imagio MP 5000SP/4000SP セキュリティカード タイプ 9 付き

セキュリティターゲット

作成者　　:株式会社リコー　柿井弘、清水剛、佐久間剛、瀧田史
作成日付　　:2010 年 2 月 18 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	2010-02-18	柿井弘、清水剛、佐久間剛、瀧田史	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、および 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。

ST タイトル　：imagio MP 5000SP/4000SP セキュリティカード タイプ 9 付きセキュリティターゲット

ST バージョン　：1.00

作成日付　：2010 年 2 月 18 日

発行者　：株式会社リコー　柿井弘、清水剛、佐久間剛、瀧田史

1.2 TOE 参照

TOE の識別情報を以下に示す。

製造者　：株式会社リコー

TOE 名称　：Ricoh imagio MP 5000SP/4000SP セキュリティカード タイプ 9 付き

TOE バージョン：TOE は構成ファームウェア、ASIC およびオプションの 3 種のバージョンにより特定される。構成ファームウェアはシステムバージョンで特定する。システムバージョンは、本体に搭載されている複数のファームウェアバージョンの組み合わせに対して与えられるバージョンである。ASIC およびオプションは、搭載されているそれぞれのバージョン一覧で特定する。本 TOE のバージョンは以下の通りである。

・構成ファームウェア

システムバージョン　:V2.16-00

構成ファームウェア名とバージョン	
System/Copy	1.11.1
Network Support	7.26
Network DocBox	1.10C
Web Support	1.59
Web Uapl	1.15
animation	1.3
Scanner	01.24
RPDL	7.33
Printer	1.11
MSIS	7.15.02

RPCS Font	1.01
Engine	1.04:05
OpePanel	1.01
LANG0	1.01
LANG1	1.01
ADF	15.000:15

・ASIC

Ic Key バージョン　:1100

・オプション

Data Erase Opt バージョン　:1.01m

キーワード　:　デジタル複合機、文書、コピー、印刷、スキャナー、ネットワーク、オフィス

1.3 TOE 概要

本章では、本 TOE の種別および主要セキュリティ機能、TOE の利用環境を述べる。

1.3.1 TOE 識別および主要セキュリティ機能

本 TOE は、IT製品であるデジタル複合機（以降、MFP）である。本 ST における TOE の主要なセキュリティ機能は以下のとおりである。

- 監査機能
- 識別認証機能
- アクセス制御機能
- ネットワーク保護機能
- 残存情報消去機能
- セキュリティ管理機能
- ソフトウェア検証機能

1.3.2 TOE の利用環境

TOE の利用環境を図示し解説する。

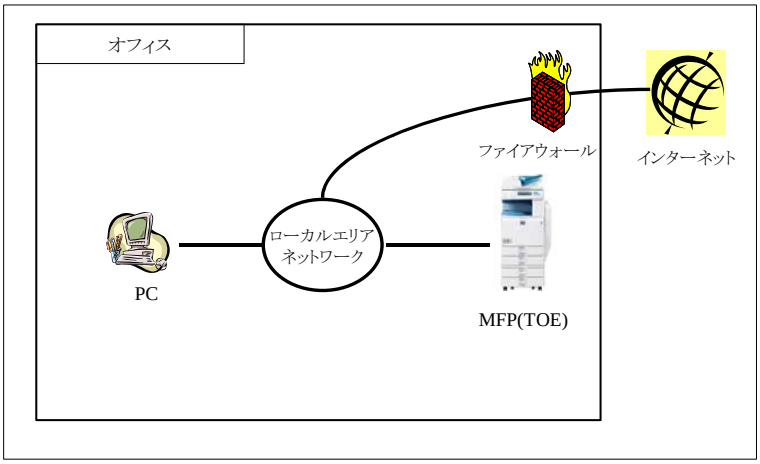

図 1：TOE の利用環境

TOE はオフィス内で利用されることを想定している。以下その環境について記述する。

[ローカルエリアネットワーク]

オフィス内で利用されているローカルエリアネットワーク（以降、LAN）をさす。

[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
- コピー操作による紙文書のコピー
- プリンター操作により受信した利用者文書の印刷
- スキャナー操作による本体内への利用者文書蓄積
- ドキュメントボックス操作による利用者文書操作

[PC]

クライント PC として動作し、LAN を経由し MFP と通信し、以下の処理が可能である。

- Webブラウザ経由での MFP 本体の各種設定
- Web ブラウザ経由での利用者文書操作
- プリンタードライバー経由の利用者文書蓄積

[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。

1.4 TOE 記述

本章では、TOE の物理的範囲、関係者定義、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、LAN インタフェース、USB インタフェース、SD スロット、パネルインタフェースのハードウェアから構成される MFP である。

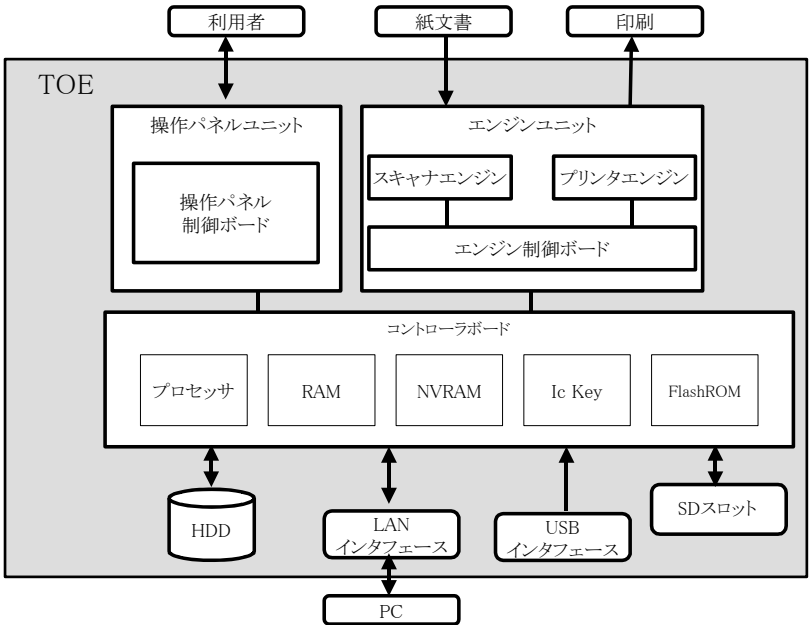

図 2：TOE のハードウェア構成

■ 操作パネルユニット（以降、操作パネルという）

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 MFP 制御ソフトウェアに転送する。
2. MFP 制御ソフトウェア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。

操作パネル制御ソフトウェアは、TOE を識別する要素のうち、OpePanel、LANG0、LANG1 が相当する。LANG0、LANG1 は、操作パネルに表示する文字データである。

■ 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エンジンの状態を MFP 制御ソフトウェアに送信、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エンジンを動作させる。エンジン制御ソフトウェアは、TOE を識別する要素のうち、Engine、ADF が相当する。

- コントローラボード
  プロセッサ、RAM、NVRAM、IcKey、FlashROM が載ったデバイス。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
    MFP 制御ソフトウェア本体がインストールされている不揮発性メモリ。MFP 制御ソフトウェアとは、TOE に組込むソフトウェアの１つで、TOE を識別する要素のうち、System/Copy、Network Support、Scanner、Printer、Web Support、Web Uapl、Network Doc Box、animation、RPDL、MSIS、RPCS Font が相当する。MFP を構成するユニットやデバイスのリソースを管理し動作を制御する。
- HDD
  不揮発性メモリであるハードディスクドライブ。利用者文書、削除された利用者文書、一時的な文書あるいはその断片や一般利用者のログインユーザー名、一般利用者ログインパスワードが保管されている。
- LAN インタフェース
  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 インタフェース
  PC から直結して印刷を行う場合に、TOE と 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 スロット
  SD カードを挿入するためのスロット。SD カードには残存情報消去機能ソフトウェア（Data Erase Opt）が保持されている。SD スロットは機器内部にあり、カスタマー・エンジニアのみが設置時にカバーを開けて利用する。

1.4.2 ガイダンス

本 TOE を構成するガイダンス文書は以下のとおりである。

- imagio MP 5000/4000 シリーズ使用説明書<セキュリティ編>
- imagio MP 5000/4000 シリーズ使用説明書<本機のご利用にあたって>

- imagio MP 5000/4000 シリーズ使用説明書<こんなときには>
- imagio MP 5000/4000 シリーズ使用説明書<コピー機能/ドキュメントボックス機能編>
- imagio MP 5000/4000 シリーズ使用説明書<プリンター機能編>
- imagio MP 5000/4000 シリーズ使用説明書<スキャナー機能編>
- imagio MP 5000/4000 シリーズ使用説明書<ネットワークガイド>
- imagio MP 5000/4000 シリーズ使用説明書<初期設定編>
- imagio MP 5000/4000 シリーズ同梱されている使用説明書
- imagio MP 5000/4000 シリーズクイックガイド
- セキュリティー機能をお使いの方へ
- IEEE Std. 2600.1-2009 準拠でお使いになる管理者の方へ
- imagio セキュリティカードタイプ7 imagio セキュリティカードタイプ 9 使用説明書

1.4.3 利用者役割

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し、TOE を利用するためのなんらかの権限を与えられているものをさす。利用者は、一般利用者と管理者から構成され、そ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通常のMFP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、文書管理権限を持つことができる。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持つ 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 管理者ログインパスワードの削除と新規登録する権限を持つ。
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	利用者文書を管理する権限。利用者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いう。

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、保守をする者をいう。

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。

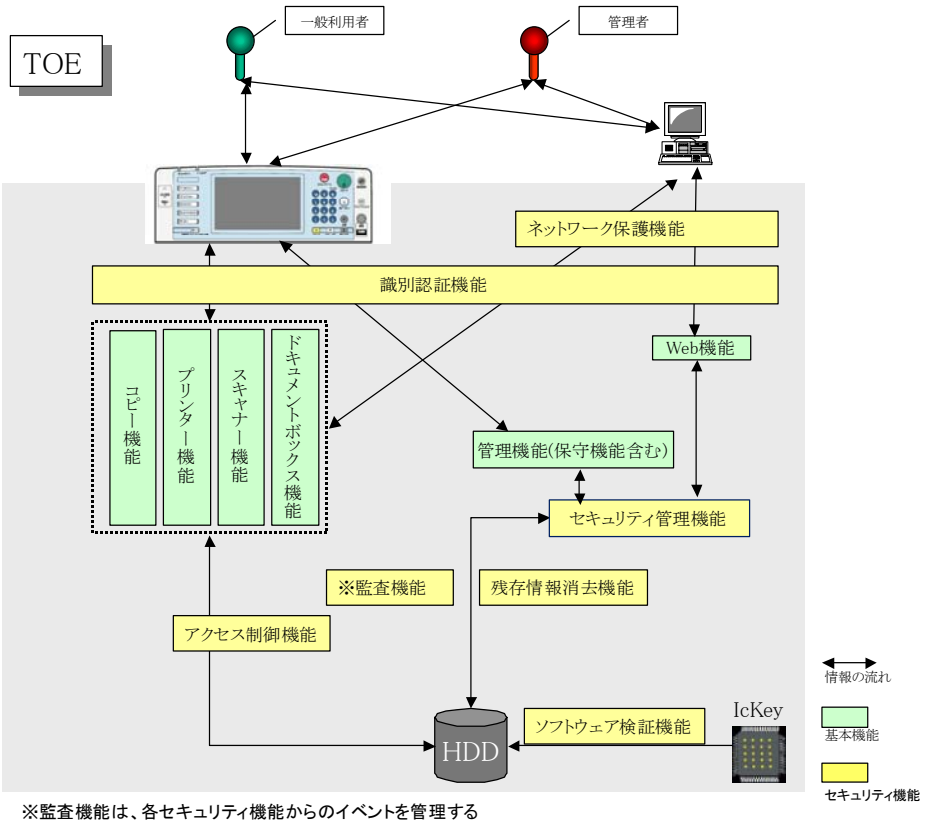

図 3：TOE の論理的範囲

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、紙文書をスキャンし、読取った画像を、指定する部数、倍率、編集指定に従って印刷する機能である。コピー機能を利用する際、一般利用者は操作パネルよりログインしコピー処理を実施する。

■プリンター機能

プリンター機能は

- ネットワーク経由でPCからの印刷情報を利用者文書として蓄積する機能
- 蓄積された利用者文書の印刷操作を実施する機能
- ネットワーク経由で PC からの印刷情報を直接印刷する機能

の3つからなる。一般利用者はガイダンスに従って最初に指定のプリンタードライバーを自身の PC にインストールして利用する。

実際にプリンター機能を利用するときは、一般利用者として PC にて印刷しようとする文書を選択し蓄積指示し、その後、操作パネルあるいはWebブラウザから印刷処理を実施するか、PC にて印刷しようとする文書を選択し直接印刷を指示して印刷処理を実施する。

■スキャナー機能

スキャナー機能は、紙文書をスキャンし、

- 利用者文書として本体内に蓄積する機能
- 蓄積された利用者文書に対して、PC からのダウンロード操作をする機能

の2つからなる。

実際にスキャナー機能を利用するときは、一般利用者として操作パネルからスキャン操作を実施し、その後、PCにてWebブラウザ経由で蓄積された利用者文書のダウンロード処理を実施する。

■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、MFP 本体内の HDD に蓄積された利用者文書の操作をさす。上記のプリンター機能の蓄積された利用者文書の印刷操作を実施する機能、スキャナー機能の蓄積された利用者文書に対して、PC からのダウンロード操作をする機能は、このドキュメントボックス機能を利用している。

■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。操作パネルあるいはWebブラウザ経由で実施する。

■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行う。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している状態での稼動を評価範囲とする。

■Web 機能

Web 機能は、TOE の利用者が PC から TOE をリモート操作するための機能である。リモート操作するためには、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。

1.4.4.2. セキュリティ機能

以下セキュリティ機能を記述する。

■監査機能

監査機能は、TOE の運用状況を確認したり、セキュリティ侵害を検知したりするために事象発生時に監査ログを記録する機能と、記録した監査ログを、MFP 管理者だけに読出し、削除の操作を許可する機能である。監査ログの読出し、削除操作は Web 機能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に対して識別認証機能、認証を連続失敗した利用者に対してのロックアウト機能、パネル操作時のログインパスワード入力時認証フィードバック領域の保護機能である。プリンター機能利用時は、プリンタードライバーにログインユーザー名とログインパスワードを入力して識別認証を行う。

■アクセス制御機能

アクセス制御機能は、識別認証機能で認証された TOE 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操作権限に基づいた制御をする機能である。

■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保護する機能である。Web ブラウザからは暗号化通信有効な 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。

■残存情報消去機能

HDD 上の削除された利用者文書、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を完全に消去する機能である。

■セキュリティ管理機能

セキュリティ管理機能は、管理者が行うセキュリティ管理に関連した管理機能全般をさす。

■ソフトウェア検証機能

ソフトウェア検証機能は、FlashROM にインストールされている MFP 制御ソフトウェアの実行コードの完全性をチェックすることで、MFP 制御ソフトウェアが正規のものであることを確認する機能である。

1.4.5 保護資産

ここでは、保護資産を定義する。TOE が守るべき保護資産を、クラス、タイプとその内容として以下の表 3 に、またそれらの資産がどこに存在するかを 表 4 にまとめた。以降本文にて、単に保護資産と表現する場合は、これらすべての情報を対象とする。

表 3：資産定義

クラス	タイプ	内容
利用者情報	文書情報	デジタル化された TOE の管理下にある利用者文書、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。
TSF 情報	保護情報	ログインユーザー名、利用者ジョブのステータス、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、年月日設定、時刻設定、保守機能移行禁止設定。本 ST 内では「TSF 保護情報」と表現する。
	秘密情報	ログインパスワード、監査ログ。本 ST 内では「TSF 秘密情報」と表現する。

表 4：不揮発性メモリと保管情報

不揮発性メモリ	保管情報
HDD	利用者文書、 削除された利用者文書、一時的な文書あるいはその断片、 一般利用者ログインパスワード、 監査ログ
NVRAM	管理者のログインユーザー名、 管理者用ログインパスワード、 一般利用者のログインユーザー名、 機器設定値、機器カウンタ情報、機器調整値等
Flash ROM	MFP 制御ソフトウェア
SD メモリ	残存情報消去機能ソフトウェア
IcKey	署名ルート鍵

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
ログインユーザー名	利用者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	操作パネルあるいはWebブラウザで、ログイン後一定時間アクセスがなかった場合に自動的にログアウトする機能。
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。 文字種は、英大文字、英小文字、数字、記号の 4 種がある。 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	利用者が TOE に対して操作を要求する作業。開始と終了をもつひと続きの作業を1ジョブとする。対象となる操作は、利用者文書の蓄積操作、印刷操作、ダウンロード操作、削除操作である。
文書	コピー機能、プリンター機能、スキャナー機能を利用して生成される TOE 管理下のデジタル画像情報。本体内に蓄積されている文書を本 ST では明示的に利用者文書と呼ぶ。単に文書と記述する場合はコピー時や印刷時の削除された文書、一時的な文書あるいはその断片も含む。
文書利用者リスト	利用者文書に対してアクセス権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。各利用者文書の属性として付与される。なお、アクセス権が許可されていても MFP 管理者のログインユーザー名は、このリストには含まれない。
利用機能リスト	一般利用者に対してアクセス権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 MFP を操作する時に利用する。

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 および 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 2006 年 9 月 バージョン 3.1 改訂第1版（翻訳第 1.2 版） CCMB-2006-09-001

  パート2:

  セキュリティ機能コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版（翻訳第 2.0 版） CCMB-2007-09-002

  パート3:

  セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版（翻訳第 2.0 版） CCMB-2007-09-003
- 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 および TOE が論証適合している PP は、

PP 名称/識別 : 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A

バージョン : 1.0, dated June 2009

である。

注釈: Common Criteria Portal に掲載されている PP 名称は「U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments (IEEE Std. 2600.1-2009)」である。

2.3 パッケージ主張

本 ST および TOE が適合しているパッケージは、評価保証レベル EAL3+ALC_FLR.2 である。

PP からの選択 SFR Package は

2600.1-PRT 適合

2600.1-SCN 適合

2600.1-CPY 適合

2600.1-DSR 適合

2600.1-SMI 適合

である。

2.4 適合主張根拠

本 TOE は PP に従って SFR として、Common Security Functional Requirements と SFR Package として 2600.1-PRT、2600.1-SCN、2600.1-CPY、2600.1-DSR、2600.1-SMI を選択する。

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。

認証は本 TOE により実現するために PP APPLICATION NOTE36 に従い FIA_AFL.1, FIA_UAU.7, FIA_SOS.1 を追加する。

2600.1-PRT、2600.1-SCN、2600.1-CPY、2600.1-DSR、2600.1-SMI は PP 適合である。

本 TOE にはファクス機能が搭載されていないことから 2600.1-FAX は選択しない。

本 TOE には着脱可能な不揮発性記憶媒体が存在しないことにより 2600.1-NVS は選択しない。

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。

PP を適合するにあたり、英語を日本語に訳す際、読者に分かり易くするために一部意訳したが、PP の適合要件を逸脱するものではない。

3 章、4 章では、PP を直訳すると読者に分かりにくい箇所を具体化したが、脅威、組織のセキュリティ方針、前提条件、TOE のセキュリティ対策方針および運用環境のセキュリティ方針において、これらの項目を増やしたり、減らしたりしていない。

6 章では、PP で要求している機能要件に対して 1 対 1 に対応していない部分もあるが、PP に記述されているすべての機能要件の要求事項を満足するように、TOE の実装に合わせて具体化している。

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、および前提条件について記述する。

3.1 脅威

本 TOE の利用およ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 が管理している利用者文書、削除された文書、一時的な文書あるいはその断片が、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持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閲覧されるかもしれない。

T.DOC.ALT　利用者文書の改変

TOE が管理している利用者文書が、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持っているがその利用者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持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持っているがその 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持っているがその 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持っているがその 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 利用のログインユーザー名をもった者だけが 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

TOE 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。さらに権限を持つものが、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（操作パネル、LAN、USB）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。

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、権限を持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、および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 は利用者文書、削除された利用者文書、一時的な文書あるいはその断片が、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持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の保護を保証する。

O.DOC.NO_ALT 利用者文書の改変保護

TOE は利用者文書が、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持っているがその利用者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の保護を保証する。

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持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持っているがその 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持っているがその 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持っているがその 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（操作パネル、LAN）の運用を管理することを保証する。TOE により操作パネル、オープンされている LAN ポートへのアクセス制御を行う。また、TOE は TOE で処理されたデータのみを外部インタフェースから送信する。

O.SOFTWARE.VERIFIED ソフトウェア検証

TOE は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。

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（LAN）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。そのために、MFP 管理責任者はガイダンスに従って、ファイアウォールの設定を適切に行うよう指示し、LAN インタフェースへのインターネットからの攻撃を防ぐ。さらに MFP 管理責任者はガイダンスに従って、MFP 管理者に利用しない LAN ポートのクローズ処理と設置時の USB の利用禁止設定を指示する。

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、権限を持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、その組織のセキュリティポリシーや手順に従う者に対して、ログインユーザー名、ログインパスワード、および利用者役割(スーパーバイザー、MFP 管理者、一般利用者)を与え、利用者として TOE を利用する権限を持つ許可を与えることを保証する。

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.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	✓						✓	✓											
T.DOC.ALT		✓					✓	✓											
T.FUNC.ALT			✓				✓	✓											
T.PROT.ALT				✓			✓	✓											
T.CONF.DIS					✓		✓	✓											
T.CONF.ALT						✓	✓	✓											
P.USER.AUTHORIZATION							✓	✓											
P.SOFTWARE.VERIFICATION									✓										
P.AUDIT.LOGGING										✓	✓	✓	✓						
P.INTERFACE.MANAGEMENT														✓		✓			
A.ACCESS.MANAGED															✓				
A.ADMIN.TRAINING																	✓		
A.ADMIN.TRUST																		✓	
A.USER.TRAINING																			✓

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、およ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、その組織のセキュリティポリシーや手順に従う者に対して、利用者として TOE を利用する権限を持つ許可を与え、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 により利用者文書、削除された文書、一時的な文書あるいはその断片が、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持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はない。

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、その組織のセキュリティポリシーや手順に従う者に対して、利用者として TOE を利用する権限を持つ許可を与え、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 は利用者文書が、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持っているがその利用者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はない。

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、その組織のセキュリティポリシーや手順に従う者に対して、利用者として TOE を利用する権限を持つ許可を与え、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持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、その組織のセキュリティポリシーや手順に従う者に対して、利用者として TOE を利用する権限を持つ許可を与え、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持っているがその 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、その組織のセキュリティポリシーや手順に従う者に対して、利用者としてTOE を利用する権限を持つ許可を与え、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持っているがその 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、その組織のセキュリティポリシーや手順に従う者に対して、利用者としてTOE を利用する権限を持つ許可を与え、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持っているがその 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、その組織のセキュリティポリシーや手順に従う者に対して、利用者としてTOE を利用する権限を持つ許可を与え、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.VERIFICATIN

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

O.SOFTWARE.VERIFIED により TOE は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（操作パネル、LAN）の運用を管理する。TOE により操作パネル、オープンされている LAN ポートへのアクセス制御を行い、OE.INTERFACE.MANAGED により、LAN と USB のアクセスを適切に制御する。具体的には、

① MFP 管理責任者はファイアウォールの設定を適切に行うよう指示し、LAN インタフェースへのインターネットからの攻撃を防ぐ。
② さらに MFP 管理責任者は MFP 管理者に指示し、利用しない LAN ポートをクローズする。
③ さらに設置時に USB の利用禁止設定をする。

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

A.ACCESS.MANAGED

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

OE.PHYISCAL.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、権限を持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: 外部インタフェースへの制限された情報転送	1

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 および 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、およ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(U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments (IEEE Std. 2600.1-2009)) 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: a) 監査機能の起動と終了; b) 監査の**[選択: 指定なし]**レベルのすべての監査対象事象;および 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: 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);および 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: 利用者ジョブの種別、通信先 IP アドレス、通信方向]**

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。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	独自: ・利用者文書の蓄積操作の開始と終了 ・利用者文書の印刷操作の開始と終了 ・利用者文書のダウンロード操作の開始と終了 ・利用者文書の削除操作の開

		始と終了
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。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	独自 : 記録しない
FIA_UAU.1	a) 最小: 認証メカニズムの不成功になった使用。 b)基本: 認証メカニズムのすべての使用。 c)詳細: 利用者認証以前に行われたすべての TSF 仲介アクション。	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。 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
FMT_SMF.1	a) 最小:管理機能の使用。	a) 最小:表 22 管理項目の記録
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。 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: 時間の改変。 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。 b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。 c) 基本: 高信頼チャネル機能のすべての使用の試み。 d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。	a) 最小:SSL 暗号化通信の失敗 b) 最小:通信方向(IN/OUT)と対象機 IP アドレス

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]**および**[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 FDP: 利用者情報保護

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 8 のサブジェクトとオブジェクトおよびサブジェクトとオブジェクト間の操作リスト]**に対して**[割付: 共通アクセス制御 SFP]**を実施しなければならない。

表 8：サブジェクトとオブジェクトおよびサブジェクトとオブジェクト間の操作リスト(a)

サブジェクト	オブジェクト	サブジェクトとオブジェクト間の操作
MFP 管理者プロセス	利用者文書	削除

スーパーバイザープロセス	利用者文書	なし
一般利用者プロセス	利用者文書	削除、印刷、ダウンロード
MFP 管理者プロセス	利用者ジョブ	削除
一般利用者プロセス	当該利用者ジョブ	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 9 のサブジェクトとオブジェクトおよびサブジェクトとオブジェクト間の操作リスト]**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 9：サブジェクトとオブジェクトおよびサブジェクトとオブジェクト間の操作リスト(b)

サブジェクト	オブジェクト	サブジェクトとオブジェクト間の操作
一般利用者プロセス	コピー機能	実行
一般利用者プロセス	プリンター機能	実行
一般利用者プロセス	スキャナー機能	実行
一般利用者プロセス	ドキュメントボックス機能	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 10 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: 共通アクセス制御 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
サブジェクト	スーパーバイザープロセス	スーパーバイザーのログインユーザー名
サブジェクト	MFP 管理者プロセス	MFP 管理者のログインユーザー名
オブジェクト	利用者文書	文書利用者リスト
オブジェクト	利用者ジョブ	利用者ジョブを新規作成した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 11 に示すサブジェクトのオブジェクトに対する操作と、操作に対するアクセスを管理する規則]**。

表 11： アクセスを管理する規則(a)

サブジェクト	オブジェクトに対する操作	アクセスを管理する規則
一般利用者プロセス	プリンター利用者文書の削除、印刷	ログインユーザー名とプリンター利用者文書に関連付けられた文書利用者リストの一般利用者のログインユーザー名が一致した場合、その一般利用者プロセスに対してプリンター利用者文書の削除および印刷が許可される。
	スキャナー利用者文書の削除、ダウンロード	ログインユーザー名とスキャナー利用者文書に関連付けられた文書利用者リストの一般利用者のログインユーザー名が一致した場合、その一般利用者プロセスに対してスキャナー利用者文書の削除およびダウンロードが許可される。
一般利用者プロセス	利用者ジョブの削除	ログインユーザー名と利用者ジョブに関連付けられたジョブ作成者のログインユーザー名が一致した場合、その一般利用者プロセスに対して利用者ジョブの削除が許可される。

FDP_ACF.1.3(a) TSF は、次の追加規則、**[割付: 表 12 に示すサブジェクトのオブジェクトに対する操作を明示的に許可する規則]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

表 12： アクセスを明示的に管理する規則(a)

サブジェクト	オブジェクトに対する操作	アクセスを管理する規則
MFP 管理者プロセス	利用者文書の削除	MFP 管理者プロセスに対して、蓄積されている全ての利用者文書の削除を許可する。
MFP 管理者プロセス	利用者ジョブの削除	MFP 管理者プロセスに対して、全ての利用者ジョブの削除を許可する。

FDP_ACF.1.4(a) TSF は、**[割付: スーパーバイザーログイン名でログインした場合、利用者文書と利用者ジョブへの操作を拒否する規則]**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。

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 13 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 13：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、利用機能リスト
オブジェクト	コピー機能	なし
オブジェクト	プリンター機能	なし
オブジェクト	スキャナー機能	なし
オブジェクト	ドキュメントボックス機能	なし

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 14 に示すサブジェクトのオブジェクトに対する操作と、操作に対するアクセスを管理する規則]**。

表 14：アクセスを管理する規則(b)

サブジェクト	オブジェクトに対する操作	アクセスを管理する規則
一般利用者プロセス	コピー機能の実行	ログインユーザー名に関連付けられた利用機能リストにコピー機能が存在する場合、その一般利用者プロセスに対してコピー機能の実行が許可される。
一般利用者プロセス	プリンター機能の実行	ログインユーザー名に関連付けられた利用機能リストにプリンター機能が存在する場合、その一般利用者プロセスに対してプリンター機能の実行が許可される。
一般利用者プロセス	スキャナー機能の実行	ログインユーザー名に関連付けられた利用機能リストにスキャナー機能が存在する場合、その一般利用者プロセスに対してスキャナー機能の実行が許可される。
一般利用者プロセス	ドキュメントボックス機能の実行	ログインユーザー名に関連付けられた利用機能リストにドキュメントボックス機能が存在する場合、その一般利用者プロセスに対してドキュメントボックス機能の実行が許可される。

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、**[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。

6.1.3 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 15 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 15：認証事象と不成功認証試行のリスト

認証事象
操作パネルを使用する利用者認証
PC の Web ブラウザから TOE を使用する利用者認証
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 16 に示すアクション]**をしなければならない。

表 16：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（60 分）、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（60 分）、もしくは MFP 管理者が解除、もしくは電源のオフ/オン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（60 分）、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:一般利用者のログインユーザー名、スーパーバイザーのログインユーザー名、MFP 管理者のログインユーザー名]**

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	**アクション前の利用者認証**
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]**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: 操作パネルに、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	**アクション前の利用者識別**
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]**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、スーパーバイザーのログインユーザー名、MFP 管理者のログインユーザー名]**
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 17 にリストした属性の最初の関連付けに関する規則]**

表 17： 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
スーパーバイザー	スーパーバイザープロセス	スーパーバイザーのログインユーザー名
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

FIA_USB.1.3 TSF は、以下の利用者セキュリティ属性への改変を管理する規則を、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: MFP 管理者は4人まで新規作成、削除することができる。ただし、MFP 管理者がいなくなる場合は削除できない。]**

6.1.4 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 18 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 18 の利用者役割]**に制限する**[割付: 共通アクセス制御 SFP]**を実施しなければならない。

表 18： 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	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、 改変、 新規作成、 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	問い合わせ、 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、 改変	当該 MFP 管理者
	問い合わせ	スーパーバイザー
文書利用者リスト	問い合わせ、 改変	MFP 管理者、 利用者文書を蓄積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 19 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 19 の利用者役割]**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 19: 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	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、改変、新規作成、削除	MFP 管理者
	問い合わせ	当該一般利用者
一般利用者の利用機能リスト	問い合わせ、改変	MFP 管理者
	問い合わせ	当該一般利用者

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: [割付:表 20 に示す制限的な]]**デフォルト値を与える**[割付: 共通アクセス制御 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: 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。

表 20: 静的属性初期化の特性(a)

オブジェクト	オブジェクトに関連付けられるセキュリティ属性	オブジェクト生成時のデフォルト値とその特性
利用者文書	文書利用者リスト	デフォルト値は利用者文書を蓄積した一般利用者であり、制限的な特性を持つ。
利用者ジョブ	一般利用者のログインユーザー名	デフォルト値は利用者ジョブを新規作成した一般利用者であり、制限的な特性を持つ。

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: 許可的]**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: MFP 管理者]**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 21 の TSF データのリスト]**を**[選択:問い合わせ、改変、削除、消去、[割付: 新規作成]]**する能力を**[割付: 表 21 の利用者役割]**に制限しなければならない。

表 21：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	MFP 管理者
ロックアウト解除タイマー設定	問い合わせ	MFP 管理者
ロックアウト時間	問い合わせ	MFP 管理者
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	MFP 管理者
パスワード複雑度	問い合わせ	MFP 管理者
監査ログ	問い合わせ、削除	MFP 管理者
保守機能移行禁止設定	問い合わせ	MFP 管理者、スーパーバイザー、一般利用者

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 22 に記す管理機能の特定のリスト]**。

表 22： 管理機能の特定のリスト

機能要件	管理要件	管理項目
FAU_SAR.1	a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	a) なし:利用者グループは固定
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	a) なし:アクションは固定
FDP_ACF.1(a)	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	a) MFP 管理者の管理
FDP_ACF.1(b)	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理。 b) 認証失敗の事象においてとられるアクションの管理。	a)なし:MFP 管理者によるログインパスワード入力許容回数は、初期立上げ時に設定した後は変更しない b)ロックアウト対象者に対するロックアウト解除者と、ロックアウト解除者の利用者役割 -ロックアウト対象者(一般ユーザー)、ロックアウト解除者(MFP 管理者) -ロックアウト対象者(MFP 管理者)、ロックアウト解除者(スーパーバイザー) -ロックアウト対象者(スーパーバイザー)、ロックアウト解除者(MFP 管理者)
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	なし: MFP 管理者によるパスワード最小桁数と、パスワード複雑度は、初期立上げ時に設定した後は変更しない
FIA_UAU.1	a) 管理者による認証データの管理。 b) 関係する利用者による認証データの管理。 c) 利用者が認証される前にとられるアクションのリストを管理すること。	-セキュリティ管理機能(一般利用者):MFP 管理者による一般利用者のログインパスワード管理と、一般利用者による本人の管理 -セキュリティ管理機能(MFP 管理者):MFP 管理者本人による MFP 管理者パスワードの管理 -セキュリティ管理機能(管理者情報管理):管理者による管理者の新規登録 -セキュリティ管理機能(管理者情報管理):スーパーバイザーによる管理者認証情報の管理 -セキュリティ管理機能(スーパーバイザー):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管理

FIA_UID.1	a) 利用者識別情報の管理。 b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	-MFP管理者による一般利用者のログインユーザー名の管理 -セキュリティ管理機能(一般利用者):MFP 管理者による一般利用者ログイン名の管理 -セキュリティ管理機能(MFP 管理者):MFP 管理者による自身の管理者ログイン名の管理 -セキュリティ管理機能(MFP 管理者):MFP 管理者による MFP 管理者の新規登録 -セキュリティ管理機能(スーパーバイザー):スーパーバイザーによるスーパーバイザーログイン名の管理
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし b) なし
FMT_MSA.1(a)	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。 b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし b)なし
FMT_MSA.1(b)	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。 b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし b) なし
FMT_MSA.3(a)	a) 初期値を特定できる役割のグループを管理すること。 b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。 c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a)なし:初期設定を特定できる役割のグループはない b)利用者文書のデフォルトアクセス権は MFP 管理者と当該一般利用者に制限 c)なし
FMT_MSA.3(b)	a) 初期値を特定できる役割のグループを管理すること。 b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。 c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし:初期設定を特定できる役割のグループはない b) なし c) なし
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) なし:MFP 管理者による保守機能移行禁止設定は、初期立上げ時に「禁止する」に設定した後は変更しない

FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	a) なし
FPT_STM.1	a) 時間の管理	a) 年月日時分の設定
FPT_TST.1	a) 初期立ち上げ中、定期間隔、あるいは特定の条件下など、TSF 自己テストが動作する条件の管理。 b) 必要ならば、時間間隔の管理。	a) なし b) なし
FTP_ITC.1	a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。	a) なし
FTA_SSL.3	a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定。 b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。	a) なし b) なし:パネル操作のオートログアウト時間は、初期立上げ時に設定した後は変更しない
FPT_FDI_EXP.1	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。	a) なし b) なし c) なし

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。

6.1.5　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: TSF]**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、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。

6.1.6 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、Web ブラウザ、プリンタードライバーよりログインした一般利用者および管理者の最終操作から、操作パネルの場合は機器管理権限を持つ管理者が設定したオートログアウト時間(180 秒)、Web ブラウザの場合は固定オートログアウト時間(30 分)、プリンタードライバーからの印刷情報の受信完了]**後に対話セションを終了しなければならない。

6.1.7 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およ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、および秘密情報の 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 EAL3+ALC_FLR.2 である。TOE の保証コンポーネントを表 23.に示す。これは評価保証レベルの EAL3 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 23：TOE セキュリティ保証要件(EAL3+ALC_FLR.2)

保証クラス	保証コンポーネント	
ADV: 開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.3	完全な要約を伴う機能仕様
	ADV_TDS.2	アーキテクチャ設計
AGD: 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: ライフサイクルサポート	ALC_CMC.3	許可の管理
	ALC_CMS.3	実装表現の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_DVS.1	セキュリティ手段の識別
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
	ALC_FLR.2	欠陥報告手続き
ASE: 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	導き出され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: テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト: 基本設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
AVA: 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 24 示す。表 24 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 24：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
FAU_GEN.1										✓
FAU_GEN.2										✓
FAU_STG.1										✓
FAU_STG.4										✓
FAU_SAR.1										✓
FAU_SAR.2										✓
FDP_ACC.1(a)	✓	✓	✓							
FDP_ACC.1(b)							✓			
FDP_ACF.1(a)	✓	✓	✓							
FDP_ACF.1(b)							✓			
FDP_RIP.1	✓									
FIA_AFL.1							✓			
FIA_ATD.1							✓			
FIA_SOS.1							✓			
FIA_UAU.1							✓	✓		
FIA_UAU.7							✓			
FIA_UID.1							✓	✓		
FIA_USB.1							✓			
FPT_FDI_EXP.1								✓		
FMT_MSA.1(a)	✓	✓	✓							
FMT_MSA.1(b)							✓			
FMT_MSA.3(a)	✓	✓	✓							
FMT_MSA.3(b)							✓			
FMT_MTD.1				✓	✓	✓				
FMT_SMF.1				✓	✓	✓				
FMT_SMR.1				✓	✓	✓				
FPT_STM.1										✓
FPT_TST.1									✓	
FTA_SSL.3							✓	✓		

FTP_ITC.1	✓	✓	✓	✓	✓	✓				

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、利用者文書、削除された文書、一時的な文書あるいはその断片が、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持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、下記の対策を満たすことが必要である。

(1) 利用者文書へのアクセス制御を規定して実施する
FDP_ACC.1(a)および FDP_ACF.1(a)によって、一般利用者毎にアクセスできる利用者文書、その利用者文書に対して許可する操作が決定され、その結果に従って一般利用者に利用者文書へのアクセスを許可する。

(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) 利用者文書の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、LAN インタフェースから送信される利用者文書および LAN インタフェースで受信する利用者文書が保護される。

(4) セキュリティ属性の管理
FMT_MSA.3(a)によって、利用者文書へのデフォルト許可利用者は利用者文書を蓄積した一般利用者に制限する。
FMT_MSA.1(a)によって、文書利用者リストはMFP管理者により管理される。

O.DOC.NO_DIS を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら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 利用者文書の改変保護

O.DOC.NO_ALT は、利用者文書が、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持っているがその利用者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、下記の対策を満たすことが必要である。

(1) 利用者文書へのアクセス制御を規定して実施する
FDP_ACC.1(a)および FDP_ACF.1(a)によって、一般利用者毎にアクセスできる利用者文書、その利用者文書に対して許可する操作が決定され、その結果に従って一般利用者に利用者文書へのアクセスを許可する。

(2) 利用者文書の送受信に高信頼チャネルを利用する
FTP_ITC.1 によって、LAN インタフェースから送信される利用者文書および LAN インタフェースから受信する利用者文書が保護される。

(3) セキュリティ属性の管理
FMT_MSA.3(a)によって、利用者文書へのデフォルト許可利用者は利用者文書を蓄積した一般利用者に制限する。
FMT_MSA.1(a)によって、文書利用者リストはMFP管理者により管理される。

O.DOC.NO_ALT を実現するために必要な対策は(1)、(2)、(3)である。したがって、これら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.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持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、下記の対策を満たすことが必要である。

(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)および FDP_ACF.1(a)によって、一般利用者毎にアクセスできる利用者ジョブ、その利用者ジョブに対して許可する操作が決定され、その結果に従って一般利用者に利用者ジョブへのアクセスを許可する。

(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、LAN インタフェースから送信される利用者ジョブ、および LAN インタフェースから受信する利用者ジョブが保護される。

(3) セキュリティ属性の管理
FMT_MSA.3(a)によって、利用者ジョブへのデフォルトアクセス者は利用者ジョブを新規作成した一般利用者に制限する。
FMT_MSA.1(a)によって、一般利用者のログインユーザー名はMFP管理者により管理される。

O.FUNC.NO_ALT を実現するために必要な対策は(1)、(2) 、(3)である。したがって、これら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、下記の対策を満たすことが必要である。

(1) TSF 保護情報の管理
FMT_MTD.1 によって、年月日設定、時刻設定を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、特権を持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、LAN インタフェースから送信される TSF 保護情報、および LAN インタフェースで受信する TSF 保護情報が保護される。

O.PROT.NO_ALT を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら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、下記の対策を満たすことが必要である。

(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のアクセスを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のアクセスをスーパーバイザーに許可する。管理者ログインパスワードのアクセスをスーパーバイザーと当該MFP管理者に許可する。監査ログのアクセスを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、特権を持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、LAN インタフェースから送信される TSF 秘密情報、および LAN インタフェースで受信する TSF 秘密情報が保護される。

O.CONF.NO_DIS を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら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、下記の対策を満たすことが必要である。

(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のアクセスを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のアクセスをスーパーバイザーに許可する。管理者ログインパスワードのアクセスをスーパーバイザーと当該MFP管理者に許可する。監査ログのアクセスを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、特権を持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、LAN インタフェースから送信される TSF 秘密情報、および LAN インタフェースで受信する TSF 秘密情報が保護される。

O.CONF.NO_ALT を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら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利用者の制限を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、下記の対策を満たすことが必要である。

(1) TOE 利用前に利用者を識別認証する
FIA_UID.1 によって、TOE 利用前に利用者の識別が行われる。
FIA_UAU.1 によって、TOE 利用前に登録された利用者であるか認証が行われる。

(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利用者が利用できる機能とその機能に対して許可する操作が決定されている。

(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、操作パネルに対して、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、一定時間操作がない場合にオートログアウトする。

(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は MFP 管理者、一般利用者の利用機能リストは MFP 管理者によって管理される。
FMT_MSA.3(b)によって、一般利用者が利用できる機能を、MFP 管理者が一般利用者の利用機能リストで許可した機能のみに制限する。

O.USER.AUTHORIZED を実現するために必要な対策は(1)、(2)、(3)、(4)、(5)である。したがって、これら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.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(a)、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 2600.1-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 インタフェース管理

O.INTERFACE.MANAGED は、TOE が保護資産を送受信する際に通信経路を保護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、下記の対策を満たすことが必要である。

(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、LAN インタフェースは利用前に利用者の識別が行われる。
FIA_UAU.1 によって、操作パネルあるいは LAN インタフェースは利用前に登録された利用者であるか認証が行われる。

(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。

O.INTERFACE.MANAGED を実現するために必要な対策は(1)、(2)、(3)である。したがって、これら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.1、FIA_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、FlashROM にインストールされているソフトウェアが正規の MFP 制御ソフトウェアであ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、下記の対策を満たすことが必要である。

(1) セルフチェック
FPT_TST.1 によって、起動時に FlashROM にインストールしてあるソフトウェアが正規の MFP 制御ソフトウェアであることを確認する。

O.SOFTWARE.VERIFIED を実現するために必要な対策は(1)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FTP_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、下記の対策を満たすことが必要である。

(1) 監査ログを記録する
FAU_GEN.1 および 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。

O.AUDIT.LOGGED を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら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 を達成することで O.AUDIT.LOGGED 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 25 に示す。

表 25 : 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 FIA_UID.1	FAU_GEN.1 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
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) FMT_MSA.3(a)	FDP_ACC.1(a) FMT_MSA.3(a)	なし
FDP_ACF.1(b)	FDP_ACC.1(b) FMT_MSA.3(b)	FDP_ACC.1(b) 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 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	なし
FMT_MSA.1(a)	[FDP_ACC.1(a) または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1	なし
FMT_MSA.1(b)	[FDP_ACC.1(b) または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1	なし
FMT_MSA.3(a)	FMT_MSA.1(a)	FMT_MSA.1(a)	なし

	FMT_SMR.1	FMT_SMR.1	
FMT_MSA.3(b)	FMT_MSA.1(b) FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1	なし
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 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

上記の表にある通り、要求されているすべての依存性は満たされている。

6.3.4 セキュリティ保証要件根拠

本 TOE は市販製品である MFP のソフトウェアである。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 は中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.2)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。

一方で、攻撃をより困難にするために関連情報の秘密を守る必要があり、開発環境についてもセキュアな環境であることを保証すること、すなわち開発セキュリティ(ALC_DVS.1)は重要である。

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、評価期間およびコストを考慮すると、本 TOE に対する評価保証レベルは EAL3+ALC_FLR.2 が妥当である。

7 TOE 要約仕様

本章では、6.1 章で記述された機能要件を TOE が満たす方法・メカニズムについて機能要件毎に記述する。

FAU_GEN.1（監査データ生成）

TOE は、表 26 に示す監査事象発生時に、表 26 に示す監査ログを生成し監査ログファイルへ追加する。なお、表 26 の共通監査データは、全ての監査事象で記録する情報項目で、個別監査データは、監査するために付加情報を必要とする監査事象を生成する際に記録する情報項目を示している。

表 26：監査事象と監査データ

監査対象事象	監査ログ	
	共通監査データ	個別監査データ
監査機能の開始	- 事象の日付・時刻 - 事象の種別 - サブジェクト識別情報 - 結果	－
監査機能の終了		－
利用者文書の蓄積、印刷、ダウンロード、削除		－
ログイン操作の成功と失敗		－
表 22 管理項目の記録		－
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		－
SSL 暗号化通信の失敗		通信方向（IN/OUT）と対象機 IP アドレス

－:個別監査データはなし

※監査機能の開始と終了事象は、TOE の起動事象で代用する。

FAU_GEN.2（利用者識別情報の関連付け）

TOE は、各監査対象事象の発生時に、その事象の発生原因となった利用者の識別情報（ログインユーザー名）を監査ログに付加する。

FAU_SAR.1（監査レビュー）

TOE は、識別認証に成功した MFP 管理者のみに、監査ログをテキスト形式で読み出すことを許可する。監査ログの読出しは、TOE の Web 機能から提供する。

FAU_SAR.2（限定監査レビュー）

TOE は、識別認証に成功した MFP 管理者のみに、監査ログの読出しと削除を許可する。監査ログの読出しは、TOE の Web 機能から提供する。

FAU_STG.1（保護された監査証跡格納）

TOE は、識別認証に成功した MFP 管理者のみに、監査ログの読出し、削除の操作を実行する機能を提供する。MFP 管理者以外の利用者に対しては、監査ログにアクセスするための機能を提供しない。

FAU_STG.4（監査データ損失の防止）

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。

FDP_ACC.1(a)（サブセットアクセス制御）

TOE は、MFP 管理者プロセスによる利用者文書の削除の操作を制御し、一般利用者プロセスによる利用者文書の削除、印刷、ダウンロードの操作を制御し、スーパーバイザープロセスが利用者文書を操作できないことを制御する。また、MFP 管理者プロセスによる利用者ジョブの削除の操作を制御し、一般利用者プロセスによる一般利用者自身の利用者ジョブの削除操作を制御する。

FDP_ACC.1(b)（サブセットアクセス制御）

TOE は、一般利用者プロセスによるコピー機能、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実行を制御する。

FDP_ACF.1(a)（セキュリティ属性によるアクセス制御）

TOE は、利用者文書、利用者ジョブに対してアクセスできる利用者役割と、各利用者役割に許可される操作の間の規則を表 10、表 11、表 12 に示す通り規定し、その規定に従って利用者文書、利用者ジョブにアクセスできる各利用者に対して、適切な操作を提供する。

TOE は、一般利用者プロセスに一般利用者のログインユーザー名を、スーパーバイザープロセスにスーパーバイザーのログインユーザー名を、MFP 管理者プロセスに MFP 管理者のログインユーザー名をセキュリティ属性として関連付ける。また、利用者文書には、文書利用者リストをセキュリティ属性として関連付け、利用者ジョブには、利用者ジョブを新規作成した利用者のログインユーザー名をセキュリティ属性として関連付ける。

TOE は、一般利用者プロセスによる利用者文書（プリンター利用者文書、スキャナー利用者文書）の蓄積に際して、蓄積する利用者文書（プリンター利用者文書、スキャナー利用者文書）にセキュリティ属性として文書利用者リストを設定する。

一般利用者プロセスによる利用者文書（プリンター利用者文書、スキャナー利用者文書）へのアクセスに際しては、一般利用者プロセスに関連付けられた一般利用者のログインユーザー名と、利用者文書に関連付けられた文書利用者リストの一般利用者のログインユーザー名をチェックし一致した場合に、その一般利用者プロセスに対してプリンター利用者文書の削除および印刷の操作、あるいはスキャナー利用者文書の削除およびダウンロードの操作を許可するアクセス制御を実施する。

TOE は、利用者ジョブのセキュリティ属性として、利用者ジョブを新規作成した利用者のログインユーザー名を関連付ける。

TOE は、一般利用者プロセスによる利用者ジョブへのアクセスに際して、一般利用者プロセスに関連付けられた一般利用者のログインユーザー名と、利用者ジョブに関連付けられた利用者ジョブ作成者のログインユーザー名をチェックし一致した場合に、その一般利用者プロセスに対して利用者ジョブの削除の操作を許可するアクセス制御を実施する。

また、MFP 管理者プロセスに対して、蓄積されている全ての利用者文書の削除操作、作成されている全ての利用者ジョブの削除操作を許可するアクセス制御を実施する。

ただし、スーパーバイザープロセスに対しては、蓄積されている全ての利用者文書への操作、作成されている全ての利用者ジョブへの操作を拒否するアクセス制御を実施する。

FDP_ACF.1(b)（セキュリティ属性によるアクセス制御）

TOE は、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に対してアクセスできる利用者役割と、各利用者役割に許可される操作の間の規則を表 13、表 14 に示す通り規定し、その規定に従ってコピー機能、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にアクセスできる各利用者に対して、適切な操作を提供する。

TOE は、一般利用者プロセスにセキュリティ属性として一般利用者のログインユーザー名と、利用機能リスト（一般利用者がアクセス権を許可されている機能のリスト）を関連付ける。

TOE は、一般利用者プロセスによるコピー機能、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へのアクセスに際して、一般利用者プロセスに関連付けられた利用機能リストの中に、一般利用者プロセスがアクセスしようとしている機能が存在するかどうかをチェックし、利用機能リストの中にアクセスしようとしている機能が存在する場合のみ、その一般利用者プロセスに対して機能の実行を許可するアクセス制御を実施する。

FDP_RIP.1（サブセット情報保護）

TOE は、HDD 上の削除された利用者文書、一時的に利用された文書、あるいはその断片に対して指定データを上書きすることにより、残存情報が残らないように消去する機能を提供する。

FIA_AFL.1（認証失敗時の取り扱い）

TOE は、利用者のログインユーザー名毎に利用者認証に失敗した回数をカウントする。利用者認証に成功した場合は、利用者認証に成功した利用者のログインユーザー名に対する利用者認証の失敗回数を0にリセットする。

利用者認証の失敗回数が、MFP 管理者により予め設定されたログインパスワード入力許容回数に達するまで連続して認証に失敗した場合、その利用者のログインユーザー名をロックアウトする。

ログインパスワード入力許容回数は、MFP 管理者が1回から 5 回の間で設定する回数である。

TOE は、下記のいずれかの条件を満たした利用者のロックアウトを解除する。

（1） ロックアウト時間経過による解除

利用者がロックアウトになった時点からロックアウト時間経過後にロックアウトを解除する。ロックアウト時間は、MFP 管理者が設定する時間（60 分）である。ロックアウトの経過時間は、ロックアウトとなった利用者毎に計時する。

（2） ロックアウト解除者による解除

利用者役割毎に決められたロックアウト解除者がロックアウトを解除する。各利用者役割のロックアウト解除者を表 27 に示す。

表 27：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

（3） TOE の電源オフ/オンによる解除

管理者（MFP 管理者、スーパーバイザー）がロックアウトした場合、TOE の電源オフ/オンによる再起動にて管理者のロックアウトを解除する。

FIA_ATD.1（利用者属性定義）

TOE は、一般利用者には一般利用者のログインユーザー名を、スーパーバイザーにはスーパーバイザーのログインユーザー名を、MFP 管理者には MFP 管理者のログインユーザー名をセキュリティ属性として関連付けて維持する。

FIA_SOS.1（秘密の検証）

TOE は、一般利用者、MFP 管理者、スーパーバイザーのログインパスワードを以下の（1）に記載する文字を使用して登録、変更する機能を提供する。
登録、変更するログインパスワードは、以下の（2）、（3）の条件に合致することをチェックし、条件に合致した場合はログインパスワードを登録し、条件に合致しない場合はログインパスワード登録せずエラー表示する。

(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ログイン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）

TOE は、操作パネルからログインしている利用者がいない場合は操作パネルへ利用者のログインユーザー名とログインパスワードの入力を要求する画面を表示し、PC から TOE の Web 機能へアクセスがあった場合は Web ブラウザの画面に利用者のログインユーザー名とログインパスワードの入力を要求する画面を表示する。両者とも、利用者が入力した利用者のログインユーザー名とログインパスワードで認証をする。

PC からプリンター機能として利用者文書の蓄積要求を受信した際には、利用者文書として蓄積する機能に先立って、PC から送信されてくる利用者のログインユーザー名とログインパスワードで認証する。

表 28 に識別認証機能が識別する利用者、認証方法を示す。

表 28：TOE が提供する機能と識別する利用者と認証方法

識別する利用者	認証方法
一般利用者	操作パネル、PC の Web ブラウザおよびプリンタードライバーから入力された一般利用者のログインユーザー名とログインパスワードが、TOE に登録されている一般利用者のログインユーザー名とログインパスワードに一致することを確認する。
管理者	操作パネル、PC の Web ブラウザから入力された管理者のログインユーザー名とログインパスワードが、TOE に登録されている管理者のログインユーザー名とログインパスワードに一致することを確認する。

FIA_UAU.7（保護された認証フィードバック）

TOE は、操作パネルから利用者が入力するログインパスワードに対して、ダミー文字を認証フィードバック領域に表示する。

FIA_UID.1（識別のタイミング）

TOE は、操作パネルからログインしている利用者がいない場合は操作パネルへ利用者のログインユーザー名とログインパスワードの入力を要求する画面を表示し、ログインしている利用者がいない PC から TOE の Web 機能へアクセスがあった場合は Web ブラウザの画面に利用者のログインユーザー名とログインパスワードの入力を要求する画面を表示する。両者とも、利用者が入力した利用者のログインユーザー名で識別をする。

PC からプリンター機能として利用者文書の蓄積要求を受信した際には、利用者文書として蓄積する機能に先立って、PC から送信されてくる利用者のログインユーザー名で識別する。

FIA_USB.1（利用者-サブジェクト結合）

TOE は、識別認証に成功した利用者に対して、一般利用者ならば一般利用者プロセスと結合し、スーパーバイザーならばスーパーバイザープロセスと結合し、MFP 管理者ならば MFP 管理者プロセスと結合する。さらに一般利用者プロセスには一般利用者のログインユーザー名を、スーパーバイザーにはスーパーバイ

ザーのログインユーザー名を、MFP 管理者プロセスには MFP 管理者のログインユーザー名をセキュリティ属性として関連付けて、各利用者役割に該当する操作権限を反映させる。

また、TOE は MFP 管理者を最大 4 人まで新規作成すること、MFP 管理者を削除することを許可する。ただし、MFP 管理者がいなくなる場合には削除することを許可しない。

FMT_MSA.1(a)（セキュリティ属性の管理）

TOE は、表 18 に記述するセキュリティ属性に対して表 18 に記述する操作を表 18 に記述する利用者役割に許可する機能を提供する。

TOE は、MFP 管理者に、一般利用者のログインユーザー名と MFP 管理者のユーザーログイン名、および文書利用者リストに対する以下の操作を許可する機能を提供する。

- 一般利用者のログインユーザー名の問い合わせ、改変、新規作成、削除
- MFP 管理者のログインユーザー名の新規作成
- MFP 管理者自身のログインユーザー名の問い合わせ、改変
- 文書利用者リストの問い合わせ、改変

TOE は、スーパーバイザーに、スーパーバイザーのログインユーザー名と MFP 管理者のログインユーザー名に対する以下の操作を許可する機能を提供する。

- スーパーバイザーのログインユーザー名の問い合わせ、改変
- MFP 管理者のログインユーザー名の問い合わせ

TOE は、一般利用者に、一般利用者のログインユーザー名と文書利用者リストに対する以下の操作を許可する機能を提供する。

- 一般利用者自身のログインユーザー名の問い合わせ
- 一般利用者自身が蓄積した利用者文書の文書利用者リストの問い合わせ、改変

FMT_MSA.1(b)（セキュリティ属性の管理）

TOE は、表 19 に記述するセキュリティ属性に対して表 19 に記述する操作を表 19 に記述する利用者役割に許可する機能を提供する。

TOE は、MFP 管理者に、一般利用者のログインユーザー名と一般利用者の利用機能リストに対する以下の操作を許可する機能を提供する。

- 一般利用者のログインユーザー名の問い合わせ、改変、新規作成、削除
- 一般利用者の利用機能リストの問い合わせ、改変

TOE は、一般利用者に、一般利用者のログインユーザー名と一般利用者の利用機能リストに対する以下の操作を許可する機能を提供する。

- 一般利用者自身のログインユーザー名の問い合わせ
- 一般利用者自身の利用機能リストの問い合わせ

FMT_MSA.3(a)（静的属性初期化）

TOE は、一般利用者が利用者文書を蓄積した際に、蓄積した利用者文書にセキュリティ属性として文書利用者リストを関連付ける。文書利用者リストは、蓄積した利用者文書へのアクセスを許可される利用者であり、文書利用者リストのデフォルト値には、利用者文書を蓄積した一般利用者のログインユーザー名を設定する。

TOE は、一般利用者が利用者ジョブを新規作成した際に、新規作成した利用者ジョブにセキュリティ属性として一般利用者のログインユーザー名を関連付ける。デフォルト値には、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を設定する。

FMT_MSA.3(b)（静的属性初期化）

TOE は、一般利用者がコピー機能、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を実行するために、一般利用者プロセスにセキュリティ属性として利用機能リストを関連付ける。

利用機能リストは、一般利用者に対して実行を許可された機能（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）のリストであり、実行を許可された機能が設定される。利用機能リストのデフォルト値は、全ての機能（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）の実行許可が設定されおり、一般利用者の登録時に MFP 管理者が一般利用者に対して実行を許可する機能を設定する。

FMT_MTD.1（TSF データの管理）

TOE は、表 21 にリストしている TSF 情報（TSF データ）に対して、表 21 に記述する操作を、表 21 に記述する利用者役割に許可する機能を提供する。

TOE は、スーパーバイザーに、以下に示す操作を許可する機能を提供する。

- スーパーバイザーのログインパスワードの改変
- MFP 管理者のログインパスワードの改変
- 年月日時分設定の問い合わせ
- 保守機能移行禁止設定の問い合わせ

TOE は、MFP 管理者に、以下に示す操作を許可する機能を提供する。

- 一般利用者のログインパスワードの新規作成、改変
- MFP 管理者のログインパスワードの新規作成
- MFP 管理者自身のログインパスワードの改変
- ログインパスワード入力許容回数の問い合わせ
- ロックアウト解除タイマー設定の問い合わせ
- ロックアウト時間の問い合わせ
- 年月日時分設定の問い合わせ、改変
- 監査ログの問い合わせ、削除
- 保守機能移行禁止設定の問い合わせ

TOE は、一般利用者に、以下に示す操作を許可する機能を提供する。

- 一般利用者自身のログインパスワードの改変
- 年月日時分設定の問い合わせ

- 保守機能移行禁止設定の問い合わせ

FMT_SMF.1（管理機能の特定）

TOE は、表 22 に示したセキュリティ管理機能を提供する。

- MFP 管理者の管理
- 一般利用者のログインパスワードの管理
- MFP 管理者のログインパスワードの管理
- スーパーバイザーのログインパスワードの管理
- 一般利用者のログインユーザー名の管理
- MFP 管理者のログインユーザー名の管理
- スーパーバイザーのログインユーザー名の管理
- 利用者文書の文書利用者リストの管理
- 年月日時分設定の管理

FMT_SMR.1（セキュリティの役割）

TOE は、識別認証に成功した利用者に対して利用者に関連付けられた利用者役割のプロセスを結合して維持し、利用者を TOE に登録する際に、一般利用者、スーパーバイザー、MFP 管理者の利用者役割を割り付ける。

さらに、TOE は、利用者のログインユーザー名、ログインパスワードへの操作を定められた利用者に限定することで、セキュリティ役割を維持する。

以下の操作を MFP 管理者に限定する。

- 一般利用者のログインユーザー名の新規作成、削除
- MFP 管理者のログインユーザー名の新規作成
- 一般利用者のログインパスワードの新規作成
- MFP 管理者のログインパスワードの新規作成

以下の操作を MFP 管理者自身に限定する。

- MFP 管理者のログインユーザー名の改変

以下の操作を一般利用者自身と MFP 管理者に限定する。

- 一般利用者のログインユーザー名の問い合わせ
- 一般利用者のログインパスワードの改変

以下の操作を MFP 管理者自身とスーパーバイザーに限定する。

- MFP 管理者のログインユーザー名の問い合わせ
- MFP 管理者のログインパスワードの改変

以下の操作をスーパーバイザーに限定する。

- スーパーバイザーのログインユーザー名の問い合わせ、改変
- スーパーバイザーのログインパスワードの改変

FPT_STM.1（高信頼タイムスタンプ）

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。

FPT_TST.1（TSF テスト）

TOE は、電源投入後の初期立上げ中に自己テストのスイートを実行し、MFP 制御ソフトウェアの実行コードの完全性と、監査ログデータファイルの完全性を検証する。MFP 制御ソフトウェアの実行コードの完全性の検証により異常が認められた場合には、操作パネルにエラー表示し、一般利用者が TOE を利用できない状態で動作停止する。監査ログデータファイルの完全性の検証により異常が認められた場合には、操作パネルにエラー表示し、一般利用者が TOE を利用できない状態で動作停止する。MFP 制御ソフトウェアの実行コードの完全性と監査ログデータファイルの完全性の検証でともに異常が認められなかった場合は、利用者が TOE を利用できる状態にする。

FPT_FDI_EXP.1（外部インタフェースへの制限された情報転送）

TOE は、操作パネルあるいは LAN インタフェースからの入力情報に対しては、かならず TSF による識別認証が行われ、その後に各種機器設定変更あるいは利用者文書としてドキュメントボックスへの保存処理が行われる。したがって、それらの処理無しに、入力情報を LAN インタフェース経由で転送する機能を提供しない。

FTA_SSL.3（TSF 起動による終了）

TOE は、利用者が操作パネルよりログイン後、操作パネルからの最終操作から、機器管理権限を持つ管理者が予め設定したオートログアウト時間（180 秒）を経過した場合に、強制的にオートログアウトする機能を提供する。

TOE は、利用者が Web ブラウザよりログイン後、Web ブラウザからの最終操作から、固定オートログアウト時間（30 分）経過した場合に、強制的にオートログアウトする機能を提供する。

なお、本 TOE は、プリンタードライバーからのインタフェースを含んでおり、プリンタードライバーからの印刷情報を受け取った直後、強制的にログアウトする機能を提供する。

FTP_ITC.1（TSF 間高信頼チャネル）

TOE は、高信頼 IT 製品である PC 起動の Web ブラウザ経由の操作、および高信頼製品である PC 起動のプリント操作において、TOE と PC 間の LAN 経由通信を保護するために、高信頼チャネルとして SSL 暗号化通信を提供する。TSF 起動の高信頼チャネル通信は存在しない。