データセキュリティキット

AR-FR12M

セキュリティターゲット

Version 0.25

シャープ株式会社

【履歴】

日付	バージョン	変更点	作成	承認
2003 年 11 月 7 日	0.01	・ 初版作成	釘宮	黒川
2003 年 12 月 19 日	0.02	・ 全般に渡る見直し	岩崎	黒川
2004 年 2 月 6 日	0.03	・ TOE バージョン変更 ・ 指摘内容反映	岩崎	黒川
2004 年 2 月 20 日	0.04	・ 全般に渡る見直し	岩崎	黒川
2004 年 3 月 19 日	0.05	・ 指摘内容反映	岩崎	黒川
2004 年 4 月 2 日	0.06	・ 指摘内容反映	岩崎	山中
2004 年 4 月 9 日	0.07	・ 指摘内容反映	岩崎	山中
2004 年 5 月 18 日	0.08	・ 指摘内容反映	岩崎	山中
2004 年 5 月 20 日	0.09	・ 指摘内容反映	岩崎	山中
2004 年 6 月 4 日	0.10	・ 指摘内容反映	岩崎	山中
2004 年 6 月 22 日	0.11	・ 指摘内容反映	岩崎	山中
2004 年 7 月 6 日	0.12	・ 指摘内容反映	岩崎	山中
2004 年 7 月 12 日	0.13	・ 指摘内容反映	岩崎	山中
2004 年 7 月 21 日	0.14	・ 指摘内容反映	岩崎	山中
2004 年 7 月 27 日	0.15	・ 指摘内容反映	岩崎	山中
2004 年 8 月 5 日	0.16	・ 指摘内容反映	岩崎	山中
2004 年 9 月 8 日	0.17	・ 指摘内容反映	岩崎	山中
2004 年 9 月 14 日	0.18	・ 指摘内容反映	岩崎	山中
2004 年 9 月 24 日	0.19	・ 指摘内容反映	岩崎	山中
2004 年 10 月 22 日	0.20	・ 指摘内容反映	岩崎	山中
2004 年 12 月 13 日	0.21	・ 指摘内容反映	岩崎	山中
2005 年 1 月 6 日	0.22	・ 指摘内容反映	岩崎	山中
2005 年 1 月 7 日	0.23	・ 指摘内容反映	岩崎	山中
2005 年 1 月 17 日	0.24	・ ガイダンス文書名変更	岩崎	山中
2005 年 2 月 22 日	0.25	・ 指摘内容反映	岩崎	山中

【目次】

【表のリスト】

【図のリスト】

1 ST 概説

1.1 ST 識別

本書と TOE を識別するための情報を記載する。

ST 名称: データセキュリティキット AR-FR12M セキュリティターゲット
バージョン: 0.25
作成日: 2005 年 2 月 22 日
製作者: シャープ株式会社
TOE 識別: AR-FR12M VERSION M.20
CC 識別: CC バージョン 2.1, ISO/IEC 15408:1999, JIS X 5070:2000
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、シャープのデータセキュリティキット AR-FR12M 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、PCFAX 機能、ファクス送信機能、ファクス受信機能で構成し、販売される事務機械である。本 TOE は、この MFD のデータセキュリティ機能を強化するためのファームウェア アップグレード キットである。このキットはデジタル複合機の MSD にスプール保存されている実イメージデータからの情報漏洩を防止する。

1.3 CC 適合

本書は、以下を満たしている。

a) CC バージョン 2.1 パート2適合
b) CC バージョン 2.1 パート3適合
c) EAL3 追加
追加コンポーネント: ADV_SPM.1
d) 本 ST が参照する PP はない。

1.4 参照資料

本書作成について、表 1記載の資料を参照している。

表 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 1999 年 8 月 バージョン 2.1 CCIMB-99-031 (平成 13 年 1 月翻訳第 1.2 版 情報処理振興事業協会 セキュリティセンター)
[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 1999 年 8 月 バージョン 2.1 CCIMB-99-032 (平成 13 年 1 月翻訳第 1.2 版 情報処理振興事業協会 セキュリティセンター)
[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 1999 年 8 月 バージョン 2.1 CCIMB-99-033 (平成 13 年 1 月翻訳第 1.2 版 情報処理振興事業協会 セキュリティセンター)

略称	文書名
[HOSOKU-0210]	補足-0210

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。セキュリティ機能要件コンポーネントに関するコモンクライテリア(CC)の運用を示すため、及び特別の意味を持った文章を区別するために使われる規約を以下の通り定める。

a) *単純イタリック体* はテキストを強調するために使用する。
b) 割付操作は、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。括弧［ ］の中の値が割り付けられたことを意味している。
c) 詳細化操作は、要件に詳細付加のために使用され、要件をさらに限定する。
d) 選択操作は、要件記述にコモンクライテリア(CC)が備える複数のオプションから、選択するために使用される。選択操作は ［ 下線付き ］ で示される。
e) 繰り返される機能コンポーネント要件は、コモンクライテリア(CC)のコンポーネントの名称、短縮名称、及び機能エレメントの名前に対して( )内に繰り返し数値を付記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 2に示す。

表 2: 専門用語

用語	定義
FAX基板	TOEであるデータセキュリティキットを搭載可能とするMFDを構成する一つのユニットであり、プリント基板に部品を半田付け搭載したものを指す。FAX通信機能を担う。
GDI基板	本TOEを搭載可能なMFDのプリンタ機能を実現する構成する一つのユニット。SPLC言語を搭載している。
IMC基板	TOEであるデータセキュリティキットを搭載可能とするMFDを構成する一つのユニットであり、プリント基板に部品を半田付け搭載したものを指す。また、TOEの物理的提供物の一部。画像処理機能を担う。
MCU基板	TOEであるデータセキュリティキットを搭載可能とするMFDを構成する一つのユニットであり、プリント基板に部品を半田付け搭載したものを指す。MFD全体の制御機能を担う。
PCL基板	TOEであるデータセキュリティキットを搭載可能とするMFDを構成する一つのユニットであり、プリント基板に部品を半田付け搭載したものを指す。PDLの一種と位置づけられるシャープPCLに対応し、プリンタ機能を担う。
イメージデータ	MFDにてコピー、プリント、スキャン、もしくはファクス送信のため、原稿画像を読み込みデジタル化したデータ。PCFAX、ファクス送信、ファクス受信においては、電話回線への送信、もしくは電話回線から受信したデータを含み、このデータをMFDで取扱可能な様に変換したデータもイメージデータと呼ぶ。
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。
キーオペレーター	TOEのセキュリティ管理機能、あるいは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。

用語	定義
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。
ジョブ	MFD機能（コピー、プリント、スキャン送信、PCFAX、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。
データセキュリティキット	シャープのデジタル複合機専用のアップグレード キットAR-FR12M。
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。
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。
実イメージデータ	イメージデータから管理領域を除いた実イメージデータ部分。
全データエリア消去	MFDが搭載している不揮発性メモリについて、スプール保存に利用される全ての実イメージデータ領域に対する上書き消去処理。
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、ユーザI/Fのためのデバイス。または、そのユニット。
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メモリのこと。半導体素子、あるいは磁気記憶を用いたものがある。

1.5.3 略語

本書で使用する略語を表 3に示す。

表 3: 略語

略語	定義
AES	NIST(米国商務省標準技術局)で制定された米国政府標準暗号(Advanced Encryption Standard)。
DSK	データセキュリティキット(Data Security Kit)。
EEPROM	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 (Electronically Erasable Programmable ROM)。
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)。
I/F	インタフェース(Interface)。
MSD	大容量ストレージ機器(Mass Storage Device)。本TOEの場合、ファイルシステムにより管理されているIMC基板に搭載されている揮発性メモリ、PCL基板に搭載されている揮発性メモリ、及びFAX基板に搭載されているFlashメモリがMSDに相当する。
OS	オペレーティングシステム(Operating System)。
PCL	プリンタ制御言語（Printer Control Language）。
PDL	ページ記述言語(Page Description Language)。ページプリンタを制御するコマンド、またその言語体系。
PS	PostScript。米Adobe社によって開発されたページ記述言語。本TOEが搭載可能なMFDについては、PostScript互換のオプション、AR-PK1が動作可能。
RAM	任意に読み書き可能なメモリ(Random Access Memory)。
ROM	読み出し専用メモリ(Read Only Memory)。
SPDL2	シャープ ページ記述言語（Page Description Language 2）。本TOEが搭載可能なMFDには、標準でSPDL2言語を搭載しているもの、またはオプションで搭載可能なものがある。

略語	定義
SPLC	シャープ プリンタ言語 (SHARP Printer Language with Compression)。

2 TOE 記述

2.1 TOE の概要

2.1.1 TOE 種別

TOE は、データセキュリティキットであり、これは MFD のファームウェア製品である。

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、PCFAX、ファクス送信、及びファクス受信する実イメージデータを FAX 基板に搭載している Flash メモリにスプール保存する前に暗号化する。この暗号操作機能により、ジョブ完了に伴うデータ消去機能が動作する前の状態においても、暗号鍵を入手しない限り、Flash メモリから取得した実イメージデータからイメージとして表示不能である。

データ消去機能は、コピー、プリント、スキャン送信のジョブ完了後、IMC 基板に搭載している揮発性メモリ、PCL 基板に搭載している揮発性メモリに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を上書きする。また、PCFAX、ファクス送信、及びファクス受信のジョブ完了後については、Flash メモリに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

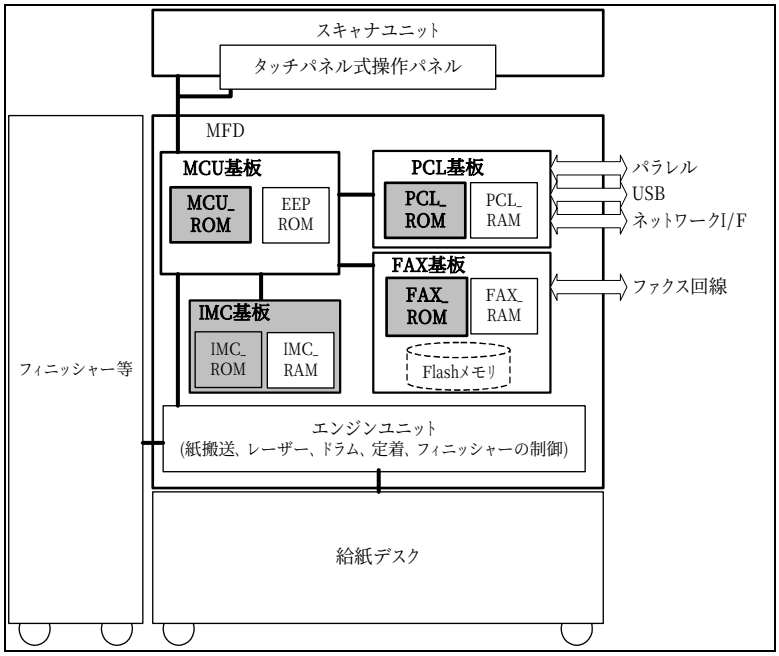

図 1: MFD の物理的構成と TOE

TOE である AR-FR12M は、MCU_ROM、PCL_ROM、FAX_ROM、及び IMC 基板により提供される。これらを図 1に網掛けで示す。

TOE が動作する MFD は、シャープ デジタル複合機 AR-M236, AR-M236J, AR-M276, AR-M276J, AR-M237, AR-M237J, AR-M277, AR-M277J, AR-266S, AR-266G, AR-266FG, AR-266FP である。
TOE の物理的範囲は、以下の通りである。

a) MCU ファームウェア
MCU 基板に搭載する MCU_ROM に格納されており、MCU 基板を制御するファームウェアである。
b) IMC ファームウェア
IMC 基板に搭載されている ROM に格納されており、IMC 基板を制御するファームウェアである。
c) PCL ファームウェア
PCL 基板に搭載する PCL _ROM に格納されており、PCL 基板を制御するファームウェアである。
d) FAX ファームウェア
FAX 基板に搭載する FAX _ROM に格納されており、FAX 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。図中、TOE を太い枠線内として示す。長方形はファームウェアの機能であり、角を丸くした長方形をハードウェアとして示す。ファームウェアの機能のうち、網掛け部がセキュリティ機能である。また、TOE 内の破線は物理的範囲との対応を示すものであり、破線枠上部に物理的範囲名称を記載する。

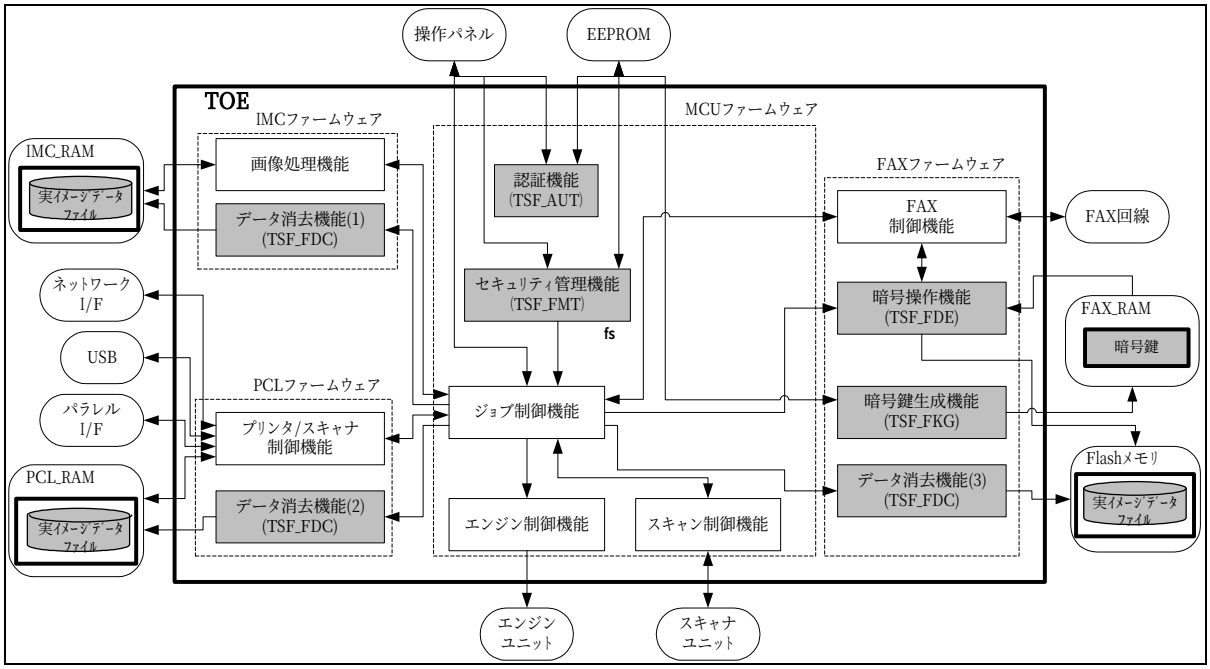

図 2: TOE の論理的構成図

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)
PCFAX ジョブ、ファクス送信ジョブ、及びファクス受信ジョブに関し、実イメージデータを暗号化した後、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)
コピージョブ、プリントジョブ、スキャン送信ジョブ、PCFAX ジョブ、ファクス送信ジョブ、もしくはファクス受信ジョブにより、MSD 内にスプール保存され、イメージデータファイルとして管理されてい

る対応する実イメージデータ領域に対して、ランダム値、または固定値を上書きすることにより、実イメージデータを消去する。(各ジョブ完了後の自動消去)
また、MSD にスプール保存することが可能な全領域に対して、ランダム値、または固定値を上書きすることにより上書き消去を行う。(キーオペレーターの操作による全データエリア消去)
以下の2つ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
  (ジョブ完了後、ジョブが使用した実イメージデータ領域の消去)
  ジョブ処理において、揮発性メモリにスプール保存されている実イメージデータ格納領域については、ランダム値を上書き消去し、Flash メモリにスプール保存されている実イメージデータ格納領域については、Flash メモリの各ビットに固定値を上書き消去する。
  データ消去機能(1)は、IMC 基板に搭載されている揮発性メモリ (IMC_RAM) に対する上書き消去、データ消去機能(2)は、PCL 基板に搭載されている揮発性メモリ (PCL_RAM) に対する上書き消去、データ消去機能(3)は、FAX 基板に搭載されている Flash メモリに対する上書き消去を実施する。
- キーオペレーターの操作による全データエリア消去
  (注釈: ジョブが正常に完了しなかった場合、及びジョブが未完了の場合、実イメージデータ領域に対する消去機能であり、MFD の所有者が変わる、もしくは MFD 廃棄等において、実イメージデータからの情報漏洩を防止するために使用する)
  IMC 基板に搭載されている揮発性メモリ (IMC_RAM)、PCL 基板に搭載されている揮発性 RAM (PCL_RAM) の全ての実イメージデータ領域をランダム値で上書き消去し、FAX 基板に搭載されている Flash メモリの全ての実イメージデータ領域を固定値で上書き消去する。
  また、キーオペレーターの操作による全データエリア消去は、キーオペレーターにより上書き消去を中止することができる。

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／スキャナ制御機能
TOE を搭載可能な MFD のうち、PCL 基板を標準搭載、もしく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、パラレル、USB、もしくはネットワーク 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。

なお、TOE を搭載可能な MFD のうち、GDI 基板を標準搭載、もしくはオプションにより搭載した場合は、スキャナ制御機能は有しておらず、またネットワーク I/F もない。

i) FAX 制御機能
PCFAX 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
印刷に関し、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、PCFAX ジョブ、ファクス送信ジョブ、ファクス受信ジョブがあり、それぞれ以下のように制御される。

- コピージョブ: MFD のコピー動作を制御する。
- プリントジョブ: MFD のプリント動作を制御する。
- スキャン送信ジョブ: MFD のスキャン送信動作を制御する。
- PCFAX ジョブ: MFD の PCFAX ジョブを制御する。
- ファクス送信ジョブ: MFD のファクス送信動作を制御する。
- ファクス受信ジョブ: MFD のファクス受信動作を制御する。

2.3 TOE の利用

本節は、TOE の利用方法、及び運用方法について述べる。

2.3.1 TOE 利用方法

MFD の持つコピー、プリンタ、スキャン送信、PCFAX、ファクス受信、ファクス送信の各機能を利用することにより、MFD の利用者は TOE の機能を意識することなく利用することができる。TOE の利用環境を図3に示す。

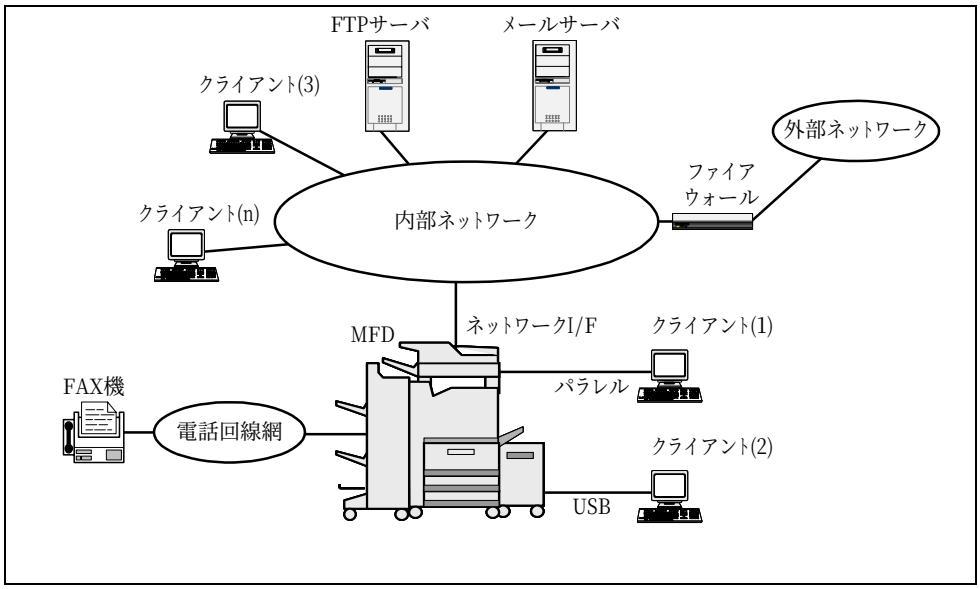

図 3: TOE の利用環境

a) コピー機能

MFD のコピー機能は、原稿を読み取り、読み取った画像を印字する機能である。
MFD の操作パネルにてコピー部数等の必要な設定の後、スタートキーを押下することにより実施される。

① MFD のスキャナユニットに利用者が原稿をセットし、操作パネルで必要な設定の後、スタートボタンを押下することによりコピージョブが開始される。
② スキャナユニットで原稿をスキャンし、実イメージデータとして読み取る。
③ 読み取った実イメージデータを、エンジンユニットで印字する。

b) プリンタ機能

MFD のプリンタ機能は、クライアントから送付されてくるプリントデータを印字する機能である。
プリンタ機能の動作において、クライアントからプリントデータの受信は、以下の3種類の方法がある。

1) 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、必要な設定の後、印刷開始ボタン(”OK”ボタン)をクリックすると、プリンタドライバにてプリントデータが生成される。MFD は、パラレル、USB、もしくはネットワークを介して生成されたプリントデータを受信する。(プリント機能)

2) ネットワークに接続されているメールサーバに MFD のメールアカウントを登録し、MFD 自身がメールサーバに到着している MFD 宛のメールの有無を定期的に確認する。MFD は、MFD 宛のメールがある場合、そのメールを添付されているファイル（プリントデータ）と共に受信する。（E-mail プリント機能）

3) ネットワークに接続されているクライアントの Web ブラウザから、ファイル（プリントデータ）を MFD に対し送信する。MFD は、プリンタドライバを介していないクライアントからのファイル（プリントデータ）を、直接ネットワーク I/F を介して受信する。（コンピュータ上のファイルの直接印刷機能）

① MFD が、クライアント、もしくはメールサーバからプリントデータを受信することによりプリントジョブが開始される。

② クライアント、もしくはメールサーバから受信したプリントデータは、MFD で直接印刷が行えないため、MFD で印刷を行える実イメージデータに変換する。

③ 変換された実イメージデータを、エンジンユニットで印字する。

（この機能は TOE を搭載可能な MFD のうち、シャープ PCL 言語に対応したプリンタ機能を標準搭載しているもの、もしく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。SPCL 言語に対応したプリンタ機能を標準搭載しているもの、もしくはオプションにより搭載した場合は、ネットワークからのプリントデータ受信を除く 1）のみの実施が可能となる。）

c) スキャン送信機能

MFD のスキャン送信機能は、スキャンした実イメージデータを、指定された形式に変換し、ネットワークに接続されている FTP サーバ、もしくはメールサーバに転送する機能である。
MFD の内蔵する Web 画面から送信先を登録しておき、MFD の操作パネルから送信先を指定する。また、メールサーバへの転送では、メールアドレスを直接入力することも可能となっている。
（FTP サーバへ送信する Scan-to-FTP、クライアントで稼働している FTP サーバへ送信する Scan-to-Desktop、及びメールサーバへ送信する Scan-to-Email が可能である。Scan-to-Desktop によるスキャン送信機能を利用するためには、クライアントにスキャンツールをインストールし、クライアントにてスキャンツール（FTP サーバ）を稼動させておく必要がある。）

① MFD の操作パネルからの操作の場合は、MFD のスキャナユニットに利用者が原稿をセットし、操作パネルで必要な設定の後、本体スタートボタンを押下することによりスキャン送信ジョブが開始される。

② スキャナユニットで原稿をスキャンし、実イメージデータとして読み取る。

③ 読み取った実イメージデータを、操作パネルの設定に基づく形式に変換し、ネットワークに送出することにより、操作パネルにて指定された送信先に送信する。

（この機能は TOE を搭載可能な MFD のうち、シャープ PCL 言語に対応したプリンタ機能を標準搭載しているもの、もしく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。）

d) PCFAX 機能

MFD の PCFAX 機能は、クライアントから送付されてくる PCFAX データをファクス送信する機能である。
送信先の指定はクライアント側で行い、パラレル、USB、もしくはネットワークに接続されているネットワーク I/F を介して、クライアントから PCFAX データを受信することにより実施される。

① MFD 用の PCFAX 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、必要な設定の後、プレビューウィンドウにて完了ボタンをクリックすると、PCFAX ドライバにて PCFAX データが生成される。生成された PCFAX データは、パラレル、USB、もしくはネットワーク I/F を介して MFD に転送される。MFD がこの PCFAX データを受信することにより PCFAX ジョブが開始される。

② クライアントから受信した PCFAX データは、ファクス回線に送出できないため、ファクス回

線へ送出可能な実イメージデータに変換する。

③ 実イメージデータをファクス回線に送出することにより、送信先 FAX 機へファクス送信する。

（この機能は TOE を搭載可能な MFD のうち、プリンタ機能、及び FAX 機能を標準搭載しているもの、もしく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。）

e) ファクス送信機能

MFD のファクス送信機能は、MFD の操作パネルにて指定した送信先 FAX 機にファクス送信する機能である。

送信先番号の入力は MFD の操作パネルで行う。また、MFD の操作パネルから登録されているオートダイヤル登録番号を利用することも可能である。

操作パネルにて、送信先等の必要な設定の後、スタートキーを押下することにより実施される。

① MFD のスキャナユニットに利用者が原稿をセットし、操作パネルで必要な設定の後、スタートボタンを押下することによりファクス送信ジョブが開始される。

② スキャナユニットで原稿をスキャンし、実イメージデータとして読み取る。

③ 実イメージデータを、ファクス回線へ送出可能な実イメージデータに変換する。

④ 実イメージデータをファクス回線に送出することにより、送信先 FAX 機へファクス送信する。

（この機能は TOE を搭載可能な MFD のうち、FAX 機能を標準搭載しているもの、もしく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。）

f) ファクス受信機能

MFD のファクス受信機能は、送信元 FAX 機より MFD に対してファクス送信した場合、MFD がファクス受信し印字する機能である。

ファクス送信元 FAX 機より MFD に対してファクス送信することにより実施される。

① ファクス回線より、ファクス受信したことを検知し、ファクス受信ジョブを開始する。

② ファクス回線より実イメージデータ（ファクス受信データ）を取得する。

③ ファクス回線より受信した実イメージデータは、MFD で直接印刷が行えないため、MFD で印刷を行える実イメージデータに変換する。

④ 変換された実イメージデータを、エンジンユニットで印字する。

（この機能は TOE を搭載可能な MFD のうち、FAX 機能を標準搭載しているもの、もしく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。）

2.3.2 TOE の運用方法

TOE は、識別認証（TSF_AUT）されたキーオペレーターのみが運用可能である。キーオペレーターとして認証後、TOE のセキュリティ管理機能(TSF_FMT)、及びデータ消去機能(TSF_FDC)により、下記の設定、実行が可能となる。

- キーオペレーターコードの変更（改変）
- キーオペレーターの操作による全データエリア消去

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、PCFAX、ファクス送信、ファクス受信処理終了後、もしくは各処理の中止により、MFD 内の揮発性メモリ、もしくは不揮発性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。

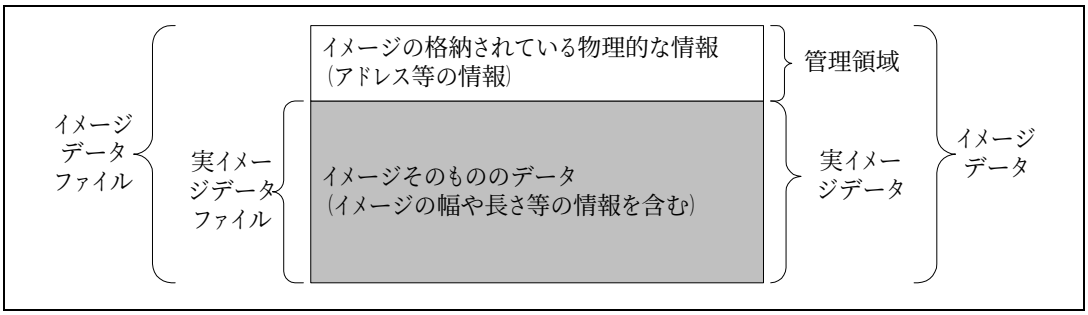

図 4: 実イメージデータ説明

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洩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

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 4で詳述する環境が必要となる。

表 4: 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 5に示す。

表 5: 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洩させる。

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 6に示す。

表 6: 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、PCFAX、ファクス送信、ファクス受信ジョブ終了、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

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 7に示す。

表 7: TOE のセキュリティ対策方針

識別子	定義
O.RESIDUAL	コピー、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信ジョブ終了、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て上書き消去する。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て上書き消去を実施する。
O.REMOVE	TOEが組込まれている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。

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 8に示す。

表 8: 環境のセキュリティ対策方針

識別子	定義
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。
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。

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

5.1.1.1 クラス FCS: 暗号サポート

a) 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_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

b) 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、及び 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: 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: 利用者のデータ保護

a) 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

a) 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

b) 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、[入力された文字数だけの"*"表示]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

c) FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 認証のタイミング

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

d) 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

5.1.1.4 クラス FMT: セキュリティ管理

a) 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〔 キーオペレーターの操作による全データエリア消去機能 〕[を動作させる、を停止させる]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_SMR.1 セキュリティ役割
FMT_SMF.1 機能管理の特定

b) 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

c) 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_SMR.1 セキュリティ役割
FMT_SMF.1 機能管理の特定

d) 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

e) 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 9に示す TOE の管理項目を管理する機能]。

依存性: なし。

表 9: TOE の管理項目

機能要件	管理項目
FCS_CKM.1	なし（暗号鍵の属性の変更を行っていない）
FCS_COP.1、FIA_UAU.7、FMT_MSA.2、FMT_SMF.1	なし（管理項目要請なし）
FDP_RIP.1	なし（上書き消去のタイミングはオブジェクトからの資源の割当て解除時のみであるため管理する必要はない）
FIA_UAU.2	キーオペレーターコード
FIA_UID.2	なし（利用者識別情報、識別操作が固定であるため管理しない）
FIA_SOS.1	なし（品質尺度は固定値であり管理を行わない）
FMT_MOF.1、FMT_MTD.1	なし（TSF の機能（TSF データ）と相互に影響を及ぼす役割グループは固定であるため管理の必要がない）
FMT_SMR.1	なし（役割の一部をなす利用者はキーオペレーターのみであるため管理の必要がない）

5.1.1.5 クラス FPT: TSF の保護

a) 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 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 10に示す。表 10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 10:　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

5.1.3　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、FIA_UAU.7、FIA_SOS.1 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

TOE のセキュリティ対策方針に対処する IT 環境はない。

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 11に示す。表 11は、セキュリティ機能要件と TOE セキュリティ仕様ついて、その対応を記載している節を示したものである。

表 11: セキュリティ機能要件と TOE セキュリティ仕様

セキュリティ機能要件	TOE セキュリティ仕様				
	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT
FCS_CKM.1	6.1.1節				
FCS_COP.1		6.1.2節			
FDP_RIP.1			6.1.3節		
FIA_UAU.2			6.1.3節	6.1.4節	
FIA_UAU.7			6.1.3節	6.1.4節	
FIA_UID.2			6.1.3節	6.1.4節	
FIA_SOS.1					6.1.5節
FMT_MOF.1			6.1.3節	6.1.4節	
FMT_MSA.2	6.1.1節				
FMT_MTD.1				6.1.4節	6.1.5節
FMT_SMR.1				6.1.4節	6.1.5節
FMT_SMF.1					6.1.5節
FPT_RVM.1	6.1.1節	6.1.2節	6.1.3節	6.1.4節	6.1.5節

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 基板に搭載されている揮発性メモリ（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。

a) 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 基板に搭載されている揮発性メモリ（IMC_RAM）にスプ

ール保存されている IMC_RAM 内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、実イメージデータとして PCL 基板に搭載されている揮発性メモリ（PCL_RAM）にスプール保存されている PCL_RAM 内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、実イメージデータとして FAX 基板に搭載されている Flash メモリにスプール保存されている Flash メモリ内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。

b) キーオペレーターの操作による全データエリア消去
キーオペレーターの操作による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。
キーオペレーターの操作によ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 基板に搭載されている揮発性メモリ（IMC_RAM）、PCL 基板に搭載されている揮発性メモリ（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。
キーオペレーターの操作によ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、入力数に対応し”*”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、キーオペレーターの操作による全データエリア消去のタイミングは、各ジョブ完了後、キーオペレーターの操作による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 基板に搭載されている揮発性メモリ、PCL 基板に搭載されている揮発性メモリ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)のうちのキーオペレーターの操作による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 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 12に示す。

表 12: 保証手段

コンポーネント	コンポーネント名	保証手段
ACM_CAP.3	許可の管理	デジタル複合機データセキュリティキットAR-FR12M 構成管理説明書, デジタル複合機データセキュリティキットAR-FR12M VERSION M.20 構成リスト
ACM_SCP.1	TOEのCM範囲	
ADO_DEL.1	配付手続き	デジタル複合機データセキュリティキットAR-FR12M 配付手順説明書
ADO_IGS.1	設置、生成、及び 立上げ手順	AR-FR12M設置手順書, AR-FR12M設置手順書(英独仏西語版)
ADV_FSP.1	非形式的機能仕様	デジタル複合機データセキュリティキットAR-FR12M セキュリティ機能仕様書
ADV_HLD.2	セキュリティ 実施上位レベル設計	デジタル複合機データセキュリティキットAR-FR12M 上位レベル設計書
ADV_RCR.1	非形式的対応の実証	デジタル複合機データセキュリティキットAR-FR12M 表現対応分析書
ADV_SPM.1	非形式的なTOEセキュリティ方針モデル	デジタル複合機データセキュリティキットAR-FR12M セキュリティ方針モデル仕様書
AGD_ADM.1	管理者ガイダンス	取扱説明書セキュリティキット AR-FR12M, 注意書セキュリティキット AR-FR12M, AR-FR12M Data Security Kit Operation Manual, AR-FR12M 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, 取扱説明書デジタル複合機コピー編, 取扱説明書デジタル複合機ファクス編, 取扱説明書デジタル複合機ネットワークスキャナ編, オンラインマニュアル(ネットワークプリンタ編)
AGD_USR.1	利用者ガイダンス	
ALC_DVS.1	セキュリティ手段の識別	デジタル複合機データセキュリティキットAR-FR12M 開発セキュリティ仕様書
ATE_COV.2	カバレージの分析	デジタル複合機データセキュリティキットAR-FR12M カバレージ分析書
ATE_DPT.1	テスト:上位レベル設計	デジタル複合機データセキュリティキットAR-FR12M 上位レベル設計テスト分析書
ATE_FUN.1	機能テスト	デジタル複合機データセキュリティキットAR-FR12M 機能テスト仕様書
ATE_IND.2	独立テスト - サンプル	TOE
AVA_MSU.1	ガイダンスの検査	取扱説明書セキュリティキット AR-FR12M, 注意書セキュリティキット AR-FR12M, AR-FR12M Data Security Kit Operation Manual, AR-FR12M 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, 取扱説明書デジタル複合機コピー編, 取扱説明書デジタル複合機ファクス編, 取扱説明書デジタル複合機ネットワークスキャナ編, オンラインマニュアル(ネットワークプリンタ編)
AVA_SOF.1	機能強度	デジタル複合機データセキュリティキットAR-FR12M セキュリティ機能強度分析書

コンポーネント	コンポーネント名	保証手段
AVA_VLA.1	開発者脆弱性分析	デジタル複合機データセキュリティキットAR-FR12M 脆弱性分析書

6.3 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セキュリティ機能は、FIA_UAU.2、FIA_UAU.7 に対応する認証(TSF_AUT)、及びデータ消去(TSF_FDC)、FIA_SOS.1 に対応するセキュリティ管理(TSF_FMT)が該当する。認証とセキュリティ管理は、パスワードに関わるメカニズムを提供するものであり、確率的順列的メカニズムである。これらのセキュリティ機能強度は、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、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 13に検証する。表 13は、脅威、前提条件、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を示したものである。

表 13: セキュリティ対策方針根拠

セキュリティ対策方針	脅威	前提条件	組織のセキュリティ方針
	T.RECOVER	A.OPERATOR	P.RESIDUAL
O.RESIDUAL			8.1.3節
O.REMOVE	8.1.1節		
OE.OPERATE		8.1.2節	
OE.ERASEALL			8.1.3節

8.1.1 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（FAX_RAM、PCL_RAM 及び IMC_RAM）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。

8.1.2 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。

8.1.3 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 14に示す。表 14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を示したものである。

表 14: TOE セキュリティ機能要件根拠

機能要件	セキュリティ対策方針	
	O.RESIDUAL	O.REMOVE
FCS_CKM.1		8.2.1.2節
FCS_COP.1		8.2.1.2節
FDP_RIP.1	8.2.1.1節	
FIA_UAU.2	8.2.1.1節	
FIA_UAU.7	8.2.1.1節	
FIA_UID.2	8.2.1.1節	
FIA_SOS.1	8.2.1.1節	
FMT_MOF.1	8.2.1.1節	
FMT_MSA.2		8.2.1.2節
FMT_MTD.1	8.2.1.1節	
FMT_SMR.1	8.2.1.1節	
FMT_SMF.1	8.2.1.1節	
FPT_RVM.1	8.2.1.1節	8.2.1.2節

8.2.1.1 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、ジョブ完了後、キーオペレーターの操作による全データエリア消去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、FIA_UID.2 にて、キーオペレーターを識別認証する。

c) キーオペレーターのみ、全データエリア消去機能の起動と停止が、FMT_MOF.1 により可能となる。

d) 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。

e) キーオペレーターは、FMT_MOF.1、及び FMT_MTD.1 により、TOE の管理の役割を任され、この役割は FMT_SMR.1 にて維持されるため、キーオペレーター操作による全データエリア消去の起動および停止、キーオペレーターコードの問合せおよび変更が、キーオペレーターに制限されるため、キーオペレーターからの指示に従い MSD の全データ領域に対して上書き消去を行うことができる。

f) 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。

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

8.2.1.2 O.REMOVE

O.REMOVE は、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り、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_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。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。また、FPT_RVM.1 により、O.REMOVE を実現する機能要件を迂回できないようにサポートする。

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 15に示す。表 15は、CC が規定するセキュリティ機能要件が満たすべき依存性と、本 TOE が満たしている依存性、及び本 TOE が依存性を満足していないことの妥当性を記載している節を示したものである。

表 15: セキュリティ機能要件の依存性

機能要件	満足すべき依存性	満足している依存性	依存性不満足の妥当性
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	8.2.2.1節
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	8.2.2.1節
FDP_RIP.1	なし	なし	
FIA_UAU.2	FIA_UID.1	FIA_UID.2(*)	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2(*)	
FIA_UID.2	なし	なし	
FIA_SOS.1	なし	なし	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1	ADV_SPM.1, FMT_SMR.1	8.2.2.2節
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	
FMT_SMR.1	FIA_UID.1	FIA_UID.2(*)	
FMT_SMF.1	なし	なし	
FPT_RVM.1	なし	なし	

(*) FIA_UID.1 及び FIA_UAU.1 への依存性は、上位階層の FIA_UID.2 及び FIA_UAU.2 によって満足される。

8.2.2.1 FCS_CKM.4 の依存性を必要としない根拠

暗号鍵は揮発性メモリ（FAX_RAM）内に保存しているが、電源断（電源オフ）により、暗号鍵が保存された揮発性メモリ内の電荷が消失し、暗号鍵が破棄されるため依存性を必要としない。

8.2.2.2 FMT_MSA.1 及び FDP_ACC.1 の依存性を必要としない根拠

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 は必要がない。同様にアクセス制御は必要がないため、FDP_ACC.1 は必要がない。

8.2.3 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 16に示す。

表 16: セキュリティ要件の相互作用

機能要件	防御を提供している要件	
	迂回	非活性化
FCS_CKM.1	FPT_RVM.1	なし
FCS_COP.1	FPT_RVM.1	なし
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_UAU.2	FPT_RVM.1	なし
FIA_UAU.7	FPT_RVM.1	なし
FIA_UID.2	FPT_RVM.1	なし
FIA_SOS.1	FPT_RVM.1	なし
FMT_MOF.1	FPT_RVM.1	なし
FMT_MSA.2	なし	なし
FMT_MTD.1	FPT_RVM.1	なし
FMT_SMR.1	なし	なし
FMT_SMF.1	なし	なし

8.2.3.1 迂回

表 16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るために迂回できない。
b) 暗号操作 FCS_COP.1 は、実イメージデータを必ず暗号化してスプール保存する。また、暗号化した実イメージデータは必ず復号して利用するため迂回できない。
c) サブセット残存情報保護 FDP_RIP.1 は、ジョブ完了時、キーオペレーター操作による全データエリア消去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、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実行の場合、必ずキーオペレーターの識別認証を必要とし、また全データエリア消去の中断の場合、キャンセル操作後、必ずキーオペレーター認証が呼び出されるため迂回できない。
g) TSF データの管理 FMT_MTD.1 は、必ずキーオペレーターの識別認証を必要とし、設定値は EEPROM 内に保存されるため迂回できない。

8.2.3.2 非活性化

表 16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ことを保証する。

8.2.3.3 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。

8.2.4 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洩させることである。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。

8.2.5 最小機能強度根拠

データセキュリティキット AR-FR12M 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。AR-FR12M 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_UAU.2、FIA_UAU.7、FIA_SOS.1 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 11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

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

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

FDP_RIP.1 は、各ジョブ完了後の終了後の自動消去について、TSF_FDC による揮発性メモリ（コピージョブ、プリントジョブ完了後の自動消去は IMC 基板に搭載されている揮発性メモリ、スキャン送信ジョブ完了後の自動消去は PCL 基板に搭載されている揮発性メモリ、PCFAX ジョブ、ファクス送信、ファクス受信ジョブについては Flash メモリ）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ことにより残存情報を保護するため、またキーオペレーターの操作による全データエリア消去について、TSF_FDC による 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ことにより残存情報を保護するため、満足される。

8.3.1.4 FIA_UAU.2

FIA_UAU.2 は、TSF_AUT により、セキュリティ管理機能（キーオペレータープログラム）にアクセスするためには、キーオペレーターコードの入力による認証を行うため、満足される。また、TSF_FDC により、キーオペレーターの操作による全データエリア消去の中断の場合、キーオペレーターコードの入力を要求するため、満足される。

8.3.1.5 FIA_UAU.7

FIA_UAU.7 は、TSF_AUT による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、入力文字に対応して”*”を表示するため、満足される。また、TSF_FDC により、キーオペレーターの操作による全データエリア消去の中断の場合のキーオペレーターコード入力において、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”*”を表示するため、満足される。

8.3.1.6 FIA_UID.2

FIA_UID.2 は、TSF_AUT によるキーオペレータープログラムの選択、TSF_FDC によるキャンセル操作の選択によりキーオペレーターを識別しているため、満足される。

8.3.1.7 FIA_SOS.1

FIA_SOS.1 は、TSF_FMT によるキーオペレーターコードの変更（改変）は、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することにより、満足される。

8.3.1.8 FMT_MOF.1

FMT_MOF.1 は、TSF_AUT によるキーオペレーターの識別認証後、TSF_FDC によるキーオペレーターの操作による全データエリア消去の実行、また TSF_FDC によるキーオペレーターの識別認証により、全データエリア消去の中断を可能とするため、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もと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_SMR.1

FMT_SMR.1 は、TSF_AUT による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により、役割への関連づけ行っているため、満足される。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ため、満足される。

8.3.1.12 FMT_SMF.1

FMT_SMF.1 は、FIA_UAU.2 の管理項目である TSF_FMT によるキーオペレーターコードを管理する能力を持っており、満足される。

なお、暗号鍵属性は、ADV_SPM.1 により保証された暗号鍵の生成を行っており、属性の変更管理は必要がなく、FCS_CKM.1、FMT_MSA.2 についての管理項目は要請されていない。上書き消去のタイミングは、オブジェクトからの資源の割当て解除時のみであるため管理する必要はなく、FDP_RIP.1 についての管理項目はない。秘密の検証尺度についても、固定値（5文字及び数字）であり、管理する必要がないため、FIA_SOS.1 についての管理項目はない。利用者識別情報は、識別操作が固定であるため管理する必要がなく、FIA_UID.2 についての管理項目はない。TSF の機能や TSF データと相互に影響を及ぼす役割グループは固定であるため管理の必要はなく、FMT_MOF.1、FMT_MTD.1 の管理項目はない。

役割の一部をなす利用者は、キーオペレーター1人のみであり、管理の必要がないため FMT_SMR.1 の管理項目もない。

8.3.1.13 FPT_RVM.1

FPT_RVM.1 は、以下に示す IT セキュリティ機能により、該当する機能要件が必ず実施され、迂回されないため満足する。

a) FCS_CKM.1 は、MFD の電源が ON になると、必ず TSF_FKG にて暗号鍵が生成されるため、満足される。

b) FCS_COP.1 は、実イメージデータを揮発性メモリにスプール保存する場合、必ず TSF_FDE にて暗号化される。また、揮発性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出してジョブ処理する場合、必ず TSF_FDE にて復号されるため、満足される。

c) FDP_RIP.1 は、各ジョブが完了した場合、キーオペレーターの操作による全データエリア消去が実行された場合、必ず TSF_FDC により上書き消去が実施されるため、満足される。

d) FIA_UAU.2、及び FIA_UID.2 は、キーオペレーターを識別認証する場合、必ず TSF_AUT、及び TSF_FDC にてキーオペレーターの識別認証が実行されるため、満足される。

e) FIA_UAU.7 は、キーオペレーター認証時に、必ず TSF_AUT、及び TSF_FDC にて入力数に対応し"*"を表示するため、満足される。

f) FIA_SOS.1 は、キーオペレーターコードの変更（改変）時に、必ず TSF_FMT にて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が実行されるため、満足される。

g) FMT_MOF.1 は、キーオペレーターの操作による全データエリア消去の実行及び中断は、必ず TSF_AUT 及び TSF_FDC によるキーオペレーターの識別認証後に、TSF_FDC にて全データエリア消去の実行及び中断が実施されるため、満足される。

h) FMT_MTD.1 は、TSF_AUT によるキーオペレーターの識別認証後に、必ず TSF_FMT により、キーオペレーターコードの変更（改変）が実施されるため満足される。

8.3.2 TOE 保証手段根拠

6.2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: デジタル複合機データセキュリティキットAR-FR12M構成管理説明書,
デジタル複合機データセキュリティキット AR-FR12M VERSION M.20 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: デジタル複合機データセキュリティキット AR-FR12M 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-FR12M 設置手順書

内容: サービスマンが行う 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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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 の方針の間の対応を規定し、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: 取扱説明書セキュリティキット AR-FR12M,
注意書セキュリティキット AR-FR12M,
AR-FR12M Data Security Kit Operation Manual,
AR-FR12M 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,
取扱説明書デジタル複合機コピー編,
取扱説明書デジタル複合機ファクス編,
取扱説明書デジタル複合機ネットワークスキャナ編,
オンラインマニュアル（ネットワークプリンタ編）

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: 取扱説明書セキュリティキット AR-FR12M,
注意書セキュリティキット AR-FR12M,
AR-FR12M Data Security Kit Operation Manual,
AR-FR12M 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,
取扱説明書デジタル複合機コピー編,
取扱説明書デジタル複合機ファクス編,
取扱説明書デジタル複合機ネットワークスキャナ編,
オンラインマニュアル（ネットワークプリンタ編）

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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 機能テスト仕様書

内容: 全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: 取扱説明書セキュリティキット AR-FR12M,
注意書セキュリティキット AR-FR12M,
AR-FR12M Data Security Kit Operation Manual,
AR-FR12M 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,
取扱説明書デジタル複合機コピー編,
取扱説明書デジタル複合機ファクス編,
取扱説明書デジタル複合機ネットワークスキャナ編,
オンラインマニュアル（ネットワークプリンタ編）

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: デジタル複合機データセキュリティキット AR-FR12M 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: デジタル複合機データセキュリティキット AR-FR12M 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

TOE が提供される確率的または順列的メカニズムは、利用するセキュリティ機能がキーオペレーター認証（TSF_AUT）、データ消去（TSF_FDC）、及びキーオペレーターコード改変（TSF_FMT）である。これらのセキュリティ機能強度は SOF 基本である。一方 TOE の最小機能強度は SOF 基本である。従って、両者の機能強度レベルは矛盾していないのでセキュリティ機能強度 SOF 基本は妥当である。