Aficio MP 4001/5001 series

with DataOverwriteSecurity Unit Type I

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　　：2011 年 03 月 10 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	2011-03-10	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、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。

タイトル : Aficio MP 4001/5001 series with DataOverwriteSecurity Unit Type I セキュリティターゲット

バージョン : 1.00

作成日付 : 2011 年 03 月 10 日

作成者 : 株式会社リコー

1.2 TOE 参照

本 TOE の識別は、TOE を構成するデジタル複合機(以下、MFP と言う)、ファクスコントローラユニット(以下、FCU と言う)、セキュリティカード(残存情報消去オプション)、および蓄積文書暗号化カードの識別情報で行う。MFP の識別情報は、製品名称、およびバージョンである。MFP 製品名称は、販売地域、販売会社によって名称が異なるが、名称が違うだけで MFP の構成要素は同じである。MFP バージョンは、ソフトウェアとハードウェアのバージョンで構成される。FCU、セキュリティカードの識別情報は、それぞれの名称とバージョンであり、蓄積文書暗号化カードの識別情報はその名称である。TOE の識別情報を表 1 に示す。

表 1 : TOE の識別情報

名称		バージョン	
MFP 製品名称	Ricoh Aficio MP 4001、 Ricoh Aficio MP 4001G、 Ricoh Aficio MP 5001、 Ricoh Aficio MP 5001G、 Savin 9240、 Savin 9240G、 Savin 9250、 Savin 9250G、 Lanier LD140、 Lanier LD140G、 Lanier LD150、 Lanier LD150G、 Lanier MP 4001、	ソフトウェア	
		System/Copy	1.02
		Network Support	7.34
		Scanner	01.24
		Printer	1.01
		Fax	02.00.00
		RemoteFax	02.00.00
		Web Support	1.04
		Web Uapl	1.02
		Network DocBox	1.00
		animation	1.3
		Option PCL	1.03

名称		バージョン	
	Lanier MP 5001、 Gestetner MP 4001、 Gestetner MP 4001G、 Gestetner MP 5001、 Gestetner MP 5001G、 nashuatec MP 4001、 nashuatec MP 5001、 Rex-Rotary MP 4001、 Rex-Rotary MP 5001、 infotec MP 4001、 infotec MP 5001	OptionPCLFont	1.01
		Engine	1.00:01
		OpePanel	1.08
		LANG0	1.07
		LANG1	1.07
		ハードウェア	
		Ic Key	1100
		Ic Hdd	01
FCU 名称	Fax Option Type 5001	GWFCU3-19(WW)	02.00.00
セキュリティカード名称	DataOverwriteSecurity Unit Type I	Data Erase Opt	1.01m
蓄積文書暗号化カード名称	HDD Encryption Unit Type A	—	

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、ファクス

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 製品であるデジタル複合機(以降、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。

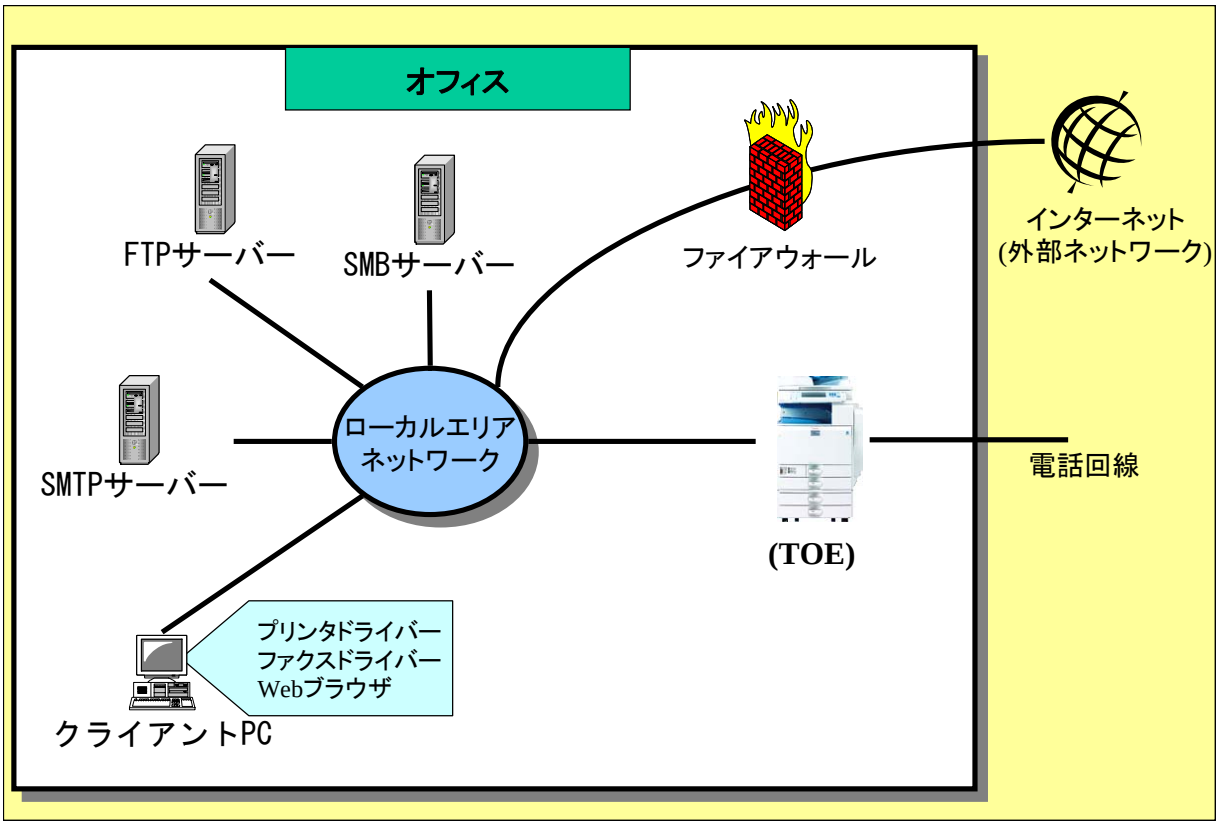

図 1 : TOE の利用環境

TOE は図 1 に示すオフィス環境において使用されることを想定している。利用者は TOE が備える操作パネルおよびローカルエリアネットワークに接続されるクライアント PC から TOE を操作することができる。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
- 紙文書のコピー・ファクス送信・蓄積・ネットワーク送信
- 蓄積文書の印刷・ファクス送信・ネットワーク送信・削除

また、TOE は電話回線を通じて受信した情報を文書として蓄積することができる。

[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 から以下の 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。

- 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の印刷・ファクス送信・ネットワーク送信・削除

・ プリンタードライバー経由の文書蓄積・印刷
・ ファクスドライバー経由の文書の蓄積・ファクス送信

[電話回線]

外部ファクスと送受信するための、公衆回線を指す。

[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 の文書を E メール送信する場合に、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
・ ファクス回線分離機能

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、ファクスユニット、コントローラボード、HDD、Ic Hdd、ネットワークユニット、USB ポート、SD カードスロット、および SD カードのハードウェアから構成される MFP である。

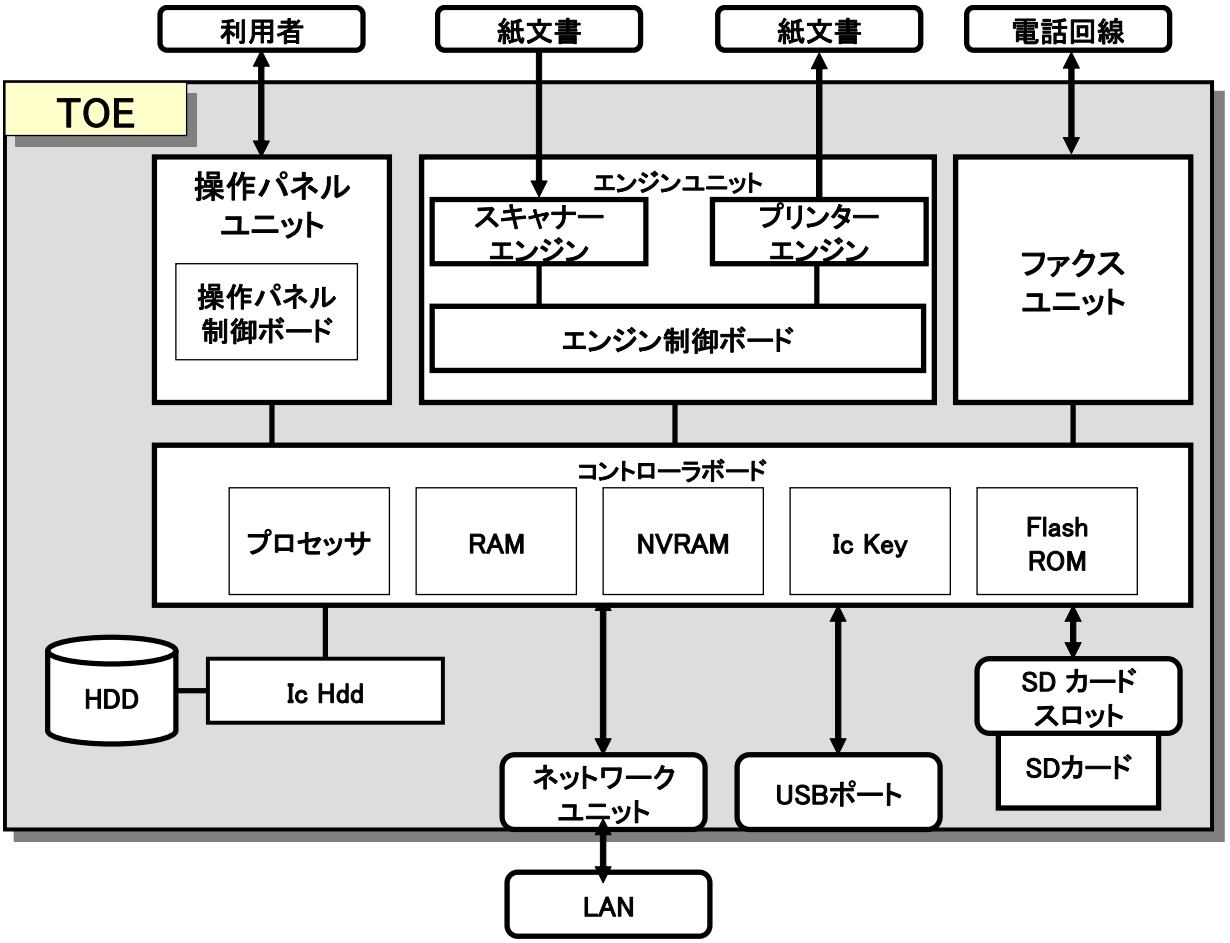

図 2 : TOE のハードウェア構成

■ コントローラボード

プロセッサ、RAM、NVRAM、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
  TOE を構成する MFP 制御ソフトウェアのうち、System/Copy、Network Support、Scanner、Printer、Fax、RemoteFax、Web Support、Web Uapl、Network DocBox、animation、Option PCL、OptionPCLFont、LANG0、および LANG1 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上の 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 が相当する。
- 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ー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 が相当する。
- ファクスユニット
  モデム機能を持ち電話回線と接続し、G3 規格で他のファクス装置とファクスの送受信をするユニット。コントローラボードと接続し、MFP 制御ソフトウェアとファクスユニットの制御情報の送受信、ファクス文書の送受信をする。TOE を識別する要素のうち FCU が該当する。
- 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、一般利用者のログインパスワードが保管されている。
- Ic Hdd
  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。
  物理的にはオプションではなく、標準装備である。
- 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/SD カードスロット
  SD カードは、MFP 制御ソフトウェアのうち Data Erase Opt が書き込まれているメモリであり、機器内部にある SD カードスロットに挿入して使用する。SD カードスロットへの SD カードのセットは、カスタマー・エンジニアのみが設置時にカバーを開けて行う。

1.4.2 ガイダンス

本 TOE のガイダンス文書には、[英語版-1]、[英語版-2]、[英語版-3]、[英語版-4]、[英語版-5]のガイダンスセットがあり、販売地域および販売会社に応じていずれかのガイダンスのセットを配付する。ガイダンスは TOE を構成する製品毎に配付される。以下に、ガイダンスセット毎のガイダンス文書を製品別に示す。

[英語版-1]

表 2：英語版-1 のガイダンス

TOE を構成する製品	製品のガイダンス文書
MFP	• 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions About This Machine • 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions Troubleshooting • Notes for Users D092-7727 • App2Me Start Guide • Manuals for Users 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Manuals for Administrators 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Notes for Users D060-7781 • Notes for Users G189-6775

	• Notes for Users D092-7905 • To Users of This Machine • Operating Instructions Notes On Security Functions • Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 • VM Card Manuals • Help(83NHAQENZ)
FCU	—
セキュリティカード	• Manuals DataOverwriteSecurity Unit Type H/I • Notes for Users
蓄積文書暗号化カード	—

[英語版-2]

表 3：英語版-2 のガイダンス

TOE を構成する製品	製品のガイダンス文書
MFP	• 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions About This Machine • 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 Operating Instructions Troubleshooting • Notes for Users D092-7729 • App2Me Start Guide • Manuals for Users 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Manuals for Administrators

	9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Notes for Users D060-7782 • Notes for Users G189-6776 • Notes for Users D092-7905 • To Users of This Machine • Operating Instructions Notes On Security Functions • Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 • VM Card Manuals • Help(83NHAQENZ)
FCU	—
セキュリティカード	• Manuals DataOverwriteSecurity Unit Type H/I • Notes for Users
蓄積文書暗号化カード	—

[英語版-3]

表 4：英語版-3 のガイダンス

TOE を構成する製品	製品のガイダンス文書
MFP	• Quick Reference Copy Guide • Quick Reference Fax Guide • Quick Reference Printer Guide • Quick Reference Scanner Guide • Manuals for This Machine • Safety Information for Aficio MP 4001/Aficio MP 5001

	• Notes for Users D092-7726A • App2Me Start Guide • Manuals for Users MP 4001/5001 Aficio MP 4001/5001 A • Manuals for Administrators Security Reference MP 4001/5001 Aficio MP 4001/5001 • Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Notes for Users D060-7781 • Notes for Users G189-6785 • Notes for Users D092-7907 • To Users of This Machine • Operating Instructions Notes On Security Functions • Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 • VM Card Manuals • Help(83NHAQENZ)
FCU	—
セキュリティカード	• Manuals DataOverwriteSecurity Unit Type H/I • Notes for Users
蓄積文書暗号化カード	—

[英語版-4]

表 5：英語版-4 のガイダンス

TOE を構成する製品	製品のガイダンス文書
MFP	• Quick Reference Copy Guide

	• Quick Reference Fax Guide • Quick Reference Printer Guide • Quick Reference Scanner Guide • Manuals for This Machine • Safty Information for MP 4001/MP 5001 • Notes for Users D092-7726A • App2Me Start Guide • Manuals for Users MP 4001/5001 Aficio MP 4001/5001 A • Manuals for Administrators Security Reference MP 4001/5001 Aficio MP 4001/5001 • Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Notes for Users D060-7781 • Notes for Users G189-6785 • Notes for Users D092-7907 • To Users of This Machine • Operating Instructions Notes On Security Functions • Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 • VM card Manuals • Help(83NHAQENZ)
FCU	—
セキュリティカード	• Manuals DataOverwriteSecurity Unit Type H/I • Notes for Users
蓄積文書暗号化カード	—

[英語版-5]

表 6：英語版-5 のガイダンス

TOE を構成する製品	製品のガイダンス文書
MFP	• MP 4001/MP 5001 MP 4001/MP 5001 Aficio MP 4001/5001 Operating Instructions About This Machine • MP 4001/MP 5001 MP 4001/MP 5001 Aficio MP 4001/5001 Operating Instructions Troubleshooting • Quick Reference Copy Guide • Quick Reference Printer Guide • Quick Reference Scanner Guide • Notes for Users D092-7730 • App2Me Start Guide • Manuals for Users MP 4001/5001 Aficio MP 4001/5001 • Manuals for Administrators MP 4001/5001 Aficio MP 4001/5001 • Manuals for Administrators Security Reference Supplement 9240/9250 MP 4001/5001 LD140/LD150 Aficio MP 4001/5001 • Notes for Users D060-7781 • Notes for Users G189-6775 • Notes for Users D092-7905 • To Users of This Machine • Operating Instructions Notes On Security Functions • Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std. 2600.1™-2009 • VM Card Manuals

	• Help(83NHAQENZ)
FCU	• Quick Reference Fax Guide
セキュリティカード	• Manuals DataOverwriteSecurity Unit Type H/I • Notes for Users
蓄積文書暗号化カード	—

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 7)。

表 7：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、ファクス機能、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 8)。

表 8：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	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。

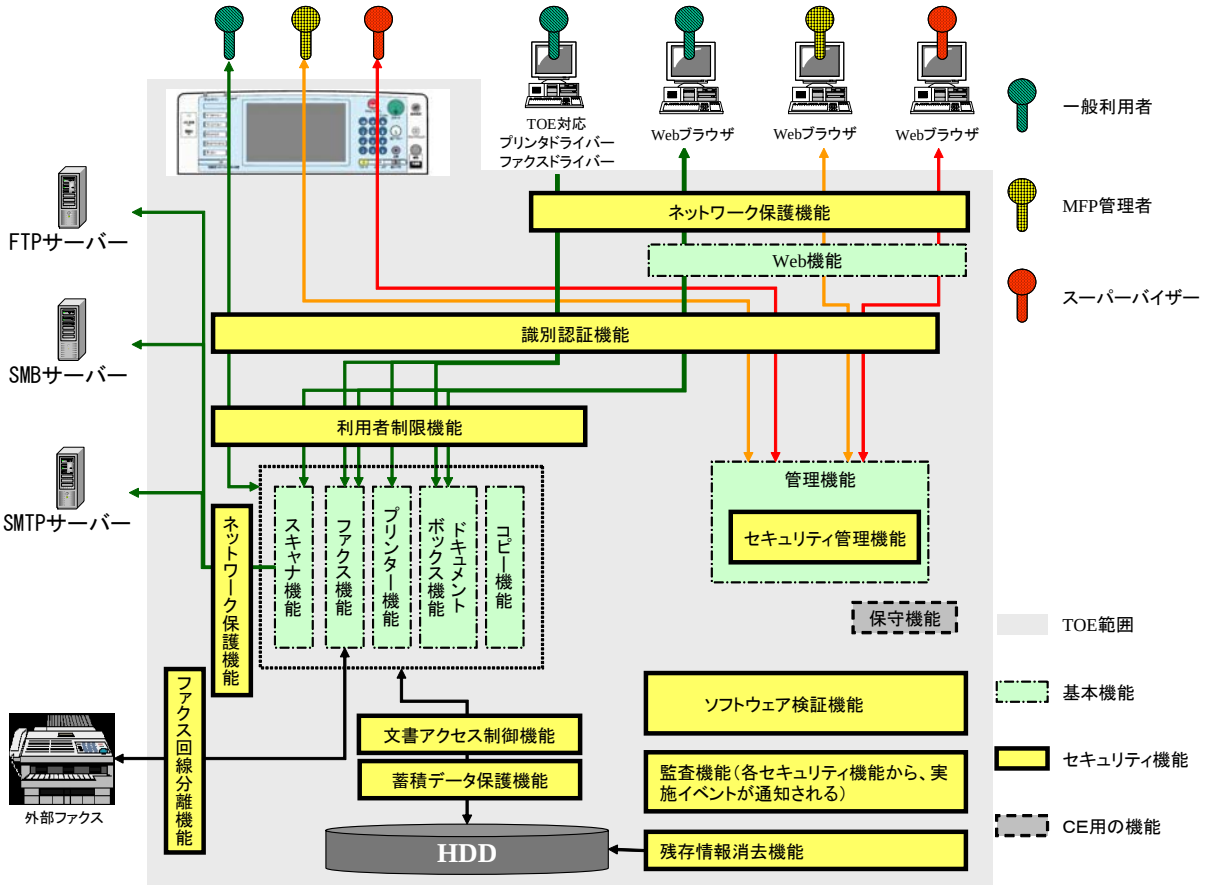

図 3 : TOE の論理的範囲

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、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。また、印刷と同時に、読取った画像を利用者文書として本体内へ蓄積することができる。本機能で蓄積した利用者文書は、ドキュメントボックス利用者文書である。コピー機能は、一般利用者が操作パネルより操作する。

■プリンター機能

プリンター機能は

- ネットワーク経由でクライアント PC からの印刷情報をドキュメントボックス利用者文書として蓄積する機能
- ネットワーク経由でクライアント PC からの印刷情報を直接印刷する機能

の 2 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クライアント PC にインストールして利用する。

プリンター機能を利用するときは、一般利用者としてクライアント PC にて印刷しようとする文書を選択し蓄積か直接印刷を指示する。

■スキャナー機能

スキャナー機能は、紙文書をスキャンして電子的な文書を作成し、その文書をフォルダー送信、メール送信、あるいはスキャナー利用者文書として TOE 内に蓄積、さらに蓄積しているスキャナー利用者文書をフォルダー送信、メール送信、または削除する機能である。本機能は、一般利用者が操作パネルより操作する。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。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およびメールアドレスに対してのみ行える。

■ファクス機能

ファクス機能は、電話回線を通して、外部ファクスとの送受信を行うものであり、下記機能から構成される。

- ファクス蓄積機能
  一般利用者は、ファクス送信利用者文書を TOE 内に蓄積することができる。ファクス送信利用者文書とは、TOE 内に蓄積されたファクス送信するための利用者文書である。ファクス送信利用者文書を蓄積する方法には、操作パネルからの操作によって紙文書をスキャンしファクス送信利用者文書を生成して蓄積する方法と、クライアント PC のファクスドライバーから受信した情報からファクス送信利用者文書を生成して蓄積する方法がある。
- ファクス送信機能
  外部のファクス装置に文書を送信する機能。送信できる文書は、紙文書、クライアント PC のファクスドライバーから受信した情報、ファクス蓄積機能で TOE 内に蓄積したファクス送信利用者文書である。紙文書は、操作パネルの操作によって、紙文書をスキャンしてファクス送信する。クライアント PC のファクスドライバーから受信する情報は、クライアント PC のファクスドライバーを操作して

ファクス送信する。ファクス送信利用者文書は、操作パネルから TOE にアクセスしてファクス送信する。ファクス送信は、予め TOE に登録された電話番号だけにファクス送信することを許可する。

- ファクス送信利用者文書操作機能
  ファクス送信利用者文書を、印刷、削除する機能。この機能は、一般利用者が操作パネルから操作を実施する。
- ファクスのフォルダー送信機能
  ファクス送信利用者文書を、操作パネルからの操作でフォルダー送信する。
  フォルダー送信の送信先サーバーは、TOE とセキュア通信できるサーバーを MFP 管理者が予め登録しておく。利用者は、MFP 管理者が登録したサーバーの中から送信先を選択してフォルダー送信する。
- ファクス受信機能
  外部ファクスから電話回線を介して受信した情報を TOE 内に蓄積する機能である。TOE 内に蓄積した文書をファクス受信文書と言う。
- ファクス受信利用者文書操作機能
  一般利用者によって操作パネルあるいは Web ブラウザからファクス受信利用者文書が操作される機能。操作パネルからは、印刷、削除を実施することができ、Web ブラウザからは印刷、削除、およびダウンロードを実施することができる。

■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、一般利用者が操作パネルと Web ブラウザから利用できる。
操作パネルからは、ドキュメントボックス利用者文書の蓄積、印刷、および削除と、ファクス送信文書の印刷と削除ができる。
Web ブラウザからは、ドキュメントボックス利用者文書の印刷および削除、ファクス送信利用者文書のファクス送信、印刷、ダウンロード、および削除、スキャナー利用者文書のフォルダー送信、メール送信、ダウンロード、およ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。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。リモート操作するためには、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。

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

識別認証機能には、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がある。プリンタードライバー/ファクスドライバーからプリンター機能/ファクス機能を利用しようとする利用者に対しては、プリンタードライバー/ファクス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識別認証を行う。

■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 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て、利用者文書およびジョブへの操作に関する制御を行う機能である。

■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 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て、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、ファクス機能)の操作に関する制御を行う機能である。

■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および改ざんを検出する機能である。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。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事で保護機能を有効化する。ファクス機能のうち PC ファクス機能利用時は、ファクス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。

■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洩から保護するため、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、特定の利用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、MFP 制御ソフトウェアの実行コードと FCU 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 制御ソフトウェアと FCU 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。

■ファクス回線分離機能

電話回線(本機能名にあるファクス回線と同意)からの入力情報をファクス受信のみに限定することにより、回線からの不正侵入を防止する機能、及びファクス転送制御により電話回線から LAN への不正侵入を防止する機能である。

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、および機能である。

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 9 にてタイプ毎に定義する。

表 9：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。

1.4.5.2. TSF 情報

TSF 情報は、保護情報と機密情報のタイプに分類される。TSF 情報について表 10 にてタイプ毎に定義する。

表 10：TSF 情報定義

タイプ	内容
保護情報	編集権限を持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。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、S/MIME 利用者情報、送信先フォルダー、蓄積受信文書ユーザー、文書利用者リスト、利用機能リスト。

秘密情報	編集権限を持った利用者以外の変更から保護し、参照権限を持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。 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、スキャナー機能、およびファクス機能)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 11 において特定の用語の意味を定義する。

表 11：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 と SD カードに格納されている。TOE を識別するソフトウェアの中では、System/Copy、Network Support、Scanner、Printer、Fax、RemoteFax、Web Support、Web Uapl、Network DocBox、animation、Option PCL、OptionPCLFont、LANG0、LANG1、および Data Erase Opt があたる。
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 機能からログイン中に、予め定められたオートログアウト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。 操作パネルのオートログアウト時間: MFP 管理者が設定したオートログアウト時間(180 秒) Web 機能のオートログアウト時間: 30 分(利用者は変更することができない時間)。固定オートログアウト時間とも言う。
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。

用語	定義
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、ファクス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	コピー機能、プリンター機能、スキャナー機能、ファクス機能、またはドキュメントボックス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で、利用者が操作パネルまたは Web ブラウザから操作する文書(本 ST では明示的に利用者文書と呼ぶ)、削除された文書、一時的な文書あるいはその断片の総称。
文書利用者リスト	利用者文書に対して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。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。
文書種別	利用者文書に関連付けられる属性の 1 つ。文書種別によって、アクセス制御のルールおよびその利用者文書に適用できる操作の種類が決定される。文書種別には以下のものがある。 ・ドキュメントボックス利用者文書: コピー機能、ドキュメントボックス機能およびプリンター機能によって、ドキュメントボックス蓄積が行われた場合の値 ・スキャナー利用者文書: スキャナー機能によって蓄積が行われた場合の値 ・ファクス送信利用者文書: ファクス機能での読取蓄積、PC ファクスによる蓄積が行われた場合の値 ・ファクス受信利用者文書: ファクスを受信蓄積した場合の値。この文書は外部から受信された「利用者が特定できない」文書である。
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、ファクスの各機能の総称。
実行中アプリケーション種別	一般利用者プロセスに関連付けられる属性。 一般利用者が利用している MFP アプリケーションを識別するための属性。一般利用者が MFP アプリケーションのいずれも操作していない状態も識別できる。
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、ファクス機能)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。
蓄積受信文書ユーザー	ファクス受信利用者文書の読み出し、削除を許可された一般利用者のリスト。
フォルダー送信	TOE 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、スキャナー機能あるいはファクス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利用者文書を送信することができる。 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、送信先のサーバーおよ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。

用語	定義
メール送信	TOE からネットワーク経由で SMTP サーバーに対して、電子メール形式で文書を送信する機能。メール送信できる文書は、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利用者文書を送信することができる。 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。
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。
PC ファクス	ファクス機能の 1 つ。クライアント PC 上のファクスドライバーを利用して、ファクス送信、文書蓄積を行う機能。PC FAX と記述されることもある。

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 2009 年 7 月 バージョン 3.1 改訂第 3 版 最終版 [翻訳第 1.0 版 最終版] CCMB-2009-07-001

  パート 2:

  セキュリティ機能コンポーネント 2009 年 7 月 バージョン 3.1 改訂第 3 版 最終版 [翻訳第 1.0 版 最終版] CCMB-2009-07-002

  パート 3:

  セキュリティ保証コンポーネント 2009 年 7 月 バージョン 3.1 改訂第 3 版 最終版 [翻訳第 1.0 版 最終版] CCMB-2009-07-003

- 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-FAX 適合

2600.1-DSR 適合

2600.1-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、HCDs が搭載する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および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 を追加している。
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。P.STORAGE_ENCRYPTION および 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、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と言える。
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、および 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。

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 SFR Package から選択した 2600.1-PRT、2600.1-SCN、2600.1-CPY、2600.1-FAX、2600.1-DSR、2600.1-SMI からなり、PP に従ったものである。

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。

本 TOE では受信したファクス受信文書の所有権の扱いについて、文書の所有権を意図された利用者に譲渡する特徴がある。これは PP APPLICATION NOTE 93 に従っている。

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を主張し、そのために FCS_CKM.1、FCS_COP.1 を追加する。
PP の FDP_ACC.1(a)および FDP_ACF.1(a)では、D.DOC に対してアクセス制御することを要求しているのに対して、本 ST では D.DOC に相当する文書のうち、利用者文書だけアクセス制御をするとし、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はアクセス制御を要求していない。これは、TOE が削除された文書、一時的な文書あるいはその断片をアクセスするための機能を提供せず、かつ TOE の残存情報消去機能が、削除された文書、一時的な文書あるいはその断片を利用者が読み出す前に、利用不可にするため、これら文書に対してアクセス制御をする必要が無いためである。よって、本 ST の FDP_ACC.1(a)および FDP_ACF.1(a)は、PP において求められている機能要件の内容を満たしている。

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、[PP]で抽象的に記述されているセキュリティ属性を、本 TOE で利用者文書、利用者ジョブのアクセス制御に実際に使用しているセキュリティ属性に具体化しておりこれは PP を逸脱していない。

FDP_ACF.1.2(a)では、ST では文書種別と TOE の各機能(実行中アプリケーション種別)により操作が異なるが、権限のある利用者に対して実施されるアクセス制御における処理は、操作パネルにおいても、プリンタードライバー経由、Web ブラウザ経由、ファクスドライバー経由の処理においても同様であり、これは PP を逸脱せずに具現化しているものである。

FDP_ACF.1.4(a)ではスーパーバイザーによる利用者文書と利用者ジョブへの操作を拒否する規則を追加している。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 が利用者文書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ことから、PP を逸脱していない。

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 TOE 機能の一部であるファクス受信機能だけを許可するとなっている。TOE は MFP 管理者に、利用者文書や利用者ジョブの削除を許可しており(共通アクセス制御 SFP、FDP_ACC.1(a)及び 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。また電話回線から受信のためアクセスするファクス受信のためのプロセスは、管理者権限で操作する利用者と見なすことができる。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。

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

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。

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している。O.STORAGE.ENCRYPTED 実現のために機能要件

FCS_CKM.1、FCS_COP.1 を追加し、それと依存関係にある他の機能要件にも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阻害するものではない。

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持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

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、電話回線)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 は、内蔵する HDD に対して、その記録内容を暗号化しなければならない。

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、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持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、電話回線、USB)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、電話回線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 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(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ため、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。また、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 12 に示す。

表 12：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	O.STORAGE.ENCRYPTED	OE.AUDIT_STORAGE.PROTCTED	OE.AUDIT_ACCESS_AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.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															✓		✓			
P.STORAGE.ENCRYPTION											✓									
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持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持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、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.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(操作パネル、LAN、USB、電話回線)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と、電話回線から使用できる機能の制限を行う。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。

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 に対する読み書きに暗号化・復号処理を行い、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;及び c) **[割付: 表 13 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);及び b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、**[割付: 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、Web 機能による通信の通信方向、Web 機能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、メール送信における宛先メールアドレス]。**

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 13 に記す。

表 13: 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	独自: ・利用者文書の蓄積の開始と終了 ・利用者文書の印刷の開始と終了

	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。	終了 ・利用者文書のダウンロードの開始と終了 ・利用者文書のファクス送信の開始と終了 ・利用者文書のメール送信の開始と終了 ・利用者文書のフォルダー送信の開始と終了 ・利用者文書の削除の開始と終了 上記における「蓄積・印刷・ダウンロード・ファクス送信・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。 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。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 33 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: 時間の変更; 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	a) 最小: オートログアウトによ

	よる対話セションの終了。	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: 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 14 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 14 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 14 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 14: 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 15 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 15 に示す暗号アルゴリズム]**と暗号鍵長**[割付: 表 15 に示す暗号鍵長]**に従って、**[割付: 表 15 に示す暗号操作]**を実行しなければならない。

表 15: 暗号操作のリスト

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
HDD 暗号鍵	FIPS197	AES	256 ビット	- HDD に書き込むデータの暗号化 -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 16 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 16：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、ファクス送信、メール送信、フォルダー送信
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 17 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 17：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	MFP アプリケーション	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 18 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 18：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 ・実行中アプリケーション種別
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	・文書種別 ・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 19 に記す利用者文書に関する規則と、表 20 に記す利用者ジョブに関する規則]**。

表 19：利用者文書に関する規則

<table>
<tr><th>サブジェクト</th><th>オブジェクト</th><th>アクセスを管理する規則</th></tr>
<tr><td>一般利用者プロセス</td><td>利用者文書</td><td>TOE は、利用者文書を下記 1)、2)の規則の順で操作を制御する。
1) MFP アプリケーションによる文書種別の制限
2) 一般利用者毎の操作制限

1) MFP アプリケーションによる文書種別の制限
一般利用者が操作する箇所、一般利用者プロセスに関連付けられた実行中アプリケーション種別、利用者文書に関連付けられた文書種別で決定する。下表に実行中アプリケーションと利用できる文書種別の関係を記す。
<table>
<tr><th>操作
箇所</th><th>実行中
アプリケーション種別</th><th>利用できる文書種別</th></tr>
<tr><td rowspan="3">操作
パネル</td><td>ドキュメントボックス機能</td><td>ドキュメントボックス利用者文書
ファクス送信利用者文書</td></tr>
<tr><td>スキャナー機能</td><td>スキャナー利用者文書</td></tr>
<tr><td>ファクス機能</td><td>ファクス送信利用者文書、
ファクス受信利用者文書</td></tr>
<tr><td rowspan="2">クライアント
PC(Web ブラウザ)</td><td>ドキュメントボックス機能</td><td>ドキュメントボックス利用者文書
スキャナー利用者文書(当該一般利用者にスキャナー機能の利用権限が必要)
ファクス送信利用者文書(当該一般利用者にファクス機能の利用権限が必要)</td></tr>
<tr><td>ファクス機能</td><td>ファクス受信利用者文書</td></tr>
<tr><td>クライアント
PC(プリンタードライバー)</td><td>プリンター機能</td><td>ドキュメントボックス利用者文書</td></tr>
<tr><td>クライアント
PC(ファクスドライバー)</td><td>ファクス機能</td><td>ファクス送信利用者文書</td></tr>
</table>
2) 一般利用者毎の操作制限
一般利用者プロセスに関連付けられた一般利用者ログインユーザー名が、利用者文書に関連付けられた文書利用者リストに含まれているとき、当該一般利用者プロセスに利用者文書の読出し(印刷、ダウンロード、ファクス送信、メール送信、フォルダー送信)と削除操作を許可する。</td></tr>
</table>

表 20：利用者ジョブに関する規則(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	利用者ジョブの削除	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 21 に示すサブジェクトのオブジェクトに対するアクセスを明示的に許可する規則]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

表 21：アクセスを明示的に許可する規則(a)

サブジェクト	オブジェクトに対する操作	アクセスを明示的に許可する規則
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、次の追加規則、**[割付：スーパーバイザーのログインユーザー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 22 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 22：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	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 23 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 23 : MFP アプリケーションの操作を制御する規則(b)

サブジェクト	オブジェクトに対する操作	操作を制御する規則
一般利用者プロセス	MFP アプリケーションの実行	一般利用者プロセスに関連付けられた利用機能リストに、一般利用者プロセスが利用しようとする MFP アプリケーションに関連付けられた機能種別が含まれている場合、一般利用者プロセスに対して、利用しようとする MFP アプリケーションの操作を許可する。 利用機能リストには、予め一般利用者が利用できる MFP アプリケーションを MFP 管理者が登録する。

FDP_ACF.1.3(b) TSF は、次の追加規則、**[割付: 管理者権限として動作するファクス受信機能の実行は、必ず許可される]**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: 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。

6.1.4 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 24 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 24 : 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
クライアント PC の Web ブラウザから TOE 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
クライアント PC から PC ファクスを利用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 25 に示すアクション]**をしなければならない。

表 25：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：表 26 の利用者毎に表 26 のセキュリティ属性のリストを維持する]**

表 26：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 ・利用機能リスト
スーパーバイザー	・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　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、Web ブラウザからのヘルプの参照、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、ファクス受信の実行]**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　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、Web ブラウザからのヘルプの参照、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、ファクス受信の実行]**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、実行中アプリケーション種別、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、利用機能リスト]**
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 27 にリストした属性の最初の関連付けに関する規則]**

表 27：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 ・実行中アプリケーション種別 ・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	・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 28 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 28 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 28：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
実行中アプリケーション種別	許可される操作は無し	―
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
文書種別	許可される操作は無し	―

文書種別が、ドキュメントボックス利用者文書、スキャナー利用者文書、ファクス送信利用者文書になっている利用者文書の文書利用者リスト	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
文書種別が、ファクス受信利用者文書になっている利用者文書の文書利用者リスト	問い合わせ、改変	MFP 管理者

－: TOE が操作を許可する利用者役割は無し

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 29 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 29 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 29：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
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
機能種別	許可される操作は無し	－

－: TOE が操作を許可する利用者役割は無し

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: [割付:表 30 に示すセキュリティ属性毎の特性]]**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。

表 30：静的属性初期化の特性(a)

オブジェクト	セキュリティ属性	デフォルト値	特性
利用者文書	文書種別	利用者文書を蓄積する際に利用した MFP アプリケーションに対応する値。 コピー機能、プリンター機能、ドキュメントボックス機能にて蓄積された場合、「ドキュメントボックス利用者文書」である。スキャナー機能にて蓄積された場合、「スキャナー利用者文書」である。ファクス蓄積機能にて蓄積された場合、「ファクス送信利用者文書」である。ファクス受信機能にて蓄積された場合、「ファクス受信利用者文書」である。	制限的
利用者文書 (文書種別が、ドキュメントボックス利用者文書、スキャナー利用者文書、ファクス送信利用者文書の場合)	文書利用者リスト	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である。	制限的
利用者文書 (ファクス受信利用者文書)	文書利用者リスト	蓄積受信文書ユーザーにリストされている一般利用者のログインユーザー名。	制限的
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である。	制限的

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 31 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 31：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
利用者文書	文書種別	・許可された識別された役割はなし
利用者文書 (文書種別が、ドキュメントボックス利用者文書、スキャナー利用者文書、ファクス送信利用者文書の場合)	文書利用者リスト	・MFP 管理者 ・当該利用者文書を蓄積した一般利用者
利用者文書 (ファクス受信利用者文書)	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: [割付:利用機能リストに許可的、機能種別に制限的]]**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: 利用機能リストは、MFP 管理者。機能種別は、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 32 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 32 の利用者役割]**に制限しなければならない。

表 32 : 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

TSF 情報	操作	利用者役割
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
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
蓄積受信文書ユーザー	問い合わせ、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 33 に記す管理機能]**

表 33 : 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
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
MFP 管理者による、パスワード複雑度の問い合わせ
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
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
MFP 管理者による、ロックアウト時間の問い合わせ
MFP 管理者による、文書利用者リストの問い合わせと改変

文書を蓄積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、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、改変、問い合わせ、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、改変、問い合わせ、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、蓄積受信文書ユーザーの問い合わせと改変

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、FCU 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、電話回線]**で受け取った情報を、TSF による追加の処理無しに**[割付: LAN および電話回線]**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: 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印刷情報の受信完了、ファクスドライバーからの送信情報の受信完了]**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、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 34 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 34 : 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

保証クラス	保証コンポーネント	
	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	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: 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 35 示す。表 35 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 35：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										✓	
FAU_GEN.2										✓	
FAU_STG.1										✓	
FAU_STG.4										✓	
FAU_SAR.1										✓	
FAU_SAR.2										✓	
FCS_CKM.1											✓
FCS_COP.1											✓
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、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) 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、利用者文書の読出しは利用者の役割、さらに一般利用者は、その一般利用者に与えられた操作権限によって制限している。一般利用者に対しては、実行中の MFP アプリケーションによって、利用できる利用者文書の文書種別を限定し、さらに当該一般利用者に対して読出し権限を与えられている利用者文書だけとしている。MFP 管理者とスーパーバイザーに対しては利用者文書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) 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
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。
利用者文書(オブジェクト)のセキュリティ属性である、文書利用者リスト、文書種別は、FMT_MSA.3(a)によって、利用者文書が生成された時に、必ず定められたデフォルトの値がセットされる。

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 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持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) 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、利用者文書の削除(利用者文書の編集操作は無い)は利用者の役割、さらに一般利用者は、その一般利用者に与えられた操作権限によって制限している。一般利用者に対しては、実行中の MFP アプリケーションによって、利用できる利用者文書の文書

種別を限定し、さらに当該一般利用者に対して削除権限を与えられている利用者文書だけとしている。MFP 管理者には、利用者文書の削除を許可する。スーパーバイザーに対しては利用者文書の削除を許可しない。

(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) 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。

(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。
利用者文書(オブジェクト)のセキュリティ属性である、文書利用者リスト、および文書種別は、FMT_MSA.3(a)によって、利用者文書が生成された時に、必ず定められたデフォルトの値がセットされる。

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_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)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
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。
利用者文書(オブジェクト)のセキュリティ属性である、文書利用者リスト、および文書種別は、FMT_MSA.3(a)によって、利用者ジョブが生成された時に、ジョブを生成した一般利用者のログインログインユーザー名がデフォルト値として関連付けられる。

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、年月日、時刻、S/MIME 利用者情報、送信先フォルダー、蓄積受信文書ユーザーの管理を 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。

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。

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。

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 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、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、操作パネル、Web ブラウザから一定時間操作がないままオートログアウト時間が経過した時、オートログアウトする。プリンタードライバーまたはファクス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、利用機能リストに許可的なデフォルト値を設定し、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 2600.1-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 TOE による外部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、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、電話回線で受信したデータを、TSF による追加の処理無しに LAN、電話回線から送信することを防止する。

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、MFP 制御ソフトウェアと FCU 制御ソフトウェアが正規の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 制御ソフトウェアと FCU 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 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、下記の対策を実施する必要がある。

(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。

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、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 に対する書き込みにおいて暗号化することを、および読み出しにおいて復号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、特権を持つ利用者を維持する

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 FCS_CKM.1、FCS_COP.1、FMT_MTD.1、FMT_SMF.1 および 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 36 に示す。

表 36 : 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
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] 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] 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) 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_SMR.1	FMT_MSA.1(a) FMT_SMR.1	なし
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

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 37 に示す監査事象発生時に、表 37 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 37 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 37：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(*1)	- 事象の開始日付・時刻 - 事象の終了日付・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(*1)		―
ログイン操作の成功と失敗		―
表 33 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		―
Web 機能の通信		通信方向(IN/OUT)と通信先 IP アドレス
フォルダー送信		通信先 IP アドレス
メール送信		宛先メールアドレス
ネットワークを介した印刷		通信先 IP アドレス
ネットワークを介した PC ファクス		通信先 IP アドレス
利用者文書の蓄積		―
利用者文書の読出し(印刷、ダウンロード、ファクス送信、メール送信、フォルダー送信)		―
利用者文書の削除		―
S/MIME 利用者情報の新規作成、改変、削除の成功と失敗		―
送信先フォルダーの新規作成、改変、削除の成功と失敗		―

―：個別監査データはなし

(*1): 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。

FCS_CKM.1 (暗号鍵生成)

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、標準 BSI-AIS31 に準拠した暗号鍵生成アルゴリズム TRNG で 256 ビットの HDD 暗号鍵を生成し、TOE 内の記憶領域に保管する。

FCS_COP.1 (暗号操作)

TOE は、HDD に書き込む直前にデータを暗号化し、HDD から読み出した直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。具体的な暗号操作は、以下の通りである。

表 38：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			

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、メール送信、フォルダー送信、ファクス送信の操作を制御し、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 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、ファクス機能、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 18、表 19、表 20、表 21 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。

一般利用者による利用者文書へのアクセスに際しては、まず、一般利用者が操作する箇所、利用者が実行している MFP アプリケーションから、利用できる利用者文書の文書種別を下記の通り決定する。

- 操作パネルから実行している MFP アプリケーションがドキュメントボックス機能の場合、ドキュメントボックス利用者文書に対し、印刷および削除の操作が許可され、ファクス送信利用者文書に対して、印刷および削除の操作が許可される。
- 操作パネルから実行している MFP アプリケーションがスキャナー機能の場合、スキャナー利用者文書に対し、メール送信、フォルダー送信、および削除の操作が許可される。
- 操作パネルから実行している MFP アプリケーションがファクス機能の場合、ファクス送信利用者文書に対し、ファクス送信、フォルダー送信、印刷、および削除の操作が許可され、ファクス受信利用者文書に対しては、操作パネルから印刷および削除の操作が許可される。
- Web ブラウザから実行している MFP アプリケーションがドキュメントボックス機能の場合、ドキュメントボックス利用者文書に対し印刷および削除の操作が許可され、スキャナー利用者文書に対しメール送信、フォルダー送信、ダウンロード、および削除操作が許可され、ファクス送信利用者文書に対してファクス送信、印刷、ダウンロード、および削除の操作が許可される。ただし、スキャナー利用者文書を操作するためには、当該一般利用者がスキャナー機能の利用権限を持っている必要があり、ファクス送信利用者文書を操作するためには当該一般利用者がファクス機能の利用権限を持っている必要がある。
- Web ブラウザから実行している MFP アプリケーションがファクス機能の場合、ファクス受信利用者文書に対し印刷、ダウンロード、および削除の操作が許可される。
- プリンタードライバーから実行している MFP アプリケーションがプリンター機能の場合、ドキュメントボックス利用者文書の蓄積の操作が許可される。
- ファクスドライバーから実行している MFP アプリケーションがファクス機能の場合、ファクス送信利用者文書の蓄積の操作が許可される。

一般利用者プロセスによる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、上記で特定された操作が許可される。

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、ファクス機能、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 22、表 23 に示す通り規定し、その規定に従って MFP アプリケーション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 MFP アプリケーション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 MFP アプリケーションの属性である機能種別(コピー機能、プリンター機能、スキャナー機能、ファクス機能、ドキュメントボックス機能のいずれか)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。
管理者権限として動作するファクス受信機能の実行は、必ず許可される。

FDP_RIP.1 (サブセット情報保護)

TOE は、利用者の操作によって利用者文書を削除した時、HDD 上にある利用者文書のデジタル画像情報が書き込まれている領域に対して指定パターンデータで上書きする。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、指定パターンデータで上書きする。

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 39 に示す。

表 39：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ログインユーザー名、および利用機能リストを、スーパーバイザーにはスーパーバイザーログインユーザー名を、MFP 管理者には MFP 管理者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、クライアント 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。

クライアント PC からプリンター機能として印刷および利用者文書の蓄積要求を受信した際には、印刷および利用者文書として蓄積する機能に先立って、クライアント 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。クライアント PC から PC ファクスを利用して利用者文書の送信および蓄積要求を受信した際には、送信および利用者文書として蓄積する機能に先立って、クライアント 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。

TOE は電話回線からファクスを受信した際に、受信したデータをファクス受信利用者文書として蓄積する機能に先立っての認証機能を持たない。TOE は電話回線からは認証情報を受け取ることはなく、TOE は受信した情報を用いてファクス受信機能を実行する。

TOE はクライアント PC からの Web 機能へのアクセスにおいて、利用者の認証状態に関わらず、ヘルプの参照操作を許可する。

TOE は、利用者の認証状態に関わらず、以下の操作を許可する: 利用者ジョブ一覧の参照、Web ブラウザからのヘルプの参照、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、ファクス受信の実行。

表 40 に識別認証機能が識別する利用者、認証方法を示す。

表 40 : 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、クライアント PC の Web ブラウザ、プリンタードライバー、およびファクス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、クライアント 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クライアント 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。

クライアント PC からプリンター機能として印刷および利用者文書の蓄積要求を受信した際には、印刷および利用者文書として蓄積する機能に先立って、クライアント 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。クライアント PC から PC ファクスを利用して利用者文書の送信および蓄積要求を受信した際には、送信および利用者文書として蓄積する機能に先立って、クライアント 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。

TOE は電話回線からファクスを受信した際に、受信したデータをファクス受信利用者文書として蓄積する機能に先立っての識別機能を持たない。TOE は電話回線からは識別情報を受け取ることはなく、TOE は受信した情報を用いてファクス受信機能を実行する。

TOE はクライアント PC からの Web 機能へのアクセスにおいて、利用者の識別状態に関わらず、ヘルプの参照操作を許可する。

TOE は、利用者の識別状態に関わらず、以下の操作を許可する: 利用者ジョブ一覧の参照、Web ブラウザからのヘルプの参照、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、ファクス受信の実行。

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ログインユーザー名と実行中アプリケーション種別、および利用機能リストを、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、共通アクセス制御 SFP に関するセキュリティ属性のうち、利用者による操作(新規作成、問い合わせ、改変、削除)が可能なセキュリティ属性に対する操作を特定の利用者だけに操作箇所から提供する。
表 41 に利用者による操作が可能なセキュリティ属性をリストし、各セキュリティ属性を操作できる利用者と許可された操作、操作できる箇所を記す。

表 41 : 共通アクセス制御 SFP のセキュリティ属性の管理

セキュリティ属性	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 Web ブラウザ	新規作成、 問い合わせ、 改変、 削除	MFP 管理者
		問い合わせ	当該一般利用者
実行中アプリケーション種別	操作可能箇所は無し	許可される操作は無し	―
スーパーバイザーのログインユーザー名	操作パネル Web ブラウザ	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	操作パネル Web ブラウザ	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
文書種別	操作可能箇所は無し	許可される操作は無し	―
文書種別が、ドキュメントボックス利用者文書、スキャナー利用者文書、ファクス送信利用者文書になっている利用者文書の文書利用者リスト	操作パネル Web ブラウザ	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
文書種別が、ファクス受信利用者文書になっている利用者文書の文書利用者リスト(*1)	操作パネル Web ブラウザ	問い合わせ、 改変	MFP 管理者

―: TOE が操作を許可する利用者役割は無し

(*1): MFP 管理者が蓄積受信文書ユーザーを改変した時に、文書種別がファクス受信利用者文書になっている利用者文書の文書利用者リストは、蓄積受信文書ユーザーの値に改変される。

FMT_MSA.1(b) (セキュリティ属性の管理)

TOE は、TOE 機能アクセス制御 SFP に関するセキュリティ属性の操作を特定の利用者だけに操作箇所から提供する。

表 42 に利用者による操作が可能なセキュリティ属性をリストし、各セキュリティ属性を操作できる利用者と許可された操作、操作できる箇所を記す。

表 42 : TOE 機能アクセス制御 SFP のセキュリティ属性の管理

セキュリティ属性	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 Web ブラウザ	新規作成、 問い合わせ、 改変、 削除	MFP 管理者
		問い合わせ	当該一般利用者

利用機能リスト	操作パネル Web ブラウザ	問い合わせ、改変、	MFP 管理者
		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	―

―: TOE が操作を許可する利用者役割は無し

FMT_MSA.3(a) (静的属性初期化)

TOE は、表 43 にリストしたオブジェクト生成時に、表 43 で当該オブジェクトに対応するセキュリティ属性に表 43 で当該セキュリティ属性に対応するデフォルト値を設定する。

表 43 : 共通アクセス制御 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
利用者文書	文書種別	利用者文書を蓄積する際に利用した MFP アプリケーションが、コピー機能、プリンター機能、ドキュメントボックス機能の場合、「ドキュメントボックス利用者文書」。 スキャナー機能の場合、「スキャナー利用者文書」。 ファクス蓄積機能の場合、「ファクス送信利用者文書」。 ファクス受信機能の場合、「ファクス受信利用者文書」。
利用者文書(文書種別が、ドキュメントボックス利用者文書、スキャナー利用者文書、ファクス送信利用者文書の場合)	文書利用者リスト	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
利用者文書 (ファクス受信利用者文書の場合)	文書利用者リスト	蓄積受信文書ユーザーにリストされている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。

FMT_MSA.3(b) (静的属性初期化)

TOE は、利用機能リストと機能種別のデフォルト値を設定する。

一般利用者を新規登録するとき、利用機能リストには、いずれの MFP アプリケーションも使用できる値が設定される。

機能種別は、MFP アプリケーション毎に設定値が決定されている。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、ファクス機能にはファクス機能を識別する値がそれぞれ設定される。

FMT_MTD.1 (TSF データの管理)

TOE は、表 44 に記すとおり TSF 情報(TSF データ)に対する操作を特定の利用者だけに操作箇所から提供する。

表 44 : TSF データの管理

TSF 情報	操作箇所	操作	利用者役割
一般利用者のログインパスワード	操作パネル Web ブラウザ	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	操作パネル 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 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 Web ブラウザ	問い合わせ	MFP 管理者
ロックアウト解除タイマー	Web ブラウザ	問い合わせ	MFP 管理者
ロックアウト時間	Web ブラウザ	問い合わせ	MFP 管理者
年月日	操作パネル Web ブラウザ	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
時刻	操作パネル Web ブラウザ	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	操作パネル	問い合わせ	MFP 管理者
パスワード複雑度	操作パネル	問い合わせ	MFP 管理者
監査ログ	Web ブラウザ	問い合わせ、 削除	MFP 管理者
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 Web ブラウザ	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	操作パネル Web ブラウザ	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

TSF 情報	操作箇所	操作	利用者役割
蓄積受信文書ユーザー	操作パネル Web ブラウザ	問い合わせ、 改変	MFP 管理者

FMT_SMF.1 (管理機能の特定)

TOE は、以下に示したセキュリティ管理機能を操作パネル及び Web ブラウザから提供する。

- 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
- 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
- MFP 管理者による、パスワード複雑度の問い合わせ
- 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
- 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
- MFP 管理者による、ロックアウト時間の問い合わせ
- MFP 管理者による、文書利用者リストの問い合わせと改変
- 文書を蓄積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、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、改変、問い合わせ、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、改変、問い合わせ、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、蓄積受信文書ユーザーの問い合わせと改変

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、改変、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
- 蓄積受信文書ユーザーの管理
- HDD 暗号鍵の管理
- S/MIME 利用者情報の新規作成、改変、削除
- 送信先フォルダーの新規作成、改変、削除

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
- S/MIME 利用者情報の問い合わせ
- 送信先フォルダーの問い合わせ

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する。

FCU については、制御ソフトウェア実行コードの完全性検証のために、TOE は利用者に対して検証情報を提供する。利用者はその TOE からの検証情報を、ガイダンス文書に記された検証情報と比較することによって FCU の完全性を検証し、異常が認められなかった場合にのみ TOE を利用する。

FCU 以外の構成要素については、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。電話回線からの入力情報に対して、回線から利用できる機能を TOE のファクス受信機能だけに限定しており、ファクスのプロトコルに適合しない通信は拒否する。ファクスプロトコルに則した通信のうち転送に該当する機能は、初期設置により禁止しているためデータが転送されることはない。

したがって、操作パネル、LAN インタフェース、電話回線は TSF により制御され、無処理で情報転送処理がされることはない。

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。また、ファクスドライバーからのインタフェースを含んでおり、ファクスドライバーからの送信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 IT 製品である PC 起動のプリント操作、ファクス送信操作、ファクス蓄積操作において、TOE とクライアント 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。TOE は、高信頼 IT 製品である FTP サーバーおよび SMB サーバーへのフォルダー送信操作において、TOE とサーバー間の LAN 経由通信を保護するために、TSF 起動の高信頼チャネルとして IPSec 通信を提供する。

TOE は、高信頼 IT 製品である SMTP サーバーへのメール送信操作において、TOE とサーバー間の LAN 経由通信を保護するために、TSF 起動の高信頼チャネルとして S/MIME 通信を提供する。