デジタル複合機

データセキュリティキット

AR-FR10

セキュリティターゲット

Version 0.21

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 7 月 25 日	0.01	・ 初版作成	岩崎	谷口
2003 年 8 月 29 日	0.02	・ 全般に渡る指摘内容反映	岩崎	谷口
2003 年 9 月 5 日	0.03	・ 全般に渡る指摘内容反映	岩崎	谷口
2003 年 9 月 16 日	0.04	・ セキュリティ要件変更 ・ 表現、誤植修正	岩崎	谷口
2003 年 10 月 10 日	0.05	・ ASE001-01、ASE002-01、ASE003-01、ASE004-01、ASE005-01、ASE006-01 対応 ・ 指摘内容反映	岩崎	谷口
2003 年 10 月 24 日	0.06	・ ASE007-01、ASE008-01、ASE009-01、ASE010-01、ASE011-01、ASE012-01 対応	岩崎	谷口
2003 年 11 月 20 日	0.07	・ ASE013-01、ASE014-01、ASE015-01 対応 ・ ASE016-01、ASE017-01、ASE018-01 対応	岩崎	黒川
2003 年 12 月 3 日	0.08	・ TOE 識別変更 ・ 指摘内容反映 ・ 作成者、承認者欄を追加	岩崎	黒川
2003 年 12 月 5 日	0.09	・ 指摘内容反映	岩崎	黒川
2003 年 12 月 19 日	0.10	・ ASE019-01、ASE020-01、ASE021-01、ASE022-01 対応	岩崎	黒川
2003 年 12 月 19 日	0.11	・ 誤植修正	岩崎	黒川
2003 年 12 月 24 日	0.12	・ 指摘内容反映	岩崎	黒川
2003 年 12 月 26 日	0.13	・ 指摘内容反映	岩崎	黒川
2004 年 1 月 30 日	0.14	・ ASE023-01、ASE024-01、ASE025-01、ASE026-01、ASE027-01、ASE028-01、ASE029-01 対応	岩崎	黒川
2004 年 2 月 3 日	0.15	・ 指摘内容反映	岩崎	黒川
2004 年 2 月 3 日	0.16	・ 指摘内容反映	岩崎	黒川
2004 年 2 月 10 日	0.17	・ ASE030-01、ASE031-01、ASE032-01、ASE033-01 対応	岩崎	黒川
2004 年 2 月 12 日	0.18	・ 指摘内容反映	岩崎	黒川
2004 年 2 月 19 日	0.19	・ ASE034-01 対応	岩崎	黒川
2004 年 2 月 19 日	0.20	・ 誤植修正	岩崎	黒川
2004 年 2 月 21 日	0.21	・ 指摘内容反映	岩崎	黒川

【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:	デジタル複合機データセキュリティキット AR-FR10 セキュリティターゲット
バージョン:	0.21
作成日:	2004 年 2 月 20 日
製作者:	シャープ株式会社
TOE 識別:	AR-FR10 データセキュリティキット VERSION S.10
CC 識別:	CC バージョン 2.1, ISO/IEC 15408:1999, JIS X 5070:2000
評価機関:	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, オブジェクト再利用, 残存情報保護、暗号化、データ暗号化、データ消去

1.2 ST 概要

本 ST は、シャープのデジタル複合機データセキュリティキット AR-FR10 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、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、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。このキットはセキュリティを要求されているオフィス環境でのコピー、ファクスのジョブの処理途上、MFD にスプール保存されているイメージデータから、不正なアクセス者に情報が開示される危険を大幅に減ずる機能を有する。即ち、MFD がジョブを受け付けた後、イメージデータを暗号化してスプール保存し、ジョブ処理完了後は物理的にスプール保存された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、イメージデータの不正な再生を阻む機能を有する。

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）

略称	文書名
[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-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) 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。

b) 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。セキュリティ要件の詳細化操作は**太字**で示される。

c) 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 [*下線付きイタリック体*] で示される。

d) 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。

e) *単純イタリック体* はテキストを強調するために使用される。

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、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。ファクス受信においては、電話回線を通じて受信したデータ、及びこのデータを伸張したデータ。また、これらを圧縮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、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ファームウェア　アップグレード　キットAR-FR10。
メモリ	記憶装置、特に半導体素子による記憶装置。

用語	定義
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	イメージデータファイル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が搭載している全てのMSDについて、スプール保存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。

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)。
HD	ハードディスク(Hard Disk)。
HDD	ハードディスクドライブ(Hard Disk Drive)。
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、HDDあるいは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)。
RTC	リアルタイムクロック、時計回路 (Real-time Clock) 。

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、主としてデータ消去機能と暗号操作機能からなる。

データ消去機能は、コピーのジョブ完了後、HDD 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。ファクス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実イメージデータ領域に対し固定値を上書きする。

暗号操作機能は、実イメージデータを MSD 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、MSD 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。

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

MFD の物理的構成を図 1に示す。

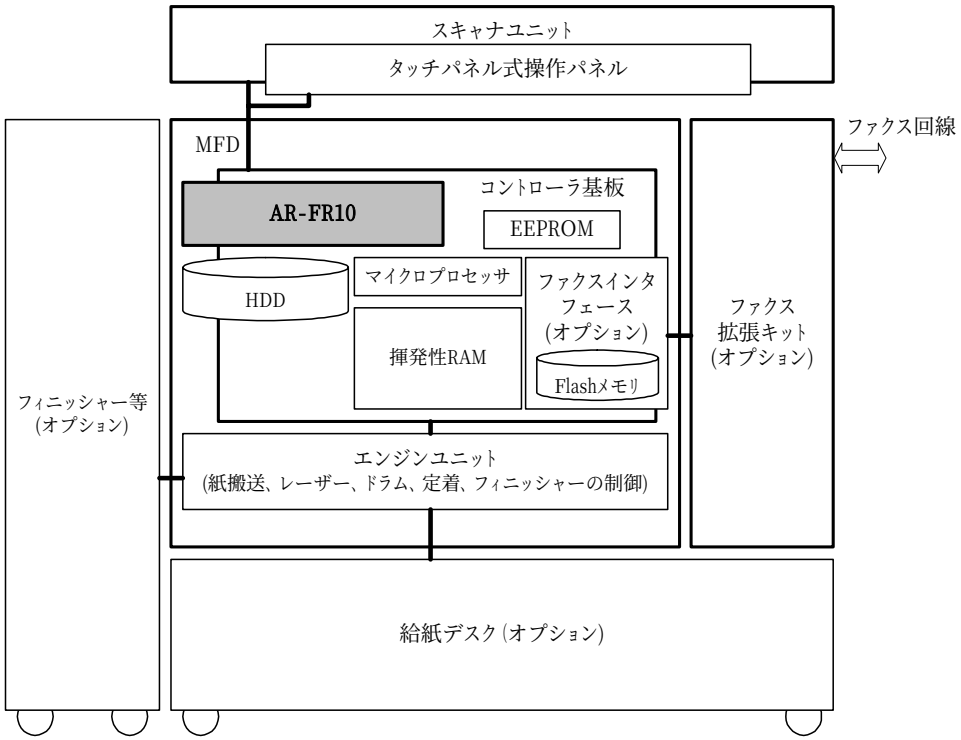

図 1: MFD の物理的構成と TOE

図において、MFD に搭載した TOE である AR-FR10 の設置位置を網掛けで示す。TOE は、MFD のコントローラ基板上で動作し、セキュリティ機能を追加するファームウェアであり、物理的に2枚の ROM 基板と

して構成される。各 ROM 基板は、ROM チップ等を実装した約 25mm×60mm のプリント基板であり、一辺にエッジコネクタを有し、エッジコネクタを介して MFD 内のコントローラ基板に装着する。
また、TOE が動作する MFD は、シャープ デジタル複合機 AR-555S、AR-625S、及び AR-705S 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 を網掛けで示し、長方形はソフト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。
Flash メモリは、ファクスインタフェース基板上に搭載されていることを示したものである。

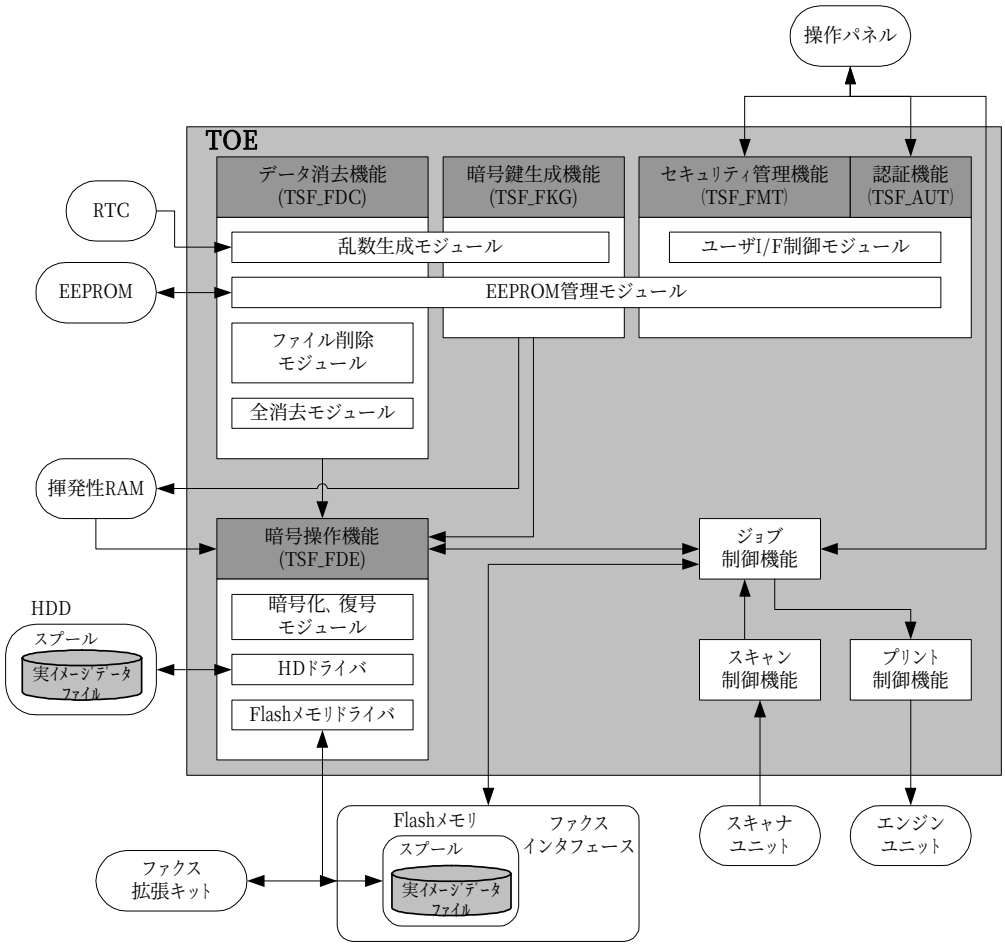

図 2: TOE の論理的構成図

TOE は、MFD にセキュリティ機能を追加するファームウェア 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 のコントローラ基板の制御を行う。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)
スプール保存する実イメージデータを暗号化し、MSD（HDD もしくは Flash メモリ）に保存する。また、MSD にスプール保存されている実イメージデータを復号する。

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

c) データ消去機能(TSF_FDC)
コピージョブにより HDD 内に、もしくはファクス送受信ジョブにより Flash メモリ内にスプール保存された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、実イメージデータ領域を消去をする。（各ジョブ完了後の自動消去）
また、ジョブが正常に完了しなかった場合、消去されなかった実イメージデータ領域対して、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。以下の3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（HDD と Flash メモリ）
  （ジョブ完了後、ジョブが使用した実イメージデータ領域の消去）
- 電源 ON 時の自動消去（HDD のみ）
  （ジョブが正常に完了しなかった場合、消去されなかった実イメージデータ領域に対する消去）
- キーオペレーターの操作による全データエリア消去（HDD と Flash メモリ）
  （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）
  （注釈： MFD の所有者が変わる、もしくは MFD 廃棄等における実イメージデータからの情報漏洩を防止するための機能）

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)
以下の設定を提供する。
- 電源 ON 時の自動消去の実行、もしくは不実行設定
- 各ジョブ完了後のデータ消去回数の設定（HDD への上書き消去回数のみ）
- キーオペレーターの操作による全データエリア消去回数の設定（HDD への上書き消去回数のみ）
- 電源 ON 時の自動消去における消去回数の設定（HDD への上書き消去回数のみ）
- キーオペレーターコードの変更

f) スキャン制御機能
コピージョブ、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。スキャンされた実イメージデータは揮発性 RAM に格納される。

g) プリント制御機能
コピージョブ、ファクス受信ジョブにおいて、揮発性 RAM に格納されている実イメージデータを、エンジンユニットに転送し印字を行わせる。

h) ジョブ制御機能
ジョブには、コピージョブ、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。
- 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 MFD の機能から TOE 利用

MFD の持つコピー機能、ファクス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。MFD には、主電源スイッチと電源スイッチがあり、通常利用の間は、主電源スイッチ“入”、電源スイッチ“入”の状態で利用する。

a) コピー機能
MFD のコピー機能は、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、以下のシーケンスで実施される。
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 スキャン制御機能により、原稿をスキャンし、実イメージデータを揮発性 RAM に取得する。

③ 揮発性 RAM の実イメージデータを、暗号操作機能（TSF_FDE）により、暗号化して MSD（コピージョブの場合は HDD）にスプール保存する。

④ 暗号操作機能により、MSD にスプール保存されている暗号化された実イメージデータを読み出し、暗号操作機能（TSF_FDE）により復号して揮発性 RAM に格納する。

⑤ 揮発性 RAM に格納された実イメージデータをプリント制御機能を介して、エンジンユニットに転送することにより、実イメージデータを印字する。

原稿画像のスキャンによる実イメージデータの取得については、②及び③を必要回数繰り返し、印字を行うため④及び⑤を必要回数繰り返す。

⑥ 操作パネルにて設定された条件にて、セットされた原稿分のプリントが終了すると、データ消去機能（TSF_FDC）にて MSD 内にスプール保存されている実イメージデータ領域を上書き消去する。

b) 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、ファクス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、以下のシーケンスで実施される。

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 スキャン制御機能により、原稿をスキャンし、実イメージデータを揮発性 RAM に取得する。

③ 揮発性 RAM の実イメージデータを、暗号操作機能（TSF_FDE）により、暗号化して MSD（ファクス送信ジョブの場合は Flash メモリ）にスプール保存する。

④ 暗号操作機能により、MSD にスプール保存されている暗号化された実イメージデータを読み出し、暗号操作機能（TSF_FDE）により復号して揮発性 RAM に格納する。

⑤ 揮発性 RAM に格納された実イメージデータをファクスインタフェースに転送することにより、ファクス拡張キットよりファクス送信を行う。

原稿画像のスキャンによる実イメージデータの取得については、②及び③を必要回数繰り返し、ファクス送信を行うため④及び⑤を必要回数繰り返す。

⑥ 操作パネルにて設定された条件にて、セットされた原稿分のファクス送信が終了すると、データ消去機能（TSF_FDC）にて MSD 内にスプール保存されている実イメージデータ領域を上書き消去する。

c) ファクス受信機能

MFD のファクス受信機能は、ファクス回線よりファクスインタフェースを介して、ファクス受信通知があった場合、以下のシーケンスで実施される。

① ファクス回線より、ファクス拡張キットがファクス受信したことを検知する。ファクス拡張キットは、ファクスインタフェースを介してコントローラユニットにファクス受信通知を行い、ファクス受信ジョブを開始する。

② ファクスインタフェースより、実イメージデータ（ファクス受信データ）を揮発性 RAM に取得する。

③ 揮発性 RAM の実イメージデータを、暗号操作機能（TSF_FDE）により、暗号化して MSD（ファクス受信ジョブの場合は Flash メモリ）にスプール保存する。

④ 暗号操作機能により、MSD にスプール保存されている暗号化された実イメージデータを読み出し、暗号操作機能（TSF_FDE）により復号して揮発性 RAM に格納する。

⑤ 揮発性 RAM に格納された実イメージデータをプリント制御機能を介して、エンジンユニットに転送することにより、実イメージデータを印字する。

ファクス回線からの実イメージデータの取得については、②及び③を必要回数繰り返し、印字を行うため④及び⑤を必要回数繰り返す。

⑥ ファクスインタフェースを介し、ファクス拡張キットに対してコントローラユニットにファクス受信完了通知が行われ、ファクス受信した分のプリントが終了すると、データ消去機能（TSF_FDC）にて MSD 内にスプール保存されている実イメージデータ領域を上書き消去する。

ファクス受信には、夜間や休日などのように MFD 本体は使用しないが、ファクスの自動受信を行う機能を備えている。このファクスの自動受信は、MFD の主電源スイッチを“入”、電源スイッチを“切”状態で実施され、上記ファクス受信機能のうち①から③を実施した状態で停止しており、MFD の主電源スイッチを“入”、電源スイッチを“入”状態となった時に、ファクス受信機能の④以降が実施される。

2.3.2 TOE の運用

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。

- 電源 ON 時の自動消去の実行、もしくは不実行設定
- 各ジョブ完了後のデータ消去回数の設定
- キーオペレーターの操作による全データエリア消去回数の設定
- 電源 ON 時の自動消去における消去回数の設定
- キーオペレーターコードの変更
- 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、利用者が意図することなく、MFD 自身がコピー、もしくはファクス送受信処理のために MFD 内の HDD、もしくは Flash メモリに一時的にスプール保存された実イメージデータである。

3 TOE セキュリティ環境

本章は、TOE セキュリティ環境について述べる。

3.1 前提条件

TOE の使用、運用時に、表 4で詳述する環境が必要となる。

表 4: 想定環境

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: TOE に対する脅威

識別子	定義
T.RECOVER	攻撃者が、MFD内のMSDに、MFD以外の装置を使用することによりMSD内の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はない。

4 セキュリティ対策方針

本章は、セキュリティ対策方針における施策について述べる。

4.1 TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 6に示す。

表 6: TOE のセキュリティ対策方針

識別子	定義
O.RESIDUAL	スプール保存されているMSDの実イメージデータ領域に対して上書き消去する。
O.REMOVE	TOEが組込まれているMFDのMSDに対し、MSD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MSDにスプール保存する。
O.MANAGE	TOEのセキュアな運用を維持するための機能をキーオペレーターのみに提供する。

4.2 環境のセキュリティ対策方針

TOE 環境に対するセキュリティ対策方針を表 7に示す。

表 7: 環境のセキュリティ対策方針

識別子	定義
OE.OPERATE	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

5.1.1.1 クラス FCS: 暗号サポート

a) FCS_CKM.1(1) 暗号鍵生成(1)
下位階層: なし
FCS_CKM.1.1(1) TSF は、以下の［ SHARP 標準 ］に合致する、指定された暗号鍵生成アルゴリズム［ 循環付き遅延フィボナッチ乱数拡張アルゴリズム ］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

b) FCS_CKM.1(2) 暗号鍵生成(2)
下位階層: なし
FCS_CKM.1.1(2) TSF は、以下の［ SHARP 標準 ］に合致する、指定された暗号鍵生成アルゴリズム［ MSN 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

c) FCS_COP.1 暗号操作
下位階層: なし
FCS_COP.1.1 TSF は、[FIPS PUB 197]に合致する、特定された暗号アルゴリズム [Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[実イメージデータの暗号化、及び復号]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

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:[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.2　アクション前の利用者識別

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.2　アクション前の利用者認証

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(1)　セキュリティ機能のふるまいの管理(1)

下位階層:　なし

FMT_MOF.1.1(1)　TSF は、機能［　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_MOF.1(2)　セキュリティ機能のふるまいの管理(2)

下位階層:　なし

FMT_MOF.1.1(2)　TSF は、機能［　電源 ON 時の自動消去機能　］[　*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

c)　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

d) FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[電源 ON 時の実行もしくは不実行設定、キーオペレーターコード、キーオペレーターの操作による全データエリア消去における HDD 上の全ての実イメージデータファイルに対する上書きの回数、電源 ON 時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数、各ジョブ完了時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数]を[*デフォルト値変更、問合せ* [なし]] 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

e) 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.2 アクション前の利用者識別

f) 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 8に示す TOE の管理項目]。

依存性: なし。

表 8: TOE の管理項目

機能要件	管理項目
FCS_CKM.1(1)、FCS_CKM.1(2)	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	上書き消去タイミング
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(1)、FMT_MOF.1(2) 、	なし（TSF の機能（TSF データ）と相互に影響を及ぼす役

機能要件	管理項目
FMT_MTD.1	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 9に示す。表 9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 9: 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.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。
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は FIA_UAU.2 と、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

本 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 10に示す。表 10は、機能概要と仕様概要ついて、その対応を記載している節を示したものである。

表 10: 機能要件と仕様概要

機能要件	仕様概要				
	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT
FCS_CKM.1(1)	6.1.1節				
FCS_CKM.1(2)	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(1)			6.1.3節	6.1.4節	
FMT_MOF.1(2)			6.1.3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			6.1.3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 AES Rijndael アルゴリズムを実施するため2つの暗号鍵（共通鍵）が生成される。一つは、循環付き遅延フィボナッチ乱数拡張アルゴリズムを用いて、MFD 内の HDD にスプール保存、または読出される実イメージデータの暗号、及び復号用の暗号鍵（共通鍵）である。もう一つは、MSN 拡張アルゴリズムを用いて、MFD 内の Flash メモリにスプール保存、または読出される実イメージデータの暗号、及び復号用の暗号鍵（共通鍵）である。鍵は、いずれも 128 ビット長である。これらの暗号鍵は揮発性 RAM 内に保存する。

6.1.2 暗号操作(TSF_FDE)

通常の動作の間、ジョブ処理の途上において、MFD はジョブのデータである実イメージデータを MSD にスプール保存する。ファクス回線からの送受信における実イメージデータは Flash メモリ領域に、コピーの対象となる実イメージデータは HDD 領域にそれぞれ保存する。スプール保存するにあたり、揮発性 RAM 内に保存している暗号化鍵を用い AES Rijndael アルゴリズムによって暗号化の後、MSD にスプール保存する。また、スプール保存された実イメージデータを実際に処理（利用）する際には、ジョブ処理の過程で必要となるデータ断片（処理中ジョブ 1 件の実イメージデータの一部）を必要の都度、MSD から読み出し、復号することにより得る。

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を消去するデータ消去機能を有する。本機能は、以下の3プログラムで構成される。

a) 各ジョブ完了後の自動消去
コピージョブ完了後、コピージョブが利用した実イメージデータファイルが存在していた HDD 上の領域に、ランダム値をセキュリティ管理機能 (TSF_FMT) により設定されている回数繰り返して上書き消去し、ファクスの送受信ジョブ完了後、ファクスの送受信ジョブが利用した実イメージデータファイルが存在していた Flash メモリ上の領域に、Flash メモリの各ビットに固定値(0)を上書き消去する機能。

b) 電源 ON 時の自動消去
電源 ON 時の自動消去が実行状態に設定されている場合において、MFD の電源が ON になった際、ジョブが正常に完了せず消去されなかった HDD 上の実イメージデータファイルに、ランダム値をセキュリティ管理機能 (TSF_FMT) により設定されている回数繰り返して上書き消去する機能。

c) 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識別認証後、キーオペレーターの操作により、スプール保存のために利用される HDD 上の全ての実イメージデータファイルに、ランダム値をセキュリティ管理機能 (TSF_FMT) により設定されている回数繰り返して上書き消去する。また、スプール保存のために利用される Flash メモリ上の実イメージデータファイルについて、Flash メモリの全ビットをデバイスのブロック消去機能により固定値(1)で埋める機能。単に、全データエリア消去とも呼ぶ。

電源 ON 時の自動消去、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を中断させる場合、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。

なお、HDD 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、キーオペレーターに対し、キーオペレータープログラムの選択による識別後、アクセスのために5桁の暗証番号、即ち、キーオペレーターコードの入力を要求する。キーオペレーターコードを正しく入力する手順によって、キーオペレーターとして認証される。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。

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、及びセキュリティ管理(TSF_FMT)は、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)

このセキュリティ管理(TSF_FMT)は、キーオペレータープログラム選択とキーオペレーターコードの入力により、キーオペレーターが識別認証される手順を経た後に、以下のセキュリティ機能の設定を提供する。

a) 電源 ON 時の自動消去実行、もしくは不実行の設定
設置時のデフォルトでは、電源 ON 時の自動消去は実行と設定されている。
デフォルト値の問合せ、及び変更ができる。

b) 各ジョブ完了時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数
消去回数は、1回から7回までの間で設定でき、デフォルト値の問合せ及び変更ができる。

c) キーオペレーターの操作による全データエリア消去における HDD 上の全ての実イメージデータファイルに対する上書きの回数
消去回数は、1回から7回までの間で設定でき、デフォルト値の問合せ、及び変更ができる。

d) 電源 ON 時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数
消去回数は、1回から7回までの間で設定でき、デフォルト値の問合せ、及び変更ができる。

e) 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は十進数字 5 桁であり、TOE は桁数が 5 桁であることを検査する。
キーオペレーターコードのデフォルト値の問合せ、及び変更ができる。

各設定値を変更すると、MFD 内の EEPROM 内にデフォルト値として保存される。

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 11に示す。

表 11: 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-FR10 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-FR10 version S.10 構成リスト
ACM_SCP.1	TOEのCM範囲	デジタル複合機データセキュリティキットAR-FR10 構成管理範囲説明書
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-FR10 配付手順説明書
ADO_IGS.1	設置、生成、及び立上げ手順	デジタル複合機データセキュリティキットAR-FR10 配付手順説明書, AR-FR10設置手順書
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-FR10 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-FR10 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-FR10 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-FR10 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-FR10, 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 ファクス編
AGD_USR.1	利用者ガイダンス	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 ファクス編
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-FR10 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-FR10 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-FR10 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-FR10 機能テスト仕様書
ATE_IND.2	独立テスト - サンプル	デジタル複合機データセキュリティキットAR-FR10 独立テスト環境･ツール説明書

コンポーネント	コンポーネント名	保証手段
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-FR10, 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　ファクス編
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-FR10 セキュリティ機能強度分析書
AVA_VLA.1	開発者脆弱性分析	デジタル複合機データセキュリティキットAR-FR10 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 に対応する認証（TSF_AUT）、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 12に検証する。表 12は、脅威、前提条件とセキュリティ対策方針の対応について、その根拠を記載している節を示したものである。

表 12: 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
	T.RECOVER	A.OPERATOR
O.RESIDUAL	8.1.1節	
O.REMOVE	8.1.1節	
O.MANAGE	8.1.1節	
OE.OPERATE		8.1.2節

8.1.1 T.RECOVER

T.RECOVER に対して、スプール保存されている MSD の実イメージデータを読み出せないように、O.RESIDUAL にて上書き消去を実施することにより対抗する。また、O.MANAGE により、TOE のセキュアな運用のため、キーオペレーターのみが TOE 管理機能を利用することで対抗する。

何らかのトラブルにより上書き消去が実施できなかった場合、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。これにより MSD 内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、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。

8.2 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 13に示す。表 13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 13: 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	O.MANAGE
FCS_CKM.1(1)		8.2.1.2節	
FCS_CKM.1(2)		8.2.1.2節	
FCS_COP.1		8.2.1.2節	
FDP_RIP.1	8.2.1.1節		
FIA_UAU.2			8.2.1.3節

機能要件	セキュリティ対策方針		
	O.RESIDUAL	O.REMOVE	O.MANAGE
FIA_UAU.7			8.2.1.3節
FIA_UID.2			8.2.1.3節
FIA_SOS.1			8.2.1.3節
FMT_MOF.1(1)			8.2.1.3節
FMT_MOF.1(2)			8.2.1.3節
FMT_MSA.2		8.2.1.2節	
FMT_MTD.1			8.2.1.3節
FMT_SMR.1			8.2.1.3節
FMT_SMF.1	8.2.1.1節		8.2.1.3節
FPT_RVM.1	8.2.3節を参照		

8.2.1.1 O.RESIDUAL

O.RESIDUAL は、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実行であり、ジョブ完了後、電源 ON 時、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発動され、FDP_RIP.1 により利用者データ保護が実施される。また、FMT_SMF.1 により、FDP_RIP.1 の上書き消去タイミングを管理する。

8.2.1.2 O.REMOVE

O.REMOVE は、MFD 内の MSD に対し、MSD 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、何らかのトラブルにより MFD の MSD 内にスプール保存された実イメージデータが FDP_RIP.1 により上書き消去されなかった場合においても、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、MSD 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(1)と、FCS_CKM.1(2)により暗号鍵を生成する。暗号鍵は、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。

8.2.1.3 O.MANAGE

O.MANAGE は、以下の機能要件の組み合わせにより実現できる。

a) FIA_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。

b) キーオペレーターにのみ下記機能を実行可能とする。
   ・FMT_MTD.1 にて、電源 ON 時の自動消去の実行もしくは不実行設定、キーオペレーターコードの変更、キーオペレーターの操作による全データエリア消去における HDD 上の実イメージデータファイルに対する上書きの回数、電源 ON 時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数、各ジョブ完了時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数のセキュリティ設定が可能となる。
   ・全データエリア消去機能の起動と停止が、FMT_MOF.1(1)により可能となる。
   ・電源 ON 時の自動消去機能の停止が、FMT_MOF.1(2)により可能となる。

c) FMT_MTD.1 においてキーオペレーターコードを変更する場合、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、確実なキーオペレーターコードが設定される。

d) キーオペレーターは、FMT_MOF.1(1)、FMT_MOF.1(2)、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、常に正当なキーオペレーターが管理機能を実行できる。

e) FMT_SMF.1 により、FDP_RIP.1 の上書き消去タイミングを管理することにより、確実に上書き消去が実行することが可能であり、また 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、常に正当なキーオペレーターを識別認証することが可能となる。

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 14に示す。表 14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 14: 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(1)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	8.2.2.1節
FCS_CKM.1(2)	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	FCS_CKM.1	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(1)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	
FMT_MOF.1(2)	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	

(*) FIA_UAU.1 及び FIA_UID.1 への依存性は、上位階層の FIA_UAU.2 及び FIA_UID.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

暗号鍵を保存しているのは、揮発性 RAM 内であり、TOE もしくは MFD の電源断により、揮発性 RAM に格納された暗号鍵は、消失する。電荷を蓄える回路を記憶素子として利用している揮発性 RAM は、情報の記憶を電荷によって行っており、揮発性 RAM 内に保存された暗号鍵は、TOE もしくは MFD の電源断によって、蓄えられていた電荷が無くなることで暗号鍵を読み出すことができなくなる。このため、TOE の機能として暗号鍵を破壊する必要はなく、FCS_CKM.4 は必要がない。

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 15に示す。

表 15: 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(1)	FPT_RVM.1	なし
FCS_CKM.1(2)	FPT_RVM.1	なし
FCS_COP.1	FPT_RVM.1	なし
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1(1), FMT_MOF.1(2)
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(1)	FPT_RVM.1	なし
FMT_MOF.1(2)	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 15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(1)、FCS_CKM.1(2)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) 利用者のデータ保護 FDP_RIP.1 は、ジョブ完了時、電源 ON 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(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) セキュリティ機能のふるまい管理 FMT_MOF.1(2)は、電源 ON 時の自動消去の中断の場合、キャンセル操作後、必ずキーオペレーター認証が必ず呼び出されるため迂回できない。

h) 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 15に関し、FDP_RIP.1 は、FMT_MOF.1(1)、及び FMT_MOF.1(2)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 には、アクセス制御がなく、不正なサブジェクトが存在しない。このため 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、攻撃者が、MFD 内の MSD にアクセスし、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が、これには上書き消去と暗号化という簡単なメカニズムで対抗することができる。このため本 TOE は、商用として十分である EAL3+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

デジタル複合機データセキュリティキット AR-FR10 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。攻撃者は認証を迂回して、AR-FR10 のセキュリティ設定を利用することはできず、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ため、AR-FR10 の最小機能強度レベルは“SOF 基本”である。

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

IT セキュリティ要件に対する、TOE セキュリティ仕様概要の有効性を表 16に示す。表 16は、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、その根拠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と TOE セキュリティ仕様

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(1)	8.3.1.1節				
FCS_CKM.1(2)	8.3.1.2節				
FCS_COP.1		8.3.1.3節			
FDP_RIP.1			8.3.1.4節		
FIA_UAU.2			8.3.1.5節	8.3.1.5節	
FIA_UAU.7			8.3.1.6節	8.3.1.6節	
FIA_UID.2			8.3.1.7節	8.3.1.7節	
FIA_SOS.1					8.3.1.8節
FMT_MOF.1(1)			8.3.1.9節	8.3.1.9節	
FMT_MOF.1(2)			8.3.1.10節		

機能要件	TOE セキュリティ仕様				
	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT
FMT_MSA.2	8.3.1.11節				
FMT_MTD.1				8.3.1.12節	8.3.1.12節
FMT_SMR.1				8.3.1.13節	8.3.1.13節
FMT_SMF.1			8.3.1.14節	8.3.1.14節	8.3.1.14節
FDP_RVM.1	8.2.3節を参照				

8.3.1.1 FCS_CKM.1(1)

FCS_CKM.1(1)は、MFD の電源投入時に TSF_FKG の循環付き遅延フィボナッチ乱数拡張アルゴリズムにより 128 ビットの暗号鍵（共通鍵）を生成するため、満足される。

8.3.1.2 FCS_CKM.1(2)

FCS_CKM.1(2)は、MFD の電源投入時に TSF_FKG の MSN 拡張アルゴリズムにより 128 ビットの暗号鍵（共通鍵）を生成するため、満足される。

8.3.1.3 FCS_COP.1

FCS_COP.1 は、TSF_FDE による FIPS PUB 197 で規格化された 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。

8.3.1.4 FDP_RIP.1

FDP_RIP.1 は、各ジョブ完了後の自動消去と、電源 ON 時の自動消去について、TSF_FDC による MSD（コピージョブ完了後の自動消去及び電源 ON 時の自動消去は HDD、ファクス送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実イメージデータファイルの再利用を不能とするため、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 MSD（HDD 及び Flash メモリ）に保存された全ての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実イメージデータファイルの再利用を不能とするため、満足される。

8.3.1.5 FIA_UAU.2

FIA_UAU.2 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）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が必要であるため、満足される。また、TSF_FDC により、電源 ON 時の自動消去、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、電源 ON 時の自動消去、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は、キーオペレーターコードの桁数が5桁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(1)

FMT_MOF.1 (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_MOF.1(2)

FMT_MOF.1 (2)は、TSF_FDC によるキーオペレーターの識別認証により、電源 ON 時の自動消去の中断を可能とするため、満足される。

8.3.1.11 FMT_MSA.2

FMT_MSA.2 は、TSF_FKG の処理の中で、ADV_SPM.1 によりセキュアな論理により、暗号鍵が循環付き遅延フィボナッチ乱数拡張アルゴリズム、及び MSN 拡張アルゴリズムにより生成されるため、満足される。

8.3.1.12 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 により電源 ON 時の自動消去実行もしくは不実行設定の問合せ及びデフォルト値の変更、キーオペレーターコードの問合せと設定、キーオペレーターの操作による全データエリア消去における HDD 上の実イメージデータファイルに対する上書きの回数の問合せと設定、電源ON時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数の問合せと設定、及び各ジョブ完了時の自動消去における HDD 上の実イメージデータファイルに対する上書きの回数の問合せと設定できるため、満足される。

8.3.1.13 FMT_SMR.1

FMT_SMR.1 は、TOE の管理者であるキーオペレーターのみがキーオペレーターコードを知り得ていて、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、及び役割を維持し続けるため、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。

8.3.1.14 FMT_SMF.1

FMT_SMF.1 は、FDP_RIP.1 の管理項目である TSF_FDC による上書き消去タイミング、FIA_UAU.2 の管理項目である TSF_AUT 及び 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(1)、FCS_CKM.1(2)、FMT_MSA.2 についての管理項目は要請されていない。秘密の検証尺度についても、固定値（5文字の数字）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(1)、FMT_MOF.1 (2)、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。

8.3.1.15 FPT_RVM.1

a) FCS_CKM.1(1)、及び FCS_CKM.1(2)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 MSD 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、MSD 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、各ジョブが完了後した場合、電源 ON 時の自動消去が実行状態に設定されている場合における MFD の電源が ON の場合、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時に、必ず TSF_FMT にてキーオペレーターコードが十進数字 5 桁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(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 にて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_MOF.1(2)は、電源 ON 時の自動消去の中断を行う場合、必ず TSF_FDC にてキーオペレーターの識別認証後に、電源 ON 時の自動消去の中断が実施されるため、満足される。

i) FMT_MTD.1 は、以下の項目が必ず TSF_FMT にて実行されることにより、満足される。
- 電源 ON 時の自動消去実行もしくは不実行設定
- 各ジョブ完了後の HDD 上の実イメージデータファイルに対する消去回数の設定
- キーオペレーターの操作による全データエリア消去の HDD 上の実イメージデータファイルに対する消去回数の設定
- 電源 ON 時の自動消去における HDD 上の実イメージデータファイルに対する消去回数の設定
- キーオペレーターコードの変更

8.3.2 TOE 保証手段根拠

6.2節の保証手段の有効性を検証する。表 11に示すように、全ての TOE セキュリティ保証要件は、保証手段により示されたドキュメントにより対応付けられており、また保証手段に示されたドキュメントによって、本書が規定した TOE セキュリティ保証要件 EAL3+ADV_SPM.1 が要求している証拠に合致している。

8.3.3 TOE セキュリティ機能強度根拠

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) およびキーオペレーターコード変更 (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。