ZB3501040
セキュリティターゲット

Version 0.03

履歴

日付	Ver.	変更点	作成	確認	発行
2008/2/12	0.01	• 初版作成	中川	岩崎	辻井
2008/5/7	0.02	• 所見報告書 ASE001-01 による修正。	中川	岩崎	薬師寺
2008/5/27	0.03	• 所見報告書 ASE002-01 による修正。	中川	岩崎	薬師寺

目次

表のリスト

図のリスト

1 ST概説

1.1 ST識別

本書セキュリティターゲット (ST) 及び CC 評価対象 (TOE) を識別するための情報を記載する。

ST 名称: ZB3501040 セキュリティターゲット

バージョン: 0.03

発行日: 2008 年 5 月 27 日

作成者: シャープ株式会社

TOE 識別: ZB3501040 VERSION S.10

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

1.2 ST概要

本 ST は、上記 TOE すなわち ZB3501040 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) は事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能及びファクス機能を有する。TOE は IT 製品であり、Océ Imagistics Inc. が販売する MFD のデータ保護を目的とする。

TOE 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データの削除後に残存する実イメージデータを不正に取得する試みに対抗することを目的とした別売オプション品であり、MFD のファームウェアに対するアップグレードキットである。TOE の主なセキュリティ機能は以下の通りであり、本 ST はこれらについて説明する。

- イメージデータの暗号化
- イメージデータ削除時の上書き消去

1.3 CC適合

本 ST は、以下を満たしている。

a) CC v2.3 パート 2 適合。

b) CC v2.3 パート 3 適合。

c) 保証パッケージは EAL2 に ADV_SPM.1 を追加。

d) 補足-0512 を適用。

e) 適合する PP はない。

1.4 参照資料

本ST作成にあたり、表 1.1 記載の資料を参照している。本ST中の [CC_PART1], [CC_PART2] または [CC_PART3] の参照は、特に断らない限り [CC_INTPR] による修正を含むものとする。

表 1.1: 参照資料

略称	文書名
[CC_PART1]	情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル 2005年8月 バージョン2.3 CCMB-2005-08-001 (平成17年12月翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_PART2]	情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 2005年8月 バージョン2.3 CCMB-2005-08-002 (平成17年12月翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_PART3]	情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 2005年8月 バージョン2.3 CCMB-2005-08-003 (平成17年12月翻訳第1.0版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC_INTPR]	補足-0512 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

1.5 規約、専門用語、略語

本 ST 記述の規約、専門用語、及び略語を規定する。

1.5.1 規約

本節は、本 ST 記述の規約を述べる。

以下は、特別の意味を持った文章を区別するために使用される規約である。

a) *単純な斜体 (italic)* はテキストを強調するために使用される。

以下は CC 機能及び保証コンポーネントに対し、許可された操作の使用を表すために使用される規約である。

b) 割付 (assignment) 操作は、コンポーネントにおいて、例えばパスワードの長さのような不確定のパラメータに特定の値を割り付けるために使われる。パラメータに割り付ける値を、ブラケット [ ] 内に示す。必要に応じ、パラメータ名を丸括弧 ( ) に入れ、値に付記する。

c) 詳細化 (refinement) 操作は、コンポーネントに対する詳細付加のために使用され、TOE をさらに限定する。追加のテキストは **太字** で示し、削除するテキストを丸括弧 ( ) に入れる。

d) 選択 (selection) 操作は、コンポーネントにおいて与えられた複数の項目から、一つあるいはそれ以上の項目を選択するために使用される。選択された項目を、斜体のブラケット *[ ]* 内に *[下線付き斜体]* で示す。

e) 繰返し (iteration) 操作は、同一の要件の異なる側面をカバーするために使われる。コンポーネントの名称、コンポーネントのラベル、及びエレメントのラベルに対し丸括弧 ( ) 内に一連番号を後置することで、固有識別子とする。

1.5.2 専門用語

本ST固有の専門用語を表 1.2 に示す。

表 1.2: 専門用語

用語	定義
イメージデータ	本STでは特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
エンジン	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。プリントエンジン、エンジンユニットともいう。
各ジョブ完了後の自動消去	MFD内のMSDに保存された、個々のジョブに対応するイメージデータを上書き消去するための機能。ジョブ完了または中止の際に呼び出される。
揮発性メモリ	電源を切れば記憶内容が消失する記憶装置。
基板	プリント基板に部品を半田付け実装したものを指す。
コントローラ基板	MFD全体を制御する基板。TOEのファームウェアを実行するためのマイクロプロセッサ、揮発性メモリ等を有する。

用語	定義
コントローラファームウェア	MFDのコントローラ基板を制御するファームウェア。ROM基板に格納してコントローラ基板に搭載する。
ジョブ	MFDのコピー、プリンタ、イメージ送信、ファクス送受信及びPC-Faxの各機能において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
スキャナユニット	原稿をスキャンしてイメージデータを得る装置。コピー、イメージ送信及びファクス送信の際に使用する。
スプール	入出力効率のため、ジョブのイメージデータを一時的にMSDに保持すること。
全データエリア消去	MFD内のMSD上にあるすべてのイメージデータを上書き消去するための機能。管理者の操作により呼び出される。
操作パネル	MFDの正面にあるUI用ユニット。スタートキー、数字キー、機能キー及びタッチ操作式の液晶ディスプレイを含む。
タンデム印刷	大量の印刷部数を、2台のMFDで折半することにより倍速でこなす機能。
タンデムコピー	MFDのコピー機能におけるタンデム印刷のこと。
標準ファームウェア	TOE設置前のMFDに搭載されているコントローラファームウェア。TOEはコントローラファームウェアを含んでおり、TOE設置時に標準ファームウェアを取り外す。
ファームウェア	機器のハードウェアを制御するために、機器に組み込まれたソフトウェア。本STでは特に、コントローラファームウェアを指す。
不揮発性メモリ	電源を切っても記憶内容を保持することができる記憶装置。
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去及び任意部分の再書き込みを可能にしたROM (Flash Memory)。
メモリ	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。

1.5.3 略語

本STで使用する略語を表 1.3 に示す。

表 1.3: 略語

略語	定義
AES	Advanced Encryption Standard — 米国の商務省標準技術局 (NIST) が制定した米国政府標準暗号。
EEPROM	Electronically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM。
I/F	Interface (インタフェース)
MFD	Multi Function Device — デジタル複合機。事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能及びファクス機能を有する。本書では、2.2.1節で識別する対象機種を指す。
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特に、スプールに使用するMFD内のメモリ、すなわち揮発性メモリの一部及びFlashメモリを指す。
ROM	Read Only Memory — 読み出し専用メモリ。
UI	User Interface (ユーザーインタフェース)
USB	Universal Serial Bus — IT機器間を接続するシリアルバス標準の名称。

2 TOE記述

2.1 TOEの概要

2.1.1 TOE種別

TOE は IT 製品であり、ROM に格納された MFD 用ファームウェアである。MFD の標準ファームウェアを置き換えることにより、セキュリティ機能を提供すると共に MFD 全体の制御を行う。

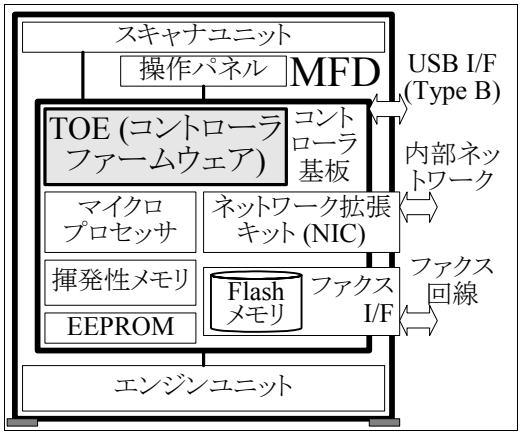

図 1: MFDの物理的構成とTOE

2.1.2 TOEセキュリティ機能の概要

TOE セキュリティ機能は、主として暗号操作機能とデータ消去機能からなり、TOE を搭載した MFD 内部に残存する実イメージデータからの情報漏洩を防止することを目的とする。

暗号操作機能は、PC-Fax、ファクス送信、ファクス受信の各ジョブにおいて、ファクス送受信する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、イメージ送信、PC-Fax、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

TOEが動作するMFDはOcé Imagistics Inc. が販売するim3512, im3512J, im4512 及びim4512Jである。図 1 にMFDの物理的構成を示し、TOEを網掛けで示す。TOEの物理的範囲は以下の通り。

- コントローラファームウェア: MFD の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。TOE外のハードウェアを、角を丸くした長方形で示す。TOEの機能を長方形で示し、その中のセキュリティ機能を網掛けで示す。図中、データの流れを矢印で示す。TOEの機能間で受け渡されるデータは、一時的に揮発性メモリを経由するが、セキュリティ機能上の意味を持つ場合を除いて省略している。

TOE は MFD 用のファームウェアであり、セキュリティ機能を提供すると共に、MFD 全体の制御を行う。以下の機能が TOE の論理的範囲に含まれる。

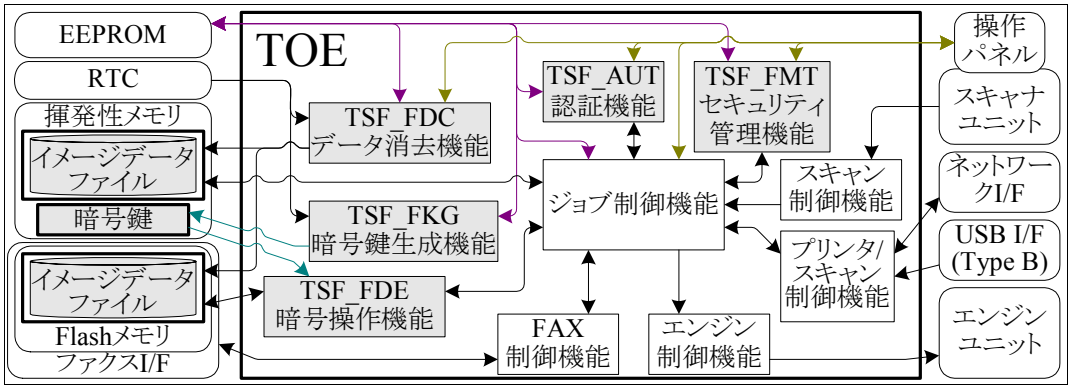

図 2: TOEの論理的構成図

a) 暗号操作機能 (TSF_FDE): PC-Fax、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): 暗号操作機能で使用する暗号鍵を生成する。生成された暗号鍵は、揮発性メモリに保存する。暗号鍵のシード (seed) は TOE の設置時に一度生成され、その後は、MFD の電源がオンになると、このシードを元に常に同じ暗号鍵を生成する。

c) データ消去機能 (TSF_FDC): MSDからの情報漏えいを防ぐため, MSDに対し上書き消去する。各ジョブ完了後の自動消去 (Auto Clear at Job End), 及び、全データエリア消去 (Clear All Memory) を行う。各ジョブ完了後の自動消去は、ジョブ制御機能により、ジョブ処理終了及び中止の際に呼び出される。

d) 認証機能 (TSF_AUT): 管理者パスワードにより管理者の識別認証を行う。

e) セキュリティ管理機能 (TSF_FMT): 管理者として認証された場合において、管理者パスワードの変更 (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、イメージ送信ジョブ、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、USB I/F またはネットワーク 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。
- イメージ送信ジョブにおいては、スキャンされた実イメージデータを、指定された形式に変換後にネットワーク I/F を介して、ネットワークに送出する。

i) FAX 制御機能: PC-Fax ジョブ、ファクス送信ジョブにおいてファクス回線への送出、またファクス受信ジョブにおいてファクス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、イメージ送信ジョブ、PC-Fax 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、イメージ送信、PC-Fax、ファクス送信、ファクス受信の各動作を制御する。

2.3 MFD機能及びその利用方法

標準ファームウェアと同様に、TOEはMFD機能、すなわちコピー、プリンタ、イメージ送信、ファクス送信、ファクス受信及びPC-Faxの各機能を持つ。TOEはそれら各MFD機能の実行中にTOEセキュリティ機能 (TSF) の一部を自動的に実行する。TOEのこの性質は、TSFを知らない、または意識しない利用者をも保護する。TOEを設置するMFDの利用環境を図 3 に示す。

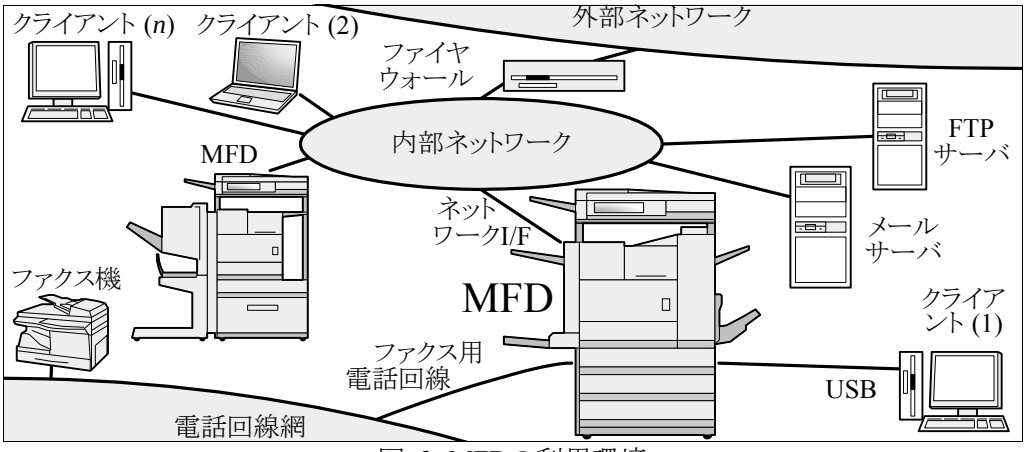

図 3: MFDの利用環境

以下、TOE が持つ MFD 機能について説明する。多くの機能は MFD の操作パネルでの操作によって発動する。一部の機能はデータ受信により発動する。さらに一部の機能は TOE の Web, すなわち TOE が内蔵するリモート操作用の Web の操作によって発動する。

以下に述べる各機能はイメージデータを MFD のスキャナユニットまたは外部から受け取り、MFD 内の MSD にスプールし、イメージデータを MFD のエンジンユニット (印刷) または外部 (送信) へ送る。

a) コピー: 操作パネルでの操作により、原稿を読み取り、その画像を印刷する。タンデムコピーが指示された場合、管理者が予め指定した MFD にイメージデータを送る。

b) プリンタ: 外部より受信したデータを印刷する。

- プリンタドライバ: クライアントで印刷データを生成し、ネットワークまたは USB 経由で MFD に送る。タンデム印刷が指示された場合、2 台の MFD にイメージデータを送る。
- プッシュプリント: クライアントより印刷データを E-mail または Web 経由で MFD に送る。MFD からのタンデム印刷要求も同様。
- プルプリント: 操作パネルの操作で FTP サーバ内の印刷データを取得する。

c) イメージ送信: 操作パネルでの操作により原稿を読み取り、原稿のイメージデータを以下の手段により送信する。

- E-mail: E-mail 添付ファイルとして送る。
- ファイルサーバ: FTP サーバに送る。
- デスクトップ: クライアント (MFD 同梱ソフトウェア要) 宛に FTP で送る。
- 共有フォルダ: Windows 共有フォルダに送る。

d) ファクス送信: 操作パネルでの操作により原稿を読み取り、原稿のイメージデータをファクス送信する。

e) ファクス受信: 他機から送られたファクスを受信し印刷する。

f) PC-Fax: クライアントからのデータをファクス送信する。PCFAX とも呼ぶ。

2.4 TOEの保護資産

本節では、TOE セキュリティ機能が保護対象とする資産について述べる。

2.4.1 保護資産の概要

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、イメージ送信、PC-Fax、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。

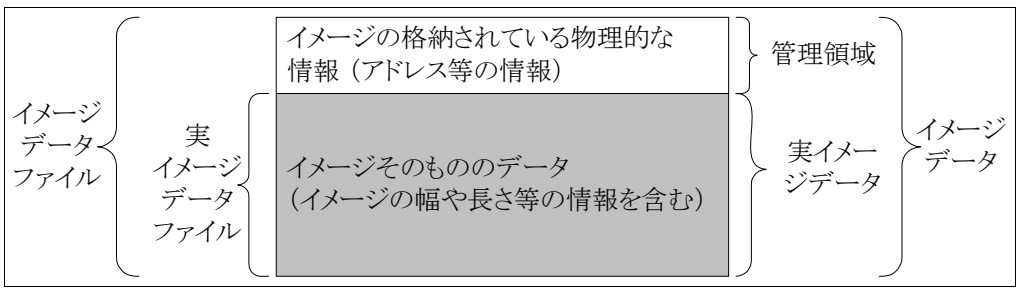

図 4: 実イメージデータ説明

MFD は資源の割当て解除のために、処理終了または中止により用済みになったファイルを削除する際に、管理領域に削除情報を与えることによって、データ (実イメージデータ) 保持のために使用していた

領域を、未使用状態にする。この点、一般のパーソナルコンピュータに接続されたハードディスク上のデータファイルを削除する場合と同様である。すなわち、未使用状態とされた領域が他のファイルの領域として再利用されるまでの間、削除された実イメージデータは残存し得る。そこで本 ST は、MFD 内の揮発性メモリ、もしくは Flash メモリに残存する実イメージデータを保護資産とする。TOE は、低レベルの攻撃者により、TOE の保護資産である残存する実イメージデータからの情報漏えいを防止することを目的とする。

以下、各保護資産の具体的な内容を述べる。

2.4.2 Flashメモリに残存する実イメージデータ

PC-Fax、ファクス送信、ファクス受信の各ジョブにおいて、ファクス送受信する実イメージデータをスプール保存するために Flash メモリが使用される。ファクス送受信処理終了後または中止後の実イメージデータは不揮発性の Flash メモリに残存するため、攻撃者が読み出し漏えいさせた場合、機密情報の漏えいとなり得る。また、組織のセキュリティ方針として、暗号化するか否か、読み出しの脅威があるか否かに関わらず、実イメージデータの上書き消去を必須とする。従って、本 ST はこれを保護資産とする。

2.4.3 揮発性メモリに残存する実イメージデータ

同様に、コピー、プリント、イメージ送信の各ジョブの実イメージデータをスプール保存するために揮発性メモリが使用される。これらのジョブ終了後または中止後に実イメージデータが揮発性メモリ内に残存しても、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。ただし、上記のような組織のセキュリティ方針のため、本 ST は揮発性メモリに残存する実イメージデータもまた保護資産とする。

2.5 TOEの関係者

本節では、本 TOE、及び、本 TOE を設置する MFD の関係者について述べる。

- 所有者: TOE 及び MFD を占有し、管理下におく組織。
- 組織の責任者: 所有者に属し、MFD の管理責任を負う人物。
- 管理者: TOE 及び MFD の運用管理を任された人物。組織の責任者が任命する。

3 TOEセキュリティ環境

3.1 前提条件

TOEの使用、運用時に、表 3.1 で詳述する環境が必要となる。

表 3.1: 前提条件

識別子	定義
A.OPERATOR	管理者は、TOEに対して不正をせず信頼できるものとする。

3.2 脅威

TOEに対する脅威を表 3.2 に示す。

表 3.2: 脅威

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

3.3 組織のセキュリティ方針

組織のセキュリティ方針を表 3.3 に示す。

表 3.3: 組織のセキュリティ方針

識別子	定義
P.RESIDUAL	コピー、プリント、イメージ送信、PC-Fax、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、管理者により、MSDのスプール領域全体は上書き消去されなければならない。

4 セキュリティ対策方針

4.1 TOEのセキュリティ対策方針

TOEのセキュリティ対策方針を表 4.1 に示す。

表 4.1: TOE のセキュリティ対策方針

識別子	定義
O.REMOVE	TOEが組み込まれているMFDのFlashメモリに対し、スプール保存を実行したMFD自身以外から読み取られても、イメージとして表示不能なように、MFD固有の暗号鍵で実イメージデータを暗号化してから、Flashメモリにスプール保存する。
O.RESIDUAL	TOEは、コピー、プリント、イメージ送信、PC-Fax、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、管理者の指示により、MSDの全イメージデータ領域に対し、上書き消去を実施する。

4.2 環境のセキュリティ対策方針

環境のセキュリティ対策方針を表 4.2 に示す。

表 4.2: 環境のセキュリティ対策方針

識別子	定義
OE.ERASEALL	管理者は、MFDの廃棄、または所有者変更の際、MSDのスプール領域全体の上書き消去を実施する。
OE.OPERATE	TOEを搭載したMFDを所有する組織の責任者が、管理者の役割を理解した上で、管理者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

本節ではTOEが満たすべきセキュリティ機能要件を [CC_PART2] のクラス別に記述する。最小機能強度は、5.1.2節で規定する。

5.1.1.1 クラスFCS: 暗号サポート

●FCS_CKM.1　暗号鍵生成

下位階層:　なし

FCS_CKM.1.1　TSF は、以下の[データセキュリティキット用暗号基準書]に合致する、指定された暗号鍵生成アルゴリズム[MSN-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_CKM.2 暗号鍵配付 または FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

●FCS_COP.1　暗号操作

下位階層:　なし

FCS_COP.1.1　TSF は、[FIPS PUB 197]に合致する、特定された暗号アルゴリズム[AES Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[

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

]を実行しなければならない。

依存性:　[FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または FDP_ITC.2 セキュリティ属性付き利用者データのインポート
または FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

5.1.1.2 クラスFDP: 利用者データ保護

●FDP_RIP.1　サブセット残存情報保護

下位階層:　なし

FDP_RIP.1.1　TSF は、以下のオブジェクト*[* からの資源の割当て解除 *]* において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [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

●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、[管理者認証操作における最後の認証成功以降の不成功認証試行]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、[

- 不成功認証が 3 回に達したとき: 5 分間の認証試行受付を停止
- 停止より 5 分経過: 認証失敗回数をクリアし自動的に復帰

]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

●FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[5 文字の数字]に合致することを検証するメカニズムを提供しなければならない。

依存性: なし

●FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

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

依存性: FIA_UID.1 識別のタイミング

●FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1 TSF は、認証を行っている間、[入力された文字の個数]だけを利用者に提供しなければならない。

依存性: FIA_UAU.1 認証のタイミング

●FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

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

依存性: なし

5.1.1.4 クラスFMT: セキュリティ管理

●FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1 TSF は、機能[全データエリア消去] *[* を動作させる, を停止する *]* 能力を[管理者]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

●FMT_MSA.2 セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1 TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性: ADV_SPM.1 非形式的 TOE セキュリティモデル
[FDP_ACC.1 サブセットアクセス制御 または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

●FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[管理者パスワード]を*[* 改変, 問い合わせ *]*する能力を[管理者]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

●FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[
管理者パスワードの改変]。

注: 管理要件への考慮は8.2.2節で述べる。

依存性: なし。

●FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[管理者]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

5.1.1.5 クラスFPT: TSFの保護

●FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

5.1.2 TOE最小機能強度

本 TOE の全体のセキュリティ最小機能強度は SOF-基本 である。

また、本 TOE が満足する機能要件のうち、確率的または順列的メカニズムを利用するのは FIA_UAU.2, FIA_UAU.7, FIA_SOS.1 及び 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。

5.1.3 TOEセキュリティ保証要件

本STが選択した保証レベルについての保証コンポーネントを表 5.1 に示す。表 5.1 は、EAL2 + ADV_SPM.1 を主張するために満たすべき保証要件である。

表 5.1: 保証要件

コンポーネント	コンポーネント名称	依存性
ACM_CAP.2	構成要素	なし
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.1	記述的上位レベル設計	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
ATE_COV.1	カバレージの証拠	ADV_FSP.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_SOF.1	TOEセキュリティ機能強度評価	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	開発者脆弱性分析	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.2 IT環境に対するセキュリティ要件

環境のセキュリティ対策方針が TOE の IT 環境に要求するセキュリティ要件はない。

6 TOE要約仕様

本章は、セキュリティ要件に対する TOE のセキュリティ機能と保証手段を述べる。

6.1 TOEセキュリティ機能 (TSF)

TOEセキュリティ機能要件とTOEセキュリティ機能の関連性を表 6.1 に示す。表中に、各々の対応関係を記載している節番号を示す。

表 6.1: セキュリティ機能要件と TOE セキュリティ仕様

機能 機能要件	TSF_FKG	TSF_FDE	TSF_FDC	TSF_AUT	TSF_FMT
FCS_CKM.1	6.1.1				
FCS_COP.1		6.1.2			
FDP_RIP.1			6.1.3		
FIA_AFL.1			6.1.3	6.1.4	
FIA_SOS.1					6.1.5
FIA_UAU.2			6.1.3	6.1.4	
FIA_UAU.7			6.1.3	6.1.4	
FIA_UID.2			6.1.3	6.1.4	
FMT_MOF.1			6.1.3	6.1.4	
FMT_MSA.2	6.1.1				
FMT_MTD.1				6.1.4	6.1.5
FMT_SMF.1					6.1.5
FMT_SMR.1				6.1.4	6.1.5
FPT_RVM.1	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5

6.1.1 暗号鍵生成 (TSF_FKG)

TOE は、暗号鍵 (共通鍵) の生成を行い、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。

TOE は、セキュアなシードを元に、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し、暗号アルゴリズム AES Rijndael で使用するために、揮発性メモリ内に保存する。MSN-J 拡張アルゴリズムは、データセキュリティキット用暗号基準書を満たす暗号鍵生成アルゴリズムである。

暗号鍵のセキュリティ属性であるシードは、TOEセキュリティ方針 (TSP) モデルに従うセキュアな方法で TOEにより生成される。TOEセキュリティ保証要件ADV_SPM.1 の保証手段 (表 6.2) が、TSPモデルを規定している。TOEはこのTSPモデルに従い、設置の際、MFD 1 台ごとに異なるシードを生成する。これにより、各MFD内のTOEは常に同じシードから同じアルゴリズムで暗号鍵を生成する。

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。

暗号化及び復号には FIPS PUBS 197 に基づく AES Rijndael アルゴリズムと、暗号鍵生成 (TSF_FKG) により生成された 128 ビット長の暗号鍵を用いる。

6.1.3 データ消去 (TSF_FDC)

本 TSF はスプール保存されたイメージデータを消去する。以下の各機能は本 TSF に含まれる。

- 各ジョブ完了後の自動消去 (Auto Clear at Job End)
- 全データエリア消去 (Clear All Memory)

各機能とも揮発性メモリにはランダム値を 1 回以上上書きする。また, Flash メモリには固定値を 1 回上書きする。揮発性メモリ上書き回数は本 TSF の設定に従う。

以下、各機能及びその設定について記述する。

6.1.3.1 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、イメージ送信ジョブ完了後、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。

PC-Fax 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。

6.1.3.2 全データエリア消去

本機能は、TSF_AUT で識別認証された管理者により操作パネルにて起動され、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し、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。

途中で中止する場合、キャンセル操作を選択後、管理者パスワードの入力による管理者の識別認証を必ず要求する。管理者パスワード入力中、TOE は入力した文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。正しい入力が完了した場合のみ、上書き消去を中止する。

連続して 3 回認証に失敗した場合、認証受付を停止する。認証受付停止からの経過時間が 5 分に達すれば、自動的に認証受付停止を解除、すなわち、認証失敗回数をクリアして通常状態に復帰する。

6.1.4 認証 (TSF_AUT)

本 TSF は、管理者パスワードにより管理者の識別認証を行う。

TOE は、管理機能の起動操作によって管理者を識別し、かつ、正しい管理者パスワードによって管理者認証に成功した場合に限り、管理者向け機能へのインタフェースを提供する。これにより管理者を特定し、管理者の役割を利用者に関連付ける。管理者パスワード入力時、入力した文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。

連続して 3 回認証に失敗した場合、認証受付を停止する。認証受付停止からの経過時間が 5 分に達すれば、自動的に認証受付停止を解除、すなわち、認証失敗回数をクリアして通常状態に復帰する。

データ消去 (TSF_FDC) のうち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) の管理者パスワードの問い合わせと改変は、操作を許可する前に必ず管理者として認証 (TSF_AUT) されなければならない。

6.1.5 セキュリティ管理 (TSF_FMT)

管理者パスワードは、本 TSF により管理されている。本 TSF の使用を許可する前に必ず認証 (TSF_AUT) による管理者識別認証を行い、成功した場合に限り本 TSF の使用を許可する。このため、認証 (TSF_AUT) と同じく、管理者を特定し、利用者と役割を関連付けている。また、管理者パスワードを改変 (変更) 後も、管理者として役割が維持される。

本 TSF は管理者パスワード変更機能を提供する。これにより管理者パスワードの改変 (変更) が可能で、新しい管理者パスワードが 5 文字の数字であることを必ず検査する。設定値は MFD 内の EEPROM に保存する。

6.2 TSFセキュリティ機能強度

確率的または順列的メカニズムに基づく TSF は以下の通り。

- 認証 (TSF_AUT): 管理者パスワード認証入力が FIA_AFL.1, FIA_UAU.2 及び FIA_UAU.7 に対応する。

- データ消去 (TSF_FDC): 同上。
- セキュリティ管理 (TSF_FMT): 管理者パスワード変更が FIA_SOS.1 に対応する。

これらのセキュリティ機能強度は、いずれも SOF-基本 である。

6.3 保証手段

本STにおけるセキュリティ保証要件の各コンポーネントに対する保証手段となるドキュメントを表 6.2 に示す。

表 6.2: 保証手段

コンポーネント	保証手段
ACM_CAP.2	ZB3501040 構成管理説明書 ZB3501040 VERSION S.10 構成リスト
ADO_DEL.1	ZB3501040 配付手順説明書
ADO_IGS.1	ZB3501040 Installation Manual
ADV_FSP.1	ZB3501040 セキュリティ機能仕様書
ADV_HLD.1	ZB3501040 上位レベル設計書
ADV_RCR.1	ZB3501040 表現対応分析書
ADV_SPM.1	ZB3501040 セキュリティ方針モデル仕様書
AGD_ADM.1 AGD_USR.1	Operation Manual Data Security Kit ZB3501040 Administrator Settings Guide
ATE_COV.1	ZB3501040 カバレージマップ
ATE_FUN.1	ZB3501040 機能テスト仕様書 ZB3501040 テスト環境・ツール説明書
ATE_IND.2	TOE
AVA_SOF.1	ZB3501040 セキュリティ機能強度分析書
AVA_VLA.1	ZB3501040 脆弱性分析書

7 PP主張

本 TOE が適合する PP はない。

8 根拠

本章は、本 ST の完全性と一貫性を検証する。

8.1 セキュリティ対策方針根拠

TOEセキュリティ環境に示した前提条件、脅威、組織のセキュリティ方針に対して、セキュリティ対策方針で示した対策が有効であることを表 8.1 に検証する。表 8.1 は、前提条件、脅威、組織のセキュリティ方針の対応について、その根拠を記載している節番号を示したものである。

表 8.1: セキュリティ対策方針根拠

TOEセキュリティ環境 セキュリティ対策方針	A.OPERATOR	T.RECOVER	P.RESIDUAL
O.REMOVE		8.1.2	
O.RESIDUAL			8.1.3
OE.ERASEALL			8.1.3
OE.OPERATE	8.1.1		

8.1.1 A.OPERATOR

A.OPERATOR は、管理者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、管理者の役割を理解した上で、管理者の人選は厳重に行うことにより実施できる。

8.1.2 T.RECOVER

T.RECOVER に対して、本 TOE の保護資産のうち Flash メモリ内に保存されている実イメージデータについては、低レベルの攻撃者が実イメージデータを読み出すことができたとしても、O.REMOVE にて、実イメージデータを人間にとって意味のあるものとして判読できないように、MFD 固有の暗号鍵で実イメージデータを暗号化後にスプール保存することで対抗する。

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。

8.1.3 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 により管理者が、O.RESIDUAL にて MSD のスプール領域全体の上書き消去を行うことにより実施できる。

8.2 セキュリティ要件根拠

セキュリティ対策方針に対して、IT セキュリティ要件が有効であることを検証する。

8.2.1 セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応について表 8.2 に示す。表 8.2 は、セキュリティ機能要件とセキュリティ対策方針の対応について、その根拠を記載している節番号を示したものである。

表 8.2: TOEセキュリティ機能要件根拠

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

8.2.1.1 O.REMOVE

O.REMOVE の目的は T.RECOVER への対抗であり、すなわち MFD 内の Flash メモリに対し、Flash メモリにスプール保存を実行した MFD 自身以外からアクセスされても、実イメージデータからのイメージ表示を阻止することである。これは、以下の機能要件の組み合わせにより実現できる。

- FCS_COP.1 により、スプール保存される実イメージデータが暗号化されるため、Flash メモリにスプール保存を実行した MFD 自身以外からアクセスされても、イメージ表示は阻止される。
- FCS_CKM.1 により、FCS_COP.1 を実施するための暗号鍵を生成する。
- 暗号鍵のシードは、TOE 自身が生成したものであり、FMT_MSA.2 によりセキュアなセキュリティ属性として受け入れられる。
- FPT_RVM.1 により、O.REMOVE を実現する各機能要件を迂回できないようにサポートする。

上記 FCS_CKM.1 と FMT_MSA.2 は、FCS_COP.1 の依存性の要件なので競合は発生しない。
FPT_RVM.1 は相互サポートのための要件であるので競合は発生しない。以上から、O.REMOVE を達成する上で機能要件の競合は発生しない。

8.2.1.2 O.RESIDUAL

O.RESIDUAL は、以下の機能要件の組み合わせにより実現できる。

a) FDP_RIP.1 により、各ジョブ完了後の自動消去、及び、全データエリア消去の実行時に、スプール保存されている実イメージデータが格納された領域の上書き消去を行うことで、利用者データ保護が可能となる。

b) FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 及び FIA_UID.2 にて管理者を識別認証する。

c) 以下の各機能要件により、管理者の役割が実現される。

- FMT_SMR.1 (1) にて、管理者の役割は維持され、管理者はその役割に関連づけられる。
- 管理者パスワードの問合せと変更 (改変) が、FMT_MTD.1 により管理者のみ可能となる。
- 管理者パスワードを変更 (改変) する場合、FIA_SOS.1 により、入力された管理者パスワードが 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管理者パスワードが設定される。
- FMT_SMF.1 により、FIA_UAU.2 の管理者パスワードを管理することにより、確実に管理者を識別認証することが可能となる。

d) FMT_MOF.1 及び上のc) により、FDP_RIP.1 の管理 (全データエリア消去機能の起動と中止) を行う能力は、管理者に制限される。

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

上記b) 及びc) の各機能要件は相互にサポートし合う関係にあり、それらの間に競合はない。d) はa) の管理であり、また、b) 及びc) によりサポートされるので、それらの間に競合はない。e) は相互サポートのための機能要件であるので競合は発生しない。以上から、O.RESIDUALを実現する上で、機能要件の競合は発生しない。

8.2.2 TOEセキュリティ管理機能の一貫性根拠

TOE セキュリティ機能要件のいくつかは、セキュリティ管理機能を必要とする。[CC_PART2] は各機能コンポーネントに予見される管理アクティビティ (management activities foreseen) を、各コンポーネントの管理要件 (management requirements) として提案している。

表 8.3 は、すべてのTOEセキュリティ機能要件コンポーネントについて、そのコンポーネントが必要とする管理機能を、管理要件への考慮とともに示す。FMT_SMF.1 が特定する管理機能と、表中で示された必要な管理機能とは、一致している。

よって、TOE セキュリティ要件は、セキュリティ管理機能に関し、内部的に一貫している。

表 8.3: TOEの管理機能

管理機能 被管理要件	必要な管理機能	管理要件への考慮
FCS_CKM.1	—	鍵の属性は変更しない
FCS_COP.1	—	(管理要件なし)
FDP_RIP.1	—	残存情報保護の実施タイミングは、割当て解除時に固定
FIA_AFL.1	—	閾値とアクションは固定
FIA_SOS.1	—	品質尺度は固定
FIA_UAU.2	管理者パスワードの改変	管理要件に合致
FIA_UAU.7	—	(管理要件なし)
FIA_UID.2	—	管理者の識別は固定
FMT_MOF.1	—	役割のグループなし
FMT_MSA.2	—	(管理要件なし)
FMT_MTD.1	—	役割のグループなし
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1	—	利用者のグループなし
FPT_RVM.1	—	(管理要件なし)

8.2.3 セキュリティ機能要件の依存性根拠

セキュリティ機能要件の依存性について表 8.4 に示す。表 8.4 は、CCが規定するセキュリティ機能要件が満足すべき依存性と、本TOEが満足している依存性、満足していない依存性、及び本TOEが依存性を満足していないことの正当性を記載している節番号を示したものである。表中で * を付された依存性は、それの上位階層関係にあるコンポーネントにより満足されている。

表 8.4: セキュリティ機能要件の依存性

依存性 機能要件	満足すべき	満足している	不満足	正当性
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FMT_MSA.2	FCS_CKM.4	8.2.3.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FMT_MSA.2	FCS_CKM.4	同上
FDP_RIP.1	—	—	—	—
FIA_AFL.1	FIA_UAU.1 *	FIA_UAU.2	—	—
FIA_SOS.1	—	—	—	—
FIA_UAU.2	FIA_UID.1 *	FIA_UID.2	—	—
FIA_UAU.7	FIA_UAU.1 *	FIA_UAU.2	—	—
FIA_UID.2	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	ADV_SPM.1	FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	8.2.3.2
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1 *	FIA_UID.2	—	—
FPT_RVM.1	—	—	—	—

8.2.3.1 FCS_CKM.4 不満足の正当性

暗号鍵は揮発性メモリ内に保存している。電源断 (電源オフ) により、揮発性メモリ内の電荷が消失し、暗号鍵が破棄される。そのため、標準の方法を用いて暗号鍵を破棄する必要性がなく、標準を特定するFCS_CKM.4 は必要がない。

8.2.3.2 FMT_MSA.2 の依存性不満足の正当性

暗号操作に関するセキュリティ属性である暗号鍵のシードは、TOE 自身が管理しており、管理者に対しても変更を許容していないため、FMT_MSA.1 及び FMT_SMR.1 は必要がない。同様に、暗号鍵やシードを利用者及び管理者からアクセスされることがなく、外部から受け入れることもないので、FDP_ACC.1 及び FDP_IFC.1 はいずれも必要がない。

8.2.4 セキュリティ要件の相互作用

セキュリティ要件の相互作用の関係について表 8.5 に示す。

8.2.4.1 迂回

表 8.5 に関し、以下に、各機能要件に対する迂回について述べる。

a) 暗号鍵生成 FCS_CKM.1 は、電源 ON 時に必ず呼び出され迂回できない。

b) 暗号操作 FCS_COP.1 は、実イメージデータを Flash メモリにスプール保存する前に必ず暗号化し、読み出し後に復号され、いずれも迂回できない。

c) サブセット残存情報保護 FDP_RIP.1 は、各ジョブの完了または中止時、及び、管理者の全データエリア消去操作時に必ず呼び出されるため迂回できない。

d) 管理者の識別認証に関する FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 及び FIA_UID.2 は、管理者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、管理者パスワードの変更 (改変) 時に必ず呼び出されるため迂回できない。

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

g) TSF データの管理 FMT_MTD.1 は、必ず管理者認証 FIA_UAU.2 を経ることを必要とし、迂回できない。

表 8.5: セキュリティ要件の相互作用

防御 機能要件	迂回	非活性化
FCS_CKM.1	FPT_RVM.1	—
FCS_COP.1	FPT_RVM.1	—
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1	FPT_RVM.1	—
FIA_SOS.1	FPT_RVM.1	—
FIA_UAU.2	FPT_RVM.1	—
FIA_UAU.7	FPT_RVM.1	—
FIA_UID.2	FPT_RVM.1	—
FMT_MOF.1	FPT_RVM.1	—
FMT_MSA.2	—	—
FMT_MTD.1	FPT_RVM.1	—
FMT_SMF.1	—	—
FMT_SMR.1	—	—
FPT_RVM.1	—	—

8.2.4.2 非活性化

表 8.5 に関し、FDP_RIP.1 は、FMT_MOF.1 により管理者のみに制限されるため非活性化行為から保護される。

8.2.4.3 干渉

本 TOE は、管理者のみにセキュリティ機能のふるまい管理を許可しているだけである。このため、不正なサブジェクトが存在せずアクセス制御の必要はなく、TSF が破壊されることはない。

8.2.5 最小機能強度根拠

本 TOE は、一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃である。このため、攻撃者の攻撃力は “低レベル” である。本 TOE の最小機能強度レベルは SOF-基本 であり、これにより低レベルの攻撃能力を持つ攻撃者からの公開情報を利用した不正行為に対抗できる。FIA_AFL.1, FIA_SOS.1, FIA_UAU.2 及び FIA_UAU.7 の明示された機能強度はそれぞれ SOF-基本 であり、最小機能強度と矛盾しない。

8.2.6 TOEセキュリティ保証要件根拠

本TOEは、MFD用の別売オプション品、すなわち商用の製品である。また、脅威は、低レベルの攻撃者が、MFD内のMSDに、MFD以外の装置を使用する物理的手段によりMSD内の情報を読み出し漏えいさせることである。このため本TOEは、通常のオフィスで使用される商用の製品として、脅威からの保護に

関する信頼性の確保について有意な保証を与えるEAL2 + ADV_SPM.1 を評価保証レベルとする。ADV_SPM.1 については、機能要件FMT_MSA.2 において、ADV_SPM.1 への依存性が示されているための選択である。表 5.1 に示す通り、すべての依存性は満足されている。

ADV_SPM.1 を除く保証要件は EAL2 のパッケージを適用しているので、各要件が相互に競合することはない。ADV_SPM.1 は TSP モデルという個別仕様の保証要件なので、他の要件との競合は発生しない。

8.3 TOE要約仕様根拠

本節は、IT セキュリティ要件に対する、TOE セキュリティ機能とその保証手段の有効性を検証する。

8.3.1 TOEセキュリティ機能根拠

表 6.1 に示したセキュリティ機能要件とTOEセキュリティ機能の対応について、下記に根拠を示す。

8.3.1.1 FCS_CKM.1

TSF_FKG は、MFD の電源投入時に MSN-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。MSN-J拡張アルゴリズムは、開発者 (本ST作成者) のデータセキュリティキット用暗号基準書に基づくアルゴリズムである。よって FCS_CKM.1 は満足される。

8.3.1.2 FCS_COP.1

FCS_COP.1 は、TSF_FDE による FIPS PUB 197 で規格化された AES Rijndael アルゴリズムに従い MSD に保存する利用者データ及び TSF データの暗号化、及び復号を行うため、満足される。

8.3.1.3 FDP_RIP.1

TSF_FDC が以下の通り残存情報を上書き消去することにより、FDP_RIP.1 は満足される。

- 各ジョブ完了後の自動消去により、揮発性メモリ (コピー、プリント及びイメージ送信ジョブで使用) あるいは Flash メモリ (ファクス送信、ファクス受信及び PC-Fax ジョブで使用) に保存された実イメージデータファイルに対し上書き消去する。
- 全データエリア消去により、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。

8.3.1.4 FIA_AFL.1

TSF_AUT 及び TSF_FDC は管理者認証を行う。これらは FIA_AFL.1 が定める認証失敗対応を備えている。よって FIA_AFL.1 は満足される。

8.3.1.5 FIA_SOS.1

TSF_FMT による管理者パスワードの変更時、入力された新しい管理者パスワードが 5 文字の数字であることを検査し、それ以外は受け付けない。これにより FIA_SOS.1 は満足される。

8.3.1.6 FIA_UAU.2

TSF_AUT は管理者向け機能の操作に先立ち、管理者パスワード入力による認証を行う。TSF_FDC は、実行中の全データリア消去を中止する際、管理者パスワード入力による認証を行う。これらにより FIA_UAU.2 は満足される。

8.3.1.7 FIA_UAU.7

TSF_AUT は、管理者認証中における保護されたフィードバックとして、入力文字数に応じた代替文字のみを表示する。TSF_FDC による消去中止時の管理者認証も同様である。これらにより FIA_UAU.7 は満足される。

8.3.1.8 FIA_UID.2

TSF_AUT は管理者向け機能の操作に先立ち、管理者の識別操作を必要とする。TSF_FDC による全データリア消去のキャンセル操作は、管理者識別に相当する。これらにより FIA_UID.2 は満足される。

8.3.1.9 FMT_MOF.1

TSF_FDC による全データエリア消去の起動は、TSF_AUT による管理者認証後に可能となる。TSF_FDC による全データエリア消去の中止は、TSF_FDC による管理者認証後に可能となる。これらにより FMT_MOF.1 は満足される。

8.3.1.10 FMT_MSA.2

FMT_MSA.2 は、ADV_SPM.1 に、必ずセキュアなシードを元に暗号鍵が生成されることが説明されており、暗号鍵生成 TSF_FKG により FMT_MSA.2 が満足される。

8.3.1.11 FMT_MTD.1

FMT_MTD.1 は、TSF_AUT により識別認証された管理者が、TSF_FMT による管理者パスワ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_SMF.1

TSF_FMT は管理者パスワードの改変を行う能力を持っている。よって FMT_SMF.1 は満足される。

8.3.1.13 FMT_SMR.1

TSF_AUT は管理者の識別認証により、管理者を特定することで、役割への関連づけを行っている。また、TSF_FMT によって管理者パスワードを変更 (改変) しても役割への関連づけ、及び役割を維持し続ける。これらにより FMT_SMR.1 は満足される。

8.3.1.14 FPT_RVM.1

8.2.4.1節で述べたFPT_RVM.1 によるサポートが、各TSFにより実施されていることを以下に示す。

a) TSF_FKG は、MFD 電源 ON 時に必ず FCS_CKM.1 が定める通り暗号鍵を生成する。

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

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

d) TSF_AUT 及び TSF_FDC は、管理者識別認証の際、FIA_UID.2 に基づく管理者識別操作、FIA_UAU.2 に基づく管理者パスワード認証、FIA_UAU.7 に基づく管理者パスワードのフィードバック保護、及び、FIA_AFL.1 に基づく管理者パスワード認証受付停止を必ず実行する。

e) TSF_FMT は、管理者パスワードの変更時に必ず FIA_SOS.1 が定める通り管理者パスワードが 5 文字の数字であることを検証する。

f) TSF_FDC は FMT_MOF.1 に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、全データエリア消去を起動するインタフェースを提供し、TSF_FDC による管理者認証が呼び出され成功した場合に限り、全データエリア消去の中止を許可する。

g) TSF_FMT は FMT_MTD.1 に則り、TSF_AUT による管理者認証が呼び出され成功した場合に限り、管理者パスワード変更のインタフェースを提供する。

8.3.2 TOEセキュリティ機能強度根拠

確率的または順列的メカニズムによって実現されるTSFは、6.2節で述べた通り、認証 (TSF_AUT), データ消去 (TSF_FDC) 及びセキュリティ管理 (TSF_FMT) である。それらはいずれもセキュリティ機能強度 SOF-基本 を持つ。

よって、TSFのセキュリティ機能強度の最小値はSOF-基本 であり、5.1.2節で述べたTOE最小機能強度と一貫している。

8.3.3 TOE保証手段根拠

6.3節の保証手段は、以下に示す各保証手段の内容より、TOEセキュリティ保証要件を満足する。

a) ACM_CAP.2

保証手段: ZB3501040 構成管理説明書
ZB3501040 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。

b) ADO_DEL.1

保証手段: ZB3501040 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: ZB3501040 Installation Manual

内容: TOE の設置手段、手続きについて規定している。

d) ADV_FSP.1

保証手段: ZB3501040 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.1

保証手段: ZB3501040 上位レベル設計書

内容: TOE のサブシステム設計における TSF の構造を明確化し、TOE セキュリティ機能要件を漏れなく正確に具体化していることを確認できるよう記述している。

f) ADV_RCR.1

保証手段: ZB3501040 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: ZB3501040 セキュリティ方針モデル仕様書

内容: 機能仕様、セキュリティ方針モデルと TSP の方針の間に対応を規定し、またセキュアな値だけがセキュリティ属性として受け入れられることの保証を提供している。

h) AGD_ADM.1

保証手段: Operation Manual Data Security Kit ZB3501040
Administrator Settings Guide

内容: TOE の管理者に対し、TOE を正しい方法で保守し管理することを目的として書かれた資料 (取扱説明書) である。

i) AGD_USR.1

保証手段: (AGD_ADM.1 に同じ)

内容: TOE 利用者に対し、TOE をセキュアに使用してもらうことを目的とした資料 (取扱説明書) である。

j) ATE_COV.1

保証手段: ZB3501040 カバレージマップ

内容: 機能テストとセキュリティ機能仕様との対応関係を記述している。

k) ATE_FUN.1

保証手段: ZB3501040 機能テスト仕様書
ZB3501040 テスト環境・ツール説明書

内容: すべてのセキュリティ機能の実行が、仕様通りであることを実証するテストについて記述したものである。

l) ATE_IND.2

保証手段: TOE

内容: テストに適した TOE。

m) AVA_SOF.1

保証手段: ZB3501040 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。

n) AVA_VLA.1

保証手段: ZB3501040 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。