CM2510250
セキュリティターゲット

Version 0.02

履歴

日付	Ver.	変更点	作成	確認	発行
2008/2/12	0.01	• 初版作成	中川	岩崎	辻井
2008/6/19	0.02	• 所見報告書 ASE001-01 に基づく修正	中川	岩崎	薬師寺

目次

表のリスト

図のリスト

1 ST 概説

1.1 ST 識別

本書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: CM2510250 セキュリティターゲット

バージョン: 0.02

発行日: 2008 年 6 月 19 日

作成者: シャープ株式会社

TOE 識別: CM2510250 Version M.10

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

1.2 ST 概要

本 ST は、上記 TOE すなわち CM2510250 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) は事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。TOE は IT 製品であり、Océ Imagistics Inc. が販売する MFD のデータ保護を目的とする。

TOE は、MFD 内の HDD または Flash メモリ上に保存あるいは残存するイメージデータが開示される危険性を減ずることを目的とした IT 製品であり、二つの部分から構成される。一部は MFD 内のハードウェアであり、MFD にて提供される。他の部分はファームウェア製品であり、MFD のファームウェアに対する、アップグレードキットとして提供される。TOE の主なセキュリティ機能は以下の通りであり、本 ST はこれらについて説明する。

- イメージデータおよび関連データの暗号化
- イメージデータおよび関連データ削除時の上書き消去
- 利用者が HDD に保存するイメージデータおよび関連データのパスワード保護

TOE のファームウェア部分は、MFD のセキュリティを強化するためのオプション製品 “Data Security Kit CM2510250” (DSK と略称) により提供される。TOE のハードウェア部分は MFD 内の HDC である。TOE のファームウェア部分は、HDC 内セキュリティ機能を活性化し、制御する。

1.3 CC 適合

本 ST は、以下を満たしている。

a) CC v2.3 パート 2 適合。

b) CC v2.3 パート 3 適合。

c) 保証パッケージは EAL2 に ADV_SPM.1 を追加。

d) 補足-0512 を適用。

e) 適合する PP はない。

1.4 参照資料

本 ST 作成にあたり、表 1.1 記載の資料を参照している。本 ST 中の [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。

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 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

1.5 規約、専門用語、略語

本 ST 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 ST 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。

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。必要に応じ、パラメータ名を丸括弧 ( ) に入れ、値に付記する。

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** で示し、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 ST 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
アドレス帳/本体内登録データ消去	HDD上のアドレス帳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。
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。
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、および、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。

用語	定義
揮発性メモリ	電源を切れば記憶内容が消失する記憶装置。
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、揮発性メモリ, HDC, 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。
再操作	ファイリング保存したイメージデータに対する操作。
サブネットワーク	その内部にルータを含まない単一のネットワーク。
ジョブ	MFDのコピー、プリンタ、スキャナ、ファクス送受信およびPC-Faxの各機能において、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。
ジョブ完了記録	完了したジョブに関する記録。MFD内のHDDに保持される。
ジョブ状況完了エリア消去	HDD上のジョブ完了記録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。
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、ファクス送信およ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内のMSD上にあるすべてのイメージデータおよびジョブ完了記録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。
操作パネル	MFDの正面にあるUI用ユニット。スタートキー、数字キー、機能キーおよびタッチ操作式の液晶ディスプレイを含む。
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。
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はコントローラファームウェアを含んでおり、TOE設置時に標準ファームウェアを取り外す。
ファームウェア	機器のハードウェアを制御するために、機器に組み込まれたソフトウェア。本STでは特に、コントローラファームウェアを指す。
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。
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。

用語	定義
不揮発性メモリ	電源を切っても記憶内容を保持することができる記憶装置。
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去および任意部分の再書き込みを可能にしたROM (Flash Memory)。
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 ST 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。
DSK	Data Security Kit CM2510250 — MFDの別売オプション品。TOEのファームウェア部分を含む。
EEPROM	Electronically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM。
HDC	Hard Disk Controller (ハード ディスク コントローラ) — MFD内のHDCはTOEのハードウェア部分を含む。
HDD	Hard Disk Drive (ハード ディスク ドライブ)
HTTP	Hypertext Transfer Protocol — 主にWebで用いられる通信プロトコルの名称。
HTTPS	HTTP over SSL — SSLにより保護されたHTTP。
I/F	Interface (インタフェース)
IPP	Internet Printing Protocol — 印刷用通信プロトコルの名称。
IPP-SSL	IPP over SSL — SSLにより保護されたIPP。
LDAP	Lightweight Directory Access Protocol — ディレクトリサービス用通信プロトコルの名称。
MFD	Multi Function Device — デジタル複合機。事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。本書では、2.2.1節で識別する対象機種を指す。
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特にMFD内のHDDおよび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)
OS	Operating System (オペレーティングシステム)
ROM	Read Only Memory — 読み出し専用メモリ。
SSL	Secure Socket Layer — 計算機ネットワーク用暗号通信プロトコルの名称。
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 製品である。

TOE の主要部分は、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。

MFD 内蔵ハードウェアである HDC が TOE に含まれ、ファームウェア部分から呼び出される。

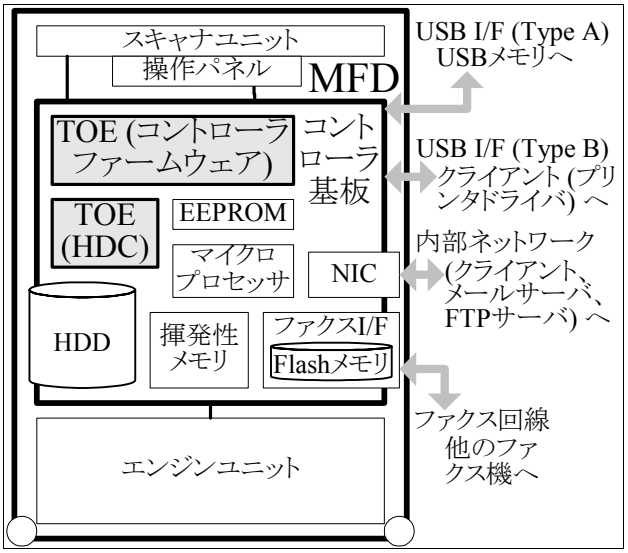

図 1: MFDの物理的構成とTOE

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、および、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等を 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

本節は、TOE の物理的、論理的構成について述べる。

2.2.1 TOE の物理的構成

TOE の主要部分は 2 枚の ROM 基板により提供される。また、実装上の都合上、セキュリティ機能の一部を HDC 内に実装しており、これも TOE の範囲に含む。これを図 1 に網掛けで示す。

TOE が動作する MFD は Océ Imagistics Inc. が販売する cm2510 および cm2510J である。

TOE の物理的範囲は、以下の通りである。

- コントローラファームウェア: コントローラ基板に搭載する 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。
- HDC: コントローラ基板に実装されている 1 個の集積回路部品である。

2.2.2 TOE の論理的構成

TOE の論理的構成を図 2 に示す。TOE の論理的範囲を太い枠線内として示す。TOE 外のハードウェアを、角を丸くした長方形で示す。TOE 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。また、揮発性メモリ, HDD, Flash メモリ, および EEPROM 上にあるデータのうち、セキュリティ機能が扱うデータ (利用者データおよび TSF データ) を、同じく網掛けで示す。

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 の主要部分は、MFD 用のファームウェアであり、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。また、TOE セキュリティ機能 (TSF) の一部は HDC 内に実装され、ファームウェア内の TSF から呼び出される。以下の機能が TOE の論理的範囲に含まれる。

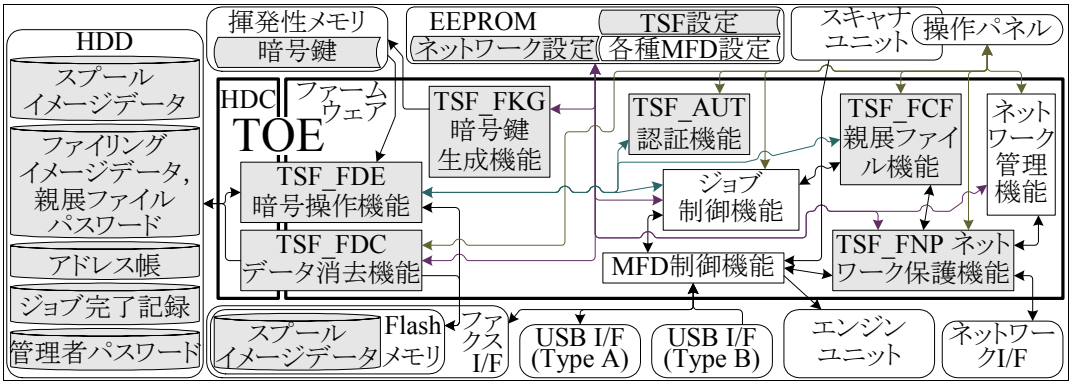

図 2: TOEの論理的構成図

a) 暗号操作機能 (TSF_FDE): MSD に書き込む利用者データおよび TSF データを暗号化する。また、MSD から読み出した利用者データおよび TSF データを復号する。ジョブ制御機能 (各種ジョブ、アドレス帳機能、およびドキュメントファイリング機能) により呼び出される。本機能の一部は HDC 内にあり、ファームウェア部分から呼び出される。

b) 暗号鍵生成機能 (TSF_FKG): 暗号操作機能で使用する暗号鍵を生成する。生成された暗号鍵は、揮発性メモリに保存する。

c) データ消去機能 (TSF_FDC): MSD からの情報漏えいを防ぐため, MSD に対し上書き消去する。本機能の一部は HDC 内にあり、ファームウェア部分から呼び出される。データ消去の各プログラム (各ジョブ完了後の自動消去、全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去) ならびに、その設定機能 (データ消去設定) からなる。各ジョブ完了後の自動消去は、ジョブ制御機能 (各種ジョブおよびドキュメントファイリング機能) により呼び出される。

d) 認証機能 (TSF_AUT): 管理者パスワードにより管理者の識別認証を行う。管理者パスワードを変更する管理機能を持つ。

e) 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 (2.3.2 節) 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。再操作 (印刷や送信) の際に親展ファイルパスワードを要求し認証を行う。連続 3 回認証失敗した親展ファイルをロックする。ロックは管理者のみが解除できる。

f) ネットワーク保護機能 (TSF_FNP): 以下の 3 要素からなる。

- フィルタ機能: IP アドレスまたは MAC アドレスにより通信相手を制限する。
- 通信データ保護機能: SSL により通信データを保護する。ただし、SSL に対応できないクライアントやプロトコルを使用する場合は、本機能を使用することができない。
- ネットワーク設定保護: 以下のネットワーク管理機能を管理者のみに提供し、他の利用者には使用させない。

g) ジョブ制御機能: MFD の各種機能、すなわち各種ジョブ、アドレス帳機能およびドキュメントファイリング機能において、UI を提供し、動作を制御する。ジョブをキュー管理し、ジョブ完了記録を HDD 内に保持する。

h) MFD 制御機能: 各種 MFD ハードウェアを制御する。また、通信を伴うジョブにおいて、送受信するデータと MFD 内のイメージデータとの間でデータ形式を変換する。

i) ネットワーク管理機能: 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、ポート設定 (各ネットワークサービスのポート番号および無効化), その他のネットワーク設定を行う管理者機能である。ネットワーク保護機能 (TSF_FNP) により呼び出される。

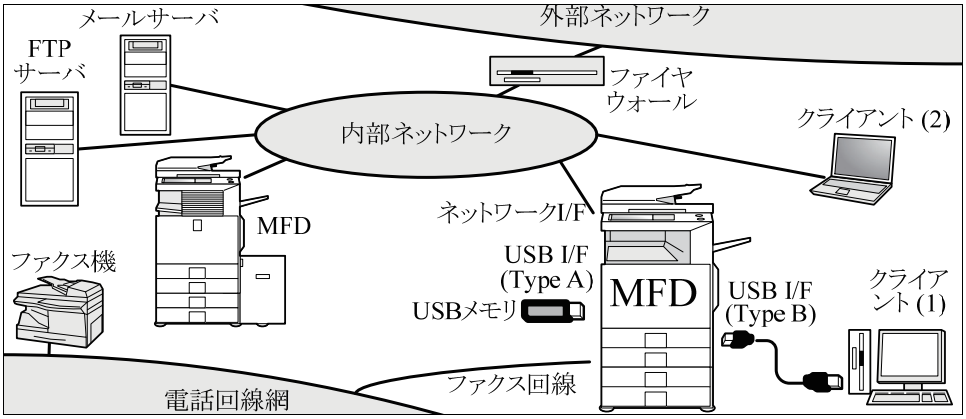

図 3: MFDの利用環境

2.3 MFD 機能及びその利用方法

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、プリンタ、スキャナ、ファクス送信、ファクス受信および PC-Fax 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 (TSF) の一部を自動的に実行する。TOE のこの性質は、TSF 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。

以下、TOE が持つ MFD 機能について説明する。多くの機能は MFD の操作パネルでの操作によって発動する。一部の機能はデータ受信により発動する。さらに一部の機能は TOE の Web, すなわち TOE が内蔵するリモート操作用の Web の操作によって発動する。

2.3.1 ジョブ機能

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。ジョブ制御機能および MFD 制御機能により実現される。

a) コピー: 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。タンデムコピーが指示された場合、管理者が予め指定した MFD にイメージデータを送る。

b) プリンタ: 外部より受信したデータを印刷する。

- プリンタドライバ: クライアントで印刷データを生成し、ネットワークまたは USB 経由で MFD に送る。タンデム印刷が指示された場合、2 台の MFD にイメージデータを送る。
- プッシュプリント: クライアントより印刷データを E-mail, FTP または Web 経由で MFD に送る。MFD からのタンデム印刷要求も同様。
- プルプリント: 操作パネルの操作で FTP サーバまたは USB メモリ内の印刷データを取得する。

c) スキャナ: 操作パネルでの操作により原稿を読み取り、原稿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送る。
- ファイルサーバ: FTP サーバに送る。
- デスクトップ: クライアント (MFD 同梱ソフトウェア要) 宛に FTP で送る。
- 共有フォルダ: Windows 共有フォルダに送る。
- USB メモリ: MFD に取り付けた USB メモリに書き込む。
- リモート PC: クライアント (MFD 同梱ソフトウェア要) 宛に TWAIN で送る。
- 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送る。

d) ファクス送信: 操作パネルでの操作により原稿を読み取り、原稿のイメージデータをファクス送信する。

e) ファクス受信: 他機から送られたファクスを受信し印刷する。

f) PC-Fax: クライアントからのデータをファクス送信またはインターネット Fax 送信する。

2.3.2 ドキュメントファイリング機能

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: スキャナ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。

プリンタドライバのジョブは、印刷せず保存のみ行うよう指定することもできる。スキャン保存は、送信せず保存のみ行うスキャナジョブと考えてよい。

2.3.3 アドレス帳機能

送信先のファクス番号や E-mail アドレスを登録し、送信する際の操作を簡略化する。データは HDD に保存され、操作パネルまたは Web での操作により登録、変更または削除できる。ジョブ制御機能により実現される。

2.4 TOE の運用方法

TOE は、セキュアな運用を維持するための機能として、以下の管理機能を有する。TOE は、管理者のみが、以下の管理機能によって運用可能である。

- 認証に関する設定:
  - 管理者パスワードの変更 (改変)
- ネットワークアクセス制限の設定:
  - IPアドレスフィルタ設定
  - MACアドレスフィルタ設定
- セキュリティに関する各種設定:
  - SSL設定
  - 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時の自動消去の対象別有効設定
  - 電源ON時の自動消去回数
  - ドキュメントファイリング禁止設定
  - ホールド以外のプリントジョブ禁止設定
  - 親展ファイルのロック解除
- データ消去機能の起動:
  - 全データエリア消去
  - アドレス帳/本体内登録データ消去
  - ドキュメントファイリングデータ消去

- ジョブ状況完了エリア消去

● データ消去機能の中止:
- 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中止
- 電源ON時の自動消去の中止

2.5 TOE の保護資産

本 TOE が対象とする保護資産は、以下の利用者データである。

a) MFD 機能がジョブ処理時にスプール保存するイメージデータ

b) 利用者が親展ファイルとしてファイリング保存したイメージデータ

c) アドレス帳データ

d) ジョブ完了記録データ

e) ネットワーク設定データ

上記各項の具体的内容を、以下の各節で記述する。

2.5.1 MFD 機能がジョブ処理時にスプール保存するイメージデータ

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 自身が本章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イメージデータを、本 ST は保護資産とする。これは各利用者の機密情報、すなわち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。

ジョブ完了またはキャンセルの際、MFD は資源の割当て解除のために上記のイメージデータを削除する。この削除とは、管理領域に削除情報を与えることによって、イメージデータ保持のために使用していた領域を、未使用状態にすることであり、一般のパーソナルコンピュータに接続されたハードディスク上のデータファイルを削除する場合と同様である。すなわち、未使用状態とされた領域が他のジョブにより再利用されるまでの間、削除されたイメージデータは残存し得る。そこで本 ST は、MFD 内の HDD または Flash メモリに残存する削除済みイメージデータを保護資産に含める。

2.5.2 利用者が親展ファイルとしてファイリング保存したイメージデータ

利用者がドキュメントファイリング機能により HDD 内に親展ファイルとしてファイリング保存したイメージデータを、本 ST は保護資産とする。これも前項と同様、各利用者の機密情報を含み得る。

これは利用者が削除できるが、前節と同様、削除後も HDD に残存し得る。HDD に残存する削除済みイメージデータも保護資産に含まれる。

2.5.3 アドレス帳データ

利用者がアドレス帳機能によって登録し HDD 内に保存されるアドレス帳データを、本 ST は保護資産とする。これは正当な利用者たちが共同で扱う個人情報 (宛先の名前、メールアドレス、ファクス番号等) であり、組織の機密情報を含み得る。

正当な利用者以外にとって、操作パネルの前に立って一件ずつ目視と手操作でアクセスする以外にアドレス帳データを読み出しまたは改変する手段がなければ、必ずしも対抗すべき脅威があるとはいえない。しかし、HDD から直接に、または Web インタフェースを利用して内部ネットワーク経由で、正当な利用者以外がアドレス帳データをまとめて読み出しまたは改変する可能性からは、保護されねばならない。

2.5.4 ジョブ完了記録データ

ジョブ制御機能が HDD 内に保存するジョブ完了記録データを、本 ST は保護資産とする。これはプリンタドライバからのジョブの利用者名や文書名、ファクス送受信の相手先等、組織の機密情報を含み得る。

正当な利用者以外にとって、操作パネルの前に立って一件ずつ目視と手操作でアクセスする以外にジョブ完了記録データを読み出す手段がなければ、必ずしも対抗すべき脅威があるとはいえない。しかし、

HDD から直接に正当な利用者以外がジョブ完了記録データをまとめて読み出す可能性からは、保護されねばならない。

2.5.5 ネットワーク設定データ

管理者がネットワーク管理機能によって EEPROM 内に登録した、以下のネットワーク設定データを、本 ST は保護資産とする。これは組織の機密情報であり、内部ネットワークの脅威につながり得る。また、不正に改ざんされれば、他の保護資産の脅威につながり得る。

a) TCP/IP 設定: TCP/IP 有効設定, DHCP 有効設定, IP アドレス設定

b) DNS 設定: プライマリ/セカンダリ DNS サーバ, ドメイン名

c) WINS 設定: WINS 有効設定, プライマリ/セカンダリ WINS サーバ, WINS スコープ ID

d) SMTP 設定: SMTP サーバ

e) LDAP 設定: LDAP 有効設定, LDAP サーバ

f) タンデム設定: 子機 IP アドレス, タンデム送信禁止

g) ポート設定: 各ネットワークサービスの有効設定およびポート番号

2.6 TOE の関係者

本節では、本 TOE、及び、本 TOE を設置する MFD の関係者について述べる。

- 所有者: TOE 及び MFD を占有し、管理下におく組織。
- 組織の責任者: 所有者に属し、MFD の管理責任を負う人物。
- 管理者: TOE 及び MFD の運用管理を任された人物。組織の責任者が任命する。

3 TOE セキュリティ環境

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: 前提条件

識別子	定義
A.NETWORK	MFDは、外部ネットワークからの攻撃から保護された内部ネットワークにおける、MFDとの通信を認める機器だけが接続されたサブネットワークに接続するものとする。
A.OPERATOR	管理者は、TOEに対して不正をせず信頼できるものとする。

3.2 脅威

TOE に対する脅威を表 3.2 に示す。いずれも、低い攻撃能力 (low attack potential) を持つ攻撃者を想定している。

表 3.2: 脅威

識別子	定義
T.RECOVER	攻撃者が、MFDからMSDを取り出し、MSD内の利用者データ (削除後に残存しているデータを含む) を読み出し漏えいさせる。
T.REMOTE	MFDへのアクセスを認められていない攻撃者が、内部ネットワーク経由でMFD内のアドレス帳データを、まとめて読み出しまたは改変する。
T.SPOOF	攻撃者が、他の利用者になりすますことにより、操作パネルまたは内部ネットワーク経由で、利用者が親展ファイルとしてファイリング保存したイメージデータを、読み出し漏えいさせる。
T.TAMPER	攻撃者が、管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを、読み出しまたは改変する。
T.TAP	正当な利用者がMFDに対して通信する際、攻撃者が内部ネットワーク上を流れる利用者データを盗聴する。

3.3 組織のセキュリティ方針

組織のセキュリティ方針を表 3.3 に示す。

表 3.3: 組織のセキュリティ方針

識別子	定義
P.RESIDUAL	ジョブ完了または中止時、MSDにスプール保存された利用者データの領域は、少なくとも1回上書き消去されなければならない。 MSDにおいて、利用者が削除した利用者データの領域は、少なくとも1回上書き消去されなければならない。 MFDの廃棄または所有者変更の際、MSDの利用者データの領域はすべて、少なくとも1回上書き消去されなければならない。

4 セキュリティ対策方針

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.FILTER	TOEは、MFDへのアクセスを認められていない利用者が使用する機器からの、ネットワーク経由アクセスを拒否する手段を提供する。
O.MANAGE	TOEは、正当な管理者を識別認証する機能を提供する。
O.REMOVE	TOEは、利用者データをMSDに書き込む際、MFD固有の鍵により暗号化する。
O.RESIDUAL	TOEは、ジョブ完了または中止時、MSDにスプール保存された利用者データの領域を、少なくとも1回上書き消去する。 TOEは、利用者の削除操作により、指定されたMSDの利用者データの領域を、少なくとも1回上書き消去する。 TOEは、管理者の操作により、MSDの利用者データの領域全体を少なくとも1回上書き消去する機能を提供する。
O.TRP	TOEは、内部ネットワーク上を流れる利用者データを盗聴より保護する機能を提供する。
O.USER	TOEは、正当な親展ファイル保存者を識別認証する機能を提供する。

4.2 環境のセキュリティ対策方針

環境の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.CIPHER (1)	管理者は、MFDの利用者がTOEと通信する際にTOEの通信データ保護機能が働くよう、TOEを設定することにより、通信データを盗聴より保護する。
OE.CIPHER (2)	管理者は、MFDの利用者がTOEと通信する際、TOEが設置される内部ネットワーク環境下において、通信データを盗聴より保護するための必要な措置 (暗号化スイッチを設置する、データの受け渡しにUSBメモリを使用させる、等) を実施する。
OE.ERASEALL	管理者は、MFDの廃棄または所有者変更の際、TOEの機能を用いて、MSDの利用者データ領域全体を少なくとも1回上書き消去する。
OE.FIREWALL	管理者は、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を、外部ネットワークからの攻撃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、管理者の役割を理解した上で、管理者の人選は厳重に行う。
OE.PC-USER	管理者は、内部ネットワーク上でMFDへの接続を認める機器において、MFDの正当な利用者のみが利用できるよう、許可利用者を識別認証する機能を動作させる。
OE.SUBNET	管理者は、TOEが設置されるサブネットワークに、MFDとの通信を認める機器のみを接続し、その状態を維持管理する。
OE.USER	管理者は、TOEおよびMFDの利用者に対して、親展ファイルパスワードが漏れないよう安全に管理させるものとする。

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 が満たすべき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、5.1.2 節で規定する。

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[データセキュリティキット用暗号基準書]に合致する、指定された暗号鍵生成アルゴリズム[MSN-R 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、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[AES Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[

- MSD に書き込む利用者データの暗号化
- MSD に書き込む TSF データの暗号化
- MSD から読み出した利用者データの復号
- MSD から読み出した TSF データの復号

]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 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 **少なくとも 1 回上書き消去することにより** 利用できなくすることを保証しなければならない: [

- HDD 上のスプールイメージデータファイル
- HDD 上のファイリングイメージデータファイル
- HDD 上のアドレス帳データファイル
- HDD 上のジョブ完了記録データファイル
- Flash メモリ上のスプール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、[

- 管理者認証操作における最後の認証成功以降の不成功認証試行

]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、[

- 不成功認証が 3 回に達したとき: 5 分間の認証試行受付を停止
- 停止より 5 分経過: 認証失敗回数をクリアし自動的に復帰

]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、[

- 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

]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、[

- 不成功認証が 3 回に達したとき: 認証試行受付を停止し、当該親展ファイルをロック
- 管理者による親展ファイルのロック解除操作: 認証失敗回数をクリアし復帰

]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、 **管理者パスワード** (秘密) が[5 文字以上 32 文字以下の英数記号]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 (2) 秘密の検証(2)

下位階層: なし

FIA_SOS.1.1 (2) TSF は、 **親展ファイルパスワード** (秘密) が[5 文字以上 8 文字以下の数字]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、その **管理者** (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 **管理者** (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。

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、その **親展ファイル保存者** (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 **親展ファイル保存者** (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。

依存性: FIA_UID.1 識別のタイミング

●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、 **管理者の** 認証を行っている間、[入力された文字の個数]だけを **管理者** (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_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) TSF は、 **親展ファイル保存者の** 認証を行っている間、[入力された文字の個数] だけを **親展ファイル保存者** (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、その **管理者** (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 **管理者** (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、その **親展ファイル保存者** (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 **親展ファイル保存者** (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 (1) セキュリティ機能のふるまいの管理(1)

下位階層: なし

FMT_MOF.1.1 (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, アドレス帳/本体内登録データ消去, ジョブ状況完了エリア消去] *[を動作させる]* 能力を[管理者]に制限しなければならない。

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_MOF.1 (2) セキュリティ機能のふるまいの管理(2)

下位階層: なし

FMT_MOF.1.1 (2) 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[管理者]に制限しなければならない。

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_MOF.1 (3) セキュリティ機能のふるまいの管理(3)

下位階層: なし

FMT_MOF.1.1 (3) TSF は、機能[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, ドキュメントファイリング機能, ネットワーク保護機能] *[のふるまいを改変する]* 能力を[管理者]に制限しなければならない。

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_MSA.2 セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1 TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性: ADV_SPM.1 非形式的 TOE セキュリティモデル
[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_MSA.1 セキュリティ属性の管理
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、[管理者パスワード]を*[改変]* する能力を[管理者]に制限しなければならない。

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 (2) TSF データの管理(2)

下位階層: なし

FMT_MTD.1.1 (2) TSF は、[親展ファイルパスワード]を*[改変、* [作成 (*その他の操作*)] *]* 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 管理機能の特定
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、[

- IP アドレスフィルタ
- MAC アドレスフィルタ
- SSL 設定
- 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 時の自動消去の対象別有効設定
- 電源 ON 時の自動消去回数
- ドキュメントファイリング禁止設定
- ホールド以外のプリントジョブ禁止設定

]を*[問い合わせ、改変]* する能力を[管理者]に制限しなければならない。

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_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:[

- 全データエリア消去の起動および中止
- ドキュメントファイリングデータ消去の起動および中止
- 電源 ON 時の自動消去の中止
- アドレス帳/本体内登録データ消去の起動
- ジョブ状況完了エリア消去の起動
- 各ジョブ完了後の自動消去回数の設定
- データエリア消去回数の設定
- 電源 ON 時の自動消去の対象別有効設定
- 電源 ON 時の自動消去回数の設定
- 親展ファイルのロック解除
- 管理者パスワードの改変
- 親展ファイルパスワードの改変
- ドキュメントファイリング禁止設定
- ホールド以外のプリントジョブ禁止設定
- IP アドレスフィルタおよび MAC アドレスフィルタの管理
- SSL 保護対象サービスの管理

]。

注: 管理要件への考慮は 8.2.2 節で述べる。

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[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[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 (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

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

5.1.1.6 クラス FTA: TOE アクセス

●FTA_TSE.1 TOE セション確立

下位階層: なし

FTA_TSE.1.1 TSF は、[IP アドレスおよび MAC アドレス]に基づきセション確立を拒否できなければならない。

依存性: なし

5.1.1.7 クラス FTP: 高信頼パス/チャネル

●FTP_TRP.1 高信頼パス

下位階層: なし

FTP_TRP.1.1 TSF は、それ自身と*[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およ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、*[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、*[* [TOE の Web による通信サービス、プリンタドライバ用通信サービス (*高信頼パスが要求される他のサービス*)] *]* に対して、高信頼パスの使用を要求しなければならない。

依存性: なし

5.1.2 TOE 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_AFL.1 (1), FIA_AFL.1 (2), FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2 (1), FIA_UAU.2 (2), FIA_UAU.7 (1) および FIA_UAU.7 (2) 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。

5.1.3 TOE セキュリティ保証要件

本 ST 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 5.1 に示す。表 5.1 は、EAL2 + ADV_SPM.1 を主張するために満たすべき保証要件である。

表 5.1: 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.2	構成要素	なし
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.1	記述的上位レベル設計	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	非形式的対応の実証	なし
ADV_SPM.1	非形式的なTOEセキュリティ方針モデル	ADV_FSP.1
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
ATE_COV.1	カバレージの証拠	ADV_FSP.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
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

5.2 IT 環境に対するセキュリティ要件

環境のセキュリティ対策方針が TOE の IT 環境に要求するセキュリティ要件はない。

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)

セキュリティ機能要件と TOE のセキュリティ機能の関連性を表 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: セキュリティ機能要件と TOE セキュリティ仕様

機能 機能要件	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FCF	TSF_FNP
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		6.1.6
FIA_AFL.1 (2)					6.1.5	
FIA_SOS.1 (1)				6.1.4		
FIA_SOS.1 (2)					6.1.5	
FIA_UAU.2 (1)			6.1.3	6.1.4		6.1.6
FIA_UAU.2 (2)					6.1.5	
FIA_UAU.7 (1)			6.1.3	6.1.4		6.1.6
FIA_UAU.7 (2)					6.1.5	
FIA_UID.2 (1)			6.1.3	6.1.4		6.1.6
FIA_UID.2 (2)					6.1.5	
FMT_MOF.1 (1)			6.1.3			
FMT_MOF.1 (2)			6.1.3			
FMT_MOF.1 (3)			6.1.3		6.1.5	6.1.6
FMT_MSA.2	6.1.1					
FMT_MTD.1 (1)				6.1.4		
FMT_MTD.1 (2)					6.1.5	
FMT_MTD.1 (3)			6.1.3		6.1.5	6.1.6
FMT_SMF.1			6.1.3	6.1.4	6.1.5	6.1.6
FMT_SMR.1 (1)				6.1.4		
FMT_SMR.1 (2)					6.1.5	
FPT_RVM.1	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.1.6
FTA_TSE.1						6.1.6
FTP_TRP.1						6.1.6

6.1.1 暗号鍵生成 (TSF_FKG)

TOE は、暗号鍵 (共通鍵) の生成を行い、利用者データおよび TSF データの暗号化機能をサポートする。MFD の電源がオンになると、必ず暗号鍵 (共通鍵) を生成する。

TOE は、セキュアなシードを元に、MSN-R 拡張アルゴリズムを用いて 128 ビット長のセキュアな鍵を生成し、暗号アルゴリズム AES Rijndael で使用するために、揮発性メモリ内に保存する。MSN-R 拡張アルゴリズムは、データセキュリティキット用暗号基準書を満たす暗号鍵生成アルゴリズムである。

暗号鍵のセキュリティ属性であるシードは、TSP モデルに従うセキュアな方法で TOE により生成される。TOE セキュリティ保証要件 ADV_SPM.1 の保証手段 (表 6.2) が、TSP モデルを規定している。

6.1.2 暗号操作 (TSF_FDE)

利用者データおよび TSF データを MSD に書き込む必要が生じたときは、必ずそれらのデータを暗号化してから書き込む。また、それらのデータが必要になれば、MSD から読み出し、復号して利用する。

対象となる利用者データは以下の通り:

- HDD 上にスプール保存されるイメージデータ
- Flash メモリ上にスプール保存されるイメージデータ
- HDD 上にファイリング保存されるイメージデータ
- HDD 上のアドレス帳データ
- HDD 上のジョブ完了記録データ

対象となる TSF データは以下の通り:

- HDD 上の親展ファイルパスワード
- HDD 上の管理者パスワード

暗号化および復号には FIPS PUBS 197 に基づく AES Rijndael アルゴリズムと、暗号鍵生成 (TSF_FKG) により生成された 128 ビット長の暗号鍵を用いる。

6.1.3 データ消去 (TSF_FDC)

TOE はスプール保存およびファイリング保存されたイメージデータファイル、またはアドレス帳データファイル、ジョブ完了記録データファイルを消去するデータ消去機能を有する。以下の各プログラムは、本機能に含まれる。

- 各ジョブ完了後の自動消去プログラム
- 全データエリア消去プログラム
- アドレス帳/本体内登録データ消去プログラム
- ドキュメントファイリングデータ消去プログラム
- ジョブ状況完了エリア消去プログラム
- 電源 ON 時の自動消去プログラム

各プログラムとも HDD にはランダム値を 1 回以上上書きする。また, Flash メモリには固定値を 1 回上書きする。HDD 上書き回数は本 TSF の設定に従う。

以下、各プログラムおよびその設定について記述する。

6.1.3.1 各ジョブ完了後の自動消去プログラム

本プログラムは以下の通り、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イメージデータを、当該ジョブ完了時に上書き消去する。
- ドキュメントファイリング機能 (親展ファイル機能を含む) により HDD に保存されたイメージデータを、利用者の操作により削除される際に上書き消去する。

いずれの場合も、本プログラムは所定のタイミングで必ず起動され、非活性化する手段は提供されない。

6.1.3.2 全データエリア消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者により操作パネルにて起動され、以下のデータを上書き消去する。

- HDD 上にあるすべてのスプールイメージデータ
- HDD 上にあるすべてのファイリングイメージデータ
- HDD 上にあるジョブ完了記録データ
- Flash メモリ上にあるすべてのスプールイメージデータ

本プログラムは、アドレス帳データは消去しない。

本プログラムは中止機能を持つ。本プログラムを途中で中止する場合、キャンセル操作を選択後、本 TSF は本プログラムを起動した管理者の認証を必ず要求する。認証入力中, 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。正しい入力が完了した場合のみ、上書き消去を中止する。

中止機能の認証入力において、連続して 3 回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

6.1.3.3 アドレス帳/本体内登録データ消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者の操作により, HDD 上のアドレス帳データを上書き消去する。

所要時間は比較的短いので、中止機能はない。

6.1.3.4 ドキュメントファイリングデータ消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者の操作により, HDD 上のイメージデータを上書き消去する。対象データは以下の選択肢から一つ以上を、起動時に管理者が指定する。

- HDD 上にあるすべてのスプールイメージデータ
- HDD 上にあるすべてのファイリングイメージデータ

本プログラムは、全データエリア消去と同様の中止機能を持つ。

6.1.3.5 ジョブ状況完了エリア消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者により操作パネルにて起動され, HDD 上のジョブ完了記録データを上書き消去する。所要時間は比較的短いので、中止機能はない。

6.1.3.6 電源 ON 時の自動消去プログラム

TOE の電源 ON 時に上書き消去を実行する。ただし、スキャナまたはファクス送信の予約ジョブがある場合、および、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。

本プログラムの有効または無効、すなわち、電源 ON 時に本プログラムを実行するか否かは、予め設定された値に従う。本プログラムを実行する際の消去対象データも同様である。

本プログラムの消去対象データは、上記の全データエリア消去の対象となるすべてのデータ、または指定された HDD のデータのいずれかである。指定可能な HDD のデータは、スプールイメージデータ、ファイリングイメージデータ、および、ジョブ完了記録データのうち一つ以上である。

本プログラムは、全データエリア消去と同様の中止機能を持つ。

6.1.3.7 データ消去設定

本 TSF は、上記の各プログラムに対し、以下の設定機能を提供する。

- 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プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。
- データエリア消去回数:
  全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、および、ジョブ状況完了エリア消去の各プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。
- 電源 ON 時の自動消去:
  電源 ON 時の自動消去プログラムの、対象別有効設定。既定値はすべて無効。
- 電源 ON 時の自動消去回数:
  電源 ON 時の自動消去プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。

上記の各設定は、TSF_AUT で識別認証された管理者のみ、問い合わせと改変が許される。

6.1.4 認証 (TSF_AUT)

本 TSF は、管理者パスワードにより管理者の識別認証を行う。管理者パスワードは、本 TSF で識別認証された管理者のみが変更でき、5 文字以上 32 文字以下の英数記号のみを許す。

管理者向け以外の機能は、管理者識別認証を経ることなく利用できる。

管理機能の起動操作、または、管理者ログイン操作によって管理者を識別し、かつ、正しい管理者パスワードによって管理者認証に成功した場合に限り、管理者向け機能へのインタフェースを提供する。なお、管理者ログイン操作とは、操作パネルまたは Web における、管理者識別と管理者パスワード認証を含む操作である。

操作パネルでの管理者パスワード入力時、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。

Web では、クライアントに対しパスワード形式の入力を指定する。これは、クライアントの Web ブラウザに対し、利用者が入力した文字を代替文字のような方式で隠蔽するよう要求する。

管理者パスワード認証において、連続して 3 回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

6.1.5 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 はコピー、プリンタドライバ、PC-Fax およびスキャン保存の各機能に、親展ファイル保存のインタフェースを提供し、親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることを検査する。

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 は利用者に親展ファイル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 (星型記号) を表示するが、入力した文字は表示しない。本 TSF は、親展ファイルパスワードが入力され、かつ、保存の際に設定された親展ファイル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、親展ファイルパスワードが入力され、かつ、保存の際に設定された親展ファイル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、再操作 (プレビューを含むすべて) を許す。本 TSF は親展ファイルパスワード入力の際、クライアントに対しパスワード形式の入力を指定する。これは、クライアントの Web ブラウザに対し、利用者が入力した文字を代替文字のような方式で隠蔽するよう要求する。

親展ファイルの再操作に先立つ親展ファイル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 は認証受付を停止し、当該親展ファイルをロックする。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。ロックの解除は、TSF_AUT で識別認証された管理者のみに許される。

本 TSF は再操作の一種として親展ファイルパスワード変更の機能を提供し、新パスワードが 5 文字以上 8 文字以下の数字であることを検査する。

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、親展ファイル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、親展ファイルパスワードを指定する必要があり、かつ親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることを検査する。

本 TSF は暗号化されたデータをクライアントの Web ブラウザへエクスポートする。本 TSF はまた、暗号化されたデータも暗号化されていないデータも共に、クライアントの Web ブラウザよりインポートする。

本 TSF は、ドキュメントファイリング機能に関し、以下の管理機能を持つ。これらはいずれも TSF_AUT で識別認証された管理者のみが実行できる。

- 親展ファイルによる保護の実効性を高めるための管理機能:
  - ドキュメントファイリング禁止設定: ジョブ種類別に各保存モードを禁止できる。親展でない (パスワードのない) モードをすべて禁止する設定が既定値であり、推奨値である。

- ホールド以外のプリントジョブ禁止設定: 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。出力された用紙が第三者に持ち去られるリスクの高い環境において推奨される。

- 親展ファイルのロックに関する管理機能:
  - 親展ファイルのロック解除: 親展ファイルパスワード認証失敗によりロックされた親展ファイルに対し、ロックを解除する。本管理機能は “ファイル/フォルダ操作禁止の解除” の名称で提供される。

6.1.6 ネットワーク保護機能 (TSF_FNP)

本 TSF は以下の各要素からなる。

- フィルタ機能
- 通信データ保護機能
- ネットワーク設定保護

以下、各要素について記述する。

6.1.6.1 フィルタ機能

管理者による事前の設定に基づき、意図しない通信相手との通信を拒絶する。IP アドレスによる条件と MAC アドレスによる条件を設定できる。本 TSF は、条件に合わない通信相手からのネットワークパケットを、必ず破棄し、レスポンスおよび処理をしない。本機能の設定は TSF_AUT で識別認証された管理者のみが実行できる。

IP アドレスによる条件は、範囲を四つまで指定し、それらを許可するかまたは拒否するかを指定する。

MAC アドレスによる条件は、許可する MAC アドレスを 10 個まで指定する。

6.1.6.2 通信データ保護機能

クライアントと TOE の Web との通信を、盗聴より保護するために、HTTPS 通信機能を提供する。また、クライアントのプリンタドライバから送信される印刷データを、盗聴より保護するために、IPP-SSL 通信機能を提供する。

HTTPS 通信は、クライアントの Web ブラウザからの接続で開始し、切断されるまで通信を維持する。
IPP-SSL 通信も同様にクライアントのプリンタドライバからの接続で開始し、切断されるまで通信を維持する。

採用される暗号アルゴリズムは RSA, DES, Triple-DES, AES および SHA-1 である。管理者の設定によって、サーバ秘密鍵と公開鍵がインストールされる。

HTTPS 通信および IPP-SSL 通信の管理機能である SSL 設定は、TSF_AUT で識別認証された管理者のみが実行でき、HTTPS 通信および IPP-SSL 通信の使用/未使用 (無効) の設定によって、ネットワーク保護機能の動作を変更することができる。

HTTPS 通信および IPP-SSL 通信を未使用にした場合、ネットワーク保護機能は各々が無効の状態で動作する。

6.1.6.3 ネットワーク設定保護

2.5.5 節に記述したネットワーク設定データを扱うインタフェースを、操作パネルおよび TOE の Web で提供する。これらのインタフェースは管理者のみに対して提供し、他の利用者のアクセスより保護する。そのために、本 TSF はネットワーク設定データを扱うインタフェースの提供に先立ち、TSF_AUT と同様の識別認証を実施する。

6.2 TSF セキュリティ機能強度

確率的または順列的メカニズムに基づく TSF は以下の通り。

- 管理者パスワード: FIA_AFL.1 (1), FIA_SOS.1 (1), FIA_UAU.2 (1) および FIA_UAU.7 (1) に対応し、認証 (TSF_AUT) 機能、データ消去 (TSF_FDC) 機能、および、ネットワーク保護 (TSF_FNP) 機能により実現される。
- 親展ファイルパスワード: FIA_AFL.1 (2), FIA_SOS.1 (2), FIA_UAU.2 (2) および FIA_UAU.7 (2) に対応し、親展ファイル (TSF_FCF) 機能により実現される。

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。

6.3 保証手段

本 ST におけるセキュリティ保証要件の各コンポーネントに対し、その保証手段となる文書等を表 6.2 に示す。本 ST で使用する各保証手段の略称を、表中にブラケット [ ] 囲みで示す。

表 6.2: 保証手段

コンポーネント	保証手段
ACM_CAP.2	CM2510250 CM4010250 構成管理説明書 [CMC] CM2510250 Version M.10 構成リスト [CL]
ADO_DEL.1	CM2510250 CM4010250 配付手順説明書 [DEL]
ADO_IGS.1	CM2510250 Installation Manual [MI]
ADV_FSP.1	CM2510250 CM4010250 セキュリティ機能仕様書 [FSP]
ADV_HLD.1	CM2510250 CM4010250 上位レベル設計書 [HLD]
ADV_RCR.1	CM2510250 CM4010250 表現対応分析書 [RCR]
ADV_SPM.1	CM2510250 CM4010250 セキュリティ方針モデル仕様書 [SPM]
AGD_ADM.1 AGD_USR.1	CM2510250 Operation Manual Data Security Kit [MDSK] CM2510250 Data Security Kit Notice [NOTICE]
ATE_COV.1	CM2510250 CM4010250 カバレージ分析書 [COV]
ATE_FUN.1	CM2510250 機能テスト仕様書 [FUN] CM2510250 CM4010250 テスト環境・ツール説明書 [TT]
ATE_IND.2	TOE
AVA_SOF.1	CM2510250 CM4010250 セキュリティ機能強度分析書 [SOF]
AVA_VLA.1	CM2510250 CM4010250 脆弱性分析書 [VLA]

7 PP 主張

本 TOE が適合する PP はない。

8 根拠

本章は、本 ST 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前提条件、脅威、組織のセキュリティ方針に対して、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、前提条件、脅威、組織のセキュリティ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

TOE セキュリティ環境 / セキュリティ対策方針	A.NETWORK	A.OPERATOR	T.RECOVER	T.REMOTE	T.SPOOF	T.TAMPER	T.TAP	P.RESIDUAL
O.FILTER				8.1.4				
O.MANAGE				8.1.4	8.1.5	8.1.6	8.1.7	8.1.8
O.REMOVE			8.1.3					
O.RESIDUAL								8.1.8
O.TRP							8.1.7	
O.USER					8.1.5			
OE.CIPHER (1)							8.1.7	
OE.CIPHER (2)							8.1.7	
OE.ERASEALL								8.1.8
OE.FIREWALL	8.1.1							
OE.OPERATE		8.1.2						
OE.PC-USER				8.1.4				
OE.SUBNET	8.1.1							
OE.USER					8.1.5			

8.1.1 A.NETWORK

前提条件 A.NETWORK は、TOE を設置する MFD を内部ネットワークに接続し、その内部ネットワークが外部ネットワークからの攻撃から保護され、かつ、内部ネットワーク内において少なくとも MFD と同じサブネットワークには MFD との通信を認める機器だけが接続されることを求めている。これは OE.FIREWALL と OE.SUBNET の組み合わせにより実現できる。

8.1.2 A.OPERATOR

A.OPERATOR は、管理者が信頼できることを求めており、OE.OPERATE は、TOE を搭載した MFD を所有する組織の責任者が、管理者の役割を理解した上で、管理者の人選は厳重に行うことにより実施できる。

8.1.3 T.RECOVER

T.RECOVER に対して、O.REMOVE が定める通り、TOE は、利用者データを MSD に書き込む際、MFD 固有の鍵により暗号化する。これにより、低レベルの攻撃者が、MSD 上に保存されている、または、削除後に残存している情報を読み出すことができたとしても、意味のあるものとして判読できない。

なお、MFD のメモリ (揮発性メモリ) を取り外すとデータは消失し (揮発性メモリは通電の遮断によってすべての記憶データが消失するため), また MFD 稼動中に直接メモリ上のデータを読み出すためのインタフェースは存在せず、MFD の端子や配線などに直接プローブを当ててデータを読み出すにはデータ領域や転送中データの特定などの高度な技術力を必要とするため、低レベルの攻撃者の技術能力では不可能である。このため揮発性メモリに保存している暗号鍵を読み出すことはできない。

よって、上記の各対策により HDD および Flash メモリ内の情報漏えいが防止できる。

8.1.4 T.REMOTE

T.REMOTE に対して、以下のように対抗する。

- O.FILTER が定める通り、TOE は、MFD へのアクセスを認められていない利用者が使用する機器からのネットワーク経由アクセスを拒否する手段を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- OE.PC-USER が定める通り、管理者は、内部ネットワーク上で上記手段により拒否されず MFD への接続を認める機器において、MFD の正当な利用者のみが利用できるよう、許可利用者を識別認証する機能を動作させる。

これらの対策により、MFD へのアクセスを認められていない攻撃者が、内部ネットワーク経由で MFD にアクセスすることを防ぎ、MFD 内のアドレス帳データを保護することができる。

8.1.5 T.SPOOF

T.SPOOF に対して、以下のように対抗する。

- O.USER が定める通り、TOE は、正当な親展ファイル保存者を識別認証する機能を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- 正当な親展ファイル保存者の識別認証に必要な親展ファイルパスワードは、漏れないよう安全に管理されなければならない。これは OE.USER が定める通り、管理者が TOE および MFD の利用者に行わせる。

これらの対策により、攻撃者が、正当な利用者になりすますことにより生ずる脅威に対抗できる。

8.1.6 T.TAMPER

T.TAMPER に対して、O.MANAGE が定める通り、TOE は正当な管理者を識別認証する機能を提供する。これにより、攻撃者が管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを読み出しまたは改変することを防止できる。

8.1.7 T.TAP

T.TAP に対して、以下のように対抗する。

- O.TRP が定める通り、TOE は、内部ネットワーク上を流れる利用者データを盗聴より保護する機能を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- OE.CIPHER (1) が定める通り、管理者は、MFD の利用者が TOE と通信する際に TOE の通信データ保護機能が働くよう、TOE を設定することにより、通信データを盗聴より保護する。
- OE.CIPHER (2) が定める通り、管理者は、MFD の利用者が TOE と通信する際、TOE が設置される内部ネットワーク環境下において、通信データを盗聴より保護するための必要な措置 (暗号化スイッチを設置する、データの受け渡しに USB メモリを使用させる、等) を実施する。これは、クライアントあるいはプロトコルが対応しない等の事情により TOE の通信データ保護機能が使用できない場合において必要である。

表 8.2: TOE セキュリティ機能要件根拠

対策方針 要件	O.FILTER	O.MANAGE	O.REMOVE	O.RESIDUAL	O.TRP	O.USER
FCS_CKM.1			8.2.1.3			
FCS_COP.1			8.2.1.3			
FDP_RIP.1				8.2.1.4		
FIA_AFL.1 (1)		8.2.1.2				
FIA_AFL.1 (2)						8.2.1.6
FIA_SOS.1 (1)		8.2.1.2				
FIA_SOS.1 (2)						8.2.1.6
FIA_UAU.2 (1)		8.2.1.2				
FIA_UAU.2 (2)						8.2.1.6
FIA_UAU.7 (1)		8.2.1.2				
FIA_UAU.7 (2)						8.2.1.6
FIA_UID.2 (1)		8.2.1.2				
FIA_UID.2 (2)						8.2.1.6
FMT_MOF.1 (1)				8.2.1.4		
FMT_MOF.1 (2)				8.2.1.4		
FMT_MOF.1 (3)				8.2.1.4	8.2.1.5	8.2.1.6
FMT_MSA.2			8.2.1.3			
FMT_MTD.1 (1)		8.2.1.2				
FMT_MTD.1 (2)						8.2.1.6
FMT_MTD.1 (3)	8.2.1.1			8.2.1.4	8.2.1.5	8.2.1.6
FMT_SMF.1	8.2.1.1	8.2.1.2			8.2.1.5	8.2.1.6
FMT_SMR.1 (1)		8.2.1.2				
FMT_SMR.1 (2)						8.2.1.6
FPT_RVM.1	8.2.1.1	8.2.1.2	8.2.1.3	8.2.1.4	8.2.1.5	8.2.1.6
FTA_TSE.1	8.2.1.1					
FTP_TRP.1					8.2.1.5	

これらの対策により、正当な利用者が MFD に対して通信する際、攻撃者が内部ネットワーク上を流れる利用者データを盗聴することを防止できる。

8.1.8 P.RESIDUAL

P.RESIDUAL は、以下の対策により実施できる。

- O.RESIDUAL が定める通り、TOE は、ジョブ完了または中止時、MSD にスプール保存された利用者データの領域を、少なくとも 1 回上書き消去する。
- O.RESIDUAL が定める通り、TOE は、利用者の削除操作により、指定された MSD の利用者データの領域を、少なくとも 1 回上書き消去する。
- OE.ERASEALL が定める通り、管理者は、MFD の廃棄または所有者変更の際、MSD の利用者データ領域全体を少なくとも 1 回上書き消去する。そのためには TOE の支援が必要であり、次項の機能が利用できる。
- O.RESIDUAL が定める通り、TOE は、管理者の操作により MSD の利用者データ領域全体を少なくとも 1 回上書き消去する機能を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。

これらの対策により、P.RESIDUAL は実施可能である。

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 セキュリティ機能要件根拠

セキュリティ機能要件と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、セキュリティ機能要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。

8.2.1.1 O.FILTER

O.FILTER は、以下の機能要件の組み合わせにより実現できる。

- FTA_TSE.1 にて、TOE は、IP アドレスおよび MAC アドレスに基づき、セション確立を拒否できる。
- FMT_SMF.1 にて、TOE は、前項の運用に必要な、IP アドレスフィルタおよび MAC アドレスフィルタの管理機能を行う能力を提供する。
- FMT_MTD.1 (3) にて、前項の IP アドレスフィルタおよび MAC アドレスフィルタを、問い合わせまたは改変する能力は、管理者に制限される。
- FPT_RVM.1 にて、セション確立が許可される前に、IP アドレスおよび MAC アドレスの検査が必ず呼び出され、成功することが保証される。また、FMT_MTD.1 (3) を迂回できないようにサポートする。

上記 FMT_SMF.1 と FMT_MTD.1 (3) は一貫して FTA_TSE.1 の管理を規定し、これらの間で競合は発生しない。また、FPT_RVM.1 は相互サポートのための機能要件であるので競合は発生しない。以上から、O.FILTER を実現する上で、機能要件の競合は発生しない。

8.2.1.2 O.MANAGE

O.MANAGE は、以下の機能要件の組み合わせにより実現できる。

a) FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) によって、管理者を識別および認証する。

b) FMT_SMF.1 にて、TOE は、上記の管理者認証の運用に必要な、管理者パスワードの改変を行う能力を提供する。

c) FIA_SOS.1 (1) により、管理者パスワードを改変する際、管理者パスワードが 5 文字以上 32 文字以下の英数記号であることが保証される。

d) FMT_MTD.1 (1) にて、O.MANAGE を実施する TSF データである管理者パスワードを改変する能力は、管理者のみに制限される。

e) FMT_SMR.1 (1) にて、管理者の役割は維持され、管理者はその役割に関連づけられる。

f) FPT_RVM.1 により O.MANAGE を実現する各機能要件を迂回できないようにサポートする。

上記 a) は管理者識別認証の事象に関するものであり、b), c) および d) は管理者パスワード改変の事象に関するものである。これら二つの事象は独立に発生し、相互に競合しない。a) の四つの機能要件は、管理者識別認証を実施するために相互補完的に作用するので、競合は発生しない。b), c) および d) の三つの機能要件は、管理者パスワード改変を実施するために相互補完的に作用するので、競合は発生しない。e) は d) の依存性の要件であり a) にサポートされるので、競合は発生しない。f) は相互サポートのための機能要件であるので競合は発生しない。以上から、O.MANAGE を実現する上で、機能要件の競合は発生しない。

8.2.1.3 O.REMOVE

O.REMOVE の目的は T.RECOVER への対抗であり、すなわち MFD から MSD を取り出されたとしても、MSD に保存されたデータが再生されないようにすることである。これは、以下の機能要件の組み合わせにより実現できる。

a) FCS_COP.1 により、以下の通り MSD に保存されたデータを保護する。

- FCS_COP.1 により保存される利用者データが暗号化されるため、MSD への保存を実行した MFD 自身以外に MSD を接続して利用者データの再生を試みても、利用者データの再生は阻止される。
- 利用者データと同様に、FCS_COP.1 により、TSF データに含まれる管理者パスワードおよび親展ファイルパスワードもまた、HDD に保存される際に暗号化される。そのため、攻撃者がこれらのパスワードを読み出して、なりすましを謀ることによる、間接的な利用者データの読み出しもまた阻止される。

b) FCS_CKM.1 により、FCS_COP.1 を実施するための暗号鍵を生成する。

c) 暗号鍵のシードは、TOE 自身が生成したものであり、FMT_MSA.2 によりセキュアなセキュリティ属性として受け入れられる。

d) FPT_RVM.1 により、O.REMOVE を実現する各機能要件を迂回できないようにサポートする。

上記 FCS_CKM.1 と FMT_MSA.2 は、FCS_COP.1 の依存性の要件なので競合は発生しない。
FPT_RVM.1 は相互サポートのための要件であるので競合は発生しない。以上から、O.REMOVE を達成する上で機能要件の競合は発生しない。

8.2.1.4 O.RESIDUAL

O.RESIDUAL は、以下の機能要件の組み合わせにより実現できる。

a) FDP_RIP.1 によって、以下のオブジェクトからの資源の割当て解除において、それらの領域に対し少なくとも 1 回以上上書き消去する。

- 対象となるオブジェクトは、HDD 上のスプールイメージデータファイル、HDD 上のファイリングイメージデータファイル、HDD 上のアドレス帳データファイル、HDD 上のジョブ完了記録データファイル、および、Flash メモリ上のスプールイメージデータファイルである。
- それらのオブジェクトからの資源の割当て解除が発生するのは、ジョブ完了または中止時、利用者の親展ファイル削除操作時、および、管理者の操作により特定のデータ消去機能のプログラムが実行されたときである。
- 前項で述べたプログラムは、全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去である。

b) 以下の各機能要件にて、FDP_RIP.1 に関する管理能力は、管理者に制限される。

- FMT_MOF.1 (1) にて、FDP_RIP.1 に関する TSF のうち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、アドレス帳/本体内登録データ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去の各機能を動作させる能力が、管理者に制限される。
- FMT_MOF.1 (2) にて、FDP_RIP.1 に関する TSF のうち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、および、電源 ON 時の自動消去の各機能を停止する能力が、管理者に制限される。
- FMT_MOF.1 (3) にて、FDP_RIP.1 に関する TSF のうちドキュメントファイリングデータ消去機能および電源 ON 時の自動消去機能のふるまいを改変する能力が、管理者に制限される。
- FMT_MTD.1 (3) にて、FDP_RIP.1 に関する TSF データ、すなわち、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 時の自動消去の対象別有効設定、および、電源 ON 時の自動消去回数を、問い合わせまたは改変する能力は、管理者に制限される。

c) FPT_RVM.1 により O.RESIDUAL を実現する各機能要件を迂回できないようにサポートする。

上記 b) の各事象は独立事象であり、それらは a) の管理であるので、a) および b) の各事象が相互に競合することはない。また、a) および b) は各独立事象に対し各々ただ一つの機能要件が対応するので、機能要件の競合はあり得ない。上記 c) は相互サポートのための機能要件であるので競合は発生しない。以上から、O.RESIDUAL を実現する上で、機能要件の競合は発生しない。

8.2.1.5 O.TRP

O.TRP は、以下の機能要件の組み合わせにより実現できる。

- FTP_TRP.1 により、利用者と TSF 間に高信頼通信を確立し、維持することができる。
- FMT_MOF.1 (3) により、FTP_TRP.1 に関する TSF すなわちネットワーク保護機能のふるまいを改変する能力は、管理者に制限される。
- FMT_MTD.1 (3) により、FTP_TRP.1 に関する TSF データ、すなわち SSL 設定を問い合わせまたは改変する能力は、管理者に制限される。
- FMT_SMF.1 により、その運用管理が可能となる。
- FPT_RVM.1 により、O.TRP を実現する各機能要件を迂回できないようにサポートする。

上記 FMT_MOF.1 (3), FMT_MTD.1 (3) および FMT_SMF.1 は相互補完的に FTP_TRP.1 の管理を規定し、これらの間で競合は発生しない。また、FPT_RVM.1 は相互サポートのための機能要件であるので競合は発生しない。以上から、O.TRP を実現する上で、機能要件の競合は発生しない。

8.2.1.6 O.USER

O.USER は、以下の機能要件の組み合わせにより実現できる。

a) FIA_AFL.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) および FIA_UID.2 (2) によって、親展ファイル保存者を識別認証する。これにより、親展ファイルへのアクセス (親展ファイルパスワード管理を含む) が、親展ファイル保存者にのみ可能となる。

b) FIA_SOS.1 (2) により、親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることが保証される。

c) FMT_MOF.1 (3) にて、O.USER を実施するドキュメントファイリング機能 (親展ファイル機能を含む) のふるまいを改変する能力が、管理者に制限される。

d) FMT_MTD.1 (2) にて、親展ファイルパスワードを変更する能力は、親展ファイル保存者のみに制限される。

e) FMT_MTD.1 (3) にて、親展ファイルによる保護の実効性に関わる TSF のふるまい管理能力、すなわち、ドキュメントファイリング禁止設定およびホールド以外のプリントジョブ禁止設定を、問い合わせまたは改変する能力は、管理者に制限される。

f) FMT_SMR.1 (2) にて、親展ファイル保存者の役割は維持され、親展ファイルを保存した利用者はその役割に関連づけられる。

g) FMT_SMF.1 により、親展ファイルパスワードの管理運用が可能となる。

h) FPT_RVM.1 により、O.USER を実現する各機能要件を迂回できないようにサポートする。

上記 a) は親展ファイル保存者識別認証の事象に関するものであり、b), d) および g) は親展ファイルパスワード変更の事象に関するものであり、c) および e) は管理者による管理の事象に関するものである。これら三つの事象は独立に発生し、相互に競合しない。a) の四つの機能要件は、親展ファイル保存者識別認証を実施するために相互補完的に作用するので、競合は発生しない。b), d), および g) の三つの機能要件は、親展ファイルパスワード改変を実施するために相互補完的に作用するので、競合は発生しない。c) および e) の二つの機能要件は、管理者による管理を実施するために相互補完的に作用するので、競合は発生しない。f) は d) の依存性の要件であり a) にサポートされるので、競合は発生しない。h) は相互サポートのための機能要件であるので競合は発生しない。以上から、O.USER を実現する上で、機能要件の競合は発生しない。

8.2.2 TOE セキュリティ管理機能の一貫性根拠

TOE セキュリティ機能要件のいくつかは、セキュリティ管理機能を必要とする。[CC_PART2] は各機能コンポーネントに予見される管理アクティビティ (management activities foreseen) を、各コンポーネントの管理要件 (management requirements) として提案している。

表 8.3 は、すべての TOE セキュリティ機能要件コンポーネントについて、そのコンポーネントが必要とする管理機能を、管理要件への考慮とともに示す。FMT_SMF.1 が特定する管理機能と、表中で示された必要な管理機能とは、一致している。

よって、TOE セキュリティ要件は、セキュリティ管理機能に関し、内部的に一貫している。

表 8.3: TOE の管理機能

管理機能 被管理要件	必要な管理機能	管理要件への考慮
FCS_CKM.1	—	暗号鍵の属性は変更しない
FCS_COP.1	—	(管理要件なし)
FDP_RIP.1	• 全データエリア消去の起動および中止 • ドキュメントファイリングデータ消去の起動および中止 • 電源ON時の自動消去の中止 • アドレス帳/本体内登録データ消去の起動 • ジョブ状況完了エリア消去の起動 • 各ジョブ完了後の自動消去回数の設定 • データエリア消去回数の設定 • 電源ON時の自動消去の対象別有効設定 • 電源ON時の自動消去回数の設定	残存情報保護の実施タイミングは、割当て解除時に固定
FIA_AFL.1 (1)	—	閾値とアクションは固定
FIA_AFL.1 (2)	• 親展ファイルのロック解除	閾値とアクションは固定
FIA_SOS.1 (1)	—	品質尺度は固定
FIA_SOS.1 (2)	—	品質尺度は固定
FIA_UAU.2 (1)	• 管理者パスワードの改変	管理要件に合致
FIA_UAU.2 (2)	• 親展ファイルパスワードの改変 • ドキュメントファイリング禁止設定 • ホールド以外のプリントジョブ禁止設定	管理要件に合致
FIA_UAU.7 (1)	—	(管理要件なし)
FIA_UAU.7 (2)	—	(管理要件なし)
FIA_UID.2 (1)	—	管理者の識別は固定
FIA_UID.2 (2)	—	各親展ファイル保存者の識別は固定
FMT_MOF.1 (1)	—	役割のグループはない
FMT_MOF.1 (2)	—	役割のグループはない
FMT_MOF.1 (3)	—	役割のグループはない
FMT_MSA.2	—	(管理要件なし)
FMT_MTD.1 (1)	—	役割のグループはない
FMT_MTD.1 (2)	—	役割のグループはない
FMT_MTD.1 (3)	—	役割のグループはない
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1 (1)	—	利用者のグループはない
FMT_SMR.1 (2)	—	利用者のグループはない
FPT_RVM.1	—	(管理要件なし)
FTA_TSE.1	• IPアドレスフィルタおよびMACアドレスフィルタの管理	管理要件に合致
FTP_TRP.1	• SSL保護対象サービスの管理	管理要件に合致

8.2.3 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 8.4 に示す。表 8.4 は、CC が規定するセキュリティ機能要件が満足すべき依存性と、本 TOE が満足している依存性、満足していない依存性、および本 TOE が依存性を満足していないことの正当性を記載している節番号を示したものである。表中で * を付された依存性は、それの上位階層関係にあるコンポーネントにより満足されている。

表 8.4: 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	正当性
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
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_SOS.1 (1)	—	—	—	—
FIA_SOS.1 (2)	—	—	—	—
FIA_UAU.2 (1)	FIA_UID.1 *	FIA_UID.2 (1)	—	—
FIA_UAU.2 (2)	FIA_UID.1 *	FIA_UID.2 (2)	—	—
FIA_UAU.7 (1)	FIA_UAU.1 *	FIA_UAU.2 (1)	—	—
FIA_UAU.7 (2)	FIA_UAU.1 *	FIA_UAU.2 (2)	—	—
FIA_UID.2 (1)	—	—	—	—
FIA_UID.2 (2)	—	—	—	—
FMT_MOF.1 (1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MOF.1 (2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MOF.1 (3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	ADV_SPM.1	FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	8.2.3.2
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 (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)	—	—
FPT_RVM.1	—	—	—	—
FTA_TSE.1	—	—	—	—
FTP_TRP.1	—	—	—	—

8.2.3.1 FCS_CKM.4 不満足の正当性

暗号鍵は揮発性メモリ内に保存している。電源断 (電源オフ) により、揮発性メモリ内の電荷が消失し、暗号鍵が破棄される。そのため、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。

8.2.3.2 FMT_MSA.2 の依存性不満足の正当性

暗号操作に関するセキュリティ属性である暗号鍵のシードは、TOE 自身が管理しており、管理者に対しても変更を許容していないため、FMT_MSA.1 および FMT_SMR.1 は必要がない。同様に、暗号鍵やシードを利用者および管理者からアクセスされることがなく、外部から受け入れることもないので、FDP_ACC.1 および FDP_IFC.1 はいずれも必要がない。

8.2.4 セキュリティ要件の相互作用

セキュリティ要件の相互作用の関係について表 8.5 に示す。

表 8.5: セキュリティ要件の相互作用

防御機能要件	迂回	非活性化
FCS_CKM.1	FPT_RVM.1	—
FCS_COP.1	FPT_RVM.1	—
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1 (2), FMT_MTD.1 (3)
FIA_AFL.1 (1)	FPT_RVM.1	—
FIA_AFL.1 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_SOS.1 (1)	FPT_RVM.1	—
FIA_SOS.1 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UAU.2 (1)	FPT_RVM.1	—
FIA_UAU.2 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UAU.7 (1)	FPT_RVM.1	—
FIA_UAU.7 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UID.2 (1)	FPT_RVM.1	—
FIA_UID.2 (2)	FPT_RVM.1	FMT_MOF.1 (3)
FMT_MOF.1 (1)	FPT_RVM.1	—
FMT_MOF.1 (2)	FPT_RVM.1	—
FMT_MOF.1 (3)	FPT_RVM.1	—
FMT_MSA.2	—	—
FMT_MTD.1 (1)	FPT_RVM.1	—
FMT_MTD.1 (2)	FPT_RVM.1	—
FMT_MTD.1 (3)	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1 (1)	—	—
FMT_SMR.1 (2)	—	—
FPT_RVM.1	—	—
FTA_TSE.1	FPT_RVM.1	—
FTP_TRP.1	FPT_RVM.1	FMT_MOF.1 (3)

8.2.4.1 迂回

表 8.5 に関し、以下に、各機能要件に対する迂回について述べる。

a) 暗号鍵生成 FCS_CKM.1 は、電源 ON 時に必ず呼び出され迂回できない。

b) 暗号操作 FCS_COP.1 は、利用者データおよび TSF データを MSD に書き込む前に必ず暗号化し、復号は読み出し後のみ実施され、いずれも迂回できない。

c) サブセット残存情報保護 FDP_RIP.1 は、ジョブ完了時、全データエリア消去操作時、アドレス帳/本体内登録データ消去操作時、ドキュメントファイリングデータ消去操作時、ジョブ状況完了エリア消去操作時、および、電源 ON 時に必ず呼び出されるため迂回できない。

d) 管理者の識別認証に関する FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) は、管理者の識別認証時に必ず呼び出されるため迂回できない。

e) 親展ファイル保存者の識別認証に関する FIA_AFL.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) および FIA_UID.2 (2) は、親展ファイル保存者の識別認証時に必ず呼び出されるため迂回できない。

f) 秘密の検証 FIA_SOS.1 (1) は、管理者パスワードの変更 (改変) 時に必ず呼び出されるため迂回できない。

g) 秘密の検証 FIA_SOS.1 (2) は、親展ファイル保存時、親展ファイルパスワード変更 (改変) 時、および、親展ファイル以外の親展への属性変更に必ず呼び出されるため迂回できない。

h) セキュリティ機能のふるまい管理 FMT_MOF.1 (1) は、データ消去を動作させるための操作に先立ち、必ず管理者認証 FIA_UAU.2 (1) を経る必要があり迂回できない。

i) セキュリティ機能のふるまい管理 FMT_MOF.1 (2) は、データ消去を停止させるための操作に先立ち、必ず管理者認証 FIA_UAU.2 (1) が呼び出されるため迂回できない。

j) セキュリティ機能のふるまい管理 FMT_MOF.1 (3) は、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、ドキュメントファイリング機能、および、ネットワーク保護機能のふるまいを改変するための操作に先立ち、必ず管理者認証 FIA_UAU.2 (1) を経る必要があり迂回できない。

k) TSF データの管理 FMT_MTD.1 (1) は、必ず管理者認証 FIA_UAU.2 (1) を経る必要があり迂回できない。

l) TSF データの管理 FMT_MTD.1 (2) は、必ず親展ファイル保存者認証 FIA_UAU.2 (2) を経る必要があり迂回できない。

m) TSF データの管理 FMT_MTD.1 (3) は、必ず管理者認証 FIA_UAU.2 (1) を経る必要があり迂回できない。

n) TOE セション確立 FTA_TSE.1 は、ネットワーク I/F がネットワークパケットを検出した際に必ず呼び出されるため迂回できない。

o) 高信頼パス FTP_TRP.1 は、リモート利用者から高信頼パスの要求があれば必ず呼び出されるため迂回できない。

8.2.4.2 非活性化

表 8.5 に関し、以下に、各機能要件に対する非活性化について述べる。

- FDP_RIP.1 は、以下の通り、非活性化行為から保護される。
  - 全データエリア消去およびドキュメントファイリングデータ消去プログラムの停止は FMT_MOF.1 (2) により、管理者のみに制限される。
  - 電源 ON 時の自動消去プログラムを無効化する設定、および、停止は、各々FMT_MTD.1 (3) および FMT_MOF.1 (2) によりいずれも管理者のみに制限される。
- FIA_AFL.1 (2), FIA_SOS.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) および FIA_UID.2 (2) は、以下の通り、非活性化行為から保護される。
  - ドキュメントファイリング機能のふるまい改変は FMT_MOF.1 (3) により、管理者のみに制限される。
- FTP_TRP.1 は、以下の通り、非活性化行為から保護される。
  - ネットワーク保護機能のふるまい改変は FMT_MOF.1 (3) により、管理者のみに制限される。

8.2.4.3 干渉

本 TOE は、管理者のみにセキュリティ機能のふるまい管理を許可しているだけである。このため、不正なサブジェクトが存在せずアクセス制御の必要はなく、TSF が破壊されることはない。

8.2.5 最小機能強度根拠

本 TOE は、一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃である。このため、攻撃者の攻撃力は “低レベル” である。本 TOE の最小機能強度レベルは *SOF-基本* であり、これにより低レベルの攻撃能力を持つ攻撃者からの公開情報を利用した不正行為に対抗できる。FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.2 (1), FIA_UAU.2 (2), FIA_UAU.7 (1) および FIA_UAU.7 (2) の明示された機能強度はそれぞれ *SOF-基本* であり、最小機能強度と矛盾しない。

8.2.6 TOE セキュリティ保証要件根拠

本 TOE は、MFD の一部および MFD 用の別売オプション品、すなわち商用の製品である。また、主要な脅威は、低レベルの攻撃者が、MFD 内の MSD に、MFD 以外の装置を使用する物理的手段により MSD 内の情報を読み出し漏えいさせることである。このため本 TOE は、通常のオフィスで使用される商用の製品として、脅威からの保護に関する信頼性の確保について有意な保証を与える EAL2 + ADV_SPM.1 を評価保証レベルとする。ADV_SPM.1 については、機能要件 FMT_MSA.2 において、ADV_SPM.1 への依存性が示されているための選択である。表 5.1 に示す通り、すべての依存性は満足されている。

ADV_SPM.1 を除く保証要件は EAL2 のパッケージを適用しているので、各要件が相互に競合することはない。ADV_SPM.1 は TSP モデルという個別仕様の保証要件なので、他の要件との競合は発生しない。

8.3 TOE 要約仕様根拠

本節は、IT セキュリティ要件に対する、TOE セキュリティ機能とその保証手段の有効性を検証する。

8.3.1 TOE セキュリティ機能根拠

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

8.3.1.1 FCS_CKM.1

TSF_FKG は、MFD の電源投入時に MSN-R 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。MSN-R 拡張アルゴリズムは、シャープ株式会社のデジタル複合機に用いるデータセキュリティキット用暗号基準書に基づくアルゴリズムである。よって FCS_CKM.1 は満足される。

8.3.1.2 FCS_COP.1

FCS_COP.1 は、TSF_FDE による FIPS PUB 197 で規格化された AES Rijndael アルゴリズムに従い MSD に保存する利用者データおよび TSF データの暗号化、および復号を行うため、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プログラム実行時に, 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プログラム実行時に, MSD (HDD および 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およびジョブ完了記録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イメージデータの再生を不能とする。これを電源 ON 時の自動消去プログラム実行時に行うようにも設定できる。

TSF_FDC は、ドキュメントファイリングデータ消去プログラム実行時に、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イメージデータの再生を不能とする。これを電源 ON 時の自動消去プログラム実行時に行うようにも設定できる。

TSF_FDC は、ジョブ状況完了エリア消去プログラム実行時に、ジョブ完了記録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ジョブ完了記録データの再生を不能とする。これを電源 ON 時の自動消去プログラム実行時に行うようにも設定できる。

TSF_FDC は、アドレス帳/本体内登録データ消去プログラム実行時に、アドレス帳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アドレス帳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_AUT および TSF_FNP は管理者の識別認証を行う。TSF_FDC の中止機能は管理者認証を行う。これらはすべて 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)

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 回の失敗で認証受付を停止し、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_FCF 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 による認証を経た管理者にのみ許される。これにより FIA_AFL.1 (2) が満足される。

8.3.1.6 FIA_SOS.1 (1)

TSF_AUT による管理者パスワードの変更時、入力された新しい管理者パスワードが 5 文字以上 32 文字以下の英数記号であることを検査し、それ以外は受け付けない。これにより FIA_SOS.1 (1) は満足される。

8.3.1.7 FIA_SOS.1 (2)

TSF_FCF による親展ファイルの保存時、親展ファイルパスワード変更時、および、親展ファイル以外の親展への属性変更時において、入力された親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることを検査し、それ以外は受け付けない。これにより FIA_SOS.1 (2) は満足される。

8.3.1.8 FIA_UAU.2 (1)

TSF_AUT は管理者向け機能の操作に先立ち、管理者パスワード入力による認証を行う。TSF_FNP はネットワーク設定データを扱うインタフェースの提供に先立ち、管理者パスワード入力による認証を行う。TSF_FDC は、全データリア消去、ドキュメントファイリングデータ消去、および、電源 ON 時の自動消去を中止する際、管理者パスワード入力による認証を行う。これらにより FIA_UAU.2 (1) は満足される。

8.3.1.9 FIA_UAU.2 (2)

TSF_FCF は親展ファイル再操作の際、親展ファイルパスワード入力による認証を行う。よって FIA_UAU.2 (2) は満足される。

8.3.1.10 FIA_UAU.7 (1)

TSF_AUT および TSF_FNP は、管理者認証中における保護されたフィードバックとして、入力文字数に応じた代替文字のみを表示する。また、TSF_FDC の中止機能による管理者認証も同様である。これらにより FIA_UAU.7 (1) は満足される。

8.3.1.11 FIA_UAU.7 (2)

TSF_FCF は、親展ファイルパスワード認証中における保護されたフィードバックとして、入力文字数に応じた代替文字を表示する。よって FIA_UAU.7 (2) は満足される。

8.3.1.12 FIA_UID.2 (1)

TSF_AUT は管理者向け機能の操作に先立ち、管理者の識別操作を必要とする。TSF_FNP はネットワーク設定データを扱うインタフェースの提供に先立ち、管理者の識別操作を必要とする。TSF_FDC による全データリア消去、ドキュメントファイリングデータ消去、および、電源 ON 時の自動消去の中止操作は、管理者識別に相当する。これらにより FIA_UID.2 (1) は満足される。

8.3.1.13 FIA_UID.2 (2)

TSF_FCF による親展ファイル再操作時には、親展ファイルを選択する操作が必要であり、これは親展ファイル保存者の識別に相当する。よって FIA_UID.2 (2) は満足される。

8.3.1.14 FMT_MOF.1 (1)

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、アドレス帳/本体内登録データ消去、および、ジョブ状況完了エリア消去を起動するインタフェースを、管理者のみに提供する。電源 ON 時の自動消去を有効化する設定も同様である。これらにより FMT_MOF.1 (1) は満足される。

8.3.1.15 FMT_MOF.1 (2)

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、および、電源 ON 時の自動消去を中止するインタフェースを、管理者のみに提供する。電源 ON 時の自動消去を無効化する設定も同様である。これらにより FMT_MOF.1 (2) は満足される。

8.3.1.16 FMT_MOF.1 (3)

TSF_FDC は、ドキュメントファイリングデータ消去のふるまいを改変する、すなわち対象データを選択するインタフェースを、ドキュメントファイリングデータ消去起動時に管理者のみに提供する。

TSF_FDC は、電源 ON 時の自動消去のふるまいを改変するインタフェースである、データ消去設定 (6.1.3.7 節) における “電源 ON 時の自動消去” の設定機能を、管理者のみに提供する。

TSF_FCF は、ドキュメントファイリング機能のふるまいを改変するインタフェースである、“ドキュメントファイリング禁止設定” 機能、および “ホールド以外のプリントジョブ禁止” 機能を、管理者のみに提供する。

TSF_FNP は、ネットワーク保護機能のふるまいを改変するインタフェースである SSL 設定機能を、管理者のみに提供する。

以上により FMT_MOF.1 (3) は満足される。

8.3.1.17 FMT_MSA.2

FMT_MSA.2 は、ADV_SPM.1 に、必ずセキュアなシードを元に暗号鍵が生成されることが説明されており、暗号鍵生成 TSF_FKG により FMT_MSA.2 が満足される。

8.3.1.18 FMT_MTD.1 (1)

FMT_MTD.1 (1) は、TSF_AUT により識別認証された管理者が、TSF_AUT による管理者パスワードの改変を可能とするため、満足される。

8.3.1.19 FMT_MTD.1 (2)

TSF_FCF による親展ファイルパスワードを改変するインタフェースは、TSF_FCF により識別認証された親展ファイル保存者に提供し、それ以外には提供しない。

TSF_FCF による親展ファイルパスワードを作成するインタフェースは、親展ファイルを保存するときと、TSF_FCF により識別認証された親展ファイル保存者が属性を親展に変更するときに提供し、それ以外には提供しない。

これらにより FMT_MTD.1 (2) は満足される。

8.3.1.20 FMT_MTD.1 (3)

IP アドレスフィルタを問い合わせおよび改変するインタフェースは TSF_FNP により提供される。

MAC アドレスフィルタを問い合わせおよび改変するインタフェースは TSF_FNP により提供される。

SSL 設定を問い合わせおよび改変するインタフェースは TSF_FNP により提供される。

各ジョブ完了後の自動消去回数を問い合わせおよび改変するインタフェースは TSF_FDC により提供される。

データエリア消去回数を問い合わせおよび改変するインタフェースは TSF_FDC により提供される。

電源 ON 時の自動消去の対象別有効設定を問い合わせおよび改変するインタフェースは TSF_FDC により提供される。

電源 ON 時の自動消去回数を問い合わせおよび改変するインタフェースは TSF_FDC により提供される。

ドキュメントファイリング禁止設定を問い合わせおよび改変するインタフェースは TSF_FCF により提供される。

ホールド以外のプリントジョブ禁止設定を問い合わせおよび改変するインタフェースは TSF_FCF により提供される。

上記の各インタフェースは、TSF_AUT により識別認証された管理者のみに提供されるので、FMT_MTD.1 (3) は満足される。

8.3.1.21 FMT_SMF.1

TSF_FDC は全データエリア消去の起動および中止を行う能力を持っている。

TSF_FDC はドキュメントファイリングデータ消去の起動および中止を行う能力を持っている。

TSF_FDC は電源 ON 時の自動消去の中止を行う能力を持っている。

TSF_FDC はアドレス帳/本体内登録データ消去の起動を行う能力を持っている。

TSF_FDC はジョブ状況完了エリア消去の起動を行う能力を持っている。

TSF_FDC は各ジョブ完了後の自動消去回数の設定を行う能力を持っている。

TSF_FDC はデータエリア消去回数の設定を行う能力を持っている。

TSF_FDC は電源 ON 時の自動消去の対象別有効設定を行う能力を持っている。

TSF_FDC は電源 ON 時の自動消去回数の設定を行う能力を持っている。

TSF_FCF は親展ファイルのロック解除を行う能力を持っている。

TSF_AUT は管理者パスワードの改変を行う能力を持っている。

TSF_FCF は親展ファイルパスワードの改変を行う能力を持っている。
TSF_FCF はドキュメントファイリング禁止設定を行う能力を持っている。
TSF_FCF はホールド以外のプリントジョブ禁止設定を行う能力を持っている。
TSF_FNP は IP アドレスフィルタおよび MAC アドレスフィルタの管理を行う能力を持っている。
TSF_FNP は SSL 保護対象サービスの管理を行う能力を持っている。
以上により FMT_SMF.1 は満足される。

8.3.1.22 FMT_SMR.1 (1)

TSF_AUT は管理者の識別認証により、管理者を特定することで、役割への関連づけを行っている。また、管理者パスワードを変更 (改変) しても役割への関連づけ、および役割を維持し続ける。これらにより FMT_SMR.1 (1) は満足される。

8.3.1.23 FMT_SMR.1 (2)

TSF_FCF は親展ファイル保存者の識別認証により、親展ファイル保存者を特定することで、役割への関連づけを行っている。また、親展ファイルパスワードを変更 (改変) しても役割への関連づけ、および役割を維持し続ける。これらにより FMT_SMR.1 (2) は満足される。

8.3.1.24 FPT_RVM.1

8.2.4.1 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。

a) TSF_FKG は、MFD 電源 ON 時に必ず FCS_CKM.1 が定める通り暗号鍵を生成する。

b) TSF_FDE は MSD に利用者データまたは TSF データを書き込む際、必ず FCS_COP.1 が定める通り暗号化し、読み出した後の利用者データまたは TSF データに対してのみ復号する。

c) TSF_FDC は、各ジョブの完了または中止時、利用者の親展ファイル削除操作時、および、管理者のデータ消去操作時には、必ず FDP_RIP.1 に基づく上書き消去を実行する。
TSF_FDC は、電源 ON 時の自動消去を実行するよう、管理者の操作により設定されていれば、電源 ON 時には必ず FDP_RIP.1 に基づく上書き消去を実行する。

d) TSF_FDC, TSF_AUT および TSF_FNP は、管理者識別認証の際、FIA_UID.2 (1) に基づく管理者識別操作、FIA_UAU.2 (1) に基づく管理者パスワード認証、FIA_UAU.7 (1) に基づく管理者パスワードのフィードバック保護、および、FIA_AFL.1 (1) に基づく管理者パスワードロックを必ず実行する。
TSF_FDC は、TSF_FDC による管理者識別認証が呼び出され成功した場合に限り、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、および、電源 ON 時の自動消去の中止を許可する。
TSF_FDC, TSF_FCF および TSF_FNP は、TSF_AUT による管理者識別認証が呼び出され成功した場合に限り、管理者向け機能のインタフェースを提供する。
TSF_FNP は、TSF_FNP による管理者識別認証が呼び出され成功した場合に限り、ネットワーク設定データを扱うインタフェースを提供する。

e) TSF_FCF は、親展ファイル再操作に先立ち、FIA_UID.2 (2) に基づく親展ファイル選択操作、FIA_UAU.2 (2) に基づく親展ファイルパスワード認証、FIA_UAU.7 (2) に基づく親展ファイルパスワードのフィードバック保護、および、FIA_AFL.1 (2) に基づく親展ファイルロックを必ず実行する。

f) TSF_AUT は、管理者パスワードの変更時に必ず FIA_SOS.1 (1) が定める通り管理者パスワードが 5 文字以上 32 文字以下の英数記号であることを検証する。

g) TSF_FCF は、親展ファイル保存時、親展ファイルパスワード変更時、および、親展ファイル以外の親展への属性変更時に、必ず FIA_SOS.1 (2) が定める通りパスワードが 5 文字以上 8 文字以下の数字であることを検証する。

h) TSF_FDC は FMT_MOF.1 (1) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、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、アドレス帳/本体内登録データ消去、および、ジョブ状況完了エリア消去の各プログラムを起動するインタフェース、ならびに、電源 ON 時の自動消去プログラムを有効化するインタフェースを提供する。

i) TSF_FDC は FMT_MOF.1 (2) に則り、TSF_FDC による管理者認証が呼び出され成功した場合に限り、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および電源 ON 時の自動消去の中止を許可する。
TSF_FDC は同じく FMT_MOF.1 (2) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、電源 ON 時の自動消去プログラムを無効化するインタフェースを提供する。

j) TSF_FDC は FMT_MOF.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、ドキュメントファイリングデータ消去機能および電源 ON 時の自動消去機能のふるまいを改変するインタフェースを提供する。
TSF_FCF は FMT_MOF.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、ドキュメントファイリング機能のふるまいを改変するインタフェースを提供する。
TSF_FNP は FMT_MOF.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、ネットワーク保護機能のふるまいを改変するインタフェースを提供する。

k) TSF_AUT は FMT_MTD.1 (1) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、管理者パスワード変更のインタフェースを提供する。

l) TSF_FCF は FMT_MTD.1 (2) に則り、TSF_FCF による親展ファイル保存者認証が呼び出され成功した場合に限り、親展ファイルパスワード変更のインタフェースを提供する。

m) TSF_FNP は FMT_MTD.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、SSL 設定の問い合わせまたは改変のインタフェースを提供する。
TSF_FDC は FMT_MTD.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、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 時の自動消去の対象別有効設定、および、電源 ON 時の自動消去回数の問い合わせまたは改変のインタフェースを提供する。
TSF_FCF は FMT_MTD.1 (3) に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、ドキュメントファイリング禁止設定およびホールド以外のプリントジョブ禁止設定の問い合わせまたは改変のインタフェースを提供する。

n) TSF_FNP は、ネットワーク I/F が検出したネットワークパケットのレスポンスおよび処理に先立ち、必ず FTA_TSE.1 が定める通り IP アドレスおよび MAC アドレスを検査し、設定に照らして受け入れてよいものと判断されることを必要とする。

o) TSF_FNP は、リモート利用者が高信頼パスを要求した場合、保護されるべき通信データの送受信に先立ち、必ず FTP_TRP.1 が定める通り、保護された通信パスが確立されることを必要とする。

8.3.1.25 FTA_TSE.1

TSF_FNP のフィルタ機能は、管理者による事前の IP アドレスおよび MAC アドレス設定に基づき、意図しない通信相手からのネットワークパケットを破棄し、あらゆるセション確立を拒否する。よって FTA_TSE.1 は満足される。

8.3.1.26 FTP_TRP.1

TSF_FNP の通信データ保護機能は、クライアントにおけるリモート利用者と、TOE が設置された MFD の間に、SSL により保護された通信パス、すなわち HTTPS および IPP-SSL を用いた通信パスを提供する。これらの通信パスは、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および改変や暴露からの通信データの保護を提供する能力を持つ。

この機能は、クライアントにおけるリモート利用者による要求、すなわちクライアントの Web ブラウザまたはプリンタドライバからの接続に対し、SSL により保護された高信頼パスを介して通信を開始することを許可する能力を持つ。

この機能は、TOE の Web による通信サービス、および、プリンタドライバ用通信サービスに対して、SSL により保護された高信頼パスの使用を要求する能力を持つ。

以上により FTP_TRP.1 は満足される。

8.3.2 TOE セキュリティ機能強度根拠

確率的または順列的メカニズムによって実現される TSF は、6.2 節で述べた通り、認証 (TSF_AUT), データ消去 (TSF_FDC), ネットワーク保護 (TSF_FNP) および親展ファイル (TSF_FCF) である。それらはいずれもセキュリティ機能強度 *SOF-基本* を持つ。

よって、TSF のセキュリティ機能強度の最小値は *SOF-基本* であり、5.1.2 節で述べた TOE 最小機能強度と一貫している。

8.3.3 TOE 保証手段根拠

6.3 節の保証手段は、以下に示す各保証手段の内容より、TOE セキュリティ保証要件を満足する。

- ACM_CAP.2 — [CMC], [CL]: 構成要素を一意に識別し、また利用者が TOE のどの段階のものを使用しているかを知ることができることを保証するための手段、手続きを規定している。
- ADO_DEL.1 — [DEL]: TOE のセキュリティ維持のため、TOE が開発元から利用者までの配付に関し、使用される手段、手続きについて規定している。
- ADO_IGS.1 — [MI]: TOE の設置手段、手続きについて規定している。
- ADV_FSP.1 — [FSP]: TSF のふるまいと、利用者から見えるインタフェースについて規定している。
- ADV_HLD.1 — [HLD]: TOE のサブシステム設計における TSF の構造を明確化し、TOE セキュリティ機能要件を漏れなく正確に具体化していることを確認できるよう記述している。
- ADV_RCR.1 — [RCR]: TOE 要約仕様、機能仕様、上位レベル設計の対応について規定している。
- ADV_SPM.1 — [SPM]: 機能仕様、セキュリティ方針モデルと TSP の方針の間に対応を規定し、またセキュアな値だけがセキュリティ属性として受け入れられることの保証を提供している。
- AGD_ADM.1 — [MDSK], [NOTICE]: TOE の管理者に対し、TOE を正しい方法で保守し管理することを目的として書かれた資料 (取扱説明書) である。
- AGD_USR.1 — (同上): TOE 利用者に対し、TOE をセキュアに使用してもらうことを目的とした資料 (取扱説明書) である。
- ATE_COV.1 — [COV]: 機能テストとセキュリティ機能仕様との対応関係を記述している。
- ATE_FUN.1 — [FUN], [TT]: すべてのセキュリティ機能の実行が、仕様通りであることを実証するテストについて記述したものである。
- ATE_IND.2 — TOE: テストに適した TOE。
- AVA_SOF.1 — [SOF]: 確率的順列的メカニズムに対する機能強度分析を実施したものである。
- AVA_VLA.1 — [VLA]: TOE の明白なセキュリティ脆弱性の存在と、TOE の意図する環境においてそれらが悪用され得ないことの分析を実施したものである。