SHARP

AR-FR25
セキュリティターゲット

Version 0.03

シャープ株式会社

履歴

日付	Ver.	変更点	作成	確認	発行
2007/3/14	0.01	• 初版作成	中川	岩崎	久保田
2007/8/31	0.02	• 1.5.2, 2.2.1, 2.2.2, 2.3, 5.1.1.4, 6.3, 8.2.2, 8.3.1.10 の各節の誤記訂正	中川	岩崎	久保田
2007/9/21	0.03	• 6.3, 8.3.2 の各節を一部修正	中川	岩崎	久保田

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: AR-FR25 セキュリティターゲット

バージョン: 0.03

発行日: 2007 年 9 月 21 日

作成者: シャープ株式会社

TOE 識別: AR-FR25 VERSION M.10

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

ST 評価者: 社団法人電子情報技術産業協会 IT セキュリティセンター

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 AR-FR25 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、スキャナ機能、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り、MFD に搭載されている記憶デバイスにスプール保存されてい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する。

本 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。

- イメージデータの暗号化
- イメージデータ削除時の上書き消去

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 EAL3 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 [下線付き] 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 用語

本 ST 固有の専門用語を表 1.2 に示す。本 ST で使用する略語を表 1.3 に示す。

表 1.2: 専門用語

用語	定義
FAX基板	本TOE搭載可能なMFDを構成するユニットの一つ。ファクス機能を提供する。ただしMFD機種により標準、オプション、または非対応である。
FAX_RAM	FAX基板のRAMであり揮発性メモリ。
FAX_ROM	FAX基板のROM。TOEの物理的提供物の一部。
GDI基板	本TOE搭載可能なMFDを構成するユニットの一つ。USB及びパラレルI/Fを備え、プリンタ機能の一部を提供する。PCL基板を持たないMFDのうち一部機種のみが内蔵する。
IMC基板	本TOE搭載可能なMFDを構成するユニットの一つ。TOEの物理的提供物の一部。画像処理機能を担う。

用語	定義
IMC_RAM	IMC基板のRAMであり揮発性メモリ。
IMC_ROM	IMC基板のROM。TOEの物理的提供物の一部。
MCU基板	本TOE搭載可能なMFDを構成するユニットの一つ。MFD全体の制御機能を担う。
MCU_RAM	MCU基板のRAMであり揮発性メモリ。
MCU_ROM	MCU基板のROM。TOEの物理的提供物の一部。
PCL基板	本TOE搭載可能なMFDを構成するユニットの一つ。NIC, USB及びパラレルI/Fを備え、プリンタ機能及びスキャン送信機能を提供する。ただしMFD機種により標準、オプション、または非対応である。
PCL_RAM	PCL基板のRAMであり揮発性メモリ。
PCL_ROM	PCL基板のROM。TOEの物理的提供物の一部。
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。
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。ジョブ完了または中止の際に呼び出される。
キーオペレーター	TOEのセキュリティ管理機能およびMFD管理機能にアクセス可能な、認証された利用者。
キーオペレーターコード	キーオペレーターの認証の際に用いられるパスワード。
キーオペレータープログラム	TOEのセキュリティ管理機能。MFD管理機能でもある。キーオペレータープログラムにアクセスするためには、キーオペレーターとして識別認証されなければならない。
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。
ジョブ	MFDのコピー、プリンタ、スキャン送信、ファクスの各機能において、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。
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、スキャン送信及びファクス送信の際に使用する。
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を上書き消去するための機能。キーオペレーター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、機能キー及びタッチ操作式の液晶ディスプレイを含む。
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。
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、電気的な一括消去及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。

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	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。
I/F	Interface (インタフェース)
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特にMFD内のIMC_RAM, PCL_RAM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。

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。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。

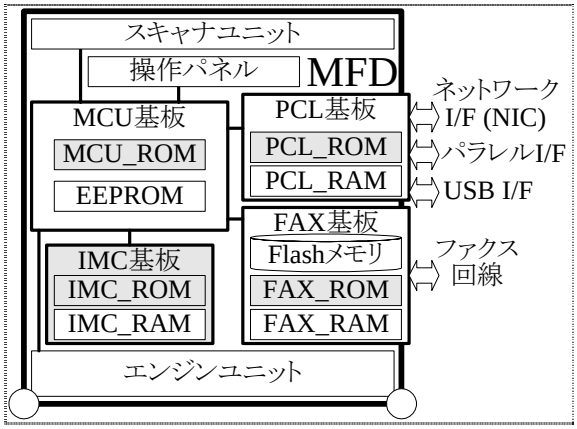

図 1: MFDの物理的構成とTOE

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とデータ消去機能からなり、TOE を搭載した MFD 内部に残存する実イメージデータからの情報漏洩を防止することを目的とする。

暗号操作機能は、ファクス機能の各ジョブにおいて、実イメージデータを Flash メモリにスプール保存する前に暗号化する。

データ消去機能は、コピー、プリンタ、スキャン送信、ファクスの各ジョブの完了後、スプール保存されている実イメージデータが存在している領域に対しランダム値、または固定値を上書きする。

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

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。

- MCU ファームウェア:
  MCU 基板に装着する MCU_ROM に格納され、MCU 基板を制御するファームウェアである。
- IMC ファームウェア:
  IMC 基板に実装された IMC_ROM に格納され、IMC 基板を制御するファームウェアである。
- PCL ファームウェア:
  PCL 基板に装着する PCL_ROM に格納され、PCL 基板を制御するファームウェアである。
- FAX ファームウェア:
  PCL 基板に装着する FAX_ROM に格納され、FAX 基板を制御するファームウェアである。

TOE は MCU_ROM, PCL_ROM, FAX_ROM 及び IMC 基板により提供される。TOE 未設置の MFD は、セキュリティ機能を持たないファームウェアを内蔵している。TOE を設置する際は、内蔵の MCU_ROM 及び IMC 基板を外し、TOE の部品で置き換える。MFD に PCL 基板あるいは FAX 基板が取り付けられていれば、それらの ROM も置き換える。

TOE が動作する MFD はシャープの AR-317FG, AR-317FP, AR-317G, AR-317S, AR-5631, AR-M316, AR-M317, AR-M317J 及び AR-M318 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。図中、データの流れを矢印で示す。

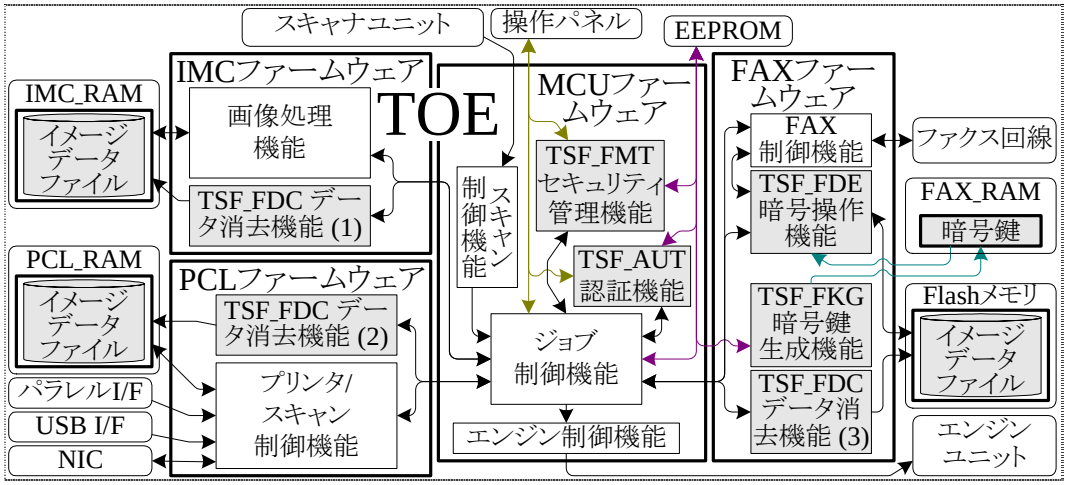

図 2: TOE の論理的構成図

TOE 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。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): ファクス機能で扱う実イメージデータを暗号化した後に Flash メモリにスプール保存し、イメージデータファイルとして管理する。また、Flash メモリにスプール保存されている実イメージデータを読み込み、復号した後に利用する。

b) 暗号鍵生成機能 (TSF_FKG): 暗号操作機能で提供する暗号化及び復号のための暗号鍵を生成する。生成された暗号鍵は、揮発性メモリ (FAX_RAM) に保存する。

c) データ消去機能(1), データ消去機能(2), データ消去機能(3) (TSF_FDC): MSD 内の実イメージデータに対し上書き消去する。コピージョブ、プリントジョブ、スキャン送信ジョブ及びファクスジョブの完了または中止時、当該ジョブの実イメージデータを上書き消去する (各ジョブ完了後の自動消去)。また、キーオペレーターの操作により、MSD 内の実イメージデータすべてを上書き消去する (全データエリア消去)。

d) 認証機能 (TSF_AUT): キーオペレーターコード (パスワード) により、キーオペレーター (管理者) の識別認証を行う。

e) セキュリティ管理機能 (TSF_FMT): キーオペレーターとして認証された場合において、キーオペレーターコードの変更 (改変) 機能を提供する。

f) エンジン制御機能: コピージョブ、プリントジョブ、ファクス受信ジョブにおいて、エンジンユニットの制御を行う。

g) スキャン制御機能: コピージョブ、スキャン送信ジョブ、ファクス送信ジョブにおいて、原稿を読み取るため、スキャナユニットの制御を行う。

h) プリンタ/スキャン制御機能: TOE を搭載可能な MFD のうち、PCL 基板を標準またはオプションにより搭載した場合に実施が可能な機能である。

- プリントジョブにおいては、ネットワーク、USB またはパラレル I/F を介して、受信した印刷データをプリントするために、ビットマップイメージを作成する。
- スキャン送信ジョブにおいては、スキャンされた実イメージデータを、指定された形式に変換後にネットワーク I/F を介して、ネットワークに送出する。

i) FAX 制御機能: PC-Fax ジョブ、ファクス送信ジョブにおいて FAX 回線への送出、またファクス受信ジョブにおいて FAX 回線からの受信を制御する。

j) 画像処理機能: デジタル複合機の特徴的機能を利用する印刷のための画像処理を行う。

k) ジョブ制御機能: ジョブには、コピージョブ、プリントジョブ、スキャン送信ジョブ及びファクスジョブがあり、それぞれ MFD のコピー、プリント、スキャン送信、ファクスの各動作を制御する。

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、スキャン送信及びファクスの各機能を持つ。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。

以下に述べる各機能はイメージデータを 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。

a) 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。

b) プリンタ機能: 外部より以下の手段により受信したデータを印刷する。

- プリンタドライバ: MFD 用のプリンタドライバがインストールされているクライアントにおいて、利用者の操作に応じて生成された印刷データを、ネットワーク、USB またはパラレル I/F 経由で受信する。
- E-mail: E-mail 添付ファイルとしてネットワーク経由で受信する。
- Web: リモート操作用 Web で提供する “プリントジョブの送信” ページにクライアントよりアップロードされたファイルを、ネットワーク経由で受信する。

c) スキャン送信機能: 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。

d) ファクス機能: 電話回線経由でファクスを送受信する。

- ファクス送信機能: 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。
- ファクス受信機能: 他機から送られたファクスを受信し印刷する。
- PC-Fax 機能: クライアントからのデータをファクス送信する。PCFAX とも呼ぶ。

FAX 基板及び PCL 基板は、MFD 機種により標準、オプションまたは非対応である。ファクス機能は FAX 基板を必要とする。スキャン送信機能は PCL 基板を必要とする。PCL 基板の代わりに GDI 基板 (TOE に含まない) があれば USB またはパラレル I/F 経由のプリントジョブは可能だが、スキャン送信機

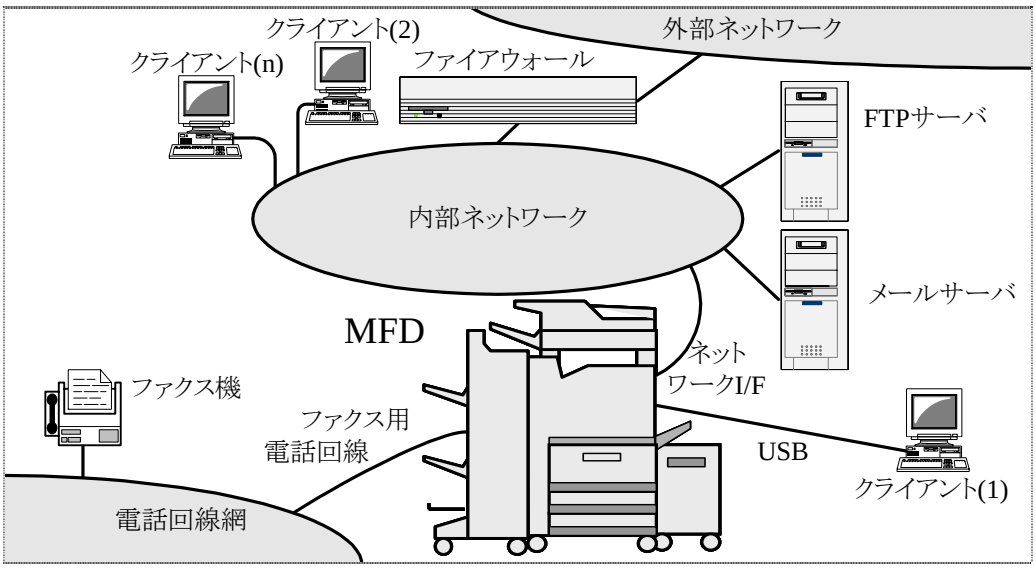

図 3: MFDの利用環境

能は使えない。

2.4 TOE の保護資産

本 TOE における保護資産は、利用者が MFD を使用した場合、MFD 自身がコピー、プリント、スキャン送信、ファクス処理終了後、もしくは各処理の中止により、MFD 内の揮発性メモリ、もしくは Flash メモリに保存されているイメージデータファイルを、資源の割当て解除のため削除後に残存する実イメージデータである。

実イメージデータについて、図 4 に説明する。実イメージデータは、管理領域と共にイメージデータを構成する。一方、実イメージデータファイルは、イメージを管理するファイルシステムが取り扱うためのオブジェクトであり、実イメージデータそのものである。

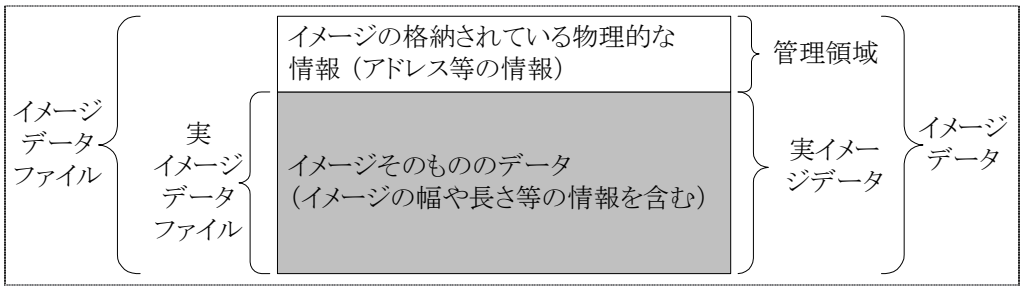

図 4: 実イメージデータ説明

TOE は、低レベルの攻撃者により、TOE の保護資産である残存する実イメージデータからの情報漏えいを防止することを目的とする。

なお、揮発性メモリ内に保存された保護資産は、低レベルの攻撃者には読み出すことができず、攻撃の対象とはならない。

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.OPERATOR	キーオペレーターは、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。

表 3.2: 脅威

識別子	定義
T.RECOVER	低レベルの攻撃者が、MFD内のFlashメモリに、MFD以外の装置を使用することにより、Flashメモリ内に残存する実イメージデータを読み出し漏えいさせる。

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	コピー、プリント、スキャン送信、ファクスジョブ終了、もしくはジョブを中止した場合、MSDにスプール保存された実イメージデータ領域は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、キーオペレーターにより、MSDのスプール領域全体は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.REMOVE	TOEが組み込まれているMFDのFlashメモリに対し、スプール保存を実行したMFD自身以外から読み取られても、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、Flashメモリにスプール保存する。
O.RESIDUAL	TOEは、コピー、プリント、スキャン送信、ファクスジョブ終了、もしくはジョブを中止した場合、MSDにスプール保存されている実イメージデータ領域に対し、上書き消去する。また、キーオペレーターの指示により、MSDの全イメージデータ領域に対し、上書き消去を実施する。

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.ERASEALL	キーオペレーターは、MFDの廃棄、または所有者変更の際、MSDのスプール領域全体の上書き消去を実施する。
OE.OPERATE	TOEを搭載したMFDを所有する組織の責任者が、キーオペレーターの役割を理解した上で、キーオペレーターの人選は厳重に行う。

5 IT セキュリティ要件

5.1 TOE セキュリティ要件

本節は、TOE 及びその環境が満たすべき IT セキュリティ要件について述べる。

5.1.1 TOE セキュリティ機能要件

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-A 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、[

- Flash メモリにスプール保存する実イメージデータの暗号化
- Flash メモリに暗号化スプール保存されている実イメージデータの復号

]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 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保証しなければならない: [

- IMC_RAM 内の実イメージデータファイル
- PCL_RAM 内の実イメージデータファイル
- Flash メモリ内の実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_SOS.1　秘密の検証

下位階層:　なし

FIA_SOS.1.1　TSF は、秘密が[5 文字の数字]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　アクション前の利用者認証

下位階層:　FIA_UAU.1 認証のタイミング

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

依存性:　FIA_UID.1 識別のタイミング

●FIA_UAU.7　保護された認証フィードバック

下位階層:　なし

FIA_UAU.7.1　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　アクション前の利用者識別

下位階層:　FIA_UID.1 識別のタイミング

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

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] [を動作させる, を停止する] 能力を[キーオペレーター]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　TSF データの管理

下位階層:	なし
FMT_MTD.1.1	TSFは、[キーオペレーターコード]を[改変, 問い合わせ]する能力を[キーオペレーター]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:[キーオペレーターコードの改変]。 *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	セキュリティ役割
下位階層:	なし
FMT_SMR.1.1	TSF は、役割[キーオペレーター]を維持しなければならない。
FMT_SMR.1.2	TSF は、利用者を役割に関連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

5.1.2 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_SOS.1, FIA_UAU.2 及び FIA_UAU.7 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、EAL3 + ADV_SPM.1 適合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.3	許可の管理	ACM_SCP.1, 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
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
ALC_DVS.1	セキュリティ手段の識別	なし
ATE_COV.2	カバレージの分析	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	テスト: 上位レベル設計	ADV_HLD.1, ATE_FUN.I
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_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

5.2 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)

TOE セキュリティ機能要件と TOE 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_FMT
FCS_CKM.1	6.1.1				
FCS_COP.1		6.1.2			
FDP_RIP.1			6.1.3		
FIA_SOS.1					6.1.5
FIA_UAU.2			6.1.3	6.1.4	
FIA_UAU.7			6.1.3	6.1.4	
FIA_UID.2			6.1.3	6.1.4	
FMT_MOF.1			6.1.3	6.1.4	
FMT_MSA.2	6.1.1				
FMT_MTD.1				6.1.4	6.1.5
FMT_SMF.1					6.1.5
FMT_SMR.1				6.1.4	6.1.5
FPT_RVM.1	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5

6.1.1 暗号鍵生成 (TSF_FKG)

TOE は、暗号鍵 (共通鍵) の生成を行い、実イメージ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。暗号鍵は、データセキュリティキット用暗号基準書に基づき、暗号化アルゴリズム AES Rijndael を実施するための暗号鍵生成アルゴリズムである MSN-A 拡張アルゴリズムを用いて、128 ビット長のセキュアな鍵として生成する。この暗号鍵は FAX_RAM 内に保存する。

6.1.2 暗号操作 (TSF_FDE)

PCFAX、ファクス送信、及びファクス受信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 FAX 基板に搭載している Flash メモリに、必ず暗号化後にスプール保存する。また、実イメージデータを実際に処理 (利用) する際は、Flash メモリから暗号化後にスプール保存されている実イメージデータを読み出し、必ず復号後に利用する。
暗号化、復号については、暗号鍵生成 (TSF_FKG) により生成された 128 ビット長の暗号化鍵を用い、FIPS PUBS 197 に基づき、AES Rijndael アルゴリズムにより実イメージデータを暗号化、もしくは復号する。

6.1.3 データ消去 (TSF_FDC)

TOE は、スプール保存された実イメージデータファイルを消去するデータ消去機能を有する。本機能は、以下の 2 プログラムで構成される。

- 各ジョブ完了後の自動消去
  コピージョブ、プリントジョブ完了後、IMC_RAM 内にスプール保存された当該ジョブの実イメージデータファイルをランダム値で上書き消去する。

スキャン送信ジョブ完了後、PCL_RAM 内にスプール保存された当該ジョブの実イメージデータファイルをランダム値で上書き消去する。
PCFAX ジョブ、ファクス送信ジョブ、ファクス受信ジョブにおいては、Flash メモリ内にスプール保存された当該ジョブの実イメージデータファイルを固定値で上書き消去する。

- 全データエリア消去
  全データエリア消去機能の実行と中断は、必ずキーオペレーターの識別認証を必要とする。
  全データエリア消去実行の場合、キーオペレーターの識別認証後、キーオペレーターの操作により、IMC_RAM 及び PCL_RAM 上のスプール保存のために利用される全ての実イメージデータをランダム値で上書き消去する。また、FAX 基板に搭載されている Flash メモリ上のスプール保存のために利用される全ての実イメージデータを固定値で上書き消去する。
  全データエリア消去中断の場合、キャンセル操作を選択後キーオペレーターコードの入力によるキーオペレーターの識別認証を要求する。キーオペレーターコードを入力している間、TOE は入力した文字を隠蔽、及び入力文字数を示すため、入力された文字数と同数のアスタリスク (星型記号) を表示する。キーオペレーターコードは、入力文字と比較するための認証データとして EEPROM 内に管理されており、キーオペレーターの識別認証機能、及び文字の隠蔽機能は必ず実施され、キーオペレーターとして識別認証された場合についてのみ、上書き消去を中断する。

各ジョブ完了後の自動消去、全データエリア消去のタイミングは、各ジョブ完了後、全データエリア消去発動時に実施するよう管理されている。また、各ジョブ完了後の自動消去およびキーオペレーター操作による全データエリア消去は必ず実施される。

なお、IMC_RAM 及び PCL_RAM に対する上書き消去で使用するランダム値は、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する。

6.1.4 認証 (TSF_AUT)

TOE は、TOE のセキュリティ管理機能であるキーオペレータープログラムの操作は、必ずキーオペレーターの識別認証を必要とする。これにより、キーオペレーターを特定し、利用者と役割を関連付けている。キーオペレーターの識別認証は、キーオペレータープログラムの選択後キーオペレーターコードの入力によるキーオペレーターの識別認証を要求する。キーオペレーターコードを入力している間、TOE は入力した文字を隠蔽、及び入力文字数を示すため、入力数に対応し”*”を表示する。キーオペレーターの識別認証機能、及び文字の隠蔽機能は必ず実施され、キーオペレーターとして識別認証された場合についてのみ、キーオペレータープログラムの操作が可能である。

データ消去 (TSF_FDC) のうちの全データエリア消去の実行、及びセキュリティ管理 (TSF_FMT) のキーオペレーターコードの問い合わせと改変は、必ずキーオペレーターとして認証 (TSF_AUT) された場合についてのみ操作を可能とする。

6.1.5 セキュリティ管理 (TSF_FMT)

セキュリティ管理 (TSF_FMT) は、キーオペレーターコード問い合わせ及び改変の機能を提供する。キーオペレーターコードは、セキュリティ管理 (TSF_FMT) により管理されている。セキュリティ管理 (TSF_FMT) は必ず認証 (TSF_AUT) によりキーオペレーターを識別認証された後に実施可能とする。このため、認証 (TSF_AUT) と同じく、キーオペレーターを特定し、利用者と役割を関連付けている。また、キーオペレーターコードを改変 (変更) 後も、キーオペレーターとして役割が維持される。

変更のため、新たに入力されるキーオペレーターコードについて、必ず 5 文字の数字であることを検査し、MFD 内の EEPROM 内に保存される。

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。

- 認証 (TSF_AUT): キーオペレーターコード認証入力が FIA_UAU.2 及び FIA_UAU.7 に対応する。
- データ消去 (TSF_FDC): 同上。
- セキュリティ管理 (TSF_FMT): キーオペレーターコード変更が FIA_SOS.1 に対応する。

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する保証手段となるドキュメントを表 6.2 に示す。

表 6.2: 保証手段

コンポーネント	保証手段
ACM_CAP.3 ACM_SCP.1	AR-FR24 AR-FR25 構成管理説明書 AR-FR25 VERSION M.10 構成リスト
ADO_DEL.1	AR-FR24 AR-FR25 配付手順説明書
ADO_IGS.1	AR-FR24/FR25 設置手順書 AR-FR24/FR25 設置手順書 (海外版)
ADV_FSP.1	AR-FR24 AR-FR25 セキュリティ機能仕様書
ADV_HLD.2	AR-FR24 AR-FR25 上位レベル設計書
ADV_RCR.1	AR-FR24 AR-FR25 表現対応分析書
ADV_SPM.1	AR-FR24 AR-FR25 セキュリティ方針モデル仕様書
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 AR-FR25 AR-FR25 Data Security Kit Operation Manual 注意書データセキュリティキット AR-FR24 AR-FR25 AR-FR24 AR-FR25 Data Security Kit Notice 取扱説明書デジタル複合機キーオペレータープログラム編
ALC_DVS.1	AR-FR24 AR-FR25 開発セキュリティ仕様書
ATE_COV.2	AR-FR24 AR-FR25 カバレージ分析書
ATE_DPT.1	AR-FR24 AR-FR25 上位レベル設計テスト分析書
ATE_FUN.1	AR-FR25 機能テスト仕様書 AR-FR24 AR-FR25 テスト環境・ツール説明書
ATE_IND.2	TOE
AVA_SOF.1	AR-FR24 AR-FR25 セキュリティ機能強度分析書
AVA_VLA.1	AR-FR24 AR-FR25 脆弱性分析書

7 PP 主張

本 ST 及び本 TOE の適合を主張する 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.OPERATOR	T.RECOVER	P.RESIDUAL
O.REMOVE		8.1.2	
O.RESIDUAL			8.1.3
OE.ERASEALL			8.1.3
OE.OPERATE	8.1.1		

8.1.1 A.OPERATOR

A.OPERATOR は、キーオペレーター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、キーオペレーターの役割を理解した上で、キーオペレーターの人選は厳重に行うことにより実施できる。

8.1.2 T.RECOVER

T.RECOVER に対して、本 TOE の保護資産のうち Flash メモリ内に保存されている実イメージデータについては、低レベルの攻撃者が実イメージデータを読み出すことができたとしても、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、MFD 固有の暗号鍵で実イメージデータを暗号化後にスプール保存することで対抗する。

FAX_RAM に保存している暗号鍵と、本 TOE の保護資産のうち PCL_RAM 及び IMC_RAM に保存されている実イメージデータについては、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の暗号鍵や実イメージ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 FAX_RAM に保存している暗号鍵を読み出すことができず、Flash メモリ内の情報漏洩が防止できる。また、PCL_RAM 内及び IMC_RAM 内にスプール保存している実イメージデータからの情報漏洩が防止できる。

8.1.3 P.RESIDUAL

P.RESIDUAL は、各ジョブの完了後 MSD にスプール保存されている実イメージデータについて、O.RESIDUAL にて各ジョブ完了後の上書き消去を行うことにより実施できる。また、MFD の廃棄、所有者変更の際は OE.ERASEALL によりキーオペレーターが、O.RESIDUAL にて MSD のスプール領域全体の上書き消去を行うことにより実施できる。

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 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。

表 8.2: TOE セキュリティ機能要件根拠

対策方針 / 要件	O.REMOVE	O.RESIDUAL
FCS_CKM.1	8.2.1.1	
FCS_COP.1	8.2.1.1	
FDP_RIP.1		8.2.1.2
FIA_SOS.1		8.2.1.2
FIA_UAU.2		8.2.1.2
FIA_UAU.7		8.2.1.2
FIA_UID.2		8.2.1.2
FMT_MOF.1		8.2.1.2
FMT_MSA.2	8.2.1.1	
FMT_MTD.1		8.2.1.2
FMT_SMF.1		8.2.1.2
FMT_SMR.1		8.2.1.2
FPT_RVM.1	8.2.1.1	8.2.1.2

8.2.1.1 O.REMOVE

O.REMOVE の目的は T.RECOVER への対抗であり、すなわち MFD 内の Flash メモリに対し、Flash メモリにスプール保存を実行した MFD 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。これは、以下の機能要件の組み合わせにより実現できる。

- FCS_COP.1 により、スプール保存される実イメージデータが暗号化されるため、Flash メモリにスプール保存を実行した MFD 自身以外からアクセスされても、イメージ表示は阻止される。
- 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。
- 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。
- 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。

8.2.1.2 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 により、各ジョブ完了後の自動消去、及び、全データエリア消去の実行時に、スプール保存されている実イメージデータが格納された領域の上書き消去を行うことで、利用者データ保護が可能となる。

b) FIA_UAU.2, FIA_UAU.7 及び FIA_UID.2 にてキーオペレーターを識別認証する。

c) 以下の各機能要件により、FDP_RIP.1 の管理 (全データエリア消去機能の起動と中止) を行う能力は、キーオペレーターに制限される。

- 全データエリア消去機能の起動と停止が、FMT_MOF.1 によりキーオペレーターのみ可能となる。
- キーオペレーターコードの問合せと変更 (改変) が、FMT_MTD.1 によりキーオペレーターのみ可能となる。
- キーオペレーターコードを変更 (改変) する場合、FIA_SOS.1 により、入力されたキーオペレーターコードが 5 文字の数字であることの検証を行うことにより、定義された品質尺度をもつキーオペレーターコードが設定される。
- FMT_SMF.1 により、FIA_UAU.2 のキーオペレーターコードを管理することにより、確実にキーオペレーターを識別認証することが可能となる。

d) 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 c) 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) 及び c) の各事象が相互に競合することはない。また、a) 及び c) 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。b) は a) とも c) とも独立であり、かつ三つの機能要件が識別認証を実施するために補完的に作用するので、競合は発生しない。各事象が相互に競合することはない。上記 d) 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。

8.2.2 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	—	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_SOS.1	—	品質尺度は固定
FIA_UAU.2	• キーオペレーターコードの改変	管理要件に合致
FIA_UAU.7	—	(管理要件なし)
FIA_UID.2	—	キーオペレーターの識別は固定
FMT_MOF.1	—	役割のグループはない
FMT_MSA.2	—	(管理要件なし)
FMT_MTD.1	—	役割のグループはない
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1	—	利用者のグループはない
FPT_RVM.1	—	(管理要件なし)

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、及び本 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 FDP_ITC.2 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_SOS.1	—	—	—	—
FIA_UAU.2	FIA_UID.1 *	FIA_UID.2	—	—
FIA_UAU.7	FIA_UAU.1 *	FIA_UAU.2	—	—
FIA_UID.2	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.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	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1 *	FIA_UID.2	—	—
FPT_RVM.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、キーオペレーターに対しても変更を許容していないため、FMT_MSA.1 及び FMT_SMR.1 は必要がない。同様に、暗号鍵やシードを利用者及びキーオペレーター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 及び 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。

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、実イメージデータを Flash メモリにスプール保存する前に必ず暗号化し、読み出し後に復号され、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、各ジョブの完了または中止時、及び、キーオペレーターの全データエリア消去操作時に必ず呼び出されるため迂回できない。

d) キーオペレーターの識別認証に関する FIA_UAU.2, FIA_UAU.7 及び FIA_UID.2 は、キーオペレーターの識別認証時に必ず呼び出されるため迂回できない。

e) 秘密の検証 FIA_SOS.1 は、キーオペレーターコードの変更 (改変) 時に必ず呼び出されるため迂回できない。

f) セキュリティ機能のふるまい管理 FMT_MOF.1 は、全データエリア消去を動作させるための操作に先立ち、必ずキーオペレーター認証 FIA_UAU.2 を経ることを必要とし、キャンセル操作後、実際に中断される前に必ずキーオペレーター認証が呼び出されるため、いずれも迂回できない。

g) TSF データの管理 FMT_MTD.1 は、必ずキーオペレーター認証 FIA_UAU.2 を経ることを必要とし、迂回できない。

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
FIA_SOS.1	FPT_RVM.1	—
FIA_UAU.2	FPT_RVM.1	—
FIA_UAU.7	FPT_RVM.1	—
FIA_UID.2	FPT_RVM.1	—
FMT_MOF.1	FPT_RVM.1	—
FMT_MSA.2	—	—
FMT_MTD.1	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1	—	—
FPT_RVM.1	—	—

8.2.4.2 非活性化

表 8.5 に関し、FDP_RIP.1 は、FMT_MOF.1 によりキーオペレーターのみに制限されるため非活性化行為から保護される。

8.2.4.3 干渉

本 TOE は、キーオペレーター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 TOE セキュリティ保証要件根拠

本 TOE は、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、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、商用として十分である EAL3 + ADV_SPM.1 を品質保証レベルとする。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 EAL3 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。

8.2.6 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_SOS.1, FIA_UAU.2 及び FIA_UAU.7 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。

8.3 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 要約仕様根拠

表 6.1 に示したセキュリティ機能要件と TOE セキュリティ仕様の対応について、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-A 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-A 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スプール保存する実イメージデータの暗号化、及び復号を行うため、満足される。

8.3.1.3 FDP_RIP.1

TSF_FDC が以下の通り上書き消去により残存情報を保護するので、FDP_RIP.1 は満足される。

- 各ジョブ完了後の自動消去プログラム実行時に、IMC_RAM (コピー及びプリントジョブで使用), PCL_RAM (スキャン送信ジョブで使用) あるいは Flash メモリ (ファクスジョブで使用) に保存された実イメージデータファイルに対し上書き消去する。
- 全データエリア消去プログラム実行時に、IMC_RAM, PCL_RAM 及び Flash メモリに保存された全ての実イメージデータに対し上書き消去する。

8.3.1.4 FIA_SOS.1

TSF_FMT によるキーオペレーターコードの変更時、入力された新しいキーオペレーターコードが 5 文字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 は満足される。

8.3.1.5 FIA_UAU.2

TSF_AUT はキーオペレーター向け機能の操作に先立ち、キーオペレーターコード入力による認証を行う。TSF_FDC は、実行中の全データリア消去を中止する際、キーオペレーターコード入力による認証を行う。これらにより FIA_UAU.2 は満足される。

8.3.1.6 FIA_UAU.7

TSF_AUT は、キーオペレーター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。TSF_FDC による消去中止時のキーオペレーター認証も同様である。これらにより FIA_UAU.7 は満足される。

8.3.1.7 FIA_UID.2

TSF_AUT はキーオペレーター向け機能の操作に先立ち、キーオペレーターの識別操作を必要とする。TSF_FDC による全データリア消去のキャンセル操作は、キーオペレーター識別に相当する。これらにより FIA_UID.2 は満足される。

8.3.1.8 FMT_MOF.1

TSF_FDC による全データエリア消去の起動は、TSF_AUT によるキーオペレーター認証後に可能となる。TSF_FDC による全データエリア消去の中止は、TSF_FDC によるキーオペレーター認証後に可能となる。これらにより FMT_MOF.1 は満足される。

8.3.1.9 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。

8.3.1.10 FMT_MTD.1

FMT_MTD.1 は、TSF_AUT により識別認証されたキーオペレーターが、TSF_FMT によるキーオペレーターコードの問合せと改変を可能とするため、満足される。

8.3.1.11 FMT_SMF.1

TSF_FMT はキーオペレーターコードの改変を行う能力を持っている。よって FMT_SMF.1 は満足される。

8.3.1.12 FMT_SMR.1

TSF_AUT はキーオペレーターの識別認証により、キーオペレーターを特定することで、役割への関連づけを行っている。また、TSF_FMT によってキーオペレーターコードを変更 (改変) しても役割への関連づけ、及び役割を維持し続ける。これらにより FMT_SMR.1 は満足される。

8.3.1.13 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 は実イメージデータを Flash メモリにスプール保存する際、必ず FCS_COP.1 が定める通り暗号化し、Flash メモリの実イメージデータはジョブ処理時のみ読み出し復号する。

c) TSF_FDC は、各ジョブの完了または中止時、及び、キーオペレーターの全データエリア消去操作時には、必ず FDP_RIP.1 に基づく上書き消去を実行する。

d) TSF_AUT 及び TSF_FDC は、キーオペレーター識別認証の際、FIA_UID.2 に基づくキーオペレーター識別操作、FIA_UAU.2 に基づくキーオペレーターコード認証、及び、FIA_UAU.7 に基づくキーオペレーターコードのフィードバック保護を必ず実行する。

e) TSF_FMT は、キーオペレーターコードの変更時に必ず FIA_SOS.1 が定める通りキーオペレーターコードが 5 文字の数字であることを検証する。

f) TSF_FDC は FMT_MOF.1 に則り、TSF_AUT によるキーオペレーター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を起動するインタフェースを提供し、TSF_FDC によるキーオペレーター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の中止を許可する。

g) TSF_FMT は FMT_MTD.1 に則り、TSF_AUT によるキーオペレーター認証が呼び出され成功した場合に限り、キーオペレーターコード変更のインタフェースを提供する。

8.3.2 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。

a) ACM_CAP.3, ACM_SCP.1

保証手段: AR-FR24 AR-FR25 構成管理説明書
AR-FR25 VERSION M.10 構成リスト

内容: 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。

この保証手段の管理下に置かれている要素に対してのみ変更を管理することができ、TOE 実装及び ST の他の保証コンポーネントが要求する評価証拠について、適切な許可を伴う管理された方法で修正がなされることの保証を規定している。

b) ADO_DEL.1

保証手段: AR-FR24 AR-FR25 配付手順説明書

内容: 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。

c) ADO_IGS.1

保証手段: AR-FR24/FR25 設置手順書
AR-FR24/FR25 設置手順書 (海外版)

内容: TOE の設置手段、手続きについて規定している。

d) ADV_FSP.1

保証手段: AR-FR24 AR-FR25 セキュリティ機能仕様書

内容: 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。

e) ADV_HLD.2

保証手段: AR-FR24 AR-FR25 上位レベル設計書

内容: TOE 機能要件の実装に適したアーキテクチャを、TOE が提供することの保証を、TOE の主要な構成単位 (サブシステム) 及びこれらの単位をこれらが提供する機能と関係付ける観点から規定している。

f) ADV_RCR.1

保証手段: AR-FR24 AR-FR25 表現対応分析書

内容: 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。

g) ADV_SPM.1

保証手段: AR-FR24 AR-FR25 セキュリティ方針モデル仕様書

内容: 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。

h) AGD_ADM.1

保証手段: 取扱説明書データセキュリティキット AR-FR25
AR-FR25 Data Security Kit Operation Manual
注意書データセキュリティキット AR-FR24 AR-FR25
AR-FR24 AR-FR25 Data Security Kit Notice
取扱説明書デジタル複合機キーオペレータープログラム編

内容: 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。

i) AGD_USR.1

保証手段: (AGD_ADM.1 に同じ)

内容: 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。

j) ALC_DVS.1

保証手段: AR-FR24 AR-FR25 開発セキュリティ仕様書

内容: TOE の開発環境で使用されている物理的、手続き的、人的セキュリティ手段を規定している。

k) ATE_COV.2
保証手段: AR-FR24 AR-FR25 カバレージ分析書
内容: 機能テスト仕様書記述のテストにおいて、TSF が機能仕様通りに動作することを実証するに十分であることを記述したものである。

l) ATE_DPT.1
保証手段: AR-FR24 AR-FR25 上位レベル設計テスト分析書
内容: 機能テスト仕様書記述のテストにおいて、TSF が上位レベル設計書通りに動作することを実証するに十分であることを記述したものである。

m) ATE_FUN.1
保証手段: AR-FR25 機能テスト仕様書
AR-FR24 AR-FR25 テスト環境・ツール説明書
内容: 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。

n) ATE_IND.2
保証手段: TOE
内容: テストに適した TOE。

o) AVA_MSU.1
保証手段: (AGD_ADM.1 に同じ)
内容: TOE の管理者に対する TOE を正しい方法での保守管理方法と、TOE 利用者に対する TOE のセキュアな使用について書かれた資料 (取扱説明書) である。

p) AVA_SOF.1
保証手段: AR-FR24 AR-FR25 セキュリティ機能強度分析書
内容: 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。

q) AVA_VLA.1
保証手段: AR-FR24 AR-FR25 脆弱性分析書
内容: 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。

8.3.3 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) 及びセキュリティ管理 (TSF_FMT) 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 節が規定する TOE 最小機能強度と一貫している。