RICOH

imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series

セキュリティターゲット

作成者　　：株式会社リコー　船木靖，柿井弘，佐藤専
作成日付　　: 2009 年 10 月 30 日
バージョン　　: 1.13

更新履歴

バージョン	日付	作成者	詳細
1.00	2008-12-16	船木靖 柿井弘 佐藤専	初版
1.01	2009-02-10	船木靖	指摘事項修正
1.02	2009-03-31	船木靖	指摘事項修正
1.03	2009-04-10	船木靖	指摘事項修正
1.04	2009-04-14	船木靖	誤記訂正
1.05	2009-04-23	船木靖	指摘事項修正 誤記訂正
1.06	2009-06-02	船木靖	指摘事項修正 誤記訂正
1.07	2009-06-11	船木靖	誤記訂正
1.08	2009-06-15	船木靖	指摘事項修正
1.09	2009-07-10	船木靖	指摘事項修正 誤記訂正
1.10	2009-10-06	船木靖	指摘事項修正 誤記訂正
1.11	2009-10-07	船木靖	指摘事項修正
1.12	2009-10-23	船木靖	指摘事項修正
1.13	2009-10-30	船木靖	指摘事項修正

目次

図一覧

表一覧

1 ST 概説

1.1 ST 識別

本書と TOE を識別するための情報を以下に示す。

ST タイトル : imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series セキュリティターゲット

ST バージョン : 1.13

作成日付 : 2009 年 10 月 30 日

作成者 : 株式会社リコー 船木靖，柿井弘，佐藤専

TOE :

<日本語版>

Ricoh imagio MP 4000/5000 シリーズ

<英語版>

Ricoh Aficio MP 4000/5000 series

「Ricoh imagio MP 4000/5000 シリーズ」および「Ricoh Aficio MP 4000/5000 series」の製品名称は表 1 を参照。

TOE バージョン:

「Ricoh imagio MP 4000/5000 シリーズ」および「Ricoh Aficio MP 4000/5000 series」は、以下のソフトウェアとハードウェアで識別する。

ソフトウェア	System/Copy:	1.09
	Network Support	7.23
	Scanner:	01.23
	Printer:	1.09
	Fax	03.00.00
	Web Support:	1.57
	Web Uapl:	1.13.1
	Network Doc Box:	1.09.3C
ハードウェア	Ic Key	1100
	Ic Hdd	01

注釈:Printer のバージョン(X.YY と表示)の右横に「e」が追記されている場合がある。これは、言語に関する識別(「e」がない場合は日本語、「e」が追記されている場合は英語)でありセキュリティ機能には影響しない。セキュリティ機能に関する識別は、X.YY で行なう。

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

CC バージョン : Common Criteria for Information Technology Security Evaluation Ver2.3
補足-0512 適用

表 1：TOE リスト

シリーズ(series)名称	シリーズ(series)詳細
Ricoh imagio MP 4000/5000 シリーズ	Ricoh imagio MP 4000SP Ricoh imagio MP 4000SPF Ricoh imagio MP 5000SP Ricoh imagio MP 5000SPF
Ricoh Aficio MP 4000/5000 series	Ricoh Aficio MP 4000SP Ricoh Aficio MP 4000SPF Ricoh Aficio MP 5000SP Ricoh Aficio MP 5000SPF Savin 9040SP Savin 9040SPF Savin 9050SP Savin 9050SPF Lanier LD040SP Lanier LD040SPF Lanier LD050SP Lanier LD050SPF Lanier MP 4000SP Lanier MP 4000SPF Lanier MP 5000SP Lanier MP 5000SPF Gestetner MP 4000SP Gestetner MP 4000SPF Gestetner MP 5000SP Gestetner MP 5000SPF Nashuatec MP 4000SP Nashuatec MP 4000SPF Nashuatec MP 5000SP Nashuatec MP 5000SPF Rex-Rotary MP 4000SP Rex-Rotary MP 4000SPF Rex-Rotary MP 5000SP Rex-Rotary MP 5000SPF Infotec MP 4000SP Infotec MP 4000SPF Infotec MP 5000SP Infotec MP 5000SPF

1.2 ST 概要

本書は、「1.1 ST 識別」の TOE に記載した株式会社リコー製のデジタル複合機（以下、MFP と言う）のセキュリティ要件と仕様について記載したセキュリティターゲットである。MFP とは、コピー機能にスキャナー、ファクス、プリンターの各機能を組合せて構成される画像 I/O 製品であり、一般的にはオフィスの LAN に接続し

て文書データの入力・蓄積・出力に利用される。MFP は、MFP 内に蓄積された文書データを保護し、クライアントと MFP との間で送受信する文書データの漏洩に対処する。

1.3 CC 適合

この ST は以下の CC に適合している。

CC パート 2 適合

CC パート 3 適合

EAL3 適合

この ST が適合する PP はない。

1.4 用語

1.4.1 本 ST における用語

本 ST を明確に理解するために、特定の用語の意味を表 2 に定義する。

表 2: 本 ST に関連する特定の用語

用語	定義
MFP	デジタル複合機の略称。 本STでは TOE を指す。
MFP 制御ソフトウェア	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 、Fax 、Web Support、Web Uapl、Network Doc Box を含んでいる。 MFP を構成するユニットやデバイスのリソース管理を行ない、動作を制御する。
HDD	ハードディスクドライブの略称。TOE 内に取り付けられた HDD を指す。
Ic Key	暗号処理専用のマイクロプロセッサと、セキュア通信で利用される秘密鍵を含んだ EEPROM が内蔵されたチップ。 正当性確認や暗号処理などに利用する鍵と乱数の種が保管されている。
Ic Hdd	HDD に書込むデータを暗号化し、HDD から読込むデータを復号するハードウェア装置。
操作パネル	タッチパネル付き液晶ディスプレイ、ハードキー、LED で構成され、利用者が MFP の操作に利用する表示入力装置。 操作パネルユニットとも言う。
内部ネットワーク	MFP が設置されている組織が管理するネットワーク。通常はイントラネットとして構築されているオフィス内 LAN 環境のこと。
外部ネットワーク	MFP が設置されている組織が管理できないネットワーク。一般的には汎用インターネットのことを指す。

用語	定義
SMTP サーバー	Simple Mail Transfer Protocol（簡易メール転送プロトコル）を用いて、電子メールを送信するためのサーバー。
FTP サーバー	File Transfer Protocol（ファイル転送プロトコル）を用いて、クライアントとファイルを送受信するためのサーバー。
SMB サーバー	Server Message Block(サーバメッセージブロック)プロトコルを用いて、クライアントとファイルを共有するためのサーバー。
D-BOX	HDD 上の文書データを格納する領域。
印刷データ	クライアントPC内の文書を、印刷またはファクス送信するためにクライアントPCから TOE へ送信するデータ。印刷データを印刷するためにはプリンタドライバー、ファクス送信するためにはファクスドライバーをクライアント PC にインストールしておく必要がある。 印刷データはネットワークユニットおよび USB ポートから TOE に取り込まれる。
文書データ	MFPの許可利用者が、以下に記す2通りの操作のいずれかで MFP に取込んだ電子データ。 1. MFPの許可利用者の操作によって、紙原稿のイメージをスキャンしデジタル化した電子データ。 2. MFPの許可利用者が MFP に送信した印刷データを、MFP が受信し MFP が扱う形式にした電子データ。
文書データ利用者リスト	文書データ毎に設定される一般ユーザーのアクセス制御リスト。
カスタマー・エンジニア（CE）	メーカー、サービス会社、販売会社に所属して TOE の保守をする専門知識を有する者。
MFP 管理責任者	MFP を設置する組織の中で、MFP の管理者とスーパーバイザーを選任する権限を持った者（あるいは、組織の責任者）。 例：MFP の購入者、MFP の所有者、MFP を設置する部署の責任者、IT部門の責任者
管理者	TOE の許可利用者のひとつで、TOE を管理する者。管理者には、管理者役割が付与され、管理者役割に沿った管理作業を実施する。管理者は4名まで登録でき、1つ以上の管理者役割が付与される。
管理者役割	管理者に付与する管理機能。管理者役割にはユーザー管理、機器管理、ネットワーク管理、文書管理の4つがあり、それぞれの管理者役割は、登録されている管理者のいずれかに割り当てられる。
ユーザー管理	管理者役割のひとつで、一般ユーザの管理を実施する役割。ユーザー管理の役割を持った管理者をユーザー管理者と言う。
機器管理	管理者役割のひとつで、機器の管理、および監査を実施する役割。機器管理の役割を持った管理者を機器管理者と言う。
ネットワーク管理	管理者役割のひとつで、TOE ネットワーク接続の管理を実施する役割。ネットワーク管理の役割を持った管理者をネットワーク管理者と言う。
文書管理	管理者役割のひとつで、TOE に蓄積されている文書データが保存されている D-BOX と、文書データのアクセス制御リストである文書データ利用者リストの管理を実施する役割。文書管理の役割を持った管理者を文書管理者と言う。

用語	定義
スーパーバイザー	TOE の許可利用者のひとつで、管理者のパスワードを管理する者。
一般ユーザー	TOE の許可利用者のひとつで、TOE の基本機能を利用する者。
アドレス帳	一般ユーザー情報をレコードとして登録したデータ。
アドレス帳のバックアップ/リストア	アドレス帳を SD カードにバックアップ、あるいは SD カードにバックアップしているアドレス帳を TOE にリストアすること。
一般ユーザー情報	一般ユーザーに関する情報をデータ項目として構成されるレコード。データ項目には、一般ユーザーID、一般ユーザー認証情報、文書データデフォルトアクセス権リスト、S/MIME 利用者情報が含まれる。
S/MIME 利用者情報	S/MIME を利用するあたって必要となる一般ユーザー毎の情報。メールアドレス、ユーザー証明書、S/MIME 利用規定値が含まれる。
文書データデフォルトアクセス権リスト	一般ユーザー情報のデータ項目のひとつ。 新規で蓄積する文書データの文書データ利用者リストに設定するデフォルト値のこと。
文書オーナ	文書データの所有者として文書データ利用者リストに登録された一般ユーザーのこと。
文書利用者	文書データ利用者リストに登録された、文書オーナを除く一般ユーザーのこと。
蓄積受信	受信ファクスデータを印刷せずに TOE 内の HDD に蓄積する機能のこと。TOE 内に蓄積したファクスデータを蓄積受信文書データという。
直接印刷	TOE が受信した印刷データを、用紙に印刷する機能のこと。
蓄積印刷	TOE が受信した印刷データを文書データに変換し D-BOX に蓄積する機能のこと。D-BOX に蓄積した文書データは、後から印刷することができる。
直接送信	原稿スキャン前にダイヤルし、原稿をスキャンしながらファクスデータをファクス送信する機能のこと。
メモリ送信	スキャンした原稿をメモリに蓄積してからダイヤルし、ファクスデータをファクス送信する機能のこと。
蓄積文書ファクス送信	予めファクス送信のために D-BOX に蓄積されている文書データをファクス送信する機能のこと。
PC ファクス送信	クライアント PC をネットワークまたは USB で接続し、クライアント PC 内の文書データを、TOE を介してファクス送信する機能のこと。
IP-ファクス	TCP/IP を使用しているネットワークに直接接続されたファクス同士で文書の送受信をする機能のこと。また、電話回線に接続されたファクスに文書を送信することもできる。
インターネットファクス	ファクスの原稿を読込んでから E-Mail 形式に変換し、インターネットを使ってメールアドレスを持っている機器に送信する機能のこと。
メール送信	TOE から文書データを添付した電子メールを送信する機能のこと。
フォルダ配信	TOE からネットワーク経由で SMB サーバー、FTP サーバーのフォルダに文書データを送信する機能のこと。

用語	定義
ロックアウト	特定の利用者 ID に対して TOE へのアクセスを禁止すること。
MFP 制御データ	MFP の動作を決定する設定値項目の総称。
機器制御データ	MFP 制御データのうち、セキュリティ機能のふるまいに係わるデータ項目。
ネットワーク制御データ	MFP 制御データのうち、MFP をネットワークに接続するためのデータ項目。
ログインパスワード入力許容回数	同一利用者 ID で、パスワード認証失敗によりロックアウトとなるまでの回数。
ロックアウト解除タイマー設定	管理者が予め設定した時間でロックアウトが解除される動作を有効または無効にする設定。この設定が無効の場合は、管理者が直接操作することでロックアウトが解除される。
ロックアウトフラグ	許可利用者毎に割り付けられるデータで、ロックアウトされた利用者のロックアウトフラグは「有効」にセットされ、ロックアウト解除された利用者のロックアウトフラグは「無効」にリセットされる。ロックアウトフラグの操作が許可された管理者またはスーパーバイザーは、ロックアウトされた利用者のロックアウトフラグを「無効」に設定することで、ロックアウトされた利用者のロックアウトを解除できる。
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。
印刷条件	印刷時の用紙サイズ、変倍率、加工印刷情報（両面、集約など）のこと。
蓄積データ保護機能	HDD に記録されている文書データを漏洩から保護する機能。

2 TOE 記述

本章では、TOE の種別、TOE の利用環境、TOE の物理的範囲、TOE の関連者役割、TOE の論理的範囲、保護資産の概要を記述する。

2.1 TOE の種別

TOE はIT製品であり、紙文書の電子化、文書管理、印刷をするためのコピー機能、スキャナー機能、プリンター機能、ファクス機能（オプション）を提供する MFP である。

2.2 TOE の利用環境

TOE は、オフィスに設置されることを想定する。オフィスでは、利用者の必要に応じて IT 製品と TOE を、ネットワーク接続、電話回線接続、あるいは USB 接続することができる。利用者は TOE を、TOE の操作パネル、内部ネットワークに接続されたクライアント PC、または USB 接続されたクライアント PC から操作することができる。想定する TOE の利用環境について図 1 に図示し解説する。

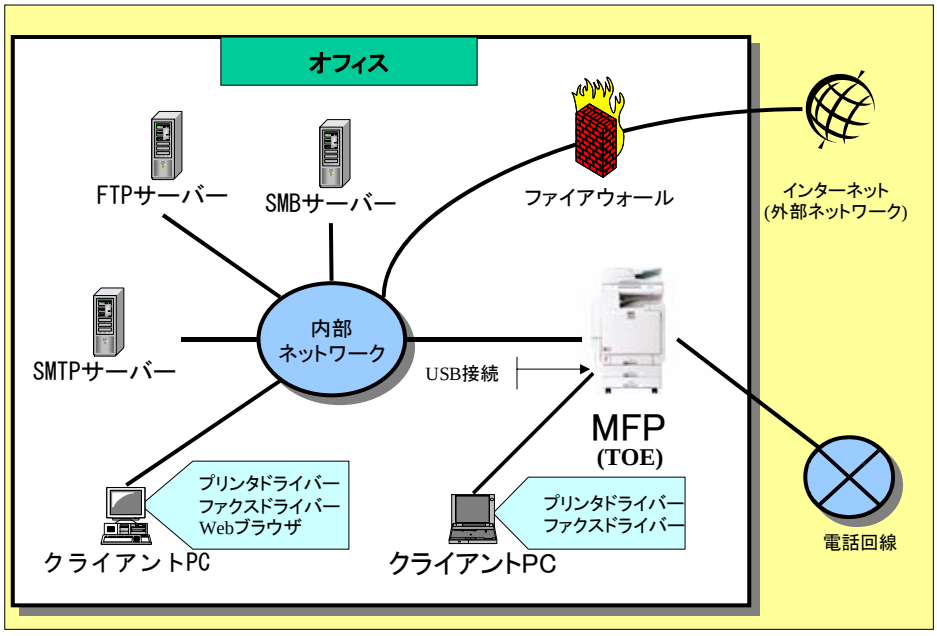

図 1：TOE の利用環境

TOE の設置場所

TOE は一般的なオフィスに設置されることを想定する。

操作パネルからの TOE 操作

操作パネルは、TOE に取り付けられているユーザーインターフェース装置で、ハードキー、LED、タッチパネル付き液晶ディスプレイで構成されている。ハードキーは利用者が TOE に情報を入力するための役割を持ち、LED は TOE が利用者に対して情報を表示する役割を持ち、タッチパネル付き液晶ディスプレイは、その両方の役割を持つ。

TOE と内部ネットワークの接続

TOE を内部ネットワークへ接続することによって、内部ネットワークに接続されている IT 製品と通信することができる。内部ネットワークは IPv4 環境を想定する。TOE が通信する IT 製品と用途について以下に記述する。

[クライアント PC からの TOE 操作]
内部ネットワークに接続したクライアント PC の Web ブラウザから TOE にアクセスして TOE の操作とデータ通信ができる。
クライアント PC には、Internet Explorer 6.0 以降をインストールしておく必要がある。

[クライアント PC からの印刷]
内部ネットワークに接続したクライアント PC 内の文書を TOE から印刷することができる。印刷するためには、ユーザーズガイダンスに記載するホームページから RPCS プリンタドライバーをクライアント PC へダウンロードしインストールする必要がある。

[クライアント PC からのファクス送信]
内部ネットワークに接続したクライアント PC 内の文書を、TOE を介してファクス送信することができる。ファクス送信するためには、ユーザーズガイダンスに記載するホームページからファクスドライバーをクライアント PC へダウンロードしインストールする必要がある。

[TOE からクライアント PC へのメール送信]
TOE は、SMTP サーバーを経由して文書データが添付されたメールをクライアント PC に送信することができる。

[FTP サーバー]
TOE は、文書データをFTPサーバーのフォルダに転送することができる。

[SMB サーバー]
TOE は、文書データをSMBサーバーのフォルダに転送することができる。

TOE と電話回線の接続

TOE を電話回線に接続することによって、ファクス送受信することができる。

TOE とクライアント PC の USB 接続

TOE とクライアント PC を USB ケーブルで接続することによって、クライアント PC から印刷、またはファクス送信することができる。

内部ネットワークと外部ネットワークの接続

内部ネットワークと外部ネットワークを接続する場合、内部ネットワークと外部ネットワークの間にファイアウォールを設置して、内部ネットワークを外部ネットワークから保護する。

2.3 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、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、Ic Hdd、HDD、ネットワークユニット、USB ポート、SD CARD スロットのハードウェアで構成される MFP である。このうちファクスユニットはオプションで、ファックスユニットを取り外した構成も適用範囲とする。TOE のハードウェア構成要素を図 2 に図示して概要を記述する。

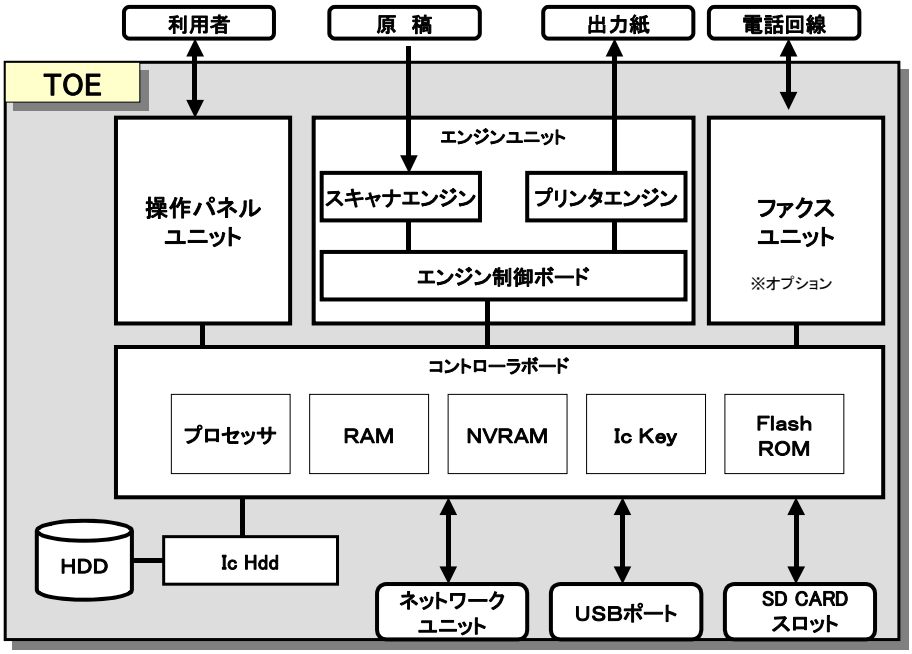

図 2：TOE のハードウェア構成

操作パネルユニット（以下、操作パネルと言う）

操作パネルは TOE に組み付けられた TOE の利用者が TOE 操作に使用するインターフェース装置で、ハードキー、LED、タッチパネル付き液晶ディスプレイと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は、ハードキーやタッチパネル付き液晶ディスプレイからの入力を MFP 制御ソフトウェアに送信、あるいは MFP 制御ソフトウェアからの指示を受信して LED の点灯および消灯、タッチパネル付き液晶ディスプレイの画面表示を実行する。

エンジンユニット

エンジンユニットは、スキャナーエンジン、プリンタエンジン、エンジン制御ボードで構成される。スキャナーエンジンは紙文書を読込むための入力装置で、プリンタエンジンは紙文書を印刷し排出する出力装置であ

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したり、MFP 制御ソフトウェアの指示によってスキャナーエンジンやプリンタエンジンを動作させたりする。

ファクスユニット（オプション）

ファクスユニットはモデム機能を持ち電話回線と接続してファクスの送受信を行なう装置である。
ファクスユニットには MFP 制御ソフトウェアとのインターフェースがあり、MFP 制御ソフトウェアにファクス通信状態を通知したり、MFP 制御ソフトウェアの指示によってファクス通信の制御を実行したりする。

コントローラボード

コントローラボードはプロセッサ、RAM、NVRAM、Ic Key、FlashROM が載った基板である。コントローラボードは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、ネットワークユニット、USB ポート、SD CARD スロット、Ic Hdd と接続される。Ic Hdd にはさらに HDD が接続される。プロセッサ、RAM、NVRAM、Ic Key 、FlashROM の概要を以下に記載する。

[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]
画像メモリとして利用される揮発性メモリ。

[NVRAM]
MFP の動作を決定する MFP 制御データが入った不揮発性メモリ。

[Ic Key]
乱数発生、暗号鍵生成の機能を持ち、MFP 制御ソフトウェアの改ざん検知に利用されるセキュリティチップ。

[FlashROM]
MFP 制御ソフトウェアがインストールされているメモリ。

Ic Hdd

Ic Hdd は HDD に保管する情報を暗号化し、HDD から読出す情報を復号する機能を持ったセキュリティチップである。

HDD

HDD は画像データ、識別認証に利用するユーザー情報が書込まれるハードディスクドライブである。

ネットワークユニット

ネットワークユニットは Ethernet（100BASE-TX/10BASE-T）をサポートしたネットワークのインターフェース基板である。

USB ポート

USB ポートは、クライアント PC と TOE を USB 接続し、クライアント PC から印刷、あるいはファクス送信するために使用する。

SD CARD スロット

SD CARD スロットは、CE が SD カードを使った保守作業するために使用するスロットであり、TOE の側面にあって、通常はカバーで覆われネジ止めされている。CE は、保守作業をする際に、このカバーを外して SD カードを出し入れする。
特に設置時には、CE が蓄積データ保護機能を活性化するための SD カードをこのスロットにセットして、蓄積データ保護機能を活性化にする。

2.4 TOE の関連者役割

TOE の運用に関連する者の役割について記述する。

2.4.1 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 の管理者とスーパーバイザーを選任する役割を持った者のことを言う。
MFP 管理責任者は、4名までの管理者と、スーパーバイザーを1名選任する。管理者を選任する際には、ユーザー管理、機器管理、ネットワーク管理、文書管理の管理者役割の内、少なくとも1つ以上の管理者役割を管理者に与える。

2.4.2 管理者

管理者とは、TOE に管理者として登録された利用者のことで、TOE には管理者を1から4名まで登録する。管理者の管理者役割は、ユーザー管理、機器管理、ネットワーク管理、文書管理がある。管理者は、管理者役割を兼任することができ、管理者役割は必ず1人以上の管理者に割り当てられる。TOE の工場出荷時には管理者が1人設定され、その管理者が4つの管理者役割を兼任する設定になっており、TOE の設置時に MFP 管理責任者に管理者として選任された者が、選任された管理者の ID、パスワード、管理者役割を設定変更する。表 3 に管理者役割毎の管理作業を記述する。

表 3：管理者役割一覧

管理者役割	説明
ユーザー管理	一般ユーザーを管理する。
機器管理	機器の管理と、監査をする。
ネットワーク管理	TOE のネットワーク接続を管理する。
文書管理	TOE 内に蓄積されている文書を管理する。

2.4.3 スーパーバイザー

スーパーバイザーとは、管理者パスワードの管理をする役割をもった利用者で、管理者パスワードを変更することができる。TOE には、スーパーバイザーが1名登録されている。工場出荷時の TOE には、デフォルトのスーパーバイザーが登録されており、MFP 管理責任者がスーパーバイザーとして選任した者がデフォルトのスーパーバイザーID とパスワードを設定しなおす。

2.4.4 一般ユーザー

一般ユーザーとは、ユーザー管理者によってアドレス帳に登録された TOE の許可利用者のことであり、TOE への文書データ蓄積と、TOE に蓄積されている文書データに対して操作することができる。

2.4.5 カスタマー・エンジニア

カスタマー・エンジニア（以下、CE と言う）とは、メーカー、サービス会社、販売会社に所属して TOE の保守をする専門知識を有する者を言う。

2.5 TOE の論理的範囲

TOE の論理的範囲は、TOE が提供する機能である。本章では、TOE が利用者に提供するサービスである「基本機能」と、TOE の脅威に対抗するための「セキュリティ機能」について図 3 に図示し、記述する。

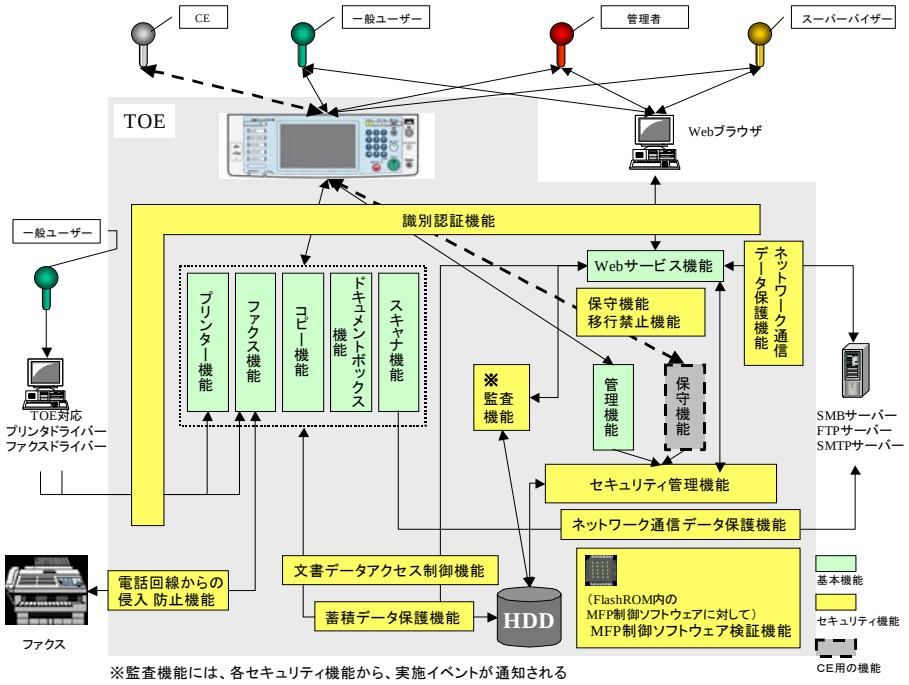

図 3：TOE の論理的範囲

2.5.1 基本機能

基本機能には、コピー機能、プリンター機能、ファクス機能、スキャナー機能、ドキュメントボックス機能、管理機能、Web サービス機能がある。本章では、これら基本機能について記述する。

基本機能は、操作パネルまたはクライアント PC の Web ブラウザから操作することができる。
操作パネルから操作する場合は、図 4 に示す操作パネルから利用する機能を選択する。一般ユーザーは、操作パネル上の左側にある「コピー」、「ドキュメントボックス」、「ファクス」、「プリンター」、「スキャナー」ボタンを押下して、コピー機能、ドキュメントボックス機能、プリンター機能、ファクス機能、スキャナー機能を利用する。管理者、スーパーバイザーは、操作パネル上の左上にある「初期設定/カウンター/問い合わせ情報」ボタンを押下して管理機能を利用する。

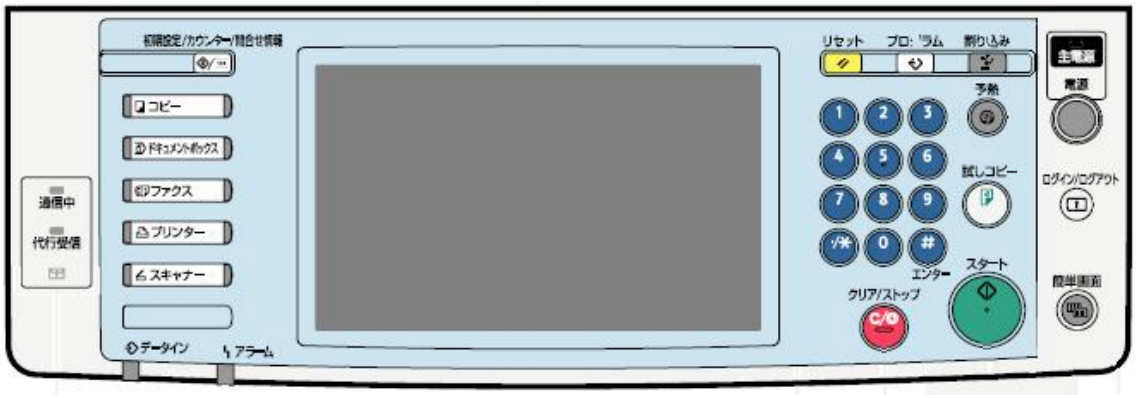

図 4：操作パネル

また、一般ユーザー、管理者、スーパーバイザーは、クライアント PC の Web ブラウザから TOE の Web サービス機能にアクセスし、利用者役割に対応した機能を利用することができる。以下に、基本機能の概要を記述する。

2.5.1.1 コピー機能

コピー機能は、原稿をスキャンし、読み取ったイメージデータを利用者が指定する部数、倍率、編集指定（たとえば複数ページの原稿イメージを1枚の用紙に印刷する集約指定）などの印刷条件に従って印刷する機能である。また、読み取った原稿イメージを文書データとして D-BOX に蓄積することができる。コピー機能で D-BOX に蓄積された文書データは、「2.5.1.5 ドキュメントボックス機能」を使って印刷、削除することができる。

2.5.1.2 プリンター機能

プリンター機能は、クライアント PC から送られる印刷データを印刷する機能である。TOE はクライアント PC からネットワークまたは USB ポートで印刷データを受信する。TOE は受信した印刷データを直接印刷あるいは蓄積印刷によって印刷する。蓄積印刷では、印刷データは文書データとして D-BOX に蓄積され、蓄積された文書データは「2.5.1.5 ドキュメントボックス機能」を使って印刷、削除することができる。

2.5.1.3 ファクス機能

ファクス機能は、電話回線を通してファクス装置と送受信する機能である。ファクス機能には、ファクス受信機能（以下、ファクス受信と言う）、ファクス送信機能（以下、ファクス送信と言う）、ファクス送受信データを印刷や削除する機能がある。

ファクス受信は、受信したファクスデータを印刷するか、ファクス受信データに変換し D-BOX に蓄積する。D-BOX に蓄積したファクス受信データは、ファクス機能または「2.5.1.5 ドキュメントボックス機能」を使って印刷、削除することができる。

ファクス送信には、操作パネルから操作する直接送信、メモリ送信、蓄積文書ファクス送信と、クライアント PC から操作する PC ファクス送信がある。ファクスで送信するために、D-BOX に蓄積した文書データは、「2.5.1.5 ドキュメントボックス機能」を使って印刷、削除することができる。

尚、MFP はファクス機能の一部として IP-ファクスとインターネットファクス機能を提供するが、IP-ファクスとインターネットファクス機能は、本評価の対象外である。

2.5.1.4 スキャナー機能

スキャナー機能は、紙原稿を電子化してクライアント PC で扱えるようにするために、原稿をスキャンし、読み取ったイメージデータを文書データとしてネットワーク経由でフォルダ配信、メール送信する機能である。また、読み取ったイメージデータを D-BOX に文書データとして蓄積することができる。スキャナー機能を使って D-BOX に蓄積した文書データはスキャナー機能で、メール送信、フォルダ配信、削除することができる。

2.5.1.5 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、原稿をスキャンし、読み取ったイメージデータを D-BOX に文書データとして蓄積する機能である。また、コピー機能、プリンター機能、ファクス機能およびドキュメントボックス機能で D-BOX に蓄積された文書データを印刷、削除することができる。ただし、スキャナー機能で蓄積された文書データは扱うことができない。

2.5.1.6 管理機能

管理機能は、機器動作を決定する情報、TOE をネットワーク接続するための情報、利用者に関する情報、文書データを利用制限するための情報を設定する機能で、TOE の許可利用者(一般ユーザー、管理者、スーパーバイザー)それぞれの役割に応じて、設定できる情報が決められている。管理機能は、操作パネルから操作するか、クライアント PC から Web サービス機能にアクセスして操作することができる。設定する情報によっては、操作パネルからだけ設定できる情報、クライアント PC からだけ設定できる情報もある。管理機能のうち、セキュリティに係わる機能を「2.5.2.6 セキュリティ管理機能」に記載する。
尚、本機能で利用制限するアドレス帳のバックアップ/リストアは、本評価の対象外である。

2.5.1.7 Web サービス機能

Web サービス機能は、TOE の許可利用者(一般ユーザー、管理者、スーパーバイザー)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 Web ブラウザをインストールし、TOE とクライアント PC をネットワークで接続する必要がある。利用者は、Web ブラウザから TOE の Web サーバーに接続することで Web サービス機能が利用できる。リモート操作できる TOE の操作は以下の通りである。

1. D-BOX に蓄積している文書データの印刷、送信、削除、ダウンロード
   但し、印刷はコピー機能、ドキュメントボックス機能、ファクス機能、プリンター機能で蓄積した文書データのみ。送信は、スキャナー機能で蓄積した文書データのみ。ダウンロードは、スキャナー機能、またはファクス機能で蓄積した文書データのみ。
2. 管理機能の一部
3. TOE の状態確認

2.5.2 セキュリティ機能

セキュリティ機能には、監査機能、識別認証機能、文書データアクセス制御機能、蓄積データ保護機能、ネットワーク通信データ保護機能、セキュリティ管理機能、保守機能移行禁止機能、電話回線からの侵入防止機能、MFP 制御ソフトウェア検証機能がある。本章では、これらセキュリティ機能について記述する。

2.5.2.1 監査機能

監査機能は、TOE の運用状況を確認、あるいはセキュリティ侵害を検知するために必要な事象発生時に監査ログを記録する機能である。記録した監査ログは、機器管理者だけに読出し、削除の操作を許可する。監査ログの読出しは Web サービス機能、監査ログの削除は操作パネルと Web サービス機能を利用して実施できる。

2.5.2.2 識別認証機能

識別認証機能は、操作パネル、クライアント PC から TOE を利用しようとする者に利用者 ID と認証情報を入力させ利用者の特定と本人確認をする機能である。ただし、クライアント PC からの印刷あるいはファクス送信の場合は、TOE ではないプリンタドライバーまたはファクスドライバーから利用者が、利用者 ID と認証情報を入力後に TOE へ送信する。TOE は、受信した利用者 ID と認証情報で識別認証をする。
また、識別認証機能には、同じ利用者 ID で認証に連続で失敗した回数がログインパスワード入力許容回数に達した場合、その利用者 ID を一時的にログインできなくするアカウントロック、利用者がパスワードを入力中に盗み見られないよう、認証フィードバックエリアに表示するパスワードを伏字で表示する認証フィードバックエリア保護、予めユーザー管理者が設定するパスワード最小桁数とパスワード複雑度の条件を満たすパスワードだけを登録するパスワード品質維持が含まれる。
本 TOE が持つ識別認証機能は他にもあるが、上記以外の識別認証機能は、本評価の対象外である。

2.5.2.3 文書データアクセス制御機能

文書データアクセス制御機能は、識別認証機能で認証された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、文書データへの操作を許可する機能である。
文書データに対する操作には、以下の3通りがある。

1. 文書データ読出し:D-BOX に蓄積している文書データを読出すこと
2. 文書データ編集 :D-BOX に蓄積している文書データの印刷条件の変更を登録すること
3. 文書データ削除 :D-BOX に蓄積している文書データを削除すること

文書管理者には、D-BOX に蓄積している全文書データに対して削除操作が許可される。一般ユーザーには、文書データ毎に、閲覧、編集、編集/削除、フルコントロールのうちいずれかのアクセス権が設定されるか、アクセス権なしが設定される。一般ユーザーの文書データに対するアクセス権と文書データに対する操作の関係を表 4 に記述する。

表 4：文書データのアクセス権と操作の対応表

アクセス権＼文書データへの操作	文書データ読出し	文書データ編集	文書データ削除
閲覧	X		
編集	X	X	
編集/削除	X	X	X
フルコントロール	X	X	X

X:操作可能　空欄:操作不可

2.5.2.4　蓄積データ保護機能

蓄積データ保護機能は、HDD に記録されている文書データを漏洩から保護するため、文書データを正規の方法で読出す以外は文書データの内容を理解することを困難にする機能である。

2.5.2.5　ネットワーク通信データ保護機能

ネットワーク通信データ保護機能は、ネットワーク上の文書データと印刷データを不正なアクセスから保護する機能である。文書データまたは印刷データの送信方法によって、通信データを保護するための通信プロトコルは異なる。以下に、送信方法と保護手段の対応関係を記述する。
尚、使用する通信プロトコルは、ネットワーク管理者が TOE の設置環境や TOE の用途に応じて決定する。

1. クライアント PC から Web サービス機能を利用した文書データのダウンロード（SSL プロトコル）
2. クライアント PC からの印刷、またはファクス送信（SSL プロトコル）
3. TOE から FTP サーバー、または SMB サーバーへの文書データ配信（IPSec プロトコル）
4. TOE からクライアント PC へ文書データを添付したメールの送信（S/MIME）

2.5.2.6　セキュリティ管理機能

セキュリティ管理機能は、「2.5.2.2 識別認証機能」で認証に成功した管理者、スーパーバイザー、一般ユーザーに対して、その利用者役割に応じたセキュリティ管理のための操作を許可する機能である。

1. 文書データ利用者リスト管理
   文書データ利用者リスト管理は、文書データ利用者リストの改変を特定の利用者だけに許可する機能である。文書データ利用者リストの改変には、文書オーナの変更、文書データ利用者リストへ文書利用者を新規登録、文書データ利用者リストに登録済みの文書利用者の削除、文書利用者の操作権限の変更がある。このうち、文書オーナの変更は、文書管理者にのみに許可する。その他の操作は、文書管理者、文書オーナ、文書データに対してフルコントロールの権限を持つ文書利用者に許可される。

文書データ蓄積時の、文書データ利用者リストには、文書データデフォルトアクセス権リストが設定される。

2. 管理者情報管理
管理者情報管理とは、管理者の登録と削除、管理者役割の追加と削除、管理者 ID と管理者パスワードの変更を特定の利用者に許可することである。
管理者の登録と管理者役割の追加は、管理者だけに許可される操作である。管理者の削除、管理者役割の削除、管理者 ID の変更は当該管理者に許可される操作である。管理者パスワードの変更は、当該管理者とスーパーバイザーに許可される操作である。尚、管理者役割の追加は、自身に割り当てられている管理者役割に限るという条件があり、管理者役割の削除には、他の管理者が削除対象の管理者役割を持っている場合だけに限ると言う条件がある。
管理者は、1つ以上の管理者役割を持つ必要があるため、管理者が他の管理者を登録する際には、自身が持つ管理者役割の中から1つ以上を新規の管理者に付与(追加)する必要がある。また、管理者が自身の管理者役割を全て削除した場合、その管理者の管理者情報は自動で削除される。

3. 一般ユーザー情報管理
一般ユーザー情報管理とは、一般ユーザー情報の新規作成、変更、削除の操作を特定の利用者役割だけに許可することである。利用者役割と許可される操作の関係は、ユーザー管理者には、一般ユーザー情報の新規作成、変更、削除が許可され、一般ユーザーには、アドレス帳に登録されている自身の一般ユーザー情報の変更が許可される。ただし、一般ユーザーは自身の一般ユーザー情報であっても一般ユーザーID を変更できない。

4. スーパーバイザー情報管理
スーパーバイザーの ID とパスワードの変更をスーパーバイザーに許可する。

5. 機器制御データ管理
機器管理者、ユーザー管理者、および文書管理者の役割に応じた機器制御データのデータ項目の設定を、それぞれの管理者に許可する。

2.5.2.7 保守機能移行禁止機能

保守機能は、機器管理者から依頼を受けた CE が操作パネルから TOE の保守サービスを実行する機能で、保守機能移行禁止機能は、保守機能の操作を禁止する機能である。本 ST では保守機能移行禁止機能を稼動させた状態を評価範囲とする。

2.5.2.8 電話回線からの侵入防止機能

電話回線からの侵入防止機能は、ファクスユニットが装着された機器において、TOE に接続した電話回線からは許可された通信だけを受付ける機能である。

2.5.2.9 MFP 制御ソフトウェア検証機能

MFP 制御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。

2.6 保護資産

TOE が保護対象とする資産は、文書データ、印刷データである。以下に文書データ、印刷データについて記述する。

2.6.1 文書データ

文書データは、TOE 外から様々な手段で TOE 内に取込まれる。TOE 内に取込まれた文書データは、TOE 内に蓄積するか、TOE 外に出力することができる。TOE 内に蓄積している文書データは、印刷条件を編集することや削除することもできる。

2.6.1.1 文書データの取込み

文書データの取込みには、以下の2通りがある。

1. スキャナーユニットからの取込み
   TOE のスキャナーから紙原稿のイメージを読込み文書データを生成する。
2. ネットワーク/USB からの取込み
   TOE がネットワーク回線あるいは USB から受信した印刷データを TOE が扱う形式に変換し文書データを生成する。

2.6.1.2 文書データの蓄積

TOE 内に蓄積している文書データは、D-BOX に蓄積される。D-BOX に蓄積されている文書データは、不正アクセスと漏洩から保護される。

2.6.1.3 文書データの出力

文書データの出力には、以下の5通りがある。

1. クライアント PC（メール宛先）に送信
2. SMB サーバーおよび FTP サーバーに送信
3. TOE からクライアント PC にダウンロード
4. 印刷
5. ファクス送信

このうち、1.から 3.の出力方式において、通信経路上にある文書データは、漏洩から保護され、改ざんがあった場合は検知される。

2.6.2 印刷データ

印刷データとは、印刷あるいはファクスの出力イメージが記述されたデータで、印刷あるいはファクスする際にクライアント PC 内の文書からクライアント PC にインストールされているプリンタドライバーあるいはファクスドライバーによって生成され、内部ネットワーク経由または USB ポートから TOE に取り込まれる。印刷データは、クライアント PC から TOE に送信される際の内部ネットワーク経路において、漏洩から保護され、改ざんがあった場合は検知される。

3 TOE セキュリティ環境

本章は、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 前提条件

本 TOE の利用環境に関わる前提条件を識別し、記述する。

A.ADMIN **（管理者の条件）**

管理者は、管理者に課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、一般ユーザーに TOE をセキュアに運用させるものとする。さらに、管理者は、管理者の特権を利用して悪意を持った不正をしないものとする。

A.SUPERVISOR **（スーパーバイザーの条件）**

スーパーバイザーは、スーパーバイザーに課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、スーパーバイザーの特権を利用して悪意を持った不正をしないものとする。

A.NETWORK **（ネットワークの接続条件）**

TOE が接続されるネットワークをインターネットなどの外部ネットワークと接続する場合は、外部ネットワークから内部ネットワークを保護するものとする。

3.2 脅威

本 TOE の利用及び利用環境において想定される脅威を識別し、記述する。本章に記述する脅威は、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者による攻撃であり、攻撃者は低レベルの攻撃能力を持つ者とする。

T.ILLEGAL_USE **（TOE の不正利用）**

攻撃者が、TOE の外部インターフェース（操作パネル、ネットワークインターフェース、USB インターフェース、または SD CARD インターフェース）から TOE に不正にアクセスし文書データを読出す、あるいは文書データを削除するかもしれない。

T.UNAUTH_ACCESS （TOE 内に蓄積されている保護資産へのアクセス違反）

TOE の許可利用者が、TOE の許可利用者に提供する TOE の外部インターフェース（操作パネル、ネットワークインターフェース、あるいは USB インターフェース）から文書データに対して利用権限を越えたアクセスをするかもしれない。

T.ABUSE_SEC_MNG （セキュリティ管理機能の不正利用）

セキュリティ管理機能の利用を許可されないものが、セキュリティ管理機能を不正に利用するかもしれない。

T.SALVAGE （メモリの持ち去り）

攻撃者が、TOE から HDD を持去り、文書データを暴露するかもしれない。

T.TRANSIT （通信経路上の盗聴、改ざん）

攻撃者が、内部ネットワーク上の TOE が送受信する文書データと印刷データを不正に入手し漏洩、または改ざんするかもしれない。

T.FAX_LINE （電話回線からの侵入）

攻撃者が電話回線から TOE に不正にアクセスするかもしれない。

3.3 組織のセキュリティ方針

IT製品にインストールされたソフトウェアの完全性を要求する組織のために、以下のセキュリティ方針を想定する。

P.SOFTWARE （ソフトウェアの完全性確認）

TOE 内の FlashROM にインストールされている 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手段が提供されていること。

4 セキュリティ対策方針

本章では、「3.1 前提条件」、「3.2 脅威」、「3.3 組織のセキュリティ方針」に対する TOE のセキュリティ対策方針と環境のセキュリティ対策方針について記述する。

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.AUDIT **（監査）**

TOE は、セキュリティ機能関連事象を監査ログとして記録し、セキュリティ侵害の事後検出を可能とするための監査ログ読み出し機能を機器管理者だけに提供しなければならない。

O.I&A **（利用者の識別認証）**

TOE は、利用者が TOE のセキュリティ機能を利用するのに先立って識別認証を実施し、認証に成功した利用者には、その利用者が操作権限を有する機能の利用を許可しなければならない。

O. DOC_ACC **（保護資産のアクセス制御）**

TOE は、一般ユーザーに対して、文書データ毎に設定する文書データの許可利用者とその利用者の操作権限に従って、文書データへのアクセスを保証しなければならない。また TOE は、文書管理者に対して D-BOX に蓄積している文書データの削除を許可しなければならない。

O. MANAGE **（セキュリティ管理）**

TOE は、セキュリティ機能のふるまい、TSF データ、セキュリティ属性の管理を、セキュリティが維持できる特定の利用者だけに許可しなければならない。

O.MEM.PROTECT **（メモリ蓄積データの暴露防止）**

TOE は、HDD に蓄積されている文書データを解読が困難な形式にしなければならない。

O. NET.PROTECT **（ネットワーク伝送データの保護）**

TOE は、通信経路上の文書データ、印刷データを盗聴から保護し、改ざんを検知しなければならない。

O.GENUINE　　（MFP 制御ソフトウェアの完全性保護）

TOE は、FlashROM にインストールされている 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を TOE の利用者に提供しなければならない。

O.LINE_PROTECT　（電話回線からの侵入防止）

TOE は、ファクスユニットに接続されている電話回線から TOE への不正なアクセスを防がなければならない。

4.2　環境のセキュリティ対策方針

本章では、環境のセキュリティ対策方針について記述する。

OE.ADMIN　　（信頼できる管理者）

MFP 管理責任者は、信頼のおける人を管理者として選任し、その管理者に対して管理者の役割に応じた教育を実施しなければならない。教育を受けた管理者は、TOE の管理者ガイダンスに明示された一般ユーザーに対するセキュアな運用のための遵守事項を、一般ユーザーに周知徹底するよう指導しなければならない。

OE.SUPERVISOR　（信頼できるスーパーバイザー）

MFP 管理責任者は、信頼のおける人をスーパーバイザーとして選任し、そのスーパーバイザーに対してスーパーバイザーの役割に応じた教育を実施しなければならない。

OE.NETWORK　　（TOE を接続するネットワーク環境）

TOE を接続する内部ネットワークをインターネットなどの外部ネットワークと接続する場合、内部ネットワークを運用管理する組織が、外部ネットワークと内部ネットワーク間の不要なポートを閉じなければならない。（例えば、ファイアウォールの設置）

5 IT セキュリティ要件

5.1 TOE セキュリティ機能要件

本章には、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 セキュリティ機能要件を記載する。[CC]で定義された割付と選択操作を行なった部分は、**[太文字と括弧]**で識別する。
また依存性について、本章では CC で要求する依存性の記述とし、本 ST で満たす依存性については 8.2.3 章に記述する。

5.1.1 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 5 に示す TOE の監査対象事象]**。

機能要件毎に割り付けられた監査対象とすべきアクション(CC における規定)と、それに対応する TOE の監査対象事象を表 5 に記述する。

表 5：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	TOE の監査対象事象
FAU_GEN.1	なし	―
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	監査事象は記録しない
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	監査事象は記録しない
FAU_STG.1	なし	―
FAU_STG.4	a) 基本: 監査格納失敗によってとられるアクション	監査事象は記録しない
FCS_CKM.1	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	<個別に定義した監査対象事象> 1.HDD 暗号鍵生成(結果:成功/失敗)
FCS_COP.1	a) 最小: 成功と失敗及び暗号	<個別に定義した監査対象事象>

機能要件	監査対象とすべきアクション	TOE の監査対象事象
	操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	1.文書データの蓄積の成功 2.文書データの読出しの成功
FDP_ACC.1	なし	―
FDP_ACF.1	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。	<個別に定義した監査対象事象> 1.文書データの蓄積の成功 2.文書データの読出しの成功 3.文書データの削除の成功
FDP_IFC.1	なし	―
FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。	a) 最小 1. ファクス機能:受信
FIA_AFL.1	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	a) 最小 1.ロックアウトの開始 2.ロックアウトの解除
FIA_ATD.1	なし	―
FIA_SOS.1	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	b) 基本 1.一般ユーザー認証情報の新規作成(結果:成功/失敗) 2.一般ユーザー認証情報の変更(結果:成功/失敗) 3.管理者認証情報の変更(結果:成功/失敗) 4.スーパーバイザー認証情報の変更(結果:成功/失敗)
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべて	基本 1.ログイン(結果:成功/失敗)

機能要件	監査対象とすべきアクション	TOE の監査対象事象
	の使用。	
FIA_UAU.7	なし	－
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; 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 1.ログイン（結果：成功/失敗）
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)	b) 基本 1.ログイン（結果：成功/失敗）
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	<個別に定義した監査対象事象> 1.管理者役割の追加、削除 2.文書データ利用者リストの変更
FMT_MSA.3	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	監査事象は記録しない
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	<個別に定義した監査対象事象> 1.一般ユーザー認証情報の新規作成 2.一般ユーザー認証情報の変更 3. 一般ユーザー認証情報の削除 4.管理者認証情報の変更 5.スーパーバイザー認証情報の変更 6.システム時計の日時変更 7.監査ログの全削除
FMT_SMF.1	a) 最小：管理機能の使用	<個別に定義した監査対象事象> 1.管理者役割の追加、削除 2.ロックアウト解除者によるロックアウト解除 3.システム時計の日時変更
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。	a) 最小 1.管理者役割の追加、削除
FPT_RVM.1	なし	－
FPT_SEP.1	なし	－
FPT_STM.1	a) 最小: 時間の変更;	a) 最小 1.システム時計の日時変更

機能要件	監査対象とすべきアクション	TOE の監査対象事象
	b) 詳細: タイムスタンプの提供	
FPT_TST.1	a) 基本: TSF 自己テストの実行とテストの結果。	－
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。	<個別に定義した監査対象事象> 1.高信頼性 IT 製品との通信(結果:成功/失敗、通信先 IP アドレス)
FTP_TRP.1	a) 最小: 高信頼パス機能の失敗。 b) 最小: もし得られれば、すべての高信頼パス失敗に関係する利用者の識別情報。 c) 基本: 高信頼パス機能の使用についてのすべての試み。 d) 基本: もし得られれば、すべての高信頼パス呼出に関係する利用者の識別情報。	<個別に定義した監査対象事象> 1.リモート利用者との通信(結果:成功/失敗)

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

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

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、**[割付:通信先 IP アドレス、他者の利用者認証情報を新規作成/変更/削除した場合の対象者 ID、ロックアウト対象者、ロックアウト解除対象者、ロックアウト解除方法、操作対象文書データ ID]**

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

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、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2　TSF は、監査証跡内の格納された監査記録への不正な改変を**[選択:防止]** 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

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]**を行わねばならない。

5.1.2　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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.1.1　TSF は、以下の**[割付:表 6 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 6 **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 6 **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 6：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のインポート、または
FDP_ITC.2 セキュリティ属性付き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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1　TSF は、**[割付: 表 7 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 7 に示す暗号アルゴリズム]**と暗号鍵長**[割付: 表 7 に示す暗号鍵長]**に従って、**[割付: 表 7 に示す暗号操作]**を実行しなければならない。

表 7：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	- 文書データを HDD に書込む際の暗号化 - 文書データを HDD から読込む際の復号

5.1.3　クラス FDP：利用者データ保護

FDP_ACC.1　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　TSF は、**[割付: 表 8 のサブジェクトとオブジェクト及びサブジェクトとオブジェクト間の操作リスト]**に対して**[割付: MFP 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及びサブジェクトとオブジェクト間の操作リスト

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
管理者プロセス	文書データ	文書データ削除
一般ユーザープロセス	文書データ	文書データ蓄積 文書データ読出し 文書データ編集 文書データ削除

FDP_ACF.1　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 TSF は、以下の**[割付: 表 9 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: MFP 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とセキュリティ属性

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	管理者プロセス	- 管理者 ID - 管理者役割
サブジェクト	一般ユーザープロセス	- 一般ユーザーID - 文書データデフォルトアクセス権リスト
オブジェクト	文書データ	- 文書データ利用者リスト

FDP_ACF.1.2 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 10 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 10：アクセスを管理する規則

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
一般ユーザープロセス	文書データ蓄積	一般ユーザーは、文書データを蓄積をすることができる。文書データが蓄積される際、一般ユーザープロセスに関連付けられた文書データデフォルトアクセス権リストが、蓄積する文書データに関連付けられた文書データ利用者リストにコピーされる。
	文書データ読出し	一般ユーザープロセスに関連付けられた一般ユーザーID と文書データに関連付けられた文書データ利用者リストの文書オーナ ID か文書利用者 ID のいずれかが一致し、一致した ID の操作権限が、閲覧か編集か編集/削除かフルコントロールの場合、その一般ユーザープロセスに対して文書データの読出しが許可される。
	文書データ編集	一般ユーザープロセスに関連付けられた一般ユーザーID と文書データに関連付けられた文書データ利用者リストの文書オーナ ID か文書利用者 ID のいずれかが一致し、一致した ID の操作権限が、編集か編集/削除かフルコントロールの場合、その一般ユーザープロセスに対して文書データの印刷条件の編集を登録することが許可される。

	文書データ削除	一般ユーザープロセスに関連付けられた一般ユーザーID と文書データに関連付けられた文書データ利用者リストの中文書オーナ ID か文書利用者 ID のいずれかが一致し、一致した ID に付与された操作権限が編集/削除かフルコントロールの場合、その一般ユーザープロセスに対して文書データの削除が許可される。

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: **[割付: 表 11 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承認する規則]**。

表 11：アクセスを明示的に管理する規則

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
管理者 プロセス	文書データの削除	管理者プロセスに関連付けられた管理者役割に文書管理者が含まれる場合、管理者プロセスに D-BOX に蓄積されている全ての文書データの削除操作を許可する。

FDP_ACF.1.4 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_IFC.1 サブセット情報フロー制御

下位階層:なし

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 TSF は、**[割付: 表 12 にリストしたサブジェクト、情報、及び操作]に対して[割付: 電話回線情報フローSFP]**を実施しなければならない。

表 12：サブジェクト、情報、及び操作のリスト

サブジェクト	情報	操作
- ファクスユニットのファクスプロセス - コントローラボードのファクス受信プロセス	電話回線から受信したデータ	受渡し

FDP_IFF.1 単純セキュリティ属性

下位階層:なし

依存性: FDP_IFC.1 サブセット情報フロー制御

FMT_MSA.3 静的属性初期化

FDP_IFF.1.1 TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、**[割付: 電話回線情報フローSFP]**を実施しなければならない: **[割付: 表 13 に示すサブジェクトまたは情報と、各々に対応するセキュリティ属性]**。

表 13：サブジェクトまたは情報に対応するセキュリティ属性

種別	サブジェクトまたは情報	セキュリティ属性
サブジェクト	ファクスユニットのファクスプロセス	セキュリティ属性はなし
サブジェクト	コントローラボードのファクス受信プロセス	セキュリティ属性はなし
情報	電話回線から受信したデータ	データ種別

FDP_IFF.1.2　TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: **[割付:電話回線から受信したデータの種別が、ファクスデータの場合、ファクスユニットのファクスプロセスはコントローラボードのファクス受信プロセスに電話回線から受信したデータの通過を許可する。]**。

FDP_IFF.1.3　TSFは、**[割付: 追加の情報フロー制御SFP規則はなし]**を実施しなければならない。

FDP_IFF.1.4　TSF は、以下の**[割付: 追加の SFP 能力のリストなし]**を提供しなければならない。

FDP_IFF.1.5　TSF は、以下の規則に基づいて、情報フローを明示的に承認しなければならない: **[割付: セキュリティ属性に基づいて、明示的に情報フローを承認する規則はなし]**

FDP_IFF.1.6　TSF は、次の規則に基づいて、情報フローを明示的に拒否しなければならない: **[割付: セキュリティ属性に基づいて、明示的に情報フローを拒否する規則はなし]**

5.1.4　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 14 に示す認証事象における、利用者毎の認証失敗累積回数]**に関して、**[選択:「[割付: 1 から 5]内における管理者（詳細化:機器管理者）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 14：認証事象のリスト

認証事象
操作パネルを使用する利用者認証
クライアント PC 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 からファクス送信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に達するか上回ったとき、TSF は、**[割付: 表 15 に示すロックアウト解除アクションのいずれかが取られるまで、認証試行に失敗した利用者をロックアウトする]**をしなければならない。

表 15：ロックアウト解除アクション

ロックアウト解除アクション	内容
オートロックアウト解除	不成功の認証試行が定義した回数に達してから、予め設定されたロックアウト時間（機器管理者が設定する1分から9999分で設定）経過後、ロックアウトになっている利用者の最初の識別認証実施でロックアウトが解除される。なお、機器管理者はロックアウト時間を無期限と設定することもでき、その場合は、時間経過によるロックアウト解除は行われず、他のロックアウト解除操作によってのみ解除でできる。
マニュアルロックアウト解除	機器管理者のロックアウト解除時間の設定値に係わらず、ロックアウトした利用者役割ごとに定められている、ロックアウト解除者の解除操作によって、当該利用者のロックアウトが解除される。ロックアウト対象者とロックアウト解除者の関係については FMT_MTD.1 で規定する。 なお、特別なロックアウト解除操作として、管理者（全管理者役割）およびスーパーバイザーがロックアウトした場合は、TOE の再起動が TOE の再起動がロックアウト解除者による解除操作と同じ効果を持つ。

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**[割付:一般ユーザーID、文書データデフォルトアクセス権リスト、管理者 ID、管理者役割、スーパーバイザーID]**を維持しなければならない。

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:

一般ユーザーの場合

ユーザー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
管理者、スーパーバイザーの場合
ユーザー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:ユーザー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。ユーザー管理者は、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.2　アクション前の利用者認証

下位階層:FIA_UID.1

依存性:　FIA_UID.1 識別のタイミング

FIA_UAU.2.1　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

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:パスワード1文字に対して、ダミー文字(＊:アスタリスク、または●黒丸)を認証フィードバックエリアに表示]**だけを利用者に提供しなければならない。

FIA_UID.2　アクション前の利用者識別

下位階層:FIA_UID.1

依存性:　なし

FIA_UID.2.1　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

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、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:**[割付:一般ユーザーID、文書データデフォルトアクセス権リスト、管理者 ID、管理者役割、スーパーバイザーID]**

FIA_USB.1.2　TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: **[割付:　表　16 にリストした属性の最初の関連付けに関する規則]**

表 16：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
一般ユーザー	一般ユーザープロセス	一般ユーザーID、 文書データデフォルトアクセス権リスト
管理者	管理者プロセス	管理者 ID、 管理者役割
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ID

FIA_USB.1.3　TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: **[割付:管理者は自身に割り当てられた管理者役割を他の管理者に追加することができる。また、自身の管理者役割を削除することができる。ただし、管理者が管理者役割を削除することによって、その管理者役割を持つ管理者がいなくなる場合は削除できない。]**

5.1.5　クラス FMT：セキュリティ管理

FMT_MSA.1　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_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.1.1 TSF は、セキュリティ属性**[割付: 表 17 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、変更、追加]]**をする能力を**[割付: 表 17 の利用者/役割]**に制限するために**[割付: MFP アクセス制御 SFP]**を実施しなければならない。

表 17：セキュリティ属性の管理役割

セキュリティ属性	操作	利用者役割
一般ユーザーID（一般ユーザー情報のデータ項目）	問い合わせ、 新規作成、 削除	- ユーザー管理者
	問い合わせ	- 一般ユーザー
管理者 ID	新規作成	- 管理者
	問い合わせ、 変更	- 当該管理者
	問い合わせ	- スーパーバイザー
管理者役割	問い合わせ、 追加、 削除	- 当該管理者役割を割り当てられている管理者

スーパーバイザーID	問い合わせ、 変更	- スーパーバイザー
文書データ利用者リスト	問い合わせ、 改変	- 文書管理者 - 文書オーナ - 当該文書データに対してフルコントロールの操作権限を持つ一般ユーザー
文書データデフォルトアクセス権リスト(一般ユーザー情報のデータ項目)	問い合わせ、 改変	- ユーザー管理者 - 当該一般ユーザー

FMT_MSA.3　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 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として、**[選択: [割付:表 18 に示す限定的な]]**デフォルト値を与える**[割付: MFP アクセス制御 SFP]**を実施しなければならない。

FMT_MSA.3.2 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指定することを許可しなければならない。

表 18：静的属性初期化の特性

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
一般ユーザーが 蓄積する文書データ	文書データ利用者リスト	予め当該一般ユーザー(文書オーナ)の文書データデフォルトアクセス権リストとして設定された値。この値は、ユーザー管理者または当該一般ユーザーにより任意の設定が可能であり、制限的でも許可的でもなく、限定的な特性を持つ。

FMT_MTD.1　TSF データの管理

下位階層:なし

依存性:　FMT_SMF.1　管理機能の特定

FMT_SMR.1　セキュリティ役割

FMT_MTD.1.1 TSF は、**[割付: 表 19 の TSF データ管理のリスト]を[選択:問い合わせ、改変 、削除、[割付:登録、変更、全削除、新規作成]]**する能力を**[割付: 表 19 の役割]**に制限しなければならない。

表 19：TSF データ管理のリスト

TSF データ	操作	利用者役割
一般ユーザー認証情報（一般ユーザー情報のデータ項目）	新規作成、 変更、 削除	ユーザー管理者
	変更	一般ユーザー情報の当該一般ユーザー
スーパーバイザー認証情報	変更	スーパーバイザー
管理者認証情報	変更	スーパーバイザー、 当該管理者
ログインパスワード入力許容回数	問い合わせ、 改変	機器管理者
ロックアウト解除タイマー設定	問い合わせ、 改変	機器管理者
ロックアウト時間	問い合わせ、 改変	機器管理者
システム時計の日時 年月日設定、時刻（時分秒）設定	問い合わせ、 改変	機器管理者
	問い合わせ、	一般ユーザー、 ユーザー管理者、 ネットワーク管理者、 文書管理者 スーパーバイザー
パスワード最小桁数	問い合わせ、 改変	ユーザー管理者
パスワード複雑度	問い合わせ、 改変	ユーザー管理者
HDD 暗号鍵	問い合わせ、 新規作成	機器管理者
監査ログ	問い合わせ、 全削除	機器管理者
保守機能移行禁止設定	問い合わせ、 改変	機器管理者
	問い合わせ	一般ユーザー、 ユーザー管理者、 ネットワーク管理者、 文書管理者 スーパーバイザー
一般ユーザーのロックアウトフラグ	問い合わせ、 改変	ユーザー管理者
管理者のロックアウトフラグ	問い合わせ、 改変	スーパーバイザー
スーパーバイザーのロックアウトフラグ	問い合わせ、 改変	機器管理者

TSF データ	操作	利用者役割
S/MIME 利用者情報(一般ユーザー情報のデータ項目)	問い合わせ、 新規作成、 削除、 変更	ユーザー管理者、 S/MIME 利用者情報の当該一般ユーザー
	問い合わせ	一般ユーザー
フォルダ配信先情報	問い合わせ	ユーザー管理者 一般ユーザー

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、以下のセキュリティ管理機能を行う能力を持たねばならない:**[割付:表 20 に記述する管理機能の特定のリスト]**。

表 20:管理機能の特定のリスト

機能要件	管理要件	管理項目
FAU_GEN.1	なし	―
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)管理者役割の中の機器管理者の管理
FAU_SAR.2	なし	―
FAU_STG.1	なし	―
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)。	なし:アクションは固定であり、管理対象とならない
FCS_CKM.1	a)暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共有)、有効期間、用途(例えば、デジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし:暗号鍵属性は固定であり、管理対象とならない
FCS_COP.1	なし	―
FDP_ACC.1	なし	―
FDP_ACF.1	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)管理者役割の中の文書管理者の管理
FDP_IFC.1	なし	―
FDP_IFF.1	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) セキュリティ管理機能(機器制御データ管理):機器管理者によるログインパスワード入力許容回数の管理 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操作の管理

FIA_ATD.1	a)もし割付に示されれていれば、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:利用者に対する追加のセキュリティ属性を定義する機能はない
FIA_SOS.1	a)秘密の検証に使用される尺度の管理。	セキュリティ管理機能(機器制御データ管理):ユーザー管理者が機器制御データの次の設定項目を管理 -パスワード最小桁数 -パスワード複雑度
FIA_UAU.2	管理者による認証データの管理: このデータに関係する利用者による認証データの管理。	-セキュリティ管理機能(一般ユーザー情報管理):ユーザー管理者による一般ユーザー認証情報の管理と、一般ユーザーによる本人の一般ユーザー認証情報の管理 -セキュリティ管理機能(管理者情報管理):管理者本人による管理者認証情報の管理 -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(スーパーバイザー情報管理):スーパーバイザーによるスーパーバイザー認証情報の管理
FIA_UAU.7	なし	―
FIA_UID.2	a)利用者識別情報の管理。	-セキュリティ管理機能(一般ユーザー情報管理):ユーザー管理者による一般ユーザーID の管理 -セキュリティ管理機能(管理者情報管理):管理者による自身の管理者 ID 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(スーパーバイザー情報管理):スーパーバイザーによるスーパーバイザーID 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:デフォルトのサブジェクトのセキュリティ属性は定義できない。 b)管理者は、自身に割り当てられている管理者役割を他の管理者に追加できるとともに、管理者役割を削除できる。
FMT_MSA.1	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。	管理者による管理者役割の管理

FMT_MSA.3	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。	a)なし:初期設定を特定できる役割のグループはない b) 文書データデフォルトアクセス権リストの管理 -ユーザー管理者にアドレス帳に登録されている全ての一般ユーザー情報の文書データデフォルトアクセス権リストの改変を許可 -一般ユーザーに自身の一般ユーザー情報の文書データデフォルトアクセス権リストの改変を許可
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。	なし:TSF データと相互に影響を及ぼし得る役割のグループはない
FMT_SMF.1	なし	―
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	管理者による管理者役割の管理
FPT_RVM.1	なし	―
FPT_SEP.1	なし	―
FPT_STM.1	a) 時間の管理。	セキュリティ管理機能(機器制御データ管理):機器管理者が、機器制御データの次の設定項目を管理 -システム時計の年月日、時刻(時、分、秒)
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:TSF 自己テストが動作する条件は固定。 b)なし:時間間隔に管理はない
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設定。	なし:TSF 間高信頼チャネルを要求するアクションは固定であるため
FTP_TRP.1	a) もしサポートされていれば、高信頼パスを要求するアクションの設定。	なし:高信頼パスを要求するアクションは固定であるため

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:一般ユーザー、管理者(機器管理者、文書管理者、ユーザー管理者、ネットワーク管理者)、スーパーバイザー]**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。

5.1.6 クラス FPT：TSF の保護

FPT_RVM.1 TSP の非バイパス性

下位階層:なし

依存性: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

FPT_SEP.1 TSF ドメイン分離

下位階層:なし

依存性: なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

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、それ自身の実行のために、高信頼タイムスタンプを提供できなければならない。

FPT_TST.1 TSF テスト

下位階層:なし

依存性: FPT_AMT.1 抽象マシンテスト

FPT_TST.1.1 TSF は、[選択: [割付:Ic Hdd の暗号化機能]]の正常動作を実証するために、[選択: 初期立ち上げ中]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: HDD 暗号鍵]]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。

5.1.7 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、それ自身とリモート高信頼 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データ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]**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: TOE から SMB サーバーへのフォルダ配信サービス(IPSec)、 TOE から FTP サーバーへのフォルダ配信サービス(IPSec)]**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。

FTP_TRP.1 **高信頼パス**

下位階層:なし

依存性: なし

FTP_TRP.1.1 TSF は、それ自身と**[選択: リモート]**利用者間に、他の通信パス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通信データの保護を提供する通信パスを提供しなければならない。

FTP_TRP.1.2 TSF は、**[選択:TSF、リモート利用者]**が、高信頼パスを介して通信を開始することを許可しなければならない。

FTP_TRP.1.3 TSF は、**[選択: 最初の利用者認証、[割付:TOE の Web サービス、クライアント PC からの印刷サービス、クライアント PC からのファクス送信サービス、TOE からクライアント PC へのメール送信サービス]]**に対して、高信頼パスの使用を要求しなければならない。

FTP_TRP.1.2 に示す高信頼パスを介して通信をする各利用者が使用する、FTP_TRP.1.3 で示された高信頼パスが要求されるサービスを表 21 に記述する。

表 21：高信頼パスが要求されるサービス

通信関係者	高信頼パスが要求されるサービス
TSF	TOE からクライアント PC へのメール送信サービス(S/MIME)
リモート利用者	最初の利用者認証(SSL) クライアント PC からの TOE の Web サービス(SSL) クライアント PC からの印刷サービス(SSL) クライアント PC からのファクス送信サービス(SSL)

5.2 最小機能強度主張

本 TOE の最小機能強度を SOF-基本とする。5.1 章の TOE セキュリティ機能要件のうち、確率的または順列的メカニズムを利用する TOE セキュリティ機能要件は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2 であり、最小機能強度レベルに関連する。本 TOE が満たす FCS_CKM.1 および FCS_COP.1 で特定するアルゴリズムは、各々暗号アルゴリズムであり、その強度は CC の適用範囲外であるため、最小機能強度主張の対象としない。

5.3 TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL3 である。TOE の保証コンポーネントを表 22.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であり、他の要件は追加していない。

表 22: TOE セキュリティ保証要件(EAL3)

保証クラス	保証コンポーネント	
ACM: 構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
ADO: 配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
ADV: 開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
AGD: ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ALC: ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
ATE: テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト:上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テストーサンプル
AVA: 脆弱性評定	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.4 環境に対するセキュリティ要件

環境に対する機能要件はない。

6 TOE 要約仕様

本章では、TOE セキュリティ機能、機能強度の主張、保証手段について記述する。

6.1 TOE セキュリティ機能

TOE は、5.1 章で記述した TOE セキュリティ機能要件を満たすため、以下の TOE セキュリティ機能を提供する。

SF.AUDIT 監査機能

SF.I&A 利用者識別認証機能

SF.DOC_ACC 文書データアクセス制御機能

SF.SEC_MNG セキュリティ管理機能

SF.CE_OPE_LOCK 保守機能移行禁止機能

SF.CIPHER 暗号化機能

SF.NET_PROT ネットワーク通信データ保護機能

SF.FAX_LINE 電話回線 I/F 侵入防止機能

SF.GENUINE MFP 制御ソフトウェア検証機能

これら TOE セキュリティ機能は、5.1 章で記述したセキュリティ機能要件と表 23 の通り対応している。

表 23：TOE セキュリティ機能要件と TOE セキュリティ機能の関連

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.2	X								
FAU_STG.1	X								
FAU_STG.4	X								
FCS_CKM.1						X			
FCS_COP.1						X			
FDP_ACC.1			X						

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FDP_ACF.1			X						
FDP_IFC.1								X	
FDP_IFF.1								X	
FIA_AFL.1		X		X					
FIA_ATD.1		X							
FIA_SOS.1		X							
FIA_UAU.2		X							
FIA_UAU.7		X							
FIA_UID.2		X							
FIA_USB.1		X		X					
FMT_MSA.1				X					
FMT_MSA.3				X					
FMT_MTD.1	X			X	X	X			
FMT_SMF.1		X		X					
FMT_SMR.1		X		X					
FPT_RVM.1	X	X	X	X	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X	X	X	X	X
FPT_STM.1	X								
FPT_TST.1						X			X
FTP_ITC.1							X		
FTP_TRP.1							X		

以下に、これら TOE セキュリティ機能について記述する。

6.1.1 SF.AUDIT 監査機能

TOE は、電源が供給され TOE が起動する時に監査機能を開始し、TOE への電源が断たれるまで稼動を続ける。監査機能が稼動している間は、監査事象発生時に監査ログを記録する。記録した監査ログは、監査前に損失しないよう保護する。監査ログの読出し、および監査ログの全削除は機器管理者だけに許可する。

また TOE は、監査機能が確実に実行されることを保証し、監査機能の外部から監査機能への干渉および改ざんから保護する。

6.1.1.1 監査ログの生成

TOE は、監査事象発生時に監査ログを生成し監査ログファイルへ追加する。監査ログは、共通監査情報と個別監査情報で構成される。共通監査情報は、全ての監査事象で記録するデータ項目で、個別監査情報は、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データ項目である。各監査対象事象に対する監査情報を表 24 に示す。
監査ログを監査ログファイルに追加する際、監査ログファイルに空き領域が無い場合は、監査ログの事象の日時・時刻が最も古い監査ログに上書きする。

表 24：監査事象と監査情報

監査事象	監査ログ	
	共通監査情報	個別監査情報
監査機能の開始(*1)	- 事象の日付・時刻 - 事象の種別（本表の監査事象） - サブジェクト識別情報（*4） - 結果	―
ログイン		―
ロックアウトの開始		ロックアウト対象者
ロックアウトの解除(*2)		ロックアウト解除対象者 解除方法（オートロックアウト解除/マニュアルロックアウト解除）
TOE 起動時のロックアウト解除		―
HDD 暗号鍵生成		―
文書データの蓄積の成功		操作対象文書データ ID
文書データの読出しの成功(*3)		操作対象文書データ ID
文書データの削除の成功		操作対象文書データ ID
ファクス受信		―
利用者パスワードの変更（パスワードの新規作成、削除も含む）		他者の利用者認証情報を新規作成/変更/削除した場合の対象者 ID
管理者役割の削除		―
管理者役割の追加		―
文書データ利用者リストの変更		操作対象文書データ ID
システム時計の日時変更		―
高信頼 IT 製品との通信		通信先 IP アドレス
リモート利用者との通信		―
監査ログの全削除		―

―：個別監査情報はなし

*1：監査機能の開始事象は、TOE の起動事象で代用する。本 TOE では、監査機能の終了事象を記録しない。監査機能の開始と終了は、監査機能が稼動していない状態を監査するものであるが、本

TOE は、TOE の機能が動作している間は監査機能が常に稼動しており、監査機能が稼動していない状態を監査する必要はないため監査機能の終了事象を記録しなくとも監査機能として十分である。

*2：マニュアルロックアウト解除の特別な操作となる TOE の再起動による管理者およびスーパーバイザーのロックアウト解除については、TOE の起動事象で代用する。

*3：文書データの読出しの成功で、操作対象文書データ ID に記録するのは、D-BOX に蓄積している文書データの印刷、メール送信、フォルダ配信、Web サービス機能からのダウンロードが対象となる。

*4：共通監査事象のサブジェクト識別情報には、記録する事象が利用者の操作によって発生した事象の場合は利用者 ID、TOE が発生させた事象の場合は、利用者 ID と重複しないシステムを識別できる ID が設定される。

6.1.1.2 監査ログの読出し

TOE は、機器管理者だけに Web サービス機能から監査ログをテキスト形式で読出すことを許可する。

6.1.1.3 監査ログの保護

TOE は、機器管理者だけに操作パネルと Web サービス機能から監査ログを全削除することを許可する。

6.1.1.4 タイムスタンプ

TOE は、監査ログの事象の日付・時刻に、TOE 内のシステム時間の日時を提供する。

6.1.2 SF.I&A 利用者識別認証機能

TOE は、許可利用者に役割や権限に応じた TOE の操作を許可するため、TOE のセキュリティ機能を利用するに先立って識別認証をする。

また TOE は、利用者識別認証機能が確実に実行されることを保証し、利用者識別認証機能の外部から利用者識別認証機能への干渉および改ざんから保護する。

6.1.2.1 利用者の識別認証

TOE は、操作パネルまたは Web サービス機能から TOE のセキュリティ機能を利用しようとする者に対してログイン画面を表示して利用者 ID とパスワードの入力を要求し、利用者によって入力された利用者 ID とパスワードでが識別認証要求をする。

また TOE は、クライアント PC から、印刷要求あるいはファクス送信要求を受けたときは、クライアント PC から送信される利用者 ID とパスワードで識別認証をする。

TOE は、いずれの識別認証においても、認証に成功した利用者と、その利用者の利用者役割（一般ユーザー、管理者、スーパーバイザー）に応じたプロセス（一般ユーザープロセス、管理者プロセス、スーパーバイザープロセス）を結合し、各プロセスにセキュリティ属性を関連付けて維持する。利用者が一般ユーザーの場合は、一般ユーザーに一般ユーザープロセスを結合し、一般ユーザープロセスに一般ユーザーID と文書データデフォルトアクセス権リストを関連付け維持し、利用者が管理者の場合は、管理者に管理者プ

ロセスを結合し、管理者プロセスに管理者 ID と管理者役割を関連付け維持し、利用者がスーパーバイザーの場合は、スーパーバイザーにスーパーバイザープロセスを結合し、スーパーバイザープロセスにスーパーバイザーID を関連付け維持する。
認証方法は、利用者役割毎に異なる。利用者役割毎の認証方法を表 25 に記述する。

表 25：利用者役割と認証方法

利用者役割	認証方法
一般ユーザー	利用者が TOE に入力した利用者 ID とパスワードが、アドレス帳に登録されている一般ユーザーID とそのパスワードと一致することを確認する。
管理者	利用者が TOE に入力した利用者 ID とパスワードが、TOE に登録されている管理者 ID とそのパスワードと一致することを確認する。
スーパーバイザー	利用者が TOE に入力した利用者 ID とパスワードが、TOE に登録されているスーパーバイザーID とそのパスワードと一致することを確認する。

6.1.2.2 識別認証失敗時のアクション

TOE は、「6.1.2.1 利用者の識別認証」に記した識別認証の失敗回数を利用者 ID 毎にカウントし、失敗回数の累積がログインパスワード入力許容回数に達した利用者をロックアウトし、当該利用者のロックアウトフラグを「有効」にセットする。ログインパスワード入力許容回数は機器管理者が1から 5 回の間で設定する回数である。
また、TOE は、「6.1.2.1 利用者の識別認証」に記した識別認証で認証に成功した場合、認証に成功した利用者の失敗回数の累積をリセットし、0からカウントする。
TOE は、ロックアウトフラグが有効になっている利用者に対し下記2通りうちいずれかのロックアウト解除アクションが取られた時、その利用者のロックアウトフラグを「無効」にセットし、ロックアウトを解除する。

(1) オートロックアウト解除
利用者がロックアウトになった時からロックアウト解除時間経過後の最初の識別認証時にロックアウトを解除する。ロックアウト経過時間は、機器管理者が1分から 9999 分(分単位)の間で設定する時間。なお、機器管理者は、ロックアウト解除時間を無期限に設定することもできる。無期限とした場合は、利用者のロックアウトは、マニュアルロックアウト解除によってのみ解除される。

(2) マニュアルロックアウト解除
表 26 に示す利用者役割毎に決められたロックアウト解除者が Web サービス機能からロックアウト解除することを許可する。なお、特別なロックアウト解除操作として、管理者(全管理者役割)およびスーパーバイザーがロックアウトした場合は、TOE の再起動によって、そのロックアウトが解除される。

表 26：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
一般ユーザー	ユーザー管理者
管理者(全管理者役割)	スーパーバイザー
スーパーバイザー	機器管理者

6.1.2.3 パスワードのフィードバックエリア保護

TOE は、一般ユーザー、管理者、スーパーバイザーが、操作パネルおよびクライアント PC の Web ブラウザから入力するパスワード1文字毎に、伏字(＊:アスタリスク、あるいは●:黒丸)を表示する。

6.1.2.4 パスワードの登録

TOE は、操作パネルと Web サービス機能から一般ユーザー、管理者、スーパーバイザーの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パスワードを登録し、条件に合致しない場合は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:

一般ユーザーの場合
ユーザー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
管理者、スーパーバイザーの場合
ユーザー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:ユーザー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。ユーザー管理者は、パスワード複雑度に複雑度1か複雑度2を設定する。

6.1.3 SF.DOC_ACC 文書データアクセス制御機能

TOE は、利用者による文書データの蓄積、読出し、編集、削除の操作をアクセス制御する。文書データのアクセス制御は、識別認証機能で認証された許可利用者の利用者役割に対して与えられた権限、または利用者毎に与えられた権限に基づいて、アクセス可能な文書データだけを許可利用者が認証された操作パネル、あるいはクライアント PC に表示する。本章では、文書データのアクセス制御を利用者役割毎に記述する。
また TOE は、文書データアクセス制御機能が確実に実行されることを保証し、文書データアクセス制御機能の外部から文書データアクセス制御機能への干渉および改ざんから保護する。

6.1.3.1 一般ユーザーの文書データ操作

TOE は、文書データの蓄積を一般ユーザーに許可し、蓄積されている文書データの読出し、編集、削除の操作を文書データ利用者リストに従って許可する。文書データ利用者リストには、文書データの操作を許可する一般ユーザーの一般ユーザーID と、当該文書データに対するアクセス権が一般ユーザー毎に記録されている。TOE は、一般ユーザープロセスに関連付けられている一般ユーザーID が、文書データ利用者リストに登録されていれば、その一般ユーザーID に与えられたアクセス権の範囲で操作を許可する。

アクセス権とアクセス権に対応する文書データ操作は表 4 に示す。
尚、文書データを蓄積した際の、文書データ利用者リストの値は、表 27 に記述する値とする。

表 27：：文書データ利用者リストの初期値

文書データのタイプ	文書データ利用者リストの初期値
一般ユーザーが蓄積する文書データ	文書データデフォルトアクセス権リスト

6.1.3.2 文書管理者の文書データ操作

TOE は、操作パネルまたは Web サービス機能からログインしている利用者が文書管理者である場合、その利用者に対して文書データを一覧表示し、選択した文書データまたは表示された全ての文書データを全削除することを許可する。

6.1.4 SF.SEC_MNG セキュリティ管理機能

TOE は、「SF.I&A 利用者識別認証機能」で識別認証された利用者の利用者役割に応じたセキュリティ管理機能を提供する。
また TOE は、セキュリティ管理機能が確実に実行されることを保証し、セキュリティ管理機能の外部からセキュリティ管理機能への干渉および改ざんから保護する。

6.1.4.1 文書データ利用者リスト管理

文書データ利用者リスト管理とは、操作パネルまたは Web サービス機能から文書データ利用者リストの操作を特定の利用者だけに許可する機能である。文書データ利用者リストへの操作には、文書オーナの変更、文書オーナのアクセス権変更、文書利用者の新規登録、文書利用者の削除、および文書利用者のアクセス権変更があり、それぞれに操作することを許可される利用者が決められている。文書データ利用者リストへの操作と操作を許可された利用者の関係を表 28 に記述する。

表 28：文書データ利用者リストへの操作と操作可能者

文書データ利用者リストへの操作	操作可能者
文書オーナの変更	- 文書管理者
文書オーナのアクセス権変更	- 文書管理者 - 文書オーナ - フルコントロール権限を持つ一般ユーザー
文書利用者の新規登録	- 文書管理者 - 文書オーナ - フルコントロール権限を持つ一般ユーザー
文書利用者の削除	- 文書管理者 - 文書オーナ - フルコントロール権限を持つ一般ユーザー
文書利用者のアクセス権変更	- 文書管理者

	- 文書オーナ - フルコントロール権限を持つ一般ユーザー

TOE は、ログインしている利用者が文書管理者ならば、全ての文書データ利用者リスト対して文書オーナーの変更、文書オーナのアクセス権変更、文書利用者の新規登録、文書利用者の削除、および文書利用者のアクセス権変更の操作を許可する。
ログインしている利用者が一般ユーザーならば、その一般ユーザーがフルコントロール権限で設定されている文書データ利用者リストに対してだけ、文書オーナのアクセス権変更、文書利用者の新規登録、文書利用者の削除、および文書利用者のアクセス権変更の操作を許可する。ただし、文書オーナは、フルコントロール権限が設定されていなくとも、オーナになっている文書データの文書データ利用者リストを文書オーナのアクセス権変更、文書利用者の新規登録、文書利用者の削除、文書利用者のアクセス権変更することを許可する。

6.1.4.2 管理者情報管理

管理者情報管理は、操作パネルまたは Web サービス機能から管理者情報に関する操作を特定の利用者だけに許可する機能である。
管理者情報には、管理者 ID、管理者認証情報、管理者役割がある。管理者情報の操作には、管理者の新規登録、管理者 ID の変更、管理者認証情報の変更、および管理者役割の追加、削除があり、それぞれ操作を許可される利用者が決められている。管理者情報の操作と、管理者情報の操作を許可される利用者の関係をを表 29 に記述する。

表 29：管理者情報へのアクセス

管理者情報の操作	操作可能者
管理者の新規登録	管理者
管理者 ID の変更	当該管理者
管理者 ID の参照	スーパーバイザー
管理者認証情報の変更	当該管理者、スーパーバイザー
管理者役割の追加	当該管理者役割を持つ管理者
管理者役割の削除	当該管理者役割を持つ管理者 ただし、他に当該管理者役割を持つ管理者がいない場合は不可

TOE は、ログインしている利用者が管理者あるいはスーパーバイザーならば、それぞれに表 29 に記述した操作を許可する。

6.1.4.3 スーパーバイザー情報管理

スーパーバイザー情報管理は、スーパーバイザーID とスーパーバイザー認証情報の変更を、操作パネルまたは Web サービス機能からスーパーバイザーだけに許可する機能である。
TOE は、操作パネルまたはクライアント PC からログインした利用者がスーパーバイザーならば、スーパーバイザーID とスーパーバイザー認証情報を変更することを許可する。

6.1.4.4 一般ユーザー情報管理

一般ユーザー情報管理は、利用者 ID、利用者認証情報、文書データデフォルトアクセス権リストを含む一般ユーザー情報の新規作成、変更、削除の全部または一部操作を操作パネルまたは Web サービス機能から特定の利用者に許可する機能である。
TOE は、操作パネルまたは Web サービス機能からログインしている利用者が、ユーザー管理者、または一般ユーザーならば、その利用者に対して表 30 に記述する操作を許可する。

表 30：一般ユーザー情報に対する許可操作

一般ユーザー情報に対する操作	操作可能者
アドレス帳へ一般ユーザー情報の新規作成	ユーザー管理者
アドレス帳に登録されている一般ユーザー情報の編集（利用者 ID、利用者認証情報、文書データデフォルトアクセス権リスト、S/MIME 利用者情報）	ユーザー管理者
アドレス帳に登録されている一般ユーザー情報の編集（利用者認証情報、文書データデフォルトアクセス権リスト、S/MIME 利用者情報）	一般ユーザー情報の当該一般ユーザー
アドレス帳に登録されている一般ユーザー情報の削除	ユーザー管理者

尚、一般ユーザー情報を新規作成した際の、文書データデフォルトアクセス権リストの値は、新規作成する一般ユーザーID が文書オーナーとして設定され、文書データに許可される操作は文書データの読出しと文書データ利用者リストの改変になる。

6.1.4.5 機器制御データ管理

機器制御データ管理は、機器制御データの設定を特定の利用者だけに許可する機能である。
TOE は、機器制御データを設定する機能を、特定の利用者に特定の箇所から許可する。TOE が許可する機器制御データ毎の設定許可者、設定値の範囲、設定箇所を表 31 に示す。
尚、TOE は、全ての許可利用者にシステム時間の参照を許可し、ユーザー管理者と一般ユーザーにフォルダ配信先情報の参照を許可する。

表 31：機器制御データの管理者リスト

機器制御データ項目	設定値	設定許可者	操作箇所
ログインパスワード入力許容回数	1～5(回)の整数値	機器管理者	Web サービス機能
ロックアウト解除タイマー設定	有効または無効	機器管理者	Web サービス機能
ロックアウト時間	1～9999(分)の整数値	機器管理者	Web サービス機能
パスワード最小桁数	8～32(桁)の整数値	ユーザー管理者	操作パネル
パスワード複雑度	複雑度1または複雑度2	ユーザー管理者	操作パネル
システム時計の日時	年月日、時刻(時、分、	機器管理者	操作パネル

	秒)		Web サービス機能
一般ユーザーのロックアウトフラグ	無効	ユーザー管理者	Web サービス機能
管理者のロックアウトフラグ	無効	スーパーバイザー	Web サービス機能
スーパーバイザーのロックアウトフラグ	無効	機器管理者	Web サービス機能

6.1.5 SF.CE_OPE_LOCK 保守機能移行禁止機能

保守機能移行禁止機能は、機器管理者が設定する保守機能移行禁止設定の設定値に従って、CE の保守機能利用を制御する機能である。
TOE は、操作パネルから保守機能移行禁止設定を設定する機能を機器管理者に提供し、全ての許可利用者に設定値を参照する機能を提供する。保守機能移行禁止設定が「しない」の場合は、CE が保守機能を操作することを許可し、「保守機能移行禁止設定」が「する」の場合は、CE が保守機能を利用することを許可しない。
また TOE は、保守機能移行禁止機能が確実に実行されることを保証し、保守機能移行禁止機能の外部から保守機能移行禁止機能への干渉および改ざんから保護する。

6.1.6 SF.CIPHER 暗号化機能

TOE は、HDD に蓄積する文書データを暗号化する。
また TOE は、暗号化機能が確実に実行されることを保証し、暗号化機能の外部から暗号化機能への干渉および改ざんから保護する。

6.1.6.1 文書データの暗号化

TOE は、HDD に書込む直前にデータを Ic Hdd で暗号化し、HDD から読出した直後にデータを Ic Hdd で復号する。この処理は、HDD に書込み/読出しする全てのデータに対して行われ、文書データも同様に TOE によって暗号化/復号される。
HDD 暗号鍵は、機器管理者が生成する。TOE は、ログインしている利用者が機器管理者の場合、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。
機器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、HDD のデータ書込み/読出しの際には表 32 に示す暗号操作を実施する。

表 32：HDD 蓄積データ暗号操作のリスト

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 へのデータ書込み	暗号化	FIPS197	AES	256 ビット
HDD からのデータ読出し	復号			

HDD 暗号鍵は印刷することもできる。TOE は、ログインしている利用者が機器管理者の場合、HDD 暗号鍵の印刷をするための画面を操作パネルから機器管理者に提供する。印刷した暗号鍵は、TOE 内の暗号鍵

が壊れた場合に、暗号鍵を復旧するために使用する。
またTOEは、起動時にIc Hddの暗号化機能が正常に動作することと、HDD暗号鍵の完全性を検証する。HDD暗号鍵の完全性が確認できなかった場合は、HDD暗号鍵が変更されていることを表示する。

6.1.7 SF.NET_PROT ネットワーク通信データ保護機能

ネットワーク通信データ保護機能は、内部ネットワーク上を流れる文書データ、印刷データを漏洩から保護し、文書データ、印刷データの改ざんを検知する機能である。
また TOE は、ネットワーク通信データ保護機能が確実に実行されることを保証し、ネットワーク通信データ保護機能の外部からネットワーク通信データ保護機能への干渉および改ざんから保護する。

6.1.7.1 クライアント PC からの Web サービス機能利用

TOEは、クライアントPCからWebサービス機能を利用する要求があると、クライアントPCとTOE間を高信頼パスとしてSSLプロトコルで接続する。

6.1.7.2 クライアント PC からの印刷とファクス送信

TOEは、クライアントPCから印刷要求、あるいはファクス送信要求を受信すると、クライアントPCとTOE間を高信頼パスとしてSSLプロトコルで接続する。

6.1.7.3 TOE からのメール送信

TOEは、TOEからクライアントPCに文書データをメール送信する際に、文書データを電子メールに添付し、その電子メールをS/MIME送信する。なお、S/MIME送信先情報は、一般ユーザー情報管理のS/MIME利用者情報として管理され、利用者はこの管理された送信先情報のみを使用してメールする。

6.1.7.4 TOE からのフォルダ配信

TOEは、TOEからSMBサーバー、またはFTPサーバーにフォルダ配信サービスする際、TOEとSMBサーバー間、またはTOEとFTPサーバー間を高信頼チャネルとしてIPSecプロトコルで接続する。なお、フォルダ配信先情報は、予めTOEに機器制御データとして登録管理され、利用者はこの管理された配信先情報のみを使用してフォルダ配信する。

6.1.8 SF.FAX_LINE 電話回線 I/F 侵入防止機能

TOE は、ファクスユニットが電話回線から受信したデータの種別がファクスデータの場合は、受信データをコントローラボードに引渡し、受信したデータの種別がファクスデータ以外の場合は、受信したデータをコントローラボードに渡さず読み捨てる。
またTOEは、電話回線I/F侵入防止機能が確実に実行されることを保証し、電話回線I/F侵入防止機能の外部から電話回線I/F侵入防止機能への干渉および改ざんから保護する。

6.1.9 SF.GENUINE MFP 制御ソフトウェア検証機能

MFP制御ソフトウェア検証機能は、TOE起動時にFlashROMにインストールされている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。

TOE は、TOE 起動時に 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。完全性が確認できた場合は、利用者が TOE を利用できる状態にする。完全性が確認できなかった場合は、MFP 制御ソフトウェアが正規のものでなかったことを表示する。
また TOE は、MFP 制御ソフトウェア検証機能が確実に実行されることを保証し、MFP 制御ソフトウェア検証機能の外部から MFP 制御ソフトウェア検証機能への干渉および改ざんから保護する。

6.2 機能強度の主張

機能強度レベルに関連する確率的または順列的メカニズムによって実現される TOE セキュリティ機能は SF.I&A である。この TOE セキュリティ機能の機能強度レベルは SOF-基本である。

6.3 保証手段

この章では TOE の保証手段を記述する。以下の表 33 に示される保証手段は、5.3 章で記述された TOE セキュリティ保証要件を満たすものである。尚、AGD クラスの保証手段は、販売地域によって、表 33 で分類している[日本語版]、[英語版-1]、[英語版-2]、[英語版-3]のうち、いずれかが TOE に同梱される。

表 33: EAL3 の保証要件と保証手段

保証クラス	保証コンポーネント	保証手段
ACM: 構成管理	ACM_CAP.3	-imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 構成管理書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 構成管理リスト
	ACM_SCP.1	
ADO: 配付と運用	ADO_DEL.1	- Imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 配付手続き書
	ADO_IGS.1	- Imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 設置、生成及び立上げ書
ADV: 開発	ADV_FSP.1	-imagio MP 4000/5000 シリーズ機能設計書
	ADV_HLD.2	-imagio MP 4000/5000 シリーズ上位レベル設計書
	ADV_RCR.1	-imagio MP 4000/5000 シリーズ表現対応書

保証クラス	保証 コンポーネント	保証手段
AGD: ガイダンス文書	AGD_ADM.1	[日本語版] - imagio MP 5000/4000 シリーズ使用説明書<セキュリティー編> (D012-7950) -セキュリティー機能をお使いの方へ (D011-7750A) - imagio MP 5000/4000 シリーズ使用説明書<本機のご利用にあたって> (D012-7750) - IT セキュリティ評価及び認証制度に基づいた設定でお使いになる管理者の方へ (D011-7781) [英語版-1] -9040/9040b/9050/9050b MP 4000/MP 4000B/MP 5000/MP 5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions About This Machine (D012-7753) -9040/9040b/9050/9050b MP 4000/MP 4000B/MP 5000/MP 5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions About This Machine (D012-7757) - Manuals for Administrators Security Reference 9040/9040b/9050/9050b MP 4000/5000/4000B/5000B LD040/LD050/LD040B/LD050B Aficio MP 4000/5000/4000B/5000B(D009-7504A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) -Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7782) -Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7784)

保証クラス	保証 コンポーネント	保証手段
		[英語版-2] - Manuals for Administrators Security Reference MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7512A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7783) [英語版-3] - MP 4000/MP 4000B/MP 5000/MP 5000B MP 4000/MP 4000B/MP 5000/MP 5000B Aficio MP 4000/4000B/5000/5000B MP 4000/MP 4000B/MP 5000/MP 5000B Operating Instructions About This Machine (D012-7755) - Manuals for Administrators Security Reference MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7508A) - Manuals for Administrators Security Reference Supplement 9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B(D011-7790A) - Notes for Administrators: Using this Machine in a CC-Certified Environment (D011-7782)
	AGD_USR.1	[日本語版] -本機をお使いのお客さまへ (D015-7103) -imagio MP 5000/4000 シリーズ使用説明書<こんなときには> (D012-7800) -imagio MP 5000/4000 シリーズ同梱されている使用説明書 (D012-7501) -imagio MP 5000/4000 シリーズクイックガイド (D012-7658) -使用説明書・ドライバー＆ユーティリティー imagio MP 5000/4000(D0097500A)

保証クラス	保証 コンポーネント	保証手段
		[英語版-1] -9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions Troubleshooting (D012-7803) -9040/9040b/9050/9050b MP 4000/4000B/5000/5000B LD040/LD040B/LD050/LD050B Aficio MP 4000/4000B/5000/5000B Operating Instructions Troubleshooting (D012-7807) -Manuals 9040/9040b/9050/9050b MP 4000/MP 5000/MP 4000B/MP 5000B LD040/LD050/LD040B /LD050B Aficio MP 4000/5000/4000B/5000B(D009-7502A) - Notes for Users Back Up/Restore Address Book (D015-7108) - Notes for Users Back Up/Restore Address Book (D015-7105) [英語版-2] -Manuals General Setting Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7510) -Manuals Functions and Network Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/4000B/5000/5000B(D009-7514A) - Notes for Users Back Up/Restore Address Book (D015-7109) [英語版-3] - MP 4000/MP 4000B/MP 5000/MP 5000B MP 4000/MP 4000B/MP 5000/MP 5000B Aficio MP 4000/4000B/5000/5000B MP 4000/MP 4000B/MP 5000/MP 5000B Operating Instructions Troubleshooting (D012-7805) -Manuals MP 4000/5000/4000B/5000B Aficio MP 4000/5000/4000B/5000B(D009-7506A) - Notes for Users Back Up/Restore Address Book (D015-7107)

保証クラス	保証 コンポーネント	保証手段
ALC: ライフサイクル サポート	ALC_DVS.1	- imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 開発セキュリティ -開発セキュリティ 大森事業所 -開発セキュリティ 新横浜事業所 -開発セキュリティ サービス統括センター -開発セキュリティ 御殿場事業所 -開発セキュリティ RME -開発セキュリティ RCA -開発セキュリティ RAI -開発セキュリティ RPL -開発セキュリティ REI -開発セキュリティ 情報のセキュリティ
ATE: テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1	-imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 外部仕様テスト計画書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 外部仕様テスト仕様書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 外部仕様テスト結果報告書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 内部仕様テスト計画書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 内部仕様テスト仕様書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series 内部仕様テスト結果報告書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series テストカバレッジ分析書 -imagio MP 4000/5000 シリーズ, Aficio MP 4000/5000 series テスト深さ分析書
	ATE_IND.2	-TOE
AVA: 脆弱性評定	AVA_MSU.1	- imagio MP 4000/5000, Aficio MP 4000/5000 シリーズ 脆弱性評定書

7 PP 主張

本 ST において適合する PP はない。

8 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠、PP主張根拠について記述する。

8.1 セキュリティ対策方針根拠

本章では、「3.1 前提条件」、「3.2 脅威」、「3.3 組織のセキュリティ方針」に対して、「4.1 TOE のセキュリティ対策方針」または「4.2 環境のセキュリティ対策方針」が少なくとも1つ以上対応していることを表 34 で示す。また、「3.1 前提条件」、「3.2 脅威」、「3.3 組織のセキュリティ方針」に対して十分なセキュリティ対策方針が取れていることを記述する。

表 34：セキュリティ環境とセキュリティ対策方針の関連

TOE セキュリティ環境 / セキュリティ対策方針	A.ADMIN	A.SUPERVISOR	A.NETWORK	T.ILLEGAL_USE	T.UNAUTH_ACCESS	T.ABUSE_SEC_MNG	T.SALVAGE	T.TRANSIT	T.FAX_LINE	P.SOFTWARE
O.AUDIT				X		X	X	X	X	
O.I&A				X	X	X				
O.DOC_ACC					X					
O.MANAGE						X				
O.MEM.PROTECT							X			
O.NET.PROTECT								X		
O.GENUINE										X
O.LINE_PROTECT									X	
OE.ADMIN	X									
OE.SUPERVISOR		X								
OE.NETWORK			X							

A.ADMIN **（管理者の条件）**

A.ADMIN は、管理者は、管理者に課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、一般ユーザーに TOE をセキュアに運用させるものとする。さらに、管理者は、管理者の特権を利

用した悪意持った不正をしないことを前提としている。
OE.ADMIN によって、MFP 管理責任者が信頼のおける人を管理者に選任し、管理者の役割に応じた教育を実施する。教育を受けた管理者は、TOE の管理者ガイダンスに明示された一般ユーザーに対するセキュアな運用のための遵守事項を一般ユーザーに周知徹底するよう指導する。よって A.ADMIN は実現できる。

A.SUPERVISOR　　（スーパーバイザーの条件）

A.SUPERVISOR は、スーパーバイザーが、スーパーバイザーに課せられた作業において TOE をセキュアに運用するための必要な知識を持ち、スーパーバイザーの特権を利用した悪意を持った不正をしないことを前提としている。
OE.SUPERVISOR によって、MFP 管理責任者が信頼をおける人をスーパーバイザー選任し、スーパーバイザーの役割に応じた教育を実施する。よって A. SUPERVISOR は実現できる。

A.NETWORK　　(ネットワークの接続条件)

A.NETWORK は、TOE が接続されるネットワークをインターネットなどの外部ネットワークと接続する場合は、外部ネットワークから内部ネットワーク保護することを前提としている。
OE.NETWORK によって、TOE を接続する内部ネットワークをインターネットなどの外部ネットワークと接続する場合、内部ネットワークを運用管理する組織が、外部ネットワークと内部ネットワークの不要なポートを閉じる。よって、A.NETWORK は実現できる。

T.ILLEGAL_USE　　(TOE の不正利用)

本脅威に対して TOE は、O.I&A によって利用者が TOE のセキュリティ機能を利用するのに先立って識別認証し、認証に成功した許可利用者に対して、その利用者が操作権限を有する機能の利用を許可する。
また、O.AUDIT によって、O.I&A 実施を監査ログとして記録し、機器管理者が O.I&A のセキュリティ侵害の事後検出をするため、監査ログ読出し機能を機器管理者だけに提供する。
従って、TOE は T.ILLEGAL_USE に対抗できる。

T.UNAUTH_ACCESS　　(TOE 内に蓄積されている保護資産へのアクセス違反)

本脅威に対して TOE は、O.I&A によって識別された許可利用者に対して O.DOC_ACC によって許可利用者の役割と許可利用者に割り当てられた文書データのアクセス権に応じて、文書データへのアクセスを許可する。具体的には、許可利用者が一般ユーザーならば、その一般ユーザーに与えられた文書データの操作権限に従って文書データへの操作を許可し、許可利用者が文書管理者ならば D-BOX に蓄積している文書データの削除を許可する。
従って、TOE は T.UNAUTH_ACCESS に対抗できる。

T.ABUSE_SEC_MNG　　(セキュリティ管理機能の不正利用)

本脅威に対して TOE は、O.I&A にて認証に成功した利用者に TOE のセキュリティ機能の使用を許可する。さらに、O.MANAGE によってセキュリティ機能のふるまい、TSF データ、セキュリティ属性の管理を特定の利用者に制限する。また、O.AUDIT によって、O.I&A および O.MANAGE の実施を監査ログとして記録し、機器管理者が O.I&A および O.MANAGE のセキュリティ侵害の事後検出をするため、監査ログ読出し機能を機器管理者だけに提供する。
従って、TOE は T.ABUSE_SEC_MNG に対抗できる。

T.SALVAGE　　(メモリの持ち去り)

本脅威に対して TOE は、O.MEM.PROTECT によって、HDD を TOE 以外の IT 製品に取り付けて文書データを読出して解読することが困難な形式に変換する。また、O.AUDIT によって、O. MEM.PROTECT の実施を監査ログとして記録し、O. MEM.PROTECT が必ず実施されていることを、機器管理者が事後検出するため、監査ログ読出し機能を機器管理者だけに提供する。
従って、TOE は T.SALVAGE に対抗できる。

T.TRANSIT　　(通信経路上の盗聴、改ざん)

本脅威に対して TOE は、O.NET.PROTECT によって、通信経路上の文書データ、印刷データを漏洩から保護し、改ざんを検知する。また O.AUDIT によって、O.NET.PROTECT の実施を監査ログとして記録し、O.NET.PROTECT が実施されたことを、機器管理者が事後確認するため、監査ログ読出し機能を機器管理者だけに提供する。
従って、TOE は T.TRANSIT に対抗できる。

T.FAX_LINE　　(電話回線からの侵入)

本脅威に対して TOE は、O.LINE_PROTECT によってファクスユニットに接続された電話回線から TOE への侵入を防ぐ。また、O.AUDIT によって、O.LINE_PROTECT の実施を監査ログとして記録し、O.LINE_PROTECT 必ず実施されていることを、機器管理者が事後検出するため、監査ログ読出し機能を機器管理者だけに提供する。
従って、TOE は T.FAX_LINE に対抗できる。

P.SOFTWARE　　(ソフトウェアの完全性確認)

本組織のセキュリティ方針に対して TOE は、O.GENUINE によって TOE の利用者が FlashROM にインストールされている MFP 制御ソフトウェアが正規のものであることを確認できる。
従って、TOE は P.SOFTWARE に対抗できる。

8.2　セキュリティ要件根拠

8.2.1　機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 35 に示す。

表 35:セキュリティ対策方針と機能要件の関連

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FAU_GEN.1	X							

FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1					X			
FCS_COP.1					X			
FDP_ACC.1			X					
FDP_ACF.1			X					
FDP_IFC.1								X
FDP_IFF.1								X
FIA_AFL.1		X						
FIA_ATD.1		X						
FIA_SOS.1		X						
FIA_UAU.2		X						
FIA_UAU.7		X						
FIA_UID.2		X						
FIA_USB.1		X						
FMT_MSA.1				X				
FMT_MSA.3				X				
FMT_MTD.1				X				
FMT_SMF.1				X				
FMT_SMR.1				X				
FPT_RVM.1	X	X	X	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X	X	X	X
FPT_STM.1	X							
FPT_TST.1					X		X	
FTP_ITC.1						X		
FTP_TRP.1						X		

表 35 から、TOE セキュリティ機能要件が1つ以上の TOE セキュリティ対策方針対応していることが分かる。次に、TOE セキュリティ対策方針が、表 35 にて対応付けた TOE セキュリティ機能要件によって実現できることを記述する。

O. AUDIT　　監査

以下の a)から e)に、O.AUDIT を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.AUDIT が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) 監査ログを記録する
O.AUDIT 実現するためには、セキュリティ機能の実施を監査ログとして記録する必要がある。
これに対して FAU_GEN.1 は、監査機能の開始と終了、識別認証機能の実施、利用者による保護資産の操作、保護資産の暗号化、および主要な管理機能の実施時に、監査情報を生成する。事象の発生日付・時刻、事象の種別、サブジェクトの識別情報、事象の結果を記録する。

b) 監査機能を提供する
O.AUDIT 実現するためには、監査できる形式の監査ログを機器管理者だけに提供する必要がある。
これに対して、FAU_SAR.1 は、機器管理者が、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、機器管理者以外が監査ログを読出すことを禁止する。

c) 監査ログを保護する
O.AUDIT 実現するためには、監査ログを適切に保護する対策が必要である。
これに対して、FAU_STG.1 は、監査ログを不正な削除から保護し、不正な改ざんを防止する。また、FAU_STG.4 は、監査ログファイルがいっぱいになった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に新しい監査ログを上書きすることで最新の監査ログが損失することを防止する。

d) 信頼できる事象発生時間
O.AUDIT を実現するためには、セキュリティ侵害を適切に管理するために正確な事象発生時間を記録する対策が必要である。
これに対して、FPT_STM.1 は、信頼できるタイムスタンプを提供する。

e) 監査は確実に実行される
O.AUDIT を実現するためには、a)から d)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトからの干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)から d)の対策は確実に実行され、FPT_SEP.1 によってセキュリティドメインと信頼できないサブジェクトは分離される。

O.I&A　　利用者の識別認証

以下の a)から d)に、O.I&A を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.I&A が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) 利用者が TOE を利用する前に利用者の識別認証をする
O.I&A を実現するためには、利用者が TOE のセキュリティ機能を利用するのに先立って、許可利用者であることを識別認証しなければならない。
これに対して FIA_UID.2 は、利用者が TOE のセキュリティ機能を利用する前に利用者の識別を行ない、FIA_UAU.2 は、識別された利用者の認証を行なう。

b) 識別認証が成功した利用者に TOE の利用を許可する
O.I&A を実現するためには、利用者が TOE のセキュリティ機能利用前に実施する認証に成功した場合、その利用者が操作権限を持つ機能の利用を許可しなければならない。
これに対して FIA_ATD.1 と FIA_USB.1 は、識別認証に成功した利用者に対して、その利用者を代行するサブジェクトを結合する。さらに、サブジェクトにセキュリティ属性を関連付け維持する。

c) パスワードの解読を困難にする
O.I&A を実現するためには、利用者認証に使うパスワードを、利用者が入力中に盗み見られたり、簡単に推測されたりすることを防止しなければならない。

これに対して、FIA_UAU.7 は、利用者がパスワードを1文字入力する毎に、認証フィードバックエリアに伏字（＊:アスタリスクまたは●:黒丸）を表示することでパスワードの盗み見を防止し、FIA_SOS.1は、ユーザー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推測が困難なパスワードだけを有効にし、FIA_AFL.1 は、操作パネルからの利用者認証、クライアント PC の Web ブラウザからの利用者認証、クライアント PC から印刷する際の利用者認証、およびクライアントPCからファクス送信する際の利用者認証の失敗回数累計が、機器管理者が設定したログインパスワード入力許容回数に達した利用者をロックアウトすることで、パスワード解読の機会を少なくしている。

d) 識別認証は確実に実行される
O.I&A を実現するためには、a)からc）の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトからの干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)からc）の対策は必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O. DOC_ACC 保護資産のアクセス制御

以下の a)から b）に、O.DOC_ACC を実現するために必要な対策詳細示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.DOC_ACC が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) 文書データへのアクセス制御を規定して実施する
O.DOC_ACC を実現するためには、利用者に結び付けられたサブジェクトの種類と、サブジェクトに関連付けられたセキュリティ属性毎に定められた文書データの操作権限に準じて、各利用者に文書データの操作を許可しなければならない。
これに対して FDP_ACC.1 と FDP_ACF.1 は、管理者プロセスに関連付けられた管理者役割が文書管理者ならば、その管理者プロセスに文書データを削除する操作を許可する。一般ユーザーに対しては、一般ユーザープロセスに対して文書データの蓄積を許可し、さらに一般ユーザープロセスに関連付けられた一般ユーザーID が、各文書データの文書データ利用者リストに登録されていれば、その文書データを操作することを許可する。許可する操作は、文書データ利用者リストに一般ユーザーID毎に設定されているアクセス権に従う。

b) 保護資産へのアクセス制御を確実に実行する
O.DOC_ACC を実現するためには、a)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)の対策が必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O. MANAGE セキュリティ管理

以下の a)から e）に、O.MANAGE を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.MANAGE が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) セキュリティ属性の管理
O.MANAGE を実現するためには、 セキュリティ属性の管理を特定の利用者に限定しなければならな

い。また、セキュリティ属性のひとつである文書データ利用者リストのデフォルト値に限定的な値をセットしなければならない。
これに対してFMT_MSA.1は、一般ユーザーIDの問い合わせ、新規作成、変更をユーザー管理者に許可し、一般ユーザーIDの問い合わせを一般ユーザーに許可し、管理者IDの問い合わせ、新規作成を管理者に許可し、管理者IDの問い合わせ、変更を当該管理者に許可し、管理者IDの問い合わせをスーパーバザーに許可し、管理者役割の問い合わせ、追加、削除を当該管理者役割を持った管理者に許可し、スーパーバイザーID の問い合わせ、変更をスーパーバイザーに許可し、文書データ利用者リストの問い合わせ、改変を文書管理者、文書オーナ、および当該文書データに対してフルコントロールの操作権限を持つ一般ユーザーに許可し、文書データデフォルトアクセス権リストの問い合わせ、改変をユーザー管理者と当該一般ユーザーに許可する。FMT_MSA.3 は、文書データを新規蓄積する際の文書データ利用者リストのデフォルト値を限定的な値に設定する。

b) TSF データの管理と保護
O.MANAGE を実現するためには、TSF データへのアクセスを特定の利用者に限定しなければならない。
これに対して、FMT_MTD.1 は、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、およびスーパーバイザーのロックアウトフラグの問い合わせと設定、システム時計の日時と保守機能移行禁止設定の設定、HDD 暗号鍵の新規作成と問い合わせ、ならびに監査ログの問い合わせと全削除を機器管理者に限定し、システム時計の日時、保守機能移行禁止設定の問い合わせを TOE の許可利用者に許可し、パスワード最小桁数、パスワード複雑度、および一般ユーザーのロックアウトフラグの問い合わせと設定をユーザー管理者に限定し、一般ユーザー認証情報の設定と、S/MIME 利用者情報の新規作成、削除、変更をユーザー管理者と当該一般ユーザーに限定し、S/MIME 利用者情報の問い合わせ、フォルダ配信先情報の問い合わせをユーザー管理者と一般ユーザーに限定し、管理者のロックアウトフラグの問い合わせと設定、スーパーバイザー認証情報の設定をスーパーバイザーに限定し、管理者認証情報の変更をスーパーバイザーと当該管理者に限定する。

c) 管理機能の特定
O.MANAGE を実現するためには、実装する TSF に対して必要なセキュリティ管理機能を実施しなければならない。
これに対して、FMT_SMF.1 は、セキュリティ機能要件に対する必要なセキュリティ管理機能を特定している。

d) セキュリティ管理機能の利用許可
O.MANAGE を実現するためには、セキュリティ管理機能を許可利用者役割に応じてセキュリティ管理機能の利用を許可するため、許可利用者に対してセキュリティ管理の役割と操作権限を関連付け維持しなければならない。
FMT_SMR.1 は、許可利用者に対して一般ユーザー、管理者（ユーザー管理者、機器管理者、文書管理者、ネットワーク管理者）、スーパーバイザーのうちいずれかの役割を関連付け維持する。

e) セキュリティ管理を確実に実行する
O.MANAGE を実現するためには、a)からd)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a) からd)の対策が必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O.MEM.PROTECT メモリ蓄積データの暴露防止

以下の a)から b)に、O.MEM.PROTECT を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O. MEM.PROTECT が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) 適切な暗号鍵生成と暗号操作をする
O.MEM.PROTECT を実現するためには、HDD に蓄積されている文書データが、TOE を利用した正規の手段で読出す以外は、文書データの解読が困難な形式にしなければならない。
これに対して、FCS_CKM.1 は、BSI-AIS31 に基づく暗号鍵生成アルゴリズム TRNG で鍵長 256 ビットの暗号鍵を生成し、FCS_COP.1 は、生成された暗号鍵を使って FIPS197 に合致する暗号アルゴリズム AES で、文書データが HDD に蓄積される時に文書データを暗号化し、文書データが HDD から読出されるときに復号する。さらに、FTP_TST.1 は TOE 起動時に、暗号鍵の正当性のテストと暗号操作をする Ic Hdd の動作テストをテストし、文書データが暗号化されずに HDD に蓄積されることを防ぐ。

b) 暗号化/復号が確実に行われる
O. MEM.PROTECT を実現するためには、a)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)の対策は必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O.NET.PROTECT ネットワーク通信データの保護

以下の a)から b)に、O.NET.PROTECT を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.NET.PROTECT が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) 通信経路の資産を保護
O.NET.PROTECT を実現するためには、通信経路上の文書データまたは印刷データを漏洩から保護し、改ざんを検知しなければならない。
これに対して、FTP_ITC.1 は、TOE と FTP サーバー、および TOE と SMB サーバー間のフォルダ配信において IPSec プロトコルに対応することで、ネットワーク上の文書データに対して漏洩から保護し、改ざんを検知する。また FTP_TRP.1 は、TOE とリモート利用者間に後述する高信頼パスを対応することで、ネットワーク上の文書データに対して漏洩から保護し、改ざんを検知する。TOE からクライアント PC へのメール送信サービスにおいて S/MIME でのメール送信に対応、クライアント PC からの Web サービス利用、クライアント PC からの印刷サービス利用、クライアント PC からのファクス送信サービス利用において SSL プロトコルに対応して、通信経路上の文書データまたは印刷データを漏洩から保護し、改ざんを検知する。

b) ネットワーク通信データの保護が確実に行われる
O.NET.PROTECT を実現するためには、a)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)の対策は必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O.GENUINE　　MFP 制御ソフトウェアの完全性保護

以下の a)から b)に、O.GENUINE を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.GENUINE が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) MFP 制御ソフトウェアの完全性チェック
O.GENUINE を実現するためには、FlashROM にインストールされている MFP 制御ソフトウェアが正規のものであること検証しなければならない。
これに対して、FPT_TST.1 は、TOE の起動時に 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テストし正規のものであることを確認する。

b) MFP 制御ソフトウェアの完全性チェックの確実な実行
O.GENUINE を実現するためには、a)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)の対策は必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

O.LINE_PROTECT　　電話回線からの侵入防止

以下の a)から b)に、O.LINE_PROTECT を実現するために必要な対策詳細を示す。次に、対策詳細に対応するセキュリティ機能要件を明記し、O.LINE_PROTECT が表 35 で対応付けているセキュリティ機能要件で実現する根拠とする。

a) ファクス回線侵入禁止
O.LINE_PROTECT を実現するためには、攻撃者が電話回線を介して TOE へ不正アクセスすることを防止しなければならない。
これに対して、FDP_IFC.1 および FDP_IFF.1 は、ファクスユニットに接続された電話回線から受信したデータの種類がファクスデータのときのみ、ファクスユニットのファクスプロセスからコントローラボードのファクス受信プロセスに受信データを通過させる。

b) ファクス回線侵入禁止の確実な実行
O.LINE_PROTECT を実現するためには、a)の対策がバイパスされず、セキュリティドメインを信頼できないサブジェクトによる干渉と改ざんから保護しなければならない。
これに対して、FPT_RVM.1 によって a)の対策は必ず実行され、FPT_SEP.1 によりセキュリティドメインと信頼できないサブジェクトは分離される。

8.2.2　最小機能強度レベル根拠

本 TOE は、オフィスなど組織の施設内に設置され、外部ネットワークからの脅威から保護された内部ネットワークと電話回線に接続される。よって、TOE の利用を許可されていない者を含めたオフィス内の人物が脅威になりえるエージェントであり、想定される脅威のリスクは低い。よって、攻撃者は低レベルであり、最小機能強度レベルは SOF-基本が妥当である。
本 ST は、TOE に最小機能強度レベルとして SOF-基本を求めており一貫している。
明示された機能強度が指定された機能要件は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2 である。

8.2.3 セキュリティ機能要件の依存性

TOE セキュリティ機能要件について、本 ST での依存性の対応状況を表 36 に示す。

表 36: TOE セキュリティ機能要件の依存性対応表

TOE セキュリティ機能要件	CC が要求する依存性	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_SAR.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_SAR.2	FAU_SAR.1	FAU_SAR.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
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP.1	FCS_CKM.4 FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1	FCS_CKM.4 FMT_MSA.2
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	なし
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	なし
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3	なし
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_ATD.1	なし	なし	なし
FIA_SOS.1	なし	なし	なし
FIA_UAU.2	FIA_UID.1	FIA_UID.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_UID.2	なし	なし	なし
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	なし
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	なし

TOE セキュリティ機能要件	CC が要求する依存性	ST の中で満たしている依存性	ST の中で満たしていない依存性
	FMT_SMR.1	FMT_SMR.1	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	なし
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.2	FIA_UID.1
FPT_RVM.1	なし	なし	なし
FPT_SEP.1	なし	なし	なし
FPT_STM.1	なし	なし	なし
FPT_TST.1	FPT_AMT.1	なし	FPT_AMT.1
FTP_ITC.1	なし	なし	なし
FTP_TRP.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 では、HDD 暗号鍵は、Ic Hdd 内の外部からアクセスできない場所に格納される。また、TOE の運用開始時に管理者が生成した後は、暗号鍵の削除は行われず、新たな暗号鍵への上書きによる変更だけが行われる。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。

FMT_MSA.2 への依存性除去理由

本 TOE では、HDD 暗号鍵、鍵タイプや有効期限など、鍵生成時の属性はない。従って、セキュリティ属性の管理の機能要件は不要である。

FIA_UAU.1 への依存性除去理由

FIA_UAU.1 の上位階層である FIA_UAU.2 を採用しているため、FIA_AFL.1、および FIA_UAU.7 から FIA_UAU.1 への依存性は満たされる。

FIA_UID.1 への依存性除去理由

FIA_UID.1 の上位階層である FIA_UID.2 を採用しているため、FIA_UAU.2、および FMR_SMR.1 から FIA_UID.1 への依存性は満たされる。

FPT_AMT.1 への依存性除去理由

TOE はハードウェア、ソフトウェア両方を含んでおり、TSF が動作するために依存する TOE 外のハードウェアやファームウェアは存在しない。このため、FPT_AMT.1 による抽象マシンテストは不要である。

8.2.4 保証要件根拠

本 TOE は市販製品である MFP である。MFP は一般的なオフィスで使用されることを想定しており、本 TOE は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、上位レベル設計の評価(ADV_HLD.2)は市販製品の正当性を示すのに十分である。さらに、TSF を回避あるいは改ざん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明白な脆弱性の分析(AVA_VLA.1)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。

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 が妥当である。

8.2.5 セキュリティ要件の相互サポート

セキュリティ要件の相互サポートの関係を表 37 に示す。

表 37: セキュリティ要件の相互サポート

機能要件	バイパス防止	非活性化防止	改ざん防止	無効化検知
FAU_GEN.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_SAR.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FAU_SAR.2	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_STG.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FAU_STG.4	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FCS_CKM.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FCS_COP.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FDP_ACC.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FDP_ACF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FDP_IFC.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FDP_IFF.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_AFL.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_ATD.1	N/A	N/A	FPT_SEP.1	N/A
FIA_SOS.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_UAU.2	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_UAU.7	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FIA_UID.2	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FIA_USB.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FMT_MSA.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MSA.3	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_MTD.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FMT_SMF.1	N/A	N/A	FPT_SEP.1	FAU_GEN.1

機能要件	バイパス防止	非活性化防止	改ざん防止	無効化検知
FMT_SMR.1	N/A	N/A	FPT_SEP.1	FAU_GEN.1
FPT_RVM.1	N/A	N/A	FPT_SEP.1	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A
FPT_STM.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FPT_TST.1	FPT_RVM.1	N/A	FPT_SEP.1	N/A
FTP_ITC.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1
FTP_TRP.1	FPT_RVM.1	N/A	FPT_SEP.1	FAU_GEN.1

8.2.5.1 バイパス防止

FAU_GEN.1、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4、FCS_CKM.1、FCS_COP.1、FDP_ACC.1、FDP_ACF.1、FDP_IFC.1、FDP_IFF.1、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7 FIA_UID.2、FIA_USB.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FPT_STM.1、FPT_TST.1、FTP_ITC.1、FTP_TRP.1 は、バイパスされることによってセキュリティ機能が正常に動作しないが、FPT_RVM.1 によって機能が呼び出されバイパスは防止される。
FIA_ATD.1、FMT_SMF.1、および FMT_SMR.1 は、それぞれセキュリティ属性、セキュリティ管理機能、およびセキュリティ役割を定義、列挙する機能要件であり、バイパスする方法が存在しないので、FPT_RVM.1 によるバイパス防止の対象とはならない。

8.2.5.2 非活性化防止

FAU_GEN.1、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4、FCS_CKM.1、FCS_COP.1、FDP_ACC.1、FDP_ACF.1、FDP_IFC.1、FDP_IFF.1、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FIA_USB.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FPT_RVM.1、FPT_SEP.1、FPT_STM.1、FPT_TST.1、FTP_ITC.1、FTP_TRP.1 は常に実施され、停止する手段が提供されないため、非活性化は問題にはならない。
FIA_ATD.1、FMT_SMF.1、および FMT_SMR.1 は、それぞれセキュリティ属性、セキュリティ管理機能、およびセキュリティ役割を定義、列挙する機能要件であり、非活性化は問題にならない。

8.2.5.3 改ざん防止

FPT_SEP.1 によりセキュリティドメインを分離および維持することで、信頼できないサブジェクトによる干渉を防止しているため、TOE セキュリティ機能要件は改ざんから保護される。

8.2.5.4 無効化検出

各セキュリティ機能に対し、表 37 の「無効化検知」の列に FAU_GEN.1 とマークしたセキュリティ機能の使用を監査対象事象とした監査ログが生成される。これによりセキュリティ機能の動作状況に関する事後分析を可能とする。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能の根拠

この章では、6.1 章で定義された TOE セキュリティ機能が、5.1 章で指定された TOE セキュリティ機能要件を実現することを以下に実証する。
まず、表 23 に示すように、TOE セキュリティ機能が1つ以上の TOE セキュリティ機能要件に対応する。次に、各セキュリティ機能要件が、表 23 対応する TOE セキュリティ機能により実現できることを記述する。

FAU_GEN.1（監査データ生成）

FAU_GEN.1 は、監査ログを記録すべき TOE の監査対象事象と、監査対象事象発生時に記録する監査情報について要求している。
SF.AUDIT は、表 24 に示す通り FAU_GEN.1 で要求する監査対象事象発生時に、FAU_GEN.1 で要求する監査情報を監査ログとして生成し記録することを保証している。FAU_GEN.1 では、監査機能の開始と終了を記録することを要求しているのに対して、SF.AUDIT では監査機能の開始は TOE の起動事象で代用し、監査機能の終了は記録しないとしている。監査機能の開始を TOE の起動事象で代用することについては、監査機能は TOE の起動と同じ条件で開始されるため代用できると言える。また、監査機能の終了を記録しないことについては、監査機能の開始と終了を記録するのは、監査機能が動作していない状態を監査するためであるが、本 TOE の監査機能は、TOE へ電源投入した時に起動し、TOE への電源が断たれるまで稼動し続ける。また、TOE への電源供給が断たれている間（監査機能が非稼動の間）、TOE の全ての機能は動作しない。よって、TOE が記録すべき監査事象が発生する状態にある間は、本 TOE の監査機能は必ず動作していることになり、本 TOE は監査機能の動作していない状態を監査する必要はないと言える。以上より、SF.AUDIT は、監査機能の終了を記録しなくとも監査機能として十分である。TOE 起動時のロックアウト解除事象においては、TOE 起動事にロックアウトフラグが有効になっている管理者およびスーパーバイザーのロックアウトを必ず解除するため TOE の起動事象で TOE 起動時のロックアウト解除事象を代行できる。文書データの暗号化/復号の監査事象を、それぞれ文書データの蓄積の成功事象/文書データの読出しの成功事象としているのは、TOE の機構上、文書データを蓄積する時は必ず文書データを暗号化し、文書データを読出す時は必ず文書データを復号し、さらに蓄積に失敗した時は文書データを HDD 上に書込むことは無く、読出しに失敗した時は文書データを解読できる状態にはしなためである。文書データの読出しの成功で、個別監査情報となる操作対象文書データ ID の記録対象を D-BOX に蓄積している文書データの印刷、メール送信、フォルダ配信、Web サービス機能からのダウンロードに限定し、D-BOX に蓄積している文書データのファクス送信は含めていない。D-BOX に蓄積している文書データのファクス送信は、送信操作時の操作対象文書データ ID 情報がなくても、機器管理者が D-BOX に蓄積している文書データのうち、ファクス送信対象となった文書データを他の監査ログ情報から特定または限定でき、それら情報に基づいて、ファクス送信操作者とファクス送信対象文書の送信是非を監査できるためである。
従って、SF.AUDIT の実装によって FAU_GEN.1 は実現できる。

FAU_SAR.1（監査レビュー）、FAU_SAR.2（限定監査レビュー）

FAU_SAR.1 は、機器管理者が、検証できる形式の監査ログを読み出せることを要求し、FAU_SAR.2 は、機器管理者以外の利用者が、監査ログの読出しをできないことを要求している。

SF.AUDIT は、テキスト形式の監査ログ読出しを機器管理者だけに許可する。
従って、SF.AUDIT の実装によって FAU_SAR.1 と FAU_SAR.2 は実現できる。

FAU_STG.1（保護された監査証跡格納）

FAU_STG.1 は、監査ログを不正な削除から保護し、不正な改変を防止することを要求している。
SF.AUDIT は、監査ログの削除を機器管理者のみに許可する。監査ログの改変については、監査ログの改変するためのインターフェースが無いため不正な監査ログの改変はない。監査ログを削除できる機器管理者は、管理者の特権を利用した悪意を持った不正をしない。よって監査ログは不正な削除と改変から保護される。
従って、SF.AUDIT の実装によって FAU_STG.1 は実現できる。

FAU_STG.4（監査データ喪失の防止）

FAU_STG.4 は、最新の監査ログを失わないよう、監査ログファイルの領域が一杯になった場合に、最も古い監査ログに上書きすることを要求している。
SF.AUDIT 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、最新の監査ログを最も古い監査ログに上書きする。
従って、SF.AUDIT の実装によって FAU_STG.4 は実現できる。

FCS_CKM.1（暗号鍵生成）

FCS_CKM.1 は、HDD 暗号鍵の生成について、標準、暗号鍵生成アルゴリズム、暗号鍵長の条件を要求している。
SF.CIPHER は、文書データを HDD 蓄積/読出しする際に、文書データを暗号化/復号するための HDD 暗号鍵を、BSI-AIS31 に準拠した暗号鍵生成アルゴリズム TRNG によって鍵長 256 ビットで生成する。また HDD 暗号鍵の生成標準、暗号鍵生成アルゴリズム、暗号鍵長は、FCS_CKM.1 の要件に合致する。
従って、SF.CIPHER の実装によって FCS_CKM.1 は実現できる。

FCS_COP.1（暗号操作）

FCS_COP.1 は、HDD 暗号鍵の暗号操作の標準、暗号アルゴリズム、暗号鍵長の条件を要求している。
SF.CIPHER は、文書データを HDD 蓄積/読出しする際の文書データ暗号化/復号は、暗号鍵長が 256 ビットの暗号鍵を使って、FIPS 197 に基づいた AES 暗号アルゴリズムで暗号化/復号する。これは、FCS_COP.1 の要件に合致する。
従って、SF.CIPHER の実装によって FCS_COP.1 は実現できる。

FDP_ACC.1（サブセットアクセス制御）、FDP_ACF.1（セキュリティ属性によるアクセス制御）

FDP_ACC.1 は、文書データの蓄積、読出し、編集、削除ができる利用者役割と、各利用者役割に許可される操作の関係を表 8 に示す通り定義し、FDP_ACF.1 は、文書データ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 9、表 10、表 11 に示す通り規定する。
SF.DOC_ACC は、文書管理者に対して文書データの削除を許可し、一般ユーザーに対して文書データ毎に保持する文書データ利用者リストに従って文書データの蓄積、読出し、編集、削除の操作を許可する。
従って、SF.DOC_ACC の実装によって FDP_ACC.1 と FDP_ACF.1 は実現できる。

FDP_IFC.1（サブセット情報制御フロー）、FDP_IFF.1（単純セキュリティ属性）

FDP_IFC.1 と FDP_IFF.1 は、電話回線からファクスユニットのファクスプロセスがデータを受信した時、電話回線情報フローSFP を実施し、ファクスユニットのプロセスは受信したデータの種別がファクスデータの場合、そのデータをコントローラボードのファクス受信プロセスに引き渡すことを要求している。
SF.FAX_LINE は、ファクスユニットが電話回線から受信したデータの種別がファクスデータの場合はコントローラボードに引渡し、ファクスデータ以外の場合は受信したデータをコントローラボードに渡さず読み捨てる。
従って、SF.FAX_LINE の実装によって FDP_IFC.1 と FDP_IFC.1 は実現できる。

FIA_AFL.1(認証失敗時の取り扱い)

FIA_AFL.1 は、表 14 に記す認証事象での利用者認証失敗回数の累積が、機器管理者が設定したログインパスワード入力許容回数に達した利用者を検知し、表 15 に記すロックアウト解除アクションが取られるまで、その利用者をロックアウトすることを要求している。
SF.I&A は、「6.1.2.2 識別認証失敗時のアクション」に示す通り、表 14 の認証事象に対する利用者認証の失敗回数を利用者 ID 毎にカウントし、失敗回数の累積がログインパスワード入力許容回数に達した場合、その利用者をロックアウトし、当該利用者 ID のロックアウトフラグを有効にする。認証に成功した場合は、認証に成功した利用者 ID の失敗回数の累積を0からカウントしなおす。
ロックアウトの解除については、表 15 で定義されたロックアウト解除アクションのオートロックアウト解除か、マニュアルロックアウト解除のいずれかで行われる。
ログインパスワード入力許容回数は1から5回の値で設定し、ロックアウト時間は1分から9999分、または無期限の値で設定する。ログインパスワード入力許容回数とロックアウト時間は、SF.SEC_MNG によって機器管理者によって管理される。
従って、SF.I&A、SF.SEC_MNG の実装によって FIA_AFL.1 は実現できる。

FIA_ATD.1(利用者属性定義)

FIA_ATD.1 は、一般ユーザーID、文書データデフォルトアクセス権リスト、管理者 ID、管理者役割、スーパーバイザーID を個々の利用者に属するセキュリティ属性として維持することを要求する。
SF.I&A は、一般ユーザーには一般ユーザーID と文書データデフォルトアクセス権リストを、管理者には管理者 ID と管理者役割を、スーパーバイザーにはスーパーバイザーID をセキュリティ属性として関連付けて維持する。
従って、SF.I&A の実装によって FIA_ATD.1 は実現できる。

FIA_SOS.1（秘密の検証）

FIA_SOS.1 は、許可された利用者のパスワード品質が以下の内容に合致することを要求する。

- 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)
- 登録可能な桁数:
  一般ユーザーの場合
  ユーザー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

管理者、スーパーバイザーの場合

ユーザー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

・ 規則:ユーザー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。ユーザー管理者は、パスワード複雑度に複雑度1か複雑度2を設定する。

SF.I&A は、上記パスワード品質を満たす場合のみパスワード登録を許可する。
従って、SF.I&A の実装によって FIA_SOS.1 は実現できる。

FIA_UAU.2(アクション前の利用者認証)

FIA_UAU.2 は、利用者が TOE のセキュリティ機能を利用する前に認証に成功すること要求する。
SF.I&A 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 ID と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 Web サービス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 ID とパスワードの入力を要求する画面を表示し、利用者が入力した利用者 ID とパスワードで認証をする。
クライアント PC からの印刷要求あるいはファクス送信要求の場合は、印刷あるいはファクス送信の要求に先立って、クライアント PC から送信される利用者 ID とパスワードで認証をする。
従って、SF.I&A の実装によって FIA_UAU.2 は実現できる。

FIA_UAU.7(保護された認証フィードバック)

FIA_UAU.7 は、TOE の利用者がパスワード入力をしている間、パスワード1文字に対して、1文字の伏字(＊:アスタリスク、または●:黒丸)を認証フィードバックエリアに表示することを要求する。
SF.I&A は、TOE の利用者がパスワードを1文字入力すると、1文字の伏字(＊:アスタリスク、または●:黒丸)を認証フィードバックエリアに表示する。
従って、SF.I&A の実装によって FIA_UAU.7 は実現できる。

FIA_UID.2(アクション前の利用者識別)

FIA_UID.2 は、利用者が TOE のセキュリティ機能を利用する前に識別をすること要求する。
SF.I&A 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 ID と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 Web サービス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 ID とパスワードの入力要求する画面を表示し、利用者が入力した利用者 ID で識別をする。
クライアント PC からの印刷要求あるいはファクス送信要求の場合は、印刷あるいはファクス送信の要求に先立って、クライアント PC から送信される利用者 ID で識別する。
従って、SF.I&A の実装によって FIA_UID.2 は実現できる。

FIA_USB.1(利用者・サブジェクト結合)

FIA_USB.1 は、一般ユーザーを代行する一般ユーザープロセスに一般ユーザーID と文書データデフォルトアクセス権リストを関連付け、管理者を代行する管理者プロセスに管理者 ID と管理者役割を関連付け、スーパーバイザーを代行するスーパーバイザープロセスにスーパーバイザーID を関連付けることを要求する。また、管理者には自身の管理者役割を他の管理者に追加することと、他の管理者が当該管理者役割を持っている場合だけ管理者役割の削除を許可する。
SF.I&A は、認証に成功した利用者が、一般ユーザーならば一般ユーザープロセスと結合し、管理者ならば管理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する。さらに一般ユ

ーザープロセスには一般ユーザーID と文書データデフォルトアクセス権リストを、管理者プロセスには管理者 ID と管理者役割を、スーパーバイザープロセスにはスーパーバイザーID をセキュリティ属性として関連付け維持する。
また、SF.SEC_MNG は、サブジェクト（管理者プロセス）のセキュリティ属性の管理として FIA_USB.1.3 で定義された規則を実施し、管理者が自身の管理者役割を他の管理者に追加することと、他の管理者が当該管理者役割を持っている場合だけ管理者役割を削除することを許可する。
従って、SF.I&A、SF.SEC_MNG によって FIA_USB.1 を実現できる。

FMT_MSA.1（セキュリティ属性の管理）

FMT_MSA.1 は、セキュリティ属性を表 17 の通り管理することを要求する。
SF.SEC_MNG は、アクセス制御 SFP を実施することで、表 17 に記述するセキュリティ属性に対して表 17 に記述する操作を表 17 に記述する利用者役割に許可する。
従って、SF. SEC_MNG の実装によって FMT_MSA.1 は実現できる。

FMT_MSA.3（静的属性初期化）

FMT_MSA.3 は、一般ユーザーが文書データを蓄積する際に、蓄積する文書データの文書データ利用者リストに、文書データを蓄積する一般ユーザーの文書データデフォルトアクセス権リストをデフォルト値としてして設定することと、文書データデフォルトアクセス権リストは、ユーザー管理者と当該一般ユーザーが任意に設定することができる限定的な特性を持つ値であることを要求する。
SF.SEC_MNG は、一般ユーザーが蓄積する文書データが生成されるときに初期設定される文書データアクセス制御リストに対し、MFP アクセス制御 SFP を実施するためのセキュリティ属性のデフォルト値として、表 18 で定義される限定的な値をもつ「文書データデフォルトアクセス権リスト」を当該一般ユーザーのセキュリティ属性として設定する機能を提供する。また、この設定機能はユーザー管理者または当該一般ユーザーのみに限定して提供される。
従って、SF. SEC_MNG の実装によって FMT_MSA.3 は実現できる。

FMT_MTD.1（TSF データの管理）

FMT_MTD.1 は、TSF データへのアクセスを、表 19 に示す通り管理することを要求する。
SF.SEC_MNG、SF.CIPHER、SF.AUDIT、および SF.CE_OPE_LOCK は、表 19 にリストしている TSF データに対して、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。
従って、SF. SEC_MNG、SF.CIPHER、SF.AUDIT、および SF.CE_OPE_LOCK の実装によって FMT_MTD.1 は実現できる。

FMT_SMF.1（管理機能の特定）

FMT_SMF.1 は、表 20 に示す通り、各機能要件を選択した場合に CC 規定によりセキュリティ管理対象とすべき項目と、それに対応する TOE のセキュリティ管理項目について要求する。
SF.SEC_MNG、および SF.I&A は、上述する表 20 のセキュリティ管理項目を提供する。
従って、SF. SEC_MNG、および SF.I&A の実装によって FMT_SMF.1 は実現できる。

FMT_SMR.1（セキュリティ役割）

FMT_SMR.1 は、利用者を TOE に登録する際に、登録する利用者に一般ユーザー、管理者、スーパーバイザーのうちいずれかのセキュリティ役割を設定し、登録された利用者が TOE を利用する際には、各々の

利用者に設定されたセキュリティ役割を関連付け維持することを要求する。
SF.I&A は、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維持する。SF.SEC_MNG は、利用者を TOE に登録する際に、一般ユーザー、管理者、スーパーバイザーの利用者役割を割り付ける。さらに、アドレス帳への一般ユーザー情報の新規作成と、アドレス帳からの一般ユーザー情報の削除をユーザー管理者に限定し、管理者の登録と削除は管理者に限定し、管理者役割の追加、削除は管理者役割を持つ管理者に限定し、スーパーバイザーの変更はスーパーバイザーに限定することで、セキュリティ役割を維持する。
従って、SF.I&A、SF. SEC_MNG の実装によって FMT_SMR.1 は実現できる。

FPT_RVM.1（TSP の非バイパス性）

FPT_RVM.1 は、各機能の動作進行が許可される前に、TSP 実施機能が呼び出され、その成功を保証することを要求する。
SF.AUDIT、SF.I&A、SF.DOC_ACC、SF.SEC_MNG、SF.CE_OPE_LOCK、SF.CIPHER、SF.NET_PROT、SF.FAX_LINE、および SF.GENUINE は、それぞれがバイパスされることなく確実に実行するよう実装されている。
従って、SF.AUDIT 、SF.I&A 、SF.DOC_ACC 、SF.SEC_MNG 、SF.CE_OPE_LOCK 、SF.CIPHER 、SF.NET_PROT、SF.FAX_LINE、および SF.GENUINE の実装によって FPT_RVM.1 は実現できる。

FPT_SEP.1（TSF ドメイン分離）

FPT_SEP.1 は、TSF が自身の実行のために、信頼できないサブジェクトによる干渉と改ざんから自身を保護するためのセキュリティドメインを維持することを要求する。
SF.AUDIT、SF.I&A、SF.DOC_ACC、SF.SEC_MNG、SF_CE_OPE_LOCK、SF.CIPHER、SF.NET_PROT、SF.FAX_LINE、および SF.GENUINE は、信頼できないサブジェクトによる干渉と改ざんから自身を保護する。
従って、SF.AUDIT 、SF.I&A 、SF.DOC_ACC 、SF.SEC_MNG 、SF_CE_OPE_LOCK 、SF.CIPHER 、SF.NET_PROT、SF.FAX_LINE、および SF.GENUINE の実装によって FPT_SEP.1 は実現できる。

FPT_STM.1（高信頼タイムスタンプ）

FPT_STM.1 は、TSF に高信頼タイムスタンプを提供することを要求する。
SF.AUDIT は、監査事象の発生日時を記録するため、システム時計の年月日と時刻を提供する。
従って、SF.AUDIT の実装によって FPT_STM.1 は実現できる。

FPT_TST.1（TSF テスト）

FPT_TST.1 は、TSF を自己テストすることを要求する。
SF.CIPHER は、TOE への電源投入時に Ic Hdd の HDD 暗号化機能の動作と HDD 暗号鍵の完全性のテストをする。
SF.GENUINE は、TOE への電源投入時に MFP 制御ソフトウェアの実行コードの完全性をチェックし、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。
従って、SF.CIPHER 、SF. GENUINE の実装によって FPT_TST.1 は実現できる。

FTP_ITC.1（TSF 間高信頼チャネル）

FTP_ITC.1 は、TSF が IT 製品と通信する際に TSF と IT 製品間に高信頼チャネルを生成することを要求する。
SF.NET_PROT は、フォルダ配信において TOE と FTP サーバー、TOE と SMB サーバー間を高信頼チャネルとして IPSec プロトコルに対応している。
従って、SF.NET_PROT の実装によって FTP_ITC.1 は実現できる。

FTP_TRP.1（高信頼パス）

FTP_TRP.1 は、TSF およびリモート利用者が通信する際に、高信頼パスで通信することを要求する。
SF.NET_PROT は、TOE からクライアント PC へのメール送信サービスにおいて高信頼パスとして S/MIME プロトコルに対応し、クライアント PC からの Web サービス利用、クライアント PC からの印刷サービス利用、クライアント PC からのファクス送信サービス利用においては、高信頼パスとして SSL プロトコルに対応する。
従って、SF.NET_PROT の実装によって FTP_TRP.1 は実現できる。

8.3.2 機能強度主張の根拠

本 TOE において、確率的または順列的メカニズムを含むセキュリティ機能は SF.I&A のパスワードを活用した認証である。これらのセキュリティ機能強度は 6.2 章において SOF-基本を指定している。また、本 TOE の最小機能強度レベルは、5.2 章において SOF-基本を指定している。従って、両者は一貫している。

8.3.3 保証手段の根拠

6.3 章において、EAL3 で必要とされる全てのセキュリティ保証要件に対して、保証手段となる文書および TOE が対応付けられている。また、各文書および TOE によって、セキュリティ保証要件が要求する証拠は網羅されている。従って、TOE セキュリティ保証要件は満たされている。

8.4 PP 主張根拠

本 ST において適合する PP はない。