SHARP

MX-FR11

セキュリティターゲット

Version 0.04

シャープ株式会社

履歴

日付	Ver.	変更点	作成	確認	発行
2009-02-02	0.01	• 初版作成	中川	坂本	小高
2009-03-31	0.02	• 一貫性および誤記等に関し修正	中川	坂本	小高
2009-04-24	0.03	• ガイダンスの一意識別子を記入	中川	坂本	山口
2013-03-11	0.04	• TOEバージョン C.11 対応	中川	岩崎	中平

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。

名称: MX-FR11 セキュリティターゲット

バージョン: 0.04

発行日: 2013-03-11

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。

名称: MX-FR11

バージョン: C.11

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 製品である。

TOE の主要部分は、ROM および HDD に格納された MFD 用ファームウェアである。これは 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。

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。

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 (ハードウェア) の一部機種が必要である。対象の機種は MX-3600FN, MX-4100FN, MX-4100N, MX-4101FN, MX-4101N, MX-4101NJ, MX-5000FN, MX-5000N, MX-5001FN, MX-5001N および MX-5001NJ である。

1.3.3 主要なセキュリティ機能

TOE セキュリティ機能は、主として以下に列挙する各機能からなり、TOE を搭載した MFD 内部の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する。

a) 暗号操作機能: MFD が扱うイメージデータ等を MFD 内の HDD または Flash メモリに書き込む前に暗号化する。

b) データ消去機能: MFD 内の HDD または Flash メモリに保存された暗号データの領域に対し、ランダム値または固定値を上書きする。

c) 親展ファイル機能: 利用者が HDD にイメージデータをファイリング保存する際、他人が無断で再利用しないよう、パスワードによる保護を提供する。

d) ネットワーク保護機能: ネットワーク経由の不正アクセス、通信データの盗聴、および、ネットワーク設定の不正な改変を防ぐ。

e) ファクスフロー制御機能: MFD のファクス I/F に接続される電話回線網から、MFD のネットワーク I/F を経由して内部ネットワークにアクセスすることを防ぐ。

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、プレビュー、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、送信またはプレビューを実行する際、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、IPsec 機能、SNMP v3 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。さらに、クライアントと MFD の通信において、IP を利用する通信では、IPsec プロトコルを使用し、IP にて送受信されるデータを通信中の盗聴から保護する。SNMP を利用する通信では、SNMP v3 プロトコルを使用し、MIB に基づいて MFD を遠隔管理するために送受信されるデータ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。

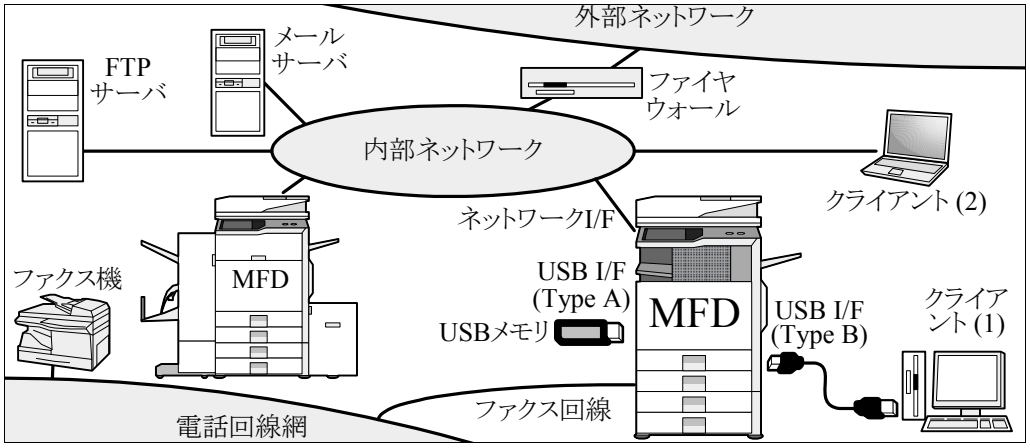

図 1: MFDの利用環境

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。連結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。連結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。インターネット Fax 受信、および、MFD からの連結印刷要求も同様。
- プルプリント: 操作パネルの操作で FTP サーバ、共有フォルダまたは 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 同梱または別途提供ソフトウェア要) 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

以下の通り、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。
- 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。連結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。

1.4 TOE 記述

1.4.1 TOE の物理的構成

TOE の物理的範囲を図 2 に網掛けで示す。TOE の主要部分は MFD のコントローラファームウェアである。これは 2 枚の ROM および USB メモリにて、シャープ製 MFD のセキュリティを強化するためのオプション製品 “データセキュリティキット MX-FR11” (DSK) として提供される。セキュリティ機能の一部を MFD の HDC 内に実装しており、これも TOE の範囲に含む。

- ROM: コントローラファームウェアの一部を格納する。MFD に TOE を設置する際、コントローラ基板から標準ファームウェア ROM 2 枚を取り外し、代わりに DSK の ROM 2 枚を取り付ける。
- MAIN: コントローラファームウェアの一部。DSK の USB メモリから MFD 内の HDD へ設置する。

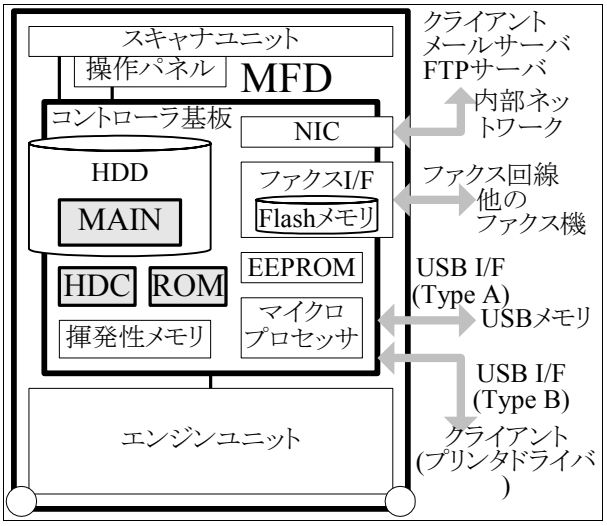

図 2: MFDの物理的構成とTOE

- HDC: 1 個の集積回路部品であり、コントローラ基板の一部として予め MFD に内蔵されている。

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。

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。

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, IPsec, SNMP v3 により通信データを保護する。ただし、SSL, IPsec, SNMP v3 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) ファクスフロー制御機能 (TSF_FFL): MFD のファクス I/F に接続される電話回線網から、MFD のネットワーク I/F を経由して内部ネットワークにアクセスすることを防ぐ。

h) 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。

i) 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。

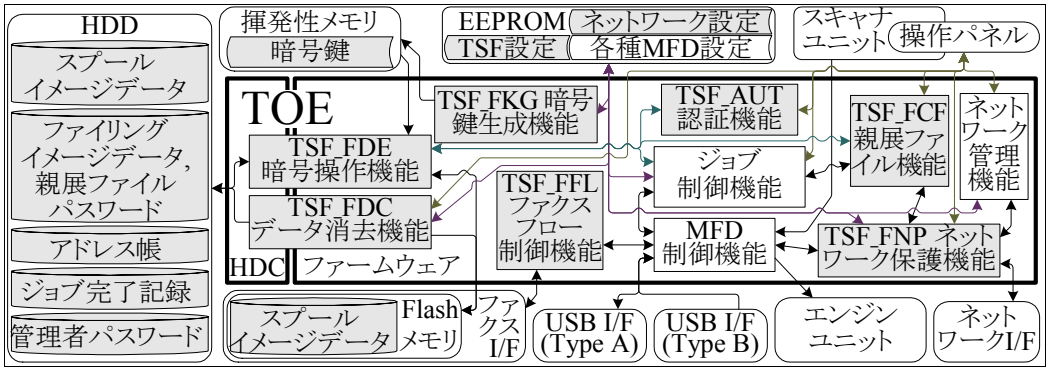

図 3: TOEの論理的構成図

j) 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

日本向け	取扱説明書データセキュリティキット MX-FR11 [CINSJ4570FC52]	注意書データセキュリティキット MX-FR11 [TCADJ2013FCZ1]
日本以外向け	MX-FR11 Data Security Kit Operation Manual [CINSZ4571FC52]	MX-FR11 Data Security Kit Notice [TCADZ2014FCZ1]

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。

a) 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

b) 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

c) アドレス帳データ

d) ジョブ完了記録データ

e) ネットワーク設定データ

f) 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。

ジョブ完了またはキャンセルの際、MFD は資源の割当て解除のために上記のイメージデータを削除する。この削除とは、管理領域に削除情報を与えることによって、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とであり、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ジョブにより再利用されるまでの間、削除されたイメージデータは残存し得る。そこで本 ST は、MFD 内の HDD または Flash メモリに残存する削除済みイメージデータを保護資産に含める。

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、前節と同様、削除後も HDD に残存し得る。HDD に残存する削除済みイメージ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。

a) TCP/IP 設定: TCP/IP 有効設定, DHCP 有効設定, IP アドレス設定
b) DNS 設定: プライマリ/セカンダリ DNS サーバ, ドメイン名
c) 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
d) SMTP 設定: SMTP サーバ
e) LDAP 設定: LDAP 有効設定, LDAP サーバ
f) 連結印刷設定: 子機 IP アドレス, 連結送信禁止
g) 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。

1.4.5 TOE の関係者

本節では、本 TOE、及び、本 TOE を搭載する 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。
- 利用者: TOE 及び MFD の MFD 機能 (1.3.5 節) を使用する人物。

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。いずれも、基本的な攻撃能力 (basic attack potential) を持つ攻撃者を想定している。表 3.1: 脅威

識別子	定義
T.RECOVER	攻撃者が、MFDからMSDを取り出し、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

組織のセキュリティ方針を表 3.2 に示す。

表 3.2: 組織のセキュリティ方針

識別子	定義
P.RESIDUAL	ジョブ完了または中止時、MSDにスプール保存された利用者データの領域は、少なくとも1回上書き消去されなければならない。 MSDにおいて、利用者が削除した利用者データの領域は、少なくとも1回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、MSDの利用者データの領域はすべて、少なくとも1回上書き消去されなければならない。
P.FAXTONET	MFDのファクスI/Fに接続される電話回線網からは、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを、できないようにしなければならない。

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	TOEを搭載する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、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利用者が使用する機器からの、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は、正当な管理者を識別認証する機能を提供する。
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、ジョブ完了または中止時、MSDにスプール保存された利用者データの領域を、少なくとも1回上書き消去する。 TOEは、利用者の削除操作により、指定されたMSDの利用者データの領域を、少なくとも1回上書き消去する。 TOEは、管理者の操作により、MSDの利用者データの領域全体を少なくとも1回上書き消去する機能を提供する。
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。
O.FAXTONET	TOEは、MFDのファクスI/Fに接続される電話回線網からの、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを防ぐ。

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: 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、IPsec機能およびSNMP v3機能を使う。すなわち、TOEおよびMFDの利用者に対して、各方式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.ERASEALL	管理者は、MFDの廃棄または所有者変更の際、TOEの機能を用いて、MSDの利用者データ領域全体を少なくとも1回上書き消去する。
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.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。

識別子	定義
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

セキュリティ課題定義に示した脅威、組織のセキュリティ方針、前提条件に対して、セキュリティ対策方針で示した対策が有効であることを表 4.3 に検証する。表 4.3 は、脅威、組織のセキュリティ方針、前提条件の対応について、その根拠を記載している節番号を示したものである。

表 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	P.RESIDUAL	P.FAXTONET	A.NETWORK	A.OPERATOR
O.FILTER		4.3.1.2							
O.MANAGE		4.3.1.2	4.3.1.3	4.3.1.4	4.3.1.5	4.3.2.1			
O.REMOVE	4.3.1.1								
O.RESIDUAL						4.3.2.1			
O.TRP					4.3.1.5				
O.USER			4.3.1.3						
O.FAXTONET							4.3.2.2		
OE.CIPHER					4.3.1.5				
OE.ERASEALL						4.3.2.1			
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、O.REMOVE が定める通り、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、基本的な攻撃能力を持つ攻撃者が、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。

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、基本的な攻撃能力を持つ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 が定める通り、TOE は、MFD へのアクセスを認められていない利用者が使用する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 が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- 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 が定める通り、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 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 が定める通り、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 が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- 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 が定める通り、管理者が TOE および MFD の利用者に行わせる。

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 が定める通り、TOE は正当な管理者を識別認証する機能を提供する。これにより、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 が定める通り、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 が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。
- 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 (O.TRP が定める TSF を使用すること、または MFD が TSF の使用に適応しない環境にある場合にその他の保護手段) 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

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組織のセキュリティ方針を実施できる根拠を示す。

4.3.2.1 P.RESIDUAL

P.RESIDUAL は、以下の対策により実施できる。

- O.RESIDUAL が定める通り、TOE は、ジョブ完了または中止時、MSD にスプール保存された利用者データの領域を、少なくとも 1 回上書き消去する。
- O.RESIDUAL が定める通り、TOE は、利用者の削除操作により、指定された MSD の利用者データの領域を、少なくとも 1 回上書き消去する。
- OE.ERASEALL が定める通り、管理者は、MFD の廃棄または所有者変更の際、MSD の利用者データ領域全体を少なくとも 1 回上書き消去する。そのためには TOE の支援が必要であり、次項の機能が利用できる。
- O.RESIDUAL が定める通り、TOE は、管理者の操作により MSD の利用者データ領域全体を少なくとも 1 回上書き消去する機能を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。

これらの対策により、P.RESIDUAL は実施可能である。

4.3.2.2 P.FAXTONET

P.FAXTONET に対して、O.FAXTONET が定める通り、TOE は、MFD のファクス I/F に接続される電話回線網からの、MFD のネットワーク I/F を経由しての内部ネットワークへのアクセスを防ぐ。これにより、P.FAXTONET は実施可能である。

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 を搭載する 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、英小文字 a, b, c, … 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.1a 暗号鍵生成 a

下位階層: なし

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_CKM.1.1a 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-R2 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。

FCS_CKM.1b 暗号鍵生成 b

下位階層: なし

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_CKM.1.1b 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-R2 拡張アルゴリズム]と指定された暗号鍵長[256 ビット]に従って、暗号鍵を生成しなければならない。

FCS_COP.1a 暗号操作 a

下位階層: なし

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

FCS_COP.1.1a 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 メモリに書き込む利用者データの暗号化
- Flash メモリから読み出した利用者データの復号

]を実行しなければならない。

FCS_COP.1b 暗号操作 b

下位階層: なし

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

FCS_COP.1.1b 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[256 ビット]に従って、[

- HDD に書き込む利用者データの暗号化
- HDD に書き込む TSF データの暗号化
- HDD から読み出した利用者データの復号
- HDD 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。

6.2.2 クラス FDP: 利用者データ保護

FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 TSF は、[

- サブジェクト: ファクス回線からファクス I/F への受信、ネットワーク IF から内部ネットワークへの送信
- 情報: ファクス回線からファクス I/F へ受信したデータ
- 操作: ファクス I/F からネットワーク I/F へ中継する

]に対して[ファクス情報フロー制御 SFP]を実施しなければならない。

FDP_IFF.1 単純セキュリティ属性

下位階層: なし

依存性: FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

FDP_IFF.1.1 TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[ファクス情報フロー制御 SFP]を実施しなければならない。: [

● ファクス回線からファクス I/F への受信 (サブジェクト): セキュリティ属性なし
● ネットワーク I/F から内部ネットワークへの送信 (サブジェクト): セキュリティ属性なし
● ファクス回線からの通信データ (情報): セキュリティ属性なし
]

FDP_IFF.1.2 TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [決して許可しない]。

FDP_IFF.1.3 TSF は、[なし (追加の情報フロー制御 SFP 規則)]を実施しなければならない。

FDP_IFF.1.4 TSF は、以下の規則、[なし]に基づいて、情報フローを明示的に許可しなければならない。

FDP_IFF.1.5 TSF は、以下の規則、[なし]に基づいて、情報フローを明示的に拒否しなければならない。

FDP_RIP.1 サブセット残存情報保護

下位階層: なし

依存性: 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。

6.2.3 クラス FIA: 識別と認証

FIA_AFL.1a 認証失敗時の取り扱い a

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1a 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.1.2a 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。

FIA_AFL.1b 認証失敗時の取り扱い b

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1b 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.1.2b 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。

FIA_SOS.1a 秘密の検証 a

下位階層: なし

依存性: なし

FIA_SOS.1.1a 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、すなわち ISO/IEC 646 情報交換用符号化文字集合における 32 番から 126 番まで 95 種の文字] 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。

FIA_SOS.1b 秘密の検証 b

下位階層: なし

依存性: なし

FIA_SOS.1.1b 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。

FIA_UAU.2a アクション前の利用者認証 a

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1a 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。

FIA_UAU.2b アクション前の利用者認証 b

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1b 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。

FIA_UAU.7a 保護された認証フィードバック a

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.7.1a 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。

FIA_UAU.7b 保護された認証フィードバック b

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.7.1b 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。

FIA_UID.2a アクション前の利用者識別 a

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1a 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。

FIA_UID.2b アクション前の利用者識別 b

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1b 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。

6.2.4 クラス FMT: セキュリティ管理

FMT_MOF.1a セキュリティ機能のふるまいの管理 a

下位階層: なし

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_MOF.1.1a 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, アドレス帳/本体内登録データ消去, ジョブ状況完了エリア消去] *[を動作させる]* 能力を[管理者]に制限しなければならない。

FMT_MOF.1b セキュリティ機能のふるまいの管理 b

下位階層: なし

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_MOF.1.1b 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。

FMT_MOF.1c セキュリティ機能のふるまいの管理 c

下位階層: なし

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_MOF.1.1c TSF は、機能[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, ドキュメントファイリング機能, ネットワーク保護機能] *[のふるまいを改変する]* 能力を[管理者]に制限しなければならない。

FMT_MTD.1a TSF データの管理 a

下位階層: なし

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.1.1a 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。

FMT_MTD.1b TSF データの管理 b

下位階層: なし

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.1.1b TSF は、[親展ファイルパスワード]を*[改変、* [作成 (*その他の操作*)] *]* 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。

FMT_MTD.1c TSF データの管理 c

下位階層: なし

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.1.1c TSF は、[
- IP アドレスフィルタ
- MAC アドレスフィルタ
- SSL 設定
- IPsec 設定
- SNMP 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。

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: 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。: [
- 全データエリア消去の起動および中止
- ドキュメントファイリングデータ消去の起動および中止
- 電源 ON 時の自動消去の中止
- アドレス帳/本体内登録データ消去の起動
- ジョブ状況完了エリア消去の起動
- 各ジョブ完了後の自動消去回数の設定
- データエリア消去回数の設定
- 電源 ON 時の自動消去の対象別有効設定
- 電源 ON 時の自動消去回数の設定
- 親展ファイルのロック解除
- 管理者パスワードの改変
- 親展ファイルパスワードの改変
- 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
- IP アドレスフィルタおよび MAC アドレスフィルタの管理
- SSL 保護対象サービスの管理
- IPsec 設定
- SNMP 設定

]

注: 管理要件への考慮は 6.4.1.9 *節で述べる。*

FMT_SMR.1a セキュリティの役割 a

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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

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

FMT_SMR.1b セキュリティの役割 b

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1b 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.1.2b TSF は、利用者を役割に関連づけなければならない。

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

依存性: 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。

6.2.6 クラス FTP: 高信頼パス/チャネル

FTP_ITC.1 TSF 間高信頼チャネル

下位階層: なし

依存性: なし

FTP_ITC.1.1 TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び **暴露** (改変や暴露) からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSF は、*[TSF]* が、 **IPsec** (高信頼チャネル) を介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3 TSF は、[

- プリンタ機能のうちプルプリント機能
- スキャナ機能

]のために、高信頼チャネルを介して通信を開始しなければならない。

FTP_TRP.1 高信頼パス

下位階層: なし

依存性: 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、*[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、 **HTTPS, IPP-SSL, IPsec, SNMPv3** (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 における管理者認証、親展ファイルの再操作、アドレス帳の読み出し、アドレス帳の改変、フィルタ設定およびネットワーク設定
- プリンタ機能におけるプリンタドライバからのイメージデータ受け取り
- プリンタ機能におけるプッシュプリントのためのイメージデータ受け取り
- MIB に基づく遠隔 MFD 管理

(*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。

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、そのままセキュリティ保証要件として使用する。

- 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
- ASE クラス: セキュリティターゲット評価
  - ASE_CCL.1 — 適合主張
  - ASE_ECD.1 — 拡張コンポーネント定義
  - ASE_INT.1 — ST 概説
  - ASE_OBJ.2 — セキュリティ対策方針
  - ASE_REQ.2 — 導き出されたセキュリティ要件
  - ASE_SPD.1 — セキュリティ課題定義
  - ASE_TSS.1 — TOE 要約仕様
- 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。

6.4.1 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 6.1 に示す。表 6.1 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 6.1: 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	O.FAXTONET
FCS_CKM.1a			6.4.1.3				
FCS_CKM.1b			6.4.1.3				
FCS_COP.1a			6.4.1.3				
FCS_COP.1b			6.4.1.3				
FDP_IFC.1							6.4.1.7
FDP_IFF.1							6.4.1.7
FDP_RIP.1				6.4.1.4			
FIA_AFL.1a		6.4.1.2					
FIA_AFL.1b						6.4.1.6	
FIA_SOS.1a		6.4.1.2					
FIA_SOS.1b						6.4.1.6	
FIA_UAU.2a		6.4.1.2					
FIA_UAU.2b						6.4.1.6	
FIA_UAU.7a		6.4.1.2					
FIA_UAU.7b						6.4.1.6	
FIA_UID.2a		6.4.1.2					
FIA_UID.2b						6.4.1.6	
FMT_MOF.1a				6.4.1.4			
FMT_MOF.1b				6.4.1.4			
FMT_MOF.1c				6.4.1.4	6.4.1.5	6.4.1.6	
FMT_MTD.1a		6.4.1.2					
FMT_MTD.1b						6.4.1.6	
FMT_MTD.1c	6.4.1.1			6.4.1.4	6.4.1.5	6.4.1.6	
FMT_SMF.1	6.4.1.1	6.4.1.2		6.4.1.4	6.4.1.5	6.4.1.6	
FMT_SMR.1a		6.4.1.2					
FMT_SMR.1b						6.4.1.6	
FTA_TSE.1	6.4.1.1						
FTP_ITC.1					6.4.1.5		
FTP_TRP.1					6.4.1.5		

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.1c 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.1c は一貫して FTA_TSE.1 の管理を規定し、これらの間で競合は発生しない。

以上から、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.1a, FIA_UAU.2a, FIA_UAU.7a および FIA_UID.2a によって、管理者を識別および認証する。

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) FIA_SOS.1a により、管理者パスワードを改変する際、管理者パスワードが 5 文字以上 32 文字以下の英数記号であることが保証される。

d) FMT_MTD.1a 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。

e) FMT_SMR.1a 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。

上記 a) は管理者識別認証の事象に関するものであり、b), c) および d) は管理者パスワード改変の事象に関するものである。これら二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、管理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 d) の三つの機能要件は、管理者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 d) 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.MANAGE を実現する上で、機能要件の競合は発生しない。

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.1a および FCS_COP.1b 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.1a および FCS_CKM.1b により、各々FCS_COP.1a および FCS_COP.1b を実施するための暗号鍵を生成する。

FCS_COP.1a および FCS_CKM.1a は、Flash メモリの暗号操作に関し相互依存である。FCS_COP.1b および FCS_CKM.1b は、HDD の暗号操作に関し相互依存である。Flash メモリおよび HDD の間で競合する要因はない。以上から、O.REMOVE を実現する上で、機能要件の競合は発生しない。

6.4.1.4 O.RESIDUAL

O.RESIDUAL は、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、管理者の操作により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。

b) FMT_SMF.1 にて、FDP_RIP.1 に関する管理機能を提供する。

c) 以下の各機能要件にて、FDP_RIP.1 に関する管理能力は、管理者に制限される。
   - FMT_MOF.1a にて、FDP_RIP.1 に関する TSF のうち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、アドレス帳/本体内登録データ消去、ジョブ状況完了エリア消去、および、電源 ON 時の自動消去の各機能を動作させる能力が、管理者に制限される。

- FMT_MOF.1b にて、FDP_RIP.1 に関する TSF のうち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、および、電源 ON 時の自動消去の各機能を停止する能力が、管理者に制限される。
- FMT_MOF.1c にて、FDP_RIP.1 に関する TSF のうちドキュメントファイリングデータ消去機能および電源 ON 時の自動消去機能のふるまいを改変する能力が、管理者に制限される。
- FMT_MTD.1c にて、FDP_RIP.1 に関する TSF データ、すなわち、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、および、電源 ON 時の自動消去回数を、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 c) の各事象は独立事象なので、c) の各機能要件は互いに競合しない。また、b) および c) は相互補完的に a) の管理を規定するので、それらの間で競合はない。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。

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_ITC.1 および FTP_TRP.1 の組み合わせにより、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が提供される。
- FMT_MOF.1c により、FTP_ITC.1 および FTP_TRP.1 に関する TSF すなわちネットワーク保護機能のふるまいを改変する能力は、管理者に制限される。
- FMT_MTD.1c により、FTP_ITC.1 および FTP_TRP.1 に関する TSF データ、すなわち SSL 設定、IPsec 設定、SNMP 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_MOF.1c, FMT_MTD.1c および FMT_SMF.1 は相互補完的に FTP_ITC.1 および FTP_TRP.1 の管理を規定し、これらの間で競合は発生しない。FTP_TRP.1 は TOE が提供する通信サービスをリモート利用者が利用する事象であり、FTP_ITC.1 は TOE が提供するリモート高信頼 IT 製品との通信機能をローカル利用者が利用する事象である。この二つの事象は独立に発生し、相互に競合しない。以上から、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.1b, FIA_UAU.2b, FIA_UAU.7b および FIA_UID.2b 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.1b 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_MOF.1c にて、O.USER を実施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) のふるまいを改変する能力が、管理者に制限される。

d) FMT_MTD.1b 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。

e) FMT_MTD.1c にて、親展ファイルによる保護の実効性に関わる TSF のふるまい管理能力、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。

f) FMT_SMR.1b 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。

g) 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。

h) FIA_AFL.1b にて、親展ファイルのロック解除操作の能力は、管理者に制限される。

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), d) および g) 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、c), e) および h) 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), d), および g) 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。c), e) および h) の二つの機能要件は、管理者による管理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。f) は d) 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 O.FAXTONET

O.FAXTONET は、機能要件 FDP_IFC.1 および FDP_IFF.1 の組み合わせにより実現できる。

これら二つの機能要件は、ファクス回線からの通信データに対し、内部ネットワークへ中継することを決して許可しないようなフロー制御を実施する。これにより、MFD のファクス I/F に接続される電話回線網からの、MFD のネットワーク I/F を経由しての内部ネットワークへのアクセスを防ぐ。

O.FAXTONET を実現する二つの機能要件は、互いに依存する機能要件であるので、競合しない。

6.4.1.8 セキュリティ機能要件全体の一貫性根拠

6.4.1.1 節から 6.4.1.7 節に示すとおり、それぞれの TOE のセキュリティ対策方針を実現するセキュリティ機能要件の間には、競合は発生せず、一貫している。また、表 4.1 に示すとおり、TOE のセキュリティ対策方針は、それぞれ独立しており、相互に競合するものではない。すなわち、TOE のセキュリティ対策方針の間には、競合は発生せず、一貫している。

以上から、TOE のセキュリティ対策方針を実現するセキュリティ機能要件全体においても、競合は発生せず、一貫している。

6.4.1.9 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 パート 2 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 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 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.1a	—	(管理要件なし)
FCS_CKM.1b	—	(管理要件なし)
FCS_COP.1a	—	(管理要件なし)
FCS_COP.1b	—	(管理要件なし)
FDP_IFC.1	—	(管理要件なし)
FDP_IFF.1	—	属性はない
FDP_RIP.1	• 全データエリア消去の起動および中止 •ドキュメントファイリングデータ消去の起動および中止 • 電源ON時の自動消去の中止 • アドレス帳/本体内登録データ消去の起動 • ジョブ状況完了エリア消去の起動 • 各ジョブ完了後の自動消去回数の設定 • データエリア消去回数の設定 • 電源ON時の自動消去の対象別有効設定 • 電源ON時の自動消去回数の設定	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.1a	—	閾値とアクションは固定
FIA_AFL.1b	• 親展ファイルのロック解除	閾値とアクションは固定
FIA_SOS.1a	—	品質尺度は固定
FIA_SOS.1b	—	品質尺度は固定
FIA_UAU.2a	• 管理者パスワードの改変	管理要件に合致
FIA_UAU.2b	• 親展ファイルパスワードの改変 •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	管理要件に合致
FIA_UAU.7a	—	(管理要件なし)
FIA_UAU.7b	—	(管理要件なし)
FIA_UID.2a	—	管理者の識別は固定
FIA_UID.2b	—	各親展ファイル保存者の識別は固定
FMT_MOF.1a	—	役割のグループはない
FMT_MOF.1b	—	役割のグループはない
FMT_MOF.1c	—	役割のグループはない
FMT_MTD.1a	—	役割のグループはない
FMT_MTD.1b	—	役割のグループはない
FMT_MTD.1c	—	役割のグループはない
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1a	—	利用者のグループはない
FMT_SMR.1b	—	利用者のグループはない
FTA_TSE.1	• IPアドレスフィルタおよびMACアドレスフィルタの管理	管理要件に合致
FTP_ITC.1	• IPsec設定	管理要件に合致
FTP_TRP.1	• SSL保護対象サービスの管理 • IPsec設定 • SNMP設定	管理要件に合致

6.4.1.10 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。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 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: 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.1a	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1a	FCS_CKM.4	J1
FCS_CKM.1b	同上	FCS_COP.1b	FCS_CKM.4	J1
FCS_COP.1a	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1a	FCS_CKM.4	J1
FCS_COP.1b	同上	FCS_CKM.1b	FCS_CKM.4	J1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	—	—
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1	FMT_MSA.3	J2
FDP_RIP.1	—	—	—	—
FIA_AFL.1a	FIA_UAU.1 *	FIA_UAU.2a	—	—
FIA_AFL.1b	FIA_UAU.1 *	FIA_UAU.2b	—	—
FIA_SOS.1a	—	—	—	—
FIA_SOS.1b	—	—	—	—
FIA_UAU.2a	FIA_UID.1 *	FIA_UID.2a	—	—
FIA_UAU.2b	FIA_UID.1 *	FIA_UID.2b	—	—
FIA_UAU.7a	FIA_UAU.1 *	FIA_UAU.2a	—	—
FIA_UAU.7b	FIA_UAU.1 *	FIA_UAU.2b	—	—
FIA_UID.2a	—	—	—	—
FIA_UID.2b	—	—	—	—
FMT_MOF.1a	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MOF.1b	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MOF.1c	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1b	—	—
FMT_MTD.1c	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1a	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1a	FIA_UID.1 *	FIA_UID.2a	—	—
FMT_SMR.1b	FIA_UID.1 *	FIA_UID.2b	—	—
FTA_TSE.1	—	—	—	—
FTP_ITC.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。
J2	FMT_MSA.3	ファクス情報フロー制御SFPは、対象の情報フローを決して許可しない。よって、SFP実施のためにセキュリティ属性を扱う必要はなく、セキュリティ属性の初期値を規定するFMT_MSA.3は不要。

6.4.2 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、主要な脅威は、基本的な攻撃能力を持つ攻撃者が、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、商用として十分である EAL3 を評価保証レベルとする。

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、セキュリティ機能要件が満たされることを示す。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	TSF_FFL
FCS_CKM.1a	7.1						
FCS_CKM.1b	7.1						
FCS_COP.1a		7.2					
FCS_COP.1b		7.2					
FDP_IFC.1							7.7
FDP_IFF.1							7.7
FDP_RIP.1			7.3				
FIA_AFL.1a			7.3	7.4		7.6	
FIA_AFL.1b					7.5		
FIA_SOS.1a				7.4			
FIA_SOS.1b					7.5		
FIA_UAU.2a			7.3	7.4		7.6	
FIA_UAU.2b					7.5		
FIA_UAU.7a			7.3	7.4		7.6	
FIA_UAU.7b					7.5		
FIA_UID.2a			7.3	7.4		7.6	
FIA_UID.2b					7.5		
FMT_MOF.1a			7.3				
FMT_MOF.1b			7.3				
FMT_MOF.1c			7.3		7.5	7.6	
FMT_MTD.1a				7.4			
FMT_MTD.1b					7.5		
FMT_MTD.1c			7.3		7.5	7.6	
FMT_SMF.1			7.3	7.4	7.5	7.6	
FMT_SMR.1a				7.4			
FMT_SMR.1b					7.5		
FTA_TSE.1						7.6	
FTP_ITC.1						7.6	
FTP_TRP.1						7.6	

7.1 暗号鍵生成 (TSF_FKG)

TOE は、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。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、MSN-R2 拡張アルゴリズムを用いて 128 ビット長および 256 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-R2 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。

よって、本 TOE は FCS_CKM.1a および FCS_CKM.1b を満たす。

7.2 暗号操作 (TSF_FDE)

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、必ず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。

対象となる利用者データは以下の通り:

- 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 データは以下の通り:

- 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

上記 Flash メモリ上の利用者データの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、および、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。よって、本 TOE は FCS_COP.1a を満たす。

上記 HDD 上の利用者データおよび TSF データの暗号化および復号には、同じく 256 ビット長の暗号鍵を用いる。よって、本 TOE は FCS_COP.1b 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 回以上上書きする。また, Flash メモリには固定値を 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。
- 本 TSF は FMT_SMF.1 および FMT_MOF.1a に従い、上記 b), c), d), e) および f) の起動を、TSF_AUT で識別認証された管理者に許す。
- 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.1a, FIA_UAU.2a, FIA_UAU.7a および FIA_UID.2a を満たす。中止機能は FIA_UID.2a および FIA_UAU.2a に従い管理者識別認証を要求する。認証の際 FIA_UAU.7a のフィードバック保護および FIA_AFL.1a の失敗対応を行う。これにより、FMT_MOF.1b 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_MOF.1c および FMT_MTD.1c 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通り、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.2a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.2aが定める管理者認証である。

認証入力中, TOEはFIA_UAU.7a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.1a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を有効にする消去対象データの設定。既定値はすべて無効。
  FMT_MTD.1.1.c における “電源 ON 時の自動消去の対象別有効設定” に該当する。
- 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.1a 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す。このとき、FIA_SOS.1a に従い、長さ 5 文字以上 32 文字以下で、ISO/IEC 646 情報交換用符号化文字集合における 32 番から 126 番まで 95 種の文字から成るパスワードのみを受け入れる。各文字の字形は実行環境により異なるが、例えば次のとおり。

- 英字 52 種: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
- 数字 10 種: 0 1 2 3 4 5 6 7 8 9
- 記号 33 種: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ および空白。

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.1a, FIA_UAU.2a, FIA_UAU.7a および FIA_UID.2a を満たす。

FIA_UID.2a 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.2a 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.7a 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、FIA_AFL.1a 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.1a 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.1b 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.2b 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.2b に従い正しい親展ファイル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.7b 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。

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.1b 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.1b 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、本 TSF で識別認証された親展ファイル保存者のみに提供し、FIA_SOS.1b に従い、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.1b 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.1b 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, FMT_MOF.1c, FMT_MTD.1c および FIA_AFL.1b 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

上記の各要素は、以下のとおり SFR に対応する。

- 上記 a) は FTA_TSE.1 を満たす。
- 上記 b) は FTP_ITC.1 および FTP_TRP.1 を満たし、TSF_FDC および TSF_FCF と共同で FMT_MOF.1c を満たす。
- c) は TSF_FDC および TSF_AUT と共同で FIA_AFL.1a, FIA_UAU.2a, FIA_UAU.7a および FIA_UID.2a を満たす。
- a), b), TSF_FDC および TSF_FCF の共同で FMT_MTD.1c 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.1c 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

本 TSF は、次の通信データ保護機能を提供する。

- クライアントと TOE の Web との通信を、盗聴より保護できるよう、FTP_TRP.1 に従い HTTPS 通信機能を提供する。HTTPS 通信は、リモート利用者がクライアント上の Web ブラウザから接続することにより開始し、切断されるまで通信を維持する。
- 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、盗聴より保護できるよう、FTP_TRP.1 に従い IPP-SSL 通信機能を提供する。IPP-SSL 通信は、リモート利用者がクライアント上のアプリケーションプログラム等で印刷操作を行うことにより、クライアントのプリンタドライバから接続することによって開始し、切断されるまで通信を維持する。
- クライアントと TOE との SNMP を利用した通信 (MIB に基づく遠隔 MFD 管理) を、盗聴より保護できるよう、FTP_TRP.1 に従い SNMP v3 機能を提供する。リモート利用者がクライアント上の SNMP マネージャから要求を発し、TOE より応答を返す。
- クライアントと TOE との IP を利用したすべての通信を、盗聴より保護できるよう、FTP_ITC.1 および FTP_TRP.1 に従い IPsec 機能を提供する。これにより、上記 Web, プリンタドライバおよび SNMP に加え、以下の通信が保護される。
  - ローカル利用者が MFD のプルプリント機能を利用し FTP サーバまたは共有フォルダのイメージデータを取得するための通信。これは FTP_ITC.1 に対応する。

- ローカル利用者が MFD のスキャナ機能を利用し、イメージデータを送信するための通信。これは FTP_ITC.1 に対応する。
- リモート利用者が MFD のプッシュプリント機能を利用するためイメージデータを MFD へ送り込むための通信。これは FTP_TRP.1 に対応する。

HTTPS 通信、および IPP-SSL 通信において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.1c 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、IPsec 通信に関する設定値である IPsec 設定、および SNMP v3 通信に関する設定値である SNMP 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。

HTTPS 通信、IPP-SSL 通信、IPsec 通信、および SNMP v3 通信の使用/未使用 (無効) の設定によって、ネットワーク保護機能の動作を変更することができる。HTTPS 通信、IPP-SSL 通信、IPsec 通信、および SNMP v3 通信を未使用にした場合、ネットワーク保護機能は各々が無効の状態で動作する。本 TSF は FMT_MOF.1c に従い、このふるまい変更を、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.2a, FIA_UAU.2a, FIA_UAU.7a および FIA_AFL.1a に従って実施される。

7.7 ファクスフロー制御 (TSF_FFL)

本 TSF は、FDP_IFC.1 および FDP_IFF.1 に従い、ファクス回線からの通信データに対し、内部ネットワークへ中継することを決して許可しないようなフロー制御を実施する。これにより、MFD のファクス I/F に接続される電話回線網からの、MFD のネットワーク I/F を経由しての内部ネットワークへのアクセスを防ぐ。

8 付章

本章では、用語の定義を示す。

8.1 専門用語

本 ST で使用している専門用語を表 8.1 に示す。

表 8.1: 専門用語

用語	定義
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)。
IPアドレス	IPにおいて通信相手となる各機器を識別するための呼出符号。
IPアドレスフィルタ	通信相手を制限する機能であって、相手側機器のIPアドレスに基づき通信の可否を判断するもの。
MACアドレス	MACにおいて通信媒体上の各機器を識別するための呼出符号。
MACアドレスフィルタ	通信相手を制限する機能であって、相手側機器のMACアドレスに基づき通信の可否を判断するもの。
MSN-R2拡張アルゴリズム	データセキュリティキット用暗号基準書に規定されている、シャープ株式会社独自の暗号鍵生成アルゴリズム。
TWAIN	スキャナ等の装置からPCがイメージデータを入力するための技術標準の一つ。
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	本書では特に、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。
管理者パスワード	セキュリティ管理機能等、TOE及びMFDの運用管理において重要な管理者専用の機能を、管理者以外に使用されないよう、保護するためのパスワード。
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、およびHDD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。

用語	定義
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。
連結印刷	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。
連結コピー	MFDのコピー機能における連結印刷のこと。
データセキュリティキット用暗号基準書	MFD用のデータセキュリティキットに用いる暗号操作アルゴリズム、および暗号操作に用いる暗号鍵の生成に関しての標準を規定した、シャープ株式会社内の文書。
データファイル	本書では、割り当てられたMSD資源からなり、情報 (イメージデータ等) を格納するオブジェクトを指す。
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。本書では、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はTOEのコントローラファームウェアに置き換えられる。
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。本書では特に、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。
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)
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-FR11 — MFDの別売オプション品。TOEのファームウェア部分を含む。
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) — MFD内のHDCはTOEのハードウェア部分を含む。
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)
IP	Internet Protocol — インターネットプロトコル。データを複数のパケットに分割し、宛先へ届ける通信プロトコルの名称。
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。
IPsec	Security Architecture for Internet Protocol — AH (Authentication Header) による完全性、認証機構、ESP (Encapsulated Security Payload) によるデータ暗号化、IKE (Internet Key Exchange protocol) による鍵交換から構成される、IPパケット単位でデータの改竄防止や秘匿機能を提供する通信プロトコルの名称。
IT	Information Technology (情報技術)
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。
MAC	Media Access Control (媒体アクセス制御) — 多数の通信機器が単一の通信媒体を共有できるよう、各機器を識別し、通信どうしが衝突しないよう調停する通信プロトコルの総称。
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、スキャナ機能およびファクス機能を有する。本書では、1.3.2節で識別する対象機種を指す。
MIB	Management Information Base — 管理情報ベース。ネットワーク機器の遠隔管理における管理情報の表現形式。SNMPのために必要である。
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)
OS	Operating System (オペレーティングシステム)
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。
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。
SNMP	Simple Network Management Protocol — ネットワーク機器を管理するための通信プロトコルの名称。
SNMP v3	SNMP version 3 — ネットワーク上を流れるSNMPパケットを認証、暗号化することにより、盗聴、なりすまし、改ざん、再送などの危険から保護する機能を実装したSNMP。
WINS	Windows Internet Name Service — NetBIOS名からIPアドレスを求めるための機能。