有効であるファイルの実行に伴うものであれば、プロセスのグループ ID は当該ファイルの所有グループに設定変更される。

管理者は、プロセスのセキュリティ属性を改変可能である。利用者は、利用者を代行するプロセスのユーザ ID と一致するユーザ ID を持つプロセスに対して、グループ ID を利用者が所属するグループ ID へ変更可能である。setuid ビット設定、setgid ビット設定は、管理者及び所有者が改変可能である。

ファイルおよびディレクトリのセキュリティ属性は、所有者である場合、所有グループ、スティッキービットを含む各パーミッションを改変可能であり、管理者は所有者、所有グループ、スティッキービットを含む各パーミッション、ext2/ext3 ファイルシステムのアトリビュートを改変可能である。また、管理者は利用者によってファイルおよびディレクトリが生成される際に付与される所有グループ、所有者のパーミッション、所有グループのパーミッション、その他の利用者のパーミッションのデフォルト値を設定可能であり、所有者となる利用者は、これらを上書きする代替の初期値を設定可能である。管理者はファイルおよびディレクトリの所有者を改変可能である。

グループ ID の登録、削除、改変の操作は管理者のみに制限される。グループに所属する利用者の改変、

削除、登録は管理者および該当グループ管理者に制限され、グループ管理者の改変、削除、登録は管理者のみに制限される。

6.1.3. 監査

6.1.3.1 監査記録の生成 (AU.1)

TOE は制御下で発生する監査事象の監査記録を生成する。監査事象は以下の通りである。

- 監査の起動と終了
- 利用者のログインにあたっての認証の成功および失敗
- 利用者のログイン中の利用者切り替えにあたっての認証の成功および失敗
- 管理者のログインにあたっての認証の成功および失敗
- 利用者のパスワード変更にあたっての再認証の失敗
- 利用者のログインにあたっての識別の成功および失敗
- 管理者のログインにあたっての識別の成功および失敗

TOE は、すべての監査事象に対して事象の日付/時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、その原因となった利用者の識別情報を記録することができる。監査記録に使用される日付/時刻は、TOE が提供する。

6.1.3.2 監査記録の閲覧 (AU.2)

監査記録は、管理者が閲覧可能な形式で提供され、管理者のみが閲覧可能である。TOE は監査分析のために事象の日付/時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)に基づいた検索、分類、並び替えのツールを提供する。

6.1.3.3 監査記録の管理 (AU.3)

監査記録のファイルは管理者のみが読み込み、書き込み可能なパーミッションで生成され、不正な改変から防止している。記録する監査事象の粒度や事象種別、生成するファイル名の設定は管理者のみが変更可能である。管理者は監査記録消失の恐れに対しファイルの最大容量を設定可能であり、この設定を超えた場合には最も古い監査記録を削除し、新しい監査記録を生成する。監査機能は管理者のみが停止可能である。日付/時刻は、管理者のみが変更可能である。

6.1.4. プロセスの分離 (PS.1)

プロセスは生成時に独立したアドレス空間を割当てられ、互いのアドレス空間は保護されており干渉しない。

6.1.5. TSF 実施 (TI.1)

TOEによって管理されているオブジェクトにアクセスするためには、利用者、管理者に関わらず、ログインによる識別/認証を行う必要がある。

6.2. セキュリティ機能強度

確率的、順列的メカニズムによって実現されるセキュリティ機能は識別/認証(IA.1～IA.2)である。識別/認証(IA.1～IA.2)の機能強度は SOF-基本である。

6.3. 保証手段

以下のドキュメントを保証手段として提供する。

表 7 :保証要件コンポーネントとドキュメントの対応関係

保証コンポーネント		ドキュメント名称
ACM_CAP.1	バージョン管理	・ MIRACLE LINUX V4.0 ・ MIRACLE LINUX V4.0 One ・ MIRACLE LINUX V4.0 x86-64 ・ MIRACLE LINUX V4.0 x86-64 One 上記の各製品梱包物一覧
ADO_IGS.1	設置、生成、及び立上げ手順	MIRACLE LINUX インストレーションガイド (2005 年 10 月 1 日)
ADV_FSP.1	非形式的機能仕様	MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64/ MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム 機能仕様書
ADV_RCR.1	非形式的対応の実証	MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64/ MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム セキュリティ機能対応一覧
AGD_ADM.1	管理者ガイダンス	MIRACLE LINUX V4.0 セキュリティガイダンス (2006 年 12 月 20 日)
AGD_USR.1	利用者ガイダンス	
ATE_IND.1	独立テスト - 準拠	TOEテスト環境一式

7. PP 主張

本 ST において適合する PP は存在しない。

8. 根拠

8.1. セキュリティ対策方針根拠

この章では、4 章で記述されたセキュリティ対策方針が、3 章のセキュリティ方針を実現することを実証する。

表 8 に、各セキュリティ対策方針が少なくとも 1 つの組織のセキュリティ方針あるいは前提条件を扱い、かつ、各組織のセキュリティ方針および前提条件が少なくとも 1 つのセキュリティ対策方針によって扱われていることを示す。

表 8 : セキュリティ対策方針と組織のセキュリティ方針の相対

	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS.1	O.DISCRETIONARY_ACCESS.2	O.AUDITING	O.LOG_SIZE	O.ADMINISTRATOR	O.PHYSICAL	O.CREDENTIAL
P.AUTHORISED_USERS	X							
P.NEED_TO_KNOW.1		X						
P.NEED_TO_KNOW.2			X					
P.ACCOUNTABILITY				X				
P.LOG_SIZE					X			
A.LOCATE							X	
A.MANAGE						X		
A.PASSWORD								X

P.AUTHORISED_USERS は、O.AUTHORIZATION によって実施される。なぜならば、認証を経由した利用者のみが TOE が管理する情報にアクセス可能となるからである。

P.NEED_TO_KNOW.1 は、O.DISCRETIONARY_ACCESS.1 によって実施される。なぜならば、TSF は、セキュリティ属性に基づきファイルおよびディレクトリへのアクセス制御を実施し、また、ファイルおよびディレクトリの所有者が該当ファイルおよびディレクトリのセキュリティ属性を管理することを許可するからであ

る。

P.NEED_TO_KNOW.2 は、O.DISCRETIONARY_ACCESS.2 によって実施される。なぜならば、TSF はプロセスへのアクセスを該当プロセスの所有者および管理者のみに制限し、また、プロセスのセキュリティ属性の管理を管理者のみに制限するからである。

P.ACCOUNTABILITY は、O.AUDITING によって実施される。なぜならば、TSF は利用者の識別/認証の監査証跡を記録し、管理者に提示するからである。

P.LOG_SIZE は、O.LOG_SIZE によって実施される。なぜならば、TSF は管理者が設定した容量で監査記録を定期的にローテーションするからである。

A.ALOCATE は、O.PHYSICAL によって実現される。なぜならば、TOE の責任者は、TOE を物理的な攻撃から保護される設備内に設置するからである。

A.MANAGE は、O.ADMINISTRATOR によって実現される。なぜならば、TOE の責任者は、悪意のない管理者を任命するからである。

A.PASSWORD は、O.CREDENTIAL によって実現される。なぜならば、管理者および許可された利用者のパスワードが、安易に推測可能ではなく、自身が設定を行い、定期的に変更するからである。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

この章では、セキュリティ機能要件がセキュリティ対策方針を実現することを実証する。セキュリティ対策方針の中で、O.ADMINISTRATOR、O.PHYSICAL、O.CREDENTIAL は運用に対するものである。表 9 に TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を示す。

表 9 : セキュリティ対策方針とセキュリティ機能の対応

	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS.1	O.DISCRETIONARY_ACCESS.2	O.AUDITING	O.LOG_SIZE
FAU_GEN.1				X	
FAU_SAR.1				X	

FAU_SAR.2				X	
FAU_SAR.3				X	
FAU_STG.1				X	
FAU_STG.3					X
FDP_ACC.1(a)		X			
FDP_ACC.1(b)			X		
FDP_ACF.1(a)		X			
FDP_ACF.1(b)			X		
FIA_ATD.1		X	X		
FIA_SOS.1	X				
FIA_UAU.2	X				
FIA_UAU.6	X				
FIA_UAU.7	X				
FIA_UID.2	X				
FIA_USB.1		X	X		
FMT_MOF.1(a)				X	
FMT_MOF.1(b)					X
FMT_MSA.1(a)		X			
FMT_MSA.1(b)		X			
FMT_MSA.1(c)		X			
FMT_MSA.3(a)		X			
FMT_MSA.3(b)		X			
FMT_MTD.1(a)	X	X	X		
FMT_MTD.1(b)	X				
FMT_MTD.1(c)	X				
FMT_MTD.1(d)	X			X	
FMT_MTD.1(e)		X			
FMT_MTD.1(f)		X			
FMT_SMF.1	X	X	X	X	X
FMT_SMR.1(a)	X	X	X	X	X

FMT_SMR.1(b)	X				
FMT_SMR.1(c)		X			
FMT_SMR.1(d)		X			
FPT_RVM.1	X				
FPT_SEP.1		X	X		
FPT_STM.1				X	

8.2.1.1 O.AUTHORIZATION

TOE へアクセスするためには、FIA_UAU.2 および FIA_UID.2 により、識別/認証を行わなければならない。これは FPT_RVM.1 により確実に実施される。

認証の際にはパスワードが用いられるが、FIA_SOS.1 によりパスワードは管理者が定めた品質尺度を満たすものだけが利用でき、FIA_UAU.7 によりパスワード入力時は、画面には入力に対するフィードバックを何も表示しない。

識別に利用されるユーザ ID の登録、改変、削除は、FMT_MTD.1(a)により管理者のみに制限される。認証に利用される利用者のパスワードの登録は、FMT_MTD.1(b)により管理者のみに制限され、FMT_MTD.1(c)により利用者のパスワード改変は該当利用者または管理者のみに制限され、FMT_MTD.1(d)により管理者のパスワード改変は管理者のみに制限される。利用者が自身のパスワードを変更する際には、FIA_UAU.6 により際認証が要求される。また、パスワードの品質尺度の設定の改変は FMT_MTD.1(d)により管理者のみが行うことができる。これらの管理役割は FMT_SMR.1(a)および FMT_SMR.1(b)により規定され、管理機能は FMT_SMF.1 により特定される。

以上のことから、O.AUTHORIZATION は達成される。

8.2.1.2 O.DISCRETIONARY_ACCESS.1

TOE 上で動作するプロセスから TOE が管理するファイルおよびディレクトリへのアクセス制御は、FDP_ACC.1(a)により実施可能な操作種別が規定され、FDP_ACF.1(a)によりその操作を実行するために必要なセキュリティ属性の一覧および許可規則が規定される。

利用者を代行して動作するプロセスのセキュリティ属性であるユーザ ID およびグループ ID は FIA_ATD.1 によって規定される。セキュリティ属性とプロセスの関連付けは、FIA_USB.1 によりプロセスを起動した利用者のセキュリティ属性が適用される。またプロセスに関連付けられたセキュリティ属性の変更管理は同じく FIA_USB.1 により、管理者が任意の値に変更可能、利用者が利用者を代行するプロセスのユーザ ID に基づいて所属するグループ ID へ変更可能、setuid ビット設定、setgid ビット設定が有効なファイルを実行した場合の規則が規定される。

ファイルおよびディレクトリのセキュリティ属性は、FMT_MSA.1(a)により所有グループ、所有者のパーミッション、所有グループのパーミッション、その他の利用者のパーミッションのデフォルト値の変更を管理者のみに制限され、FMT_MSA.1(b)により所有グループ、所有者のパーミッション、所有グループのパーミッション、その他の利用者のパーミッションの改変を管理者または所有者に制限され、FMT_MSA.1(c)により所有者の改変を管理者のみに制限される。

FMT_MSA.3(a)によりファイルおよびディレクトリの所有グループ、所有者のパーミッション、所有グループのパーミッション、その他の利用者のパーミッションは、管理者が指定する値がデフォルト値として与えられる。またこの値に変わる初期値は、同要件により当該ファイル、ディレクトリを生成した所有者に設定を制限している。また FMT_MSA.3(b)により、この他のセキュリティ属性（ファイル及び ext2/ext3 ファイルシステムのディレクトリのアトリビュート、ファイル及びディレクトリの所有者、スティッキービット属性）は、規定値がデフォルト値として与えられ、これに変わる初期値を設定することはできない。

FMT_MTD.1(a)により、ユーザ ID、グループ ID、グループ管理者の登録、改変、削除操作が管理者のみに制限される。また FMT_MTD.1(e)により、グループに所属する利用者の登録、改変、削除操作は、管理者及び当該グループ管理者に制限される。FMT_MTD.1(f)により、setuid ビット設定、setgid ビット設定の改変が管理者及び所有者に制限される。

これらの管理役割は FMT_SMR.1(a)、FMT_SMR.1(c)、FMT_SMR.1(d)により規定され、管理機能は FMT_SMF.1 により特定される。

各プロセスが独立しており、互いに干渉しないことは、FPT_SEP.1 により規定される。

以上のことから、O.DISCRETIONARY_ACCESS.1 は達成される。

8.2.1.3 O.DISCRETIONARY_ACCESS.2

TOE 上で動作するプロセスから、TOE 上で動作する他のプロセスまたはプロセスが保持するデータオブジェクトへのアクセス制御は、FDP_ACC.1(b)により実行可能な操作種別が規定され、FDP_ACF.1(b)によりその操作を実行するために必要なセキュリティ属性の一覧および許可規則が規定される。

利用者を代行して動作するプロセスのセキュリティ属性であるユーザ ID は FIA_ATD.1 によって規定される。セキュリティ属性とプロセスの関連付けは、FIA_USB.1 によりプロセスを起動した利用者のセキュリティ属性が適用される。またプロセスに関連付けられたセキュリティ属性の変更管理は同じく FIA_USB.1 により、管理者が任意の値に変更可能、利用者が利用者を代行するプロセスのユーザ ID に基づいて所属するグループ ID へ変更可能、setuid ビット設定、setgid ビット設定が有効なファイルを実行した場合の規則が規定される。

FMT_MTD.1(a)により、ユーザ ID の登録、改変、削除操作が管理者のみに制限される。

これらの管理役割は FMT_SMR.1(a)により規定され、管理機能は FMT_SMF.1 により特定される。

各プロセスが独立しており、互いに干渉しないことは、FPT_SEP.1 により規定される。

以上のことから、O.DISCRETIONARY_ACCESS.2 は達成される。

8.2.1.4 O.AUDITING

TSF は、FAU_GEN.1 により、利用者および管理者のパスワード変更の失敗および成功、利用者のパスワード変更時の際認証の成功および失敗、利用者および管理者のログイン時の識別/認証の成功および失敗を、事象の日付と時刻、種別、サブジェクト識別情報、事象の結果とともに監査記録を生成する。監査記録の日付と時刻に利用されるシステム時間は FPT_STM.1 によって提供され、変更は FMT_MTD.1(d)により管理者のみに制限される。監査記録機能のふるまいの改変、および停止は FMT_MOF.1(a)により管理者に制限される。

監査記録の閲覧は、FAU_SAR.1 により適切な情報形態にして管理者が閲覧を行う。監査記録へのアクセスは FAU_SAR.2 により読み出しを管理者のみに制限される。FAU_SAR.3 によりそれぞれの記録内容について検索、分類、並べ替えを行うことができる。また、FAU_STG.1 により監査記録の削除を管理者のみに制限し、不正な改変を防止する。

これらの管理役割は FMT_SMR.1(a)により規定され、管理機能は FMT_SMF.1 により特定される。

以上のことから、O.AUDITING は達成される。

なお、監査レベルとして指定なしを選択しており、具体的には識別/認証に関係する監査対象事象が選択されているが、O.AUDITING は、識別/認証のみを監査対象事象として要求しているためセキュリティ対策方針は達成される。

8.2.1.5 O.LOG_SIZE

TSF は FAU_STG.3 により監査証跡のファイルサイズと格納期間を超えた場合に最も古い監査証跡を削除する機能を有し、ファイルサイズおよび格納期間の設定の改変は FMT_MOF.1(b)により管理者のみに制限される。

この管理役割は FMT_SMR.1(a)により規定され、管理機能は FMT_SMF.1 により特定される。

以上のことから、O.LOG_SIZE は達成される。

8.2.2. 最小機能強度レベルの根拠

本 TOE は物理的なアクセスを防ぐ施設内に設置され、管理者、利用者に悪意がなく、パスワードが漏洩しないことを前提としているため、TOE の最小機能強度レベルとして SOF-基本は妥当である。

8.2.3. 保証要件の根拠

本 TOE は、物理的に保護された設備に設置され、責任者が悪意のない管理者を任命し、利用者は自身の管理下にあるオブジェクトに対し悪意のある行動を取らないことから、保証要件として EAL1 は妥当である。

8.2.4. セキュリティ機能要件の依存性根拠

セキュリティ機能要件の依存性根拠を表 10 に示す。

表 10 : 機能コンポーネント間の依存関係

	セキュリティ機能要件	依存するセキュリティ要件	参照先項番
1	FAU_GEN.1	FPT_STM.1	37
2	FAU_SAR.1	FAU_GEN.1	1
3	FAU_SAR.2	FAU_SAR.1	2
4	FAU_SAR.3	FAU_SAR.1	2
5	FAU_STG.1	FAU_GEN.1	1
6	FAU_STG.3	FAU_STG.1	5
7	FDP_ACC.1(a)	FDP_ACF.1	9
8	FDP_ACC.1(b)	FDP_ACF.1	10
9	FDP_ACF.1(a)	FDP_ACC.1	7
		FMT_MSA.3(a)	23
10	FDP_ACF.1(b)	FDP_ACC.1	8
		FMT_MSA.3(a)	満たさない ※下記(1)参照
11	FIA_ATD.1	―	―
12	FIA_SOS.1	―	―
13	FIA_UAU.2	FIA_UID.1	16
14	FIA_UAU.6	―	―
15	FIA_UAU.7	FIA_UAU.1	13
16	FIA_UID.2	―	―
17	FIA_USB.1	FIA_ATD.1	11
18	FMT_MOF.1(a)	FMT_SMF.1	31
		FMT_SMR.1	32

19	FMT_MOF.1(b)	FMT_SMF.1	31
		FMT_SMR.1	32
20	FMT_MSA.1(a)	FDP_ACC.1 または FDP_IFC.1	7
		FMT_SMF.1	31
		FMT_SMR.1	32
21	FMT_MSA.1(b)	FDP_ACC.1 または FDP_IFC.1	7
		FMT_SMF.1	31
		FMT_SMR.1	32、33
22	FMT_MSA.1(c)	FDP_ACC.1 または FDP_IFC.1	7
		FMT_SMF.1	31
		FMT_SMR.1	32
23	FMT_MSA.3(a)	FMT_MSA.1	20、21、22
		FMT_SMR.1	32
24	FMT_MSA.3(b)	FMT_MSA.1	満たさない ※下記(2)参照
		FMT_SMR.1	
25	FMT_MTD.1(a)	FMT_SMF.1	31
		FMT_SMR.1	32
26	FMT_MTD.1(b)	FMT_SMF.1	31
		FMT_SMR.1	32
27	FMT_MTD.1(c)	FMT_SMF.1	31
		FMT_SMR.1	32、33
28	FMT_MTD.1(d)	FMT_SMF.1	31
		FMT_SMR.1	32
29	FMT_MTD.1(e)	FMT_SMF.1	31
		FMT_SMR.1	32、35
30	FMT_MTD.1(f)	FMT_SMF.1	31
		FMT_SMR.1	32、34
31	FMT_SMF.1	―	―
32	FMT_SMR.1(a)	FIA_UID.1	16
33	FMT_SMR.1(b)	FIA_UID.1	16

34	FMT_SMR.1(c)	FIA_UID.1	16
35	FMT_SMR.1(d)	FIA_UID.1	16
36	FPT_RVM.1	―	―
37	FPT_SEP.1	―	―
38	FPT_STM.1	―	―

(1) FDP_ACF.1(b)に示されるサブジェクト、オブジェクトであるプロセスのセキュリティ属性の関連付けは、FIA_USB.1 によって初期関連付け、変更まで規定されるため、FMT_MSA.3(a)の依存関係を満たさなくとも、必要事項は十分、セキュリティ機能要件に提示されており、適用の必要はない。

(2) FMT_MSA.3(b)は、FMT_MSA.3.2(b)にて役割の割付がないため、役割維持に関する依存性は存在せず、適用の必要はない。

8.2.5. TOE セキュリティ機能要件の相互サポート

セキュリティ機能要件の相互サポートを表 11 に示す。

表 11 : 機能コンポーネント間の依存関係

	セキュリティ機能要件	バイパス防止	干渉防止	非活性化防止	無効化攻撃の検出
1	FAU_GEN.1	―	―	FAU_STG.1 FAU_STG.3 FMT_MOF.1(a)	―
2	FAU_SAR.1	―	―	―	―
3	FAU_SAR.2	―	―	―	―
4	FAU_SAR.3	―	―	―	―
5	FAU_STG.1	―	―	―	―
6	FAU_STG.3	―	―	―	―
7	FDP_ACC.1(a)	―	―	―	―
8	FDP_ACC.1(b)	―	―	―	―
9	FDP_ACF.1(a)	FIA_UAU.2 FIA_UID.2	FMT_MSA.1(a) FMT_MSA.1(b) FMT_MSA.1(c) FMT_MTD.1(e) FPT_SEP.1	―	―
10	FDP_ACF.1(b)	FIA_UAU.2 FIA_UID.2	FMT_MSA.1(c) FMT_MTD.1(e) FPT_SEP.1	―	―
11	FIA_ATD.1	―	―	―	―

12	FIA_SOS.1	—	—	—	—
13	FIA_UAU.2	FPT_RVM.1	FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c) FMT_MTD.1(d)	—	—
14	FIA_UAU.6	FPT_RVM.1	FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c) FMT_MTD.1(d)	—	—
15	FIA_UAU.7	—	—	—	—
16	FIA_UID.2	FPT_RVM.1	FMT_MTD.1(a)	—	—
17	FIA_USB.1	—	FMT_MTD.1(f)	—	—
18	FMT_MOF.1(a)	—	—	—	—
19	FMT_MOF.1(b)	—	—	—	—
20	FMT_MSA.1(a)	—	—	—	—
21	FMT_MSA.1(b)	—	—	—	—
22	FMT_MSA.1(c)	—	—	—	—
23	FMT_MSA.3(a)	—	—	—	—
24	FMT_MSA.3(b)	—	—	—	—
25	FMT_MTD.1(a)	—	—	—	—
26	FMT_MTD.1(b)	—	—	—	—
27	FMT_MTD.1(c)	—	—	—	—
28	FMT_MTD.1(d)	—	—	—	—
29	FMT_MTD.1(e)	—	—	—	—
30	FMT_MTD.1(f)	—	—	—	—
31	FMT_SMF.1	—	—	—	—
32	FMT_SMR.1(a)	—	—	—	—
33	FMT_SMR.1(b)	—	—	—	—
34	FMT_SMR.1(c)	—	—	—	—
35	FMT_SMR.1(d)	—	—	—	—
36	FPT_RVM.1	—	—	—	—
37	FPT_SEP.1	—	—	—	—
38	FPT_STM.1	—	FMT_MTD.1(d)	—	—

8.2.5.1 バイパス防止

FDP_ACF.1(a)、FDP_ACF.1(b)は、サブジェクトのセキュリティ属性を決定するために、そのプロセスを起動した利用者および管理者が識別/認証されている必要があるが、これは FIA_UAU.2 および FIA_UID.2 により実施される。

FIA_UAU.2 は、利用者および管理者が TOE にアクセスする際に実施されなければならないが、これは FPT_RVM.1 により実施される。

FIA_UAU.6 は、利用者および管理者がパスワードを変更する際に実施されなければならないが、これは FPT_RVM.1 により実施される。

FIA_UID.2 は、利用者および管理者が TOE にアクセスする際に実施されなければならないが、これは FPT_RVM.1 により実施される。

8.2.5.2 干渉防止

FDP_ACF.1(a)、は、サブジェクトおよびオブジェクトのセキュリティ属性によってアクセス制御を行うが、各セキュリティ属性の改変は FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MSA.1(c)、FMT_MTD.1(e)によって制限されており、干渉から保護される。また、他の信頼できないサブジェクトによる干渉や改竄から保護される必要があるが、これは FPT_SEP.1 により実施される。

FDP_ACF.1(b)は、サブジェクトおよびオブジェクトのユーザ ID によってアクセス制御を行うが、各ユーザ ID およびグループ ID の改変は FMT_MSA.1(c)によって制限されており、またグループに所属する利用者の改変は、FMT_MTD.1(e)によって制限されているため、干渉から保護される。また、他の信頼できないサブジェクトによる干渉や改竄から保護される必要があるが、これは FPT_SEP.1 により実施される。

FIA_UAU.2 は、パスワードによって認証を行うが、パスワードの登録、削除、改変は FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_MTD.1(c)、FMT_MTD.1(d)により制限されており、干渉から保護される。

FIA_UAU.6 は、パスワードによって認証を行うが、パスワードの登録、削除、改変は FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_MTD.1(c)、FMT_MTD.1(d)により制限されており、干渉から保護される。

FIA_UID.2 は、ユーザ ID およびグループ ID によって識別を行うが、ユーザ ID およびグループ ID の登録、削除、改変は FMT_MTD.1 により管理者のみに制限されており、干渉から保護される。

FIA_USB.1 は、setuid ビット設定、setgid ビット設定によってプロセスに設定されるセキュリティ属性値を変更するが、setuid ビット設定、setgid ビット設定は FMT_MTD.1(f)により管理者及び所有者に制限されており、干渉から保護される。

8.2.5.3 非活性化防止

FAU_GEN.1 は、監査証跡の改竄から保護される必要があるが、これは FAU_STG.1 によって実施される。また、監査記録を保存し続けることによるデータ損失の恐れから保護される必要があるが、これは FAU_STG.3 により実施される。監査機能の起動、停止を特定の利用者のみに制限する必要があるが、これは FMT_MOF.1(a)、によって実施される。

FAU_STG.3 は、監査証跡のファイルサイズと格納期間の設定の改変を特定の利用者のみに制限する必要があるが、これは FMT_MOF.1(b)によって実施される。

8.2.5.4 無効化攻撃の検出

無効化攻撃の検出を満たすべきセキュリティ機能要件は存在しない。

8.2.6. 内部一貫性の根拠

割付内容が競合する可能性のある要件として、アクセス制御に関係する要件が存在するが、FDP_ACC.1(a)および FDP_ACC.1(b)は、それぞれオブジェクトの操作のリストについて述べているが、オブジェクトがファイルおよびディレクトリとプロセスの場合を規定しているため衝突しない。

また管理要件として、TSF データを操作する役割を限定する FMT_MSA.1、FMT_MTD.1 などの要件において競合の可能性があるが、FMT_MSA.1(a)、FMT_MSA.1(b)はそれぞれオブジェクトの所有グループ、所有者のパーミッション、所有グループのパーミッション、その他のパーミッションのデフォルト値、問い合わせ、改変を規定しており、FMT_MSA.1(c)はオブジェクトの所有者の改変を規定しているため衝突しない。FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_MTD.1(c)、FMT_MTD.1(d)、FMT_MTD.1(e)は、それぞれ TSF データの改変について述べているが、FMT_MTD.1(a)はユーザ ID、グループ ID、グループ管理者の登録、削除、改変について規定し、FMT_MTD.1(b)は利用者のパスワードについて規定し、FMT_MTD.1(c)は利用者のパスワードについて規定し、FMT_MTD.1(d)は管理者のパスワード、パスワードの最小文字数、日付と時刻について規定し、FMT_MTD.1(e)はグループに所属する利用者の登録、削除、改変について規定し、FMT_MTD.1(f)は setuid ビット設定、setgid ビット設定について規定しているため衝突しない。

その他、セキュリティ対策方針に対する根拠、依存性分析、相互サポート分析により、競合する可能性は特に確認されていなく、セキュリティ要件間では一貫性が保たれている。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能の根拠

この章では、セキュリティ機能がセキュリティ機能要件を実現することを実証する。表 12 にセキュリティ機能とセキュリティ機能要件の対応関係を示す。

表 12 : セキュリティ機能とセキュリティ要件の対応

	IA.1	IA.2	DAC.1	DAC.2	DAC.3	AU.1	AU.2	AU.3	PS.1	TI.1
FAU_GEN.1						X				
FAU_SAR.1							X			
FAU_SAR.2							X			
FAU_SAR.3							X			
FAU_STG.1								X		
FAU_STG.3								X		
FDP_ACC.1(a)			X							
FDP_ACC.1(b)				X						
FDP_ACF.1(a)			X							
FDP_ACF.1(b)				X						
FIA_ATD.1			X	X						
FIA_SOS.1		X								
FIA_UAU.2	X									
FIA_UAU.6		X								
FIA_UAU.7	X									
FIA_UID.2	X									
FIA_USB.1			X	X	X					
FMT_MOF.1(a)								X		
FMT_MOF.1(b)								X		
FMT_MSA.1(a)					X					
FMT_MSA.1(b)					X					
FMT_MSA.1(c)					X					
FMT_MSA.3(a)			X							
FMT_MSA.3(b)			X							
FMT_MTD.1(a)		X			X					
FMT_MTD.1(b)		X								
FMT_MTD.1(c)		X								

	IA.1	IA.2	DAC.1	DAC.2	DAC.3	AU.1	AU.2	AU.3	PS.1	TI.1
FMT_MTD.1(d)		X						X		
FMT_MTD.1(e)					X					
FMT_MTD.1(f)					X					
FMT_SMF.1		X			X			X		
FMT_SMR.1(a)		X			X			X		
FMT_SMR.1(b)		X								
FMT_SMR.1(c)					X					
FMT_SMR.1(d)					X					
FPT_RVM.1										X
FPT_SEP.1									X	
FPT_STM.1						X				

8.3.1.1 FAU_GEN.1

FAU_GEN.1 は AU.1 により、監査機能の起動・終了を含む、日付および時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)の属性を含む監査記録が生成されるため満足される。

8.3.1.2 FAU_SAR.1

FAU_SAR.1 は AU.2 により、監査記録は管理者が閲覧可能な形式で提供され、かつ管理者だけが監査記録を閲覧できることから満足される。

8.3.1.3 FAU_SAR.2

FAU_SAR.2 は AU.2 により、監査記録への読み出しアクセスを管理者のみに制限しているため満足される。

8.3.1.4 FAU_SAR.3

FAU_SAR.3 は AU.2 により、管理者は監査記録に対して事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)により、検索、分類、並べ替えが実行可能であることから満足される。

8.3.1.5 FAU_STG.1

FAU_STG.1 は AU.3 により、監査記録ファイルは管理者のみ読み込み、書き込み可能なパーミッションで生成されることから満足される。

8.3.1.6 FAU_STG.3

FAU_STG.3 は AU.3 により、監査記録ファイルの最大容量および最大保持期間を設定することで監査記録をローテート可能であることから満足される。

8.3.1.7 FDP_ACC.1(a)

FDP_ACC.1(a)は DAC.1 により、プロセスからファイルへの読み込み、書き込み、実行の操作、ファイルおよびディレクトリの一覧取得、生成、削除、移動の操作を規定されるため満足される。

8.3.1.8 FDP_ACC.1(b)

FDP_ACC.1(b)は DAC.2 により、サブジェクトのプロセスからサブジェクト以外のプロセスに対する停止、復帰、削除の操作、およびサブジェクト以外のプロセスが保持するデータオブジェクトへの読み込み、書き込みの操作を規定されるため満足される。

8.3.1.9 FDP_ACF.1(a)

FDP_ACF.1(a)は DAC.1 により、プロセスとファイルおよびディレクトリ間のアクセスは、プロセスのユーザ ID、グループ ID とファイル、ディレクトリの所有者、所有グループ、パーミッション、ext2/ext3 ファイルシステムのアトリビュート、スティッキービットに基づいて規定されており、かつ管理者のみはその制限を受けないため満足される。

8.3.1.10 FDP_ACF.1(b)

FDP_ACF.1(b)は DAC.2 により、サブジェクトのプロセスからサブジェクト以外のプロセスに対する停止、復帰、削除の操作、およびサブジェクト以外のプロセスが保持するデータオブジェクトへの読み込み、書き込みの操作を実施できるのは、所有者または管理者であるため満足される。

8.3.1.11 FIA_ATD.1

FIA_ATD.1 は DAC.1 により、プロセス、ファイルおよびディレクトリがユーザ ID、グループ ID を保持し、DAC.2 により、プロセスがユーザ ID、グループ ID を保持するため満足される。

8.3.1.12 FIA_SOS.1

FIA_SOS.1 は IA.2 により、パスワードの変更時には管理者によって設定された品質尺度を満たすパスワードが要求されることにより満足される。

8.3.1.13 FIA_UAU.2

FIA_UAU.2 は IA.1 により、利用者および管理者が TOE へアクセスする前に、必ず認証を要求するため満足される。

8.3.1.14 FIA_UAU.6

FIA_UAU.6 は IA.2 により、利用者が自身のパスワードを変更する際には、TSF は再認証を要求することから満足される。

8.3.1.15 FIA_UAU.7

FIA_UAU.7 は IA.1 により、パスワード入力時は画面には入力に対するフィードバックは何も表示しないため満足される。

8.3.1.16 FIA_UID.2

FIA_UID.2 は IA.1 により、利用者および管理者が TOE へアクセスする前に、必ず識別を要求するため満足される。

8.3.1.17 FIA_USB.1

FIA_USB.1 は DAC.1 により、プロセスはユーザ ID、グループ ID を保持し、DAC.2 により、プロセスはユーザ ID、グループ ID を保持し、DAC.3 により、管理者および利用者がログインした際にユーザ ID、グループ ID が関連づけられ、プロセス起動の際には、プロセスに実行者自身のユーザ ID およびグループ ID が関連づけられ、プロセスのユーザ ID およびグループ ID を管理者は変更可能である。また利用者を代行するプロセスのユーザ ID と一致するユーザ ID を持つプロセスに対して、利用者は利用者が所属するグループ ID へ変更可能であり、さらに setuid ビット設定が有効であるファイルを実行した場合に起動されるプロセスは、ユーザ ID に当該ファイルの所有者が設定される（setgid ビット設定が有効の場合は、グループ ID に当該ファイルの所有グループが設定される）ことにより満足される。

8.3.1.18 FMT_MOF.1(a)

FMT_MOF.1(a)は AU.3 により、記録する監査事象の粒度や事象種別、生成するファイル名の設定の改変や、監査機能の停止は管理者のみが可能であることから満足される

8.3.1.19 FMT_MOF.1(b)

FMT_MOF.1(b)は AU.3 により、管理者は監査記録消失の恐れに対しファイルの最大容量と最大保持期間を設定可能であり、この設定を超えた場合には最も古い監査機録を削除することにより満足される。

8.3.1.20 FMT_MSA.1(a)

FMT_MSA.1(a)は DAC.3 により、該当オブジェクトの所有グループ、該当オブジェクトの所有者のパーミッション、該当オブジェクトの所有グループのパーミッション、該当オブジェクトのその他の利用者のパーミッションのデフォルト値変更を管理者のみに制限するため満足される。

8.3.1.21 FMT_MSA.1(b)

FMT_MSA.1(b)は DAC.3 により、該当オブジェクトの所有グループ、該当オブジェクトの所有者のパーミッション、該当オブジェクトの所有グループのパーミッション、該当オブジェクトのその他の利用者のパーミッションの改変をオブジェクトの所有者および管理者のみに制限するため満足される。

8.3.1.22 FMT_MSA.1(c)

FMT_MSA.1(c)は DAC.3 により、該当オブジェクトの所有者、ext2/ext3 ファイルシステムのアトリビュートの改変を管理者のみに制限するため満足される。

8.3.1.23 FMT_MSA.3(a)

FMT_MSA.3(a)は DAC.1 により、オブジェクトの生成時において該当オブジェクトの所有グループ、パーミッションのデフォルト値は管理者が設定した値が付与され、所有者がその値を上書き設定することが可能であることから満足される。

8.3.1.24 FMT_MSA.3(b)

FMT_MSA.3(b)は DAC.1 により、オブジェクトの生成時において該当オブジェクトの所有者、ext2/ext3 ファイルシステムのアトリビュート、ディレクトリの生成であればスティッキービット属性のデフォルト値は規定値が付与されることから満足される。(規定値を変更することはできない。)

8.3.1.25 FMT_MTD.1(a)

FMT_MTD.1(a)は IA.2 により、ユーザ ID の改変、削除、登録を管理者のみに制限し、DAC.3 により、グループ ID、グループ管理者の登録、改変、削除を管理者のみに制限することから満足される。

8.3.1.26 FMT_MTD.1(b)

FMT_MTD.1(b)は IA.2 により、管理者および利用者のパスワードの登録を管理者のみに制限することから満足される。

8.3.1.27 FMT_MTD.1(c)

FMT_MTD.1(c)は IA.2 により、利用者のパスワード変更を各利用者自身および管理者に制限することから満足される。

8.3.1.28 FMT_MTD.1(d)

FMT_MTD.1(d)は IA.2 により、管理者のパスワード変更を管理者自身にのみ制限し、パスワードの最小文字数の改変を管理者のみに制限し、日付および時刻の改変を管理者のみに制限することから満足される。

8.3.1.29 FMT_MTD.1(e)

FMT_MTD.1(e)は IA.2 により、グループに所属する利用者の改変、削除、登録を管理者または該当グループ管理者のみに制限していることから満足される。

8.3.1.30 FMT_MTD.1(f)

FMT_MTD.1(f)は DAC.3 により、setuidビット設定、setgidビット設定の改変を管理者または所有者のみに制限していることから満足される。

8.3.1.31 FMT_SMF.1

FMT_SMF.1 は IA.2 によりユーザ ID、パスワードの管理機能を規定し、DAC.3 によりプロセス、ファイル、ディレクトリのセキュリティ属性の管理機能及び setuid ビット設定、setgid ビット設定の管理を規定し、AU.3 により管理者の監査機能のふるまいの管理機能、日付時刻の管理機能を規定することから満足される。

8.3.1.32 FMT_SMR.1(a)

FMT_SMR.1(a)は IA.2 によりユーザ ID の登録、削除、改変、利用者のパスワード登録、改変の役割を管理者に関連付け、DAC.3 により、グループ ID、グループ管理者の登録、削除、改変、ファイルおよびディレクトリのセキュリティ属性の改変および初期値の設定、setuid ビット設定、setgid ビット設定を改変する役割を管理者に関連付け、AU.3 により、監査記録の閲覧、監査機能の設定変更、監査機能の停止、日付・時刻の改変を管理者に関連付けるため満足される。

8.3.1.33 FMT_SMR.1(b)

FMT_SMR.1(b)は IA.2 により、利用者自身のパスワード改変の役割を該当利用者に関連付けるため満足される。

8.3.1.34 FMT_SMR.1(c)

FMT_SMR.1(c)は DAC.3 によりファイルおよびディレクトリのグループ ID およびパーミッションの改変の役割、および管理者が設定したパーミッションのデフォルト値を上書きする代替の初期値の改変の役割、setuid ビット設定、setgid ビット設定を改変する役割を所有者に関連付けるため満足される。

8.3.1.35 FMT_SMR.1(d)

FMT_SMR.1(d)は IA.2 により、グループに所属する利用者の改変、削除、登録の役割を管理者および該当グループ管理者に関連付けるため満足される。

8.3.1.36 FPT_RVM.1

FPT_RVM.1 は TI.1 により TOE によって管理されているオブジェクトにアクセスするためには、利用者、管理者に関わらず、ログインによる識別/認証を行う必要があることにより満足される。

8.3.1.37 FPT_SEP.1

FPT_SEP.1 は PS.1 により、プロセスは生成時に独立したアドレス空間を割当てられ、互いのアドレス空間は保護されており干渉しないことにより満足される。

8.3.1.38 FPT_STM.1

FPT_STM.1 は AU.1 により、日付および時刻の改変を管理者だけに制限しており、監査記録には監査事象を記録した時の日付および時刻が含まれていることにより満足される。

8.3.2. セキュリティ機能強度の根拠

本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、IA1、IA2 のパスワード認証メカニズムである。これらのセキュリティ機能強度は、管理者が設定する利用者のパスワードポリシーに依存するものであるが、信頼される管理者を前提としており、SOF-基本を満たす。また、TOE の最小機能強度レベルは、5.1.2 章において SOF-基本を指定しているため、両者は一貫している。

8.3.3. セキュリティ保証手段の根拠

6.2 章の表 7 で示したように、EAL1 で必要となるすべての TOE セキュリティ保証要件に対して、保証手段を対応づけている。また、保証手段によって、本 ST で規定した TOE セキュリティ保証要件が要求する証拠を網羅している。したがって、EAL1 における TOE セキュリティ保証要件の要求を満たしている。