# RICOH Pro 8220S/8210S/8200S

# セキュリティターゲット

作成者: 株式会社リコー
作成日付: 2017 年 06 月 16 日
バージョン: 1.00

# 更新履歴

| バージョン | 日付 | 作成者 | 詳細 |
|---|---|---|---|
| 1.00 | 2017-06-16 | 株式会社リコー | 公開版 |

# 目次

# 図一覧



# 表一覧

# 1 ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、及び TOE 記述について記述する。

## 1.1 ST 参照

ST の識別情報を以下に示す。

タイトル: RICOH Pro 8220S/8210S/8200S セキュリティターゲット

バージョン: 1.00

作成日付: 2017 年 06 月 16 日

作成者: 株式会社リコー

## 1.2 TOE 参照

TOE の識別情報を以下に示す。

TOE 名称: RICOH Pro 8220S/8210S/8200S

バージョン: J-1.01

TOE 種別: デジタル複合機(以下、MFP と言う)

対象 MFP: TOE は、自動原稿送り装置(ADF)(両面同時読み取り)を装着している MFP。

RICOH Pro 8220S、RICOH Pro 8210S、RICOH Pro 8200S

CC 認証品として購入したい場合は、その旨を営業担当者に依頼すること。

## 1.3 TOE 概要

本章では、本 TOE の種別、TOE の使用方法、TOE の主要なセキュリティ機能を述べる。

### 1.3.1 TOE 種別

本 TOE は、IT 製品である MFP で、ドキュメントを入力、蓄積、出力するものである。

### 1.3.2 TOE の使用方法

TOE の利用環境を図示して、使用方法を解説する。

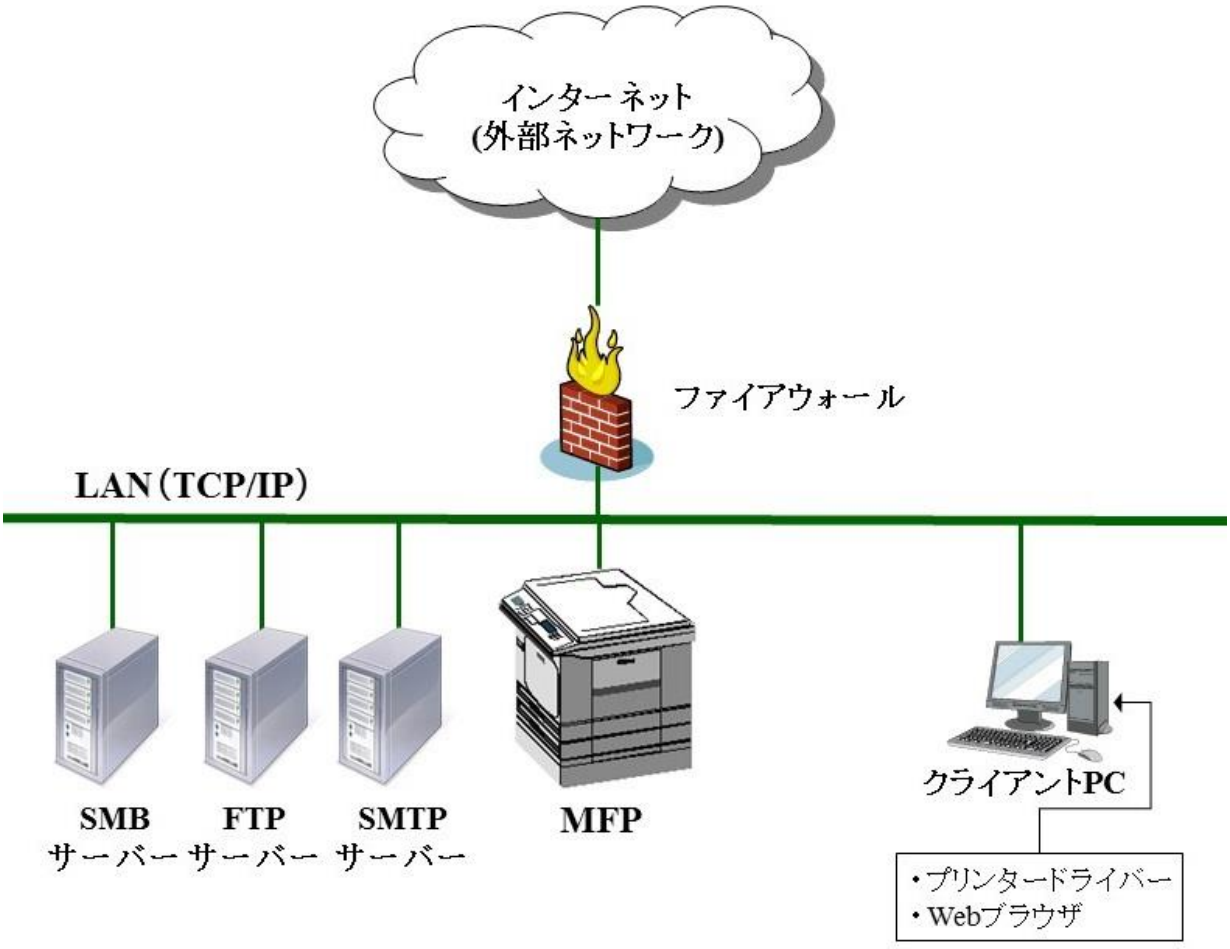



**図 1 : TOE の利用環境**

TOE は、図 1 に示すようにローカルエリアネットワーク(以下、LAN と言う)に接続して使用する。利用者は TOE が備える操作パネル、または LAN を介して通信することによって TOE を操作することができる。以下に、TOE である MFP と TOE 以外のハードウェア、ソフトウェアについて解説する。

**MFP**

TOE であり、MFP 本体はオフィス LAN に接続され、利用者は本体操作パネルから以下の処理が可能である。

- MFP 本体の各種設定
- 紙文書のコピー・蓄積・ネットワーク送信
- 蓄積文書の印刷・ネットワーク送信・編集・削除

**LAN**

TOE の設置環境で利用されるネットワーク。

**クライアント PC**

LAN に接続することによって、TOE のクライアントとして動作し、利用者は、クライアント PC から MFP をリモート操作することができる。以下に、クライアント PC からできるリモート操作を示す。

- クライアント PC にインストールした Web ブラウザから MFP の各種設定
- クライアント PC にインストールした Web ブラウザから蓄積文書を操作
- クライアント PC にインストールしたプリンタードライバーから文書を蓄積または印刷

**ファイアウォール**

インターネットからオフィス内へのネットワーク攻撃を防止するための装置。

**FTP サーバー**

TOE の文書を FTP サーバーにフォルダー送信する場合に、使用されるサーバー。

**SMB サーバー**

TOE の文書を SMB サーバーにフォルダー送信する場合に、使用されるサーバー。

**SMTP サーバー**

TOE が電子メールを送信する場合に、使用されるサーバー。

### 1.3.3 TOE の主要なセキュリティ機能

TOE は、文書を TOE 内に蓄積、あるいは LAN に接続した IT 機器と文書を送受信する。TOE はこれらの文書の機密性と完全性を保証するため、以下に記すようなセキュリティ機能を備える。

- 監査機能
- 識別認証機能
- 文書アクセス制御機能
- 利用者制限機能
- ネットワーク保護機能
- 残存情報消去機能
- 蓄積データ保護機能
- セキュリティ管理機能
- ソフトウェア検証機能

## 1.4 TOE 記述

本章では、TOE の物理的範囲、ガイダンス、利用者定義、TOE の論理的範囲、保護資産の概要を述べる。

### 1.4.1 TOE の物理的範囲

TOE の物理的範囲は、図 2 に示すように操作パネルユニット、エンジンユニット、コントローラボード、HDD、Ic Ctlr、ネットワークユニット、USB ポート、及び SD カードスロットのハードウェアから構成される MFP である。

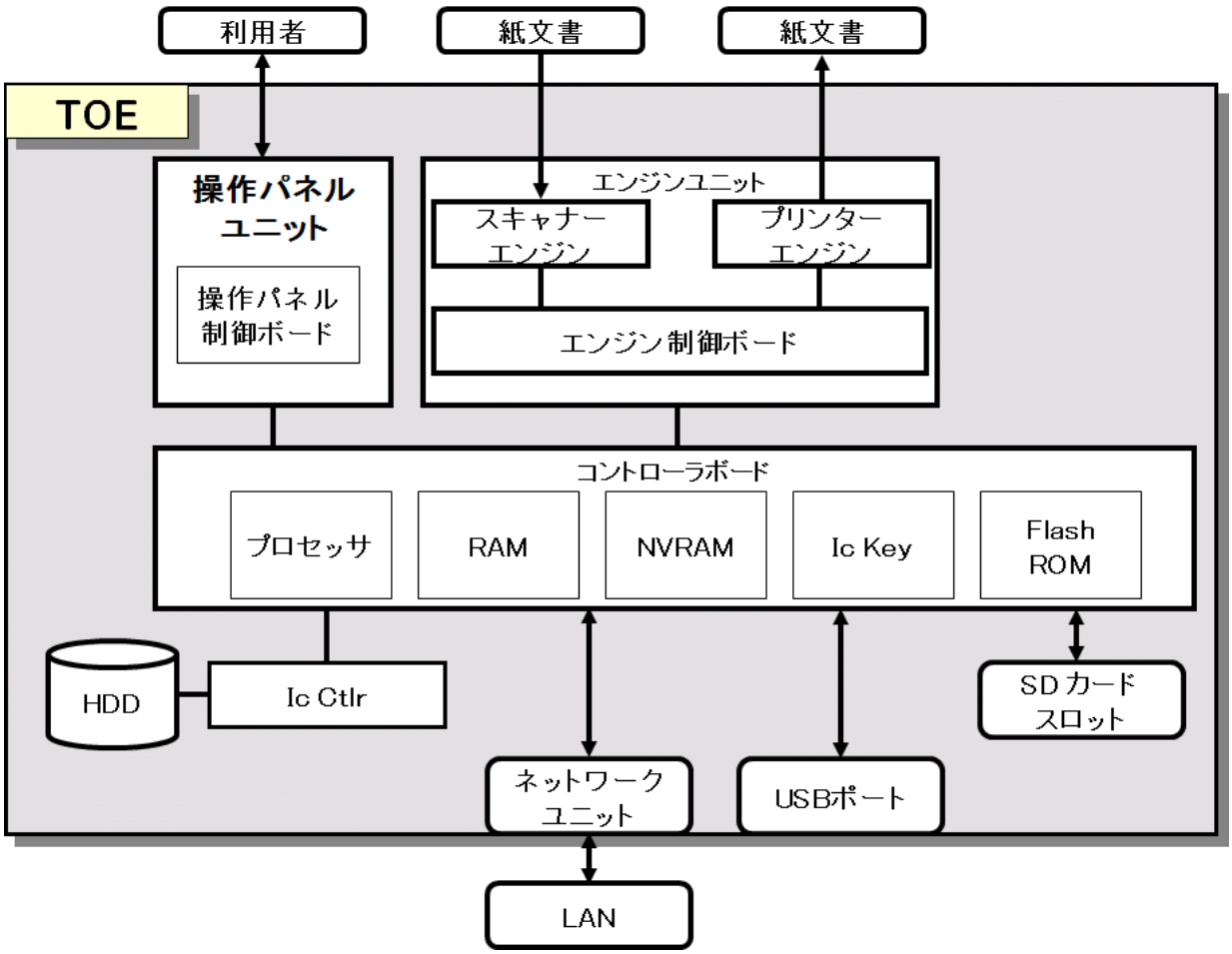



**図 2 : TOE のハードウェア構成**

コントローラボード

プロセッサ、RAM、NVRAM、Ic Key、FlashROM が載ったデバイス。コントローラボードは、MFP を構成するユニット及びデバイスと MFP を制御するための情報を送受信する。MFP を制御するための情報は、コントローラボードにある MFP 制御ソフトウェアが処理する。以下に概要を記載する。

- プロセッサ
  MFP 動作における基本的な演算処理をおこなう半導体チップ。
- RAM
  処理中の画像情報の圧縮/伸長などの画像処理や、一時的に内部情報を読み書きするための作業領域として利用される揮発性メモリ。
- NVRAM
  MFP の動作を決定する TSF 情報が保管された不揮発性メモリ。

- Ic Key
  乱数発生、暗号鍵生成、電子署名の機能をもつセキュリティチップ。内部にメモリを保持し、工場出荷時に署名ルート鍵を蓄積している。
- FlashROM
  TOE を構成する MFP 制御ソフトウェアがインストールされている不揮発性メモリ。

**操作パネルユニット(以降、操作パネルと言う)**

TOE に取り付けられた、利用者インタフェース機能を持つデバイスで、ハードキー、LED、タッチパネル式液晶ディスプレイと、これらの装置と接続する操作パネル制御ボードで構成される。操作パネル制御ボードには、操作パネル制御ソフトウェアがインストールされている。操作パネル制御ソフトウェアの動作は以下の 2 つである。

1. ハードキーやタッチパネル式液晶ディスプレイからの操作指示をコントローラボードに転送する。
2. コントローラボードからの表示指示により LED の点灯/消灯あるいはタッチパネル式液晶ディスプレイへメッセージ表示をする。

**エンジンユニット**

紙文書を読込むためのデバイスであるスキャナーエンジン、紙文書を印刷し排出するデバイスであるプリンターエンジン、エンジン制御ボードから構成される。エンジン制御ボードには、エンジン制御ソフトウェアがインストールされている。エンジン制御ソフトウェアは、スキャナーエンジンやプリンターエンジンの状態をコントローラボードに送信、あるいは MFP 制御ソフトウェアの指示を受信しスキャナーエンジンやプリンターエンジンを動作させる。

**HDD**

不揮発性メモリであるハードディスクドライブ。文書や一般利用者のログインユーザー名、一般利用者のログインパスワードが保管されている。

**Ic Ctlr**

データの暗号化/復号機能を実装した基板であり、HDD 暗号化を実現するための機能を持つ。

**ネットワークユニット**

Ethernet(100BASE-TX/10BASE-T)をサポートした LAN 用の外部インタフェース。

**USB ポート**

クライアントPCから直結して印刷を行う場合に、TOEとクライアントPCを接続する外部インタフェース。設置時に利用禁止設定とする。

**SD カードスロット**

SD カードスロットは、カスタマー・エンジニア用と利用者用がある。
カスタマー・エンジニア用の SD カードスロットは、カスタマー・エンジニアが TOE の設置時に使用するもので、TOE の運用中はカバーが取り付けられ SD カードの出し入れはできない。

利用者用の SD カードスロットは、利用者が SD カード内の文書を印刷するために用いるものである。設置時に利用禁止設定とする。

### 1.4.2 ガイダンス

本 TOE のガイダンス文書を以下に示す。.

- 本機を安全にご利用いただくために D181-2585
- はじめにお読みください D270-7402
- ユーザーガイド D270-7465
- RICOH Pro 8220S/8210S/8200S
  RICOH Pro 8220Y/8220HT/8210Y/8210HT
  使用説明書
  <ドライバーインストールガイド> D270-7467
- RICOH Pro 8220S/8210S/8200S
  RICOH Pro 8220Y/8220HT/8210Y/8210HT
  使用説明書
  <用紙ガイド> D270-7468
- RICOH Pro 8220S/8210S/8200S
  RICOH Pro 8220Y/8220HT/8210Y/8210HT
  使用説明書
  <セキュリティーガイド> D270-7469
- About Open Source Software License D270-7470
- 本機をお使いになる方へ D270-7472
- コピー/ドキュメントボックス D270-7473
- プリンター D270-7474
- スキャナー D270-7475
- こまったときには D270-7476
- ネットワークの接続/システム初期設定 D270-7477
- 用紙設定 D270-7478
- 拡張機能初期設定 D270-7479
- エミュレーション D270-7480
- セキュリティー機能をお使いになるお客様へ D181-2584
- RICOH Pro 8220S/8210S/8200S
  RICOH Pro 8220Y/8220HT/8210Y/8210HT
  使用説明書
  <IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ> D270-7463
- ヘルプ 83NHDPJAR1.00 v147

### 1.4.3 利用者定義

TOE に関連する利用者定義をする。TOE に関わる登場人物としては、通常直接 TOE を利用する関係者とそれ以外の関係者に分かれる。以下では直接的な関係者とそれ以外の関係者として説明する。

#### 1.4.3.1. 直接的利用者

本 ST で単純に"利用者"とよぶ場合は、この直接的利用者をさす。直接的利用者には、一般利用者及び管理者がある。これらの直接的利用者の定義を以下の表に示す(表 1)。

**表 1：利用者定義**

| 利用者定義 | 説明 |
|---|---|
| 一般利用者 | TOE の使用を許可された利用者。ログインユーザー名を付与され、コピー機能、スキャナー機能、プリンター機能、ドキュメントボックス機能の利用ができる。 |
| 管理者 | TOE の管理を許可された利用者。一般利用者にログインユーザー名を付与するなどの管理業務を行う。 |

管理者は、TOE 管理を目的として登録された利用者のことをさすが、その役割によってスーパーバイザーと MFP 管理者に分けられる。MFP 管理者は最大 4 人まで登録可能で、選択的にユーザー管理権限、機器管理権限、ネットワーク管理権限、文書管理権限をもつことができる。したがって複数の MFP 管理者で管理権限を分けることも可能であるが、本 ST で"MFP 管理者"とよぶ場合はすべての管理権限をもつ MFP 管理者をさすこととする(表 2)。

**表 2：管理者役割一覧**

| 管理者定義 | 管理権限 | 説明 |
|---|---|---|
| スーパーバイザー | スーパーバイザー | MFP 管理者のログインパスワードを改変する権限をもつ。 |
| MFP 管理者 | ユーザー管理権限 | 一般利用者を管理する管理権限。一般利用者に関する設定を操作することができる。 |
| | 機器管理権限 | ネットワークを除いた MFP の機器動作を決定する管理権限。機器に関する設定情報を操作することができる。監査ログの閲覧ができる。 |
| | ネットワーク管理権限 | LAN の設定をはじめネットワークを管理できる権限。ネットワーク設定情報を操作することができる。 |
| | 文書管理権限 | 蓄積文書を管理する権限。蓄積文書のアクセス管理をすることができる。 |

#### 1.4.3.2. 間接利用者

**MFP 管理責任者**

MFP 管理責任者とは、TOE を利用する組織の中で TOE の管理者を選任する役割を持った者のことを言う。

**カスタマー・エンジニア**

カスタマー・エンジニアは、TOE の保守管理する組織に所属し、TOE の設置、セットアップ、保守をする者を言う。

### 1.4.4 TOE の論理的範囲

以下に、基本機能とセキュリティ機能について記述する。

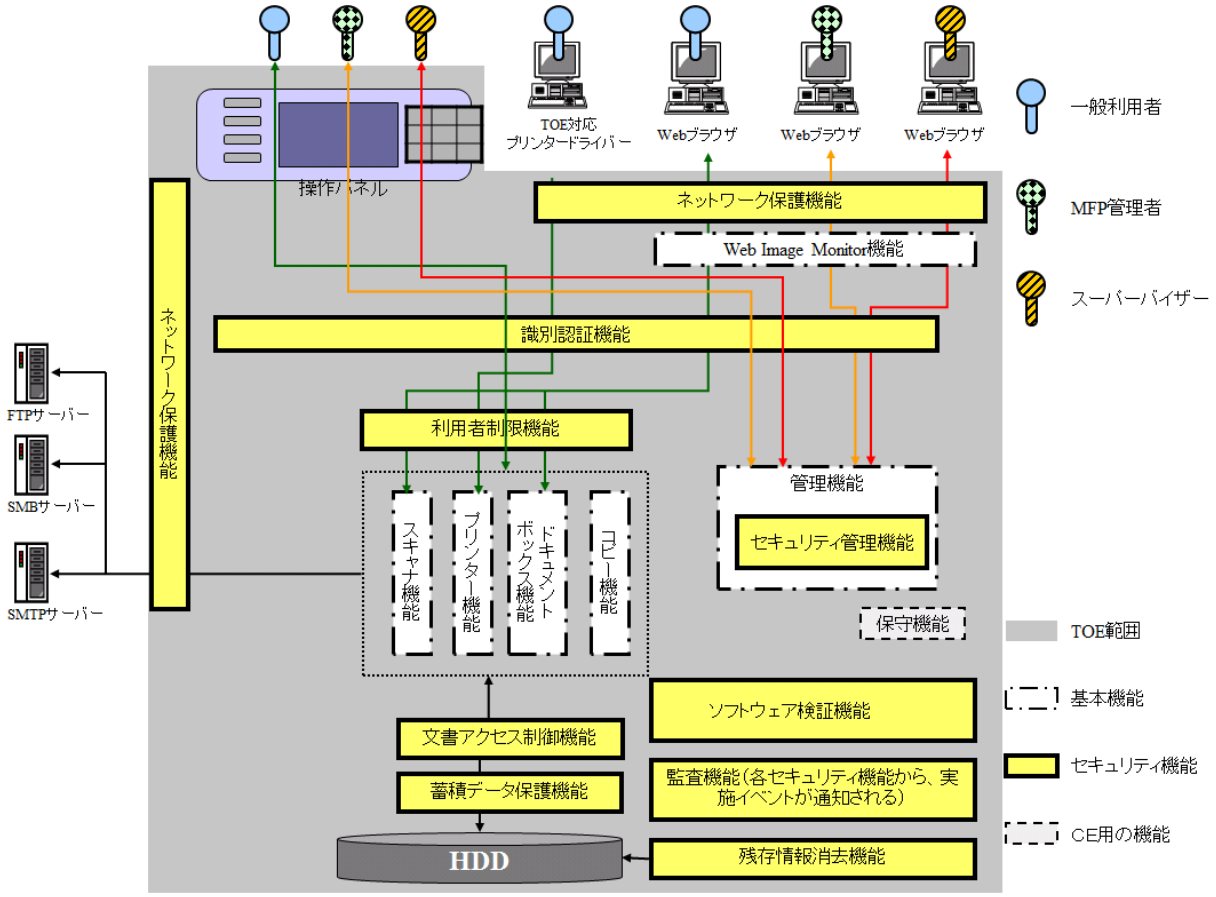



図 3：TOE の論理的範囲

#### 1.4.4.1. 基本機能

以下に、基本機能の概要を記述する。

**コピー機能**

コピー機能は、利用者による操作パネルからの操作によって、紙文書をスキャンして読取った画像を複写印刷する機能である。複写する画像は、利用者が変倍などの編集をすることができる。また、複写印刷する画像を同時に、ドキュメントボックス文書として HDD へ蓄積することができる。

**プリンター機能**

プリンター機能は、TOE がクライアント PC のプリンタードライバーから受信した文書を印刷または蓄積する機能と、利用者が操作パネルあるいはクライアント PC から TOE に蓄積している文書を印刷、削除する機能である。

- クライアント PC のプリンタードライバーからの受信
  TOE はクライアント PC のプリンタードライバーから文書を受信する。文書には、利用者がプリンタードライバーで選択した印刷方法が含まれる。印刷方法には、直接印刷、ドキュメントボックス蓄積、機密印刷、保存印刷、保留印刷、及び試し印刷がある。
  印刷方法が直接印刷の場合は、TOE が受信した文書を用紙に印刷する。文書は TOE に蓄積されない。
  印刷方法がドキュメントボックス蓄積の場合は、受信した文書をドキュメントボックス文書として HDD に蓄積する。
  印刷方法が機密印刷、保存印刷、保留印刷、及び試し印刷の場合は、受信した文書をプリンター文書として HDD に蓄積する。機密印刷では機密印刷用のパスワードを使用するが、これは評価の対象外である。
- 操作パネルからの操作
  TOE は、利用者による操作パネルからの操作に従い、プリンター文書を印刷または削除することができる。
- クライアント PC からの操作
  TOE は、利用者によるクライアント PC からの操作に従い、プリンター文書を印刷または削除することができる。
- TOE によるプリンター文書の削除
  TOE によるプリンター文書の削除は、印刷方法によって異なる。機密印刷、保留印刷、及び試し印刷のプリンター文書は、印刷終了後に TOE が削除する。保存印刷のプリンター文書は、印刷終了後も削除されない。

利用者は、最初にガイダンスに従って指定のプリンタードライバーを自身のクライアント PC にインストールして利用する。

**スキャナー機能**

スキャナー機能は、利用者が操作パネルから操作することによって、紙文書をスキャンして SMB サーバー、FTP サーバー、及びクライアント PC に送信・保存できる機能である。紙文書をスキャンした画像は、TOE 内に蓄積しておき、送信・削除することができる。
文書の送信方法には、フォルダー送信、文書添付メール送信、及び URL アドレスメール送信がある。
フォルダー送信は、MFP 管理者が予め TOE に登録するセキュアな通信が可能なサーバーにある送信先フォルダーに対してのみ行える。文書添付メール送信と URL アドレスメール送信は、MFP 管理者が予め TOE に登録するセキュアな通信が可能なメールサーバーとメールアドレスに対してのみ行える。URL アドレスメール送信で送信された電子メールを受け取った利用者は、スキャナー文書をクライアント PC へダウンロードすることができる。

**ドキュメントボックス機能**

ドキュメントボックス機能は、利用者が操作パネルとクライアント PC から TOE 内に蓄積している文書を操作する機能である。

操作パネルからは、ドキュメントボックス文書の蓄積、複製、印刷、編集、及び削除ができる。
クライアント PC からは、ドキュメントボックス文書の印刷と削除、スキャナー文書のフォルダー送信、文書添付メール送信、ダウンロード、及び削除をすることができる。

**管理機能**

管理機能は、MFP 機器の動作全体にかかわる制御機能である。管理機能は操作パネルあるいはクライアント PC から操作することができる。

**保守機能**

保守機能は機器故障時の保守サービス処理を実行する機能で、原因解析のためにカスタマー・エンジニアが操作パネルから操作する。この機能はカスタマー・エンジニアのみが保持する手段により実施できるが、MFP 管理者が保守機能移行禁止設定を移行禁止にしている場合は、カスタマー・エンジニアはこの機能を利用することはできない。
本 ST では保守機能移行禁止設定を移行禁止にしている状態での運用を評価範囲とする。

**Web Image Monitor 機能**

Web Image Monitor 機能(以下、WIM と言う)は、TOE の利用者がクライアント PC から TOE をリモート操作するための機能である。MFP 管理者は、接続した MFP の操作パネルの画面を表示することができる。
本機能を利用するためには、クライアント PC にガイダンスに従って指定の Web ブラウザをインストールし、TOE とは LAN 経由で接続する必要がある。

#### 1.4.4.2. セキュリティ機能

以下に、セキュリティ機能を記述する。

**監査機能**

監査機能は、TOE の使用の事象、及びセキュリティに関連する事象(以下、監査事象と言う)のログを監査ログとして記録し、記録した監査ログを、監査できる形式で提供する機能である。記録した監査ログは、MFP 管理者だけに読出し、削除の操作を許可する。監査ログの読出し、削除操作は WIM を利用して実施する。

**識別認証機能**

識別認証機能は、TOE を利用しようとする者が TOE の許可利用者であるかを検証し、TOE の許可利用者であることが確認できた場合に TOE の利用を許可する機能である。
利用者は、操作パネルあるいはネットワークを介して TOE を利用することができる。ネットワークを介した TOE の利用には、Web ブラウザからの利用、プリンタードライバーからの利用がある。
操作パネル、または Web ブラウザから利用しようとする者に対しては、ログインユーザー名とログインパスワードを入力させ、一般利用者、MFP 管理者、あるいはスーパーバイザーであることを検証する。
プリンタードライバーからプリンター機能を利用しようとする者に対しては、プリンタードライバーから受信するログインユーザー名とログインパスワードで一般利用者であることを検証する。

本機能には、ログインパスワード入力をする際にパスワードをダミー文字で表示する認証フィードバック領域の保護機能が含まれる。さらに、ロックアウト機能とログインパスワードの品質を保護するため、MFP 管理

者が予め制限したパスワードの最小桁数と必須使用の文字種の条件を満たしたパスワードだけを登録する機能も本機能に含まれる。

**文書アクセス制御機能**

文書アクセス制御機能は、識別認証機能で認証されたTOEの許可利用者に対して、その利用者の役割に対して与えられた権限、または利用者毎に与えられた権限に基づいて、文書と利用者ジョブへの操作を許可する機能である。

**利用者制限機能**

利用者制限機能は、識別認証機能で認証された TOE の許可利用者の役割、及び利用者毎に設定された操作権限に従って、コピー機能、プリンター機能、スキャナー機能、及びドキュメントボックス機能の操作を許可する機能である。

**ネットワーク保護機能**

ネットワーク保護機能は、LAN 利用時にネットワーク上のモニタリングによる情報漏えいを防止、及び改ざんを検出する機能である。クライアントPCからWIMを利用する場合は暗号化通信が有効なURLを指定し保護機能を有効化する。プリンター機能利用時は、プリンタードライバーにて暗号化通信選択をして保護機能を有効化する。スキャナー機能のうちフォルダー送信機能の利用時は、暗号化通信をして保護機能を有効化する。スキャナー機能のうちメール送信機能の利用時は、宛先ごとに登録されている条件での暗号化通信を行うことで保護機能を有効化する。

**残存情報消去機能**

残存情報消去機能は、HDD 上の削除された文書、一時的な文書あるいはその断片に対して、指定パターンデータを上書きすることにより残存情報の再利用を不可能とする機能である。

**蓄積データ保護機能**

蓄積データ保護機能は、HDD に記録されているデータを漏えいから保護するため、これらのデータを暗号化する機能である。

**セキュリティ管理機能**

セキュリティ管理機能は、一般利用者、MFP 管理者、及びスーパーバイザー利用者役割に与えられた権限、または利用者毎に与えられた権限に基づいて、TSF 情報への操作に関する制御を行う機能である。

**ソフトウェア検証機能**

ソフトウェア検証機能は、MFP 制御ソフトウェアの実行コードの完全性を検証し、それらが正規のものである事を確認する機能である。

### 1.4.5 保護資産

TOE が守るべき保護資産は、利用者情報、TSF 情報、及び機能である。

#### 1.4.5.1. 利用者情報

利用者情報は、文書情報と機能情報のタイプに分類される。利用者情報について表 3 にてタイプ毎に定義する。

**表 3 : 利用者情報定義**

| タイプ | 内容 |
|---|---|
| 文書情報 | デジタル化された TOE の管理下にある文書、削除された文書、一時的な文書あるいはその断片。 |
| 機能情報 | 利用者が指示したジョブ。本 ST 内では「利用者ジョブ」と表現する。 |

#### 1.4.5.2. TSF 情報

TSF 情報は、保護情報と秘密情報のタイプに分類される。TSF 情報について表 4 にてタイプ毎に定義する。

**表 4 : TSF 情報定義**

| タイプ | 内容 |
|---|---|
| 保護情報 | 編集権限をもった利用者以外の変更から保護しなければならないが、公開されてもセキュリティ上の脅威とならない情報。本 ST 内では「TSF 保護情報」と表現する。<br>ログインユーザー名、ログインパスワード入力許容回数、ロックアウト解除タイマー設定、ロックアウト時間、年月日、時刻、パスワード最小桁数、パスワード複雑度、操作パネルオートログアウト時間、WIM オートログアウト時間、S/MIME 利用者情報、送信先フォルダー、文書利用者リスト、利用機能リスト、ユーザー認証方法、IPsec 設定情報、機器証明書。 |
| 秘密情報 | 編集権限をもった利用者以外の変更から保護し、参照権限をもった利用者以外の読出しから保護しなければならない情報。本 ST 内では「TSF 秘密情報」と表現する。<br>ログインパスワード、監査ログ、HDD 暗号鍵。 |

#### 1.4.5.3. 機能

利用者情報の文書情報を操作するための機能である、MFP アプリケーション(コピー機能、ドキュメントボックス機能、プリンター機能、及びスキャナー機能)は、利用が制限される保護資産である。

## 1.5 用語

### 1.5.1 本 ST における用語

本 ST を明確に理解するために、表 5 において特定の用語の意味を定義する。

**表 5：本 ST に関連する特定の用語**

| 用語 | 定義 |
|---|---|
| MFP 制御ソフトウェア | TOE に組込むソフトウェアの 1 つ。FlashROM に格納されている。 |
| ログインユーザー名 | 一般利用者、MFP 管理者、及びスーパーバイザーに与えられている識別子。TOE はその識別子により利用者を特定する。 |
| ログインパスワード | 各ログインユーザー名に対応したパスワード。 |
| ロックアウト | 利用者に対してログインを許可しない状態にすること。 |
| オートログアウト機能 | 操作パネルあるいはクライアント PC からログイン中に、予め定められた時間アクセスが無かった時に、自動的にログアウトする機能。<br>オートログアウトとも言う。 |
| 操作パネルオートログアウト時間 | 操作パネルからオートログアウトする時間。 |
| WIM オートログアウト時間 | WIM を利用しているクライアント PC からオートログアウトする時間。 |
| パスワード最小桁数 | 登録可能なパスワードの最小桁数。 |
| パスワード複雑度 | 登録可能なパスワードの文字種組合せ数の最小数。<br>文字種は、英大文字、英小文字、数字、記号の 4 種がある。<br>パスワード複雑度には、複雑度 1 と複雑度 2 がある。複雑度 1 の場合は 2 種類以上の文字種、複雑度 2 の場合は 3 種類以上の文字種を組合せてパスワードを作らなければいけない。 |
| HDD | ハードディスクドライブの略称。本書で、単に HDD と記載した場合は TOE 内に取り付けられた HDD を指す。 |
| 利用者ジョブ | TOE のコピー、ドキュメントボックス、スキャナー、プリンターの各機能の開始から終了までの作業。利用者ジョブは、開始から終了の間に利用者によって一時停止、キャンセルされることがある。利用者ジョブがキャンセルされた場合、利用者ジョブは終了となる。 |
| 文書 | TOE が扱う紙文書、電子文書の総称。 |
| 文書情報属性 | 文書情報の属性で、+PRT、+SCN、+CPY、及び+DSR がある。 |
| +PRT | 文書情報属性のひとつ。クライアント PC から印刷する文書、あるいはクライアント PC から機密印刷、保留印刷、及び試し印刷で TOE 内に蓄積される文書。 |
| +SCN | 文書情報属性のひとつ。スキャナー機能を使って、IT 機器にメール送信、フォルダー送信する文書、あるいは MFP からクライアント PC にダウンロードする文書。 |
| +CPY | 文書情報属性のひとつ。コピー機能を使って原稿を複写した文書。 |
| +DSR | 文書情報属性のひとつ。コピー機能、スキャナー機能、ドキュメントボックス機能を使って、TOE 内に保存した文書。クライアント PC からドキュメントボックス印刷、あるいは保存印刷され TOE 内に保存された文書。 |
| 文書利用者リスト | 文書情報のセキュリティ属性。<br>アクセスを許可されている一般利用者のログインユーザー名のリストで、文書情報毎に設定できる。なお、MFP 管理者は、文書情報を管理するために文書情報へのアクセスは可能であるが、本リストに MFP 管理者のログインユーザー名は、リストされない。 |

| 用語 | 定義 |
|---|---|
| 蓄積文書 | ドキュメントボックス機能、プリンター機能、及びスキャナー機能で利用するために TOE 内に蓄積されている文書。 |
| 蓄積文書種別 | 蓄積文書の利用目的に応じて分類したもの。ドキュメントボックス文書、プリンター文書、及びスキャナー文書がある。 |
| ドキュメントボックス文書 | 蓄積文書種別のひとつ。コピー機能、ドキュメントボックス機能、及びプリンター機能の印刷方法がドキュメントボックス蓄積によって、TOE へ蓄積が行われた文書。 |
| プリンター文書 | 蓄積文書種別のひとつ。プリンター機能の印刷方法が機密印刷、保留印刷、保存印刷、試し印刷のいずれかで TOE へ蓄積が行われた文書。 |
| スキャナー文書 | 蓄積文書種別のひとつ。スキャナー機能で TOE へ蓄積が行われた文書。 |
| MFP アプリケーション | TOE が提供するコピー、ドキュメントボックス、スキャナー、プリンターの各機能の総称。 |
| 利用機能リスト | 一般利用者に対してアクセスを許可されている機能(コピー機能、プリンター機能、スキャナー機能、ドキュメントボックス機能)のリスト。各一般利用者の属性として付与される。 |
| 操作パネル | 液晶タッチパネルディスプレイとハードキーで構成される。利用者が TOE を操作する時に利用する。 |
| フォルダー送信 | MFP からネットワーク経由で SMB サーバー内の共有フォルダーに対して、SMB プロトコルで文書を送信する、もしくは FTP サーバーのフォルダーに対して、FTP で文書を送信する機能。フォルダー送信は、スキャナー機能でスキャンした文書をそのまま送信するか、同機能より一旦蓄積した文書情報を送信することができる。<br>この機能を実現するための通信は、IPsec によって保護される。 |
| 送信先フォルダー | フォルダー送信において、送信先のサーバー及びサーバー内のフォルダーへのパス情報、アクセスのための識別認証情報を含んだ情報。MFP 管理者によって登録管理される。 |
| メール送信 | MFP から SMTP サーバーを経由してクライアント PC に電子メールを送信する機能。 |
| 文書添付メール送信 | スキャナー機能で読取った文書を電子メール形式で送信する機能。この機能を実現するための通信は、S/MIME によって保護される。 |
| URL アドレスメール送信 | MFP 内に蓄積しているスキャナー文書の URL アドレスを電子メールで送信する機能。 |
| S/MIME 利用者情報 | メール送信において S/MIME を利用する際に必要となる情報。メールアドレス、ユーザー証明書、暗号化設定(S/MIME 設定)が含まれる。メール宛先 1 つにつき 1 つ存在する情報であり、MFP 管理者によって管理登録される。 |
| IPsec 設定情報 | TOE の IPsec の動作を決定する情報。 |
| 自動原稿送り装置(ADF)(両面同時読み取り) | 本装置にセットされた原稿を1枚ずつ読み取りガラスに送る装置。原稿の両面を読み取る場合は、原稿の両面を同時に読み取る。 |

# 2 適合主張

本章では適合の主張について述べる。

## 2.1 CC 適合主張

本 ST と TOE の CC 適合主張は以下の通りである。

- 適合を主張する CC のバージョン

  パート 1:

  概説と一般モデル 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-001

  パート 2:

  セキュリティ機能コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-002

  パート 3:

  セキュリティ保証コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 [翻訳第 1.0 版] CCMB-2012-09-003

- 機能要件: パート 2 拡張
- 保証要件: パート 3 適合

## 2.2 PP 主張

本 ST と TOE が論証適合している PP は、

PP 名称/識別: U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009)

バージョン: 1.0

である。

*注釈: 本 PP は Common Criteria Portal に掲載されている「IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B」に適合し、かつ「CCEVS Policy Letter #20」も満たしている。*

## 2.3 パッケージ主張

本 ST と TOE が適合しているパッケージは、評価保証レベル EAL2+ALC_FLR.2 である。

PP からの選択 SFR Package は

2600.2-PRT 適合

2600.2-SCN 適合

2600.2-CPY 適合

2600.2-DSR 適合

2600.2-SMI 適合

である。

## 2.4 適合主張根拠

### 2.4.1 PP の TOE 種別との一貫性主張

PP が対象とする製品の種別は、Hardcopy devices(以下、HCDs と言う)である。HCDs は、スキャナー装置とプリント装置で構成され、電話回線を接続するインタフェースを備えた装置であり、これらの装置を組合せて、コピー機能、スキャナー機能、プリンター機能、またはファクス機能の内、1 機能以上を搭載しているものである。さらに追加装置として、ハードディスクドライブなどの不揮発性記録媒体を設置することで、ドキュメントサーバー機能も利用できる。

本 TOE の種別は MFP である。MFP は、追加装置も含めて HCDs が持つ装置を備え、コピー機能、スキャナー機能、プリンター機能、及びドキュメントサーバー機能を搭載している。よって、本 TOE 種別は PP の TOE 種別と一貫していると言える。

### 2.4.2 PP のセキュリティ課題とセキュリティ対策方針との一貫性主張

本 ST の 3 章セキュリティ課題定義は、PP のセキュリティ課題を全て定義したうえで、P.STORAGE_ENCRYPTION を追加し、4 章セキュリティ対策方針には、PP のセキュリティ対策方針を全て定義したうえで O.STORAGE.ENCRYPTED を追加している。以下に、追加となったセキュリティ課題とセキュリティ対策方針について PP に適合する根拠を示す。

尚、PP は英語で作成されているが、本 ST の 3 章セキュリティ課題定義、及び 4 章セキュリティ対策方針は、PP を日本語訳して記述している。日本語訳するにあたって、PP の直訳が読者の理解の妨げになると判断した場合は、理解しやすい表現にしたが PP の適合要件を逸脱する表現ではない。また、記載内容を増やしたり減らしたりといったことはしていない。

**P.STORAGE_ENCRYPTION と O.STORAGE.ENCRYPTED の追加**

P.STORAGE_ENCRYPTION と O.STORAGE.ENCRYPTED は HDD に対するデータの暗号化を行うものであり、PP に含まれる他の組織のセキュリティ方針、TOE のセキュリティ対策方針のいずれをも満たしている。よって、P.STORAGE_ENCRYPTION と O.STORAGE.ENCRYPTED の追加はしているが PP には適合していると言える。

**T.DOC.DIS と T.DOC.ALT の脅威範囲の追加**

本 TOE と PP では、D.DOC の閲覧または改変できる利用者の定義は同じであるが、D.DOC の漏えいと改ざんの脅威が起こりうる範囲が、TOE が TOE 内及び TOE が通信する際の通信経路と定義しているのに対して、PP は TOE 内となっており TOE が PP を包含している。
よって、T.DOC.DIS と T.DOC.ALT は PP に適合していると言える。

**T.FUNC.ALT の脅威範囲の追加**

本 TOE と PP では、D.FUNC の改変できる利用者の定義は同じであるが、D.FUNC の改ざんの脅威が起こりうる範囲が、TOE が TOE 内及び TOE が通信する際の通信経路と定義しているのに対して、PP は TOE 内となっており TOE が PP を包含している。
よって、T.FUNC.ALT は PP に適合していると言える。

以上のことより、本 ST のセキュリティ課題とセキュリティ対策方針は、PP のセキュリティ課題とセキュリティ対策方針と一貫している。

### 2.4.3 PP のセキュリティ要件との一貫性主張

本 TOE の SFR は、Common Security Functional Requirements と 2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-DSR、2600.2-SMI からなる。
Common Security Functional Requirements は、PP が指定する必須 SFR であり、2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-DSR、2600.2-SMI は PP が指定する SFR Package から選択したものである。
尚、2600.2-NVS は TOE に着脱可能な不揮発性記憶媒体が存在しないため選択しない。
本 ST のセキュリティ要件は、PP のセキュリティ要件に対して追加、具体化している箇所があるが、PP とは一貫している。以下に、追加、具体化している箇所と、それらが PP と一貫している理由を記載する。

**FAU_STG.1、FAU_STG.4、FAU_SAR.1、FAU_SAR.2 の追加**

本 TOE が監査ログを保持管理するために PP APPLICATION NOTE7 に従い FAU_STG.1、FAU_STG.4、FAU_SAR.1、FAU_SAR.2 を追加する。

**FIA_AFL.1、FIA_UAU.7、FIA_SOS.1 の追加**

識別認証機能は本 TOE により実現するために PP APPLICATION NOTE38 に従い FIA_AFL.1、FIA_UAU.7、FIA_SOS.1 を追加する。

**FCS_CKM.1、FCS_COP.1 の追加**

本 TOE においては、管理者に着脱を許可しない不揮発性記憶媒体に対するデータ保護のセキュリティ対策方針として O.STORAGE.ENCRYPTED を主張し、これを実現するために機能要件 FCS_CKM.1、FCS_COP.1 と、これらの機能要件と依存関係にある機能要件に追加の変更を与えているが、これらの変更は PP において求められている機能要件の内容のいずれをも満たしている。

**外部インタフェースへの制限された情報転送(FPT_FDI_EXP)を追加**

本 TOE は、PP に従い、外部インタフェースへの制限された情報転送(FPT_FDI_EXP)を追加することにより機能要件のパート 2 を拡張する。

**FDP_ACF.1(a)の一貫性根拠**

PP の FDP_ACF.1.1(a)と FDP_ACF.1.2(a)では、PP の SFR パッケージ毎に定義された文書情報へのアクセス制御 SFP を要件としているのに対して、ST ではオブジェクトのセキュリティ属性である文書情報属性毎に定義された文書のアクセス制御 SFP を要件としているが、これは PP を逸脱せずに具現化しているものであ

る。
PP の FDP_ACF.1.3(a)では、文書情報と利用者ジョブのアクセス制御に関する追加の規則が無いが、本 ST では文書情報と利用者ジョブの削除を MFP 管理者に許可するとなっている。
TOE が MFP 管理者に文書情報と利用者ジョブの削除を許可するのは、文書情報と利用者ジョブに削除権限をもった一般利用者が、なんらかの事情で削除できなくなった場合に、MFP 管理者が代行して削除できるようにするためであり、PP で規定するアクセス制御 SFP を逸脱するものではない。
PP の FDP_ACF.1.4(a)では、文書情報と利用者ジョブのアクセス制御に関する追加の規則が無いが、本 ST ではスーパーバイザーによる文書情報と利用者ジョブへの操作を拒否するとしている。
スーパーバイザーは、PP では特定していない本 TOE 特有の利用者である。
これは、PP が文書情報と利用者ジョブの利用者として特定した利用者以外には操作を許可しないことを指す。
よって、本 ST の FDP_ACF.1(a)は PP の FDP_ACF.1(a)を満たしている。

**FDP_ACF.1.3(b)の追加規則について**

PP の FDP_ACF.1.3(b)では、管理者権限で操作するユーザーに TOE 機能の操作を許可するとなっているのに対して、本 ST では MFP 管理者に TOE 機能の利用を許可しないとなっている。
TOE は MFP 管理者に、文書情報や利用者ジョブの削除を許可しており(文書アクセス制御 SFP、FDP_ACC.1(a)と FDP_ACF.1(a))、この結果、制限的ではあるが TSF は、TOE 機能へのアクセスを MFP 管理者に許可しているため PP の FDP_ACF.1.3(b)の要件も同時に満たしている。
よって、本 ST の FDP_ACF.1.3(b)は PP の FDP_ACF.1.3(b)を満たしている。

**FTP_ITC.1.3 に D.DOC 及び D.FUNC が含まれていることについて**

PP では、通信経路上の D.DOC 及び D.FUNC に対して漏えいと改ざんの脅威を定義していないのに対して、FTP_ITC.1.3 では D.DOC と D.FUNC は高信頼チャネルを介して通信をするとしている。これは、本 TOE が PP より広い範囲で D.DOC と D.FUNC を保護していると言える。本 ST の FTP_ITC.1.3 は PP を満たしている。

# 3 セキュリティ課題定義

本章は、脅威、組織のセキュリティ方針、及び前提条件について記述する。

## 3.1 脅威

本 TOE の利用、及び利用環境において想定される脅威を識別し、説明する。本章に記す脅威は、TOE の動作について公開されている情報を知識として持っている利用者であると想定する。攻撃者は基本レベルの攻撃能力を持つ者とする。

**T.DOC.DIS** **文書の開示**

TOE が管理している文書が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって閲覧されるかもしれない。

**T.DOC.ALT** **文書の改変**

TOE が管理している文書が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって改変されるかもしれない。

**T.FUNC.ALT** **利用者ジョブの改変**

TOE が管理している利用者ジョブが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブへのアクセス権限をもたない者によって改変されるかもしれない。

**T.PROT.ALT** **TSF 保護情報の改変**

TOE が管理している TSF 保護情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護情報へのアクセス権限をもたない者によって改変されるかもしれない。

**T.CONF.DIS** **TSF 秘密情報の開示**

TOE が管理している TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって閲覧されるかもしれない。

**T.CONF.ALT** **TSF 秘密情報の改変**

TOE が管理している TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって改変されるかもしれない。

## 3.2 組織のセキュリティ方針

下記の組織のセキュリティ方針をとる。

**P.USER.AUTHORIZATION 利用者の識別認証**

TOE 利用の許可を受けた利用者だけが TOE を利用することができるようにしなければならない。

**P.SOFTWARE.VERIFICATION ソフトウェア検証**

TSF の実行コードを自己検証できる手段を持たなければならない。

**P.AUDIT.LOGGING 監査ログ記録管理**

TOE は TOE の使用及びセキュリティに関連する事象のログを監査ログとして記録維持し、監査ログが権限をもたない者によって開示あるいは改変されないように管理できなければならない。さらに権限をもつものが、そのログを閲覧できるようにしなければならない。

**P.INTERFACE.MANAGEMENT 外部インタフェース管理**

TOE の外部インタフェースが権限外のものに利用されることを防ぐため、それらのインタフェースは TOE と IT 環境により、適切に制御されていなければならない。

**P.STORAGE.ENCRYPTION 記憶装置暗号化**

TOE の HDD に記録しているデータは、暗号化されていなければならない。

## 3.3 前提条件

本 TOE の利用環境に関わる前提条件を識別し、説明する。

**A.ACCESS.MANAGEDアクセス管理**

ガイダンスに従って TOE を安全で監視下における場所に設置し、権限をもたない者に物理的にアクセスされる機会を制限しているものとする。

**A.USER.TRAINING 利用者教育**

MFP 管理責任者は、利用者が組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っているものとする。

**A.ADMIN.TRAINING 管理者教育**

管理者は組織のセキュリティポリシーやその手順を認識しており、ガイダンスに従ってそれらのポリシーや手順に沿った TOE の設定や処理ができるものとする。

**A.ADMIN.TRUST　　信頼できる管理者**

MFP 管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任しているものとする。

# 4 セキュリティ対策方針

本章では、TOE に対するセキュリティ対策方針、運用環境に対するセキュリティ対策方針と根拠について記述する。

## 4.1 TOE のセキュリティ対策方針

本章では、TOE のセキュリティ対策方針を記述する。

**O.DOC.NO_DIS　文書の開示保護**

TOE は、文書がログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって開示されることから、保護することを保証する。

**O.DOC.NO_ALT　文書の改変保護**

TOE は、文書がログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって改変されることから、保護することを保証する。

**O.FUNC.NO_ALT　利用者ジョブの改変保護**

TOE は利用者ジョブが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブへのアクセス権限をもたない者によって改変されることからの保護を保証する。

**O.PROT.NO_ALT　TSF 保護情報の改変保護**

TOE は TSF 保護情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護情報へのアクセス権限をもたない者によって改変されることからの保護を保証する。

**O.CONF.NO_DIS　TSF 秘密情報の開示保護**

TOE は TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって開示されることからの保護を保証する。

**O.CONF.NO_ALT　TSF 秘密情報の改変保護**

TOE は TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって改変されることからの保護を保証する。

**O.USER.AUTHORIZED　　利用者の識別認証**

TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証されることを保証する。

**O.INTERFACE.MANAGED　　TOE による外部インタフェース管理**

TOE はセキュリティポリシーに従って外部インタフェースの運用を管理することを保証する。

**O.SOFTWARE.VERIFIED　ソフトウェア検証**

TOE は TSF の実行コードを自己検証できるための手段の提供を保証する。

**O.AUDIT.LOGGED　監査ログ記録管理**

TOE は TOE の使用及びセキュリティに関連する事象のログを監査ログとして本体に記録維持し、監査ログが権限をもたない者によって開示あるいは改変されないように管理できることを保証する。

**O.STORAGE.ENCRYPTED　記憶装置暗号化**

TOE は、HDD に書き込むデータを、暗号化してから記録することを保証する。

## 4.2　運用環境のセキュリティ対策方針

本章では、運用環境のセキュリティ対策方針について記述する。

### 4.2.1　IT 環境

**OE.AUDIT_STORAGE.PROTECTED　　高信頼 IT 製品での監査ログ保護**

MFP 管理責任者は、高信頼 IT 製品にエキスポートされた監査ログが権限外の者からのアクセス、削除、改変から防御できていることを保証する。

**OE.AUDIT_ACCESS.AUTHORIZED　　高信頼 IT 製品の監査ログアクセス制限**

MFP 管理責任者は、高信頼 IT 製品にエキスポートされた監査ログが権限をもつ者にのみアクセスされ、可能性のあるセキュリティ違反行為を検出できることを保証する。

**OE.INTERFACE.MANAGED　　IT 環境による外部インタフェース管理**

IT 環境は、TOE 外部インタフェースへの管理されていないアクセスを防止する策を講じていることを保証する。

### 4.2.2 非 IT 環境

**OE.PHYSICAL.MANAGED 物理的管理**

ガイダンスに従って TOE を安全で監視下における場所に設置し、権限をもたない者に物理的にアクセスされる機会を制限することを保証する。

**OE.USER.AUTHORIZED 利用者への権限付与**

MFP 管理責任者は、組織のセキュリティポリシーや手順に従って、利用者に TOE の利用権限を付与することを保証する。

**OE.USER.TRAINED 利用者への教育**

MFP 管理責任者は、利用者に組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者がそれらのポリシーや手順に沿っていることを保証する。

**OE.ADMIN.TRAINED 管理者への教育**

MFP 管理責任者は、管理者が組織のセキュリティポリシーやその手順を承知していることを保証する。そのために、管理者はガイダンスに従ってそれらのポリシーや手順に沿った設定や処理ができるよう教育され、その能力をもち、またその時間を持つことを MFP 管理責任者により保証されている。

**OE.ADMIN.TRUSTED 信頼できる管理者**

MFP 管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任していることを保証する。

**OE.AUDIT.REVIEWED ログの監査**

MFP 管理責任者は、安全上の侵害や異常な状態を検出するために、ガイダンスの記述に従って、監査ログの監査を適切な間隔で実施していることを保証する。

## 4.3 セキュリティ対策方針根拠

本章では、セキュリティ対策方針の根拠を示す。セキュリティ対策は、規定した前提条件に対応するためのもの、脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。

### 4.3.1 セキュリティ対策方針対応関係表

セキュリティ対策方針と対応する前提条件、対抗する脅威、実現する組織のセキュリティ方針の対応関係を表 6 に示す。

**表 6：セキュリティ対策方針根拠**

| | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | OE.USER.AUTHORIZED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | OE.AUDIT_STORAGE.PROTCTED | OE.AUDIT_ACCESS_AUTHORIZED | OE.AUDIT.REVIEWED | O.INTERFACE.MANAGED | OE.PHYSICAL.MANAGED | OE.INTERFACE.MANAGED | O.STORAGE.ENCRYPTED | OE.ADMIN.TRAINED | OE.ADMIN.TRUSTED | OE.USER.TRAINED |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.DOC.DIS | X | | | | | | X | X | | | | | | | | | | | | |
| T.DOC.ALT | | X | | | | | X | X | | | | | | | | | | | | |
| T.FUNC.ALT | | | X | | | | X | X | | | | | | | | | | | | |
| T.PROT.ALT | | | | X | | | X | X | | | | | | | | | | | | |
| T.CONF.DIS | | | | | X | | X | X | | | | | | | | | | | | |
| T.CONF.ALT | | | | | | X | X | X | | | | | | | | | | | | |
| P.USER.AUTHORIZATION | | | | | | | X | X | | | | | | | | | | | | |
| P.SOFTWARE.VERIFICATION | | | | | | | | | X | | | | | | | | | | | |
| P.AUDIT.LOGGING | | | | | | | | | | X | X | X | X | | | | | | | |
| P.INTERFACE.MANAGEMENT | | | | | | | | | | | | | | X | | X | | | | |
| P.STORAGE.ENCRYPTION | | | | | | | | | | | | | | | | | X | | | |
| A.ACCESS.MANAGED | | | | | | | | | | | | | | | X | | | | | |
| A.ADMIN.TRAINING | | | | | | | | | | | | | | | | | | X | | |
| A.ADMIN.TRUST | | | | | | | | | | | | | | | | | | | X | |
| A.USER.TRAINING | | | | | | | | | | | | | | | | | | | | X |

### 4.3.2 セキュリティ対策方針記述

以下に、各セキュリティ対策方針が脅威、前提条件、及び組織のセキュリティ方針を満たすのに適している根拠を示す。

**T.DOC.DIS**

T.DOC.DIS は、O.DOC.NO_DIS、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.DOC.NO_DIS により TOE は文書を、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがそれらの文書へのアクセス権限をもたない者によって開示されることから保護する。

これらの対策方針により、T.DOC.DIS に対抗できる。

**T.DOC.ALT**

T.DOC.ALT は、O.DOC.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.DOC.NO_ALT により TOE は、文書がログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって改変されることから保護する。

これらの対策方針により、T.DOC.ALT に対抗できる。

**T.FUNC.ALT**

T.FUNC.ALT は、O.FUNC.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.FUNC.NO_ALT により TOE は利用者ジョブが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブへのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.FUNC.ALT に対抗できる。

**T.PROT.ALT**

T.PROT.ALT は、O.PROT.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.PROT.NO_ALT により TOE

は TSF 保護情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護情報へのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.PROT.ALT に対抗できる。

**T.CONF.DIS**

T.CONF.DIS は、O.CONF.NO_DIS、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.CONF.NO_DIS により TOE は TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって開示されることはない。

これらの対策方針により、T.CONF.DIS に対抗できる。

**T.CONF.ALT**

T.CONF.ALT は、O.CONF.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.CONF.NO_ALT により TOE は TSF 秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密情報へのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.CONF.ALT に対抗できる。

**P.USER.AUTHORIZATION**

P.USER.AUTHORIZATION は、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、MFP 管理責任者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.USER.AUTHORIZED により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。

これらの対策方針により、P.USER.AUTHORIZATION を順守できる。

**P.SOFTWARE.VERIFICATION**

P.SOFTWARE.VERIFICATION は、O.SOFTWARE.VERIFIED によって対抗できる。

O.SOFTWARE.VERIFIED により TOE は TSF の実行コードを自己検証できる手段を提供する。

この対策方針により、P.SOFTWARE.VERIFICATION を順守できる。

**P.AUDIT.LOGGING**

P.AUDIT.LOGGING は、O.AUDIT.LOGGED、OE.AUDIT.REVIEWED、OE.AUDIT_STORAGE.PROTECTED、OE.AUDIT_ACCESS.AUTHORIZED によって対抗できる。

O.AUDIT.LOGGED により、TOE は TOE の使用及びセキュリティに関連する事象のログを監査ログとして本体に記録維持し、監査ログが権限をもたない者によって開示あるいは改変されないように管理でき、OE.AUDIT.REVIEWED により、MFP 管理責任者は、安全上の侵害や異常な状態を検出するために、ガイダンスの記述に従って、監査ログの監査を適切な間隔で実施する。

一方、OE.AUDIT_STORAGE.PROTECTED により、MFP 管理責任者は、高信頼 IT 製品にエキスポートされた監査ログの権限外の者からのアクセス、削除、改変を防御し、OE.AUDIT_ACCESS.AUTHORIZED により、MFP 管理責任者は、高信頼 IT 製品にエキスポートされた監査ログが権限をもつ者にのみアクセスされ、可能性のあるセキュリティ違反行為を検出できる。

これらの対策方針により、P.AUDIT.LOGGING を順守できる。

**P.INTERFACE.MANAGEMENT**

P.INTERFACE.MANAGEMENT は、O.INTERFACE.MANAGED、OE.INTERFACE.MANAGED によって対抗できる。

O.INTERFACE.MANAGED により、TOE はセキュリティポリシーに従って外部インタフェースの運用を管理する。OE.INTERFACE.MANAGED により、TOE の外部インタフェースへの管理されていないアクセスを防止する IT 環境を構築する。

これらの対策方針により、P.INTERFACE.MANAGEMENT を順守できる。

**P.STORAGE.ENCRYPTION**

P.STORAGE.ENCRYPTION は、O.STORAGE.ENCRYPTED によって対抗できる。

O.STORAGE.ENCRYPTED により、TOE は HDD に書き込むデータを暗号化し、HDD 上には暗号化された情報が記録されることを保証する。

この対策方針により、P.STORAGE.ENCRYPTION を順守できる。

**A.ACCESS.MANAGED**

A.ACCESS.MANAGED は、OE.PHYSICAL.MANAGED によって運用する。

OE.PHYSICAL.MANAGED により、ガイダンスに従って TOE を安全で監視下における場所に設置し、権限をもたない者に物理的にアクセスされる機会を制限する。

この対策方針により、A.ACCESS.MANAGED を実現できる。

**A.ADMIN.TRAINING**

A.ADMIN.TRAINING は、OE.ADMIN.TRAINED によって運用する。

OE.ADMIN.TRAINED により MFP 管理責任者は、管理者が組織のセキュリティポリシーやその手順を承知しているようにする。そのために、管理者はガイダンスに従ってそれらのポリシーや手順に沿った設定や処理ができるよう教育され、その能力をもち、またその時間を持つように MFP 管理責任者が責任をもつ。

この対策方針により、A.ADMIN.TRAINING を実現できる。

**A.ADMIN.TRUST**

A.ADMIN.TRUST は、OE.ADMIN.TRUSTED によって運用する。

OE.ADMIN.TRUSTED により、MFP 管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任する。

この対策方針により、A.ADMIN.TRUST を実現できる。

**A.USER.TRAINING**

A.USER.TRAINING は、OE.USER.TRAINED によって運用する。

OE.USER.TRAINED により、MFP 管理責任者は、利用者に組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っている。

この対策方針により、OE.USER.TRAINED を実現できる。

# 5 拡張コンポーネント定義

本章では、拡張したセキュリティ機能要件を定義する。

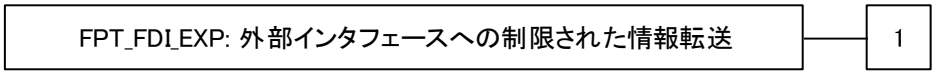
## 5.1 外部インタフェースへの制限された情報転送(FPT_FDI_EXP)

ファミリのふるまい

このファミリは、一方の外部インタフェースからもう一方の外部インタフェースへの情報の直接転送を TSF が制限するための要件を定義する。

多くの製品は固有の外部インタフェースで情報を受信し、この情報を他の外部インタフェースから送信する前に変換、処理することを目的としている。一方で、ある製品が攻撃者に、TOE や、TOE の外部インタフェースに接続された機器のセキュリティを侵害するために、外部インタフェースを悪用する能力を提供するかもしれない。そのため、異なる外部インタフェース間の処理されていないデータの直接転送は、許可された管理者役割によって明示的に許可された場合を除いて禁止される。FPT_FDI_EXP ファミリはこの種の機能性を特定するために定義された。

コンポーネントのレベル付け




FPT_FDI_EXP.1 外部インタフェースへの制限された情報転送は、定義された外部インタフェースで受信したデータを、もう一方の外部インタフェースから送信される前に、TSF で制御された処理を行うことを要求する機能性を提供する。一方の外部インタフェースから他方へのデータの直接転送は、許可された管理者役割による明示的な許可を要求する。

**管理: FPT_FDI_EXP.1**

以下のアクションは FMT における管理機能と考えられる:

a) 管理アクティビティを実行することを許可される役割の定義

b) 管理者役割によって直接転送が許可される条件の管理

c) 許可の取消し

**監査: FPT_FDI_EXP.1**

予見される監査対象事象はない。

**根拠:**

しばしば TOE は、ある外部インタフェースで受信したデータを他のインタフェースから送信するのを許可する前に、特定の検査と処理を行うことが想定される。例はファイアウォールシステムだが、入力データを送信する前に特定のワークフローを要求する他のシステムも同様である。そのような(処理されていない)データの、異なる外部インタフェース間での直接転送は、もし許されるなら、許可された役割によってのみ許可される。

直接転送を禁じ、許可された役割だけが許可できることを要求する特性を指定する単独のコンポーネントとして、この機能性を持つことは有用と見なされる。この機能は多くの製品に共通するため、拡張コンポーネントを定義するのは有用と見なされる。

CC は FDP クラスにおいて属性による利用者データフローを定義している。一方でこの ST では、利用者データと TSF データ共に、属性による制御の代わりに運用管理による制御を表現する必要がある。FDP_IFF と FDP_IFC を詳細化してこの目的に使うことは不適切であると考えられる。従って、この機能性を扱うために拡張コンポーネントを定義することとした。

この拡張コンポーネントは利用者データと TSF データ両方を保護し、そのため、FDP あるいは FPT クラスのいずれかに含まれる。この目的が TOE を悪用から保護することであるため、FPT クラスに含めるのが最適であると考えられる。いずれのクラスでも、既存のファミリにはうまく適合しないため、メンバが一つのみの新たなファミリを定義した。

**FPT_FDI_EXP.1　外部インタフェースへの制限された情報転送**

下位階層:　なし

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

FPT_FDI_EXP.1.1　TSF は、**[割付：外部インタフェースのリスト]**で受け取った情報を、TSF による追加の処理無しに**[割付：外部インタフェースのリスト]**に転送することを制限する能力を提供しなければならない。

# 6 セキュリティ要件

本章は、セキュリティ機能要件、セキュリティ保証要件、及びセキュリティ要件根拠を述べる。

## 6.1 セキュリティ機能要件

この章では、4.1 章で規定されたセキュリティ対策方針を実現するための、TOE のセキュリティ機能要件を記述する。なお、セキュリティ機能要件は、CC Part2 に規定のセキュリティ機能要件から、引用する。CC Part2 に規定されていないセキュリティ機能要件は、PP に規定の拡張セキュリティ機能要件から、引用する。

また、[CC]で定義された割付と選択操作を行った部分は、**[太文字と括弧]**で識別する。

### 6.1.1 クラス FAU: セキュリティ監査

**FAU_GEN.1 監査データ生成**

| | |
|---|---|
| 下位階層: | なし |
| 依存性: | FPT_STM.1 高信頼タイムスタンプ |
| FAU_GEN.1.1 | TSF は、以下の監査対象事象の監査記録を生成できなければならない:<br>a) 監査機能の起動と終了;<br>b) 監査の**[選択: 指定なし]**レベルのすべての監査対象事象;及び<br>c) **[割付: 表 7 に示す TOE の監査対象事象]**。 |
| FAU_GEN.1.2 | TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:<br>a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗);及び<br>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: FDP_ACF.1(a)におけるジョブタイプ、FIA_UID.1 における利用者識別を試みた全てのログインユーザー名、WIM による通信の通信方向、WIM による通信とフォルダー送信における通信先の IP アドレス、文書添付メール送信における宛先メールアドレス、ロックアウト操作種別、ロックアウト対象者、ロックアウト解除対象者]**。 |

機能要件毎に割り付けられた監査対象とすべき基本レベル以下のアクション(CC における規定)と、それに対応する TOE が監査対象とする事象を表 7 に記す。

**表 7：監査対象事象リスト**

| 機能要件 | 監査対象とすべきアクション | 監査対象事象 |
|---|---|---|
| FDP_ACF.1(a) | a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。<br>b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。<br>c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。 | 独自:<br>・文書情報の作成(蓄積)の開始と終了<br>・文書情報の作成(複製)の正常終了<br>・文書情報の印刷の開始と終了<br>・文書情報のダウンロードの開始と終了<br>・文書情報の文書添付メール送信の開始と終了<br>・文書情報のフォルダー送信の開始と終了<br>・文書情報の編集の終了<br>・文書情報の削除の開始と終了<br>上記における「作成・印刷・ダウンロード・文書添付メール送信・フォルダー送信・削除」が、PP において求められる追加情報のジョブタイプに相当する。 |
| FDP_ACF.1(b) | a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。<br>b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。<br>c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。 | 独自: 記録しない |
| FIA_AFL.1 | a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。 | a) 最小: ロックアウトの開始と解除 |
| FIA_UAU.1 | a) 最小: 認証メカニズムの不成功になった使用;<br>b) 基本: 認証メカニズムのすべての使用;<br>c) 詳細: 利用者認証以前に行われたすべての TSF 仲介アクション。 | b) 基本: ログイン操作の成功と失敗 |
| FIA_UID.1 | a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用;<br>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。 | b) 基本: ログイン操作の成功と失敗。これには、PP において求められる追加情報である利用者識別をも含む。 |
| FMT_SMF.1 | a) 最小: 管理機能の使用 | a) 最小: 表 25 管理機能の記録 |

| 機能要件 | 監査対象とすべきアクション | 監査対象事象 |
|---|---|---|
| FMT_SMR.1 | a) 最小: 役割の一部をなす利用者のグループに対する改変;<br>b) 詳細: 役割の権限の使用すべて。 | 改変はないので記録なし。 |
| FPT_STM.1 | a) 最小: 時間の変更;<br>b) 詳細: タイムスタンプの提供。 | a) 最小: 年月日時分の設定 |
| FTA_SSL.3 | a) 最小: セションロックメカニズムによる対話セションの終了。 | a) 最小: オートログアウトによるセションの終了 |
| FTP_ITC.1 | a) 最小: 高信頼チャネル機能の失敗。<br>b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。<br>c) 基本: 高信頼チャネル機能のすべての使用の試み。<br>d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。 | a) 最小: 高信頼チャネルとの通信の失敗 |

**FAU_GEN.2 利用者識別情報の関連付け**

下位階層: なし

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

FAU_GEN.2.1 識別された利用者のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

**FAU_STG.1 保護された監査証跡格納**

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

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

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を**[選択: 防止]**できねばならない。

**FAU_STG.4 監査データ損失の防止**

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、**[選択: 最も古くに格納された監査記録への上書き]**及び**[割付: 監査格納失敗時にとられるその他のアクションはない]**を行わなければならない。

**FAU_SAR.1 監査レビュー**

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.1.1 TSF は、**[割付: MFP 管理者]**が、**[割付: すべてのログ項目]**を監査記録から読み出せるようにしなければならない。

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

**FAU_SAR.2　限定監査レビュー**

下位階層:　なし

依存性:　FAU_SAR.1 監査レビュー

FAU_SAR.2.1　TSF は、明示的な読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出しアクセスを禁止しなければならない。

### 6.1.2　クラス FCS: 暗号サポート

**FCS_CKM.1　暗号鍵生成**

下位階層:　なし

依存性:　[FCS_CKM.2 暗号鍵配付、または FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1　TSFは、以下の**[割付：表 8に示す標準]**に合致する、指定された暗号鍵生成アルゴリズム**[割付：表 8 に示す暗号鍵生成アルゴリズム]**と指定された暗号鍵長**[割付：表 8 に示す暗号鍵長]**に従って、暗号鍵を生成しなければならない。

**表 8：暗号鍵生成のリスト**

| 鍵の種類 | 標準 | 暗号鍵生成アルゴリズム | 暗号鍵長 |
|---|---|---|---|
| HDD 暗号鍵 | BSI-AIS31 | TRNG | 256 ビット |

**FCS_COP.1　暗号操作**

下位階層:　なし

依存性:　[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1　TSFは、**[割付：表 9に示す標準]**に合致する、特定された暗号アルゴリズム**[割付：表 9に示す暗号アルゴリズム]**と暗号鍵長**[割付：表 9に示す暗号鍵長]**に従って、**[割付：表 9に示す暗号操作]**を実行しなければならない。

**表 9：暗号操作のリスト**

| 鍵の種類 | 標準 | 暗号<br>アルゴリズム | 暗号<br>鍵長 | 暗号操作 |
|---|---|---|---|---|
| HDD 暗号鍵 | FIPS197 | AES | 256<br>ビット | - HDD に書き込むデータの暗号化<br>- HDD から読込むデータの復号 |

### 6.1.3 クラス FDP: 利用者データ保護

**FDP_ACC.1(a) サブセットアクセス制御**

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1(a) TSF は、**[割付: 表 10 に示すサブジェクト、オブジェクト、及び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: 文書アクセス制御 SFP]**を実施しなければならない。

**表 10 : サブジェクト、オブジェクト、及びサブジェクトとオブジェクト間の操作のリスト(a)**

| | |
|---|---|
| サブジェクト | ・一般利用者プロセス<br>・MFP 管理者プロセス<br>・スーパーバイザープロセス |
| オブジェクト | ・文書情報<br>・利用者ジョブ |
| 操作 | ・読出し<br>・改変<br>・削除 |

**FDP_ACC.1(b) サブセットアクセス制御**

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1(b) TSF は、**[割付: 表 11 に示すサブジェクト、オブジェクト、及び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: TOE 機能アクセス制御 SFP]**を実施しなければならない。

**表 11 : サブジェクト、オブジェクト、及びサブジェクトとオブジェクト間の操作のリスト(b)**

| | |
|---|---|
| サブジェクト | ・一般利用者プロセス<br>・スーパーバイザープロセス |
| オブジェクト | ・MFP アプリケーション |
| 操作 | ・実行 |

**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

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

FDP_ACF.1.1(a) TSF は、以下の**[割付: 表 12 に示すサブジェクトまたはオブジェクトと、各々に対応するセキュリティ属性]**に基づいて、オブジェクトに対して、**[割付: 文書アクセス制御 SFP]**を実施しなければならない。

**表 12：サブジェクトとオブジェクトとセキュリティ属性(a)**

| 分類 | サブジェクトまたはオブジェクト | セキュリティ属性 |
|---|---|---|
| サブジェクト | 一般利用者プロセス | ・一般利用者のログインユーザー名<br>・利用者役割 |
| サブジェクト | MFP 管理者プロセス | ・利用者役割 |
| サブジェクト | スーパーバイザープロセス | ・利用者役割 |
| オブジェクト | 文書情報 | ・文書情報属性<br>・文書利用者リスト |
| オブジェクト | 利用者ジョブ | ・一般利用者のログインユーザー名 |

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を決定するために、次の規則を実施しなければならない: **[割付：表 13 に示すオブジェクトとサブジェクト間の操作を制御する規則]**。

**表 13：文書情報と利用者ジョブの操作を制御する規則(a)**

| オブジェクト | 文書情報属性 | 操作 | サブジェクト | 操作を制御する規則 |
|---|---|---|---|---|
| 文書情報 | +PRT | 削除 | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +PRT | 読出し | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +SCN | 削除 | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +SCN | 読出し | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +CPY | 削除 | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +CPY | 読出し | 一般利用者プロセス | 許可しない。ただし、文書情報を生成した一般利用者プロセスには許可する。 |
| 文書情報 | +DSR | 削除 | 一般利用者プロセス | 許可しない。ただし、文書情報の文書利用者リストに登録されている一般利用者のログインユーザー名の一般利用者プロセスには許可する。 |
| 文書情報 | +DSR | 読出し | 一般利用者プロセス | 許可しない。ただし、文書情報の文書利用者リストに登録されている一般利用者のログインユーザー名の一般利用者プロセスには許可する。 |
| 文書情報 | +DSR | 改変 | 一般利用者プロセス | 許可しない。ただし、文書情報の文書利用者リストに登録されている一般利用者のログインユーザー名の一般利用者プロセスには許可する。 |

| オブジェクト | 文書情報属性 | 操作 | サブジェクト | 操作を制御する規則 |
|---|---|---|---|---|
| 利用者ジョブ | 文書情報属性の設定なし | 削除 | 一般利用者プロセス | 許可しない。ただし、利用者ジョブのセキュリティ属性である一般利用者のログインユーザー名の一般利用者プロセスには許可する。 |

FDP_ACF.1.3(a) TSF は、次の追加規則、**[割付: 表 14 に示すオブジェクトとサブジェクト間の操作を制御する規則]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

**表 14 : 文書情報と利用者ジョブの操作を制御する追加の規則(a)**

| オブジェクト | 文書情報属性 | 操作 | サブジェクト | 操作を制御する規則 |
|---|---|---|---|---|
| 文書情報 | +PRT | 削除 | MFP 管理者プロセス | 許可する。 |
| 文書情報 | +DSR | 削除 | MFP 管理者プロセス | 許可する。 |
| 利用者ジョブ | 文書情報属性の設定なし | 削除 | MFP 管理者プロセス | 許可する。 |

FDP_ACF.1.4(a) TSF は、次の追加規則、**[割付: スーパーバイザープロセスの場合、文書情報と利用者ジョブへの操作を拒否する]**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。

**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

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

FDP_ACF.1.1(b) TSF は、以下の**[割付: 表 15 に示すサブジェクトまたはオブジェクトと、各々に対応するセキュリティ属性]**に基づいて、オブジェクトに対して、**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

**表 15 : サブジェクトとオブジェクトとセキュリティ属性(b)**

| 分類 | サブジェクトまたはオブジェクト | セキュリティ属性 |
|---|---|---|
| サブジェクト | 一般利用者プロセス | ・一般利用者のログインユーザー名<br>・利用機能リスト<br>・利用者役割 |
| | スーパーバイザープロセス | ・利用者役割 |
| オブジェクト | MFP アプリケーション | ・機能種別 |

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を決定するために、次の規則を実施しなければならない: **[割付: 表 16 に示すオブジェクトとサブジェクト間の操作を制御する規則]**。

**表 16 : MFP アプリケーションの操作を制御する規則(b)**

| オブジェクト | 操作 | サブジェクト | 操作を制御する規則 |
|---|---|---|---|
| MFP アプリケーション | 実行 | 一般利用者プロセス | MFP 管理者が、一般利用者プロセスの利用機能リストで許可した MFP アプリケーションの実行を許可する。 |

FDP_ACF.1.3(b) TSF は、次の追加規則、**[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則はなし]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4(b) TSF は、次の追加規則、**[割付: スーパーバイザープロセスの場合、MFP アプリケーションへの操作を拒否する]**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。

**FDP_RIP.1 サブセット情報保護**

下位階層: なし

依存性: なし

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

### 6.1.4 クラス FIA: 識別と認証

**FIA_AFL.1 認証失敗時の取り扱い**

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、**[割付: 表 17 に示す認証事象]**に関して、**[選択: [割付: 1～5]内における管理者設定可能な正の整数値]**回の不成功認証試行が生じたときを検出しなければならない。

**表 17 : 認証事象のリスト**

| 認証事象 |
|---|
| 操作パネルを使用する利用者認証 |
| クライアント PC から WIM を使用する利用者認証 |
| クライアント PC から印刷する際の利用者認証 |

FIA_AFL.1.2 不成功の認証試行が定義した回数**[選択: に達する]**とき、TSF は、**[割付: 表 18 に示すアクション]**をしなければならない。

**表 18：認証失敗時のアクションのリスト**

| 認証不成功者 | 認証失敗時アクション |
|---|---|
| 一般利用者 | MFP 管理者が設定したロックアウト時間、もしくは MFP 管理者が解除するまでロックアウト |
| スーパーバイザー | MFP 管理者が設定したロックアウト時間、もしくは MFP 管理者が解除、もしくは電源のオフ/オン後一定時間経過するまでロックアウト |
| MFP 管理者 | MFP 管理者が設定したロックアウト時間、もしくはスーパーバイザーが解除、もしくは電源のオフ/オン後一定時間経過するまでロックアウト |

**FIA_ATD.1　利用者属性定義**

下位階層:　なし

依存性:　なし

FIA_ATD.1.1　TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。**:[割付：表 19 の利用者毎に表 19 のセキュリティ属性のリストを維持する]**

**表 19：利用者毎の維持しなければならないセキュリティ属性のリスト**

| 利用者 | セキュリティ属性のリスト |
|---|---|
| 一般利用者 | ・一般利用者のログインユーザー名<br>・利用者役割<br>・利用機能リスト |
| スーパーバイザー | ・利用者役割 |
| MFP 管理者 | ・MFP 管理者のログインユーザー名<br>・利用者役割 |

**FIA_SOS.1　秘密の検証**

下位階層:　なし

依存性:　なし

FIA_SOS.1.1　TSF は、秘密が**[割付：以下の品質尺度]**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。

(1) 使用できる文字とその文字種
英大文字: [A-Z] (26 文字)
英小文字: [a-z] (26 文字)
数字: [0-9] (10 文字)
記号: SP(スペース) ! " # $ % & '　( ) * + , - . / : ; < = > ? @ [ ¥ ] ^ _ ` { | } ~　(33 文字)

(2) 登録可能な桁数
一般利用者の場合 ：
MFP 管理者が設定するパスワード最小桁数(8 から 32 桁)以上、128 桁以下
MFP 管理者、スーパーバイザーの場合 ：
MFP 管理者が設定するパスワード最小桁数(8 から 32 桁)以上、32 桁以下

(3) 規則

MFP 管理者が設定するパスワード複雑度に準じた文字種の組合せで作成したパスワードの登録を許可する。MFP 管理者は、パスワード複雑度に複雑度 1 か複雑度 2 を設定する。

**FIA_UAU.1　認証のタイミング**

下位階層:　なし

依存性:　FIA_UID.1 識別のタイミング

FIA_UAU.1.1　TSF は、利用者が認証される前に利用者を代行して行われる**[割付：利用者ジョブ一覧の参照、WIM のヘルプの参照、システム状態の参照、カウンタの参照、問い合わせ情報の参照]**を許可しなければならない。

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

**FIA_UAU.7　保護された認証フィードバック**

下位階層:　なし

依存性:　FIA_UAU.1 認証のタイミング

FIA_UAU.7.1　TSF は、認証を行っている間、**[割付：ダミー文字を認証フィードバックとして表示]**だけを利用者に提供しなければならない。

**FIA_UID.1　識別のタイミング**

下位階層:　なし

依存性:　なし

FIA_UID.1.1　TSF は、利用者が識別される前に利用者を代行して実行される**[割付：利用者ジョブ一覧の参照、WIM のヘルプの参照、システム状態の参照、カウンタの参照、問い合わせ情報の参照]**を許可しなければならない。

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

**FIA_USB.1　利用者-サブジェクト結合**

下位階層:　なし

依存性:　FIA_ATD.1 利用者属性定義

FIA_USB.1.1　TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:**[割付：一般利用者のログインユーザー名、MFP 管理者のログインユーザー名、利用機能リスト、利用者役割]**

FIA_USB.1.2　TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:**[割付：表 20 にリストした属性の最初の関連付けに関する規則]**

**表 20：属性の最初の関連付けに関する規則**

| 利用者 | サブジェクト | 利用者セキュリティ属性 |
|---|---|---|
| 一般利用者 | 一般利用者プロセス | ・一般利用者のログインユーザー名<br>・利用者役割<br>・利用機能リスト |
| スーパーバイザー | スーパーバイザープロセス | ・利用者役割 |
| MFP 管理者 | MFP 管理者プロセス | ・MFP 管理者のログインユーザー名<br>・利用者役割 |

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

### 6.1.5　クラス FMT: セキュリティ管理

**FMT_MSA.1(a)セキュリティ属性の管理**

下位階層:　なし

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

FMT_MSA.1.1(a) TSF は、セキュリティ属性**[割付：表 21 のセキュリティ属性]**に対し**[選択：問い合わせ、改変、削除、[割付：新規作成]]**をする能力を**[割付：表 21 の操作を許可する利用者役割]**に制限する**[割付：文書アクセス制御 SFP]**を実施しなければならない。

**表 21：セキュリティ属性の利用者役割(a)**

| セキュリティ属性 | 操作 | 操作を許可する利用者役割 |
|---|---|---|
| 一般利用者のログインユーザー名 | 問い合わせ、<br>改変、<br>削除、<br>新規作成 | MFP 管理者 |
| | 問い合わせ | 当該一般利用者 |
| スーパーバイザーのログインユーザー名 | 問い合わせ、<br>改変 | スーパーバイザー |
| MFP 管理者のログインユーザー名 | 新規作成 | MFP 管理者 |
| | 問い合わせ、<br>改変 | 当該 MFP 管理者 |
| | 問い合わせ | スーパーバイザー |
| 文書情報属性 | 許可される操作は無し | なし |

| セキュリティ属性 | 操作 | 操作を許可する利用者役割 |
|---|---|---|
| 文書利用者リスト<br>[文書情報属性が、(+PRT)、(+SCN)、及び(+CPY)の場合] | 許可される操作は無し | なし |
| 文書利用者リスト<br>[文書情報属性が、(+DSR)の場合] | 問い合わせ、<br>改変 | MFP 管理者、<br>文書情報を作成した当該一般利用者 |

**FMT_MSA.1(b)　セキュリティ属性の管理**

下位階層:　なし

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

FMT_MSA.1.1(b)TSF は、セキュリティ属性**[割付：表 22 のセキュリティ属性]**に対し**[選択：問い合わせ、改変、削除、[割付：新規作成]]**をする能力を**[割付：表 22 の操作を許可する利用者役割]**に制限する**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

**表 22：セキュリティ属性の利用者役割(b)**

| セキュリティ属性 | 操作 | 操作を許可する利用者役割 |
|---|---|---|
| 一般利用者のログインユーザー名 | 問い合わせ、<br>改変、<br>削除、<br>新規作成 | MFP 管理者 |
| | 問い合わせ | 当該一般利用者 |
| 利用機能リスト | 問い合わせ、<br>改変 | MFP 管理者 |
| | 問い合わせ | 当該一般利用者 |
| 機能種別 | 許可される操作は無し | なし |
| 利用者役割 | 許可される操作は無し | なし |

**FMT_MSA.3(a)静的属性初期化**

下位階層:　なし

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

FMT_MSA.3.1(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に対して**[選択：制限的]**デフォルト値を与える**[割付：文書アクセス制御 SFP]**を実施しなければならない。

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：表 23 に記す許可された識別された役割]**が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

**表 23 : デフォルト値を上書きできる許可された識別された役割**

| オブジェクト | セキュリティ属性 | 許可された識別された役割 |
|---|---|---|
| 文書情報 | 文書情報属性 | 許可された識別された役割はなし |
| 文書情報<br>[文書情報属性が、(+DSR)の場合] | 文書利用者リスト | MFP 管理者 |
| 文書情報<br>[文書情報属性が、(+PRT)、(+SCN)、及び(+CPY)の場合] | 文書利用者リスト | 許可された識別された役割はなし |
| 利用者ジョブ | 一般利用者のログインユーザー名 | 許可された識別された役割はなし |

**FMT_MSA.3(b)　静的属性初期化**

下位階層:　なし

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

FMT_MSA.3.1(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に対して**[選択: 制限的]**デフォルト値を与える**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

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はなし]**が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

**FMT_MTD.1 TSF データの管理**

下位階層:　なし

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

FMT_MTD.1.1　TSF は、**[割付: 表 24 の TSF データのリスト]**を**[選択: 問い合わせ、改変、削除、[割付: 新規作成]]**する能力を**[割付: 表 24 の利用者役割]**に制限しなければならない。

**表 24 : TSF データのリスト**

| TSF 情報 | 操作 | 利用者役割 |
|---|---|---|
| 一般利用者のログインパスワード | 新規作成、改変 | MFP 管理者 |
| | 改変 | 当該一般利用者 |
| スーパーバイザーのログインパスワード | 改変 | スーパーバイザー |
| MFP 管理者のログインパスワード | 改変 | スーパーバイザー |
| | 新規作成 | MFP 管理者 |
| | 改変 | 当該 MFP 管理者 |
| ログインパスワード入力許容回数 | 問い合わせ、改変 | MFP 管理者 |
| ロックアウト解除タイマー設定 | 問い合わせ、改変 | MFP 管理者 |
| ロックアウト時間 | 問い合わせ、改変 | MFP 管理者 |

| TSF 情報 | 操作 | 利用者役割 |
|---|---|---|
| 年月日時分の設定 | 問い合わせ、改変 | MFP 管理者 |
| | 問い合わせ | スーパーバイザー、一般利用者 |
| パスワード最小桁数 | 問い合わせ、改変 | MFP 管理者 |
| パスワード複雑度 | 問い合わせ、改変 | MFP 管理者 |
| 操作パネルオートログアウト時間 | 問い合わせ、改変 | MFP 管理者 |
| WIM オートログアウト時間 | 問い合わせ、改変 | MFP 管理者 |
| 監査ログ | 問い合わせ、削除 | MFP 管理者 |
| HDD 暗号鍵 | 新規作成 | MFP 管理者 |
| S/MIME 利用者情報 | 新規作成、改変、問い合わせ、削除 | MFP 管理者 |
| | 問い合わせ | 一般利用者 |
| 送信先フォルダー | 新規作成、改変、問い合わせ、削除 | MFP 管理者 |
| | 問い合わせ | 一般利用者 |
| ユーザー認証方法 | 問い合わせ | MFP 管理者 |
| IPsec 設定情報 | 問い合わせ、改変 | MFP 管理者 |
| 機器証明書 | 改変 | MFP 管理者 |

**FMT_SMF.1 管理機能の特定**

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。**:[割付: 表 25 に記す管理機能]**

**表 25 : 管理機能の特定のリスト**

| 管理機能 |
|---|
| MFP 管理者による、一般利用者のログインユーザー名の新規作成、問い合わせ、改変、及び削除 |
| 当該一般利用者による、一般利用者のログインユーザー名の問い合わせ |
| スーパーバイザーによる、スーパーバイザーのログインユーザー名の問い合わせと改変 |
| MFP 管理者による、MFP 管理者のログインユーザー名の新規作成 |
| 当該 MFP 管理者による、MFP 管理者のログインユーザー名の問い合わせと改変 |
| スーパーバイザーによる、MFP 管理者のログインユーザー名の問い合わせ |
| MFP 管理者による、一般利用者のログインパスワードの新規作成と改変 |
| 当該一般利用者による、一般利用者のログインパスワードの改変 |
| スーパーバイザーによる、スーパーバイザーのログインパスワードの改変 |
| スーパーバイザーによる、MFP 管理者のログインパスワードの改変 |

| 管理機能 |
| --- |
| MFP 管理者による、MFP 管理者のログインパスワードの新規作成 |
| 当該 MFP 管理者による、MFP 管理者のログインパスワードの改変 |
| MFP 管理者による、パスワード最小桁数の問い合わせと改変 |
| MFP 管理者による、パスワード複雑度の問い合わせと改変 |
| MFP 管理者による、操作パネルオートログアウト時間の問い合わせと改変 |
| MFP 管理者による、WIM オートログアウト時間の問い合わせと改変 |
| MFP 管理者による、ログインパスワード入力許容回数の問い合わせと改変 |
| MFP 管理者による、ロックアウト解除タイマー設定の問い合わせと改変 |
| MFP 管理者による、ロックアウト時間の問い合わせと改変 |
| MFP 管理者による、文書利用者リストの問い合わせと改変 |
| 文書を作成した当該一般利用者による、文書利用者リストの問い合わせと改変 |
| MFP 管理者による、利用機能リストの問い合わせと改変 |
| 当該一般利用者による、利用機能リストの問い合わせ |
| MFP 管理者による、文書利用者リストのデフォルト値の問い合わせと改変 |
| MFP 管理者による、年月日・時刻の問い合わせと改変 |
| スーパーバイザーによる、年月日・時刻の問い合わせ |
| 一般利用者による、年月日・時刻の問い合わせ |
| MFP 管理者による、監査ログの問い合わせと削除 |
| MFP 管理者による、HDD 暗号鍵の新規作成 |
| MFP 管理者による、S/MIME 利用者情報の新規作成、問い合わせ、改変、及び削除 |
| 一般利用者による、S/MIME 利用者情報の問い合わせ |
| MFP 管理者による、送信先フォルダーの新規作成、問い合わせ、改変、及び削除 |
| 一般利用者による、送信先フォルダーの問い合わせ |
| MFP 管理者による、ユーザー認証方法の問い合わせ |
| MFP 管理者による、IPsec 設定情報の問い合わせと改変 |
| MFP 管理者による、機器証明書の改変 |

**FMT_SMR.1 セキュリティの役割**

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割**[割付: 一般利用者、スーパーバイザー、MFP 管理者]**を維持しなければならない。

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

### 6.1.6 クラス FPT: TSF の保護

**FPT_STM.1 高信頼タイムスタンプ**

下位階層: なし

依存性: なし

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

**FPT_TST.1 TSF テスト**

下位階層: なし

依存性: なし

FPT_TST.1.1 TSF は、**[選択: [割付: MFP 制御ソフトウェア]]**の正常動作を実証するために、**[選択: 初期立上げ中]**自己テストのスイートを実行しなければならない。

FPT_TST.1.2 TSF は、許可利用者に、**[選択: [割付: 監査ログデータファイル]]**の完全性を検証する能力を提供しなければならない。

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

**FPT_FDI_EXP.1 外部インタフェースへの制限された情報転送**

下位階層: なし

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

FPT_FDI_EXP.1.1 TSF は、**[割付: 操作パネル、LAN]**で受け取った情報を、TSF による追加の処理無しに**[割付: LAN]**に転送することを制限する能力を提供しなければならない。

### 6.1.7 クラス FTA: TOE アクセス

**FTA_SSL.3 TSF 起動による終了**

下位階層: なし

依存性: なし

FTA_SSL.3.1 TSF は、**[割付: 操作パネルオートログアウト時間経過、WIM オートログアウト時間経過、プリンタードライバーからの文書情報の受信完了]**後に対話セションを終了しなければならない。

### 6.1.8 クラス FTP: 高信頼パス/チャネル

**FTP_ITC.1 TSF 間高信頼チャネル**

下位階層: なし

依存性: なし

FTP_ITC.1.1 TSFは、それ自身と他の高信頼IT製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネル情報の保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2　TSF は、**[選択: TSF、他の高信頼 IT 製品]**が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3　TSF は、**[割付: 文書情報、機能情報、保護情報、及び秘密情報の LAN 経由通信]**のために、高信頼チャネルを介して通信を開始しなければならない。

## 6.2　セキュリティ保証要件

本 TOE の評価保証レベルは EAL2+ALC_FLR.2 である。TOE の保証コンポーネントを表 26 に示す。これは評価保証レベルの EAL2 によって定義されたコンポーネントのセットに ALC_FLR.2 を追加したものである。

**表 26 : TOE セキュリティ保証要件(EAL2+ALC_FLR.2)**

| 保証クラス | 保証コンポーネント | |
|---|---|---|
| ADV:<br>開発 | ADV_ARC.1 | セキュリティアーキテクチャ記述 |
| | ADV_FSP.2 | セキュリティ実施機能仕様 |
| | ADV_TDS.1 | 基本設計 |
| AGD:<br>ガイダンス文書 | AGD_OPE.1 | 利用者操作ガイダンス |
| | AGD_PRE.1 | 準備手続き |
| ALC:<br>ライフサイクルサポート | ALC_CMC.2 | CM システムの使用 |
| | ALC_CMS.2 | TOE の一部の CM 範囲 |
| | ALC_DEL.1 | 配付手続き |
| | ALC_FLR.2 | 欠陥報告手続き |
| ASE:<br>セキュリティターゲット評価 | ASE_CCL.1 | 適合主張 |
| | ASE_ECD.1 | 拡張コンポーネント定義 |
| | ASE_INT.1 | ST 概説 |
| | ASE_OBJ.2 | セキュリティ対策方針 |
| | ASE_REQ.2 | 派生したセキュリティ要件 |
| | ASE_SPD.1 | セキュリティ課題定義 |
| | ASE_TSS.1 | TOE 要約仕様 |
| ATE:<br>テスト | ATE_COV.1 | カバレージの証拠 |
| | ATE_FUN.1 | 機能テスト |
| | ATE_IND.2 | 独立テスト - サンプル |
| AVA:<br>脆弱性評定 | AVA_VAN.2 | 脆弱性分析 |

## 6.3　セキュリティ要件根拠

本章では、セキュリティ要件の根拠を述べる。

以下に示すように、すべてのセキュリティ機能要件が満たされた場合、「4 セキュリティ対策方針」で定義した TOE のセキュリティ対策方針は達成される。

### 6.3.1 追跡性

TOE のセキュリティ対策方針に対するセキュリティ機能要件の対応関係を下記の表 27 に示す。表 27 から明らかなように、セキュリティ機能要件が少なくとも 1 つ以上のセキュリティ対策方針に対応している。

**表 27：セキュリティ対策方針と機能要件の関連**

| | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.STORAGE.ENCRYPTED |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | | | | | | x | |
| FAU_GEN.2 | | | | | | | | | | x | |
| FAU_STG.1 | | | | | | | | | | x | |
| FAU_STG.4 | | | | | | | | | | x | |
| FAU_SAR.1 | | | | | | | | | | x | |
| FAU_SAR.2 | | | | | | | | | | x | |
| FCS_CKM.1 | | | | | | | | | | | x |
| FCS_COP.1 | | | | | | | | | | | x |
| FDP_ACC.1(a) | x | x | x | | | | | | | | |
| FDP_ACC.1(b) | | | | | | | x | | | | |
| FDP_ACF.1(a) | x | x | x | | | | | | | | |
| FDP_ACF.1(b) | | | | | | | x | | | | |
| FDP_RIP.1 | x | x | | | | | | | | | |
| FIA_AFL.1 | | | | | | | x | | | | |
| FIA_ATD.1 | | | | | | | x | | | | |
| FIA_SOS.1 | | | | | | | x | | | | |
| FIA_UAU.1 | | | | | | | x | x | | | |
| FIA_UAU.7 | | | | | | | x | | | | |
| FIA_UID.1 | | | | | | | x | x | | | |
| FIA_USB.1 | | | | | | | x | | | | |

| | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.STORAGE.ENCRYPTED |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FPT_FDI_EXP.1 | | | | | | | | X | | | |
| FMT_MSA.1(a) | X | X | X | | | | | | | | |
| FMT_MSA.1(b) | | | | | | | X | | | | |
| FMT_MSA.3(a) | X | X | X | | | | | | | | |
| FMT_MSA.3(b) | | | | | | | X | | | | |
| FMT_MTD.1 | | | | X | X | X | | | | | X |
| FMT_SMF.1 | | | | X | X | X | | | | | X |
| FMT_SMR.1 | | | | X | X | X | | | | | X |
| FPT_STM.1 | | | | | | | | | | X | |
| FPT_TST.1 | | | | | | | | | X | | |
| FTA_SSL.3 | | | | | | | X | X | | | |
| FTP_ITC.1 | X | X | X | X | X | X | | | | | |

### 6.3.2 追跡性の正当化

以下に、TOE セキュリティ対策方針が、対応付けられた TOE セキュリティ機能要件によって実現できることを説明する。

**O.DOC.NO_DIS 文書の開示保護**

O.DOC.NO_DIS は、文書が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって開示されることを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 文書情報へのアクセス制御を規定して実施する
FDP_ACC.1(a)と FDP_ACF.1(a)によって、文書情報の読出しは、文書情報属性により、文書情報を生成した一般利用者または文書情報の文書利用者リストに登録されている一般利用者だけに読み出しを許可する。MFP 管理者及びスーパーバイザーに対しては文書情報の読出しを許可しない。

(2) 削除された文書、一時的な文書あるいはその断片の読出しを防ぐ
FDP_RIP.1 によって、削除された文書、一時的な文書あるいはその断片の読出しを防ぐ。

(3) 文書情報の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する文書情報は保護される。

(4) セキュリティ属性の管理
ログインユーザー名に対して可能な操作(新規作成、問い合わせ、改変、削除)、文書利用者リストに対して可能な操作(問い合わせ、改変)は、FMT_MSA.1(a)によって、それぞれの操作を特定の利用者だけに制限している。
文書情報(オブジェクト)のセキュリティ属性には、FMT_MSA.3(a)によって、文書情報が生成された時に、必ず制限的な値がセットされる。

これらの対策に必要なセキュリティ機能要件として該当する FDP_ACC.1(a)、FDP_ACF.1(a)、FDP_RIP.1、FTP_ITC.1、FMT_MSA.1(a)、FMT_MSA.3(a)を達成することで O.DOC.NO_DIS を実現できる。

**O.DOC.NO_ALT 文書の改変保護**

O.DOC.NO_ALT は、文書が、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって改変されることを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 文書情報へのアクセス制御を規定して実施する
FDP_ACC.1(a)とFDP_ACF.1(a)によって、文書情報の改変と削除は、文書情報属性により、文書情報を生成した一般利用者または文書情報の文書利用者リストに登録されている一般利用者に許可する。さらに、MFP 管理者に対しては文書の削除を許可するが、文書情報の改変は許可しない。スーパーバイザーに対しては文書情報の改変と削除を許可しない。

(2) 削除された文書、一時的な文書あるいはその断片の改変を防ぐ
FDP_RIP.1 によって、削除された文書、一時的な文書あるいはその断片を利用できないようにする。

(3) 文書情報の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する文書情報は保護される。

(4) セキュリティ属性の管理
ログインユーザー名に対して可能な操作(新規作成、問い合わせ、改変、削除)、文書利用者リストに対して可能な操作(問い合わせ、改変)は、FMT_MSA.1(a)によって、それぞれの操作を特定の利用者だけに制限している。
文書情報(オブジェクト)のセキュリティ属性には、FMT_MSA.3(a)によって、文書情報が生成された時に、必ず制限的な値がセットされる。

これらの対策に必要なセキュリティ機能要件として該当する FDP_ACC.1(a)、FDP_ACF.1(a)、FDP_RIP.1、FTP_ITC.1、FMT_MSA.1(a)、FMT_MSA.3(a)を達成することで O.DOC.NO_ALT を実現できる。

**O.FUNC.NO_ALT 利用者ジョブの改変保護**

O.FUNC.NO_ALT は、利用者ジョブが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブへのアクセス権限をもたない者によって改変されることを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 利用者ジョブへのアクセス制御を規定して実施する
FDP_ACC.1(a)とFDP_ACF.1(a)によって、利用者ジョブの削除は、MFP 管理者と当該利用者ジョブの削除権限をもつ一般利用者に対して許可する。スーパーバイザーに対しては利用者ジョブの削除を許可しない。尚、本 TOE の利用者ジョブの改変は、利用者ジョブの削除だけである。

(2) 利用者ジョブの送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する利用者ジョブは保護される。

(3) セキュリティ属性の管理
ログインユーザー名に対して可能な操作(新規作成、問い合わせ、改変、削除)は、FMT_MSA.1(a)によって、それぞれの操作を特定の利用者だけに制限している。
利用者ジョブ(オブジェクト)のセキュリティ属性には、FMT_MSA.3(a)によって、利用者ジョブを生成した時、制限的な値がセットされる。

これらの対策に必要なセキュリティ機能要件として該当する FDP_ACC.1(a)、FDP_ACF.1(a)、FTP_ITC.1、FMT_MSA.1(a)、FMT_MSA.3(a)を達成することで O.FUNC.NO_ALT を実現できる。

**O.PROT.NO_ALT TSF 保護情報の改変保護**

O.PROT.NO_ALT は、TSF 保護情報の改変を、セキュリティが維持できる利用者だけに許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) TSF 保護情報の管理
FMT_MTD.1 によって、パスワード最小桁数、パスワード複雑度、ログインパスワード入力許容回数、ロックアウト解除タイマー設定、ロックアウト時間、年月日、時刻、S/MIME 利用者情報、送信先フォルダー、IPsec 設定情報、機器証明書、操作パネルオートログアウト時間、WIM オートログアウト時間、及びユーザー認証方法の管理を MFP 管理者だけに許可する。

(2) 管理機能の特定
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能は実施されている。

(3) 役割の特定
FMT_SMR.1 によって、特権をもつ利用者を維持する。

(4) TSF 保護情報の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 保護情報は保護される。

これらの対策に必要なセキュリティ機能要件として該当する FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FTP_ITC.1 を達成することで O.PROT.NO_ALT を実現できる。

**O.CONF.NO_DIS TSF 秘密情報の開示保護**

O.CONF.NO_DIS は、TSF 秘密情報の開示を、セキュリティが維持できる利用者だけに許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) TSF 秘密情報の管理
FMT_MTD.1 によって、一般利用者のログインパスワードに対する操作を MFP 管理者と当該一般利用者に許可する。スーパーバイザーのログインパスワードに対する操作をスーパーバイザーに許可する。MFP 管理者のログインパスワードに対する操作をスーパーバイザーと当該 MFP 管理者に許可する。監査ログに対する操作を MFP 管理者だけに許可する。HDD 暗号鍵に対する操作を MFP 管理者だけに許可する。

(2) 管理機能の特定
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能は実施されている。

(3) 役割の特定
FMT_SMR.1 によって、特権をもつ利用者を維持する。

(4) TSF 秘密情報の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 秘密情報は保護される。

これらの対策に必要なセキュリティ機能要件として該当する FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FTP_ITC.1 を達成することで O.CONF.NO_DIS を実現できる。

**O.CONF.NO_ALT TSF 秘密情報の改変保護**

O.CONF.NO_ALT は、TSF 秘密情報の改変を、セキュリティが維持できる利用者だけに許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) TSF 秘密情報の管理
FMT_MTD.1 によって、一般利用者のログインパスワードに対する操作を MFP 管理者と当該一般利用者に許可する。スーパーバイザーのログインパスワードに対する操作をスーパーバイザーに許可する。MFP 管理者のログインパスワードに対する操作をスーパーバイザーと当該 MFP 管理者に許可する。監査ログに対する操作を MFP 管理者だけに許可する。HDD 暗号鍵の新規作成操作を、MFP 管理者だけに許可する。

(2) 管理機能の特定
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能は実施されている。

(3) 役割の特定
FMT_SMR.1 によって、特権をもつ利用者を維持する。

(4) TSF 秘密情報の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 秘密情報は保護される。

これらの対策に必要なセキュリティ機能要件として該当する FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FTP_ITC.1 を達成することで O.CONF.NO_ALT を実現できる。

**O.USER.AUTHORIZED 利用者の識別認証**

O.USER.AUTHORIZED は、正当な利用者だけが TOE の機能を利用するためのセキュリティポリシーに従って利用者の制限をするセキュリティ対策方針である。操作パネルまたはネットワーク上のクライアント PC から TOE を利用する一般利用者、MFP 管理者、及びスーパーバイザーについては、認証失敗時の取り扱いと秘密の検証のセキュリティポリシーの追加が必要である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) TOE 利用前に利用者を識別認証する
FIA_UID.1 と FIA_UAU.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者に対して、識別認証が行われる。

(2) 識別認証が成功した利用者に TOE の利用を許可する
FIA_ATD.1 と FIA_USB.1 によって、予め定義された利用者の保護資産へのアクセス手段を管理され、識別認証に成功した利用者に対して関連付けられる。
FDP_ACC.1(b)と FDP_ACF.1(b)によって、識別認証に成功した一般利用者に与えられた MFP アプリケーションの利用権限に従って、当該一般利用者に MFP アプリケーションの利用を許可する。

(3) ログインパスワードの解析を困難にする
FIA_UAU.7 によって、ダミー文字を認証フィードバックとして表示することで、ログインパスワードの開示を防止する。
FIA_SOS.1 によって、MFP 管理者が設定するパスワードの最小桁数、パスワードの文字種組合せを満たすパスワードだけの登録を許可することでログインパスワードの推測を困難にする。
FIA_AFL.1 によって、認証失敗を一定回数繰り返した利用者に対して、一定時間 TOE へのアクセスを許可しない。

(4) ログインを自動で終了する
FTA_SSL.3 によって、ログイン状態の操作パネル、あるいはクライアント PC からオートログアウトする。
プリンタードライバーから文書情報の受信完了時に文書情報受信のログイン状態をログアウトする。

(5) セキュリティ属性の管理
FMT_MSA.1(b)によって、一般利用者のログインユーザー名と利用機能リストは MFP 管理者によって管理され、機能種別は、利用者に対して操作を許可しない。
FMT_MSA.3(b)によって、機能種別を制限的なデフォルト値に設定する。

したがって、これらの対策に必要なセキュリティ機能要件として該当する FDP_ACC.1(b)、FDP_ACF.1(b)、FIA_UID.1、FIA_UAU.1、FIA_ATD.1、FIA_USB.1、FIA_UAU.7、FIA_AFL.1、FIA_SOS.1、FTA_SSL.3、FMT_MSA.1(b)、FMT_MSA.3(b)を達成することで O.USER.AUTHORIZED を実現できる。

なお、PP からの選択 SFR Package である 2600.2-SMI の機能(F.SMI)は、FDP_ACC.1(b)と FDP_ACF.1(b)によって、アクセス制御を行なっている機能の中で使用される機能である。したがって、F.SMI のアクセス制御は FDP_ACC.1(b)と FDP_ACF.1(b)によるアクセス制御に含めて実現している。

**O.INTERFACE.MANAGED TOE による外部インタフェース管理**

O.INTERFACE.MANAGED は、TOE がセキュリティポリシーに従って外部インタフェースの運用を管理することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 操作パネル、LAN インタフェースは利用前に利用者を識別認証する
FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者の識別が行われ、FIA_UAU.1 によって、識別された利用者の認証が行われる。

(2) 操作パネルあるいは LAN インタフェースへの接続を自動で終了する
FTA_SSL.3 によって、一定時間操作パネルあるいは LAN インタフェースの操作がない場合にセションを終了する。

(3) 外部インタフェースへの制限された情報転送
FPT_FDI_EXP.1 によって操作パネル、LAN インタフェースで受信したデータを、TSF による追加の処理無しに LAN から送信することを防止する。

これらの対策に必要なセキュリティ機能要件として該当する FIA_UID.1FIA_UAU.1、FTA_SSL.3、FPT_FDI_EXP.1 を達成することで O.INTERFACE.MANAGED を実現できる。

**O.SOFTWARE.VERIFIED ソフトウェア検証**

O.SOFTWARE.VERIFIED は、TOE は TSF の実行コードを自己検証できるための手段の提供を保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) セルフチェック
FPT_TST.1 によって、起動時に MFP 制御ソフトウェアが正規のソフトウェアであることを確認する。

この対策に必要なセキュリティ機能要件として該当する FPT_TST.1 を達成することで O.SOFTWARE.VERIFIED を実現できる。

**O.AUDIT.LOGGED 監査ログ記録管理**

O.AUDIT.LOGGED は、セキュリティ侵害を検証するために必要な監査ログの記録をし、さらに監査ログの参照を MFP 管理者に許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 監査ログを記録する
FAU_GEN.1 と FAU_GEN.2 によって、監査対象とすべき事象を監査対象とすべき事象の発生要因の識別情報とともに記録する。

(2) 監査ログを保護する
FAU_STG.1 によって監査ログは改変から保護され、FAU_STG.4 によって監査ログファイルがいっぱいの状態で監査対象の事象が発生した場合は、タイムスタンプの最も古い監査ログを削除し、新しい監査ログを記録する。

(3) 監査機能を提供する
FAU_SAR.1 によって、MFP 管理者が検証できる形式で監査ログを読み出せるようにし、FAU_SAR.2 によって、MFP 管理者以外が監査ログを読み出すことを禁止する。

(4) 信頼できる事象発生時間
FPT_STM.1 によって信頼できるタイムスタンプが提供され、監査ログには監査事象が発生した正確な時間が記録される。

これらの対策に必要なセキュリティ機能要件として該当する FAU_GEN.1、FAU_GEN.2、FAU_STG.1、FAU_STG.4、FAU_SAR.1、FAU_SAR.2、FPT_STM.1 を達成することで O.AUDIT.LOGGED を実現できる。

**O.STORAGE.ENCRYPTED 記憶装置暗号化**

O.STORAGE.ENCRYPTED は、HDD に書き込むデータを暗号化することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を実施する必要がある。

(1) 適切な暗号鍵を生成する
FCS_CKM.1 によって、暗号化のために必要な暗号鍵が生成される。

(2) 暗号操作をする
FCS_COP.1 によって、HDD に蓄積されるデータが暗号化され、HDD から読み出されるデータが復号される。

(3) TSF データを管理する
FMT_MTD.1 によって、暗号鍵は MFP 管理者によって管理される。

(4) 管理機能の特定
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能は実施されている。

(5) 役割の特定
FMT_SMR.1 によって、特権をもつ利用者を維持する

これらの対策に必要なセキュリティ機能要件として該当する FCS_CKM.1、FCS_COP.1、FMT_MTD.1、FMT_SMF.1、及び FMT_SMR.1 を達成することで O.STORAGE.ENCRYPTED を実現できる。

### 6.3.3 依存性分析

TOE セキュリティ機能要件について、本 ST での依存性の分析結果を表 28 に示す。

**表 28 : TOE セキュリティ機能要件の依存性分析結果**

| TOE セキュリティ機能要件 | 要求された依存性 | ST の中で満たしている依存性 | ST の中で満たしていない依存性 |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 | なし |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | FAU_GEN.1<br>FIA_UID.1 | なし |
| FAU_STG.1 | FAU_GEN.1 | FAU_GEN.1 | なし |
| FAU_STG.4 | FAU_STG.1 | FAU_STG.1 | なし |
| FAU_SAR.1 | FAU_GEN.1 | FAU_GEN.1 | なし |
| FAU_SAR.2 | FAU_SAR.1 | FAU_SAR.1 | なし |
| FCS_CKM.1 | [FCS_CKM.2 または FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1 | FCS_CKM.4 |
| FCS_COP.1 | [FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4 |
| FDP_ACC.1(a) | FDP_ACF.1(a) | FDP_ACF.1(a) | なし |
| FDP_ACC.1(b) | FDP_ACF.1(b) | FDP_ACF.1(b) | なし |
| FDP_ACF.1(a) | FDP_ACC.1(a)<br>FMT_MSA.3(a) | FDP_ACC.1(a)<br>FMT_MSA.3(a) | なし |
| FDP_ACF.1(b) | FDP_ACC.1(b)<br>FMT_MSA.3(b) | FDP_ACC.1(b)<br>FMT_MSA.3(b) | なし |
| FDP_RIP.1 | なし | なし | なし |
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.1 | なし |
| FIA_ATD.1 | なし | なし | なし |
| FIA_SOS.1 | なし | なし | なし |
| FIA_UAU.1 | FIA_UID.1 | FIA_UID.1 | なし |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.1 | なし |
| FIA_UID.1 | なし | なし | なし |
| FIA_USB.1 | FIA_ATD.1 | FIA_ATD.1 | なし |
| FPT_FDI_EXP.1 | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 | なし |
| FMT_MSA.1(a) | [FDP_ACC.1(a) または FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1(a)<br>FMT_SMR.1<br>FMT_SMF.1 | なし |

| TOE セキュリティ機能要件 | 要求された依存性 | ST の中で満たしている依存性 | ST の中で満たしていない依存性 |
|---|---|---|---|
| FMT_MSA.1(b) | [FDP_ACC.1(b)<br>または FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1(b)<br>FMT_SMR.1<br>FMT_SMF.1 | なし |
| FMT_MSA.3(a) | FMT_MSA.1(a)<br>FMT_SMR.1 | FMT_MSA.1(a)<br>FMT_SMR.1 | なし |
| FMT_MSA.3(b) | FMT_MSA.1(b)<br>FMT_SMR.1 | FMT_MSA.1(b)<br>FMT_SMR.1 | なし |
| FMT_MTD.1 | FMT_SMR.1<br>FMT_SMF.1 | FMT_SMR.1<br>FMT_SMF.1 | なし |
| FMT_SMF.1 | なし | なし | なし |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 | なし |
| FPT_STM.1 | なし | なし | なし |
| FPT_TST.1 | なし | なし | なし |
| FTA_SSL.3 | なし | なし | なし |
| FTP_ITC.1 | なし | なし | なし |

以下に、依存性が満たされていなくても問題ない根拠を記述する。

**FCS_CKM.4 への依存性除去理由**

本 TOE の HDD 暗号化に用いられる暗号鍵は、TOE の運用開始時に MFP 管理者が生成した後、その HDD に対して継続的に使用されるため、削除されることはない。従って、標準の方法を用いた暗号鍵廃棄の機能要件は不要である。

### 6.3.4 セキュリティ保証要件根拠

本 TOE は市販製品の MFP である。MFP は一般的なオフィスで使用されることを想定しており、本 TOE は強化基本レベル以上の攻撃能力を持つ攻撃者は想定していない。

また、TOE 設計の評価(ADV_TDS.1)は市販製品の正当性を示すのに十分である。さらに、TSF を回避あるいは改変するような攻撃には高い攻撃能力が要求され、これは今回の評価の対象外である。すなわち、一般的なニーズには基本的な攻撃能力を持つ攻撃者からの攻撃への対処(AVA_VAN.2)で十分である。

また、TOE を継続してセキュアに運用するため、運用開始後に発見された欠陥を欠陥報告手続き(ALC_FLR.2)によって適切に修正することは重要である。

従って、評価期間とコストを考慮すると、本 TOE に対する評価保証レベルは EAL2+ALC_FLR.2 が妥当である。

# 7 TOE 要約仕様

本章は、TOE 要約仕様をセキュリティ機能毎に示す。さらに、セキュリティ機能は対応するセキュリティ機能要件ごとに示す。

## 7.1 監査機能

監査機能は、TOE の使用の事象、及びセキュリティに関連する事象(以下、監査事象と言う)のログを監査ログとして記録し、記録した監査ログを監査できる形式で提供する(監査ログのレビュー)機能である。記録した監査ログは、MFP 管理者だけに読出しと削除を許可する。

**FAU_GEN.1、FAU_GEN.2**

TOE は、表 29 に示す監査事象発生時に、表 30 に示す監査ログ項目を TOE 内の HDD に記録する。
監査ログ項目には、共通ログ項目と個別ログ項目がある。共通ログ項目は、監査ログを記録するとき必ず記録する監査データ項目であり、個別ログ項目は、表 30 に示す監査ログ項目を記録する監査事象発生時のみ記録する。

**FPT_STM.1**

TOE は、監査ログに記録する日付(年月日)・時間(時分秒)を TOE のシステム時計から取得する。

**FAU_SAR.1、FAU_SAR.2、FAU_STG.1**

TOE は、MFP 管理者がアクセスした時のみ WIM の画面に監査ログの読出しの操作メニューを表示する。
MFP 管理者が監査ログの読出しを TOE に指示すると、TOE は監査ログをテキスト形式で提供する。

**FAU_STG.4**

TOE は、監査ログファイルに監査ログを追加記録する領域がない場合には、最新の監査ログを最も古い監査ログに上書きする。

**表 29：監査事象リスト**

| 監査事象 |
|---|
| 監査機能の開始 |
| 監査機能の終了 |
| ログイン操作の成功と失敗 |
| ロックアウトの開始と解除 |
| 表 25 管理機能の記録 |
| 年月日時分の設定 |
| オートログアウトによるセションの終了 |

| 監査事象 |
|---|
| WIM の通信の失敗 |
| フォルダー送信 |
| 文書添付メール送信 |
| ネットワークを介した印刷 |
| 文書情報の作成(蓄積) |
| 文書情報の作成(複製)の正常終了 |
| 文書情報の読出し(印刷、ダウンロード、文書添付メール送信、フォルダー送信) |
| 文書情報の改変(編集)の終了 |
| 文書情報の削除 |

**表 30：監査ログ項目のリスト**

| | 監査ログ項目 | 監査ログ項目への設定値 | 監査ログを記録する監査事象 |
|---|---|---|---|
| 共通ログ項目 | 事象の開始日付・時刻 | 事象発生時の TOE のシステム時計の値 | ・表 29 に示す全ての監査対象事象 |
| | 事象の終了日付・時刻 | 事象終了時の TOE のシステム時計の値 | |
| | 事象の種別 | 監査事象の識別情報 | |
| | サブジェクト識別情報 | 監査事象の発生原因となった利用者または TOE の識別情報 | |
| | 結果(*1) | 監査事象の結果(成功または失敗) | |
| 個別ログ項目 | 通信方向 | 通信方向(IN/OUT) | ・WIM の通信 |
| | 通信先 IP アドレス | 通信先 IP アドレス | ・WIM の通信<br>・フォルダー送信<br>・ネットワークを介した印刷 |
| | 宛先メールアドレス | 文書添付メール送信時の宛先メールアドレス | ・文書添付メール送信 |
| | ロックアウト操作種別 | ロックアウト開始とロックアウト解除を識別するための情報 | ・ロックアウトの開始と解除 |
| | ロックアウト対象者 | ロックアウトした利用者のログインユーザー名 | ・ロックアウトの開始と解除 |
| | ロックアウト解除対象者 | ロックアウト解除した利用者のログインユーザー名 | ・ロックアウトの開始と解除 |

(*1): 監査事象が「WIM の通信の失敗」の場合は、結果として失敗を記録する。

## 7.2 識別認証機能

識別認証機能は、TOEを利用しようとする者が許可利用者(MFP管理者、スーパーバイザー及び一般利用者)であるかを利用者から取得した識別認証情報を使って検証し、許可利用者と判断された者だけに TOEの利用を許可する機能である。

**FIA_UAU.1、FIA_UID.1**

TOE は、利用者が入力したログインユーザー名とログインパスワードで識別認証をする。ただし、利用者ジョブ一覧の参照、WIM のヘルプの参照、システム状態の参照、カウンタの参照、及び問い合わせ情報の参照は識別認証をしなくても TOE の利用を許可する。
利用者が操作パネルまたはクライアント PC から WIM を利用する場合は、ログインユーザー名とログインパスワードを入力するための画面を表示し、利用者がログインユーザー名とログインパスワードを入力するまで画面を表示し続ける。
利用者がプリンタードライバーから利用する場合は、TOE はプリンタードライバーから利用者が入力したログインユーザー名とログインパスワードを受信する。
利用者が入力したログインユーザー名が、一般利用者、MFP 管理者、またはスーパーバイザーの場合、TOE は、利用者が入力したログインパスワードと、TOE に予め登録されているログインパスワードが一致することを確認する。

**FIA_USB.1、FIA_ATD.1、FMT_SMR.1**

TOE は、FIA_UAU.1、及び FIA_UID.1 の照合の結果、認証に成功した利用者を、識別された利用者役割(一般利用者、MFP 管理者、あるいはスーパーバイザー)として TOE の利用を許可する。ログイン時に割り当てられた利用者役割は、ログアウトするまで維持する。認証に失敗した場合は TOE の利用を許可しない。

**FTA_SSL.3**

TOE は、利用者が操作パネル、Web ブラウザ、プリンタードライバーからログインしている場合、以下に示す条件を満たすとログアウトする。
操作パネルの場合、操作パネルに対する最終操作から経過した時間が、操作パネルオートログアウト時間(60～999 秒)に達した時、ログアウトする。
Web ブラウザの場合、Web ブラウザに対する最終操作から経過した時間が、WIM オートログアウト時間(3～60 分)に達した時、ログアウトする。
プリンタードライバーの場合、プリンタードライバーからの印刷情報を受信し終わった直後にログアウトする。

**FIA_UAU.7**

TOE は、操作パネルから TOE を利用しようとする者、またはクライアント PC から WIM を利用しようとする者が入力するログインパスワードについて、入力した文字を表示せず、入力した文字数分のダミー文字を表示する。

**FIA_AFL.1**

TOE は、一般利用者、MFP 管理者、及びスーパーバイザーのログインユーザー名による認証失敗が連続した回数をカウントする。連続で認証に失敗した回数が、ログインパスワード入力許容回数を越えたログインユーザー名をロックアウトする。

ロックアウトとなったログインユーザー名は、以下の条件の内いずれかが成立するまでログインできない。

・MFP 管理者が設定したロックアウト時間が経過するまで

・表 31 に示す利用者役割毎に定められたロックアウト解除者によってロックアウト解除されるまで

・MFP 管理者とスーパーバイザーは、MFP の電源 OFF/ON 後に MFP が実行可能状態になってから 60 秒経過するまで

**表 31：利用者役割毎のロックアウト解除者**

| 利用者役割(ロックアウト対象者) | ロックアウト解除者 |
|---|---|
| 一般利用者 | MFP 管理者 |
| スーパーバイザー | MFP 管理者 |
| MFP 管理者 | スーパーバイザー |

**FIA_SOS.1**

利用者のログインパスワードは、以下の条件を満たす場合だけ登録できる。

(1) 使用できる文字とその文字種

英大文字: [A-Z] (26 文字)

英小文字: [a-z] (26 文字)

数字: [0-9] (10 文字)

記号: SP(スペース)! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ¥ ] ^ _ ` { | } ~ (33 文字)

(2) 登録可能な桁数

・一般利用者の場合

MFP 管理者が設定するログインパスワード最小桁数(8 から 32 桁)以上、128 桁以下

・MFP 管理者、スーパーバイザーの場合

MFP 管理者が設定するログインパスワード最小桁数(8 から 32 桁)以上、32 桁以下

(3) 文字種の組合せ

MFP 管理者が決定する文字種の組合せ数(2 種類以上、あるいは 3 種類以上)。

**FPT_FDI_EXP.1**

操作パネルあるいは LAN インタフェースを介したクライアント PC からの入力情報は、必ず TSF による識別認証を行った後、情報入力のアクションを行うため、TSF の関与なしに入力情報が転送されることはない。

## 7.3 文書アクセス制御機能

文書アクセス制御機能は、TOE の許可利用者に対して、その利用者の役割に与えられた権限、または利用者毎に与えられた権限に基づいて、文書情報と利用者ジョブへの操作を許可する機能である。

**FDP_ACC.1(a)、FDP_ACF.1(a)**

TOE は、(1)文書情報のアクセス制御ルール、(2)利用者ジョブへのアクセス制御ルールに従って、利用者による文書情報と利用者ジョブへの操作を制限する。

(1) 文書情報のアクセス制御ルール

TOE は、蓄積文書を印刷、クライアント PC へのダウンロード、文書添付メール送信、フォルダー送信、複製、編集、削除、及び全削除するためのインタフェースを利用者に提供する。複製とはドキュメントボックス文書と同じ文書情報を新しく作成し蓄積する機能である。編集とは、ドキュメントボックス文書の任意のページに他のドキュメントボックス文書を挿入する機能と、ドキュメントボックス文書の任意のページを削除する機能である。

蓄積文書への操作が許可される利用者は、MFP 管理者と一般利用者だけで、スーパーバイザーには許可しない。

MFP 管理者と一般利用者が、操作パネルから TOE へログイン、またはクライアント PC から WIM へログインすると、操作を許可する蓄積文書の一覧と、許可する操作(印刷、ダウンロード、文書添付メール送信、フォルダー送信、複製、編集、削除、全削除)のメニューを表示する。MFP 管理者が、操作パネルから TOE へログイン、またはクライアント PC から WIM へログインした場合は、全蓄積文書の一覧と、削除、全削除の操作メニューが表示される。MFP 管理者は、蓄積文書の一覧から削除したい文書を選択して削除を実行するか、全削除を実行することができる。

蓄積文書には文書利用者リストが設定される。文書利用者リストには、操作を許可する一般利用者のログインユーザー名が登録される。文書利用者リストは蓄積文書毎に設定され、蓄積文書毎に操作を許可する一般利用者が設定される。一般利用者が、操作パネルから TOE へログイン、またはクライアント PC から WIM へログインしたとき表示される蓄積文書の一覧には、ログインした一般利用者が登録された文書利用者リストを持つ蓄積文書と表 32 の規則に従った操作メニューを表示する。尚、文書利用者リストを編集する権限については、「7.8 セキュリティ管理機能」に示す。

また TOE は、利用者がコピー機能、プリンター機能、スキャナー機能、及びドキュメントボックス機能を利用中に利用者ジョブで扱う文書情報に対して、利用者ジョブのオーナーだけに読出しと削除の操作を許可する。

利用者ジョブのオーナーを変更するためのインタフェースは提供せず、利用者ジョブのキャンセルをするためのインタフェースを提供する。利用者ジョブをキャンセルすると、当該ジョブが扱っている文書は削除する。

**表 32：一般利用者の蓄積文書アクセス制御ルール**

| 利用する I/F | 利用者の利用機能 | 一覧表示する蓄積文書の蓄積文書種別 | メニュー表示する操作 |
|---|---|---|---|
| 操作パネル | ドキュメントボックス機能 | ドキュメントボックス文書 | 印刷<br>複製<br>編集<br>削除 |
| 操作パネル | プリンター機能 | プリンター文書 | 印刷<br>削除 |
| 操作パネル | スキャナー機能 | スキャナー文書 | 文書添付メール送信<br>フォルダー送信<br>削除 |

| 利用する I/F | 利用者の利用機能 | 一覧表示する蓄積文書の蓄積文書種別 | メニュー表示する操作 |
|---|---|---|---|
| Web ブラウザ | ドキュメントボックス機能 | ドキュメントボックス文書 | 印刷<br>削除 |
| Web ブラウザ | ドキュメントボックス機能 | スキャナー文書 | 文書添付メール送信<br>フォルダー送信<br>ダウンロード<br>削除<br>(文書添付メール送信、フォルダー送信は、スキャナー機能の利用権限を持っている一般利用者に操作を許可する) |
| Web ブラウザ | プリンター機能 | プリンター文書 | 印刷<br>削除 |

*利用機能の権限確認については、「7.4 利用者権限機能」に示す。

(2) 利用者ジョブのアクセス制御ルール

TOE は、操作パネルからログインしている利用者が、利用者ジョブのキャンセルを試みた利用者ジョブのオーナーあるいは MFP 管理者の場合だけ、操作パネルに利用者ジョブをキャンセルするメニューを表示する。他の利用者には利用者ジョブへの操作を許可しない。

利用者ジョブをキャンセルすると、キャンセルされた利用者ジョブが扱っていた文書情報は削除される。ただし、キャンセルされた利用者ジョブが扱っていた文書情報が蓄積文書の場合は、TOE 内に蓄積したまま削除されない。

## 7.4 利用者制限機能

利用者制限機能は、識別認証された許可利用者の役割、及び利用者毎に設定された権限に従って、コピー機能、プリンター機能、スキャナー機能、及びドキュメントボックス機能の操作を許可する機能である。

**FDP_ACC.1(b)、FDP_ACF.1(b)**

TOE は、コピー機能、プリンター機能、スキャナー機能、及びドキュメントボックス機能の操作を開始しようとする許可利用者の役割を検証する。

役割が一般利用者の場合は、一般利用者毎に設定される利用機能リストで操作が許可されている機能の操作だけを許可する。

役割がスーパーバイザーならば、いずれの機能の操作も許可しない。

## 7.5 ネットワーク保護機能

ネットワーク保護機能は、LAN 利用時にネットワーク上のモニタリングによる情報漏えいを防止する機能と改ざんを検出する機能である。

**FTP_ITC.1**

TOE が提供する暗号化通信は、通信先により異なる。TOE が提供する暗号化通信を、表 33 に示す。

**表 33 : TOE が提供する暗号化通信**

| 通信先 | TOE が提供する暗号化通信 | |
|---|---|---|
| | プロトコル | 暗号アルゴリズム |
| クライアント PC | TLS1.0<br>TLS1.1、TLS1.2 | AES(128bits、256bits) |
| FTP サーバー | IPsec | AES(128bits、192bits、256bits)、3DES(168bits) |
| SMB サーバー | IPsec | AES(128bits、192bits、256bits)、3DES(168bits) |
| SMTP サーバー | S/MIME | AES(128bits、256bits) |

## 7.6 残存情報消去機能

残存情報消去機能は、HDD 上の削除された文書、一時的な文書あるいはその断片に対して、指定パターンデータを上書きすることにより残存情報の再利用を不可能にする機能である。

**FDP_RIP.1**

上書きする HDD 領域の消去方法には、逐次消去と一括消去がある。逐次消去は、HDD 上にある残存情報領域の有無の情報を TOE が常に監視し、残存情報の存在を発見したときに残存情報領域を上書きする方法である。TOE は、利用者の操作によって文書情報を削除した時、HDD 上にある文書情報のデジタル画像情報が書き込まれている領域に対して、MFP 管理者が指定した上書き方式で上書きする。また、利用者ジョブ終了時に TOE は、利用者ジョブの実行中に HDD 上に生成される一時的な文書、あるいはその断片が書き込まれている領域に対して、MFP 管理者が指定した上書き方式で上書きする。

一括消去は、TOE が HDD を一括で上書きする方法である。TOE は、MFP 管理者が指定した上書き方式で HDD を上書きする。

上書きの方式には、NSA 方式、DoD 方式、乱数書き込み方式がある。NSA 方式は、乱数で 2 回上書きし、Null(0)で 1 回上書きする。DoD 方式は、ある値で 1 回上書きし、そのある値の補数で 1 回上書きし、さらに乱数で上書きした後、検証する。乱数書き込み方式は、MFP 管理者が設置時に 3 から 9 回のうち指定した回数を乱数で上書きする。本 ST では残存情報消去機能と蓄積データ保護機能を組合せて使用するため、HDD を上書きする値は全て暗号化される。

## 7.7 蓄積データ保護機能

蓄積データ保護機能は、HDD に記録されているデータを漏えいから保護するため、これらのデータを暗号化する機能である。

**FCS_CKM.1、FCS_COP.1**

TOE は、HDD に書き込む前にデータを暗号化し、HDD から読み出し後にデータを復号する。この処理は、HDD に書き込み/読み出しする全てのデータに対して行われる。具体的な暗号操作を表 34 に示す。

**表 34：蓄積データ保護のための暗号操作のリスト**

| 暗号操作のトリガ | 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|---|
| HDD へのデータ書き込み | 暗号化 | FIPS197 | AES | 256 ビット |
| HDD からのデータ読み出し | 復号 | | | |

TOE は、MFP 管理者の操作を受けて、HDD 暗号鍵の生成を行う。TOE は、ログインしている利用者が MFP 管理者の場合、HDD 暗号鍵を生成するための画面を操作パネルから提供する。
MFP 管理者が操作パネルから HDD 暗号鍵の生成を指示すると、TOE は、真性乱数生成器によって標準 BSI-AIS31 に準拠した乱数を生成する。

## 7.8 セキュリティ管理機能

セキュリティ管理機能は、一般利用者、MFP 管理者、及びスーパーバイザーの利用者役割に与えられた権限、または利用者毎に与えられた権限に基づいて、TSF 情報への操作に関する制御を行う機能、セキュリティ管理機能の操作をする一般利用者、MFP 管理者、及びスーパーバイザーの利用者役割を維持する機能、セキュリティ属性に適切なデフォルト値を設定する機能からなる。

**FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MSA.3(a)、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1**

TOE は、TSF 情報に対して表 35 に記す規則に従って操作を許可する。

**表 35：TSF 情報の管理**

| TSF 情報 | 操作箇所 | 操作 | 利用者 |
|---|---|---|---|
| 一般利用者のログインユーザー名 | 操作パネル<br>Web ブラウザ | 新規作成、<br>問い合わせ、<br>改変、<br>削除 | MFP 管理者 |
| | | 問い合わせ | 当該一般利用者 |
| スーパーバイザーのログインユーザー名 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | スーパーバイザー |
| MFP 管理者のログインユーザー名 | 操作パネル<br>Web ブラウザ | 新規作成 | MFP 管理者 |
| | | 問い合わせ、<br>改変 | 当該 MFP 管理者 |
| | | 問い合わせ | スーパーバイザー |
| 文書情報属性 | 操作可能箇所は無し | 許可される操作は無し | なし |
| 文書利用者リスト<br>蓄積文書種別が、ドキュメントボックス文書、スキャナー文書、プリンター文書(保存印刷)の場合 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者、<br>文書を蓄積した当該一般利用者 |

| TSF 情報 | 操作箇所 | 操作 | 利用者 |
|---|---|---|---|
| 文書利用者リストのデフォルト値 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| 利用機能リスト | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| | Web ブラウザ | 問い合わせ | 当該一般利用者 |
| 機能種別 | 操作可能箇所は無し | 許可される操作は無し | なし |
| 利用者役割 | 操作可能箇所は無し | 許可される操作は無し | なし |
| 一般利用者のログインパスワード | 操作パネル<br>Web ブラウザ | 新規作成、<br>改変 | MFP 管理者 |
| | | 改変 | 当該一般利用者 |
| スーパーバイザーのログインパスワード | 操作パネル<br>Web ブラウザ | 改変 | スーパーバイザー |
| MFP 管理者のログインパスワード | 操作パネル<br>Web ブラウザ | 改変 | スーパーバイザー |
| | | 新規作成 | MFP 管理者 |
| | | 改変 | 当該 MFP 管理者 |
| ログインパスワード入力許容回数 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| ロックアウト解除タイマー設定 | Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| ロックアウト時間 | Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| 年月日 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| | | 問い合わせ | スーパーバイザー、<br>一般利用者 |
| 時刻 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| | | 問い合わせ | スーパーバイザー、<br>一般利用者 |
| パスワード最小桁数 | 操作パネル | 問い合わせ、<br>改変 | MFP 管理者 |
| パスワード複雑度 | 操作パネル | 問い合わせ、<br>改変 | MFP 管理者 |
| 操作パネルオートログアウト時間 | 操作パネル | 問い合わせ、<br>改変 | MFP 管理者 |
| WIM オートログアウト時間 | Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| 監査ログ | Web ブラウザ | 問い合わせ、<br>削除 | MFP 管理者 |

| TSF 情報 | 操作箇所 | 操作 | 利用者 |
|---|---|---|---|
| HDD 暗号鍵 | 操作パネル | 新規作成 | MFP 管理者 |
| S/MIME 利用者情報 | 操作パネル<br>Web ブラウザ | 新規作成、<br>改変、<br>問い合わせ、<br>削除 | MFP 管理者 |
| | | 問い合わせ | 一般利用者 |
| 送信先フォルダー | 操作パネル<br>Web ブラウザ | 新規作成、<br>改変、<br>問い合わせ、<br>削除 | MFP 管理者 |
| | | 問い合わせ | 一般利用者 |
| ユーザー認証方法 | 操作パネル<br>Web ブラウザ | 問い合わせ | MFP 管理者 |
| IPsec 設定情報 | 操作パネル<br>Web ブラウザ | 問い合わせ、<br>改変 | MFP 管理者 |
| 機器証明書 | 操作パネル<br>Web ブラウザ | 改変 | MFP 管理者 |

**FMT_MSA.3(a)、FMT_MSA.3(b)**

TOE は、表 36 に記す規則に従って、オブジェクト/サブジェクトの生成時にデフォルト値を設定する。

**表 36：文書アクセス制御 SFP のセキュリティ属性静的初期化のリスト**

| オブジェクト | セキュリティ属性 | デフォルト値 |
|---|---|---|
| 文書情報 | 文書情報属性 | +PRT:クライアント PC から直接印刷、機密印刷、保留印刷、及び試し印刷された文書<br>+SCN:MFP からフォルダー送信、文書添付メール送信する文書。<br>+CPY:MFP で複写する文書。<br>+DSR:コピー機能、スキャナー機能、ドキュメントボックス機能を使って、TOE 内に蓄積している文書。クライアント PC からドキュメントボックス印刷、あるいは保存印刷で印刷された文書。 |
| 文書情報(蓄積文書種別が、ドキュメントボックス文書、スキャナー文書の場合) | 文書利用者リスト | 文書情報を作成した一般利用者に割り当てられる文書利用者リストのデフォルトの値。 |
| 文書情報<br>(蓄積文書種別が、プリンター文書の場合) | 文書利用者リスト | 文書情報を蓄積した一般利用者のログインユーザー名。 |
| 利用者ジョブ | 一般利用者のログインユーザー名 | 利用者ジョブを新規作成した一般利用者のログインユーザー名。 |

| オブジェクト | セキュリティ属性 | デフォルト値 |
|---|---|---|
| 各 MFP アプリケーション(コピー機能、プリンター機能、スキャナー機能、ドキュメントボックス機能) | 機能種別 | コピー機能の機能種別にはコピー機能を識別する値、ドキュメントボックス機能の機能種別にはドキュメントボックス機能を識別する値、プリンター機能の機能種別にはプリンター機能を識別する値、スキャナー機能にはスキャナー機能を識別する値がそれぞれ設定される。 |

## 7.9 ソフトウェア検証機能

ソフトウェア検証機能は、MFP 制御ソフトウェアの実行コードの完全性を検証し、それらが正規のものである事を確認する機能である。

**FPT_TST.1**

TOE は、初期立上げ中にソフトウェア検証を実行する。
MFP 制御ソフトウェアの完全性の検証は、MFP 制御ソフトウェアのハッシュ値の比較または証明書の検証により、TOE が行う。取得したハッシュ値が正しい値と一致しない、または証明書が検証されない場合、TOE は、エラーを表示して停止する。取得したハッシュ値が正しい値と一致し、かつ証明書が検証された場合、TOE は、利用可能になる。さらに、TOE は、監査ログデータファイルの完全性を検証している。