デジタル複合機
データセキュリティキット
AR-FR4/AR-FR5

セキュリティターゲット

Version 0.04

2004年7月30日

シャープ株式会社

【履歴】

日付	バージョン	変更点
2004年 3月4日	0.01	・初版作成
2004年 5月18日	0.02	・指摘内容修正
2004年 5月20日	0.03	・指摘内容修正
2004年 7月30日	0.04	・指摘内容修正

目次

表のリスト

図のリスト

1 ST 概説

1.1 ST 識別

本節では本 ST と TOE を識別するための情報を記載している。

ST 名称:	デジタル複合機データセキュリティキット AR-FR4/AR-FR5 セキュリティターゲット
バージョン:	0.04
作成日:	2004 年 7 月 30 日
製作者:	シャープ株式会社
TOE 識別:	日本: データセキュリティキット AR-FR4 version M.20
	海外: Data Security Kit AR-FR4 version M.20, Data Security Kit AR-FR5 version E.20
	(言語、製品名称の違いにより TOE 識別は異なるが、同一物である。)
CC 識別:	CC バージョン 2.1, ISO/IEC 15408:1999, JIS X 5070:2000
保証パッケージ:	EAL4
評価機関:	株式会社富士総合研究所 情報セキュリティ評価センター
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-FR4、及び AR-FR5 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) はプリント機能ユニットに、コピー、イメージスキャニング、ファクス機能ユニットを顧客のニーズに合わせて選択構成し、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プリント、コピー、イメージスキャニング、ファクスのジョブの処理途上、及び完了後、MFD に保存されている残存データ 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は一旦暗号化したデータとしてスプールし、その処理完了後はスプールデータ にランダムデータ、または、固定値を上書きして、ドキュメントデータやイメージデータの不正な再生を阻む機能を有する。機能については、第2章、第6章で詳述する。

TOE の使用環境、即ち、TOE を設置するオフィスは、オフィスの定める手続きを経るように入室管理され、またそのオフィスには一般的に信頼できる従業員がいることが必要となる。

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) EAL4 適合

d) 本 ST が参照する PP はない。

1.4 参考資料

本 ST 作成について、下記の資料を参照している。

[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

[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

[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

[HOSOKU-0210] 補足-0210

1.5 規約、専門用語、略語

本節では、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

本節では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)の運用を示すためと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定めている。

本 ST で使用される表記、フォーマット、規約はコモンクライテリア(CC)で使用されるものと概ね一致している。

本ＳＴで選択した表記について説明する。

コモンクライテリア(CC)はいくつかの操作がセキュリティ機能要件コンポーネントに対して行われることを許容している。;割付、詳細化、選択、繰り返し（[CC_PART2] の 2.1.4 に記載）

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 ST に固有の用語を表 1に示す。

表 1: 専門用語

用語	定義
許可されていない利用者	善意もしくは悪意を持ってTOEセキュリティ機能 (TSF) と対話をする任意のエンティティ
残存データ	コピー、プリント、イメージスキャニング、ファクスジョブが完了、キャンセル、中断された時に大容量ストレージ機器 (MSD) に残存しているデータ
キーオペレーター	シャープのデジタル複合機用のデータセキュリティキットを管理する認証された利用者
キーオペレーター文書指示	MFDの取扱説明書、DSKの取扱説明書、及びDSKの設置チェックリストに記載されている、キーオペレーターが遵守すべき注意事項の総称
スプールデータ	MFDがコピー、プリント、イメージスキャニング、またはファクスの各ジョブで扱うドキュメントデータやイメージデータを、ジョブ単位でMFD内のMSDにスプールしたもの
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データセキュリティキット(DSK)AR-FR4、AR-FR5
メモリ	記憶装置、特に半導体素子による記憶装置

1.5.3 略語

本 ST で使用する略語を表 2に示す。

表 2: 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)
HDD	ハードディスクドライブ(Hard Disk Drive)
MSD	Mass Storage Device
OS	オペレーティングシステム (Operating System)
PIN	暗証番号(Personal Identification Number)
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)。特に、製造時に内容が決定し、製造後の消去または書き換えができないマスクROM (Masked ROM) を指す。

2 TOE 記述

本章では TOE の種類を明確にするとともに、評価される設定を詳述することで TOE 評価の内容を説明する。

2.1 TOE 概要

TOE は製品として提供される。本節では、TOE について、及びその提供形態としての製品について、それらがどのようなカテゴリーに属するものであるのかを記述する。

2.1.1 TOE 種別

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

TOE は MFD のファームウェア[1]の一部である。より正確には、対象 MFD のファームウェアに対して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 キットである。

TOE の一部は、もともとのファームウェアの一部を置き換えるコードであり、他の部分は、もともとのファームウェアに対する追加のコードであり置き換え部分から呼び出される。

TOE は、セキュリティニーズの高いオフィスに設置され、そのオフィスで働く従業員によって利用される。

2.1.2 製品の形態

製品、すなわち DSK の提供形態は、工場もしくは現場でインストール可能なセキュリティ強化ファームウェアアップグレードキットであり、対象 MFD の ROM の一部を差し替える交換用 ROM 製品という形態をとる。

アップグレード対象となる MFD 製品リストを表 3 に記載する。これらの対象 MFD はオフィスの所要ニーズにあわせてプリンタを基本としてコピー、イメージスキャナー、ファクスの機能ユニットで構成されている。これらの MFD にもともと装着されている交換対象 ROM の形態は、MFD の形態によってやや異なる2種類のバリエーションを持っている。

表 3: DSK と対象 MFD モデル

DSKモデル バージョン	名称	対象MFDモデル
AR-FR4 version M.20	MFD用データセキュリティキット	海外向MFD-model AR-M350, AR-M450, AR-M280N, AR-M350N, AR-M450N, AR-M280U, AR-M350U, AR-M450U, AR-M300U, AR-M300N, DM-3551, DM-4551 国内向MFD-model AR-310M, AR-350M, AR-450M, AR-310S, AR-350S, AR-450S, AR-310F, AR-350F, AR-450F, DM-3551, DM-4551
AR-FR5 version E.20	[2]プリンタ用データセキュリティキット	海外向model AR-P350, AR-P450, DM-3500, DM-3501, DM-4500, DM-4501

[1] ハードウェア組み込みのソフトウェアは一般に、ファームウェア (firmware) と呼ばれる。TOE は MFD のファームウェアである。すなわち、MFD に内蔵され MFD ハードウェアを制御するためのソフトウェアである。

2 MFD がプリント機能に限って設定されると、通常プリンタと呼ばれる。

2.1.3 製品形態のバリエーション

DSK の製品形態には、MFD の形態により AR-FR4、AR-FR5 の 2 種類がある。これらは、いずれも同一の DSK を内蔵し、交換対象 ROM の各形態に適合する 2 種類の交換用 ROM 形態をとる。

MFD がプリンタとしてのみ設定される場合、海外向け販売には AR-FR5 がインストールされる。プリンタ機能に加え、コピー等の機能も有する MFD（スキャナユニットを装着し、ファクス拡張キットも装着可）には、AR-FR4 がインストールされる。

MFD は機能ユニット構成により決定される、HDD、RAM（RAM ディスク）、及び Flash メモリからなる MSD を有する。この MSD には、MFD で実行されるジョブのドキュメントデータやイメージデータが保存される。DSK はアップグレード対象となる MFD 内部の MSD に一時的に保存されるドキュメントデータやイメージデータのセキュリティを確保する。

2.1.4 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データ暗号化機能からなる。

データ消去機能は、プリント、イメージスキャニング、コピーのジョブ完了後、HDD または RAM（RAM ディスク）に保存されている*スプールデータ*が存在している領域に対しランダムデータを上書きする。Flash メモリに*スプールデータ*を保存しているファクスジョブの場合は、*スプールデータ*が存在している領域に対し固定値を上書きする。

データ暗号化機能は、ドキュメントデータ、イメージデータを MSD に保存する前に暗号化する。このデータ暗号化機能により、ジョブ完了に伴うデータ消去機能が動作する以前の状態においても、暗号鍵を入手しない限り、MSD からのドキュメントデータやイメージデータを再生することは出来ない。即ち、ジョブ完了前について、MSD に保存されている*スプールデータ*に対しても、不正な開示や、不測の開示に対処している。

TOE セキュリティ機能には、上記の二つの機能のほか、それらを有効に機能させるための、暗号鍵生成機能やセキュリティ管理機能等が含まれる。詳細は、TOE 要約仕様の第 6 章に記載している。

2.2 TOE 構成の範囲と境界

本節では、TOE の物理的、論理的境界について述べる。

2.2.1 物理的範囲と境界

図 1 に MFD の物理的構成を示す。

図の中央、MFD 本体内の、コントローラユニットが、MFD 全体を制御している。

TOE は、コントローラ基板のファームウェアの交換用 ROM モジュール内に存在する。

TOE の物理的影響が及ぶ範囲は、TOE を格納する交換用 ROM のほか、ジョブをスプールするための MSD (HDD、RAM ディスク、及び Flash メモリ)、セキュリティ設定を格納する EEPROM、及び操作パネルである。

a) DSK を含むコントローラユニット
   コントローラユニットはマイクロプロセッサ、及びそれにより実行されるファームウェアを有する。また、マイクロプロセッサの動作に必要な、揮発性 RAM を有する。EEPROM については別項を立てて記述する。
   コントローラユニットのマイクロプロセッサがすべての TSF を実行する。
   暗号鍵は、本揮発性 RAM に格納される。
   DSK は、本ファームウェアを交換する形で設置する。交換用 ROM 及び交換対象 ROM の物理的形態は、1 枚または 2 枚の ROM モジュールである。AR-FR5 は 1 枚、AR-FR4 は 2 枚の ROM モジュー

ルで構成される。各 ROM モジュールは、ROM チップ等を実装した約 25mm×60mm のプリント基板モジュールであり、一辺にエッジコネクタを有する。コントローラユニットに、交換対象 ROM 及び DSK の交換用 ROM がエッジコネクタにて装着される。

b) ジョブをスプールするための MSD
これは HDD、RAM ディスク、及び Flash メモリである。オプションの HDD カードは、コントローラユニットに接続する。HDD を持たない構成では、代わりにコントローラユニットの揮発性 RAM の一部が RAM ディスクとして使用される。
ファクスジョブ用の Flash メモリは、ファクス・インタフェース・カード上にある。同カードは、オプションのファクス拡張キットの同梱品であり、ファクス拡張キットと本体 (のコントローラユニット) を接続する機能、及びファクスのスプールデータを格納する Flash メモリを有する。

c) 操作パネル
操作パネルにより、MFD/プリンタとしての各種操作を行い、また TOE のセキュリティ設定を行うことができる。TOE 境界の観点からは、TOE のセキュリティ設定操作、及びその前提となる認証操作を行うための装置と考える。
スキャナユニットを持たないプリンタは、本体の英数カナ表示操作パネルにより操作する。スキャナユニットを有する MFD は、スキャナユニットのタッチパネル式操作パネルにより操作し、本体の英数カナ表示操作パネルは使用できない。これらの操作パネルはいずれもコントローラユニットのファームウェアの管理下にある。

d) セキュリティ設定を格納する EEPROM
前項のセキュリティ設定操作による設定値は、コントローラユニットの EEPROM に格納される。セキュリティ設定値を参照または変更するには、前項の操作パネルを操作する必要があり、それ以外の手段 (例えば通信を介した遠隔操作) はない。

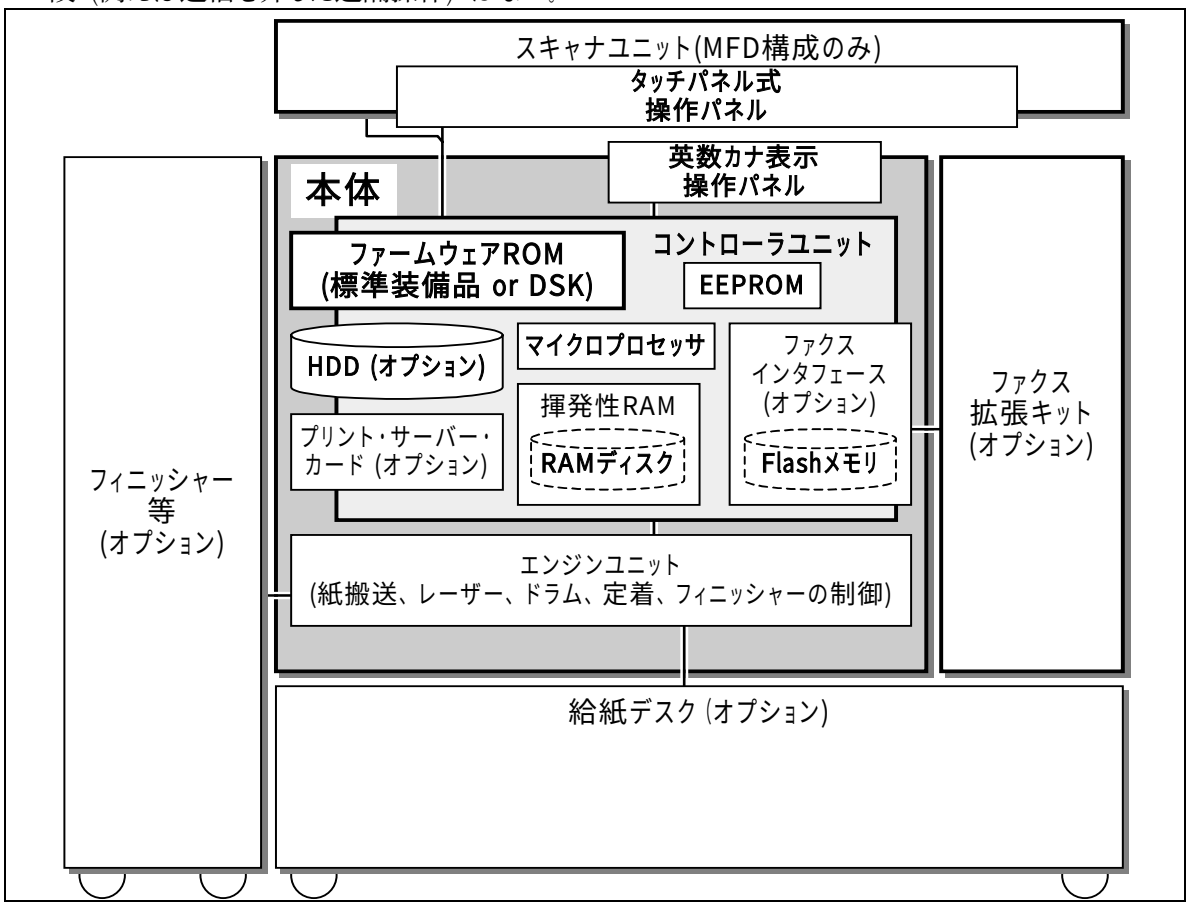

図 1: MFDの物理的構成とTOE

以下、TOE の物理的範囲と境界の外にある構成についての考察を述べる。

まず、ジョブの発生源と、ジョブの処理装置の区別を示す。ジョブの発生源とジョブの処理装置の双方に属しているものがあるが、各オプション、もしくは各ユニットの動作が異なるためである。

1) ジョブの発生源
    a) スキャナユニット
    MFD が、複写機として動作する、ネットワークスキャナとして動作する、または FAX 送信読取機能として動作する
    b) プリント・サーバー・カード（100 Base-TX / 10 Base-T ネットワークインタフェース）
    MFD がネットワークからのプリント要求を受ける場合
    c) IEEE1284 パラレルインタフェース
    MFD が IEEE1284 パラレルインタフェースからのプリント要求を受ける
    d) ファクス拡張キット
    MFD が電話回線を介して FAX 受信機能として動作する場合
2) ジョブの処理装置
    a) プリント・サーバー・カード（100 Base-TX / 10 Base-T ネットワークインタフェース）
    MFD がネットワークスキャナとして動作する場合
    b) ファクス拡張キット
    MFD が FAX 送信機能として動作する場合
    c) エンジンユニット
    d) 給紙デスク
    e) フィニッシャー

MFD が処理すべきプリント、コピー、イメージスキャニング、及びファクスのジョブは、TOE の物理的（及び論理的）範囲外で発生し、それを MFD が受け付け、スプールする。TOE はジョブをスプールする段階に関与し、スプールデータの暗号化を行う。例えば、オプションのスキャナユニットは、MFD のコントローラユニット及び操作パネルと共に、コピージョブ、イメージスキャニングジョブまたはファクス送信ジョブを発生する。

スプール済みジョブは、TOE による復号を経て、TOE の物理的（及び論理的）範囲外でジョブ処理、すなわち印刷または送信される。印刷を例に取れば、プリントジョブ、コピージョブまたはファクス受信ジョブの処理は、ジョブのスプールデータを、MFD のコントローラユニットが MFD のエンジンユニットに印刷させることである。

エンジンユニット、オプションのスキャナユニット、プリント・サーバー・カード（100 Base-TX / 10 Base-T ネットワークインタフェース）、給紙デスク、フィニッシャー等の各ユニットも、マイクロプロセッサとファームウェアを有する。しかし、DSK はそれら各ユニットのファームウェアを変更したり、動作に影響を与えたりするものではなく、それら各ユニットは TOE の物理的範囲に含まれない。

MFD のコントローラユニットは、プリントジョブを受け付けるための IEEE1284 パラレルインタフェースを有する。また、コントローラユニットには、オプションでファクス拡張キット（ファクス機能のため電話回線への接続を有する）、及びプリント・サーバー・カード（100 Base-TX / 10 Base-T ネットワークインタフェース）を装備できる。MFD はこれら外部インタフェースを通じ、ジョブの入出力を行う。パラレルインタフェース及びネットワークインタフェースよりプリントジョブを受け付け、電話回線よりファクス受信ジョブを受け付け、ファクス送信ジョブにより電話回線からの送出を行い、イメージスキャニングジョブによりネットワークインタフェースからの送出を行う。

2.2.2 論理的範囲と境界

図 2に TOE の論理的構成を示す。

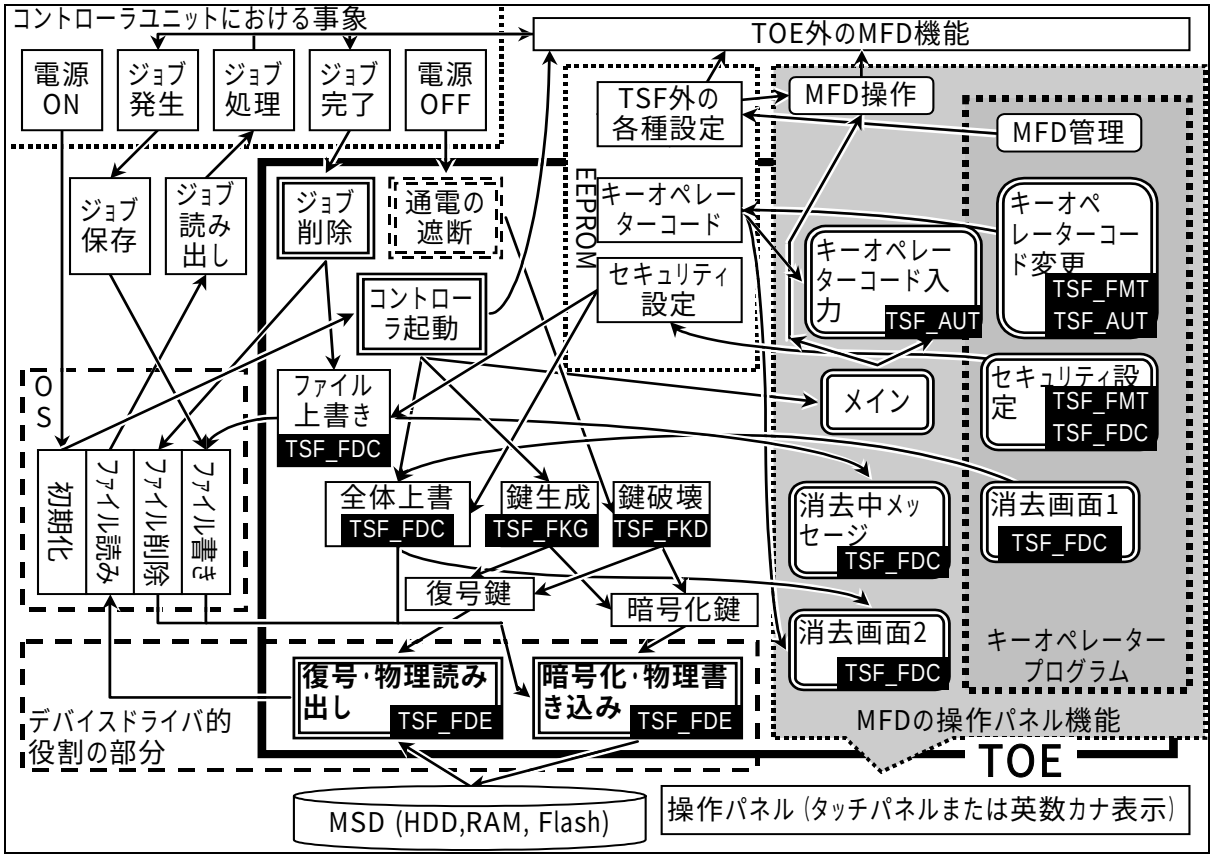

図 2: TOEの論理的構成

コントローラユニットのファームウェア（TOE を含む）は、コントローラユニット上で動作する単一のプログラムである。TOE のソフトウェア的動作環境は、コントローラユニットが使用しているマイクロプロセッサ及びＯＳである。マイクロプロセッサについては2.2.1節のa)項に記載した。

ファームウェアは、大別して三つの部分から成る。上記ＯＳの部分と、ＯＳ上で動作するアプリケーションソフトウェア的役割の部分と、ＯＳと共にハードウェアを制御するデバイスドライバ的役割の部分である。
TOE はアプリケーションソフトウェア的役割部分の一部とデバイスドライバ的役割部分の一部から成る。図中にはＯＳの機能およびデバイスドライバ的役割部分のうち、TSF に対するインタフェースを説明するために最低限必要な部分だけを図示している。

図中には MFD のハードウェアとして、MSD 及び操作パネルを示している。それ以外の記載はソフトウェア機能（プログラム、データ、または事象）である。ソフトウェア機能のうち、ＯＳの機能およびデバイスドライバ的役割部分をそれぞれ破線囲みで示す。それ以外は、アプリケーションソフトウェア的役割部分である。角を丸めた長方形で、操作パネル機能すなわちユーザインタフェースを、それ以外のソフトウェア機能を長方形で示すこととし、それらのうち TSF に対するインタフェースを二重線で示す。特定の TSF に固有の TOE 内ソフトウェア機能については、その TSF 略称を白抜き文字で示す。

TOE の論理的境界は以下の TOE セキュリティ機能（TSF）で規定される。

a) データ消去(TSF_FDC)
b) 暗号操作(TSF_FDE)
c) 暗号鍵生成(TSF_FKG)
d) 暗号鍵破壊(TSF_FKD)
e) 認証(TSF_AUT)
f) セキュリティ管理(TSF_FMT)

これら各 TSF の詳細は、第6章で説明する。ここでは、論理的範囲と境界について説明する。

a) データ消去(TSF_FDC)

通常の動作では、MFD はドキュメントデータやイメージデータを MSD にスプールする。プリンタ、コピー、イメージスキャニングの動作に関しては、HDD または RAM ディスク領域内に、ファクス動作に関しては、Flash メモリ領域にそれぞれスプールされる。

ジョブが完了すれば当該ジョブのスプールデータは無用になるので、MFD は無用になったデータファイルを MSD から削除する。これは対象 MFD においては、MSD の管理領域を書き換え、当該ファイルの登録を抹消することである。これにより、当該ファイルが占有していた管理領域及びデータ領域の占有が解かれ、他のジョブによる再利用が可能になる。この場合、削除されたファイルのデータ領域が他のジョブのスプールデータファイルに上書きされる保証はない。

TOE のデータ消去機能(TSF_FDC)は、MFD が持つファイル削除機能に対し、データ領域の上書き機能を追加する。この機能は、削除されるファイルが占有するデータ領域に対して上書きを行う。この機能を、*各ジョブ完了後の自動消去* と呼ぶ。

TOE のデータ消去機能(TSF_FDC)は、また MFD の電源 ON 時に、HDD または RAM ディスクのスプール領域全体に対し、上書きによる消去を行う。この機能を、*電源ON時の自動消去* と呼ぶ。

また、手動操作により HDD または RAM ディスク、及び Flash メモリの領域に対して上書きによる消去を行う機能を有する。この機能を、*全データエリア消去* と呼ぶ。特に本 ST では、*キーオペレーターの操作による全データエリア消去* と表記する。

MFD に TOE を設置することは、本 TSF に関しては、上書き機能のコードを追加し、既存のファイル削除のコードを、上書き機能の呼び出しを含むコードに置き換え、ファイル削除機能の初期化コード（電源 ON 時に呼び出される）を、電源ON時の自動消去機能の呼び出しを含む版に置き換え、全データエリア消去の選択肢を、管理者向けのユーザインタフェースに追加することである。TOE は、ジョブ完了時にはファイル削除に加えて当該ファイル領域の自動消去を行い、電源 ON 時には HDD または RAM ディスクのスプール領域全体の自動消去を実行し、ユーザインタフェースを通して全データエリア消去機能を提供する。

よって、本 TSF に関し、上書き機能が TOE の論理的範囲に含まれる。ジョブのスプールデータファイル削除機能のエントリポイントが論理的境界の一つとなる。このエントリポイントは、MFD がジョブ完了時に呼び出すものである。また、コントローラ起動のエントリポイントも論理的境界となる。これは、MFD が電源 ON 時に、HDD/RAM 及び Flash メモリの各ファイルシステムの管理機能を立上げるために呼び出すものである。本 TSF のユーザインタフェースは、以下の通りである。

- 消去中メッセージ
  各ジョブ完了後の自動消去 時に表示する。これは、TOE 内において、本 TSF により呼び出される。
- *全データエリア消去* 操作
  キーオペレーターの操作による全データエリア消去 のためのユーザインタフェースである。後述のセキュリティ管理（TSF_FMT）における *セキュリティ設定* ユーザインタフェースに含まれている。
- 消去画面1
  前項の操作により表示され。全データエリア消去を、本当に実行するか、やめるかを選択操作できる。TOE 内において、本 TSF により呼び出される。
- 消去画面2
  前項の操作で実行する選択をした場合、及び、*電源ON時の自動消去* 実行中に表示する。全データエリアを消去中である旨と共に、何%程度まで進捗したかを表示する。TOE 内において、本 TSF により呼び出される。

b) 暗号操作(TSF_FDE)

ジョブが発生した際、MSD にデータファイルを作成することによってジョブをスプールする。このファイル作成に際して、TOE の暗号操作（TSF_FDE）機能により、データを暗号化して MSD に書き込む。また、スプールされたジョブを実際に処理する際には、処理の過程で必要となるデータ断片（処理中ジョブ１件のスプールデータの一部）を必要の都度、暗号化されたデータ断片の MSD からの読み出し、及びその復号によって得る。復号の機能も、暗号操作（TSF_FDE）に含まれる。この暗号化及び復号の呼び出しは、ジョブのファイル読み書きの際に行われる。暗号化及び復号に使用する暗号鍵は揮発性 RAM 上に保持する。

MFD に TOE を設置することは、本 TSF に関しては、暗号化及び復号のコードを追加し、既存のファイル読み書きのコードを、暗号化及び復号の呼び出しを含むコードに置き換えることである。この暗号化のコード、及び復号のコードはそれぞれ、ジョブのスプールデータを MSD に書き込む際、及びスプールデータを MSD から読み出す際に実行される。暗号化及び復号のコードは、暗号鍵へのアクセスを含む。

よって、本 TSF に関し、ジョブのスプールデータファイル読み書き、暗号化、及び復号の各コード、並びに揮発性 RAM 上の暗号鍵が TOE の論理的範囲に含まれ、MSD に対するセクタ単位の読み書き機能をＯＳに提供するデバイスドライバのエントリポイントが論理的境界となる。これらエントリポイントは、MFD がジョブを受け付け、スプールデータを保存する際、及び、ジョブの処理にあたって、スプールデータを読み出す際に、ＯＳを介して呼び出されるものである。

TOE の意図しない暗号操作は、MFD の操作パネルからの操作、及び外部インタフェース（ネットワークインタフェース、IEEE1284 パラレルインタフェース、電話回線インタフェース）からアクセスできないことを実装として保証している。

c) 暗号鍵生成(TSF_FKG)
d) 暗号鍵破壊(TSF_FKD)

暗号鍵の生成機能、及び、暗号鍵の破壊機能は、MFD の暗号鍵情報を取り扱う。MFD の起動時に暗号鍵を生成(TSF_FKG)し、揮発性 RAM 内に保存する。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いる。揮発性 RAM 内に保存された暗号鍵は、MFD の電源がオフになるか停電によって、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ず、暗号鍵破壊(TSF_FKD)となる。暗号鍵生成（TSF_FKG）によって生成された暗号鍵は、暗号鍵破壊（TSF_FKD）まで使用される。

TSF_FKG に関しては、MFD に TOE を設置することにより、暗号鍵生成コードが追加される。すなわち、コントローラ起動時に実行されるスプール管理の初期化処理コードが、暗号鍵生成コードを呼び出す版に置き換わる。これらは、MFD 及び TOE の電源 ON 時に実行される。

TOE が含む暗号鍵生成コード及び揮発性 RAM 上の暗号鍵が TOE の論理的範囲に含まれ、上のデータ消去の項で述べたコントローラ起動のエントリポイントが論理的境界となる。TSF_FKD の論理的範囲は揮発性 RAM 上の暗号鍵であり、論理的境界は特にない。

TOE の生成する暗号鍵は揮発性 RAM 内に保存するが、MFD の操作パネルからの操作、及び外部インタフェース（ネットワークインタフェース、IEEE1284 パラレルインタフェース、電話回線インタフェース）からアクセスできないことを実装として保証している。

HDD または RAM ディスクのスプールデータの暗号化、及び復号に使用する暗号鍵は、日時データとティック時間（Tick）を用いており、日時データは RTC（時計回路）から取得している。この RTC は、MFD の電源がオンであろうと、オフであろうと稼働し続けている。RTC から取得する日時データは、キーオペレーターが設定可能であるが、MFD が暗号鍵を生成する時点の日時データ、及びティック時間を合わせるのは事実上不可能であり、同一の暗号鍵を生成することはできない。

e) 認証(TSF_AUT)

DSK の対象 MFD は、DSK 設置前より MFD 管理機能を持ち、その MFD 管理機能を *キーオペレータープログラム* と称する。MFD を設置する組織において、MFD 管理者としてキーオペレータープログラムの実行を許された利用者を、*キーオペレーター* と称する。キーオペレータープログラムを実行するには、5 桁の PIN の認証によりキーオペレーターは自らを認証しなければならない。この PIN を *キーオペレーターコード* と称する。キーオペレーターコードにより、キーオペレーターのみがキーオペレータープログラムにアクセスできる。

一般利用者は、キーオペレータープログラム以外の MFD の機能を認証無しで利用できる。

DSK はそのセキュリティ管理機能を、上記のキーオペレーターコードと同一仕様の認証により保護することとし、その認証をキーオペレーターコード認証と統合している。それに伴い、セキュリティ管理機能へのアクセスを、キーオペレータープログラムの操作メニューに統合している。すなわち DSK は、セキュリティ管理機能へのアクセスを、MFD のキーオペレータープログラムに追加し、キーオペレーターコードをセキュリティ管理機能に対する認証手段として実装する。

そのため、セキュリティ管理 (TSF_FMT) にアクセスするためには、キーオペレーターはキーオペレーターコードを入力し認証されねばならない。これにより、キーオペレーターのみがセキュリティ管理機能にアクセスできる。

キーオペレーターコードは MFD の EEPROM に保存されている。本 TSF は、利用者が入力した値と、EEPROM に保存されていた値を比較し、一致を確認することによって認証を実現する。

DSK が提供する認証ユーザインタフェースは、TOE の論理的範囲に含まれる。本 TSF に関する TOE の論理的境界は、利用者による認証ユーザインタフェースへのアクセス操作である。

f) セキュリティ管理(TSF_FMT)

MFD に TOE を設置することにより、セキュリティ管理機能で変更可能なパラメータへのアクセスが追加される。TOE 設置はまた、セキュリティ管理メニュー傘下のユーザインタフェースを追加する。そしてまた TOE 設置は、ユーザインタフェースにおける、キーオペレータープログラムのトップメニューを (セキュリティ管理を呼び出す版に) 置き換え、認証画面を (このトップメニューを呼び出す版に) 置き換える。

本 TSF のユーザインタフェースは、以下の通りである。

- セキュリティ設定
  データ消去 (TSF_FDC) 機能のふるまいについて設定する機能を持つ。操作パネルにて設定を変更することができ、設定が変更されれば MFD の EEPROM に保存している値を書き換える。また、前述の、*キーオペレーターの操作による全データエリア消去* のユーザインタフェースを含む。
- キーオペレーターコードの変更
  操作パネルにて新しい値の入力を求め、MFD の EEPROM に保存している値を書き換える。

上記ユーザインタフェース、及び認証ユーザインタフェースから上記ユーザインタフェースに至る経路となる各ユーザインタフェースが TOE の論理的範囲に含まれる。本 TSF に関する TOE の論理的境界は、認証 (TSF_AUT) にある。本 TSF 利用者による認証画面へのアクセス操作が、TOE の論理的境界を構成する。

2.3 MFD のライフサイクル及び TOE の保護資産

MFD のライフサイクル、即ち、MFD の購入から廃棄までにおける、TOE の保護資産は以下の通りである。

2.3.1 MFD 及び TOE の購入･リース開始時

MFD 及び TOE の購入、もしくはリース開始時における保護資産はない。

2.3.2 MFD 及び TOE の運用時

MFD 運用中において、以下のものを保護資産とする。

a) MFD のトラブルにより、コピー、プリント、イメージスキャニング、ファクスの各ジョブの処理途上に、MSD 内に生成されるスプールデータ。

b) 以下の TOE のセキュリティ管理機能の設定値。
- *電源 ON 時の自動消去* 実行もしくは不実行
- *各ジョブ完了後の自動消去* の消去回数
- *電源 ON 時の自動消去* の消去回数
- *キーオペレーターの操作による全データエリア消去* の消去回数
- キーオペレーターコード

以下は、保護資産であるスプールデータが MSD 内に残存したままとなる。

1) MFD のトラブルにより、コピー、プリント、イメージスキャニング、ファクスの各ジョブが完了する前に MFD の電源断となった場合。

2) MFD のジョブリテンション機能で、MSD 内のスプールデータを、MFD の操作パネルから削除する前に、MFD の電源断となった場合。
なお、ジョブリテンション機能は、MFD にハードディスクを搭載した場合に利用できる機能で、コンピュータから印刷を行う場合、即ち MFD のプリント機能を利用する場合において有効となる機能である。ジョブリテンションで可能となる機能は、以下の通りである。
- 印刷完了後ホールド
  この機能は、MFDが印刷を完了しても、印刷データをMSD内に、MFDの電源が切られるか、印刷データを削除するまで保持しており、必要に応じてMFD操作パネルから再印刷を可能とする
- 印刷せずにホールド
  この機能は、MFDが印刷を受けても、印刷はせず、MSD内に印刷データを保存し、MFD操作パネルから印刷開始操作を行うことが可能。印刷データは、MFDの電源が切られるか、データを削除するまで保持する。
- サンプルプリント
  この機能は、MFDがコンピュータから印刷データを受けると、まず1部だけ印刷し、残りの部分数をMSD内に保存し、MFD操作パネルから残りの部数分の印刷開始操作を行うことが可能。印刷データは、MFDの電源が切られるか、データを削除するまで保持する。

いずれの機能についても、コンピュータからプリント時に指定したパスコードを、MFD の操作パネルから入力することにより、印刷開始、もしくはデータ削除が可能である。このジョブリテンション機能は、上述のように MFD の操作パネルから印刷開始操作を行うための通常利用することができる機能であり、TOE のセキュリティ機能ではない。
パスコードは、ジョブリテンション機能を実現するために必要となるものである。また、TOE の保護すべき資産は、上述の a) 及び b) で示したものであり、パスコードの不正使用によるものではない。このため、TOE はパスコードの不正使用に対抗しない。

MFD は、IEEE1284 パラレルインタフェース、電話回線インタフェース、及びネットワークインタフェースを有するが、MFD の運用中、これら外部インタフェースから、MFD の意図しない使用により、MSD に保存されているスプールデータへのアクセスはできない。

2.3.3 MFD 及び TOE の廃棄･リース終了時

MFD 及び TOE の廃棄、及びリース終了時における保護資産は、2.3.2節の 1)、及び 1) のまま、MFD 及びを廃棄、もしくはリース終了に伴う MFD の返却を行うことにより、MSD に残存しているスプールデータである。

3 TOE セキュリティ環境

本章では TOE セキュリティ環境について述べる。

3.1 前提条件

本節では、TOE に対して所要の環境のセキュリティ面について説明している。環境の、物理的、人的、手続、接続性、及び、機能面に関する情報を含んでいる。操作環境はデリバリー、操作、利用者及びキーオペレーターガイダンスの保証要件の文書に準拠して管理されなければならない。TOE が使用される環境は、以下の規定状況にあると想定している。

3.1.1 想定環境

TOE のセキュリティを確保するためには、表 4 で詳述する想定環境が必要である。

表 4: 想定環境

定義	記述
A.OFFICE	TOEが組み込まれたMFDは、一般的なオフィス環境に設置される。オフィスに働く従業員が不在の場合、オフィスは施錠等による防犯対策が実施されている。また、従業員不在時の入室の際は、適切な従業員であることを確認するようオフィスは管理されている。
A.PROCEDURE	キーオペレーターは、以下の事項を遵守するものとする。 ・ TOEがインストールされていることを確認する。 ・ 消去ふるまい設定、消去回数設定を適切に行う。 ・ *キーオペレーターコード* を定期的に変更する。 ・ *キーオペレーターコード* は容易に推測できないものを設定する。 ・ *キーオペレーターコード* を他者に開示しない。

3.2 脅威

表 5 は、TOE に対する脅威を示している。TOE に対する脅威は、TOE の動作について、一般的知識を有し、MFD から物理的に MSD を取り出す技能を有し、簡単に入手することができるハードウェアやソフトウェアのツールを使用して、MSD 内の情報再生をはかる利用者が存在する事である。また、TOE のセキュリティ機能の管理に関し、消去ふるまい設定、及び消去回数設定を改変される事である。

MSD 内の情報再生については、TOE を搭載した MFD 運用中における MSD の盗難や、MSD の一時的な取り出し時、及び MFD の廃棄、売却、リース期間終了時等の事由により MFD を手放す場合、その MSD は脅威にさらされる事となる。

また、TOE のセキュリティ機能の管理については、MFD の操作パネルからの操作により、脅威にさらされる事となる。

脅威の低減は第4章、セキュリティ対策方針に記載されている目標を通じて行われる。

表 5: TOE に対する脅威

定義	記述
T.RECOVER	悪意の利用者が、MFDからMSDを物理的に取り出した後、市販のツールを使用して内容を読み出して、コピー、プリント、イメージスキャニング、ファクスの各ジョブの、MSD内の*残存データ* からドキュメントデータやイメージデータの再生を試みる可能性がある。
T.ALTER	悪意の利用者が、TOEのセキュリティ管理機能の設定値を改変する可能性がある。

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問題や脅威に対する対応を詳述している。脅威は TOE または、セキュリティ環境あるいは両者に向けられることがあるため、コモンクライテリア (CC) では、以下の 2 つのセキュリティ対策方針カテゴリーを規定している。

a) TOE に対するセキュリティ対策方針

b) 環境に対するセキュリティ対策方針

4.1 TOE に対するセキュリティ対策方針

本節では TOE に対するセキュリティ対策方針を説明する。TOE は表 6 に記載のセキュリティ対策方針を達成する。

表 6: TOE に対するセキュリティ対策方針

定義	記述
O.RESIDUAL	ジョブが完了すると、ジョブの*スプールデータ* は、MSDから設定された消去回数に従って、直ちに上書き消去されなければならない。上書き消去されないまま電源OFFになった場合、次回電源ON時に、設定された消去回数に従って上書き消去されなければならない。
O.REMOVE	TOEが組込まれているMFDのMSDに、当該MFD自身以外より、物理的手段でアクセスされても、ジョブデータの再生を不可能としなければならない。
O.AUTHENTICATION	TOEのセキュリティ管理機能を利用するためには、*キーオペレーターコード* によるキーオペレーター認証を行う。

4.2 環境に対するセキュリティ対策方針

表 7 に環境に対するセキュリティ対策方針を定義する。

表 7: 環境に対するセキュリティ対策方針

定義	記述
OE.SECURE	TOEが組み込まれたMFDを設置しているオフィスで働く従業員が不在の場合、オフィスは施錠等による防犯対策を実施する。また、従業員不在時の入室の際は、適切な従業員であることを確認するようオフィスを管理する。
OE.OPERATE	キーオペレーターには、以下を確実に実施でき、信頼できる人を指定する。 ・ TOEがインストールされていることを確認する。 ・ 消去ふるまい設定、消去回数設定を適切に行う。 ・ *キーオペレーターコード* を定期的に変更する。 ・ *キーオペレーターコード* は容易に推測できないものを設定する。 ・ *キーオペレーターコード* を他者に開示しない。

5 ITセキュリティ要件

本章では TOE またはその環境が満たすべき IT セキュリティ要件を規定する。

コモンクライテリア (CC) では、TOE セキュリティ要件を以下の2つのカテゴリーに分けている。

a) TOE のセキュリティ対策方針達成に必要な TOE 及び、そのサポート証拠が満たすべきセキュリティ機能要件 (SFR) (例:識別と認証、セキュリティ管理、利用者データ保護)。

b) TOE とその IT 環境がセキュリティ対策方針を達成する信頼性根拠を与えるセキュリティ保証要件 (SAR) (例:構成管理、テスト, 脆弱性分析)

これらの要件は以下のサブセクションで個別に論じられる。

5.1 TOE セキュリティ機能要件(SFR)

TOE は表 8で詳述のセキュリティ機能要件 (SFR) を満たす。本節の以下の部分では各コンポーネントと関連する依存性について述べる。

表 8: TOE セキュリティ機能要件(SFR)

機能コンポーネントID	機能コンポーネント名称
暗号サポート (TSF_FDE, TSF_FKG, TSF_FKD)	
FCS_CKM.1(1)	暗号鍵生成(1)
FCS_CKM.1(2)	暗号鍵生成(2)
FCS_CKM.4	暗号鍵破棄
FCS_COP.1	暗号操作
データ消去 (TSF_FDC)	
FDP_RIP.1	サブセット残存情報保護
認証(TSF_AUT)	
FIA_UAU.2	アクション前の利用者認証
FIA_UAU.7	保護された認証フィードバック
FIA_SOS.1	秘密の検証
セキュリティ管理 (TSF_FMT)	
FMT_MOF.1(1)	セキュリティ機能のふるまいの管理(1)
FMT_MOF.1(2)	セキュリティ機能のふるまいの管理(2)
FMT_MTD.1	TSFデータの管理
FMT_SMF.1	機能管理の特定
FMT_SMR.1	セキュリティ役割

5.1.1 クラス FCS: 暗号サポート

適用上の注釈:
DSK を搭載している MFD の電源がオンになると、暗号化、及び復号用の鍵を生成する。鍵が揮発性 RAM に保存され、MFD の電源がオフ、または、停電となるまでは利用可能状態にあるが、一旦鍵が失われると、それをリカバーする方法はない。暗号鍵には、HDD もしくは RAM を MSD として使用する場合の暗号鍵と、Flash メモリを MSD として使用する場合の2つが存在する。

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［ AES 準拠 ］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

（セキュリティ機能要件(SFR)では、FMT_MSA.2 について依存性が明示されているが、本 TOE は FMT_MSA.2 を必要としない。8.2.1節で詳述する。）

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［ AES 準拠 ］に合致する、指定された暗号鍵生成アルゴリズム［ MSN-T 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

（セキュリティ機能要件(SFR)では、FMT_MSA.2 について依存性が明示されているが、本 TOE は FMT_MSA.2 を必要としない。8.2.1節で詳述する。）

c) FCS_CKM.4 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 TSF は、以下の［ 指定なし ］に合致する、指定された暗号鍵破棄方法[電源オフまたは停電]に従って、暗号鍵を破棄しなければならない。

依存性: FCS_CKM.1 暗号鍵生成

（セキュリティ機能要件(SFR)では、FMT_MSA.2 について依存性が明示されているが、本 TOE は FMT_MSA.2 を必要としない。8.2.1節で詳述する。）

d) FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 TSF は、[AES 準拠]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、[ドキュメントデータ、及び、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

5.1.2 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[*<u>からの資源の割当て解除</u>*]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:[MFD のプリントジョブ、コピージョブ、イメージスキャニングジョブ、またはファクスジョブの各スプールデータ]。

依存性: なし

5.1.3 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: なし

(セキュリティ機能要件(SFR)では、FIA_UID.1 について依存性が明示されているが、本 TOE は FIA_UID.1 を必要としない。8.2.1節で詳述する。)

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_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[5文字の数字からなるキーオペレーターコード]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

5.1.4 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 [電源 ON 時の自動消去実行設定、もしくは不実行設定] [*のふるまいを決定する*]能力を [キーオペレーター] に制限しなければならない。

依存性: FMT_SMF.1 機能管理の特定、
FMT_SMR.1 セキュリティ役割

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 [キーオペレーターの操作による全データエリア消去] [*を動作させる*]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_SMF.1 機能管理の特定、
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、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 もしくは RAM（RAM ディスク）に対する上書きの回数、電源 ON 時の自動消去における HDD もしくは RAM（RAM ディスク）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 もしくは RAM（RAM ディスク）に対する上書きの回数]を[*問合せ, 改変,* [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_SMF.1 管理機能の特定、
FMT_SMR.1 セキュリティ役割

d) 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 の管理機能]。

依存性: なし

表 9: TOE の管理機能

機能要件	管理機能
FCS_CKM.1(1)、FCS_CKM.1(2)、FCS_CKM.1(4)	なし（暗号鍵の属性の変更を行っていないため、管理機能がない）
FCS_COP.1、FIA_UAU.7、FMT_MSA.2、FMT_SMF.1	なし（管理機能要請なし）
FDP_RIP.1	上書き消去に関する下記項目を管理する機能 ・電源ON時の自動消去機能実行、もしくは不実行設定値 ・ジョブ終了後のデータ消去回数設定値 ・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設定値 ・電源ON時の自動消去におけるデータ消去回数設定値
FIA_UAU.2	キーオペレーターコード変更機能
FIA_SOS.1	なし（品質尺度は固定値であるため、管理機能がない）
FMT_MOF.1(1)、FMT_MOF.1(2) 、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、管理機能がない）
FMT_SMR.1	なし（TOE を維持する役割はキーオペレーターのみであるため、管理機能がない）

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: なし

（セキュリティ機能要件(SFR)では、FIA_UID.1 について依存性が明示されているが、本 TOE は FIA_UID.1 を必要としない。8.2.1節で詳述する。）

5.2 TOE セキュリティ保証要件

表 10 は、[CC_PART3] のセキュリティ保証要件 EAL4 から選択された本セキュリティ保証コンポーネントを規定するものである。

表 10: EAL4 保証要件

保証コンポーネントID	保証コンポーネント名称	依存性
ACM_AUT.1	部分的なCM自動化	ACM_CAP.3
ACM_CAP.4	生成の支援と受入手続き	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	問題追跡のCM範囲	ACM_CAP.3
ADO_DEL.2	改変の検出	ACM_CAP.3
ADO_IGS.1	設置、生成、及び立上げ手順	AGD_ADM.1
ADV_FSP.2	完全に定義された外部インタフェース	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_IMP.1	TSFの実装のサブセット	AVD_LLD.1, ADV_RCR.1, ALC_TAT.1
AVD_LLD.1	記述的下位レベル設計	ADV_HLD.2, 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
ALC_LCD.1	開発者によるライフサイクルモデルの定義	なし
ALC_TAT.1	明確に定義された開発ツール	ADV_IMP.1
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, ATE_FUN.1
AVA_MSU.2	分析の確認	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.2	独立脆弱性テスト	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1

5.3 IT 環境に対するセキュリティ要件

IT 環境に対するセキュリティ要件はない。

5.4 本 TOE 対する明示的な要件

本 ST は当該 TOE の明示的な要件を含んでいない。すべてのセキュリティ機能要件(SFR)は [CC_PART2] から抜粋されてきたものである。

5.5 セキュリティ機能強度

本 TOE の全体のセキュリティ最小機能強度 (SOF) は SOF-基本強度である。

また、本 TOE が満足する機能要件のうち、確率的または順列的メカニズムを利用するのは、FIA_SOS.1 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。

6 TOE 要約仕様

本章では、TOE が装備しているセキュリティ機能と、それらの適正な装備を確保する為の保証手段の概要を示す。

6.1 TOE セキュリティ機能(TSF)

本節では、5.1節における SFR を満たす TOE のセキュリティ機能とその関連性を示す。

6.1.1 暗号操作(TSF_FDE)

通常の動作の間は、MFD はドキュメントデータやイメージデータを*スプールデータ*として MSD に保存する。ファクスデータは Flash メモリ領域に、コピー、イメージスキャニング、及び、プリントの対象となるドキュメントデータやイメージデータは HDD、及び RAM ディスク領域にそれぞれ*スプールデータ*として保存する。DSK は一時保存にあたり AES に準拠した Rijndael アルゴリズムによって、揮発性 RAM 内に保存している暗号化鍵に従って、暗号化して MSD にスプールする。

また、スプールされたジョブを実際に処理する際には、処理の過程で必要となるデータ断片（処理中ジョブ 1 件のスプールデータの一部）を必要の都度、暗号化されたデータ断片の MSD からの読み出し、及びその復号によって得る。

満たされる機能要件:　FCS_COP.1

6.1.2 暗号鍵生成(TSF_FKG)

DSK は、また暗号鍵（共通鍵）の生成を行い、ドキュメントデータや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 に準拠した 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 または RAM ディスクに保存または読出されるスプール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-T 拡張アルゴリズムを用いて MFD 内の Flash メモリに保存または読出されるスプール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 に保存する。

満たされる機能要件:　FCS_CKM.1

6.1.3 暗号鍵破壊（TSF_FKD）

DSK は、上記 2 本の 128 ビット長の暗号鍵を揮発性 RAM に保存している。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いる。このため揮発性 RAM 内に保存された暗号鍵は、MFD の電源がオフになるか停電によって、蓄えられていた電荷が無くなることにより、暗号鍵を読み出すことができず、暗号鍵を破壊となる。

満たされる機能要件:　FCS_CKM.4

6.1.4 データ消去 (TSF_FDC)

DSK は*スプールデータ* 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

b) 電源 ON 時の自動消去

c) キーオペレーターの操作による全データエリア消去

ジョブ完了後、HDD、及び RAM ディスク領域に保存されている*スプールデータ* については、ランダムデータを所定の回数繰り返して上書きし、Flash メモリに保存されているスプールデータについては、その各ビットに固定値(0)を上書きする。この機能を、*各ジョブ完了後の自動消去* と呼ぶ。

また、MFD の電源が ON になった際、スプール用の HDD、及び RAM ディスク領域の全体に、ランダムデータを所定の回数繰り返して上書きする。この機能を、*電源 ON 時の自動消去* と呼ぶ。

また、キーオペレーターの操作により、スプール用の HDD、及び RAM ディスク領域の全体に、ランダムデータを所定の回数繰り返して上書きし、スプール用の Flash メモリ領域の全ビットを、Flash メモリのブロック消去機能により固定値(1)で埋める。この機能を、*全データエリア消去* と呼ぶ。特に本 ST では、*キーオペレーターの操作による全データエリア消去* と表記する。

ランダムデータ上書きの繰返し回数は、キーオペレーターが設定する。

HDD の消去に固定値でなくランダムデータを用いるのは、残存磁気を増幅される虞を減らすためである。ランダムデータ上書きの繰返し回数を増やすことで、残存磁気をより低減できる。RAM ディスク領域は HDD と全く同じ扱いをしており、同一の上書き手段が適用される。

Flash メモリはその構造上、値(1)を持つビットへの値(0)上書きのみ可能で、値(0)のビットに値(1)を上書きすることはできない。値(0)のビットを値(1)に変えるにはブロックと称する大きな単位でまとめて消去するしかない。ジョブ1件のスプールデータが占有する領域のみを消去する場合、ブロック単位の消去では他のジョブまで消去してしまうため、値(0)を上書きすることによって消去している。

以下、本 TSF すなわちデータ消去機能に関する注意事項について述べる。

各ジョブ完了後の自動消去 機能は、ジョブが正常に完了した後、直ちに実行されるが、未完のジョブがある状態で、電源断、すなわち電源スイッチ操作や停電により通電が遮断された場合、それら未完のジョブは、上書き消去されないまま残存する。HDD については、ジョブ完了後であっても、不用意に電源を切れば、自動消去が完了しない可能性がある。HDD または RAM ディスク上のスプールデータは、一旦通電が遮断されれば無効扱いとなるので、電源断によって残存した HDD または RAM ディスク上のジョブはもはや *各ジョブ完了後の自動消去* の対象とならない。そのため、*電源 ON 時の自動消去* 機能が必要であり、キーオペレーターは、キーオペレーター文書指示の趣旨に則り、同機能を使用すべきである。

Flash メモリ上のファクスジョブについては、電源断にかかわらず、本当に正常処理されるまで完了とならず、必ず *各ジョブ完了後の自動消去* 機能の対象となる。それゆえ、Flash メモリは *電源 ON 時の自動消去* 機能の対象でない（対象とする必要はなく、また対象とすることは許されない）。ただし、*全データエリア消去* 機能を実行した場合は、未完であっても消去される。

次に、ジョブリテンション機能によるホールドジョブと、本 TSF すなわちデータ消去機能の関係について述べる。

通常のプリントジョブは、印刷が正常に完了した時点で、ジョブ完了扱いとなり、スプールデータが削除され、本 TSF により上書き消去される。それに対し、対象 MFD のジョブリテンション機能によるホールドジョブは、ホールドジョブリストから削除された時点で、ジョブ完了扱いとなり、スプールデータが削除され、本 TSF により上書き消去される。ホールドジョブリストから削除されるのは、MFD 操作パネルにて *削除* 操作がなされた場合、及び、MFD 操作パネルにて *プリント後データを削除* 操作がなされ、プリントが正常に完了した場合である。これ以外に、DSK の *全データエリア消去* 操作により、ホールドジョブを含む全スプールデータが消去される。

ホールドジョブを削除せずに電源を切った場合、ホールドジョブは未完のジョブの一種なので、上で述べた未完のジョブと同様に、HDD に残存する。このことについて、キーオペレーターは、キーオペレーター文書指示に従い、注意を払わなければならない。

キーオペレーター文書指示にも推奨の記載があるが、上で述べた各々のデータ残存のおそれに対処するため、キーオペレーターに対し、電源を切る前の *全データエリア消去* を推奨する。

なお、*ジョブリテンション機能* の概要は、以下の通りである。

対象 MFD に HDD を搭載すれば、プリントジョブに限り、ジョブリテンション機能を利用できる。これは印刷開始とジョブ完了のタイミングを、MFD 操作パネルで制御できる機能である。ジョブリテンション機能に

は*印刷後ホールド*, *印刷せずにホールド*, 及び*サンプルプリント* の3モードがある。*印刷後ホールド* は、通常の印刷を実行した後、ジョブを削除せず HDD に保存し、MFD 操作パネルにて再印刷できる。*印刷せずにホールド* は、ジョブを受け付けても HDD にスプールするだけで印刷を開始せず、MFD 操作パネルより印刷開始を指示でき、後で再印刷もできる。*サンプルプリント* は、複数部数を指定した場合に、大量のミスプリントを防ぐため、まず1部だけ印刷し、残部数は MFD 操作パネルにより印刷開始を指示でき、後で再印刷もできる。いずれのモードもジョブに暗証番号を付与でき、特に *印刷せずにホールド* と暗証番号を組み合わせれば、親展プリント機能として利用できる。いずれのモードも、操作パネルで、*削除*, *印刷して削除*, 及び、*印刷して保存*, の3通りを操作できる。*削除* 操作がなされた場合、または、*印刷して削除* の操作がなされ印刷が正常に完了した場合、上述の通り、ジョブ完了扱いとなり、スプールデータが削除され、本 TSF により上書き消去される。

満たされる機能要件: FDP_RIP.1, FMT_MOF.1(2), FMT_SMR.1

6.1.5 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へのアクセスのために5桁の PIN すなわ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(*)を表示して、入力した数字が見えないようにしている。

また、データ消去 (TSF_FDC)機能について、電源 ON 時の自動消去実行からの中断、及びキーオペレーター操作による全データ消去動作実行からの中断について、キーオペレーターコードの入力による認証を必要とする。

このキーオペレーターコード認証は、*確率的または順列的メカニズム* に該当する。そのセキュリティ強度 (SOF) は SOF-基本強度である。

満たされる機能要件: FMT_SMR.1, FIA_UAU.2, FIA_UAU.7, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MTD.1

6.1.6 セキュリティ管理 (TSF_FMT)

このセキュリティ管理(TSF_FMT)は、キーオペレーターコードの入力により、キーオペレーターが認証される手順を経た後に、以下のセキュリティ機能を設定することができる。

a) 電源 ON 時の自動消去機能実行、もしくは不実行の設定

また、データ消去機能に対し、HDD または RAM ディスクへのランダムデータ上書き動作回数変更ができる。

b) ジョブ終了後のデータ消去回数の設定

c) 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

d) 電源 ON 時の自動消去におけるデータ消去回数の設定

また、認証データすなわちキーオペレーターコードを変更することができる。

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。

なお、キーオペレーターコードを失念した場合、キーオペレーターコードを問い合わせ、削除、または消去するなどの復旧手段はない。

上に列挙した各設定値は、MFD 内の EEPROM に保存される。

満たされる機能要件: FMT_SMR.1, FMT_MOF.1(1), FMT_MTD.1, FIA_SOS.1, FMT_SMF.1

6.2 保証手段

本 TOE は、保証パッケージ EAL4 の保証要件を満たしている。本節では、EAL4 保証要件を満たすためにシャープ株式会社が適用する構成管理、配付と運用、開発、ガイダンス文書、ライフサイクルサポート、テスト、及び脆弱評定についての保証手段を示す。EAL4 保証パッケージと保証手段の対応について表 11に示す。

表 11: 保証コンポーネントと保証手段の対応

保証コンポーネント	保証手段
ACM_AUT.1 部分的なCM自動化	デジタル複合機データセキュリティキット 構成管理自動化ツール説明書
ACM_CAP.4 生成の支援と受入手続	デジタル複合機データセキュリティキット 構成管理システム説明書
ACM_SCP.2 問題追跡のCM範囲	デジタル複合機データセキュリティキット CM範囲説明書
ADO_DEL.2 改変の検出	デジタル複合機データセキュリティキット 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 設置手順適合確認資料
ADV_FSP.2 完全に定義 された外部インタフェース	デジタル複合機データセキュリティキット 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 上位レベル設計書
ADV_IMP.1 TSFの実装のサブセット	デジタル複合機データセキュリティキット ソースコード説明書
ADV_LLD.1 記述的下位レベル設計	デジタル複合機データセキュリティキット 下位レベル設計書
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 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 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	デジタル複合機データセキュリティキット ガイダンス文書クラス適合確認資料、 取扱説明書データセキュリティキットAR-FR4、 AR-FR4 Data Security Kit Operation Manual、 AR-FR5 Data Security Kit Operation Manual、 設置チェックリスト・取扱説明書追補版、 Installation Checklist・Supplemental Sheet、 レーザープリンタ 取扱説明書 (共通編) 、 LASER PRINTER Operation manual (for printer operation and general information)
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 開発セキュリティ仕様書
ALC_LCD.1 開発者による ライフサイクルモデルの定義	デジタル複合機データセキュリティキット ライフサイクル管理手順書
ALC_TAT.1 明確に定義された開発ツール	デジタル複合機データセキュリティキット 開発ツール資料
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 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 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 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 独立テスト環境・ツール説明書

保証コンポーネント	保証手段
AVA_MSU.2 分析の確認	デジタル複合機データセキュリティキット TOEの誤使用分析説明書、 取扱説明書データセキュリティキットAR-FR4、 AR-FR4 Data Security Kit Operation Manual、 AR-FR5 Data Security Kit Operation Manual、 設置チェックリスト・取扱説明書追補版、 Installation Checklist・Supplemental Sheet、 レーザープリンタ 取扱説明書（共通編）、 LASER PRINTER Operation manual (for printer operation and general information)
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 TOEセキュリティ機能強度評価
AVA_VLA.2 独自脆弱性分析	デジタル複合機データセキュリティキット 脆弱性分析書

7 PP 主張

本 TOE は PP には準拠していない。

8 根拠

本章では本 ST の完全性と一貫性を以下の正当化理由により実証する。

8.1 セキュリティ対策方針根拠

表 12は、TOE のセキュリティ対策方針の各々が、対抗する脅威または組織のセキュリティ方針の一つ以上へさかのぼれることを示す。表 13は、環境のセキュリティ対策方針の各々が、前提条件を構成する想定環境もしくは組織のセキュリティ方針の一つ以上へさかのぼれることを示す。

表 12: セキュリティ対策方針の根拠

TOEのセキュリティ対策方針	脅威と組織のセキュリティ方針の前提	根拠
O.RESIDUAL	T.RECOVER	O.RESIDUALによって、MSD内のドキュメントデータやイメージデータを上書き消去することで、脅威T.RECOVERが乗ずる機会を制限し、これに対抗するのに役立つ。データ消去機能は総べての*残存データ* に上書きし、*残存データ* を事実上読み取り不可能にする。
O.REMOVE	T.RECOVER	O.REMOVEによって、MSDに保存されるドキュメントデータやイメージデータを暗号化することで、脅威T.RECOVERに対抗する。 TOEが組込まれているMFDのMSDに当該MFD自身以外よりアクセスされても、ジョブデータの再生は実質不可能である。
O.AUTHENTICATION	T.ALTER	TOEのセキュリティ機能を利用するためには、O.AUTHENTICATIONによって、キーオペレーターコードを入力することによるキーオペレーター認証を行うことでT.ALTERに対抗する。

表 13: 環境に対するセキュリティ対策方針の根拠

環境に対するセキュリティ対策方針	想定環境もしくはセキュリティ方針の前提	根拠
OE.SECURE	A.OFFICE	A.OFFICEは、TOEが組み込まれたMFDが設置してあるオフィスに働く従業員が不在の場合、オフィスは施錠等による防犯対策が実施され、従業員不在時の入室の際は、適切な従業員であることを確認するようオフィス管理するよう求めている。OE.SECUREは、これを直接表現し、オフィスに働く従業員が不在の場合の施錠等による防犯対策実施と、従業員不在時の入室の際は適切な従業員であることを確認するようオフィスを管理するよう求めている。
OE.OPERATE	A.PROCEDURE	A.PROCEDUREは、キーオペレーターは以下の事項を遵守することを求めている。 ・ TOEがインストールされていることを確認する。 ・ 消去ふるまい設定、消去回数設定を適切に行う。 ・ キーオペレーターコード を定期的に変更する。 ・ キーオペレーターコード は容易に推測できないものを設定する。 ・ キーオペレーターコード を他者に開示しない。 OE.OPERATEは、これらを確実に実施でき、信頼できる人を指定することを求めている。

8.2 セキュリティ要件根拠

本節では TOE セキュリティ機能要件、及び TOE セキュリティ保証要件の適切性を示す。

8.2.1 TOE セキュリティ機能要件根拠

表 14 では TOE に対するセキュリティ対策方針がセキュリティ機能要件によって達成される根拠を述べる。表 15 ではセキュリティ対策方針と、セキュリティ機能要件のマッピングを示し、TOE セキュリティ機能要件の各々が、TOE に対するセキュリティ対策方針の一つ以上へさかのぼれることを示す。

セキュリティ機能要件(SFR)では、各機能要件について依存性が示されているが、本 TOE ではいくつかの依存性を必要としない。以下にその根拠を述べる。

(1) FMT_MSA.2 の依存性を必要としない根拠

依存性を必要としているセキュリティ機能要件:
FCS_CKM.1、FCS_CKM.4

依存性を必要としない根拠:
FMT_MSA.2 は安全な値のみがセキュリティ属性に使用されることを要求している。FCS_CKM.1 は TSF_FKG により、FCS_CKM.4 は TSF_FKD により充足される。TSF_FKG 及び TSF_FKD は、いずれもセキュリティ属性がない。したがって、FMT_MSA.2 への必要性はない。

(2) FIA_UID.1 の依存性を必要としない根拠

依存性を必要としているセキュリティ機能要件:
FIA_UAU.2、FMT_SMR.1

依存性を必要としない根拠:
MFD が利用者識別を必要とするのはキーオペレーターについてのみであり、認証だけで充足されるため、識別は不要となり FIA_UID.1 は必要がない。

表 16 は機能コンポーネントの、相互依存性、依存性充足度の対応表である。

表 16 において、各セキュリティ機能要件(SFR)での依存性についてその根拠を以下に述べる。

a) FCS_COP.1, FCS_CKM.1, FCS_CKM.4 の依存性
暗号鍵生成(FCS_CKM.1(1)、及び FCS_CKM.1(2))により暗号鍵を生成し、その暗号鍵を用いて暗号操作 (FCS_COP.1)が行われ、MFD の電源オフまたは停電による電源断により、その暗号鍵が破棄 (FCS_CKM.4)される。

b) FMT_MOF.1(1), FMT_MOF.1(2), FMT_SMR.1 の依存性
セキュリティ機能のふるまい管理である、電源 ON 時の自動消去実行設定、もしくは不実行設定(FMT_MOF.1(1))、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(FMT_MOF.1(2))は、キーオペレーターのみが管理行使を可能(FMT_SMR.1)とする。

c) FIA_UAU.7, FIA_UAU.2 の依存性
利用者がキーオペレータープログラムにアクセスする際、TOE は常にキーオペレーターコードの入力を要求し、その入力に対するフィードバックは常に(*)である。

8.2.2 TOE セキュリティ保証要件の適切性

TOE セキュリティ対策方針 (TSP) は、暗号化されないスプールデータがなく、消去されない処理済ジョブがなく、認証を経ないセキュリティ管理機能アクセスがなく、かつ認証データ(キーオペレーターコード)への想定しないアクセスがないことの保証を意図している。

これらの TSP の、顧客のサイトにおける実効性を保証するには、ソフトウェア(ファームウェア)品質、及び開発者サイトから顧客サイトに至るまでの改ざんによるセキュリティ欠陥への対策が必要である。

そこで、品質管理の製品ライフサイクル評価、上位レベル設計に留まらず下位レベル設計及びソースコードレベルの設計評価、開発者のみならず評価者による脆弱性分析、及び顧客のサイトに届き設置され立上がるまでの間に改ざんされない手順の評価をもって、顧客のサイトにおける TOE セキュリティ対策方針の実効性の保証となす。

そのため、この保証に必要であり、かつこの保証を満たす EAL4 を、本 ST は選択する。

本 TOE は、保証パッケージ EAL4 を利用しており、セキュリティ保証要件（SAR）に対する依存性は満足されている。表 17 に EAL4 のセキュリティ保証要件(SAR)の依存性を述べる。

表 14: セキュリティ機能要件(SFR)の対応根拠

TOEのセキュリティ対策方針	根拠
O.RESIDUAL	消去されなければならないスプールデータは、プリントジョブ、コピージョブ、イメージスキャニングジョブ、またはファクスジョブのいずれかによるので、FDP_RIP.1によって満たされる。FDP_RIP.1の管理機能（電源ON時の自動消去機能実行、もしくは不実行設定値、ジョブ終了後のデータ消去回数設定値、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設定値、及び電源ON時の自動消去におけるデータ消去回数設定値を管理する機能）は、FMT_SMF.1にて管理され、確実に上書き消去を実行することが可能となる。また、消去ふるまい設定、及び消去回数設定は、FMT_MOF.1(1)、FMT_MOF.1(2)、及びFMT_MTD.1によって満足され、その役割はFMT_SMR.1によって満足される。
O.REMOVE	FCS_CKM.1(1)、及びFCS_CKM.1(2)を満たす鍵を用いてFCS_COP.1に従い暗号化し、かつ鍵をFCS_CKM.4に従い破壊することで満たされる。
O.AUTHENTICATION	FIA_UAU.2, FMT_MTD.1, FMT_SMR.1は、いずれもセキュリティ管理機能の行使をキーオペレーターにのみ許容する方針の全部、または一部を表現している。また、FIA_UAU.7及びFIA_SOS.1は本方針に貢献する。FIA_UAU.2のキーオペレーターコード変更機能は、 FMT_SMF.1にて管理され、常に正当なキーオペレーターを認証することが可能となる。

表 15: セキュリティ対策方針に対する TOE セキュリティ機能要件(SFR)マッピング

TOEセキュリティ機能要件(SFR)	O.RESIDUAL	O.REMOVE	O.AUTHENTICAIOTN	SFRがセキュリティ対策方針にさかのぼれる根拠
FDP_RIP.1 サブセット残存情報保護	X			O.RESIDUALを直接表現している。
FIA_UAU.2 アクション前の利用者認証			X	TOEのセキュリティ管理機能を利用する前に、認証が必要であることを定めている。
FIA_UAU.7 保護された認証フィードバック			X	キーオペレーターコードの漏洩を防ぐために必要。
FIA_SOS.1 秘密の検証			X	キーオペレーターコードのSOFを維持するために必要。
FMT_MOF.1(1) セキュリティ機能のふるまいの管理(1)	X			電源ON時の自動消去の実行、もしくは不実行設定によるふるまい決定は、役割キーオペレーター以外に利用できないことを定めている。
FMT_MOF.1(2) セキュリティ機能のふるまいの管理(2)	X			キーオペレーターの操作による全データエリア消去の動作は、役割キーオペレーター以外に利用できないことを定めている。

TOEセキュリティ機能要件(SFR)	O.RESIDUAL	O.REMOVE	O.AUTHENTICAIOTN	SFRがセキュリティ対策方針にさかのぼれる根拠
FMT_MTD.1 TSFデータの管理	X		X	消去回数設定、及びキーオペレーターコード変更は、役割キーオペレーター以外に利用できないことを定めている。
FMT_SMF.1 管理機能の特定	X		X	上書き消去に関するセキュリティ管理機能（電源ON時の自動消去機能実行、もしくは不実行設定値、ジョブ終了後のデータ消去回数設定値、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設定値、及び電源ON時の自動消去におけるデータ消去回数設定値）を管理する機能を定めている。また、キーオペレーターコード変更機能を定めている。
FMT_SMR.1 セキュリティ役割	X		X	消去のふるまい管理、消去回数設定、及びキーオペレーターコード変更は、キーオペレーター役割の維持を定め、且つ利用者とキーオペレーター役割の関連づけを定めている。
FCS_CKM.1(1) 暗号鍵生成		X		外部でのジョブデータ再生防止に必要な暗号操作のために、鍵の生成を定めている。
FCS_CKM.1(2) 暗号鍵生成		X		外部でのジョブデータ再生防止に必要な暗号操作のために、鍵の生成を定めている。
FCS_CKM.4 暗号鍵破壊		X		外部でのジョブデータ再生防止のために、ジョブデータを復号できる鍵の破壊を定めている。
FCS_COP.1 暗号操作		X		外部でのジョブデータ再生防止に必要な暗号操作を定めている。

表 16: セキュリティ機能要件(SFR)の依存性状況

機能コンポーネントID	機能コンポーネント名称	満たすべき依存性	本TOEの満足している依存性	依存性を満足していない妥当性説明箇所	依存性充足度
FCS_CKM.1(1)	暗号鍵生成(1)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4	8.2.1節(1)項	--
FCS_CKM.1(2)	暗号鍵生成(2)	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4	8.2.1節(1)項	--
FCS_CKM.4	暗号鍵破壊	FCS_COP.1, FCS_CKM.1, FMT_MSA.2	FCS_COP.1, FCS_CKM.1	8.2.1節(1)項	--
FCS_COP.1	暗号操作	FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	--	満足
FDP_RIP.1	サブセット残存情報保護	なし	--	--	--
FIA_UAU.2	アクション前の利用者認証	FIA_UID.1	なし	8.2.1節(2)項	--

機能 コンポーネントID	機能コンポーネント名称	満たすべき 依存性	本TOEの満足 している依存性	依存性を満足していない妥当性説明箇所	依存性 充足度
FIA_UAU.7	保護された認証フィードバック	FIA_UAU.2	FIA_UAU.2	--	満足
FIA_SOS.1	TSF秘密生成	なし	--	--	--
FMT_MOF.1(1)	セキュリティ機能のふるまいの管理(1)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	満足
FMT_MOF.1(2)	セキュリティ機能のふるまいの管理(2)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	満足
FMT_MTD.1	TSFデータの管理	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	--	満足
FMT_SMF.1	管理機能の特定	なし	--	--	--
FMT_SMR.1	セキュリティ役割	FIA_UID.1	なし	8.2.1節(2)項	--

表 17: EAL4 セキュリティ保証要件(SAR)の依存性

保証コンポーネントID	保証コンポーネント名称	依存性	依存性 充足度
ACM_AUT.1	部分的なCM自動化	ACM_CAP.3	満足
ACM_CAP.4	生成の支援と受入手続き	ACM_SCP.1, ALC_DVS.1	満足
ACM_SCP.2	問題追跡のCM範囲	ACM_CAP.3	満足
ADO_DEL.2	改変の検出	ACM_CAP.3	満足
ADO_IGS.1	設置、生成、及び立上げ手順	AGD_ADM.1	満足
ADV_FSP.2	完全に定義された外部インタフェース	ADV_RCR.1	満足
ADV_HLD.2	セキュリティ実施上位レベル設計	ADV_FSP.1, ADV_RCR.1	満足
ADV_IMP.1	TSFの実装のサブセット	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	満足
ADV_LLD.1	記述的下位レベル設計	ADV_HLD.2, ADV_RCR.1	満足
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	満足
AGD_ADM.1	管理者ガイダンス	ADV_FSP.1	満足
AGD_USR.1	利用者ガイダンス	ADV_FSP.1	満足
ALC_DVS.1	セキュリティ手段の識別	なし	--
ALC_LCD.1	開発者によるライフサイクルモデルの定義	なし	--
ALC_TAT.1	明確に定義された開発ツール	ADV_IMP.1	満足
ATE_COV.2	カバレージの分析	ADV_FSP.1, ATE_FUN.1	満足
ATE_DPT.1	テスト:上位レベル設計	ADV_FSP.1, ATE_FUN.1	満足
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, ATE_FUN.1	満足
AVA_MSU.2	分析の確認	ADO_IGS.1, AGD_FSP.1, AGD_ADM.1, AGD_USR.1	満足
AVA_SOF.1	TOEセキュリティ機能強度評価	ADV_FSP.1, ADV_HLD.1	満足

保証コンポーネントID	保証コンポーネント名称	依存性	依存性充足度
AVA_VLA.2	独立脆弱性テスト	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	満足

8.2.3 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は、一般のオフィス環境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、MFD の操作パネルからの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、TOE 管理機能を利用できず、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、最小機能強度レベルは“SOF 基本”である。

8.3 TOE 要約仕様の根拠

本節は、TOE セキュリティ機能(TSF)と保証手段がセキュリティ機能要件(SFR)を満たすことを示す。

8.3.1 TOE 要約仕様の根拠

表 18 は、各セキュリティ機能要件(SFR)が、いずれかのセキュリティ機能によって満たされていることを示すセキュリティ機能要件(SFR)のマッピングと、その根拠である。

表 18: TOE セキュリティ機能(TSF)が全セキュリティ機能要件(SFR)を満たす根拠

セキュリティ機能要件 (SFR)	TOEセキュリティ機能(TSF)	根拠
FCS_CKM.1(1) 暗号鍵生成(1)	TSF_FKG 暗号鍵生成	暗号鍵（共通鍵）は電源投入時に自動生成する。
FCS_CKM.1(2) 暗号鍵生成(2)	TSF_FKG 暗号鍵生成	暗号鍵（共通鍵）は電源投入時に自動生成する。
FCS_CKM.4 暗号鍵破壊	TSF_FKD 暗号鍵破壊	各暗号鍵は電源断により破壊される。
FCS_COP.1 暗号操作	TSF_FDE 暗号操作	Rijndaelアルゴリズムに従い、TSF_FKGが生成した暗号鍵を用いて、暗号化及び復号を行う。
FDP_RIP.1 サブセット残存情報保護	TSF_FDC データ消去	MSDに記録されたスプールデータを上書き消去することにより、残存情報を保護する。
FIA_UAU.2 アクション前の利用者認証	TSF_AUT 認証	利用者がTOE管理機能にアクセスしようとすれば、TOEはキーオペレーターコードの入力を求め、合致を確認した後にTOE管理機能を発動する。
FIA_UAU.7 保護された認証フィードバック	TSF_AUT 認証	認証期間中は保護されたフィードバックとして、キーオペレーターコードの各桁の入力に対し、操作パネルに (*) を表示する。
FIA_SOS.1 秘密の検証	TSF_FMT セキュリティ管理	TSF_FMTによるキーオペレーターコードの変更は、新しく設定されるキーオペレーターコードの桁数が5桁であることを確認し、それ以外の桁数は受け付けない。
FMT_MOF.1 (1) セキュリティ機能のふるまいの管理(1)	TSF_AUT 認証, TSF_FMT データ消去	TSF_FMTによる電源ON時の自動消去の実行、もしくは不実行設定は、TSF_AUTにより、キーオペレーターにのみ許可される。

セキュリティ機能要件 (SFR)	TOEセキュリティ機能(TSF)	根拠
FMT_MOF.1 (2) セキュリティ機能のふるまいの管理(2)	TSF_AUT 認証, TSF_FDC データ消去	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は、TSF_AUTにより、キーオペレーターにのみ許可される。
FMT_MTD.1 TSFデータの管理	TSF_AUT 認証, TSF_FMT セキュリティ管理	TSF_FMTによる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の上書き回数設定、電源ON時の自動消去の上書き回数設定、各ジョブ完了時の自動消去における上書き回数設定は、TSF_AUTにより、キーオペレーターにのみに許可される。
FMT_SMF.1 管理機能の特定	TSF_FMT セキュリティ管理	電源ON時の自動消去機能実行、もしくは不実行設定値、ジョブ終了後のデータ消去回数設定値、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設定値、電源ON時の自動消去におけるデータ消去回数設定値を管理する機能、及びキーオペレーターコード変更を管理する機能は、TSF_FMTにより管理されている。
FMT_SMR.1 セキュリティ役割	TSF_AUT 認証, TSF_FMT セキュリティ管理, TSF_FDCデータ消去	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、TSF_FMTによる電源ON時の自動消去機能実行、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の上書き回数設定、電源ON時の自動消去の上書き回数設定、各ジョブ完了時の自動消去における上書き回数設定は、TSF_AUTによりキーオペレーターのみに維持する。

8.3.2 TOE 保証要件

本文書の 5.2 節は[CC_PART3] の付属書 B の表に示されているように、EAL4 の保証要件を満たすためにシャープ株式会社によって実行される保証手段を示している。表 19 は 5.2 節の保証手段に対する保証要件を示している。

表 19: 保証手段準拠マトリクス

保証手段	構成管理	配付と運用	開発	ガイダンス文書	ライフサイクルサポート	テスト	脆弱性評定
ACM_AUT.1	X						
ACM_CAP.4	X						
ACM_SCP.2	X						
ADO_DEL.2		X					
ADO_IGS.1		X					
ADV_FSP.2			X				
ADV_HLD.2			X				
ADV_IMP.1			X				
ADV_LLD.1			X				
ADV_RCR.1			X				
ADV_SPM.1			X				
AGD_ADM.1				X			
AGD_USR.1				X			
ALC_DVS.1					X		
ALC_LCD.1					X		
ALC_TAT.1					X		
ATE_COV.2						X	
ATE_DPT.1						X	
ATE_FUN.1						X	

保証手段	構成管理	配付と運用	開発	ガイダンス文書	ライフサイクルサポート	テスト	脆弱性評定
ATE_IND.2						X	
AVA_MSU.2							X
AVA_SOF.1							X
AVA_VLA.2							X

8.3.3 TOE セキュリティ機能強度

TOE が提供する確率的または順列的メカニズムは、キーオペレーター認証 (TSF_AUT) 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。

8.4 明示的な要件の根拠

本 ST は特記要件を含んでいない。