

SHARP

MX-FRX6

セキュリティターゲット

Version 0.04

シャープ株式会社

履歴

日付	Ver.	変更点	作成	確認	発行
2007/3/9	0.01	• 初版作成	中川	岩崎	久保田
2007/5/16	0.02	• 8.2.1.1 – 8.2.1.5 の各節に内部一貫性の根拠を加筆 • 1.5.2, 2.2.2, 3.1, 4.1, 5.1.1.3, 6.2, 8.1.6, 8.2.1.3, 8.2.2 及び 8.3.1.7 の各節において一部修正	中川	岩崎	久保田
2007/6/27	0.03	• 保証手段の変更を 6.2 節に反映	中川	岩崎	久保田
2007/7/10	0.04	• 2.2.1 節において誤記訂正	中川	岩崎	久保田

目次

1	ST概説.....	6
1.1	ST識別.....	6
1.2	ST概要.....	6
1.3	CC適合.....	6
1.4	参照資料.....	6
1.5	規約、専門用語、略語.....	6
1.5.1	規約.....	6
1.5.2	専門用語.....	7
1.5.3	略語.....	9
2	TOE記述.....	10
2.1	TOEの概要.....	10
2.1.1	TOE種別.....	10
2.1.2	TOEセキュリティ機能の概要.....	10
2.2	TOE構成.....	10
2.2.1	TOEの物理的構成.....	10
2.2.2	TOEの論理的構成.....	10
2.3	MFD機能及び利用方法.....	12
2.3.1	ジョブ機能.....	12
2.3.2	ドキュメントファイリング機能.....	13
2.3.3	ネットワーク管理機能.....	14
2.4	TOEの保護資産.....	14
2.4.1	MFD機能がジョブ処理時に一時保存する実イメージデータ.....	14
2.4.2	利用者が親展ファイルとして保存した実イメージデータ.....	14
2.4.3	ネットワーク関連設定.....	14
3	TOEセキュリティ環境.....	16
3.1	前提条件.....	16
3.2	脅威.....	16
3.3	組織のセキュリティ方針.....	16
4	セキュリティ対策方針.....	17
4.1	TOEのセキュリティ対策方針.....	17
4.2	環境のセキュリティ対策方針.....	17
5	ITセキュリティ要件.....	18
5.1	TOEセキュリティ要件.....	18
5.1.1	TOEセキュリティ機能要件.....	18
5.1.2	TOEセキュリティ保証要件.....	24
5.1.3	最小機能強度.....	24
5.2	IT環境に対するセキュリティ要件.....	25
5.2.1	IT環境に対するセキュリティ機能要件.....	25
5.2.2	IT環境に対するセキュリティ保証要件.....	25

6	TOE要約仕様	26
6.1	TOEセキュリティ機能 (TSF)	26
6.1.1	暗号鍵生成 (TSF_FKG)	26
6.1.2	暗号操作 (TSF_FDE)	26
6.1.3	データ消去 (TSF_FDC)	27
6.1.4	認証 (TSF_AUT)	28
6.1.5	セキュリティ管理者 (TSF_FMT)	28
6.1.6	ネットワーク設定保護 (TSF_NSP)	29
6.1.7	親展ファイル (TSF_FCF)	29
6.2	保証手段	30
6.3	セキュリティ機能強度	31
7	PP主張	32
8	根拠	33
8.1	セキュリティ対策方針根拠	33
8.1.1	T.RECOVER	33
8.1.2	T.SHUNT	33
8.1.3	T.SPOOF	33
8.1.4	A.NETWORK	33
8.1.5	A.OPERATOR	34
8.1.6	A.USER	34
8.2	セキュリティ要件根拠	34
8.2.1	TOEセキュリティ機能要件根拠	34
8.2.2	セキュリティ機能要件の依存性根拠	37
8.2.3	TOEセキュリティ機能要件の相互作用	39
8.2.4	TOEセキュリティ保証要件根拠	40
8.2.5	最小機能強度根拠	40
8.2.6	IT環境に対するセキュリティ要件根拠	40
8.3	TOE要約仕様根拠	40
8.3.1	TOEセキュリティ機能根拠	41
8.3.2	TOE保証手段根拠	45
8.3.3	TOEセキュリティ機能強度根拠	45

表のリスト

表 1.1: 参照資料	7
表 1.2: 専門用語	7
表 1.3: 略語	9
表 3.1: 想定環境	16
表 3.2: TOEに対する脅威	16
表 4.1: TOEのセキュリティ対策方針	17
表 4.2: 環境のセキュリティ対策方針	17
表 5.1: TOEの管理機能	23
表 5.2: 保証要件	24
表 6.1: 機能要件と仕様概要	26
表 6.2: 保証手段	30
表 8.1: セキュリティ対策方針根拠	33
表 8.2: TOEセキュリティ機能要件根拠	34
表 8.3: セキュリティ機能要件の依存性	37
表 8.4: TOEセキュリティ機能要件の相互作用	39
表 8.5: 管理機能の特定と実施	44

図のリスト

図 1: MFDの物理的構成とTOE	10
図 2: TOEの論理的構成図	10
図 3: MFDの利用環境	12

1 ST 概説

1.1 ST 識別

本セキュリティターゲット (ST) 及び CC 評価対象 (TOE) を識別するための情報を記載する。

ST 名称: MX-FRX6 セキュリティターゲット

バージョン: 0.04

作成日: 2007 年 7 月 10 日

作成者: シャープ株式会社

TOE 識別: MX-FRX6 VERSION M.10

CC 識別: CC v2.3 (ISO/IEC 15408:2005), 補足-0512 適用

ST 評価者: みずほ情報総研株式会社 情報セキュリティ評価室

キーワード: シャープ, シャープ株式会社, デジタル複合機, 複合機, Multi Function Printer, MFP, Multi Function Device, MFD, 暗号化, データ暗号化, データ消去

1.2 ST 概要

本 ST は、上記 TOE すなわちシャープ MX-FRX6 について説明したものである。

デジタル複合機 (Multi Function Device, 以下 MFD と略称) は、コピー機能、プリンタ機能、スキャン送信機能、ファクス機能で構成し、販売される事務機械である。本 TOE は、シャープ製 MFD のデータセキュリティ機能を強化するための別売オプション品である。

本 TOE は MFD 内の不揮発性記憶装置 (HDD 等) に書き込まれるイメージデータを不正に取得する試みに対抗することを目的とし、その主なセキュリティ機能は以下の通りである。

- a) イメージデータの暗号化
- b) イメージデータ削除時の上書き消去
- c) 利用者が HDD に保存するイメージデータのパスワード保護

1.3 CC 適合

本書は、以下を満たしている。

- a) CC バージョン 2.3 パート 2 適合。
- b) CC バージョン 2.3 パート 3 適合。
- c) EAL3 適合。
- d) 補足-0512 を適用。
- e) 適合する PP はない。

1.4 参照資料

本書作成について、表 1.1 記載の資料を参照している。本文中 [CC_PART1], [CC_PART2] または [CC_PART3] の参照は、特に断らない限り [CC_INTPR] による修正を含むものとする。

1.5 規約、専門用語、略語

本書記述の規約、専門用語、及び略語を規定する。

1.5.1 規約

本節は、本書記述の規約を述べる。

以下は、特別の意味を持った文章を区別するために使用される規約である。

表 1.1: 参照資料

略称	文書名
[CC_PART1]	情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル 2005年8月 バージョン2.3 CCMB-2005-08-001 (平成17年12月 翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_PART2]	情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 2005年8月 バージョン2.3 CCMB-2005-08-002 (平成17年12月 翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_PART3]	情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 2005年8月 バージョン2.3 CCMB-2005-08-003 (平成17年12月 翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_INTPR]	補足-0512 (Interpretations-0512) 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

a) 単純な斜体 (*italic*) はテキストを強調するために使用される。

以下は CC 機能及び保証コンポーネントに対し、許可された操作の使用を表すために使用される規約である。

b) 割付 (*assignment*) 操作は、コンポーネントにおいて、例えばパスワードの長さのような不確定のパラメータに特定の値を割り付けるために使われる。

- パラメータに割り付ける値を、ブラケット [] 内に示す。値またはその一部としてリストを示す場合、要素間の切れ目は、コンマで区切るか、または、箇条書きスタイルによって示す。
- 複数パラメータのリストに対する割付は、自明な場合を除き、各々の値に対して丸括弧 () 内にパラメータ名を付記する。
- 単一のパラメータに複数の値を割り付ける場合は、自明な場合を除き、各々の値に対して丸括弧 () 内に、各々の値を区別する情報を付記する。

c) 詳細化 (*refinement*) 操作は、コンポーネントに対する詳細付加のために使用され、TOE をさらに限定する。

- 追加のテキストは **太字** で示す。
- 元のテキスト、例えば一般的な用語を、新しいテキスト、例えばより特定の用語で置き換える場合、置き換えられる元のテキストを丸括弧 () に入れ、新しいテキストをその直前に **太字** で示す。
- リスト値は割付操作と同様にして示す。
- 編集上の詳細化 (*editorial refinement*) のために元のテキストを削除する場合、削除するテキストを丸括弧 () に入れる。

d) 選択 (*selection*) 操作は、コンポーネントにおいて与えられた複数の項目から、一つあるいはそれ以上の項目を選択するために使用される。

- 選択された項目を、斜体のブラケット [] 内に [*下線付き斜体*] で示す。

e) 繰返し (*iteration*) 操作は、同一の要件の異なる側面をカバーするために使われる。

- コンポーネントの名称、コンポーネントのラベル、及びエレメントのラベルに対し丸括弧 () 内に一連番号を後置することで、固有識別子とする。

1.5.2 専門用語

本書固有の専門用語を表 1.2 に示す。

表 1.2: 専門用語

用語	定義
イメージデータ	本STでは特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
Webにおける管理者	TOEがリモート操作用に提供するWebで、成功裏に管理者として識別し認証された利用者。

用語	定義
Webにおける管理者パスワード	TOEがリモート操作用に提供するWebで管理者を認証する際に用いられるパスワード。
エンジン	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。プリントエンジン、エンジンユニットともいう。
外部ネットワーク	組織の管理が及ばない、内部ネットワーク以外のネットワーク。
各ジョブ完了後の自動消去	MFD内のMSDに保存された、個々のジョブに対応するイメージデータを上書き消去するための機能。ジョブ完了の際、ジョブ中止の際、及び、ファイリングされたデータが利用者の操作により削除される際に、呼び出される。
管理者	組織の責任者の信頼を得て、TOEを含むMFDを管理する利用者。本利用者はWebにおける管理者あるいは操作パネルにおける管理者として、TOEを操作する。
揮発性	記憶装置に関し、電源を切れれば記憶内容が消失する性質。
基板	プリント基板に部品を半田付け実装したものを指す。
コントローラ基板	MFD全体を制御する基板。TOEのファームウェアを実行するためのマイクロプロセッサ、揮発性RAM、HDD等を有する。
コントローラファームウェア	MFDのコントローラ基板を制御するファームウェア。ROM基板に格納してコントローラ基板に搭載する。
実イメージデータ	イメージデータファイルから管理領域を除いた実イメージデータ部分。
ジョブ	MFD機能（コピー、プリンタ、ダイレクトプリント、スキャン送信、PC-FAX送信、ファクス送信、ファクス受信）において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
親展ファイル	利用者がファイリング保存したデータのうち、他人に無断で再利用されないよう、パスワード（親展ファイルパスワード）によって保護されたもの。
親展ファイルパスワード	親展ファイルを、他人に無断で再利用されないよう、保護するためのパスワード。
親展ファイル保存者	イメージデータを親展ファイルとしてファイリング保存した利用者。
スキャナユニット	原稿をスキャンしてイメージデータを得る装置。コピー、スキャン送信、ファクス送信及びスキャン保存の際に使用する。
スキャン保存	ファイリング機能の一つ。原稿を読み取って得たイメージデータをHDDに保存するが、印刷や送信は実行しない。
スプール	入出力効率のため、ジョブのイメージデータを一時的にMSDに保持すること。
全データエリア消去	MFDが搭載しているすべてのMSDについて、保存されているすべての実イメージデータを上書き消去する処理。
操作パネル	表示部、ボタンキー、タッチパネル上に形成されたボタンを含む、利用者I/Fのためのデバイス。または、そのユニット。
操作パネルにおける管理者	操作パネルで成功裏に管理者として識別し認証された利用者。
操作パネルにおける管理者パスワード	操作パネルで管理者を認証する際に用いられるパスワード。
タンデム印刷	大量の印刷部数を、2台のMFDで折半することにより倍速でこなす機能。
タンデムコピー	MFDのコピー機能におけるタンデム印刷のこと。
電源ON時の自動消去	MFDの電源ON時にMSD上のデータを上書き消去するための機能。管理者による事前の設定に基づき、MFDの電源ON時に呼び出される。
ドキュメントファイリング	MFDが取り扱うイメージデータを、利用者が後で再操作（印刷、送信、等）できるようMFD内のHDDに保存する機能。本STでは、ファイリングとも呼ぶ。
ドキュメントファイリング禁止設定	ジョブの種類別、モード別に、ファイリング保存を禁止する管理機能。親展ファイル以外のファイリング保存を禁止するために使用される。
ドキュメントファイリングデータ消去	HDD上のイメージデータを上書き消去するための機能。管理者の操作により呼び出される。ファイリングされたイメージデータの消去が主な目的だが、スプールされたイメージデータの消去も可能。
内部ネットワーク	組織の内部にあり、外部ネットワークからのセキュリティの脅威に対して保護されたネットワーク。

用語	定義
標準ファームウェア	TOE設置前のMFDに搭載されているコントローラファームウェア。TOEもコントローラファームウェアであり、TOE設置時に標準ファームウェアを取り外す。
ファイリング	ドキュメントファイリングの略。また、ドキュメントファイリング機能によりイメージデータを保存すること。
不揮発性	記憶装置に関し、電源を切っても記憶内容を保持し続ける性質。
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去及び任意部分の再書き込みを可能にしたROM (Flash Memory)。
ホールド	プリンタドライバからのジョブを、ファイリング保存すること。
ホールド以外のプリントジョブ禁止	プリンタドライバからのジョブに対し、その場での印刷出力を禁止する。ホールド指定のないジョブは拒否し、ホールドするジョブは印刷の有無を無視してホールドのみ行う。
保護対象ネットワーク設定データ	MFDのネットワーク関連設定データのうち、本STが保護資産とするもの。具体的内容は2.4.3節で述べる。
未消去データ	コピー、ファクスのジョブについて、ジョブのキャンセルを含み、ジョブの終了前に何らかのトラブルにより、MSD内に残存しているデータ。また、ジョブが正常に終了する前にスプール保存されているデータ。
メモリ	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。
ロック	誤ったパスワードが連続して入力されたとき、パスワードの受付を停止する機能。

1.5.3 略語

本書で使用する略語を表 1.3 に示す。

表 1.3: 略語

略語	定義
AES	Advanced Encryption Standard — 米国の商務省標準技術局 (NIST) が制定した米国政府標準暗号。
EEPROM	Electrically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電氣的に任意部分の書き換えを可能にしたROM。
HDD	Hard Disk Drive (ハード ディスク ドライブ)
I/F	インタフェース (Interface)
LCD	液晶ディスプレイ (Liquid Crystal Display)
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特にMFD内のHDD及びFlashメモリを指す。
NIC	Network Interface Card (ネットワークインタフェースカード) または Network Interface Controller (ネットワークインタフェースコントローラ)
RAM	Random Access Memory — 任意順に読み書き可能なメモリ
ROM	Read Only Memory — 読み出し専用メモリ
UI	User Interface (ユーザーインタフェース)
USB	Universal Serial Bus — IT機器間を接続するシリアルバス標準の名称。
SMTP	Simple Mail Transfer Protocol — E-mail転送用通信プロトコルの名称。
WINS	Windows Internet Name Service — NetBIOS名からIPアドレスを求めるための機能。

2 TOE 記述

2.1 TOE の概要

2.1.1 TOE 種別

TOEはIT製品であり、ROMに格納されたMFD用ファームウェアである。これはMFDの標準ファームウェアを置き換えることにより、セキュリティ機能を提供すると共にMFD全体の制御を行う。

2.1.2 TOE セキュリティ機能の概要

TOEセキュリティ機能は、主として暗号操作機能、データ消去機能、及び、親展ファイル機能からなり、TOEを搭載したMFD内部のイメージデータを不正に取得する試みに対抗することを目的とする。

暗号操作機能は、MFDが扱うイメージデータをMFD内のHDDまたはFlashメモリに書き込む前に暗号化する。データ消去機能は、MFD内のHDDまたはFlashメモリに保存された暗号データの領域に対し、ランダム値または固定値を上書きする。親展ファイル機能は、利用者がHDDにイメージデータをファイリング保存する際、他人が無断で再利用しないよう、パスワードを付して保存することを可能とする。

2.2 TOE 構成

TOEの物理的、論理的構成を本節に記す。

2.2.1 TOE の物理的構成

TOEが動作するMFDは、シャープのMX-M350, MX-M350F, MX-M350N, MX-M350NJ, MX-M350U, MX-M350UJ, MX-M450, MX-M450F, MX-M450N, MX-M450NJ, MX-M450U及びMX-M450UJである。このうち、型名にNを含まないMFDは、HDDを含むシャープ純正オプションを装着することによりTOEが動作する。図1にMFDの物理的構成を示し、TOEを網掛けで示す。TOEの物理的範囲は以下の通り。

- コントローラファームウェア: MFDのコントローラ基板に装着する2枚のROM基板に格納されており、コントローラ基板を制御するファームウェアである。

2.2.2 TOE の論理的構成

TOEの論理的構成を図2に示す。TOEの論理的範囲を太枠で示し、ソフトウェアの機能を長方形で示し、その中のセキュリティ機能を網掛けで示す。TOE外のハードウェアを、角の丸い長方形で示す。また、TOEが保護する利用者データが、TOE外のHDD, Flashメモリ及びEEPROM内に保持されており、これらもまた網掛けで示す。

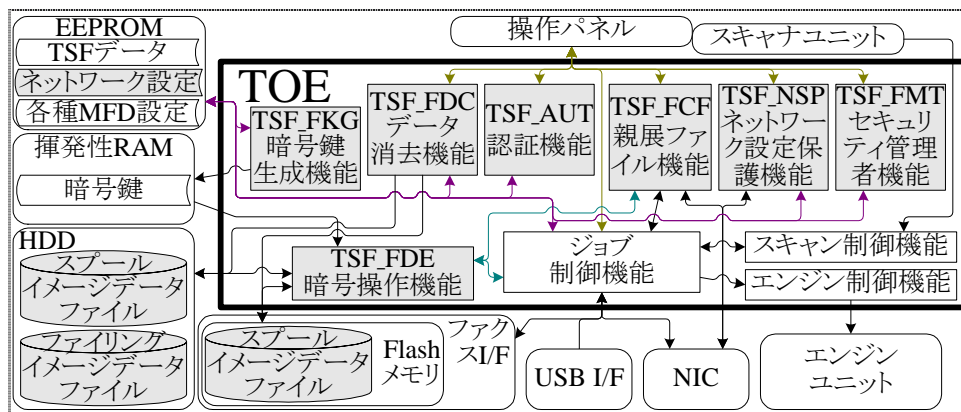


図 2: TOEの論理的構成図

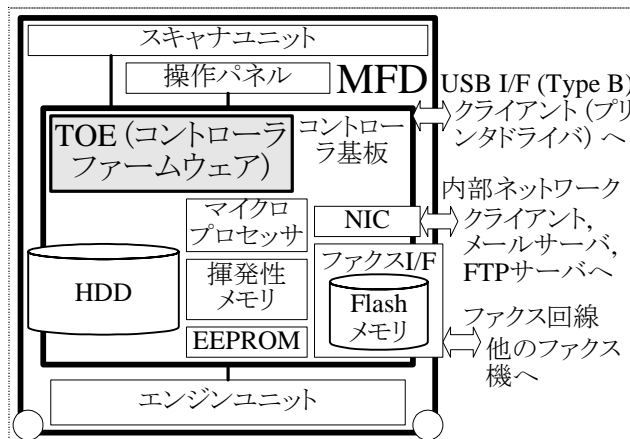


図 1: MFDの物理的構成とTOE

図中、データの流れを矢印で示す。TOE の機能間で受け渡されるデータは、一時的に揮発性メモリを経由するが、セキュリティ機能上の意味を持つ場合を除いて省略している。

TOE は、MFD にセキュリティ機能を追加するアップグレード キットであり、セキュリティ機能を提供すると共に、MFD 全体の制御を行う。以下の機能が TOE の論理的範囲に含まれる。

- a) 暗号操作機能 (TSF_FDE): MFD 内の MSD (HDD 及び Flash メモリ) を制御するデバイスドライバ機能に介在することにより、MSD に書き込む実イメージデータを暗号化し、MSD から読み出した実イメージデータを復号する。
- b) 暗号鍵生成機能 (TSF_FKG): 暗号操作機能 (前項) で提供する暗号化、及び復号の暗号鍵を生成する。生成された暗号鍵は、揮発性 RAM に保存する。
- c) データ消去機能 (TSF_FDC): ジョブ処理のために HDD または Flash メモリ内にスプール保存されたイメージデータがジョブ完了後に削除される際、及び、利用者が親展ファイル機能 (後述) で HDD 内に保存したイメージデータが利用者の操作により削除される際、ランダム値または固定値を上書きすることにより、実イメージデータ領域を消去する (各ジョブ完了後の自動消去)。また、未完のジョブのイメージデータ、及び、利用者が保存したまま削除していないイメージデータに対し、ランダム値または固定値を上書きすることにより、実イメージデータ領域を消去する (全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去)。

以下の 4 種類のデータ消去機能を提供する。

- 各ジョブ完了後の自動消去 (HDD と Flash メモリ): ジョブ完了後、ジョブが使用した実イメージデータ領域に対し、消去を行う。後述の親展ファイル機能により保存された親展ファイルが、利用者の操作により削除される場合も、同様に消去する。
- 全データエリア消去 (HDD と Flash メモリ): 管理者の操作により、残っているすべての実イメージデータ領域に対する消去を行う。TOE もしくは MFD を廃棄または所有者変更する際、管理者は本機能を実行すべきである。
- ドキュメントファイリングデータ消去 (HDD): 管理者の操作により、HDD に残っている実イメージデータに対する消去を行う。主として、利用者が HDD に保存したデータを一括消去するための機能だが、HDD にスプール保存されたジョブのイメージデータを消去することも可能である。なお、全データエリア消去とドキュメントファイリングデータ消去を、データエリア消去 と総称する。
- 電源 ON 時の自動消去 (HDD と Flash メモリ): TOE の電源 ON 時 (スキャン送信またはファクス送信の予約ジョブがある場合、及び、未出力のファクス受信またはインターネット FAX 受信ジョブがある場合を除く) に、実イメージデータ領域に対する消去を行う。管理者は、本機能の有効化または無効化 (電源 ON 時に本機能を実行するか否か) 及び対象領域を設定できる。

d) 認証機能 (TSF_AUT)

操作パネルにおける管理者パスワードにより管理者の識別認証を行う。

e) セキュリティ管理者機能 (TSF_FMT)

TOE の運用に必要な、以下の管理者機能を提供する。

- 各ジョブ完了後の自動消去回数の変更機能
- データエリア消去回数の変更機能
- 電源 ON 時の自動消去の領域別有効設定の変更機能
- 電源 ON 時の自動消去回数の変更機能
- 操作パネルにおける管理者パスワードの変更機能
- 親展ファイルのロック解除機能
- NIC リセット (Web における管理者パスワードを含むネットワーク関連設定を初期化する)

f) ネットワーク設定保護機能 (TSF_NSP)

MFD のネットワーク関連設定を、管理者以外が変更できないよう保護する。

g) 親展ファイル機能 (TSF_FCF)

利用者がドキュメントファイリング機能により MFD 内にイメージデータを保存する際、パスワードによる保護を提供する。本機能によりパスワード保護されファイルとして保存されたイメージデータを、親展フ

ファイルと呼ぶ。利用者は親展ファイル保存時にパスワードを設定し、TOE は再操作 (印刷や送信) の際にパスワードを要求し認証を行う。

本機能は、連続 3 回認証失敗した親展ファイルに対し、認証受付を拒絶する。これをロックと呼ぶ。本機能を利用してプリンタジョブを親展プリントとすることが可能である。

TOE の論理的範囲に含まれる機能のうち、ここまで述べた各機能は TOE に特有の機能である。以下は TOE の論理的範囲に含まれるが、TOE と MFD 標準ファームウェアが共に有する機能である。

h) スキャン制御機能

コピー、スキャン送信、ファクス送信及びスキャン保存の際、原稿を読み取るため、スキャナユニットの制御を行う。

i) エンジン制御機能

コピー、プリンタ、ダイレクトプリント、ファクス受信、及び、再操作の印刷の際、実イメージデータをエンジンユニットに転送し印刷を行わせる。

j) ジョブ制御機能

2.3 節で述べるコピー機能をはじめとする各種 MFD 機能を制御する。

2.3 MFD 機能及び利用方法

MFD 標準ファームウェアと同様に、TOE は MFD 機能、すなわちコピーやファクス等の各機能を持つ。TOE はそれら各 MFD 機能の実行中に TOE セキュリティ機能の一部を自動的に実行する。TOE のこの性質は、TOE セキュリティ機能を知らない、または意識しない利用者をも保護する。TOE を設置する MFD の利用環境を図 3 に示す。

図中の MFD(1) 及び MFD(2) に TOE が設置されているものとする。MFD(1) を対象に、各機能について説明する。

2.3.1 ジョブ機能

MFD 標準ファームウェアと同様に、イメージデータを MFD のスキャナユニットまたは外部から受け取り、MFD 内の MSD にスプールし、イメージデータを MFD のエンジンユニット (印刷) または外部 (送信) へ送る。ジョブ制御機能、スキャン制御機能及びエンジン制御機能により実現される。

2.3.1.1 コピー機能

操作パネルでの操作により、原稿を読み取り、その画像を印刷する。タンデムコピー指示時、管理者が予め指定した MFD にイメージデータを送る。ファイリング指示時、ジョブの保存 (2.3.2 節) を行う。

2.3.1.2 プリンタ機能

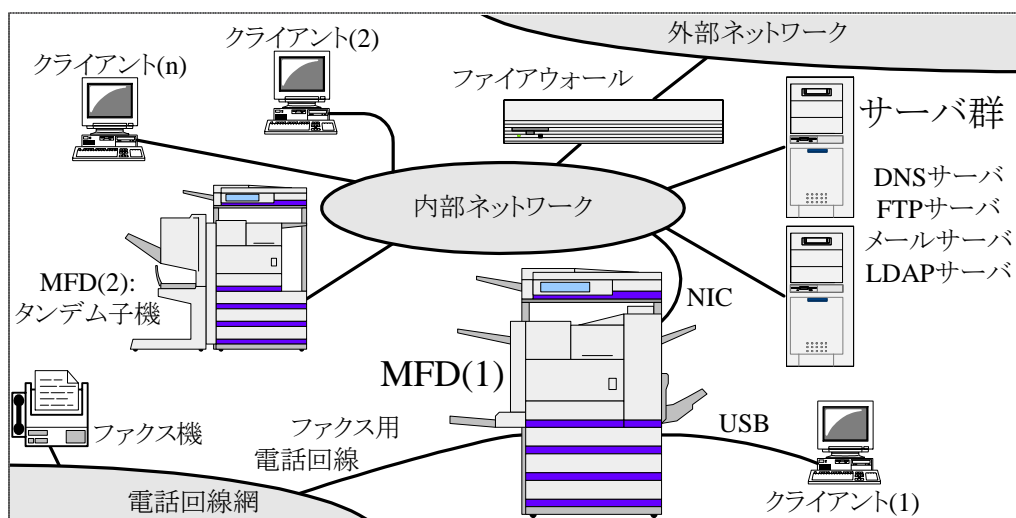


図 3: MFDの利用環境

クライアントから USB または内部ネットワーク経由で送付されてくるプリントデータを印刷する。クライアントには MFD 用のプリンタドライバをインストールしておくべきである。タンデム印刷指示時、管理者が予め指定した MFD にイメージデータを送る。ドキュメントファイリング指示時、ジョブの保存 (2.3.2 節) を行う。印刷せず保存のみ行う指示も可能である。

2.3.1.3 ダイレクトプリント機能

クライアント、FTP サーバまたは E-mail 添付ファイルからプリントデータのファイルを取得し、印刷する。プリンタ機能 (2.3.1.2 節) と異なりプリンタドライバを必要としない。本機能には以下の種類がある。

- E-mail プリント、及び、インターネット FAX 受信: TOE がメールサーバを定期的に確認してメールを受信し、受信したメールに添付されたファイルを印刷する機能。インターネット FAX として送られたメールも同じ仕組みで処理する。
- FTP Pull プリント: 操作パネルからの操作により TOE が FTP サーバにアクセスし、ファイルを取得し印刷する機能。
- FTP Push プリント: TOE が内蔵する FTP サーバに対し、クライアントよりプリントデータを送信することにより印刷する機能。
- Web プリント: TOE が内蔵する Web サーバに対し、クライアントよりプリントデータを送信することにより印刷する機能。

2.3.1.4 スキャン送信機能

原稿を読み取ることによりイメージデータを得て、そのイメージデータを以下の手段により送信する。

- E-mail: E-mail 添付ファイルとしてメールサーバに送る。
- ファイルサーバー: FTP サーバに送る。
- デスクトップ: クライアント (MFD 付属ソフトウェア要) 宛に FTP で送る。
- 共有フォルダ: Windows 共有フォルダに送る。
- インターネット FAX: インターネット FAX 標準仕様に従い E-mail 添付ファイルとしてメールサーバに送る。

2.3.1.5 ファクス送信機能

操作パネルにて指定した送信先ファクス機にファクス送信する。日時を指定して送信を予約すること (時刻指定通信) も可能である。

2.3.1.6 ファクス受信機能

他機よりファクス受信し印刷する。

2.3.1.7 PC-FAX 機能

クライアントから送付されてくるイメージデータを USB または内部ネットワークより受信し、ファクス送信またはインターネット FAX 送信する。クライアントには MFD 用の PC-FAX ドライバをインストールしておくべきである。ドキュメントファイリング指示時、ジョブの保存 (2.3.2 節) を行う。

2.3.2 ドキュメントファイリング機能

MFD 標準ファームウェアと同様、以下の通り MFD 内の HDD にイメージデータを保存し、そのイメージデータを操作パネル経由またはクライアントより Web 経由で再操作できる機能を提供する。ジョブ制御機能により実現される。

- ジョブの保存: 利用者は MFD にコピー等のジョブを与える際、そのジョブのイメージデータを保存するよう指定することができる。
- スキャン保存: 原稿を読み取って保存のみ行い、印刷や送信は行わない。
- 再操作: 保存されたイメージデータを呼び出し、以下の操作を行う。

- 印刷: 保存されたイメージデータを用紙に印刷する。タンデム印刷を指示された際は、管理者が予め指定した MFD にイメージデータを送る。
- 送信: スキャン送信機能における各送信手段のいずれか、または、ファクスにて送信する。
- プレビュー: イメージデータの概略を表示する。
- 属性変更: 親展ファイルパスワードの有無を変更する。
- パスワード変更: 親展ファイルパスワードを変更する。
- 削除: 不要になったイメージデータを取り除き、上書き消去する。
- バックアップ (エクスポート): 後ほどリストア (インポート) 可能なバイナリデータとしてクライアントに転送する。

2.3.3 ネットワーク管理機能

MFD 標準ファームウェアと同様、TOE のネットワーク機能を使用するために、MFD に付与する IP アドレス、TOE が参照すべき DNS サーバの IP アドレス、その他のネットワーク関連設定を行う機能である。

本機能の一部は、操作パネルで管理者に提供される。これは、TOE の管理者設定 UI 内にある **ネットワーク設定** という UI であり、ここで IP アドレス設定等、最低限の設定が可能である。また、タンデム設定は、このネットワーク設定でのみ可能である。

TOE は TCP/IP 使用時に限り、リモート操作用 Web を提供する。この Web が提供するページ群の一部は管理者用であり、パスワードで保護されている。本書ではそれらを **管理者ページ** と総称する。

本機能 (ネットワーク管理機能) の大部分はこの Web で管理者に提供される。ここでは TOE が DNS, WINS, SMTP 及び LDAP サーバを利用するための設定等が可能である。これらの設定を行うための設定フォームを含むページ、及び、それらフォームの送信先ページを、**ネットワーク管理ページ** と総称する。すべてのネットワーク管理ページは管理者ページである。

2.4 TOE の保護資産

本 TOE における保護資産は以下の通り。

- MFD 機能がジョブ処理時に一時保存する実イメージデータ
- 利用者が親展ファイルとして保存した実イメージデータ
- ネットワーク関連設定

各々の具体的内容を以下の各節で記述する。

2.4.1 MFD 機能がジョブ処理時に一時保存する実イメージデータ

利用者が TOE の MFD 機能を使用した場合、利用者が意図することなく TOE 自身が 2.3 節で述べた各種ジョブ処理のために MFD 内の HDD または Flash メモリに一時的にスプール保存した実イメージデータを、本 ST は保護資産とする。これは利用者データであり、利用者の機密情報 (利用者自身が所有する情報や、利用者が顧客から預かっている情報) を含み得る。

2.4.2 利用者が親展ファイルとして保存した実イメージデータ

利用者が MFD 内の HDD 内にパスワードを持つファイル (親展ファイル) として保存した実イメージデータを、本 ST は保護資産とする。これも前項と同様、利用者データであり、利用者の機密情報を含み得る。

2.4.3 ネットワーク関連設定

これは MFD の設定情報のうち、MFD 自身のネットワーク設定 (IP アドレス等)、MFD が利用する外部サーバの各種サービスの利用法設定、及び、タンデム設定であり、TOE を搭載可能な MFD のうち、ネットワーク機能を持つもののみが持つ。本 ST は以下に挙げる設定項目を保護資産とする。

- a) TCP/IP 設定
- b) DNS 設定

- c) WINS 設定
- d) SMTP 設定
- e) LDAP 設定
- f) タンデム設定

これらを本STは保護対象ネットワーク設定データと呼ぶ。これらは管理者がMFDに設定する情報であり、スキャン送信機能、ドキュメントファイリング再操作における送信機能、または、タンデム機能に影響を及ぼし得る。そのため、これらは前各項で述べた実イメージデータの保護に対し、影響を及ぼし得る。

3 TOE セキュリティ環境

本章は TOE セキュリティ環境について述べる。

3.1 前提条件

TOE の使用、運用時に、表 3.1 で詳述する環境が必要となる。

表 3.1: 想定環境

識別子	定義
A.NETWORK	TOEを設置するMFDは、盗聴されないようセキュアに管理された内部ネットワークに接続するものとし、外部ネットワークからの任意のアクセスを認めないよう保護されているものとする。
A.OPERATOR	管理者は、MFD及びTOEに対して不正をせず信頼できるものとする。
A.USER	TOEを設置するMFDの利用者（管理者を含む）は、パスワードを以下のように扱うものとする。 <ul style="list-style-type: none"> • パスワードには容易に推測可能な値を設定しない。 • パスワードは定期的に更新する。 • パスワードは安全に管理する。

3.2 脅威

TOE に対する脅威を表 3.2 に示す。TOE の攻撃者としては、TOE の動作について一般的知識を有し、MFD から物理的に MSD を取り出す技能を有し、簡単に入手することができるハードウェアやソフトウェアのツールを使用して、MSD 内の情報の再生、または不正な入手をはかる者を想定する。

表 3.2: TOE に対する脅威

識別子	定義
T.RECOVER	攻撃者がMFDから物理的にMSDを取り出し、MSD内の実イメージデータを読み出し再生する。
T.SHUNT	攻撃者がMFDのネットワーク関連設定を変更することにより、利用者がMFDに送信させようとしている実イメージデータを、攻撃者が攻撃の手段とする機材へ送信させる。
T.SPOOF	利用者がMFD内に保存している実イメージデータを、攻撃者がその利用者になりすますことにより、印刷または送信する。

3.3 組織のセキュリティ方針

本 ST が想定する組織のセキュリティ方針はない。

4 セキュリティ対策方針

本章は、セキュリティ対策方針における施策について述べる。

4.1 TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 4.1 に示す。

表 4.1: TOE のセキュリティ対策方針

識別子	定義
O.RESIDUAL	MSDにスプール保存またはファイリング保存した実イメージデータは、不要になり次第、上書き消去する。
O.REMOVE	TOEが組込まれているMFDのMSDに対し、MSDへのスプール保存またはファイリング保存を実行したMFD自身以外から読み出されても、イメージとして表示不能なように、MFD固有の暗号鍵で実イメージデータを暗号化してから保存する。
O.MANAGE	TOEのセキュアな運用を維持するためのセキュリティ管理者機能を、操作パネルにおける管理者のみに提供する。
O.NSP	MFDのネットワーク関連設定機能を、操作パネルにおける管理者、及び、Webにおける管理者のみに提供する。
O.UAU	利用者がMFD内にファイリング保存する実イメージデータを、他者から保護するために、利用者認証手段を提供する。

4.2 環境のセキュリティ対策方針

TOE 環境に対するセキュリティ対策方針を表 4.2 に示す。

表 4.2: 環境のセキュリティ対策方針

識別子	定義
OE.BROWSER	TOEのIT環境において、管理者が管理者ページにアクセスする際に使用するWebブラウザ、及び、親展ファイル保存者がMFDに保存された親展ファイルに対して再操作を行う際に使用するWebブラウザは、認証入力機能を提供する。
OE.CIPHER	TOEが設置される内部ネットワーク環境下において、TOEの通信データの盗聴を防止するための保護を実施する。
OE.CLIENT	TOEのIT環境において、TOEにプリンタジョブまたはPC-FAXジョブを送るクライアントは、ファイリング時のパスワードを、TOEにジョブを送る前に指定するための機能を利用者に提供する。
OE.FIREWALL	TOEが設置される内部ネットワークと外部ネットワークの接続は、外部ネットワークからのセキュリティの脅威から内部ネットワークを保護する機能を持った通信機器を用いることにより実施する。
OE.OPERATE	組織の責任者は、管理者の役割に適した者を厳重に人選し、その上で、それぞれの役割を理解させる。
OE.USER	組織の責任者は、管理者に対して、また、管理者は、親展ファイルの利用者に対して、以下の各事項を遵守させる。 <ul style="list-style-type: none"> パスワードには容易に推測可能な値を設定しない。 パスワードは定期的に更新する。 パスワードは安全に管理する。

5 IT セキュリティ要件

5.1 TOE セキュリティ要件

5.1.1 TOE セキュリティ機能要件

本節では TOE セキュリティ機能要件を [CC_PART2] のクラス別に記述する。最小機能強度は、5.1.3 節で規定する。本節に記述するすべての TOE セキュリティ機能要件は [CC_PART2] から抜き出したものであり、拡張要件はない。

5.1.1.1 クラス FCS: 暗号サポート

- FCS_CKM.1 暗号鍵生成
 - 下位階層: なし
 - FCS_CKM.1.1 TSFは、以下の[SHARP標準]に合致する、指定された暗号鍵生成アルゴリズム [MSN-D拡張アルゴリズム]と指定された暗号鍵長[128 ビット]に従って、**毎回の電源ON時に** 暗号鍵を生成しなければならない。
 - 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_COP.1 暗号操作
 - 下位階層: なし
 - FCS_COP.1.1 TSF は、[FIPS PUB 197]に合致する、特定された暗号アルゴリズム[Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[
 - MSD に書き込む前に、未暗号化の実イメージデータ及び親展ファイルのパスワードに対する暗号化
 - MSD から読み込んだ後に、実イメージデータ及び親展ファイルのパスワードの復号
]を実行しなければならない。
 - 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

5.1.1.2 クラス FDP: 利用者データ保護

- FDP_RIP.1 サブセット残存情報保護
 - 下位階層: なし
 - FDP_RIP.1.1 TSFは、以下のオブジェクト[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 **1 回以上の上書き消去によって** 保証しなければならない:[イメージデータファイル]。
 - 依存性: なし

5.1.1.3 クラス FIA: 識別と認証

- FIA_AFL.1(1) 認証失敗時の取り扱い(1)

- 下位階層: なし
- FIA_AFL.1.1(1) TSFは、[操作パネルにおける管理者に対する最後の認証成功以降の不成功認証試行回数]に関して、[[3 (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。
- FIA_AFL.1.2(1) 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、[認証試行 5 分間以上受付停止]をしなければならない。
- 依存性: FIA_UAU.1 認証のタイミング
- FIA_AFL.1(2) 認証失敗時の取り扱い(2)

下位階層: なし

FIA_AFL.1.1(2) TSFは、[Webにおける管理者に対する最後の認証成功以降の不成功認証試行回数]に関して、[[3 (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。

FIA_AFL.1.2(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、[認証試行 5 分間以上受付停止]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング
 - FIA_AFL.1(3) 認証失敗時の取り扱い(3)

下位階層: なし

FIA_AFL.1.1(3) TSFは、[各親展ファイルに対する最後の認証成功以降の不成功認証試行回数]に関して、[[3 (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。

FIA_AFL.1.2(3) 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、[操作パネルにおける管理者により解除されるまで当該親展ファイルのロックすなわち認証試行受付停止]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング
 - FIA_SOS.1(1) 秘密の検証(1)

下位階層: なし

FIA_SOS.1.1(1) TSFは、**操作パネルにおける管理者パスワード (秘密)** が[5 文字の十進数字]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。

依存性: なし
 - FIA_SOS.1(2) 秘密の検証(2)

下位階層: なし

FIA_SOS.1.1(2) TSFは、**Webにおける管理者パスワード (秘密)** が[5 文字以上の英大文字、英小文字、数字、または、英記号]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。

依存性: なし
 - FIA_SOS.1(3) 秘密の検証(3)

下位階層: なし

FIA_SOS.1.1(3) TSFは、**親展ファイルのパスワード (秘密)** が[5 文字の十進数字]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。

- 依存性: なし
- FIA_UAU.2(1) アクション前の利用者認証(1)
 - 下位階層: FIA_UAU.1 認証のタイミング
 - FIA_UAU.2.1(1) TSFは、**操作パネルにおける管理者** (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、**操作パネルにおける管理者** (各利用者) に自分自身を認証することを要求しなければならない。
 - 依存性: FIA_UID.1 識別のタイミング
 - FIA_UAU.2(2) アクション前の利用者認証(2)
 - 下位階層: FIA_UAU.1 認証のタイミング
 - FIA_UAU.2.1(2) TSFは、**Webにおける管理者** (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、**Webにおける管理者** (各利用者) に自分自身を認証することを要求しなければならない。
 - 依存性: FIA_UID.1 識別のタイミング
 - FIA_UAU.2(3) アクション前の利用者認証(3)
 - 下位階層: FIA_UAU.1 認証のタイミング
 - FIA_UAU.2.1(3) TSFは、**親展ファイル保存者** (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、**親展ファイル保存者** (各利用者) に自分自身を認証することを要求しなければならない。
 - 依存性: FIA_UID.1 識別のタイミング
 - FIA_UAU.6 再認証
 - 下位階層: なし
 - FIA_UAU.6.1 TSF は、条件[
 - Web における管理者パスワード変更が許可される前に、Web における管理者は、再認証されなければならない。
]のもとで利用者を再認証しなければならない。
 - 依存性: なし
 - FIA_UAU.7(1) 保護された認証フィードバック(1)
 - 下位階層: なし
 - FIA_UAU.7.1(1) TSF は、認証を行っている間、[入力された文字の個数]だけを利用者に提供しなければならない。
 - 依存性: FIA_UAU.1 認証のタイミング
 - FIA_UID.2(1) アクション前の利用者識別(1)
 - 下位階層: FIA_UID.1 識別のタイミング
 - FIA_UID.2.1(1) TSFは、**操作パネルにおける管理者** (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、**操作パネルにおける管理者** (各利用者) に自分自身を識別することを要求しなければならない。
 - 依存性: なし

- FIA_UID.2(2) アクション前の利用者識別(2)
 下位階層: FIA_UID.1 識別のタイミング
 FIA_UID.2.1(2) TSFは、**Webにおける管理者** (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、**Webにおける管理者** (各利用者) に自分自身を識別することを要求しなければならない。
 依存性: なし

- FIA_UID.2(3) アクション前の利用者識別(3)
 下位階層: FIA_UID.1 識別のタイミング
 FIA_UID.2.1(3) TSFは、**親展ファイル保存者** (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、**親展ファイル保存者** (各利用者) に自分自身を識別することを要求しなければならない。
 依存性: なし

5.1.1.4 クラス FMT: セキュリティ管理

- FMT_MOF.1 セキュリティ機能のふるまいの管理
 下位階層: なし
 FMT_MOF.1.1 TSF は、機能[
 - 全データエリア消去
 - ドキュメントファイリングデータ消去
 - 電源 ON 時の自動消去
] [を停止する] 能力を[操作パネルにおける管理者]に制限しなければならない。
 依存性: FMT_SMF.1 機能管理の特定
 FMT_SMR.1 セキュリティ役割

- FMT_MTD.1(1) TSF データの管理(1)
 下位階層: なし
 FMT_MTD.1.1(1) TSF は、[
 - 各ジョブ完了後の自動消去回数
 - データエリア消去回数
 - 電源 ON 時の自動消去の領域別有効設定
 - 電源 ON 時の自動消去回数
 - 操作パネルにおける管理者パスワード
]を[改変、問合せ] する能力を[操作パネルにおける管理者]に制限しなければならない。
 依存性: FMT_SMF.1 機能管理の特定
 FMT_SMR.1 セキュリティ役割

- FMT_MTD.1(2) TSF データの管理(2)
 下位階層: なし
 FMT_MTD.1.1(2) TSFは、[Webにおける管理者パスワード]を[改変] する能力を[Webにおける管理者]に制限しなければならない。
 依存性: FMT_SMF.1 機能管理の特定

FMT_SMR.1 セキュリティ役割

●FMT_MTD.1(3) TSF データの管理(3)

下位階層: なし

FMT_MTD.1.1(3) TSFは、[親展ファイルのパスワード]を[変更、削除]する能力を[親展ファイル保存者]に制限しなければならない。

依存性: FMT_SMF.1 機能管理の特定
FMT_SMR.1 セキュリティ役割

●FMT_MTD.1(4) TSF データの管理(4)

下位階層: なし

FMT_MTD.1.1(4) TSFは、[Webにおける管理者パスワード]を[[工場出荷時の値へ初期化 (その他の操作)]]する能力を[操作パネルにおける管理者]に制限しなければならない。

依存性: FMT_SMF.1 機能管理の特定
FMT_SMR.1 セキュリティ役割

●FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[表 5.1 に示す管理機能]。

依存性: なし

●FMT_SMR.1(1) セキュリティ役割(1)

下位階層: なし

FMT_SMR.1.1(1) TSF は、役割[操作パネルにおける管理者]を維持しなければならない。

FMT_SMR.1.2(1) TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

●FMT_SMR.1(2) セキュリティ役割(2)

下位階層: なし

FMT_SMR.1.1(2) TSF は、役割[Web における管理者]を維持しなければならない。

FMT_SMR.1.2(2) TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

●FMT_SMR.1(3) セキュリティ役割(3)

下位階層: なし

FMT_SMR.1.1(3) TSF は、役割[親展ファイル保存者]を維持しなければならない。

FMT_SMR.1.2(3) TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.5 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

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

依存性: なし

●FPT_SEP.1 TSFドメイン分離

下位階層: なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と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。

依存性: なし

表 5.1: TOE の管理機能

被管理要件	管理機能	役割
FCS_CKM.1	なし (暗号鍵に管理すべき属性がない)	—
FCS_COP.1	なし (管理要件なし)	—
FDP_RIP.1	<ul style="list-style-type: none"> 各ジョブ完了後の自動消去回数の間合せ及び変更機能 データエリア消去回数の間合せ及び変更機能 電源ON時の自動消去の領域別有効設定の間合せ及び変更機能 電源ON時の自動消去回数の間合せ及び変更機能 全データエリア消去の停止機能 ドキュメントファイリングデータ消去の停止機能 電源ON時の自動消去の停止機能 (残存情報保護の実施タイミングは、割り当て解除時に固定)	操作パネルにおける管理者
FIA_AFL.1(1)	なし (閾値とアクションは固定)	—
FIA_AFL.1(2)	なし (閾値とアクションは固定)	—
FIA_AFL.1(3)	<ul style="list-style-type: none"> 親展ファイルのロック解除機能 (閾値とアクションは固定)	操作パネルにおける管理者
FIA_SOS.1(1)	なし (品質尺度は固定)	—
FIA_SOS.1(2)	なし (品質尺度は固定)	—
FIA_SOS.1(3)	なし (品質尺度は固定)	—
FIA_UAU.2(1)	<ul style="list-style-type: none"> 操作パネルにおける管理者パスワードの間合せ及び変更機能 	操作パネルにおける管理者
FIA_UAU.2(2)	<ul style="list-style-type: none"> Webにおける管理者パスワード変更機能 	Webにおける管理者
	<ul style="list-style-type: none"> Webにおける管理者パスワードを工場出荷時の値に初期化する機能 	操作パネルにおける管理者
FIA_UAU.2(3)	<ul style="list-style-type: none"> 親展ファイルのパスワード変更機能 親展ファイルのパスワード削除機能 	親展ファイル保存者
	なし (Webにおける管理者パスワード変更機能時に必ず再認証を求める)	—
FIA_UAU.7(1)	なし (管理要件なし)	—
FIA_UID.2(1)	なし (利用者識別情報、及び識別操作が固定)	—
FIA_UID.2(2)	なし (利用者識別情報、及び識別操作が固定)	—
FIA_UID.2(3)	なし (利用者識別情報、及び識別操作が、各親展ファイルに対して固定)	—
FMT_MOF.1	なし (TSFの機能と相互に影響を及ぼす役割グループは操作パネルにおける管理者固定)	—

被管理要件	管理機能	役割
FMT_MTD.1(1)	なし (TSFデータと相互に影響を及ぼす役割のグループは操作パネルにおける管理者固定)	—
FMT_MTD.1(2)	なし (TSFデータと相互に影響を及ぼす役割のグループはWebにおける管理者固定)	—
FMT_MTD.1(3)	なし (TSFデータと相互に影響を及ぼす役割のグループは親展ファイル保存者固定)	—
FMT_MTD.1(4)	なし (TSFデータと相互に影響を及ぼす役割のグループは操作パネルにおける管理者固定)	—
FMT_SMF.1	なし (管理要件なし)	—
FMT_SMR.1(1)	なし (役割の一部をなす利用者は操作パネルにおける管理者固定)	—
FMT_SMR.1(2)	なし (役割の一部をなす利用者はWebにおける管理者固定)	—
FMT_SMR.1(3)	なし (役割の一部をなす利用者は、各親展ファイルに対し、その保存者1名限りに固定)	—
FPT_RVM.1	なし (管理要件なし)	—
FPT_SEP.1	なし (管理要件なし)	—

5.1.2 TOE セキュリティ保証要件

本書が選択した保証レベルについての保証コンポーネントを表 5.2 に示す。表 5.2 は EAL3 適合を主張するために満たすべき保証要件である。すべての依存性は満たされている。

表 5.2: 保証要件

コンポーネント	コンポーネント名称	依存性
ACM_CAP.3	許可の管理	ALC_DVS.1
ACM_SCP.1	TOEのCM範囲	ACM_CAP.3
ADO_DEL.1	配付手続き	なし
ADO_IGS.1	設置、生成、及び立上げ手順	AGD_ADM.1
ADV_FSP.1	非形式的機能仕様	ADV_RCR.1
ADV_HLD.2	セキュリティ実施上位レベル設計	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	非形式的対応の実証	なし
AGD_ADM.1	管理者ガイダンス	ADV_FSP.1
AGD_USR.1	利用者ガイダンス	ADV_FSP.1
ALC_DVS.1	セキュリティ手段の識別	なし
ATE_COV.2	カバレッジの分析	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	テスト: 上位レベル設計	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	機能テスト	なし
ATE_IND.2	独立テスト - サンプル	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.1	ガイダンスの検査	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	TOEセキュリティ機能強度評価	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	開発者脆弱性分析	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.1.3 最小機能強度

本 TOE の全体のセキュリティ最小機能強度は SOF-基本 である。

また、本 TOE が満足する機能要件のうち、確率的または順列的メカニズムを利用するのは FIA_UAU.2(1), FIA_UAU.2(2), FIA_UAU.2(3), FIA_UAU.6, FIA_SOS.1(1), FIA_SOS.1(2) 及び FIA_SOS.1(3) であり、明示された機能強度は SOF-基本 である。FCS_COP.1 は暗号アルゴリズムを利用した機能要件であるので、本機能強度レベルの対象としない。

5.2 IT 環境に対するセキュリティ要件

5.2.1 IT 環境に対するセキュリティ機能要件

本節では TOE の IT 環境が満たすべきセキュリティ機能要件について述べる。要件を満たすべきエンティティは、TOE の IT 環境内に三つある。

- Web ブラウザ

これは TOE の Web にアクセスするために、クライアント上で使用する Web ブラウザである。広く使われている Web ブラウザの多くは、以下の要件を満たしている。例えば Microsoft Internet Explorer 6.0 は、以下の要件を満たしている。

- プリントクライアント

これは TOE の プリンタ機能 (2.3.1.2 節) を利用するために、TOE へてにプリントデータを送付するクライアントである。典型的には、クライアント上で動作しプリントデータを生成するソフトウェア、すなわちプリンタドライバが、要件を満たす UI を提供する。TOE が動作する対象 MFD 機種 (2.2.1 節を参照) 用としてシャープが提供しているプリンタドライバは、以下の要件を満たしている。プリンタ機能を標準搭載した MFD 及びプリンタ機能を MFD に追加するシャープ純正オプション品には、上記のプリンタドライバが付属している。

- PC-FAX クライアント

これは TOE の PC-FAX 機能 (2.3.1.7 節) を利用するために、TOE へてにイメージデータを送付するクライアントである。典型的には、クライアント上で動作し PC-FAX 送信可能なイメージデータを生成するソフトウェア、すなわち PC-FAX ドライバが、要件を満たす UI を提供する。TOE が動作する対象 MFD 機種 (2.2.1 節を参照) 用としてシャープが提供している PC-FAX ドライバは、以下の要件を満たしている。プリンタ機能を標準搭載した MFD 及びプリンタ機能を MFD に追加するシャープ純正オプション品には、上記の PC-FAX ドライバが付属している。

これらのエンティティが満たすべき機能要件は、以下の通りである。

- FIA_UAU.7(2) 保護された認証フィードバック(2)

下位階層: なし

FIA_UAU.7.1(2) **Webブラウザ (TSF)** は、認証を行っている間、[入力された文字の個数] だけを利用者に提供しなければならない。

依存性: FIA_UAU.1 認証のタイミング

- FIA_SOS.1(4) 秘密の検証(4)

下位階層: なし

FIA_SOS.1.1(4) **プリントクライアント及びPC-FAXクライアント (TSF)** は、**親展ファイルのパスワード (秘密)** が [5 文字の十進数字] 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。

依存性: なし

5.2.2 IT 環境に対するセキュリティ保証要件

TOE の IT 環境が満たすべきセキュリティ保証要件はない。

6 TOE 要約仕様

本章は、セキュリティ要件に対する TOE のセキュリティ機能と保証手段を述べる。

6.1 TOE セキュリティ機能 (TSF)

TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係を表 6.1 に示す。表中に、各々の対応関係を記載している節番号を示す。

表 6.1: 機能要件と仕様概要

機能要件	機能	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT	TSF_NSP	TSF_FCF
FCS_CKM.1		6.1.1						
FCS_COP.1			6.1.2					
FDP_RIP.1				6.1.3				
FIA_AFL.1(1)				6.1.3	6.1.4			
FIA_AFL.1(2)							6.1.6	
FIA_AFL.1(3)					6.1.4	6.1.5		6.1.7
FIA_SOS.1(1)						6.1.5		
FIA_SOS.1(2)							6.1.6	
FIA_SOS.1(3)								6.1.7
FIA_UAU.2(1)				6.1.3	6.1.4			
FIA_UAU.2(2)							6.1.6	
FIA_UAU.2(3)								6.1.7
FIA_UAU.6							6.1.6	
FIA_UAU.7(1)				6.1.3	6.1.4			6.1.7
FIA_UID.2(1)				6.1.3	6.1.4			
FIA_UID.2(2)							6.1.6	
FIA_UID.2(3)								6.1.7
FMT_MOF.1				6.1.3				
FMT_MTD.1(1)					6.1.4			
FMT_MTD.1(2)							6.1.6	
FMT_MTD.1(3)								6.1.7
FMT_MTD.1(4)					6.1.4			
FMT_SMF.1				6.1.3		6.1.5	6.1.6	6.1.7
FMT_SMR.1(1)				6.1.3	6.1.4	6.1.5		
FMT_SMR.1(2)							6.1.6	
FMT_SMR.1(3)								6.1.7
FPT_RVM.1				6.1.3	6.1.4		6.1.6	6.1.7
FPT_SEP.1				6.1.3	6.1.4		6.1.6	6.1.7

6.1.1 暗号鍵生成 (TSF_FKG)

TSF_FKG は、FCS_CKM.1 が要求する暗号鍵 (共通鍵) の生成を行い、実イメージデータの暗号操作をサポートする。MFD の電源が ON になると、MSN-D 拡張アルゴリズムを用いて、AES Rijndael アルゴリズムを実施するための暗号鍵 (共通鍵) が生成される。この暗号鍵は 128 ビット長であり、揮発性 RAM 内に保存する。

6.1.2 暗号操作 (TSF_FDE)

MFD は、ジョブ処理の途上において、ジョブのデータである実イメージデータを MSD にスプール保存する。スプール保存するにあたり、揮発性 RAM 内に保存している暗号化鍵を用い AES Rijndael アルゴリズムによって暗号化の後、MSD にスプール保存する。また、スプール保存された実イメージデータを実際に

処理 (利用) する際には、ジョブ処理の過程で必要となるデータ断片 (処理中ジョブ 1 件の実イメージデータの一部分) を必要の都度 MSD から読み出し、復号することにより得る。

利用者が親展ファイル機能により MSD に保存する実イメージデータ及びパスワードは、スプールと同様、暗号化の後、MSD にファイリング保存する。再操作に先立つ親展ファイル保存者認証の都度、親展ファイルのパスワードを MSD から読み出し、復号することにより得る。再操作として印刷あるいは送信する際には、スプールと同様、再操作処理の過程で必要となるデータ断片 (再操作対象の実イメージデータの一部分) を必要の都度 MSD から読み出し、復号することにより得る。

それに対し、エクスポート時は復号せず、親展ファイルの実イメージデータ及びパスワードを、暗号化されたままクライアントに送信する。そのため、バックアップ機能によって親展ファイルの実イメージデータまたはパスワードが漏えいすることはない。

インポート時は、データが暗号化されているかどうかを見分け、未暗号化なら暗号化する。これは TOE 設置前のファイリングデータを移行するための仕組みである。

6.1.3 データ消去 (TSF_FDC)

本 TSF は MSD にスプール保存及びファイリング保存されたイメージデータファイルを消去する。以下の各機能は本 TSF に含まれる。

- 各ジョブ完了後の自動消去
- 全データエリア消去
- ドキュメントファイリングデータ消去
- 電源 ON 時の自動消去

各機能とも、HDD の実イメージデータを上書き消去する際には、循環付き遅延フィボナッチアルゴリズムに基づいて生成したランダム値で上書きする。このとき、セキュリティ管理者 (TSF_FMT) 機能により設定された繰返し回数が適用される。ランダム値は繰返しのたびに生成する。また、Flash メモリの実イメージデータを上書き消去する際には、固定値を 1 回上書きする。

以下、各機能について記述する。

6.1.3.1 各ジョブ完了後の自動消去

本機能は以下の通り、実イメージデータを上書き消去する。

- ジョブ処理のために HDD または Flash メモリにスプール保存された実イメージデータを、当該ジョブ完了時に上書き消去する。
- 親展ファイル機能により HDD に保存された実イメージデータを、利用者の操作により削除される際に上書き消去する。

6.1.3.2 全データエリア消去

操作パネルにおける管理者の操作により、HDD にスプール保存またはファイリング保存されている実イメージデータ、及び、Flash メモリにスプール保存されている実イメージデータに対する上書き消去を実行する。

本機能は中止機能を持つ。本機能を途中で中止する場合、キャンセル操作を選択後、本 TSF は必ず操作パネルにおける管理者パスワードの入力を要求する。操作パネルにおける管理者パスワードを入力している間、TOE は入力した文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。操作パネルにおける管理者として識別認証された場合のみ、上書き消去を中止する。この操作パネルにおける管理者認証では、連続して 3 回認証に失敗した場合、認証入力受付を 5 分間停止する (6.1.4 節で詳述する)。

6.1.3.3 ドキュメントファイリングデータ消去

操作パネルにおける管理者の操作により上書き消去を実行する。その対象は、HDD にスプール保存されているすべての実イメージデータ、HDD にファイリング保存されているすべての実イメージデータ、また

は、それら両方のいずれかであり、操作パネルにおける管理者が指定する。本機能は、全データエリア消去と同様の中止機能を持つ。

6.1.3.4 電源 ON 時の自動消去

TOE の電源 ON 時に上書き消去を実行する。ただし、スキャン送信またはファクス送信の予約ジョブがある場合、及び、未出力のファクス受信またはインターネット FAX 受信ジョブがある場合を除く。

本機能の有効または無効、すなわち、電源 ON 時に本機能を実行するか否かは、セキュリティ管理者 (TSF_FMT) 機能により設定される値に従う。本機能を実行する際の消去対象領域も同様である。

消去対象領域は、全データエリア消去と同様に全 MSD とするか、または、またはドキュメントファイリングデータ消去と同様に HDD 内の指定領域とするかのいずれかである。本機能は、全データエリア消去と同様の中止機能を持つ。

6.1.4 認証 (TSF_AUT)

TOE は、操作パネルにおける管理者としての操作を利用者に許可する前に、管理者設定の選択による利用者識別に引き続き、5桁の暗証番号、即ち、操作パネルにおける管理者パスワードの入力を必ず要求する。操作パネルにおける管理者パスワードを正しく入力する手順によって、操作パネルにおける管理者として認証される。操作パネルにおける管理者として認証された利用者のみが、TSF_FMT (6.1.5 節) の各機能及び TSF_NSP (6.1.6 節) のネットワーク設定 UI にアクセスできる。

操作パネルにおける管理者パスワード入力にあたっては、保護されたフィードバックを提供する。すなわち、操作パネルにおける管理者パスワードを入力している間、TOE は入力した文字と同数のアスタリスクを表示するが、入力した文字は表示しない。

操作パネルにおける管理者パスワードの認証では、連続して3回認証に失敗した場合、認証入力受付を5分間停止する。本 TSF は認証失敗回数を管理している。認証に成功したとき、認証失敗回数をゼロに戻す。本 TSF は認証入力受付停止の残時間を管理している。残時間があるときに TOE の電源を切られた場合、次回 TOE 起動時に、残時間を5分間に再設定する。

これと同様の認証受付停止機能が、TSF_FDC (6.1.3 節) の中止機能にもあるが、これら二つの認証受付停止機能は連動している。すなわち、両方の認証失敗回数を通算し、一方を停止しているときは他方も停止している。よって、例えば TSF_FDC が認証受付を停止した場合において、残時間がゼロになる前に管理者設定を選択した場合、本 TSF は認証を受け付けない。

6.1.5 セキュリティ管理者 (TSF_FMT)

このセキュリティ管理者 (TSF_FMT) 機能は、管理者設定選択と、操作パネルにおける管理者パスワード入力による認証 (TSF_AUT) による識別認証の手順を経た後に、以下の管理者向けセキュリティ管理機能を提供する。

- a) 各ジョブ完了後の自動消去回数:
各ジョブ完了後の自動消去が HDD 上の実イメージデータを上書きする際の上書き繰り返し回数を、1回から7回までの間で設定でき、設定値の問合せ、及び変更ができる。設定値は、MFD 内の EEPROM 内に保存する。
- b) データエリア消去回数:
全データエリア消去及びドキュメントファイリングデータ消去が HDD 上の実イメージデータを上書きする際の上書き繰り返し回数を、1回から7回までの間で設定でき、設定値の問合せ、及び変更ができる。設定値は MFD 内の EEPROM 内に保存する。
- c) 電源 ON 時の自動消去:
電源 ON 時の自動消去の有効または無効を、対象領域別に設定できる。各設定値は MFD 内の EEPROM 内に保存する。
- d) 電源 ON 時の自動消去回数:
電源 ON 時の自動消去が HDD 上の実イメージデータを上書きする際の上書き繰り返し回数を1回か

ら7回までの間で設定でき、設定値の間合せ、及び変更ができる。設定値は MFD 内の EEPROM 内に保存する。

e) 操作パネルにおける管理者パスワードの変更:

操作パネルにおける管理者パスワードの設定値の間合せ、及び変更ができる。本 ST は操作パネルにおける管理者パスワードの品質を十進数字 5 文字と定めている。本 TSF は、操作パネルにおける管理者パスワードの新しい値が入力されたとき、品質の検査を行う。設定値は MFD 内の EEPROM 内に保存する。

f) ドキュメントファイリング再操作ロックの解除:

連続して認証に失敗してロックされた親展ファイルは、本機能により操作パネルにおける管理者のみがロック解除できる。各親展ファイルがロックされているか否かは MFD 内の HDD に保存している。

g) NIC リセット:

MFD のネットワーク関連設定を、すべて工場出荷時の値に初期化する。すなわち、Web における管理者パスワード等、保護対象ネットワーク関連設定はすべて初期化される。

上記の各機能は TOE セキュリティ機能要件 FMT_SMF.1 が規定する操作パネルにおける管理者のための管理機能に対応している。

6.1.6 ネットワーク設定保護 (TSF_NSP)

本 TSF は MFD のネットワーク設定に関し、2.4.3 節に記載の保護対象ネットワーク設定データを、管理者以外の改変から保護する。本 TSF は、以下の 2 通りの設定機能で構成される。

- ネットワーク設定 UI
- ネットワーク管理ページ

保護対象ネットワーク設定データを改変する手段は、TOE の ROM 内に実装された上記の各機能以外にない。よって、保護対象ネットワーク設定データは管理者以外による改変から保護される。

以下、各機能について記述する。

6.1.6.1 ネットワーク設定 UI

操作パネルにおいて、ネットワーク設定 UI を提供する。この UI は、管理者設定選択と、操作パネルにおける管理者パスワード入力による認証 (TSF_AUT) による識別認証の手順を経た後にのみ提供される。

6.1.6.2 ネットワーク管理ページ

TOE の Web 内においてネットワーク管理ページを提供する。本 TSF はネットワーク管理ページへのアクセスに先立って必ず Web における管理者の利用者識別名とパスワードによる識別認証を要求し、識別認証に成功した利用者のみアクセスを許す。TOE の Web において、保護対象ネットワーク設定データを改変する I/F は、このネットワーク管理ページ以外にない。これにより、TOE の Web において、保護対象ネットワーク設定データは Web における管理者以外による改変から保護される。

この Web における管理者認証は、TSF_AUT と同様、連続して 3 回認証に失敗した場合、認証入力受付を 5 分間停止する。

この Web における管理者パスワード変更機能は、ネットワーク管理ページ内のパスワード設定ページにある。パスワード設定ページの機能を実行するには、Web における管理者パスワードの、現在の値を入力することによる再認証が必要である。

パスワード設定ページで、Web における管理者パスワード変更が可能である。Web における管理者パスワード変更の際、新パスワードは数字のほか、英字及び記号を含んでよいが、5 文字未満はエラーとして拒否する。

6.1.7 親展ファイル (TSF_FCF)

MFD 内に利用者が親展ファイルとして保存した実イメージデータをパスワード保護し、認証を経て再操作 (印刷等) を許す。

本 TSF は、保存すなわち親展ファイル生成の際に、パスワード設定を利用者に求め、かつそのパスワードが 5 文字の十進数字に合致することを検査する。

本 TSF は、操作パネルまたは Web 経由で親展ファイルの再操作の機能を提供する。

利用者が操作パネルで親展ファイルに対して再操作を行う場合、本 TSF は利用者にパスワード入力を必ず要求し、入力した文字と同数のアスタリスクを表示するが、入力した文字は表示しない。本 TSF は、パスワードが入力され、かつ、保存の際に設定されたパスワードと一致している場合に限り、2.3.2 節で述べた再操作（プレビューを除く）を許す。

利用者が Web で親展ファイルに対して再操作を行う場合、本 TSF は、パスワードが入力され、かつ、保存の際に設定されたパスワードと一致していることを必ず検査し、その検査に成功した場合に限り、2.3.2 節で述べた再操作を許す。

親展ファイルの再操作に先立つパスワード認証では、連続して 3 回認証に失敗した場合、本 TSF はそのファイルをロックし、再操作を禁止する。失敗回数は、各ファイルについて数える。認証に成功したとき、当該ファイルの失敗回数をゼロに戻す。本 TSF はロックをかけるが、ロックを解除することはできず、セキュリティ管理者 (TSF_FMT) 機能のみによって解除できる。

本 TSF は再操作の一種としてパスワード変更の機能を提供し、新パスワードが 5 文字の十進数字に合致することを検査する。

本 TSF は再操作の一種として属性変更の機能を提供する。親展以外の属性に変更すれば、パスワードは削除される。この逆に、属性を親展に変更する場合、パスワードを指定する必要がある、かつパスワードが 5 文字の十進数字に合致することを検査する。

6.2 保証手段

各 TOE 保証要件のコンポーネントを満たす保証手段を表 6.2 に示す。

表 6.2: 保証手段

保証要件	保証手段
ACM_CAP.3	MX-FRX5 MX-FRX6 構成管理説明書
ACM_SCP.1	MX-FRX6 VERSION M.10 構成リスト
ADO_DEL.1	MX-FRX5 MX-FRX6 配付手順説明書
ADO_IGS.1	MX-FRX5 MX-FRX6 配付手順説明書, MX-FRX6 設置手順書 (*1)
ADV_FSP.1	MX-FRX6 セキュリティ機能仕様書
ADV_HLD.2	MX-FRX5 MX-FRX6 上位レベル設計書
ADV_RCR.1	MX-FRX5 MX-FRX6 表現対応分析書
AGD_ADM.1 AGD_USR.1 AVA_MSU.1	取扱説明書データセキュリティキット MX-FRX6 (*2), 注意書データセキュリティキット MX-FRX5 MX-FRX6 (*2), MX-FRX6 Web ヘルプ (全般) (*2), MX-FRX6 Web ヘルプ (ドキュメントファイリング) (*2), 取扱説明書デジタル複合機 管理者設定編 (*2), 取扱説明書デジタル複合機 共通編/コピー編 (*2), 取扱説明書デジタル複合機 プリンタ編 (*2), 取扱説明書デジタル複合機 イメージ送信編 (*2), 取扱説明書デジタル複合機 ファクス編 (*2), MXモデル向けファクス編補足 (*2)
ALC_DVS.1	MX-FRX5 MX-FRX6 開発セキュリティ仕様書
ATE_COV.2	MX-FRX5 MX-FRX6 カバレッジ分析書
ATE_DPT.1	MX-FRX5 MX-FRX6 上位レベル設計テスト分析書
ATE_FUN.1	MX-FRX6 機能テスト仕様書,
ATE_IND.2	MX-FRX5 MX-FRX6 テスト環境・ツール説明書
AVA_SOF.1	MX-FRX5 MX-FRX6 セキュリティ機能強度分析書
AVA_VLA.1	MX-FRX5 MX-FRX6 脆弱性分析書

(*1) 5 言語で書かれている: 日本語、英語、スペイン語、フランス語及びドイツ語。

(*2) 各ガイダンス文書の日本語版及び英語版を保証手段とする。

無印のドキュメントは日本語で書かれている。

6.3 セキュリティ機能強度

TSF を実現するために使用される確率的または順列的メカニズムは、以下の通りである。

- 操作パネルにおける管理者パスワード
これにより実現される TSF は、操作パネルにおける管理者認証 (TSF_AUT 及び TSF_FDC) 及び、操作パネルにおける管理者パスワード変更 (TSF_FMT) である。これらのセキュリティ機能強度はいずれも SOF-基本 である。
- Web における管理者パスワード
これにより実現される TSF は、Web における管理者認証、Web における管理者再認証、及び、Web における管理者パスワード変更 (いずれも TSF_NSP) である。これらのセキュリティ機能強度はいずれも SOF-基本 である。
- 親展ファイルのパスワード
これにより実現される TSF は、親展ファイルの保存、再操作前の認証、及び、パスワード変更 (いずれも TSF_FCF) である。これらのセキュリティ機能強度はいずれも SOF-基本 である。

7 PP 主張

本 TOE は PP には準拠していない。

8 根拠

本章は、本書の完全性と一貫性を検証する。

8.1 セキュリティ対策方針根拠

TOE セキュリティ環境に示した脅威、前提条件に対して、セキュリティ対策方針で示した対策が有効であることを表 8.1 に検証する。表 8.1 は、脅威、前提条件とセキュリティ対策方針の対応について、その根拠を記載している節番号を示したものである。

表 8.1: セキュリティ対策方針根拠

環境 対策方針	脅威 T.RECOVER	脅威 T.SHUNT	脅威 T.SPOOF	前提条件 A.NETWORK	前提条件 A.OPERATOR	前提条件 A.USER
O.RESIDUAL	8.1.1					
O.REMOVE	8.1.1					
O.MANAGE	8.1.1					
O.NSP		8.1.2				
O.UAU			8.1.3			
OE.BROWSER		8.1.2	8.1.3			
OE.CIPHER				8.1.4		
OE.CLIENT			8.1.3			
OE.FIREWALL				8.1.4		
OE.OPERATE					8.1.5	
OE.USER						8.1.6

8.1.1 T.RECOVER

脅威 T.RECOVER に対して、O.MANAGE により、TOE のセキュアな運用のため操作パネルにおける管理者が TOE 機能の管理を行うことで対抗する。MSD の実イメージデータを読み出されないよう

O.RESIDUAL で消去し、かつ、消去前の実イメージデータが読み出されても、O.REMOVE にて、実イメージデータを人間にとって意味のあるものとして判読できないように、実イメージデータを暗号化後に MSD へ書き込むことで対抗する。これにより MSD 内の情報漏えいが防止できる。

8.1.2 T.SHUNT

脅威 T.SHUNT に対して、O.NSP でネットワーク関連設定機能を保護し、許可された管理者（操作パネルにおける管理者、及び、Web における管理者）以外が保護された機能へアクセスできないよう制限する。Web における管理者がアクセスするために、OE.BROWSER に従い認証入力機能を持つ Web ブラウザを使用する。これらにより、攻撃者がネットワーク関連設定を変更することを防止できる。

8.1.3 T.SPOOF

脅威 T.SPOOF に対して、MFD 内に保存するファイルに O.UAU 及び OE.CLIENT で利用者認証データを付与し、O.UAU 及び OE.BROWSER で利用者認証を実施することで対抗する。利用者が MFD 内へファイルを保存する際、その利用者だけが知り得るパスワードを設定することにより、攻撃者のなりすましが防止できる。

8.1.4 A.NETWORK

前提条件 A.NETWORK は、TOE が設置される内部ネットワークのセキュリティを求めている。そのために、OE.FIREWALL で内部ネットワークを外部ネットワークの脅威から保護する。また、OE.CIPHER で内部ネットワーク環境下の TOE の通信データを保護する。これらにより TOE が設置される内部ネットワークは必要なセキュリティを保つことができる。

8.1.5 A.OPERATOR

前提条件 A.OPERATOR は、管理者（操作パネルにおける管理者及び Web における管理者）が信頼できることを求めており、OE.OPERATE は、組織の責任者が、操作パネルにおける管理者及び Web における管理者の役割を理解した上で、操作パネルにおける管理者及び Web における管理者の人は厳重に行うことにより実施できる。

8.1.6 A.USER

前提条件 A.USER は、利用者がパスワードに関して遵守すべき事項を示している。そのため OE.USER が示すように、組織の責任者が管理者に遵守させ、管理者が親展ファイル利用者に遵守させることにより、パスワードを使用するすべての利用者に対して実施できる。

8.2 セキュリティ要件根拠

セキュリティ対策方針に対して、IT セキュリティ要件が有効であることを検証する。

8.2.1 TOE セキュリティ機能要件根拠

本節では、TOE セキュリティ機能要件が TOE のセキュリティ対策方針を達成するのに適していることの根拠を示す。

TOE セキュリティ機能要件と TOE のセキュリティ対策方針の対応について表 8.2 に示す。表 8.2 は、各々の対応関係について、その根拠を記載している節番号を示したものである。

表 8.2: TOE セキュリティ機能要件根拠

対策方針 要件	O.RESIDUAL	O.REMOVE	O.MANAGE	O.NSP	O.UAU
FCS_CKM.1		8.2.1.2			
FCS_COP.1		8.2.1.2			
FDP_RIP.1	8.2.1.1				
FIA_AFL.1(1)			8.2.1.3	8.2.1.4	
FIA_AFL.1(2)				8.2.1.4	
FIA_AFL.1(3)			8.2.1.3		8.2.1.5
FIA_SOS.1(1)			8.2.1.3	8.2.1.4	
FIA_SOS.1(2)				8.2.1.4	
FIA_SOS.1(3)					8.2.1.5
FIA_UAU.2(1)			8.2.1.3	8.2.1.4	
FIA_UAU.2(2)				8.2.1.4	
FIA_UAU.2(3)					8.2.1.5
FIA_UAU.6				8.2.1.4	
FIA_UAU.7(1)			8.2.1.3	8.2.1.4	8.2.1.5
FIA_UID.2(1)			8.2.1.3	8.2.1.4	
FIA_UID.2(2)				8.2.1.4	
FIA_UID.2(3)					8.2.1.5
FMT_MOF.1			8.2.1.3		
FMT_MTD.1(1)			8.2.1.3		
FMT_MTD.1(2)				8.2.1.4	
FMT_MTD.1(3)					8.2.1.5
FMT_MTD.1(4)			8.2.1.3		
FMT_SMF.1			8.2.1.3	8.2.1.4	8.2.1.5
FMT_SMR.1(1)			8.2.1.3		
FMT_SMR.1(2)				8.2.1.4	
FMT_SMR.1(3)					8.2.1.5
FPT_RVM.1			8.2.1.3	8.2.1.4	8.2.1.5
FPT_SEP.1			8.2.1.3	8.2.1.4	8.2.1.5

8.2.1.1 O.RESIDUAL

O.RESIDUAL は、MSD に保存されている実イメージデータが格納された領域、すなわちイメージデータファイルの上書き消去実行であり、各ジョブ完了後、親展ファイル削除時、全データエリア消去実行時、ドキュメントファイリングデータ消去実行時、及び、電源 ON 時に発動され、FDP_RIP.1 により利用者データ保護が実施される。

O.RESIDUAL は、単一の機能要件によって満たされ、機能要件の競合はない。

8.2.1.2 O.REMOVE

O.REMOVE は、MFD 内の MSD に対し、実イメージデータの保存を実行した TOE 自身以外からアクセスされても、実イメージデータからのイメージ表示を阻止することである。

FCS_COP.1 により MFD 内の実イメージデータはすべて暗号化済みとなり、未暗号化のまま MSD に保存されることはない。そのため、FDP_RIP.1 で未だ消去されていないイメージデータファイルに対しても、攻撃者がイメージ表示しようとする試みは阻止される。FCS_COP.1 を実施するためには、FCS_CKM.1 により暗号鍵を生成する。

O.REMOVE は、互いに依存し合う FCS_COP.1 及び FCS_CKM.1 によって満たされ、機能要件の競合はない。

8.2.1.3 O.MANAGE

O.MANAGE は、TOE のセキュアな運用のため、管理者のみが以下に示す TOE 機能の管理を行うことである。

- a) FIA_UAU.2(1), FIA_UAU.7(1), FIA_UID.2(1) 及び FIA_AFL.1(1) によって、操作パネルにおける管理者を識別認証する。これにより、以下の各機能の実行が操作パネルにおける管理者にのみ可能とする。
 - FMT_MTD.1(1) にて、各ジョブ完了後の自動消去時 HDD 上書き回数、データエリア消去時 HDD 上書き回数、電源 ON 時の自動消去の領域別有効設定、電源 ON 時の自動消去時 HDD 上書き回数、及び、操作パネルにおける管理者パスワードの変更と問合せが、操作パネルにおける管理者にのみ可能となる。
 - FMT_MTD.1(4) にて、Web における管理者パスワードを工場出荷時の値に初期化する機能を、操作パネルにおける管理者のみが使用できる。
 - 連続する認証失敗による親展ファイルのロックを解除することが、FIA_AFL.1(3) により、操作パネルにおける管理者にのみ可能となる。
 - 実行中の全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去の各機能を停止することが、FMT_MOF.1 により、操作パネルにおける管理者にのみ可能となる。
- b) FPT_RVM.1 は、操作パネルにおける管理者にのみ可能であるべき各機能の実行を許す前に、上記 a) 項で述べた操作パネルにおける管理者識別認証が必ず呼び出され、成功することを保証する。
- c) FPT_SEP.1 は、上記 a) 項で述べた各機能を保護するためのセキュリティドメインを要求している。
- d) FMT_SMF.1 に定める管理機能のうち操作パネルにおける管理者のためのものが、本セキュリティ対策方針に対応する。
- e) 以下のように、操作パネルにおける管理者パスワードに適切な SOF を確保する。
 - FIA_AFL.1(1) は、操作パネルにおける管理者パスワードに対する総当たり攻撃に対抗すべく、認証失敗が連続したときに一定時間の認証受付停止を要求している。
 - FIA_SOS.1(1) は、操作パネルにおける管理者パスワードの品質検証メカニズムを要求している。
- f) 操作パネルにおける管理者は、FMT_MOF.1 及び FMT_MTD.1(1) により、TOE の管理の役割を任せられ、この役割は FMT_SMR.1(1) にて維持されるため、常に正当な操作パネルにおける管理者が管理機能を実行できる。

上記 FIA_AFL.1(1), FIA_UID.2(1), FIA_UAU.2(1), FIA_UAU.7(1), FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(4), FMT_SMF.1 及び FMT_SMR.1(1) の間には依存に基づく支援があり、かつ、互いに競

合するような機能性を要求していない。それらの要件と FIA_AFL.1(3) の間で競合するような機能性の要求はなく、FIA_AFL.1(3) と FMT_SMF.1 は相互に支援し合い、FMT_SMR.1(1) は FIA_AFL.1(3) を支援する。それらの要件と FIA_SOS.1(1) の間で競合するような機能性の要求はなく、FIA_SOS.1(1) と FIA_AFL.1(1) は相互に支援し合う。FPT_RVM.1 及び FPT_SEP.1 は競合なくそれらを支援する。したがって O.MANAGE は競合なく一貫した要件群により満たされている。

8.2.1.4 O.NSP

本セキュリティ対策方針は、以下の各要素によって満たされる。

- ネットワーク設定 UI に対するパスワード保護
 - FIA_UAU.2(1), FIA_UAU.7(1), FIA_UID.2(1) 及び FIA_AFL.1(1) によって、操作パネルにおける管理者パスワードを用いて、操作パネルにおける管理者を識別認証する。識別認証は、保護対象ネットワーク設定データの改変を許すネットワーク設定 UI を提供する前に行う。
 - FPT_RVM.1 は、上記の識別認証が、保護対象ネットワーク設定データの改変を許すネットワーク設定 UI を提供する前に必ず呼び出され、成功することを保証する。
 - FPT_SEP.1 はネットワーク設定 UI を保護するためのセキュリティドメインを要求している。
- ネットワーク管理ページに対するパスワード保護。
 - FIA_UAU.2(2), FIA_UID.2(2) 及び FIA_AFL.1(2) によって、パスワードを用いて Web における管理者を識別認証する。識別認証は、保護対象ネットワーク設定データの改変を許すネットワーク管理ページを提供する前に行う。ここでは FIA_UAU.7(1) に代わって IT 環境要件 FIA_UAU.7(2) が適用される。
 - FPT_RVM.1 は、上記の識別認証が、保護対象ネットワーク設定データの改変を許すネットワーク管理ページを提供する前に必ず呼び出され、成功することを保証する。
 - FMT_SMF.1 は FIA_UAU.2(2) に関し、Web における管理者パスワード変更機能を要求している。その利用は、FMT_MTD.1(2) により、Web における管理者のみに許され、かつ FIA_UAU.6 により再認証が必要である。
 - 役割 Web における管理者 は TSF データのうち Web における管理者パスワードの管理を任せられ、FMT_SMR.1(2) にて維持される。
 - FPT_SEP.1 はネットワーク管理ページを保護するためのセキュリティドメインを要求している。
- 適切な SOF の確保。
 - FIA_AFL.1(1) は、操作パネルにおける管理者パスワードに対する総当たり攻撃に対抗すべく、認証失敗が連続したときに一定時間の認証受付停止を要求している。
 - FIA_AFL.1(2) は、Web における管理者パスワードに対する総当たり攻撃に対抗すべく、認証失敗が連続したときに一定時間の認証受付停止を要求している。
 - FIA_SOS.1(1) は、操作パネルにおける管理者パスワードの品質検証メカニズムを要求している。
 - FIA_SOS.1(2) は、Web における管理者パスワードの品質検証メカニズムを要求している。

Web に関する FIA_AFL.1(2), FIA_UID.2(2), FIA_UAU.2(2), FIA_UAU.7(2), FMT_MTD.1(2), FMT_SMF.1 及び FMT_SMR.1(2) の間には依存に基づく支援があり、かつ、互いに競合するような機能性を要求していない。それらの要件と FIA_UAU.6 は互いに支援し合い、かつ、互いに競合するような機能性を要求していない。

O.NSP を満たす他の要件は操作パネルに関するものであり、O.MANAGE に関して述べた通り互いに競合しない。

操作パネルにおける保護と Web における保護は、FMT_MTD.1(4) の範囲を除いて独立している。

O.NSP を満たす各要件と FMT_MTD.1(4) との間には、相互支援はあるが、互いに競合するような機能性の要求はない。

以上から、O.NSP は競合なく一貫した要件群により満たされている。

8.2.1.5 O.UAU

本セキュリティ対策方針は、次の 3 要素によって満たされる。

- 親展ファイルの再操作に対するパスワード保護。
 - FIA_UID.2(3) 及び FIA_UAU.2(3) は、親展ファイルのパスワードによって親展ファイル保存者を識別認証することで、親展ファイルの再操作を保護することを、要求している。
 - FPT_RVM.1 は、上記の識別認証が、親展ファイルの再操作を許す前に必ず呼び出され、成功することを保証する。
 - FMT_SMF.1 は FIA_UAU.2(3) に関し、親展ファイルのパスワード変更及び削除機能を要求している。その利用は、FMT_MTD.1(3) により、各々の親展ファイル保存者のみに許される。
 - 役割 親展ファイル保存者 は、TSF データのうち親展ファイルパスワードの管理を任せられ、FMT_SMR.1(3) にて維持される。
 - FPT_SEP.1 は親展ファイルの再操作を保護するためのセキュリティドメインを要求している。
- パスワード入力に適した認証入力 I/F。
 - FIA_UAU.7(1) は、パスワード入力に適した認証入力 I/F を要求している。
- 適切な SOF の確保。
 - FIA_AFL.1(3) は、ファイルの利用者認証手段に対する総当り攻撃に対抗すべく、認証失敗が連続したときに当該ファイルをロックすることを要求している。
 - FIA_AFL.1(3) は、ロックの解除を、識別認証された操作パネルにおける管理者以外には許さない。
 - FIA_SOS.1(3) は、親展ファイルのパスワードの品質検証メカニズムを要求している。

上記 FIA_UAU.2(3), FIA_UAU.7(1), FIA_UID.(3), FMT_MTD.1(3), FMT_SMF.1 及び FMT_SMR.1(3) の間には依存に基づく支援があり、かつ、互いに競合するような機能性を要求していない。それらの要件と FIA_SOS.1(3) の間で競合するような機能性の要求はなく、FIA_AFL.1(3) と FIA_SOS.1(3) は相互に支援し合う。FPT_RVM.1 及び FPT_SEP.1 は競合なくそれらを支援する。したがって O.UAU は競合なく一貫した要件群により満たされている。

8.2.2 セキュリティ機能要件の依存性根拠

セキュリティ機能要件の依存性について表 8.3 に示す。表 8.3 は、満足すべきと CC が規定する依存性と、本 TOE が満足している依存性、満足していない依存性、及び満足していないことの妥当性を記載している節番号を示したものである。

表 8.3: セキュリティ機能要件の依存性

依存性 機能要件	満足すべき	満足している	不満足	妥当性
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	8.2.2.1
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	同上	同上
FDP_RIP.1	—	—	—	—
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1)	—	—
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2)	—	—
FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.2(3)	—	—
FIA_SOS.1(1)	—	—	—	—
FIA_SOS.1(2)	—	—	—	—
FIA_SOS.1(3)	—	—	—	—
FIA_SOS.1(4)*	—	—	—	—
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1)	—	—
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2)	—	—
FIA_UAU.2(3)	FIA_UID.1	FIA_UID.2(3)	—	—

依存性 機能要件	満足すべき	満足している	不満足	妥当性
FIA_UAU.6	—	—	—	—
FIA_UAU.7(1)	FIA_UAU.1	FIA_UAU.2(1), FIA_UAU.2(3)	—	—
FIA_UAU.7(2)*	FIA_UAU.1	FIA_UAU.2(2)	—	—
FIA_UID.2(1)	—	—	—	—
FIA_UID.2(2)	—	—	—	—
FIA_UID.2(3)	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_MTD.1(2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(2)	—	—
FMT_MTD.1(3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(3)	—	—
FMT_MTD.1(4)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1(1)	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1(1)	FIA_UID.1	FIA_UID.2(1)	—	—
FMT_SMR.1(2)	FIA_UID.1	FIA_UID.2(2)	—	—
FMT_SMR.1(3)	FIA_UID.1	FIA_UID.2(3)	—	—
FPT_RVM.1	—	—	—	—
FPT_SEP.1	—	—	—	—

注: 識別子に * を付した機能要件は IT 環境の要件であり、他は TOE セキュリティ機能要件である。

8.2.2.1 FCS_CKM.4 及び FMT_MSA.2 の依存性を必要としない根拠

暗号鍵を保存しているのは、揮発性 RAM 内であり、TOE もしくは MFD の電源断により、揮発性 RAM に格納された暗号鍵は、消失する。電荷を蓄える回路を記憶素子として利用している揮発性 RAM は、情報の記憶を電荷によって行っており、揮発性 RAM 内に保存された暗号鍵は、TOE もしくは MFD の電源断によって、蓄えられていた電荷が無くなることで暗号鍵を読み出すことができなくなる。

よって、標準の方法を用いて暗号鍵を破棄する必要性がなく、標準を特定する FCS_CKM.4 は必要がない。

この暗号鍵は、電源 ON 時に生成され電源断により消失する 128 ビットの鍵そのもののみからなり、日時その他のセキュリティ属性を持たない。よって、FMT_MSA.2 によってセキュアな値を保証しなければならないセキュリティ属性が存在しない。

表 8.4: TOEセキュリティ機能要件の相互作用

8.2.3 TOE セキュリティ機能要件の相互作用

TOE セキュリティ機能要件の相互作用の関係について表 8.4 に示す。

8.2.3.1 迂回

表 8.4 に関し、迂回を防ぐ相互サポートについて述べる。

a) 操作パネルにおける管理者認証

FIA_UAU.2(1) は、操作パネルにおける管理者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

b) Web における管理者認証 FIA_UAU.2(2)

は、Web における管理者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

c) 親展ファイル保存者認証 FIA_UAU.2(3) は

親展ファイル保存者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

d) 操作パネルにおける管理者識別

FIA_UID.2(1) は、操作パネルにおける管理者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

e) Web における管理者識別 FIA_UID.2(2) は、

Web における管理者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

f) 親展ファイル保存者識別 FIA_UID.2(3) は、

親展ファイル保存者を代行する TSF 調停アクションを許可する前に呼び出され成功しなければならないが、これは FPT_RVM.1 により保証される。

上記以外の各機能要件は、迂回される性質のものではない。

8.2.3.2 非活性化

表 8.4 に関し、各 TOE セキュリティ機能要件に対する非活性化について述べる。

利用者のデータ保護 FDP_RIP.1 のうち、ジョブ完了後及び親展ファイル削除時の呼び出しを非活性化する手段はない。全データエリア消去時、ドキュメントファイリングデータ消去時、及び、電源 ON 時の自動消去時の動作を、各機能の実行中に停止する操作により非活性化する役割は、FMT_MOF.1 により操作パネルにおける管理者のみに制限される。

上記以外の各機能要件を非活性化する手段はない。

8.2.3.3 干渉

表 8.4 に関し、各 TOE セキュリティ機能要件に対する干渉について述べる。

機能要件	防御	迂回	非活性化	干渉
FCS_CKM.1	—	—	—	—
FCS_COP.1	—	—	—	—
FDP_RIP.1	—	—	FMT_MOF.1	—
FIA_AFL.1(1)	—	—	—	—
FIA_AFL.1(2)	—	—	—	—
FIA_AFL.1(3)	—	—	—	—
FIA_SOS.1(1)	—	—	—	—
FIA_SOS.1(2)	—	—	—	—
FIA_SOS.1(3)	—	—	—	—
FIA_UAU.2(1)	FPT_RVM.1	—	—	FPT_SEP.1
FIA_UAU.2(2)	FPT_RVM.1	—	—	FPT_SEP.1
FIA_UAU.2(3)	FPT_RVM.1	—	—	FPT_SEP.1
FIA_UAU.6	—	—	—	—
FIA_UAU.7(1)	—	—	—	—
FIA_UID.2(1)	FPT_RVM.1	—	—	FPT_SEP.1
FIA_UID.2(2)	FPT_RVM.1	—	—	FPT_SEP.1
FIA_UID.2(3)	FPT_RVM.1	—	—	FPT_SEP.1
FMT_MOF.1	—	—	—	—
FMT_MTD.1(1)	—	—	—	—
FMT_MTD.1(2)	—	—	—	—
FMT_MTD.1(3)	—	—	—	—
FMT_MTD.1(4)	—	—	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1(1)	—	—	—	—
FMT_SMR.1(2)	—	—	—	—
FMT_SMR.1(3)	—	—	—	—
FPT_RVM.1	—	—	—	—
FPT_SEP.1	—	—	—	—

- 操作パネルにおける管理者識別 FIA_UID.2(1) 及び同認証 FIA_UAU.2(1) によって生成される許可されたサブジェクトには、不正なサブジェクトの干渉等から保護するためのセキュリティドメインが必要であり、これは FPT_SEP.1 により保証される。
- Web における管理者識別 FIA_UID.2(2) 及び同認証 FIA_UAU.2(2) によって生成される許可されたサブジェクトには、不正なサブジェクトの干渉等から保護するためのセキュリティドメインが必要であり、これは FPT_SEP.1 により保証される。
- 親展ファイル保存者識別 FIA_UID.2(3) 及び同認証 FIA_UAU.2(3) によって生成される許可されたサブジェクトには、不正なサブジェクトの干渉等から保護するためのセキュリティドメインが必要であり、これは FPT_SEP.1 により保証される。

上記以外の各機能要件には不正なサブジェクトが存在しない。

8.2.4 TOE セキュリティ保証要件根拠

本 TOE は、MFD のファームウェア アップグレード キットであり、商用の製品である。また、脅威に対しては、上書き消去、暗号化、及びパスワード保護という簡単なメカニズムの組合せで対抗することができる。このため本 TOE は、商用として十分である EAL3 を品質保証レベルとする。

8.2.5 最小機能強度根拠

本 TOE に対する攻撃者の攻撃能力を限定することを意図して本 ST は、前提条件、及び、環境のセキュリティ対策方針を規定している。それでもなお、低い攻撃能力 (low attack potential) を有する攻撃者に対抗する必要を免れるとは言えない。

そのために必要十分な機能強度は SOF-基本 である。本 ST は TOE に対し最小機能強度として SOF-基本 を求めており、一貫している。

8.2.6 IT 環境に対するセキュリティ要件根拠

本節では IT 環境に対するセキュリティ要件が環境のセキュリティ対策方針を達成するのに適していることの根拠を示す。環境のセキュリティ対策方針のうち IT 環境に対するものは OE.BROWSER 及び OE.CLIENT であり、他は TOE の運用に対するものである。

OE.BROWSER は、Web における管理者認証及び親展ファイルのパスワード認証のための認証入力機能を要求する。この認証入力機能には、以下が必要である。

- パスワード入力に適した I/F。
 - FIA_UAU.7(2) は、保護された認証フィードバックを、Web ブラウザに要求している。

OE.CLIENT は、プリンタジョブまたは PC-FAX ジョブの親展ファイルに付与すべきパスワードを利用者が指定するための I/F の要求を含む。この I/F には、以下が必要である。

- 適切な SOF の確保。
 - FIA_SOS.1(4) は、親展ファイルのパスワードの品質検証を、プリントクライアント及び PC-FAX クライアントに要求している。

TOE はパスワードの設定と認証の両方を行うのに対し、プリントクライアント及び PC-FAX クライアントは設定のみを行うので、上記で十分である。

なお、Web における管理者パスワード設定時の品質検証は TOE セキュリティ機能要件 FIA_SOS.1(2) である。

これらのセキュリティ機能要件の依存性は、表 8.3 に示した通り、すべて満たされている。

セキュリティ保証要件を IT 環境に求める理由はなく、他の IT セキュリティ要件からの依存もない。よって、IT 環境に対するセキュリティ保証要件は必要ない。

8.3 TOE 要約仕様根拠

本節は IT セキュリティ要件に対して TOE セキュリティ機能とその保証手段の有効性について検証する。

8.3.1 TOE セキュリティ機能根拠

表 6.1 に示した TOE セキュリティ機能要件と TSF の対応について、以下に根拠を示す。

8.3.1.1 FCS_CKM.1

FCS_CKM.1 は、TOE の電源投入時に TSF_FKG が MSN-D 拡張アルゴリズムにより 128 ビットの暗号鍵 (共通鍵) を生成するため、満足される。

8.3.1.2 FCS_COP.1

TSF_FDE は MSD に書き込むすべての未暗号化の、実イメージデータ及び親展ファイルのパスワードを暗号化する。

TSF_FDE は、ジョブ処理、親展ファイル保存者認証、及び、再操作の過程で必要となるデータ断片を必要の都度 MSD から読み出し復号する。

上記以外に復号処理はない。

上記の暗号化及び復号は FIPS PUB 197 で規格化された Rijndael アルゴリズムに従う。

これらにより FCS_COP.1 は満足される。

8.3.1.3 FDP_RIP.1

TSF_FDC は、各ジョブ完了後の自動消去実行時に、MSD (HDD または Flash メモリ) に保存されたイメージデータファイルに対し 1 回以上上書き消去することにより、当該イメージデータファイルに保存されていた実イメージデータの再生を不能とする。

TSF_FDC は、全データエリア消去実行時に、MSD (HDD 及び Flash メモリ) に保存されたすべてのイメージデータファイルに対し 1 回以上上書き消去することにより実イメージデータの再生を不能とする。

TSF_FDC は、ドキュメントファイリングデータ消去または電源 ON 時の自動消去実行時に、操作パネルにおける管理者が指定した MSD 領域を対象とし、そこに保存されたすべてのイメージデータファイルに対し 1 回以上上書き消去することにより実イメージデータの再生を不能とする。

これらにより FDP_RIP.1 は満足される。

8.3.1.4 FIA_AFL.1(1)

TSF_FDC 及び TSF_AUT は操作パネルにおける管理者認証を行う。これらはいずれも FIA_AFL.1(1) が定める認証失敗対応を備えている。よって FIA_AFL.1(1) は満足される。

8.3.1.5 FIA_AFL.1(2)

TSF_NSP により、TOE の Web 内のネットワーク管理ページは、Web ブラウザでのアクセス時に Web における管理者の識別認証を経た後のみにアクセスできる。この認証は、FIA_AFL.1(2) が定める認証失敗対応を備えている。よって FIA_AFL.1(2) は満足される。

8.3.1.6 FIA_AFL.1(3)

親展ファイル再操作前の親展ファイル保存者認証において TSF_FCF は、認証失敗回数を親展ファイルごとに数えており、連続 3 回の失敗で当該親展ファイルをロックする。このロックを解除することは、TSF_FMT によるドキュメントファイリング再操作ロックの解除によってのみ可能だが、それは TSF_AUT による認証を経た操作パネルにおける管理者にのみ許される。これにより FIA_AFL.1(3) が満足される。

8.3.1.7 FIA_SOS.1(1)

TSF_FMT は操作パネルにおける管理者パスワードを変更するにあたり、新しい値の桁数が 5 桁であることを検査する。これにより FIA_SOS.1(1) は満足される。

8.3.1.8 FIA_SOS.1(2)

TSF_NSP は Web における管理者パスワードを変更するにあたり、新しい値の文字数が 5 桁以上あることを検査する。新しい値として英大文字、英小文字、数字、及び、英記号が入力可能である。これにより FIA_SOS.1(2) は満足される。

8.3.1.9 FIA_SOS.1(3)

TSF_FCF による親展ファイルの保存時、親展ファイルのパスワード変更時、及び、親展ファイル以外の親展への属性変更時において、親展ファイルのパスワードの桁数が 5 桁であることを検査する。これにより FIA_SOS.1(3) は満足される。

8.3.1.10 FIA_UAU.2(1)

以下に示すように、FIA_UAU.2(1) は TSF_FDC 及び TSF_AUT により満足される。

アクション許可に先立ち操作パネルにおける管理者認証が必要なアクション (TSF) は、以下の通りである。

- 認証機能 (TSF_AUT)
利用者が管理者設定を選択操作したときに、TSF_AUT により認証が実施される。
- データ消去の中止機能 (TSF_FDC)
全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去を実行中に、利用者が途中で中止する操作をしたときに、TSF_FDC により認証が実施される。

これらの認証はいずれも、利用者の操作によるアクション要求を受けて各 TSF が実施し、認証成功の場合のみアクションを許可する。TOE が行う操作パネルにおける管理者認証は、上記がすべてであり、いずれもアクション許可前の認証である。よって、FIA_UAU.2(1) が満足される。

8.3.1.11 FIA_UAU.2(2)

TSF_NSP により、TOE の Web 内のネットワーク管理ページは、Web ブラウザでのアクセス時に Web における管理者の識別及び認証を経た後のみにアクセスできる。これにより FIA_UAU.2(2) が満足される。

8.3.1.12 FIA_UAU.2(3)

利用者が MFD 操作パネルまたは TOE の Web において親展ファイルの再操作を行う場合、選択された親展ファイルの保存者のみが知り得るパスワードによって認証を行う。TSF_FCF はこの認証を、再操作を実行する前に行う。認証に成功しない限り TSF_FCF は再操作を実行することはない。これにより FIA_UAU.2(3) が満足される。

8.3.1.13 FIA_UAU.6

Web における管理者の識別認証後、Web における管理者パスワード変更 I/F が提供されるが、ここでさらに TSF_NSP による Web における管理者再認証により Web における管理者パスワード変更が許可される。これ以外に Web における管理者パスワードを改変する手段はない。よって FIA_UAU.6 は満足される。

8.3.1.14 FIA_UAU.7(1)

TOE が提供する認証 I/F は、以下の通りである。

- TSF_AUT による操作パネルにおける管理者認証
- TSF_FDC による中止機能の操作パネルにおける管理者認証
- TSF_FCF による親展ファイル再操作の場合のパスワード入力

いずれも認証フィードバックとして、入力された文字そのもののエコーバックに代えて、アスタリスクを表示するため、FIA_UAU.7(1) は満足される。

8.3.1.15 FIA_UID.2(1)

以下に示すように FIA_UID.2(1) は TSF_FDC 及び TSF_AUT により満足される。

アクション許可に先立ち操作パネルにおける管理者識別が必要なアクション (TSF) は、以下の通りである。

- 認証機能 (TSF_AUT)
利用者が管理者設定を選択する操作が、操作パネルにおける管理者識別に該当する。この操作機能は TSF_AUT が提供する。
- データ消去の中止機能 (TSF_FDC)
全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去を実行中に、利用者が途中で中止する操作が、操作パネルにおける管理者識別に該当する。この操作機能は TSF_FDC が提供する。

TOE が行う操作パネルにおける管理者識別は、上記がすべてであり、いずれもアクション許可前の識別である。よって、FIA_UID.2(1) が満足される。

8.3.1.16 FIA_UID.2(2)

TSF_NSP により、TOE の Web 内のネットワーク管理ページは、Web ブラウザでのアクセス時に Web における管理者の識別及び認証を経た後のみにアクセスできる。これにより FIA_UID.2(2) が満足される。

8.3.1.17 FIA_UID.2(3)

利用者が MFD 操作パネルまたは TOE の Web において親展ファイルの再操作を行う場合、選択された親展ファイルの保存者のみが知り得るパスワードによって認証を行う。TSF_FCF はこの認証を、再操作を実行する前に行う。認証に成功しない限り TSF_FCF は再操作を実行することはない。これにより FIA_UID.2(3) が満足される。

8.3.1.18 FMT_MOF.1

FMT_MOF.1 は、TSF_FDC による操作パネルにおける管理者の識別認証により、全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去を途中で中止することを可能とするため、満足される。

8.3.1.19 FMT_MTD.1(1)

管理者設定の各ジョブ完了後の自動消去回数、データエリア消去回数、電源 ON 時の自動消去、電源 ON 時の自動消去回数、及び、操作パネルにおける管理者パスワードの変更の各機能によってのみ、各ジョブ完了後の自動消去時 HDD 上書き回数、データエリア消去時 HDD 上書き回数、電源 ON 時の自動消去の領域別有効設定、電源 ON 時の自動消去時 HDD 上書き回数、及び、操作パネルにおける管理者パスワードの改変と問合せが可能となる。

管理者設定の使用は TSF_AUT による操作パネルにおける管理者識別認証後に許される。よって FMT_MTD.1(1) は満足される。

8.3.1.20 FMT_MTD.1(2)

TSF_NSP による Web における管理者の識別認証後、TSF_NSP により Web における管理者パスワード変更 I/F が提供され、さらに TSF_NSP による Web における管理者再認証により Web における管理者パスワード変更が許可される。これ以外に Web における管理者パスワードを改変する手段はない。よって FMT_MTD.1(2) は満足される。

8.3.1.21 FMT_MTD.1(3)

TSF_FCF による親展ファイル保存者の識別認証後、TSF_FCF による当該親展ファイルのパスワード変更、及び、属性変更によるパスワード削除が可能となる。これにより FMT_MTD.1(3) は満足される。

8.3.1.22 FMT_MTD.1(4)

管理者設定の NIC リセット操作によってのみ Web における管理者パスワードは工場出荷時の値にリセットされる。管理者設定の使用は TSF_AUT による操作パネルにおける管理者識別認証後に許される。よって FMT_MTD.1(4) は満足される。

8.3.1.23 FMT_SMF.1

表 8.5 は FMT_SMF.1 の特定するセキュリティ管理機能すべてが TSF によって実施されていることを示している。よって FMT_SMF.1 は満足される。

表 8.5: 管理機能の特定と実施

特定されたセキュリティ機能	TSF	TSFが実施する機能
各ジョブ完了後の自動消去時HDD上書き回数の間合せ及び変更機能	TSF_FMT	各ジョブ完了後の自動消去回数
データエリア消去時HDD上書き回数の間合せ及び変更機能	TSF_FMT	データエリア消去回数
電源ON時の自動消去の領域別有効設定の間合せ及び変更機能	TSF_FMT	電源ON時の自動消去
電源ON時の自動消去時HDD上書き回数の間合せ及び変更機能	TSF_FMT	電源ON時の自動消去回数
全データエリア消去の停止機能	TSF_FDC	全データエリア消去の中止
ドキュメントファイリングデータ消去の停止機能	TSF_FDC	ドキュメントファイリングデータ消去の中止
電源ON時の自動消去の停止機能	TSF_FDC	電源ON時の自動消去の中止
親展ファイルのロック解除機能	TSF_FMT	ドキュメントファイリング再操作ロックの解除
操作パネルにおける管理者パスワードの間合せ及び変更機能	TSF_FMT	操作パネルにおける管理者パスワードの変更
Webにおける管理者パスワードを工場出荷時の値に初期化する機能	TSF_FMT	NICリセット
Webにおける管理者パスワード変更機能	TSF_NSP	パスワード設定ページ
親展ファイルのパスワード変更機能	TSF_FCF	パスワード変更
親展ファイルのパスワード削除機能	TSF_FCF	属性変更

8.3.1.24 FMT_SMR.1(1)

操作パネルにおける管理者は、他人が知り得ないパスワードを使用した TSF_AUT 及び TSF_FDC の識別認証によって役割に関連づけられる。また、TSF_FMT による操作パネルにおける管理者パスワード変更を通じて役割を維持する。これらにより FMT_SMR.1(1) は満足される。

8.3.1.25 FMT_SMR.1(2)

Web における管理者は、他人が知り得ないパスワードを使用した TSF_NSP の識別認証によって役割に関連づけられる。また、TSF_NSP による Web における管理者パスワード変更を通じて役割を維持する。Web における管理者パスワードを初期化する機能 (TSF_NSP) の使用は、不正を行わない操作パネルにおける管理者に限定される。これらにより FMT_SMR.1(2) は満足される。

8.3.1.26 FMT_SMR.1(3)

各親展ファイルについて、保存者のみが知り得るパスワードを使用した TSF_FCF の識別認証によって役割に関連づけられる。また、TSF_FCF によるパスワード変更を通じて役割を維持する。これらにより FMT_SMR.1(3) は満足される。

8.3.1.27 FPT_RVM.1

8.2.3.1 節で述べた FPT_RVM.1 によるサポートが、各 TSF により実施されていることを以下に示す。

- TSF_FDC は、全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去を実行中に、利用者が途中で中止する操作を行ったときに、必ず操作パネルにおける管理者パスワード認証機能呼び出し、認証に成功しない限り各機能を途中で中止しない。
- TSF_AUT は、利用者が管理者設定（セキュリティ管理者機能、及び、ネットワーク設定 UI を含む）の選択操作を行った場合、必ず操作パネルにおける管理者パスワード認証機能呼び出し、認証に成功しない限り管理者設定 UI を提供しない。
- TSF_NSP は、ネットワーク管理ページに対するすべての HTTP リクエストに対し、Web における管理者の識別認証を要求し、ネットワーク管理ページに対するいかなるアクセスも Web における管理者の識別認証が成功しなければ許可しない。
- TSF_FCF は、利用者が操作パネルまたは Web を通して親展ファイル再操作を要求した場合、必ず親展ファイルパスワード認証機能呼び出し、認証に成功しない限り、再操作を実行しない。

以上各項で示したように、TSF_FDC、TSF_AUT、TSF_NSP 及び TSF_FCF が 8.2.3.1 節で述べた FPT_RVM.1 によるサポートをすべて実施しており、FPT_RVM.1 は満足される。

8.3.1.28 FPT_SEP.1

8.2.3.3 節で述べた FPT_SEP.1 によるサポートが、各 TSF により実施されていることを以下に示す。

- TSF_FDC は、操作パネルにおける管理者パスワード認証を実施することにより、セキュリティドメインを維持し、実行中の全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去を途中で中止する機能を保護している。
- TSF_AUT は、操作パネルにおける管理者パスワード認証を実施することにより、セキュリティドメインを維持し、管理者設定（セキュリティ管理者機能、及び、ネットワーク設定 UI を含む）を保護している。
- TSF_NSP は、Web における管理者の識別認証を実施することにより、セキュリティドメインを維持し、ネットワーク管理ページを保護している。
- TSF_FCF は、親展ファイルパスワード認証を実施することにより、セキュリティドメインを維持し、親展ファイル再操作機能を保護している。

以上各項で示したように、TSF_FDC、TSF_AUT、TSF_NSP 及び TSF_FCF が 8.2.3.3 節で述べた FPT_SEP.1 によるサポートをすべて実施しており、FPT_SEP.1 は満足される。

8.3.2 TOE 保証手段根拠

6.2 節の保証手段の有効性を検証する。表 6.2 に示すように、すべての TOE セキュリティ保証要件は、保証手段により示されたドキュメントにより対応付けられており、また保証手段に示されたドキュメントによって、本書が規定した TOE セキュリティ保証要件 EAL3 が要求している証拠に合致している。

8.3.3 TOE セキュリティ機能強度根拠

6.3 節で述べたとおり、確率的または順列的メカニズムによって実現されるすべての TSF は、セキュリティ機能強度 SOF-基本 を持つ。それらセキュリティ機能強度の最小値は SOF-基本 である。

これは TOE の最小機能強度である SOF-基本 に対して必要十分である。よって、TOE セキュリティ機能強度と最小機能強度は、一貫している。