

**SHARP®**

データセキュリティキット

AR-FR22

セキュリティターゲット

Version 0.09

シャープ株式会社

## 【履歴】

日付	バージョン	変更点	作成	承認
2005年 1月31日	0.01	・初版作成	岩崎	山中
2005年 2月21日	0.02	・プリンタ機能修正 ・ガイダンス文書修正 ・誤植訂正	岩崎	山中
2005年 4月5日	0.03	・指摘内容反映 ・TOEの版番号修正	岩崎	山中
2005年 4月13日	0.04	・ガイダンス文書修正 ・TOEを登載可能なMFD名修正	岩崎	山中
2005年 4月25日	0.05	・指摘内容反映	岩崎	山中
2005年 6月22日	0.06	・指摘内容反映	岩崎	山中
2005年 6月23日	0.07	・指摘内容反映	岩崎	山中
2005年 6月29日	0.08	・指摘内容反映	岩崎	山中
2005年 7月21日	0.09	・指摘内容反映	岩崎	山中

## 【目次】

1	ST 概説	1
1.1	ST 識別	1
1.2	ST 概要	1
1.3	CC 適合	1
1.4	参照資料	1
1.5	規約、専門用語、略語	2
1.5.1	規約	2
1.5.2	専門用語	2
1.5.3	略語	3
2	TOE 記述	4
2.1	TOE の概要	4
2.1.1	TOE 種別	4
2.1.2	TOE セキュリティ機能の概要	4
2.2	TOE 構成	4
2.2.1	TOE の物理的構成	4
2.2.2	TOE の論理的構成	5
2.3	TOE の利用	6
2.3.1	TOE 利用方法	6
2.3.1.1	コピー機能	7
2.3.1.2	プリンタ機能	7
2.3.1.3	スキャン送信機能	8
2.3.1.4	PCFAX 機能	8
2.3.1.5	ファクス送信機能	8
2.3.1.6	ファクス受信機能	8
2.3.2	TOE の運用方法	8
2.4	TOE の保護資産	9
3	TOE セキュリティ環境	10
3.1	前提条件	10
3.2	脅威	10
3.3	組織のセキュリティ方針	10
4	セキュリティ対策方針	11
4.1	TOE のセキュリティ対策方針	11
4.2	環境のセキュリティ対策方針	11
5	ITセキュリティ要件	12
5.1	TOE セキュリティ要件	12
5.1.1	TOE セキュリティ機能要件	12
5.1.1.1	クラス FCS: 暗号サポート	12
5.1.1.2	クラス FDP: 利用者のデータ保護	12
5.1.1.3	クラス FIA: 識別と認証	12
5.1.1.4	クラス FMT: セキュリティ管理	13
5.1.1.5	クラス FPT: TSF の保護	15
5.1.2	TOE セキュリティ保証要件	15
5.1.3	最小機能強度	15

5.2	IT 環境に対するセキュリティ要件.....	16
6	TOE 要約仕様 .....	17
6.1	TOE セキュリティ機能(TSF).....	17
6.1.1	暗号鍵生成(TSF_FKG) .....	17
6.1.2	暗号操作(TSF_FDE).....	17
6.1.3	データ消去 (TSF_FDC) .....	17
6.1.4	認証 (TSF_AUT).....	18
6.1.5	セキュリティ管理 (TSF_FMT) .....	18
6.2	保証手段 .....	19
6.3	セキュリティ機能強度 .....	19
7	PP 主張.....	21
8	根拠 .....	22
8.1	セキュリティ対策方針根拠 .....	22
8.1.1	T.RECOVER .....	22
8.1.2	A.OPERATOR.....	22
8.1.3	P.RESIDUAL .....	22
8.2	セキュリティ要件根拠 .....	22
8.2.1	セキュリティ機能要件根拠 .....	23
8.2.1.1	O.RESIDUAL .....	23
8.2.1.2	O.REMOVE .....	24
8.2.2	セキュリティ機能要件の依存性根拠.....	24
8.2.2.1	FCS_CKM.4 の依存性を必要としない根拠.....	25
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 .....	25
8.2.3	セキュリティ要件の相互作用 .....	25
8.2.3.1	迂回.....	25
8.2.3.2	非活性化.....	26
8.2.3.3	干渉.....	26
8.2.4	TOE セキュリティ保証要件根拠.....	26
8.2.5	最小機能強度根拠.....	26
8.3	TOE 要約仕様根拠.....	26
8.3.1	TOE 要約仕様根拠.....	26
8.3.1.1	FCS_CKM.1.....	26
8.3.1.2	FCS_COP.1 .....	26
8.3.1.3	FDP_RIP.1 .....	26
8.3.1.4	FIA_AFL.1 .....	27
8.3.1.5	FIA_UAU.2.....	27
8.3.1.6	FIA_UAU.7.....	27
8.3.1.7	FIA_UID.2 .....	27
8.3.1.8	FIA_SOS.1.....	27
8.3.1.9	FMT_MOF.1.....	27
8.3.1.10	FMT_MSA.2 .....	27
8.3.1.11	FMT_MTD.1.....	27
8.3.1.12	FMT_SMR.1 .....	27
8.3.1.13	FMT_SMF.1 .....	27

8.3.1.14	FPT_RVM.1.....	28
8.3.2	TOE 保証手段根拠.....	28
8.3.3	TOE セキュリティ機能強度根拠.....	30

【表のリスト】

表 1:	参照資料.....	1
表 2:	専門用語.....	2
表 3:	略語.....	3
表 4:	前提条件.....	10
表 5:	脅威.....	10
表 6:	組織のセキュリティ方針.....	10
表 7:	TOE のセキュリティ対策方針.....	11
表 8:	環境のセキュリティ対策方針.....	11
表 9:	認証失敗時のアクション.....	13
表 10:	TOE の管理項目.....	14
表 11:	保証要件.....	15
表 12:	セキュリティ機能要件と TOE セキュリティ仕様.....	17
表 13:	保証手段.....	19
表 14:	セキュリティ対策方針根拠.....	22
表 15:	TOE セキュリティ機能要件根拠.....	23
表 16:	セキュリティ機能要件の依存性.....	24
表 17:	セキュリティ要件の相互作用.....	25

【図のリスト】

図 1:	MFD の物理的構成と TOE.....	4
図 2:	TOE の論理的構成図.....	5
図 3:	TOE の利用環境.....	7
図 4:	実イメージデータ説明.....	9

# 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-FR22 セキュリティターゲット  
 バージョン: 0.09  
 作成日: 2005 年 7 月 21 日  
 製作者: シャープ株式会社  
 TOE 識別: AR-FR22 VERSION S.10  
 CC 識別: CC バージョン 2.1, ISO/IEC 15408:1999, JIS X 5070:2000, CCIMB Interpretations-0407  
 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-FR22 について説明したものである。

本 TOE は、デジタル複合機 (Multi Function Device 以下 MFD と略称) 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 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)
[HOSOKU-0407]	CCIMB Interpretations-0407

## 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
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。
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-FR22。
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MSD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。キーオペレーターのみが実施可能であるため、キーオペレーターの操作による全データエリア消去ともいう。

用語	定義
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	不揮発性メモリ的一种で、低頻度であれば電氣的に任意部分の書き換えを可能にしたROM (Electrically Erasable Programmable ROM)。
Flashメモリ	不揮発性メモリ的一种で、電氣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)。
IFAX	インターネットFAX (Internet FAX)。
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揮発性メモリ、及び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)。
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)。
TIFF-FX	インターネットFAX規格で規定された画像フォーマット。

## 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、ファクス受信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、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信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

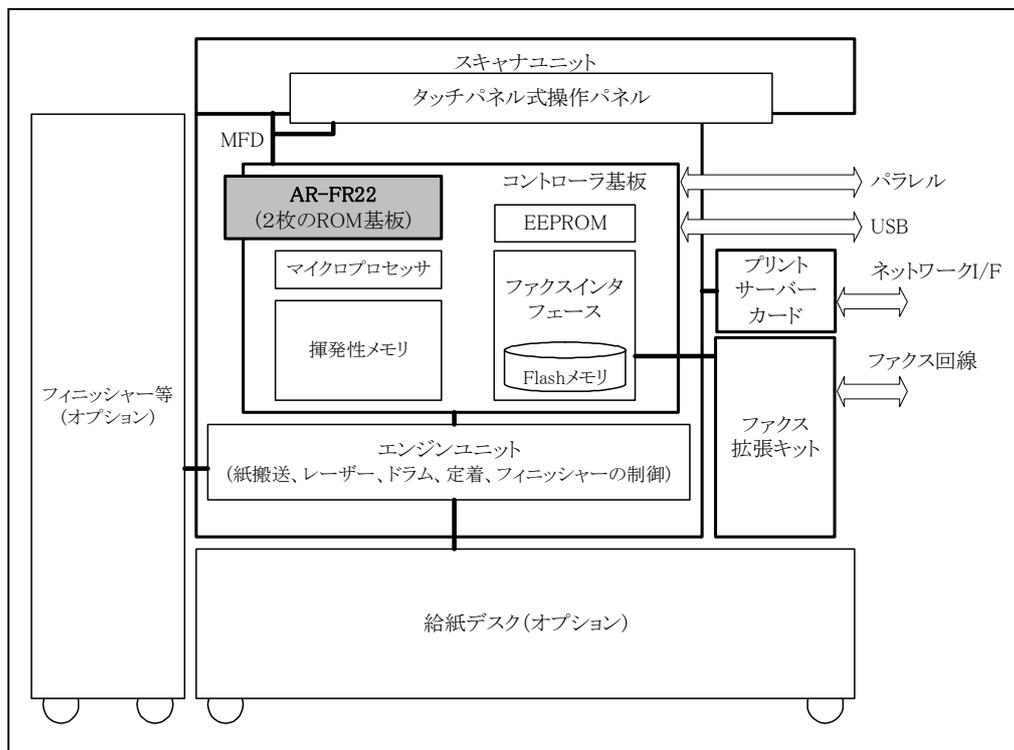


図 1: MFD の物理的構成と TOE

TOE である AR-FR22 は、2枚の ROM 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-M351U, AR-M451U, AR-M355U, AR-M455U, AR-M355UJ, AR-M455UJ, AR-311S, AR-351S, AR-451S, AR-311FP, AR-351FP, AR-451FP である。

TOE の物理的範囲は、以下の通りである。

- a) 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。

## 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。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、網掛け部分がセキュリティ機能である。

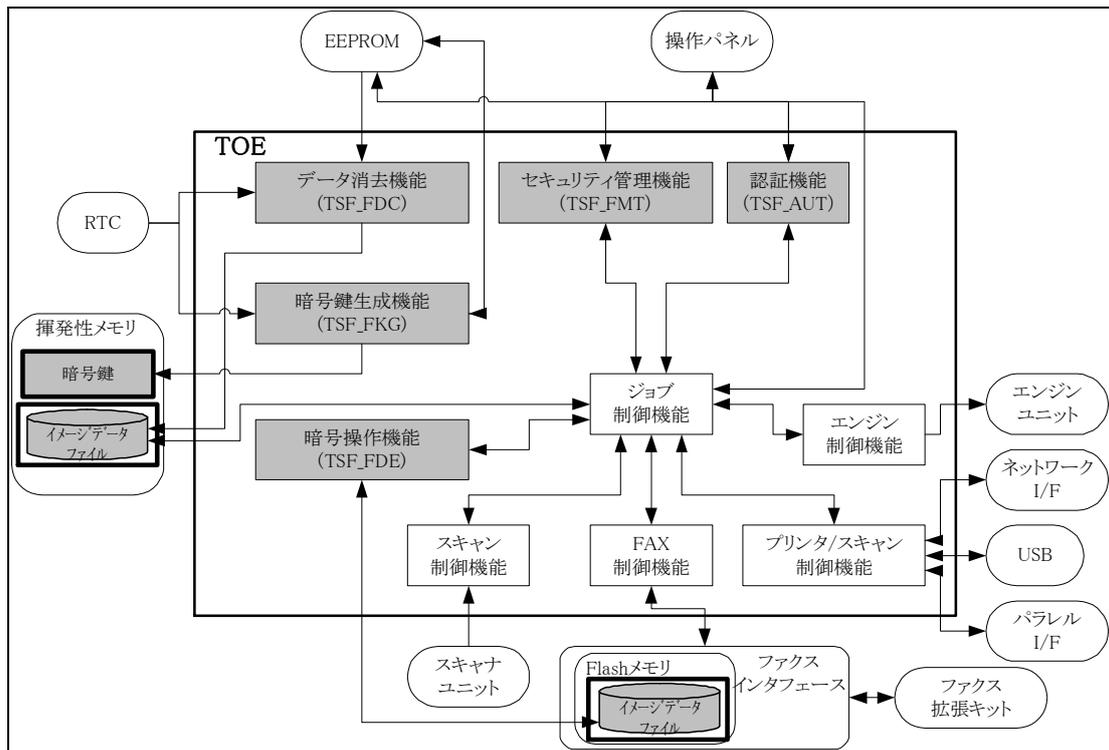


図 2: TOE の論理的構成図

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、ファクス送信、ファクス受信の各ジョブに関し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)  
 各ジョブにより 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、固定値を上書き消去する。

- キーオペレーターの操作による全データエリア消去  
(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 の所有者変更、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)  
揮発性メモリ 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、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。  
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/スキャン制御機能  
TOE を搭載可能な MFD のうち、プリンタ機能を標準、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。また、ネットワークを利用する場合はネットワーク機能をオプションにより搭載した場合に実施が可能である。
  - プリントジョブにおいては、パラレル、USB I/F、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。
- 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) 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 MFD のコピー、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信の各動作を制御する。

## 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。

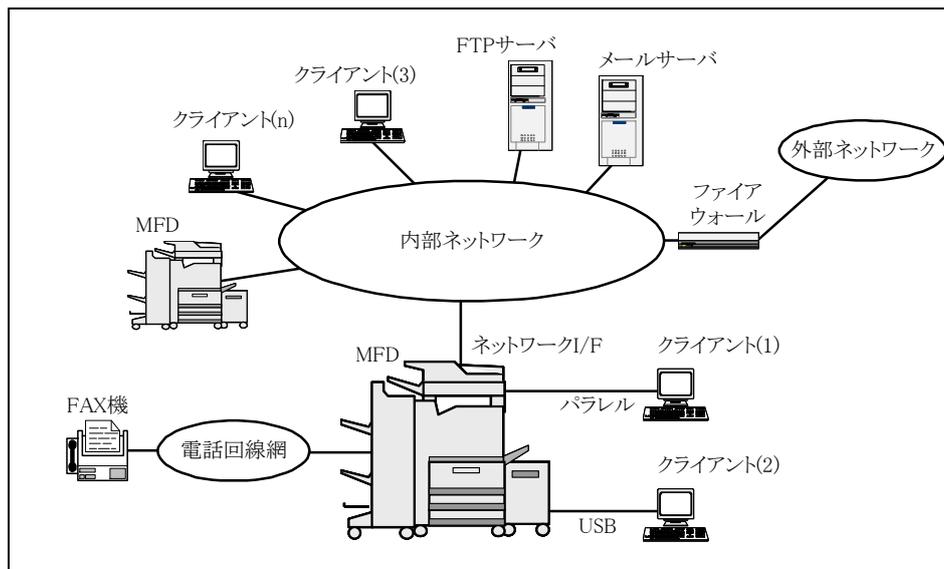


図 3: TOE の利用環境

### 2.3.1.1 コピー機能

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。

また、コピー機能の一つにタンデムコピー機能がある。この機能は TOE を搭載可能な MFD のうち、ネットワークを標準、もしくはオプションにより搭載した2台の MFD にて実施することができる。タンデムコピー機能とは、2 台の MFD が内部ネットワークに接続され、原稿を読み取った MFD (親機) が他の MFD (子機) 宛に、内部ネットワーク経由で実イメージデータを転送し、利用者が指定したコピー部数を各々折半し分担して印刷出力する機能である。ただし、親機 MFD と子機 MFD の両方に TOE が搭載されている場合はタンデムコピー機能が利用できるが、TOE を搭載した親機 MFD から、TOE を搭載していない子機 MFD に対してのタンデムコピー機能は動作しない。

### 2.3.1.2 プリンタ機能

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。

この機能は TOE を搭載可能な MFD のうち、プリンタ機能を標準、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。

MFD がプリントデータを取得するには以下の4つの方法がある。

- 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から印刷開始を指示すると、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)と共に直接ネットワーク I/F を介して受信する。(E-mail プリント機能)
- 3) ネットワークに接続されている FTP サーバに、MFD の操作パネルからの操作により、MFD 自身が FTP サーバにあるファイル(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。(FTP プルプリント機能)
- 4) 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 MFD に対し、ファイル(プリントデータ)を送信する。MFD は、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)

また、プリント機能の一つにタンデムプリント機能がある。この機能は、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からタンデム印刷指定する場合について有効となる。タンデムプリントは、タン

デムコピー機能と同様、TOE を搭載可能な MFD のうち、ネットワークを標準、もしくはオプションにより搭載した2台の MFD にて実施することができる。クライアントからプリントデータを受信した MFD (親機) が他の MFD (子機) 宛に、内部ネットワーク経由で実イメージデータを転送し、利用者が指定したプリント部数を各々折半し分担して印刷出力する機能である。ただし、親機 MFD と子機 MFD の両方に TOE が搭載されている場合はタンデムコピー機能が利用できるが、TOE を搭載した親機 MFD から、TOE を搭載していない子機 MFD に対してのタンデムコピー機能は動作しない。

### 2.3.1.3 スキャン送信機能

スキャン送信機能は、MFD が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。この機能は TOE を搭載可能な MFD のうち、プリンタ機能及びネットワーク機能を標準、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。スキャン送信機能は、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 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て、FTP サーバを稼働させておく必要がある。

また、スキャン送信機能の一つに、インターネット FAX (IFAX) 機能がある。スキャンした画像を IFAX に準拠したフォーマット (TIFF-FX) に変換し、指定された相手に対し、メールサーバへの転送と同じプロトコルにて送出する機能である。

### 2.3.1.4 PCFAX 機能

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。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、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。

ファクスの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 I/F を介して、クライアントから PCFAX データを受信し、指定された送信先に送信する。

### 2.3.1.5 ファクス送信機能

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にファクス送信する機能である。この機能は TOE を搭載可能な MFD のうち、FAX 機能を標準、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。

ファクス送信先の番号の入力は、MFD の操作パネルで行う。また、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。

### 2.3.1.6 ファクス受信機能

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 がファクスを受信し印字する機能である。この機能は TOE を搭載可能な MFD のうち、FAX 機能を標準、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、キーオペレータープログラムにおいて 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。

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

キーオペレータープログラムでは、この他にジョブ状況完了エリア消去、アドレス帳/イメージ送信登録データ消去、データエリア消去回数、電源 ON 時の自動消去、電源 ON 時の自動消去回数、各ジョブ完了後の自動消去回数、プリントホールド禁止設定、データリストプリント禁止設定、ジョブ状況完了エリア表示設定、再送信キーの使用禁止、ホールドプリントデータ操作禁止の解除等の機能も提供しているが、

これらは非セキュリティ機能である。なお、各ジョブ終了時の自動消去回数、及びキーオペレーターの操作による全データエリア消去時の消去回数は、1から7の範囲で変更が可能であるが、上書き消去処理時間調整のための非セキュリティ機能である。

## 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 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。

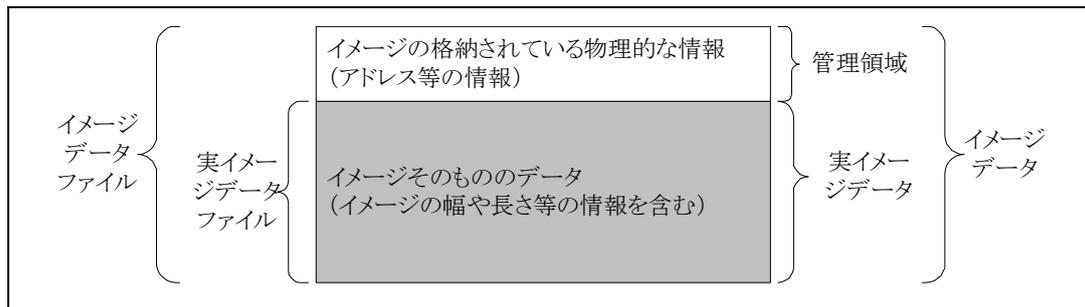


図 4: 実イメージデータ説明

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、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。
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-J 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、[ MSD にスプール保存する実イメージデータの暗号化、及び MSD 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:[ MSD 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\_AFL.1 認証失敗時の取り扱い  
 下位階層: なし  
 FIA\_AFL.1.1 TSF は、[ キーオペレーターに対する最後の認証成功以降の不成功認証試行回数 ]に関して、[ [ 3 (正の整数値) ] ] 回の不成功認証試行が生じたときを検出しなければならない。  
 FIA\_AFL.1.2 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、[ 表 9 に示すアクション ]をしなければならない。  
 依存性: FIA\_UAU.1 認証のタイミング

表 9: 認証失敗時のアクション

識別	アクション
不成功認証が3回に達した時	5分間の認証試行受付を停止
通常状態への復帰	5分間が経過すると、認証失敗回数をクリアし自動的に復帰

- b) 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
- c) 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
- d) 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
- e) 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[ 変更、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 10に示す TOE の管理項目を管理する機能 ]。  
 依存性: なし。

表 10: 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_AFL.1	なし(認証失敗回数は固定であるため管理の必要がない。 また再認証受付までの停止時間は固定であり、自動的に 通常状態へ復帰するため管理の必要がない)
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)

機能要件	管理項目
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 11に示す。表 11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 11: 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	カバレッジの分析	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	テスト: 上位レベル設計	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	機能テスト	なし
ATE_IND.2	独立テスト - サンプル	ADV_FSP.1, AGD_ADM.1, AGD_USR.1
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。

[DSK\_ST]

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、FIA\_AFL.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 12に示す。表 12は、セキュリティ機能要件と TOE セキュリティ仕様について、その対応を記載している節を示したものである。

表 12: 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_AFL.1			6.1.3節	6.1.4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-J 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する。MSN-J 拡張アルゴリズムで生成する鍵は、Flash メモリにスプール保存するための暗号操作で利用する。この暗号鍵は揮発性メモリ内に保存する。

#### 6.1.2 暗号操作(TSF\_FDE)

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 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。Flash メモリへの暗号操作には MSN-J 拡張アルゴリズムで生成された鍵を利用する。

#### 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、スキャン送信ジョブ完了後、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 Flash メモリにスプール保存されている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) キーオペレーターによる全データエリア消去  
キーオペレーターによる全データエリア消去実行の場合、認証(TSF\_AUT)による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、揮発性メモリ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、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。キーオペレーター認証において、キーオペレーターに対する最後の認証成功以降の不成功認証試行回数が連続3回の認証失敗である場合、認証入力受付を5分間停止する。認証入力停止から通常状態へは自動的に復帰し、再認証入力を受け付ける。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、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。キーオペレーター認証において、キーオペレーターに対する最後の認証成功以降の不成功認証試行回数が連続3回の認証失敗である場合、認証入力受付を5分間停止する。認証入力停止から通常状態へは自動的に復帰し、再認証入力を受け付ける。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)

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。

- a) キーオペレーターコードの変更  
キーオペレーターコードの問い合わせ、及び改変(変更)ができる。変更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する。

各設定値を変更すると、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 13に示す。

表 13: 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	データセキュリティキットAR-FR22 構成管理説明書,
ACM_SCP.1	TOEのCM範囲	データセキュリティキットAR-FR22 VERSION S.10 構成リスト
ADO_DEL.1	配付手続き	データセキュリティキットAR-FR22 配付手順説明書
ADO_IGS.1	設置、生成、及び 立上げ手順	AR-FR22設置手順書, AR-FR22設置手順書(英独仏西語版)
ADV_FSP.1	非形式的機能仕様	データセキュリティキットAR-FR22 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	データセキュリティキットAR-FR22 上位レベル設計書
ADV_RCR.1	非形式的対応の実証	データセキュリティキットAR-FR22 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	データセキュリティキットAR-FR22 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	取扱説明書データセキュリティキット AR-FR22, 注意書データセキュリティキット AR-FR22, AR-FR22 Data Security Kit Operation Manual, AR-FR22 Data Security Kit Notice,
AGD_USR.1	利用者ガイダンス	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共通編/コピー編, 取扱説明書デジタル複合機プリンタ編, 取扱説明書デジタル複合機ネットワークスキャナ編, デジタル複合機取扱説明書ファクス編
ALC_DVS.1	セキュリティ手段の識別	データセキュリティキットAR-FR22 開発セキュリティ仕様書, データセキュリティキット開発セキュリティ
ATE_COV.2	カバレッジの分析	データセキュリティキットAR-FR22 カバレッジ分析書
ATE_DPT.1	テスト: 上位レベル設計	データセキュリティキットAR-FR22 上位レベル設計テスト分析書
ATE_FUN.1	機能テスト	データセキュリティキットAR-FR22 機能テスト仕様書, データセキュリティキットAR-FR22 独立テスト環境・ツール説明 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	取扱説明書データセキュリティキット AR-FR22, 注意書データセキュリティキット AR-FR22, AR-FR22 Data Security Kit Operation Manual, AR-FR22 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共通編/コピー編, 取扱説明書デジタル複合機プリンタ編, 取扱説明書デジタル複合機ネットワークスキャナ編, デジタル複合機取扱説明書ファクス編
AVA_SOF.1	機能強度	データセキュリティキットAR-FR22 セキュリティ機能強度分析書
AVA_VLA.1	開発者脆弱性分析	データセキュリティキットAR-FR22 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のメカニズムに基づくセキュリティ機能は、FIA\_UAU.2、FIA\_UAU.7、FIA\_AFL.1 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

*[DSK\_ST]*

(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。

[DSK\_ST]

## 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 14に検証する。表 14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 14: 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。

揮発性メモリに保存している暗号鍵と、本 TOE の保護資産のうち揮発性メモリ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。

このため揮発性メモリ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、揮発性メモリ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 15に示す。表 15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 15: 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_AFL.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\_AFL.1、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の問合せと変更(改変)が、FMT\_MTD.1 により可能となる。
  - e) 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。
  - f) キーオペレーターは、FMT\_MOF.1、及び FMT\_MTD.1 により、TOE の管理の役割を任せられ、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。
  - g) 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。
  - h) 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。
- a)から g)については独立事象であるので、各事象が相互に競合することはない。a)、c)、d)、e)、g)については単一の機能要件により実施しているので、機能要件が競合する可能性はない。b)は 4 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。f)は 3 つの機能要件が管理者によるセキュリティ機能と TSF データの管理のために独立して作用するので、競合は発生しない。h)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.RESIDUAL 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.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。

FCS\_CKM.1 と FMT\_MSA.2 は、FCS\_COP.1 の依存性の要件で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。

## 8.2.2 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 16に示す。表 16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 16: セキュリティ機能要件の依存性

機能要件	満たすべき依存性	満たしている依存性	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_AFL.1	FIA_UAU.1	FIA_UAU.2 <sup>(*)</sup>	
FIA_UAU.2	FIA_UID.1	FIA_UID.2 <sup>(*)</sup>	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 <sup>(*)</sup>	
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 <sup>(*)</sup>	
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 によって満たされる。

### 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 17に示す。

表 17: 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_AFL.1	FPT_RVM.1	なし
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 17に関し、以下に、各機能要件に対する迂回について述べる。

- 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。
- 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。
- 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。
- キーオペレーターの識別認証に関する FIA\_AFL.1、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。
- 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。
- 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。
- 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 17に関し、FDP\_RIP.1 は、FMT\_MOF.1 によりキーオペレーターのみにより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より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。

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ため、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。

### 8.2.5 最小機能強度根拠

データセキュリティキット AR-FR22 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-FR22 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、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 12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-J 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-J 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、スキャン送信ジョブで利用）、Flashメモリ（PCFAX ジョブ、ファクス送信、ファクス受信ジョブで利用）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 による揮発性メモリ及び 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\_AFL.1

FIA\_AFL.1 は、TSF\_AUT によるセキュリティ管理機能(キーオペレータープログラム)へのアクセス、及び 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機能の中断のためにキーオペレーター認証時において、認証失敗時の取扱いをするため、満足される。

#### 8.3.1.5 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。

#### 8.3.1.6 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。

#### 8.3.1.7 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。

#### 8.3.1.8 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。

#### 8.3.1.9 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。

#### 8.3.1.10 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。

#### 8.3.1.11 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。

#### 8.3.1.12 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、役割への関連づけを行っているため、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。

#### 8.3.1.13 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。認証失敗回数は固定であるため管理の必要がなく、また再認証受付までの停止時間も固定であり、通常状態へは自動的に復帰するため管理する必要はなく、FIA\_AFL.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はなく、FIA\_UID.2 の管理項目はない。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。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。

#### 8.3.1.14 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 Flash 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、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\_AFL.1、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： データセキュリティキットAR-FR22構成管理説明書、  
データセキュリティキット AR-FR22 VERSION S.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： データセキュリティキット AR-FR22 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-FR22 設置手順書  
AR-FR22 設置手順書(英独仏西語版)  
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: データセキュリティキット AR-FR22 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: データセキュリティキット AR-FR22 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: データセキュリティキット AR-FR22 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: データセキュリティキット AR-FR22 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: 取扱説明書データセキュリティキット AR-FR22,  
注意書データセキュリティキット AR-FR22  
AR-FR22 Data Security Kit Operation Manual,  
AR-FR22 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共通編/コピー編,  
取扱説明書デジタル複合機プリンタ編,  
取扱説明書デジタル複合機ネットワークスキャナ編,  
デジタル複合機取扱説明書ファクス編  
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: 取扱説明書データセキュリティキット AR-FR22,  
注意書データセキュリティキット AR-FR22  
AR-FR22 Data Security Kit Operation Manual,  
AR-FR22 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共通編/コピー編,  
取扱説明書デジタル複合機プリンタ編,  
取扱説明書デジタル複合機ネットワークスキャナ編,  
デジタル複合機取扱説明書ファクス編  
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: データセキュリティキット AR-FR22 開発セキュリティ仕様書,  
データセキュリティキット開発セキュリティ  
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: データセキュリティキット AR-FR22 カバレッジ分析書  
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: データセキュリティキット AR-FR22 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: データセキュリティキット AR-FR22 機能テスト仕様書,  
データセキュリティキット AR-FR22 独立テスト環境・ツール説明書  
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: 取扱説明書データセキュリティキット AR-FR22,  
注意書データセキュリティキット AR-FR22  
AR-FR22 Data Security Kit Operation Manual,  
AR-FR22 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共通編/コピー編,  
取扱説明書デジタル複合機プリンタ編,  
取扱説明書デジタル複合機ネットワークスキャナ編,  
デジタル複合機取扱説明書ファクス編  
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: データセキュリティキット AR-FR22 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: データセキュリティキット AR-FR22 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を利用するセキュリティ機能は、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。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。