SHARP

MX-FRX8

セキュリティターゲット

Version 0.07

シャープ株式会社

履歴

日付	Ver.	変更点	作成	確認	発行
2007/10/31	0.01	• 初版作成	中川	岩崎	辻井
2007/2/15	0.02	• 一貫性エラーを修正: 1.3, 1.4, 3.1, 3.2, 3.3, 4.1, 4.3, 6.2, 6.4, 7.3, 7.6, 8.2節	中川	岩崎	辻井
2008/3/13	0.03	• 一貫性エラーを修正: 1.3, 3.1, 4.1, 4.2, 4.3, 6.4節 • 誤記訂正: 6.2, 7.1節	中川	岩崎	辻井
2008/3/24	0.04	• 一貫性エラーを修正: 1.3, 6.4節	中川	岩崎	辻井
2008/4/25	0.05	• 一貫性エラーを修正: 1.4, 6.2, 6.4, 7.3, 7.5, 7.6, 8.2節	中川	岩崎	薬師寺
2008/5/14	0.06	• 全体的な見直し	中川	岩崎	薬師寺
2008/6/30	0.07	• 一貫性エラーおよび誤記訂正: 4.2, 4.3, 6.4, 8.1節	中川	岩崎	薬師寺

目次

表のリスト

図のリスト

1 ST 概説

本章では、2.1 節に示すコモンクライテリア (CC) に基づき、本セキュリティターゲット (ST) および本 ST への適合を主張する CC 評価対象 (TOE) に関し、ST 参照、TOE 参照、TOE 概要、および TOE 記述を記載する。なお、本 ST では、8.1 節および 8.2 節に示す用語を使用している。

1.1 ST 参照

本セキュリティターゲット (ST) を識別するための情報を記載する。

ST 名称: MX-FRX8 セキュリティターゲット

バージョン: 0.07

発行日: 2008 年 6 月 30 日

作成者: シャープ株式会社

1.2 TOE 参照

本 ST への適合を主張する CC 評価対象 (TOE) を識別するための情報を記載する。

TOE 識別: MX-FRX8 Version M.10

開発者: シャープ株式会社

1.3 TOE 概要

1.3.1 TOE タイプ

TOE は MFD (デジタル複合機) 内データ保護機能を持つ IT 製品であり、その主要部分は、ROM に格納された MFD 用ファームウェア製品である。MFD 内蔵ハードウェア部品である HDC が TOE に含まれ、ファームウェア部分から呼び出される。

MFD (Multi Function Device) すなわちデジタル複合機は事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。MFD 内の標準ファームウェア ROM を外し、本製品と交換して使用する。

1.3.2 要求される TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE の動作には、シャープ製 MFD の一部機種が必要である。対象の機種は MX-M850, MX-M860, MX-M950 および MX-M1100 である。

MFD の通信に使用する Web ブラウザ、プリンタドライバおよび PC-Fax ドライバに必要な能力を以下に挙げる。上記 MFD 機種には、以下の能力を持つプリンタドライバおよび PC-Fax ドライバが付属している。

- パスワード入力の際、認証フィードバック保護を行うこと。すなわち、入力されたパスワードを表示せず、入力された文字の個数以外の情報は与えないこと。
- 次節で述べる SSL 機能を利用する場合、SSL プロトコル (SSL 3.0 または TLS 1.0 以降) に対応すること。

本 ST が識別する TOE セキュリティ機能は、マイクロソフト社の Web ブラウザ “Internet Explorer 6.0 SP2” における動作が確認されている。その他、広く普及している Web ブラウザは一般に上記の能力を持つが、使用にあたっては確認されたい。

1.3.3 主要なセキュリティ機能

TOE はイメージデータ等の利用者データ (1.4.4 節で詳述) を保護する目的で、以下の各機能を提供する。これらは、MFD 内の不揮発性記憶装置 (HDD 等) に保存あるいは残存する利用者データを不正に取得する試みに対抗することを目的とする。また、当該利用者データを MFD がネットワーク (LAN) 経由で入出力する際、盗聴の試みに対抗することを目的とする。

a) 暗号操作機能: MFD がジョブ処理中のイメージデータを HDD 等に一時的に書き込む際、また、利用者が文書のイメージデータを HDD にファイリング保存する際、書き込み前にデータを暗号化する。

b) データ消去機能: HDD 等のイメージデータが用済みになった際、自動的に上書き消去する。MFD 廃棄時もしくは運用中、必要に応じ、管理者の操作により全データを上書き消去する。

c) 親展ファイル機能: 利用者がイメージデータをファイリングする際、パスワードによる保護を提供する。

d) IP/MAC アドレスフィルタ機能: ネットワーク経由の不正アクセスを拒む。

e) SSL 機能: 通信データを盗聴から守る。

1.3.4 TOE の使用方法

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、スキャナ、ファクス送信、ファクス受信および PC-Fax の各機能を持つ。MFD 機能については後述するものとし、本節では前節のセキュリティ機能を呼び出す方法の概略を記す。

a) 利用者がコピー等の MFD 機能を利用することにより、TOE の暗号操作機能およびデータ消去機能が自動的に動作する。MFD はコピー等のジョブ処理中のイメージデータを MFD 内の MSD (HDD または Flash メモリ) に一時的にスプール保存し、読み出しながらジョブを処理し、ジョブ完了時に削除する。TOE は暗号操作機能により、スプール保存されるイメージデータを暗号化し、読み出し時に復号する。TOE はデータ消去機能により、削除されるイメージデータを上書き消去する。

b) 利用者は TOE の親展ファイル機能を利用することにより、イメージデータを MFD 内の HDD に “親展ファイル” (パスワード付きファイル) として保存し、後で再利用 (印刷、ファクス送信、PC へ画像ファイル送信、等) でき、パスワードにより他人の再利用を防ぐことができる。

- 利用者はコピー等のジョブを MFD に投入する際、保存することを指示し、パスワードを指定する。これにより、ジョブのイメージデータはジョブ完了後もパスワードとともに HDD に保存される。
- 利用者は MFD に原稿をセットし、MFD の操作パネルで “スキャン保存” の操作を行い、パスワードを指定する。これにより、TOE は MFD のスキャナユニットで原稿を読み取りイメージデータを得て、パスワードとともに HDD に保存する。
- 利用者は MFD の操作パネルから、または、ネットワーク接続されたクライアント PC から、保存されている親展ファイルを一つ選択し、パスワードを入力し、再操作 (印刷、送信、削除、等) を指定する。TOE は、入力されたパスワードを検査し、一致すれば指定された再操作を実行する。TOE は、誤ったパスワードが 3 回連続で入力されたファイルについて、再操作を禁止する。

c) 利用者が TOE の親展ファイル機能を利用して親展ファイルを保存する際、また、再操作する際、TOE の暗号操作機能が自動的に動作する。TOE は暗号操作機能により、HDD に保存されるイメージデータおよびパスワードを暗号化する。また、再操作のため入力されたパスワードを検査する際、HDD からパスワードを読み出し復号する。入力されたパスワードが正しく、印刷または送信を実行する際、イメージデータを読み出し復号する。

d) 利用者が TOE の親展ファイル機能を利用して親展ファイルを削除する際、TOE のデータ消去機能が自動的に動作する。

e) 利用者がクライアント PC にてネットワークを介して MFD と通信する際、TOE の SSL 機能を使用することができる。クライアント PC よりプリンタジョブを送る際、IPP-SSL プロトコルを使用し、印刷すべきイメージデータを通信中の盗聴から保護する。また、MFD (TOE) がリモート操作用に提供する Web ページに対し利用者がアクセスし、親展ファイル再操作等を行う際、SSL (HTTPS) プロトコルを使用し、パスワード等を通信中の盗聴から保護する。

f) 管理者が必要 (MFD 廃棄時等) に応じ、MFD の操作パネルより、全データエリア消去の操作を行う。このとき TOE はデータ消去機能により、MFD 内のイメージデータをすべて上書き消去する。

g) 管理者が TOE の Web より、フィルタ設定を行う。MFD との通信を許可または拒否する IP アドレス範囲を設定でき、また、MFD との通信を許可する MAC アドレスを設定できる。フィルタ設定がなされていれば、TOE は、許可する IP アドレス以外からの通信、拒否する IP アドレスからの通信、および、許可する MAC アドレス以外からの通信に応答しない。

1.3.5 MFD 機能の使用方法

TOE を設置する MFD の利用環境を図 1 に示す。

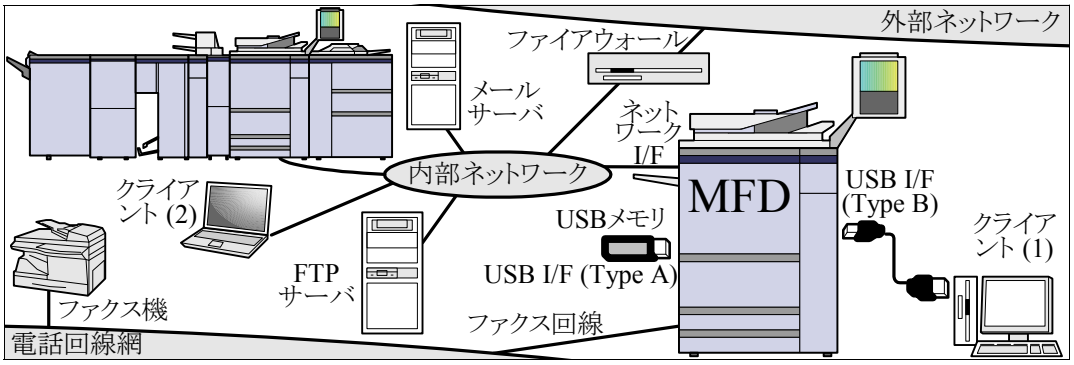

図 1: MFDの利用環境

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。

1.3.5.1 ジョブ機能

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。ジョブ制御機能および MFD 制御機能により実現される。

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, FTP 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 サーバまたは USB メモリ内の印刷データを取得する。

c) スキャナ: 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。
- USB メモリ: MFD に取り付けた USB メモリに書き込む。
- リモート PC: クライアント (MFD 同梱ソフトウェア要) 宛に TWAIN で送る。
- インターネット Fax: インターネット Fax 標準仕様に従い E-mail 添付ファイルとして送る。

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またはインターネット Fax 送信する。

1.3.5.2 ドキュメントファイリング機能

以下のとおり、MFD 内の HDD にイメージデータを保存し、そのイメージデータを操作パネル経由またはクライアントより Web 経由で再操作できる機能を提供する。ジョブ制御機能により実現される。

- ジョブの保存: 利用者は MFD にコピー等のジョブを与える際、そのジョブのイメージデータを保存するよう指定することができる。このときパスワードを指定すれば親展ファイルとなる。
- スキャン保存: 原稿を読み取って保存のみ行い、印刷や送信は行わない。
- 再操作: 保存されたイメージデータを呼び出し、以下の操作を行う。
  - 印刷: 保存されたイメージデータを用紙に印刷する。タンデム印刷を指示された際は、管理者が予め指定した MFD にイメージデータを送る。
  - 送信: スキャナ機能における各送信手段のいずれか、または、ファクスにて送信する。
  - プレビュー: イメージデータの概略を表示する。
  - 属性変更: 親展ファイルパスワードの有無を変更する。
  - パスワード変更: 親展ファイルパスワードを変更する。
  - 削除: 不要になったイメージデータを取り除き、上書き消去する。
  - バックアップ (エクスポート): 後ほどリストア (インポート) 可能なバイナリデータとしてクライアントに転送する。

プリンタドライバのジョブは、印刷せず保存のみ行うよう指定することもできる。スキャン保存は、送信せず保存のみ行うスキャナジョブと考えてよい。

1.3.5.3 アドレス帳機能

送信先のファクス番号や E-mail アドレスを登録し、送信する際の操作を簡略化する。データは HDD に保存され、操作パネルまたは Web での操作により登録、変更または削除できる。ジョブ制御機能により実現される。

1.3.6 TOE の運用方法

TOE は、セキュアな運用を維持するための機能として、以下の管理機能を有する。TOE は、管理者のみが、以下の管理機能によって運用可能である。

- 認証に関する設定:
  - 管理者パスワードの変更 (改変)
- ネットワークアクセス制限の設定:
  - IPアドレスフィルタ設定
  - MACアドレスフィルタ設定
- セキュリティに関する各種設定:
  - SSL設定
  - 各ジョブ完了後の自動消去回数
  - データエリア消去回数
  - 電源ON時の自動消去の対象別有効設定
  - 電源ON時の自動消去回数
  - ドキュメントファイリング禁止設定
  - ホールド以外のプリントジョブ禁止設定
  - 親展ファイルのロック解除
- データ消去機能の起動:
  - 全データエリア消去
  - アドレス帳/本体内登録データ消去
  - ドキュメントファイリングデータ消去
  - ジョブ状況完了エリア消去
- データ消去機能の中止:
  - 全データエリア消去の中止
  - ドキュメントファイリングデータ消去の中止
  - 電源ON時の自動消去の中止

1.4 TOE 記述

1.4.1 TOE の物理的構成

TOE の主要部分は 2 枚の ROM 基板により提供される。また、実装上の都合上、セキュリティ機能の一部を HDC 内に実装しており、これも TOE の範囲に含む。これを図 2 に網掛けで示す。

TOE の物理的範囲は、以下のとおりである。

- コントローラファームウェア: コントローラ基板に搭載する 2 枚の ROM 基板に格納されており、コントローラ基板を制御するファームウェアである。MFD の別売オプション品として提供される。
- HDC: コントローラ基板に実装されている 1 個の集積回路部品である。コントローラファームウェアの制御下で動作する。

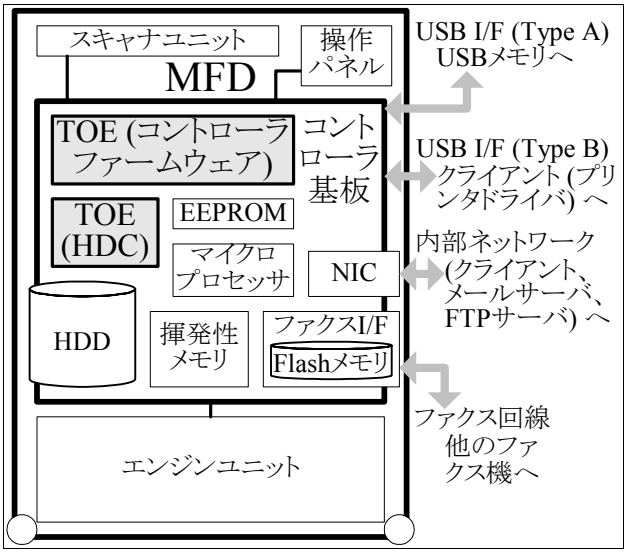

図 2: MFDの物理的構成とTOE

上記のコントローラファームウェアは、シャープ製 MFD のセキュリティを強化するための製品 “データセキュリティキット MX-FRX8” (DSK) により提供される。DSK はシャープ製 MFD 用別売オプション品であり、MFD 内に取り付けることによって機能する。MFD 製造時に標準ファームウェアおよび HDC が MFD に組み込まれるが、標準ファームウェアは HDC 内のセキュリティ機能を呼び出さないので、HDC は単に HDD のインタフェースとして機能する。MFD から標準ファームウェアを取り外し、代わりに DSK ファームウェアを取り付けることにより、HDC 内のセキュリティ機能が呼び出されるようになる。

1.4.2 TOE の論理的構成

TOE の論理的構成を図 3 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。また、揮発性メモリ, HDD, Flash メモリおよび EEPROM 上にあるデータのうち、セキュリティ機能が扱うデータ (利用者データおよび TSF データ) を、同じく網掛けで示す。

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。

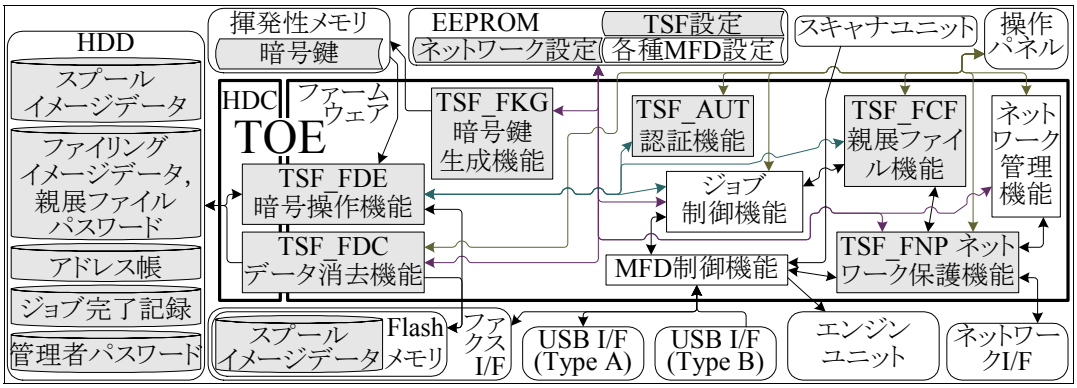

図 3: TOEの論理的構成図

TOE の主要部分は、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。また、TOE セキュリティ機能 (TSF) の一部は HDC 内に実装され、ファームウェア内の TSF から呼び出される。

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): MSD に書き込む利用者データおよび TSF データを暗号化する。また、MSD から読み出した利用者データおよび TSF データを復号する。ジョブ制御機能 (各種ジョブ、ア

ドレス帳機能、およびドキュメントファイリング機能) により呼び出される。本機能の一部は HDC 内にあり、ファームウェア部分から呼び出される。

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。本機能の一部は HDC 内にあり、ファームウェア部分から呼び出される。データ消去の各プログラム (各ジョブ完了後の自動消去、全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去) ならびに、その設定機能 (データ消去設定) からなる。各ジョブ完了後の自動消去は、ジョブ制御機能 (各種ジョブおよびドキュメントファイリング機能) により呼び出される。

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。管理者パスワードを変更する管理機能を持つ。

e) 親展ファイル機能 (TSF_FCF): 利用者がドキュメントファイリング機能 (1.3.5.2 節) により MFD 内にイメージデータを保存する際、パスワードによる保護を提供する。再操作 (印刷や送信) の際に親展ファイルパスワードを要求し認証を行う。連続 3 回認証失敗した親展ファイルをロックする。ロックは管理者のみが解除できる。

f) ネットワーク保護機能 (TSF_FNP): 以下の 3 要素からなる。

- フィルタ機能: IP アドレスまたは MAC アドレスにより通信相手を制限する。
- 通信データ保護機能: SSL により通信データを保護する。ただし、SSL に対応できないクライアントやプロトコルを使用する場合は、本機能を使用することができない。
- ネットワーク設定保護: ネットワーク管理機能 (本節内で後述) を管理者のみに提供し、他の利用者には使用させない。

g) ジョブ制御機能: MFD の各種機能、すなわち各種ジョブ、アドレス帳機能およびドキュメントファイリング機能において、UI を提供し、動作を制御する。ジョブをキュー管理し、ジョブ完了記録を HDD 内に保持する。

h) MFD 制御機能: 各種 MFD ハードウェアを制御する。また、通信を伴うジョブにおいて、送受信するデータと MFD 内のイメージデータとの間でデータ形式を変換する。

i) ネットワーク管理機能: ネットワーク機能を使用するために、MFD に付与する IP アドレス、TOE が参照すべき DNS サーバの IP アドレス、ポート設定 (各ネットワークサービスのポート番号および無効化), その他のネットワーク設定を行う管理者機能である。ネットワーク保護機能 (TSF_FNP) により呼び出される。

1.4.3 ガイダンス

表 1.1 のガイダンスが、TOE の一部として、ファームウェアに同梱して提供される。文書およびバージョンを特定する一意識別子をブラケット [ ] と共に付す。

表 1.1: ガイダンス

仕向地 目的	日本	日本以外
準備手続き	MX-FRX8 設置手順書 [TCADZ1969FCZZ]	MX-FRX8 Installation Manual [TCADZ1970FCZZ]
利用者操作	取扱説明書データセキュリティキット MX-FRX8 [CINSJ4234FC51]	MX-FRX8 Data Security Kit Operation Manual [CINSE4235FC51]
	注意書データセキュリティキット MX-FRX8 [TCADZ1967FCZZ]	MX-FRX8 Data Security Kit Notice [TCADZ1968FCZZ]

1.4.4 TOE の保護資産

本 TOE が対象とする保護資産は、以下の利用者データである。

- MFD 機能がジョブ処理時にスプール保存するイメージデータ
- 利用者が親展ファイルとしてファイリング保存したイメージデータ
- アドレス帳データ
- ジョブ完了記録データ
- ネットワーク設定データ
- ネットワーク上の通信データ

上記各項の具体的内容を、以下の各節で記述する。

1.4.4.1 MFD 機能がジョブ処理時にスプール保存するイメージデータ

利用者が TOE の MFD 機能を使用した場合、利用者が意図することなく TOE 自身が本章で述べた各種ジョブ処理のために MFD 内の HDD または Flash メモリに一時的にスプール保存したイメージデータを、本 ST は保護資産とする。これは各利用者の機密情報、すなわち利用者自身が所有する情報や、利用者が顧客から預かっている情報を含み得る。

これはジョブ完了または中止の際に削除されるが、この削除は論理的な削除であり、物理的には削除後もイメージデータ領域そのものは HDD または Flash メモリ上に残存しているため、このデータも保護資産に含まれる。

1.4.4.2 利用者が親展ファイルとしてファイリング保存したイメージデータ

利用者がドキュメントファイリング機能により HDD 内に親展ファイルとしてファイリング保存したイメージデータを、本 ST は保護資産とする。これも前項と同様、各利用者の機密情報を含み得る。

これは利用者が削除できるが、この削除は論理的な削除であり、物理的には削除後もイメージデータ領域そのものは HDD 上に残存しているため、このデータも保護資産に含まれる。

1.4.4.3 アドレス帳データ

利用者がアドレス帳機能によって登録し HDD 内に保存されるアドレス帳データを、本 ST は保護資産とする。これは正当な利用者たちが共同で扱う個人情報 (宛先の名前、メールアドレス、ファクス番号等) であり、組織の機密情報を含み得る。

正当な利用者以外にとって、操作パネルの前に立って一件ずつ目視と手操作でアクセスする以外にアドレス帳データを読み出しまたは改変する手段がなければ、必ずしも対抗すべき脅威があるとはいえない。しかし、HDD から直接に、または Web インタフェースを利用して内部ネットワーク経由で、正当な利用者以外がアドレス帳データをまとめて読み出しまたは改変する可能性からは、保護されねばならない。

1.4.4.4 ジョブ完了記録データ

ジョブ制御機能が HDD 内に保存するジョブ完了記録データを、本 ST は保護資産とする。これはプリンタドライバからのジョブの利用者名や文書名、ファクス送受信の相手先等、組織の機密情報を含み得る。

正当な利用者以外にとって、操作パネルの前に立って一件ずつ目視と手操作でアクセスする以外にジョブ完了記録データを読み出す手段がなければ、必ずしも対抗すべき脅威があるとはいえない。しかし、HDD から直接に正当な利用者以外がジョブ完了記録データをまとめて読み出す可能性からは、保護されねばならない。

1.4.4.5 ネットワーク設定データ

管理者がネットワーク管理機能によって EEPROM 内に登録した、以下のネットワーク設定データを、本 ST は保護資産とする。これは組織の機密情報であり、内部ネットワークの脅威につながり得る。また、不正に改ざんされれば、他の保護資産の脅威につながり得る。

- TCP/IP 設定: TCP/IP 有効設定, DHCP 有効設定, IP アドレス設定
- DNS 設定: プライマリ/セカンダリ DNS サーバ, ドメイン名
- WINS 設定: WINS 有効設定, プライマリ/セカンダリ WINS サーバ, WINS スコープ ID

- SMTP 設定: SMTP サーバ
- LDAP 設定: LDAP 有効設定, LDAP サーバ
- タンデム設定: 子機 IP アドレス, タンデム送信禁止
- ポート設定: 各ネットワークサービスの有効設定およびポート番号

1.4.4.6 ネットワーク上の通信データ

上記の各保護資産を MFD がネットワーク経由で入出力する際の通信データについて、盗聴の脅威を考慮し、本 ST はこれを保護資産とする。

2 適合主張

本 ST は以下を満たしている。

2.1 CC 適合主張

本 ST および TOE が適合を主張する CC のバージョンは次のとおり。

- パート 1: 概説と一般モデル
  2006 年 9 月 バージョン 3.1 改訂第 1 版 翻訳第 1.2 版
- パート 2: セキュリティ機能コンポーネント
  2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版
- パート 3: セキュリティ保証コンポーネント
  2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版

CC パート 2 に対する本 ST の適合は、CC パート 2 適合である。

CC パート 3 に対する本 ST の適合は、CC パート 3 適合である。

2.2 PP 主張

本 ST は PP 適合を主張しない。

2.3 パッケージ主張

本 ST は、EAL3 適合である。

3 セキュリティ課題定義

本章は、TOE のセキュリティ課題を定義する。

3.1 脅威

TOE に対する脅威を表 3.1 に示す。攻撃者としては、特に断りのない限り、以下の人物を想定する。

- MFD の正規の利用者、または、第三者。
- 他人の文書のイメージデータ等、保護資産 (1.4.4 節) のいずれかを不正に入手する動機を持つ。
- MFD および TOE について、取扱説明書を含む公開情報に基づく知識を有する。

表 3.1: 脅威

識別子	定義
T.RECOVER	攻撃者がMSDをMFDから物理的に取り出し、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内の利用者データ (削除後に残存しているデータを含む) を読み出し漏えいさせる。
T.REMOTE	MFDへのアクセスを認められていない攻撃者が、内部ネットワーク経由でMFD内のアドレス帳データを、まとめて読み出しまたは改変する。
T.SPOOF	攻撃者が、他の利用者になりすますことにより、操作パネルまたは内部ネットワーク経由で、利用者が親展ファイルとしてファイリング保存したイメージデータを、読み出し漏えいさせる。
T.TAMPER	攻撃者が、管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを、読み出しまたは改変する。
T.TAP	正当な利用者がMFDに対して通信する際、攻撃者が内部ネットワーク上を流れる利用者データを盗聴する。

3.2 組織のセキュリティ方針

本 ST が想定する組織のセキュリティ方針はない。

表 3.2: 組織のセキュリティ方針

(なし)

3.3 前提条件

TOE の使用、運用時に、表 3.3 で詳述する環境が必要となる。

表 3.3: 前提条件

識別子	定義
A.NETWORK	MFDは、外部ネットワークからの攻撃から保護された内部ネットワークにおける、MFDとの通信を認める機器だけが接続されたサブネットワークに接続するものとする。
A.OPERATOR	管理者は、MFDおよびTOEに対して不正をせず信頼できるものとする。

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 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.FILTER	TOEは、MFDへのアクセスを認められていない機器からの、ネットワーク経由アクセスを拒否する手段を提供する。
O.MANAGE	TOEのセキュアな運用を維持するためのセキュリティ管理者機能を、管理者のみに提供する。
O.REMOVE	TOEは、利用者データをMSDに書き込む際、MFD固有の鍵により暗号化する。
O.RESIDUAL	TOEは、MSD内の利用者データが不要になり次第、その領域を上書き消去する。
O.TRP	TOEは、内部ネットワーク上を流れる利用者データを盗聴より保護する機能を提供する。
O.USER	TOEは、正当な親展ファイル保存者を識別認証する機能を提供する。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を表 4.2 に示す。

表 4.2: 運用環境のセキュリティ対策方針

識別子	定義
OE.CIPHER	管理者は、MFDの利用者がTOEと通信する際、TOEが設置される内部ネットワーク環境下において通信データを盗聴より保護するための必要な措置 (以下に例示する) を実施する。 ● TOEのSSL機能を使う。すなわち、本STの1.3.2節に従いSSLプロトコルに対応したソフトウェアを使わせ、かつO.TRPが定める機能が働くようTOEを設定する。 ● 暗号化機能を持った通信機器 (ルータやスイッチ等) を使う。 ● ネットワークに物理的保護 (入室規制等) を施す。 ● データの受け渡しにUSBメモリ等の手段を使う。
OE.FIREWALL	管理者は、TOEが設置される内部ネットワークと外部ネットワークの接続を、外部ネットワークからの攻撃から内部ネットワークを保護する機能を持った通信機器を用いることにより実施する。
OE.NOECHO	管理者は、MFDの利用者がTOEと通信する際、本STの1.3.2節に従い、認証フィードバック保護を行うソフトウェアを使用させる。
OE.OPERATE	組織の責任者は、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。
OE.PC-USER	管理者は、内部ネットワーク上でMFDへの接続を認める機器において、MFDの正当な利用者のみが利用できるよう、許可利用者を識別認証する機能 (OSのログイン機能等) を動作させる。
OE.SUBNET	管理者は、TOEが設置されるサブネットワークに、MFDとの通信を認める機器のみを接続し、その状態を維持管理する。
OE.USER	管理者は、TOEおよびMFDの利用者に対して、親展ファイルパスワードが漏れないよう安全に管理させるものとする。

4.3 セキュリティ対策方針根拠

本 ST が定義するセキュリティ課題の各々に対して、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 4.3 に検証する。表 4.3 は、セキュリティ課題とセキュリティ対策方針との各々が対応していることについて、その根拠を記載している節番号を示したものである。

表 4.3: セキュリティ対策方針根拠

セキュリティ課題 / セキュリティ対策方針	T.RECOVER	T.REMOTE	T.SPOOF	T.TAMPER	T.TAP	A.NETWORK	A.OPERATOR
O.FILTER		4.3.1.2					
O.MANAGE	4.3.1.1	4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5		
O.REMOVE	4.3.1.1						
O.RESIDUAL	4.3.1.1						
O.TRP					4.3.1.5		
O.USER			4.3.1.3				
OE.CIPHER					4.3.1.5		
OE.NOECHO	4.3.1.1	4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5		
OE.FIREWALL						4.3.3.1	
OE.OPERATE							4.3.3.2
OE.PC-USER		4.3.1.2					
OE.SUBNET						4.3.3.1	
OE.USER			4.3.1.3				

4.3.1 脅威に対抗している根拠

以下、セキュリティ対策方針が達成された場合にすべての脅威に対抗できる根拠を示す。

4.3.1.1 T.RECOVER

T.RECOVER に対して、以下のように対抗する。

- O.RESIDUAL が定めるとおり、TOE は、MSD 内の利用者データが不要になり次第、その領域を上書き消去する。これにより、MSD 内の利用者データが読み出されることを防ぐ。
- O.REMOVE が定めるとおり、TOE は、利用者データを MSD に書き込む際、MFD 固有の鍵により暗号化する。これにより、低レベルの攻撃者が、MSD 上に保存されている、または、削除後に残存している情報を読み出すことができたとしても、意味のあるものとして判読できない。
- 前各項のサポートとして、O.MANAGE が定めるとおり、TOE のセキュアな運用のため管理者のみがセキュリティ機能の管理を行えるようにする。さらにそのサポートとして、OE.NOECHO により管理者認証入力中の覗き見を防ぐ。

なお、MFD のメモリ (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はできない。

よって、上記の各対策により HDD および Flash メモリ内の情報漏えいが防止できる。

4.3.1.2 T.REMOTE

T.REMOTE に対して、以下のように対抗する。

- O.FILTER が定めるとおり、TOE は、MFD へのアクセスを認められていない機器からのネットワーク経由アクセスを拒否する手段を提供する。これにより、内部ネットワークに接続された不正な機器から MFD へのアクセスを拒否しつつ、MFD の正当な利用者 (管理者を含む) が利用することを意図して内部ネットワークに接続された機器 (クライアント PC やサーバ PC 等) から MFD へのアクセスを維持することが可能となる。
- 前項のサポートとして、O.MANAGE が定めるとおり、TOE のセキュアな運用のため管理者のみがセキュリティ機能の管理を行えるようにする。さらにそのサポートとして、OE.NOECHO により管理者認証入力中の覗き見を防ぐ。
- MFD の正当な利用者 (管理者を含む) が利用することを意図して内部ネットワークに接続された機器 (クライアント PC やサーバ PC 等) は MFD へのアクセスを認められるべきであり、O.FILTER による拒否の対象とならない。MFD への接続を認める機器については、OE.PC-USER が定めるとおり、識別認証機能 (OS のログイン機能等) を動作させ、許可利用者のみが利用できる状態で運用すべきである。これにより、MFD への接続を認める機器 (MFD の正当な利用者のための機器) を攻撃者が悪用して (MFD の正当な利用者になりすまして) MFD 内のアドレス帳データにアクセスすることを防ぐ。

すなわち O.FILTER および OE.PC-USER が相互補完し、O.MANAGE および OE.NOECHO が O.FILTER をサポートする。これらの対策により、MFD へのアクセスを認められていない攻撃者が、内部ネットワーク経由で MFD にアクセスすることを防ぎ、MFD 内のアドレス帳データを保護することができる。

4.3.1.3 T.SPOOF

T.SPOOF に対して、以下のように対抗する。

- O.USER が定めるとおり、TOE は、正当な親展ファイル保存者を識別認証する機能を提供する。
- 前項のサポートとして、O.MANAGE が定めるとおり、TOE のセキュアな運用のため管理者のみがセキュリティ機能の管理を行えるようにする。さらにそのサポートとして、OE.NOECHO により管理者認証入力中の覗き見を防ぐ。
- 正当な親展ファイル保存者の識別認証に必要な親展ファイルパスワードは、漏れないよう安全に管理されなければならない。これは OE.USER が定めるとおり、管理者が TOE および MFD の利用者に行わせる。また、OE.NOECHO により親展ファイルパスワード認証入力中の覗き見を防ぐ。

これらの対策により、攻撃者が、正当な利用者になりすますことにより生ずる脅威に対抗できる。

4.3.1.4 T.TAMPER

T.TAMPER に対して、O.MANAGE が定めるとおり、TOE は管理者機能を管理者のみに提供する。また、OE.NOECHO により管理者認証入力中の覗き見を防ぐ。これらにより、攻撃者が管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを読み出しまたは改変することを防止できる。

4.3.1.5 T.TAP

T.TAP に対して、以下のように対抗する。

- O.TRP が定めるとおり、TOE は、内部ネットワーク上を流れる利用者データを盗聴より保護する機能を提供する。
- 前項のサポートとして、O.MANAGE が定めるとおり、TOE のセキュアな運用のため管理者のみがセキュリティ機能の管理を行えるようにする。さらにそのサポートとして、OE.NOECHO により管理者認証入力中の覗き見を防ぐ。
- OE.CIPHER が定めるとおり、管理者は、MFD の利用者が TOE と通信する際、TOE が設置される内部ネットワーク環境下において通信データを盗聴より保護するための必要な措置 (TOE の SSL 機能またはその他の保護手段) を実施する。

これらの対策により、正当な利用者が MFD に対して通信する際、攻撃者が内部ネットワーク上を流れる利用者データを盗聴することを防止できる。

4.3.2 組織のセキュリティ方針実施の根拠

本 TOE に関する組織のセキュリティ対策方針を本 ST は想定していない。よって、実施されなければならない組織のセキュリティ対策方針はない。

4.3.3 前提条件充足の根拠

以下、セキュリティ対策方針が達成された場合に前提条件をすべて満たす根拠を示す。

4.3.3.1 A.NETWORK

前提条件 A.NETWORK は、TOE を設置する MFD を内部ネットワークに接続し、その内部ネットワークが外部ネットワークからの攻撃から保護され、かつ、内部ネットワーク内において少なくとも MFD と同じサブネットワークには MFD との通信を認める機器だけが接続されることを求めている。これは OE.FIREWALL と OE.SUBNET の組み合わせにより実現できる。

4.3.3.2 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。

5 拡張コンポーネント定義

本 ST は拡張コンポーネントを定義しない。

6 セキュリティ要件

本章は、セキュリティ要件を記述する。

6.1 要件操作

本節では CC 機能および保証コンポーネントに対する操作の識別を定義する。

- 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、およびエレメントのラベルに対し ( ) 内に一連番号を後置することで、固有識別子とする。
- 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。値またはその一部としてリストを示す場合、要素間の切れ目は、コンマで区切るか、または、箇条書きスタイルによって示す。
  - パラメータ名のような、値を識別する情報を、必要に応じ丸括弧 ( ) に入れて値に付記する。
- 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。
- 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** で示す。
  - 元のテキストを削除する場合、削除するテキストを丸括弧 ( ) に入れる。
  - 元のテキストを新しいテキストで置き換える場合、置き換えられる元のテキストを丸括弧 ( ) に入れ、新しいテキストをその直前に **太字** で示す。
- *単純な斜体 (italic)* は要件操作を表すものでなく、本 ST 全体を通じて、単にテキストを強調するために使用されているに過ぎない。

6.2 セキュリティ機能要件

本節では TOE が満たすべき SFR (セキュリティ機能要件) を CC パート 2 のクラス別に記述する。

6.2.1 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[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-H 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、 **毎回の電源 ON 時に** 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

●FCS_COP.1	暗号操作
下位階層:	なし
FCS_COP.1.1	TSF は、[FIPS PUB 197]に合致する、特定された暗号アルゴリズム[AES Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[● MSD に書き込む利用者データの暗号化 ● MSD に書き込む TSF データの暗号化 ● MSD から読み出した利用者データの復号

- MSD から読み出した TSF 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 セキュリティ属性を伴う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

6.2.2 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、[

- HDD 上のスプールイメージデータファイル
- HDD 上のファイリングイメージデータファイル
- HDD 上のアドレス帳データファイル
- HDD 上のジョブ完了記録データファイル
- Flash メモリ上のスプールイメージデータファイル

]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 **少なくとも 1 回上書き消去することにより** 利用できなくすることを保証しなければならない。

依存性: なし

6.2.3 クラス FIA: 識別と認証

●FIA_AFL.1 (1) 認証失敗時の取り扱い(1)

下位階層: なし

FIA_AFL.1.1 (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 (1) 不成功の認証試行が定義した回数*[に達する]* とき、TSF は、[

- 不成功認証が 3 回に達するとき: 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_AFL.1 (2) 認証失敗時の取り扱い(2)

下位階層: なし

FIA_AFL.1.1 (2) TSF は、[

- 親展ファイルに対す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 (2) 不成功の認証試行が定義した回数*[に達する]* とき、TSF は、[

- 不成功認証が 3 回に達するとき: 認証試行受付を停止し、当該親展ファイルをロック

● 管理者による親展ファイルのロック解除操作: 認証失敗回数をクリアし復帰
]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 (1) 秘密の検証(1)

下位階層: なし

FIA_SOS.1.1 (1) TSF は、 **管理者パスワード** (秘密) が[5 文字以上 32 文字以下の英数記号]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_SOS.1 (2) 秘密の検証(2)

下位階層: なし

FIA_SOS.1.1 (2) TSF は、 **親展ファイルパスワード** (秘密) が[5 文字以上 8 文字以下の数字]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 (1) アクション前の利用者認証(1)

下位階層: FIA_UAU.1 認証のタイミング

FIA_UAU.2.1 (1) TSF は、その **管理者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **管理者** (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.2 (2) アクション前の利用者認証(2)

下位階層: FIA_UAU.1 認証のタイミング

FIA_UAU.2.1 (2) TSF は、その **親展ファイル保存者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **親展ファイル保存者** (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 (1) 保護された認証フィードバック(1)

下位階層: なし

FIA_UAU.7.1 (1) TSF は、 **管理者の** 認証を行っている間、[入力された文字の個数]だけを **管理者** (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_UAU.7 (2) 保護された認証フィードバック(2)

下位階層: なし

FIA_UAU.7.1 (2) TSF は、 **親展ファイル保存者の** 認証を行っている間、[入力された文字の個数]だけを **親展ファイル保存者** (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 (1) アクション前の利用者識別(1)

下位階層: FIA_UID.1 識別のタイミング

FIA_UID.2.1 (1) TSF は、その **管理者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **管理者** (利用者) に識別が成功することを要求しなければならない。

依存性: なし

●FIA_UID.2 (2) アクション前の利用者識別(2)

下位階層: FIA_UID.1 識別のタイミング

FIA_UID.2.1 (2) TSF は、その **親展ファイル保存者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **親展ファイル保存者** (利用者) に識別が成功することを要求しなければならない。

依存性: なし

6.2.4 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, ドキュメントファイリングデータ消去, 電源 ON 時の自動消去] *[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 セキュリティの役割

●FMT_MTD.1 (1) TSF データの管理(1)

下位階層: なし

FMT_MTD.1.1 (1) TSF は、[管理者パスワード]を*[改変]* 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 セキュリティの役割

●FMT_MTD.1 (2) TSF データの管理(2)

下位階層: なし

FMT_MTD.1.1 (2) TSF は、[親展ファイルパスワード]を*[改変、削除]* する能力を[親展ファイル保存者]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 セキュリティの役割

●FMT_MTD.1 (3) TSF データの管理(3)

下位階層: なし

FMT_MTD.1.1 (3) TSF は、[

- IP アドレスフィルタ
- MAC アドレスフィルタ
- SSL 設定
- 各ジョブ完了後の自動消去回数
- データエリア消去回数
- 電源 ON 時の自動消去の対象別有効設定
- 電源 ON 時の自動消去回数

- ドキュメントファイリング禁止設定
- ホールド以外のプリントジョブ禁止設定

]を*[問い合わせ、改変]* 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 セキュリティの役割

●FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。:[

- 停止: 全データエリア消去
- 停止: ドキュメントファイリングデータ消去
- 停止: 電源 ON 時の自動消去
- 問い合わせ、改変: 各ジョブ完了後の自動消去回数
- 問い合わせ、改変: データエリア消去回数
- 問い合わせ、改変: 電源 ON 時の自動消去の対象別有効設定
- 問い合わせ、改変: 電源 ON 時の自動消去回数
- ロック解除: 親展ファイル
- 改変: 管理者パスワード
- 改変、削除: 親展ファイルパスワード
- 問い合わせ、改変: ドキュメントファイリング禁止設定
- 問い合わせ、改変: ホールド以外のプリントジョブ禁止設定
- 問い合わせ、改変: IP アドレスフィルタ
- 問い合わせ、改変: MAC アドレスフィルタ
- 問い合わせ、改変: SSL 設定

]。

注: 管理要件への考慮は 6.4.1.7 節で述べる。

依存性: なし。

●FMT_SMR.1 (1) セキュリティの役割(1)

下位階層: なし

FMT_SMR.1.1 (1) TSF は、役割[管理者]を維持しなければならない。

FMT_SMR.1.2 (1) 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

●FMT_SMR.1 (2) セキュリティの役割(2)

下位階層: なし

FMT_SMR.1.1 (2) TSF は、役割[親展ファイル保存者]を維持しなければならない。

FMT_SMR.1.2 (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

6.2.5 クラス FTA: TOE アクセス

●FTA_TSE.1 TOE セション確立

下位階層:	なし
FTA_TSE.1.1	TSF は、[IP アドレスおよび MAC アドレス]に基づきセション確立を拒否できなければならない。
依存性:	なし

6.2.6 クラス FTP: 高信頼パス/チャネル

●FTP_TRP.1	高信頼パス
下位階層:	なし
FTP_TRP.1.1	TSF は、それ自身と*[リモート]* 利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、*[改変、暴露]* からの通信データの保護を提供する通信パスを提供しなければならない。
FTP_TRP.1.2	TSF は、*[リモート利用者]* が、高信頼パスを介して通信を開始することを許可しなければならない。
FTP_TRP.1.3	TSF は、*[* [TOE の Web による通信サービス、プリンタドライバ用通信サービス (*高信頼パスが要求される他のサービス*)] *]* に対して、高信頼パスの使用を要求しなければならない。
依存性:	なし

6.3 セキュリティ保証要件

以下、本 ST が主張する EAL3 適合の TOE セキュリティ保証要件を、CC パート 3 の保証クラス別に示す。本 ST は、CC パート 3 に定義のあるセキュリティ保証コンポーネントを、そのまま TOE セキュリティ保証要件として使用する。

- ASE クラス: セキュリティターゲット評価
  - ASE_INT.1 — ST 概説
  - ASE_CCL.1 — 適合主張
  - ASE_SPD.1 — セキュリティ課題定義
  - ASE_OBJ.2 — セキュリティ対策方針
  - ASE_ECD.1 — 拡張コンポーネント定義
  - ASE_REQ.2 — 派生したセキュリティ要件
  - ASE_TSS.1 — TOE 要約仕様
- ADV クラス: 開発
  - ADV_ARC.1 — セキュリティアーキテクチャ記述
  - ADV_FSP.3 — 完全な要約を伴う機能仕様
  - ADV_TDS.2 — アーキテクチャ設計
- AGD クラス: ガイダンス文書
  - AGD_OPE.1 — 利用者操作ガイダンス
  - AGD_PRE.1 — 準備手続き
- ALC クラス: ライフサイクルサポート
  - ALC_CMC.3 — 許可の管理
  - ALC_CMS.3 — 実装表現の CM 範囲
  - ALC_DEL.1 — 配付手続き
  - ALC_DVS.1 — セキュリティ手段の識別
  - ALC_LCD.1 — 開発者によるライフサイクルモデルの定義

- ATE クラス: テスト
  - ATE_COV.2 — カバレージの分析
  - ATE_DPT.1 — テスト: 基本設計
  - ATE_FUN.1 — 機能テスト
  - ATE_IND.2 — 独立テスト - サンプル
- AVA クラス: 脆弱性評定
  - AVA_VAN.2 — 脆弱性分析

6.4 セキュリティ要件根拠

セキュリティ対策方針に対して、セキュリティ要件が有効であることを検証する。

表 6.1: TOE セキュリティ機能要件根拠

対策方針 要件	O.FILTER	O.MANAGE	O.REMOVE	O.RESIDUAL	O.TRP	O.USER
FCS_CKM.1			6.4.1.3			
FCS_COP.1			6.4.1.3			
FDP_RIP.1				6.4.1.4		
FIA_AFL.1 (1)		6.4.1.2				
FIA_AFL.1 (2)		6.4.1.2				6.4.1.6
FIA_SOS.1 (1)		6.4.1.2				
FIA_SOS.1 (2)						6.4.1.6
FIA_UAU.2 (1)		6.4.1.2				
FIA_UAU.2 (2)						6.4.1.6
FIA_UAU.7 (1)		6.4.1.2				
FIA_UAU.7 (2)						6.4.1.6
FIA_UID.2 (1)		6.4.1.2				
FIA_UID.2 (2)						6.4.1.6
FMT_MOF.1		6.4.1.2				
FMT_MTD.1 (1)		6.4.1.2				
FMT_MTD.1 (2)						6.4.1.6
FMT_MTD.1 (3)	6.4.1.1	6.4.1.2			6.4.1.5	6.4.1.6
FMT_SMF.1	6.4.1.1	6.4.1.2			6.4.1.5	6.4.1.6
FMT_SMR.1 (1)		6.4.1.2				
FMT_SMR.1 (2)						6.4.1.6
FTA_TSE.1	6.4.1.1					
FTP_TRP.1					6.4.1.5	

6.4.1 TOE セキュリティ機能要件根拠

表 6.1 に、TOE セキュリティ機能要件とセキュリティ対策方針の対応を、各対応の根拠を記載している節番号と共に示す。

6.4.1.1 O.FILTER

O.FILTER は、以下の機能要件の組み合わせにより実現できる。

- FTA_TSE.1 にて、TOE は、IP アドレスおよび MAC アドレスに基づき、セション確立を拒否できる。
- FMT_SMF.1 にて、TOE は、前項の運用に必要な、IP アドレスフィルタおよび MAC アドレスフィルタの管理機能を行う能力を提供する。
- FMT_MTD.1 (3) にて、前項の IP アドレスフィルタおよび MAC アドレスフィルタを、問い合わせまたは改変する能力は、管理者に制限される。

上記 FMT_SMF.1 と FMT_MTD.1 (3) は一貫して FTA_TSE.1 の管理を規定するので、O.FILTER を実現する上で、機能要件の競合は発生しない。

6.4.1.2 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_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) によって、管理者を識別および認証する。これにより、以下の各機能の実行が管理者にのみ可能となる。
   - FMT_MTD.1 (1) にて、O.MANAGE を実施する TSF データである管理者パスワードを改変する能力は、管理者のみに制限される。
   - FMT_MTD.1 (3) にて、各 TSF に関する設定値の改変と問合せが管理者にのみ可能となる。
   - 連続する認証失敗による親展ファイルのロックを解除することが, FIA_AFL.1 (2) により、管理者にのみ可能となる。
   - 実行中の全データエリア消去、ドキュメントファイリングデータ消去、及び、電源 ON 時の自動消去の各機能を停止することが, FMT_MOF.1 により、管理者にのみ可能となる。

b) FMT_SMF.1 にて、TOE は、上記の管理者認証の運用に必要な、管理者パスワードの改変を行う能力を提供する。

c) 以下のように、管理者パスワードに適切な SOF を確保する。
   - FIA_AFL.1 (1) は、管理者パスワードに対する総当り攻撃に対抗すべく、認証失敗が連続したときに一定時間の認証受付停止を要求している。
   - FIA_SOS.1 (1) は、管理者パスワードの品質検証メカニズムを要求している。

d) 管理者は FMT_MOF.1 及び FMT_MTD.1 (1) により, TOE の管理の役割を任され、この役割は FMT_SMR.1 (1) にて維持されるため、常に正当な管理者が管理機能を実行できる。

上記 FIA_AFL.1 (1), FIA_UID.2 (1), FIA_UAU.2 (1), FIA_UAU.7 (1), FMT_MOF.1, FMT_MTD.1 (1), FMT_MTD.1 (3), FMT_SMF.1 及び FMT_SMR.1 (1) の間には依存に基づく支援があり、かつ、互いに競合するような機能性を要求していない。それらの要件と FIA_AFL.1 (3) の間で競合するような機能性の要求はなく、FIA_AFL.1 (2) と FMT_SMF.1 は相互に支援し合い、FMT_SMR.1 (1) は FIA_AFL.1 (2) を支援する。それらの要件と FIA_SOS.1 (1) の間で競合するような機能性の要求はなく、FIA_SOS.1 (1) と FIA_AFL.1 (1) は相互に支援し合う。したがって O.MANAGE は競合なく一貫した要件群により満たされている。

6.4.1.3 O.REMOVE

O.REMOVE の目的は T.RECOVER への対抗であり、すなわち MFD から MSD を取り出されたとしても、MSD 内の利用者データが再生されないようにすることである。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、MSD に書き込む利用者データが暗号化される。そのため、MSD への保存を実行した MFD 自身以外に MSD を接続して利用者データの再生を試みても、利用者データの再生は阻止される。
- 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。

上記 FCS_CKM.1 と FCS_COP.1 は互いに依存するので、O.REMOVE を達成する上で機能要件の競合は発生しない。

6.4.1.4 O.RESIDUAL

O.RESIDUAL は、FDP_RIP.1 によって、以下のオブジェクトからの資源の割当て解除において、それらの領域に対し少なくとも 1 回以上上書き消去する。

- 対象となるオブジェクトは、HDD 上のスプールイメージデータファイル、HDD 上のファイリングイメージデータファイル、HDD 上のアドレス帳データファイル、HDD 上のジョブ完了記録データファイル、および、Flash メモリ上のスプールイメージデータファイルである。
- それらのオブジェクトからの資源の割当て解除が発生するのは、ジョブ完了または中止時、利用者の親展ファイル削除操作時、および、管理者の操作または設定に基づき特定のデータ消去機能のプログラムが実行されたときである。

- 前項で述べたプログラムは、全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去である。

O.RESIDUAL は、単一の機能要件によって満たされ、機能要件の競合はない。

6.4.1.5 O.TRP

O.TRP は、以下の機能要件の組み合わせにより実現できる。

- FTP_TRP.1 により、利用者と TSF 間に高信頼通信を確立し、維持することができる。
- FMT_MTD.1 (3) により、FTP_TRP.1 に関する TSF データ、すなわち SSL 設定を問い合わせまたは改変する能力は、管理者に制限される。
- FMT_SMF.1 により、その運用管理が可能となる。

上記 FMT_MTD.1 (3) および FMT_SMF.1 は相互補完的に FTP_TRP.1 の管理を規定するので、O.TRP を実現する上で、機能要件の競合は発生しない。

6.4.1.6 O.USER

O.USER は、以下の機能要件の組み合わせにより実現できる。

a) FIA_AFL.1 (2), FIA_UAU.2 (2), FIA_UAU.7 (2) および FIA_UID.2 (2) によって、親展ファイル保存者を識別認証する。これにより、親展ファイルへのアクセス (親展ファイルパスワード管理を含む) が、親展ファイル保存者にのみ可能となる。

b) FIA_SOS.1 (2) により、親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることが保証される。

c) FMT_MTD.1 (2) にて、親展ファイルパスワードを変更する能力は、親展ファイル保存者のみに制限される。

d) FMT_MTD.1 (3) にて、親展ファイルによる保護の実効性に関わる管理能力、すなわち、ドキュメントファイリング禁止設定およびホールド以外のプリントジョブ禁止設定を、問い合わせまたは改変する能力は、管理者に制限される。

e) FMT_SMR.1 (2) にて、親展ファイル保存者の役割は維持され、親展ファイルを保存した利用者はその役割に関連づけられる。

f) FMT_SMF.1 により、親展ファイルパスワードの管理運用が可能となる。

上記 a) は親展ファイル保存者識別認証の事象に関するものであり、b), c) および f) は親展ファイルパスワード変更の事象に関するものであり、d) は管理者による管理の事象に関するものである。これら三つの事象は独立に発生し、相互に競合しない。a) の四つの機能要件は、親展ファイル保存者識別認証を実施するために相互補完的に作用するので、競合は発生しない。b), c), および f) の三つの機能要件は、親展ファイルパスワード改変を実施するために相互補完的に作用するので、競合は発生しない。e) は c) の依存性の要件であり a) にサポートされるので、競合は発生しない。以上から、O.USER を実現する上で、機能要件の競合は発生しない。

6.4.1.7 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 6.2: 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	—	暗号鍵の属性は変更しない
FCS_COP.1	—	(管理要件なし)
FDP_RIP.1	• 停止: 全データエリア消去 • 停止: ドキュメントファイリングデータ消去 • 停止: 電源ON時の自動消去 • 問い合わせ、改変: 各ジョブ完了後の自動消去回数 • 問い合わせ、改変: データエリア消去回数 • 問い合わせ、改変: 電源ON時の自動消去の対象別有効設定 • 問い合わせ、改変: 電源ON時の自動消去回数	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 (1)	—	閾値とアクションは固定
FIA_AFL.1 (2)	• ロック解除: 親展ファイル	閾値とアクションは固定
FIA_SOS.1 (1)	—	品質尺度は固定
FIA_SOS.1 (2)	—	品質尺度は固定
FIA_UAU.2 (1)	• 改変: 管理者パスワード	管理要件に合致
FIA_UAU.2 (2)	• 改変、削除: 親展ファイルパスワード • 問い合わせ、改変: ドキュメントファイリング禁止設定 • 問い合わせ、改変: ホールド以外のプリントジョブ禁止設定	管理要件に合致
FIA_UAU.7 (1)	—	(管理要件なし)
FIA_UAU.7 (2)	—	(管理要件なし)
FIA_UID.2 (1)	—	管理者の識別は固定
FIA_UID.2 (2)	—	各親展ファイル保存者の識別は固定
FMT_MOF.1	—	役割のグループはない
FMT_MTD.1 (1)	—	役割のグループはない
FMT_MTD.1 (2)	—	役割のグループはない
FMT_MTD.1 (3)	—	役割のグループはない
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1 (1)	—	利用者のグループはない
FMT_SMR.1 (2)	—	利用者のグループはない
FTA_TSE.1	• 問い合わせ、改変: IPアドレスフィルタ • 問い合わせ、改変: MACアドレスフィルタ	管理要件に合致
FTP_TRP.1	• 問い合わせ、改変: SSL設定	管理要件に合致

表 6.2 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。

6.4.1.8 セキュリティ機能要件の依存性根拠

表 6.3 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を示す。 “#” を付した依存性は上位の SFR により満足されている。表 6.4 は、本 TOE が依存性を満足していないことの正当性を示す。これら二つの表は、共通の識別子 (J1 のような) により対応付けられる。

表 6.3: SFR 依存性の分析

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	FCS_COP.1	FCS_CKM.4	J1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1	FCS_CKM.4	J1
FDP_RIP.1	—	—	—	—
FIA_AFL.1 (1)	FIA_UAU.1 #	FIA_UAU.2 (1)	—	—
FIA_AFL.1 (2)	FIA_UAU.1 #	FIA_UAU.2 (2)	—	—
FIA_SOS.1 (1)	—	—	—	—
FIA_SOS.1 (2)	—	—	—	—
FIA_UAU.2 (1)	FIA_UID.1 #	FIA_UID.2 (1)	—	—
FIA_UAU.2 (2)	FIA_UID.1 #	FIA_UID.2 (2)	—	—
FIA_UAU.7 (1)	FIA_UAU.1 #	FIA_UAU.2 (1)	—	—
FIA_UAU.7 (2)	FIA_UAU.1 #	FIA_UAU.2 (2)	—	—
FIA_UID.2 (1)	—	—	—	—
FIA_UID.2 (2)	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MTD.1 (1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_MTD.1 (2)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (2)	—	—
FMT_MTD.1 (3)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1 (1)	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1 (1)	FIA_UID.1 #	FIA_UID.2 (1)	—	—
FMT_SMR.1 (2)	FIA_UID.1 #	FIA_UID.2 (2)	—	—
FTA_TSE.1	—	—	—	—
FTP_TRP.1	—	—	—	—

表 6.4: SFR 依存性不満足の正当性

	不満足	正当性の根拠
J1	FCS_CKM.4	暗号鍵は揮発性メモリ内に保持する。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、標準の暗号鍵破棄方法を行うTSFを実装する必要がなく、標準を特定するFCS_CKM.4は不要。

6.4.2 TOE セキュリティ保証要件根拠

本 TOE は、MFD の一部および 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。こうした脅威に対抗するセキュリティ機能の信頼性を、商用の製品において保証することを意図して、TOE 開発時におけるセキュリティ対策の分析を含み、セキュリティ機能を安全に使用するためのガイダンス情報が含まれていることの分析を含む EAL3 を選択している。

保証要件は EAL3 適合であるので、すべての保証要件は依存性を満たす。

7 TOE 要約仕様

本章は、TOE セキュリティ機能 (TSF) の要約仕様を記述することにより、TOE セキュリティ機能要件が満たされることを示す。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 7.1 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 7.1: 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_FCF	TSF_FNP
FCS_CKM.1	7.1					
FCS_COP.1		7.2				
FDP_RIP.1			7.3			
FIA_AFL.1 (1)			7.3	7.4		7.6
FIA_AFL.1 (2)					7.5	
FIA_SOS.1 (1)				7.4		
FIA_SOS.1 (2)					7.5	
FIA_UAU.2 (1)			7.3	7.4		7.6
FIA_UAU.2 (2)					7.5	
FIA_UAU.7 (1)			7.3	7.4		7.6
FIA_UAU.7 (2)					7.5	
FIA_UID.2 (1)			7.3	7.4		7.6
FIA_UID.2 (2)					7.5	
FMT_MOF.1			7.3			
FMT_MTD.1 (1)				7.4		
FMT_MTD.1 (2)					7.5	
FMT_MTD.1 (3)			7.3		7.5	7.6
FMT_SMF.1			7.3	7.4	7.5	7.6
FMT_SMR.1 (1)				7.4		
FMT_SMR.1 (2)					7.5	
FTA_TSE.1						7.6
FTP_TRP.1						7.6

7.1 暗号鍵生成 (TSF_FKG)

本 TSF は FCS_CKM.1 に従って暗号鍵 (共通鍵) の生成を行い、利用者データおよび TSF データの暗号化機能をサポートする。

本 TSF は、TOE 設置時にセキュアなシードを自ら生成する。本 TSF はこのシードを元に、MFD の電源がオンになるたびに、MSN-H 拡張アルゴリズムを用いて 128 ビット長の鍵を生成する。MSN-H 拡張アルゴリズムは SHARP 標準に合致し、128 ビット長の暗号鍵を生成する暗号鍵生成アルゴリズムである。よって、本 TOE は FCS_CKM.1 を満たす。

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。生成した鍵は、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し、電源オフにより消失する。

7.2 暗号操作 (TSF_FDE)

本 TSF は FCS_COP.1 が定めるとおり、利用者データおよび TSF データを MSD に書き込む必要が生じたときは、それらのデータを暗号化してから書き込む。また、それらのデータが必要になれば、MSD から読み出し、復号して利用する。暗号化および復号には、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。

対象となる利用者データは以下のとおり:

- HDD 上にスプール保存されるイメージデータ
- Flash メモリ上にスプール保存されるイメージデータ
- HDD 上にファイリング保存されるイメージデータ
- HDD 上のアドレス帳データ
- HDD 上のジョブ完了記録データ

対象となる TSF データは以下のとおり:

- HDD 上の親展ファイルパスワード
- HDD 上の管理者パスワード

よって、本 TOE は FCS_COP.1 を満たす。

7.3 データ消去 (TSF_FDC)

以下、まず本 TSF の概要を述べ、続いて各構成要素を順に説明する。

7.3.1 データ消去の概要

本 TSF の全体像、および、SFR との対応を記述する。

TOE はスプール保存およびファイリング保存されたイメージデータファイル、またはアドレス帳データファイル、ジョブ完了記録データファイルを消去するデータ消去機能を有する。以下の各プログラムは、本機能に含まれる。

a) 各ジョブ完了後の自動消去プログラム

b) 全データエリア消去プログラム

c) アドレス帳/本体内登録データ消去プログラム

d) ドキュメントファイリングデータ消去プログラム

e) ジョブ状況完了エリア消去プログラム

f) 電源 ON 時の自動消去プログラム

上記の各プログラム、および、それらの設定機能が本 TSF を構成し、以下のとおり SFR に対応する。

- 各プログラムとも HDD にはランダム値を 1 回以上、Flash メモリには固定値 (ビット値 0 の列、または、ビット値 1 の列) を 1 回上書きする。各プログラムは各々担当するオブジェクト (イメージデータファイル等) を上書き消去することにより、当該オブジェクトに保存されていた情報 (イメージデータ等) の再生を不能とする。よって本 TOE は FDP_RIP.1 を満たす。
- 上記 b), d) および f) は FMT_SMF.1 に従って停止できるよう中止機能 (7.3.3 節) を持ち、後述の TSF_AUT および TSF_FNP と共同で FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) を満たす。中止機能は FIA_UID.2 (1) および FIA_UAU.2 (1) に従い管理者識別認証を要求する。認証の際 FIA_UAU.7 (1) のフィードバック保護および FIA_AFL.1 (1) の失敗対応を行う。これにより、FMT_MOF.1 が定めるとおり管理者のみが消去を途中で停止できる。
- 本 TSF は FMT_SMF.1 に従った設定機能 (7.3.8 節) の使用を、TSF_AUT で識別認証された管理者に許す。これにより本 TSF は TSF_FCF および TSF_FNP と共同で FMT_MTD.1 (3) を満たす。

次節以降、各プログラムおよびその設定について記述する。

7.3.2 各ジョブ完了後の自動消去プログラム

本プログラムは以下のとおり、イメージデータを上書き消去する。

- ジョブ処理のために HDD または Flash メモリにスプール保存されたイメージデータを、当該ジョブ完了または中止時に上書き消去する。
- ドキュメントファイリング機能 (親展ファイル機能を含む) により HDD に保存されたイメージデータを、利用者の操作により削除される際に上書き消去する。

いずれの場合も、本プログラムは所定のタイミングで必ず起動され、非活性化する手段は提供されない。

7.3.3 全データエリア消去プログラム

本プログラムは、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、以下のデータを上書き消去する。

- HDD 上にあるすべてのスプールイメージデータ
- HDD 上にあるすべてのファイリングイメージデータ
- HDD 上にあるジョブ完了記録データ
- Flash メモリ上にあるすべてのスプールイメージデータ

本プログラムは、アドレス帳データは消去しない。

本プログラムは中止機能を持つ。本プログラムを途中で中止する場合、キャンセル操作を選択後、本 TSF は本プログラムを起動した管理者のパスワード入力を必ず要求する。キャンセル操作は FIA_UID.2 (1) が定める管理者識別であり、管理者パスワード入力は FIA_UAU.2 (1) が定める管理者認証である。認証入力中、TOE は FIA_UAU.7 (1) に従い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。

中止機能の認証入力において、FIA_AFL.1 (1) が定めるとおり連続して 3 回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

7.3.4 アドレス帳/本体内登録データ消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者の操作により, HDD 上のアドレス帳データを上書き消去する。

所要時間は比較的短いので、中止機能はない。

7.3.5 ドキュメントファイリングデータ消去プログラム

本プログラムは、TSF_AUT で識別認証された管理者の操作により, HDD 上のイメージデータを上書き消去する。対象データは以下の選択肢から一つ以上を、起動時に管理者が指定する。

- HDD 上にあるすべてのスプールイメージデータ
- HDD 上にあるすべてのファイリングイメージデータ

本プログラムは、全データエリア消去と同様の中止機能を持つ。

7.3.6 ジョブ状況完了エリア消去プログラム

本プログラムは、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, HDD 上のジョブ完了記録データを上書き消去する。所要時間は比較的短いので、中止機能はない。

7.3.7 電源 ON 時の自動消去プログラム

TOE の電源 ON 時に上書き消去を実行する。ただし、スキャナまたはファクス送信の予約ジョブがある場合、および、未出力のファクス受信またはインターネット Fax 受信ジョブがある場合を除く。

本プログラムの有効または無効、すなわち、電源 ON 時に本プログラムを実行するか否かは、予め設定された値に従う。本プログラムを実行する際の消去対象データも同様である。

本プログラムの消去対象データは、上記の全データエリア消去の対象となるすべてのデータ、または指定された HDD のデータのいずれかである。指定可能な HDD のデータは、スプールイメージデータ、ファイリングイメージデータ、および、ジョブ完了記録データのうち一つ以上である。

本プログラムは、全データエリア消去と同様の中止機能を持つ。

7.3.8 データ消去設定

本 TSF は、上記の各プログラムに対し、以下の設定機能を提供する。

- 各ジョブ完了後の自動消去回数:
  各ジョブ完了後の自動消去プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。
- データエリア消去回数:
  全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、および、ジョブ状況完了エリア消去の各プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。
- 電源 ON 時の自動消去:
  電源 ON 時の自動消去プログラムの、対象別有効設定。既定値はすべて無効。
- 電源 ON 時の自動消去回数:
  電源 ON 時の自動消去プログラムの HDD 上書き回数。1 回以上 7 回以下。既定値は 1 回。

上記の各設定は、TSF_AUT で識別認証された管理者のみ、問い合わせと改変が許される。

7.4 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。本 TSF は FMT_SMF.1 および FMT_MTD.1 (1) に従い、管理者パスワードの変更を、本 TSF で識別認証された管理者のみに許し、FIA_SOS.1 (1) に従い、5 文字以上 32 文字以下の英数記号のみを受け入れる。

管理者向け以外の機能は、管理者識別認証を経ることなく利用できる。

本 TSF は、TSF_FDC および TSF_FNP と共同で FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) を満たす。

FIA_UID.2 (1) に従い、管理機能の起動操作、または、管理者ログイン操作によって管理者を識別し、かつ、FIA_UAU.2 (1) に従い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。なお、管理者ログイン操作とは、操作パネルまたは Web における、管理者識別と管理者パスワード認証を含む操作である。

操作パネルでの管理者パスワード入力時、FIA_UAU.7 (1) に従い、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。

Web では、クライアントに対しパスワード形式の入力を指定する。これは、クライアントの Web ブラウザに対し、利用者が入力した文字を代替文字のような方式で隠蔽するよう要求する。

管理者パスワード認証において、連続して 3 回認証に失敗した場合は FIA_AFL.1 (1) に従い、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

本 TSF は管理者識別認証により、管理者を特定し、役割に関連づける。また、管理者のみに管理者パスワードの変更 (改変) 機能を提供することにより、役割の維持管理を図る。これらにより TOE は FMT_SMR.1 (1) を満たす。

7.5 親展ファイル (TSF_FCF)

MFD 内に利用者が親展ファイルとして保存したイメージデータをパスワード保護し、認証を経て再操作 (印刷等) を許す。

本 TSF はコピー、プリンタドライバ、PC-Fax およびスキャン保存の各機能に、親展ファイル保存のインタフェースを提供し、FIA_SOS.1 (2) に従い、親展ファイルパスワードが 5 文字以上 8 文字以下の数字であることを検査する。

本 TSF は、操作パネルまたは Web 経由で親展ファイルの再操作の機能を提供する。FIA_UID.2 (2) に従い、対象の親展ファイルを選択する操作によって親展ファイル保存者を識別し、かつ、FIA_UAU.2 (2) に従い正しい親展ファイル保存者パスワードによって認証に成功した場合に限り、再操作のインタフェースを提供する。その認証の際は FIA_UAU.7 (2) に従い、入力された文字の個数以外の情報を見せないようにする。

利用者が操作パネルで親展ファイルに対して再操作を行う場合、本 TSF は利用者に親展ファイルパスワード入力を必ず要求し、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。本 TSF は、親展ファイルパスワードが入力され、かつ、保存の際に設定された親展ファイルパスワードと一致している場合に限り、1.3.5.2 節で述べた再操作 (プレビューを除く) を許す。

利用者が Web で親展ファイルに対して再操作を行う場合、本 TSF は、親展ファイルパスワードが入力され、かつ、保存の際に設定された親展ファイルパスワードと一致していることを必ず検査し、その検査に成功した場合に限り、再操作 (プレビューを含むすべて) を許す。本 TSF は親展ファイルパスワード入力の際、クライアントに対しパスワード形式の入力を指定する。これは、クライアントの Web ブラウザに対し、利用者が入力した文字を代替文字のような方式で隠蔽するよう要求する。

親展ファイルの再操作に先立つ親展ファイルパスワード認証では、FIA_AFL.1 (2) に従い、連続して 3 回認証に失敗した場合、本 TSF は認証受付を停止し、当該親展ファイルをロックする。失敗回数は、各ファイルについて数える。認証に成功したとき、当該ファイルの失敗回数をゼロに戻す。ロックの解除は、TSF_AUT で識別認証された管理者のみに許される。

本 TSF は FMT_MTD.1 (2) および FMT_SMF.1 に従い、再操作の一種として親展ファイルパスワード変更の機能を提供し、新パスワードが 5 文字以上 8 文字以下の数字であることを検査する。

本 TSF は再操作に先立つ親展ファイル保存者の識別認証により、親展ファイル保存者を特定し、役割に関連づける。また、親展ファイル保存者のみに親展ファイルパスワードの変更 (改変) 機能を提供することにより、役割の維持管理を図る。これらにより TOE は FMT_SMR.1 (2) を満たす。

本 TSF は再操作の一種として属性変更の機能を提供する。親展以外の属性に変更すれば、親展ファイルパスワードは削除される。この逆に、属性を親展に変更する場合、本 TSF は FIA_SOS.1 (2) に従い、5 文字以上 8 文字以下の数字からなる親展ファイルパスワードを要求する。

本 TSF は暗号化されたデータをクライアントの Web ブラウザへエクスポートする。本 TSF はまた、暗号化されたデータも暗号化されていないデータも共に、クライアントの Web ブラウザよりインポートする。

本 TSF は FMT_SMF.1 および FMT_MTD.1 (3) に従い、以下のとおりドキュメントファイリング機能に関する管理機能を持ち、TSF_AUT で識別認証された管理者に実行を許す。

- 親展ファイルによる保護の実効性を高めるための管理機能:
  - ドキュメントファイリング禁止設定: ジョブ種類別に各保存モードを禁止できる。親展でない (パスワードのない) モードをすべて禁止する設定が既定値であり、推奨値である。
  - ホールド以外のプリントジョブ禁止設定: プリンタドライバからのジョブに対し、その場での印刷出力を禁止する。ホールド指定のないジョブは拒否し、ホールドするジョブは印刷の有無を無視してホールドのみ行う。出力された用紙が第三者に持ち去られるリスクの高い環境において推奨される。
- 親展ファイルのロックに関する管理機能:
  - 親展ファイルのロック解除: 親展ファイルパスワード認証失敗によりロックされた親展ファイルに対し、ロックを解除する。本管理機能は “ファイル/フォルダ操作禁止の解除” の名称で提供される。

7.6 ネットワーク保護 (TSF_FNP)

以下、まず本 TSF の概要を述べ、続いて各構成要素を順に説明する。

7.6.1 ネットワーク保護の概要

本 TSF の構成要素、および、SFR との対応を記述する。本 TSF は以下の各要素からなる。

a) フィルタ機能

b) 通信データ保護機能

c) ネットワーク設定保護

上記 a) は FTA_TSE.1 を満たす。 b) は FTP_TRP.1 を満たす。 c) は TSF_FDC および TSF_AUT と共同で FIA_AFL.1 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_UID.2 (1) を満たす。また、a), b), TSF_FDC および TSF_FCF の共同で FMT_MTD.1 (3) および FMT_SMF.1 を満たす。以下、各要素について記述する。

7.6.2 フィルタ機能

管理者による事前の設定に基づき、意図しない通信相手との通信を拒絶する。IP アドレスによる条件と MAC アドレスによる条件を設定できる。本 TSF は、条件に合わない通信相手からのネットワークパケットを、必ず破棄し、レスポンスおよび処理をしない。

IP アドレスによる条件は、範囲を四つまで指定し、それらを許可するかまたは拒否するかを指定する。MAC アドレスによる条件は、許可する MAC アドレスを 10 個まで指定する。

本 TSF は、IP アドレスおよび MAC アドレスに基づき、意図しない通信相手との通信を拒絶できるので、FTA_TSE.1 を満たす。本 TSF は FMT_MTD.1 (3) に従い、TSF データである IP アドレスフィルタ値および MAC アドレスフィルタ値の問い合わせおよび改変を、TSF_AUT で識別認証された管理者のみに許す。

7.6.3 通信データ保護機能

クライアントと TOE の Web との通信を、盗聴より保護するために、HTTPS 通信機能を提供する。また、クライアントのプリンタドライバから送信される印刷データを、盗聴より保護するために、IPP-SSL 通信機能を提供する。

HTTPS 通信は、クライアントの Web ブラウザからの接続で開始し、切断されるまで通信を維持する。IPP-SSL 通信も同様にクライアントのプリンタドライバからの接続で開始し、切断されるまで通信を維持する。

採用される暗号アルゴリズムは RSA, DES, Triple-DES, AES および SHA-1 である。管理者の設定によって、サーバ秘密鍵と公開鍵がインストールされる。

本 TSF は FMT_MTD.1 (3) に従い、HTTPS 通信および IPP-SSL 通信に関する設定値 (TSF データ) の集合である SSL 設定の問い合わせおよび改変を、TSF_AUT で識別認証された管理者のみに許す。

7.6.4 ネットワーク設定保護

1.4.4.5 節に記述したネットワーク設定データを扱うインタフェースを、操作パネルおよび TOE の Web で提供する。これらのインタフェースは管理者のみに対して提供し、他の利用者のアクセスより保護する。そのために、本 TSF はネットワーク設定データを扱うインタフェースの提供に先立ち、TSF_AUT と同様の識別認証を実施する。本 TSF による識別認証は、TSF_AUT と同じく、FIA_UID.2 (1), FIA_UAU.2 (1), FIA_UAU.7 (1) および FIA_AFL.1 (1) に従って実施される。

8 付章

本章では、用語の定義を示す。

8.1 専門用語

本 ST 固有の専門用語を表 8.1 に示す。

表 8.1: 専門用語

用語	定義
アドレス帳/本体内登録データ消去	HDD上のアドレス帳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。
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。
外部ネットワーク	組織の管理が及ばない、内部ネットワーク以外のネットワーク。
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。ジョブ完了の際、ジョブ中止の際、および、ファイリングされたデータが利用者の操作により削除される際に、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, HDC, HDD 等を有する。
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。
再操作	ファイリング保存したイメージデータに対する操作。
サブネットワーク	内部ネットワークのうち、ルータで区切られた範囲。
ジョブ	MFDのコピー、プリンタ、スキャナ、ファクス送受信および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。
ジョブ完了記録	完了したジョブに関する記録。MFD内のHDDに保持される。
ジョブ状況完了エリア消去	HDD上のジョブ完了記録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。
親展ファイル	利用者がファイリング保存したデータのうち、他人に無断で再利用されないよう、パスワード (親展ファイルパスワード) によって保護されたもの。
親展ファイルパスワード	親展ファイルを、他人に無断で再利用されないよう、保護するためのパスワード。
親展ファイル保存者	イメージデータを親展ファイルとしてファイリング保存した利用者。
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、スキャン送信、ファクス送信およびスキャン保存の際に使用する。
スキャン保存	ファイリング機能の一つ。原稿を読み取って得たイメージデータをHDDに保存するが、印刷や送信は実行しない。
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およびジョブ完了記録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、機能キーおよ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。

用語	定義
電源ON時の自動消去	MFDの電源ON時にMSD上のデータを上書き消去するための機能。管理者による事前の設定に基づき、MFDの電源ON時に呼び出される。
ドキュメントファイリング	MFDが取り扱うイメージデータを、利用者が後で再操作 (印刷、送信、等) できるようMFD内のHDDに保存する機能。本STでは、ファイリングとも呼ぶ。
ドキュメントファイリング禁止設定	ジョブの種類別、モード別に、ファイリング保存を禁止する管理機能。親展ファイル以外のファイリング保存を禁止するために使用される。
ドキュメントファイリングデータ消去	HDD上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。ファイリングされたイメージデータの消去が主な目的だが、スプールされたイメージデータの消去も可能。
内部ネットワーク	組織の内部にあり、外部ネットワークからのセキュリティの脅威に対して保護されたネットワーク。
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。
ファイリング	ドキュメントファイリングの略。また、ドキュメントファイリング機能によりイメージデータを保存すること。
ホールド	プリンタドライバからのジョブを、ファイリング保存すること。
ホールド以外のプリントジョブ禁止	プリンタドライバからのジョブに対し、その場での印刷出力を禁止する。ホールド指定のないジョブは拒否し、ホールドするジョブは印刷の有無を無視してホールドのみ行う。
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、電気的な一括消去およ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。
ロック	誤ったパスワードが連続して入力されたとき、パスワードの受付を停止する機能。

8.2 略語

本 ST で使用している略語を表 8.2 および表 8.3 に示す。

表 8.2: CC の略語

略語	定義
CC	Common Criteria (コモンクライテリア)
EAL	Evaluation Assurance Level (評価保証レベル)
PP	Protection Profile (プロテクションプロファイル)
SAR	Security Assurance Requirement (セキュリティ保証要件)
SFR	Security Functional Requirement (セキュリティ機能要件)
ST	Security Target (セキュリティターゲット)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functions (TOEセキュリティ機能)

表 8.3: 他の略語

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。
DSK	データセキュリティキットMX-FRX8 — MFDのオプション製品であり、本TOEのファームウェア部分を提供する。 (Data Security Kit)
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。
HDC	Hard Disk Controller (ハード ディスク コントローラ)
HDD	Hard Disk Drive (ハード ディスク ドライブ)
HTTP	Hypertext Transfer Protocol — 主にWebで用いられる通信プロトコルの名称。
HTTPS	HTTP over SSL — SSLにより保護されたHTTP。
I/F	Interface (インタフェース)
IPP	Internet Printing Protocol — 印刷用通信プロトコルの名称。
IPP-SSL	IPP over SSL — SSLにより保護されたIPP。
IT	Information Technology (情報技術)
LAN	Local Area Network (ローカルエリアネットワーク)
LDAP	Lightweight Directory Access Protocol — ディレクトリサービス用通信プロトコルの名称。
MFD	Multi Function Device — デジタル複合機、すなわちコピー機能、プリンタ機能、スキャナ機能、ファクス機能等を有する事務機。
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特にMFD内のHDDおよびFlashメモリを指す。
NIC	Network Interface Card (ネットワークインタフェースカード) — または — Network Interface Controller (ネットワークインタフェースコントローラ)
PC	Personal Computer (パーソナルコンピュータ)
ROM	Read Only Memory (読み出し専用メモリ)
SSL	Secure Socket Layer — 計算機ネットワーク用暗号通信プロトコルの名称。
TLS	Transport Layer Security — 計算機ネットワーク用暗号通信プロトコルの名称。
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。
SMTP	Simple Mail Transfer Protocol — E-mail転送用通信プロトコルの名称。
WINS	Windows Internet Name Service — NetBIOS名からIPアドレスを求めるための機能。