bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 全体制御ソフトウェア A2XK0Y0-0100-G00-56

セキュリティターゲット

バージョン：1.01

発行日：2012年8月24日

作成者：コニカミノルタビジネステクノロジーズ株式会社

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2011/10/27	1.00	第1オフィスSW開発部	廣田	多田	千葉	初版
2012/08/24	1.01	第1OPシステム制御開発部	鈴木	永田	千葉	誤植修正

—【 目次 】

—【 図目次 】

—【 表目次 】

1. ST 概説

1.1. ST 参照

・ST名称 : bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 **全体制御ソフトウェア** A2XK0Y0-0100-G00-56 セキュリティターゲット

・STバージョン : 1.01

・作成日 : 2012年8月24日

・作成者 : コニカミノルタビジネステクノロジーズ株式会社

1.2. TOE 参照

・TOE名称 : 日本語名：
bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 全体制御ソフトウェア
英語名 ：
bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software

・TOE識別 : A2XK0Y0-0100-G00-56

・TOEの種別 : ソフトウェア

・製造者 : コニカミノルタビジネステクノロジーズ株式会社

1.3. TOE 概要

本節では TOE 種別、TOE の使用方法及び主要なセキュリティ機能、TOE の動作環境について説明する。

1.3.1. TOE の種別

TOE である bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 全体制御ソフトウェアとは、MFP 制御コントローラ上の SSD にあって、MFP 全体の動作を統括制御する組み込み型ソフトウェアである。

1.3.2. TOE の使用方法、及び主要なセキュリティ機能

bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 とは、コピー、プリント、スキャン、FAX の各機能を選択、組み合わせて構成されるコニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機である。（以下、これらすべての総称として MFP と呼称する。）TOE は、MFP 本体のパネルやネットワークから受け付ける操作制御処理、画像データの管理等、MFP の動作全体を制御する“bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub

C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 全体制御ソフトウェア”である。

TOE は、MFP に保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。また MFP 内に画像データを保存する媒体である HDD が不正に持ち出される等の危険性に対して、ASIC を利用し、HDD に書き込まれる画像データを含むすべてのデータを暗号化することが可能である。他に TOE は、MFP を廃棄・リース返却する際に、各種上書き削除規格に則った削除方式により HDD 上の画像データを完全に削除する機能や、ファクス機能を踏み台として内部ネットワークにアクセスする危険性に対して、FAX 公衆回線網からのアクセスを制御する機能を有し、MFP を利用する組織の情報漏洩の防止に貢献する。また、TOE は監査ログ機能を有し、MFP の不正利用の検出に貢献する。

1.4. TOE 記述

1.4.1. TOE の利用に関係する人物の役割

TOE の搭載される MFP の利用に関連する人物の役割を以下に定義する。

- **ユーザ**
  MFP に登録される MFP の利用者。（一般には、オフィス内の従業員などが想定される。）

- **管理者**
  MFP の運用管理を行う MFP の利用者。MFP の動作管理、ユーザの管理を行う。（一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される。）

- **サービスエンジニア**
  MFP の保守管理を行う利用者。MFP の修理、調整等の保守管理を行う。（一般的には、コニカミノルタビジネステクノロジーズ株式会社と提携し、MFP の保守サービスを行う販売会社の担当者が想定される。）

- **MFP を利用する組織の責任者**
  MFP が設置されるオフィスを運営する組織の責任者。MFP の運用管理を行う管理者を任命する。

- **MFP を保守管理する組織の責任者**
  MFP を保守管理する組織の責任者。MFP の保守管理を行うサービスエンジニアを任命する。

この他に、TOE の利用者ではないが TOE にアクセス可能な人物として、オフィス内に出入りする人物などが想定される。

1.4.2. TOE の物理的範囲

1.4.2.1. 利用環境

TOE の搭載される MFP の利用が想定される一般的な利用環境を図 1 に示す。また以下に利用環境にて想定される事項について箇条書きで示す。

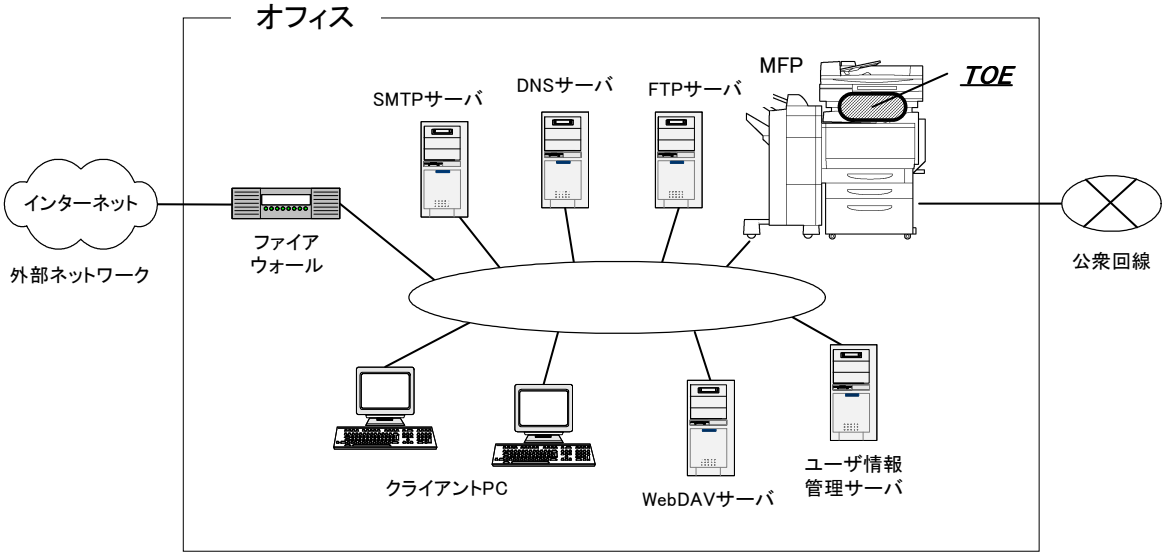

図 1　MFP の利用環境の例

- オフィス内部のネットワークとしてオフィス内 LAN が存在する。
- MFP はオフィス内 LAN を介してクライアント PC と接続され、相互にデータ通信を行える。
- オフィス内 LAN に SMTP サーバ、FTP サーバ、WebDAV サーバが接続される場合は、MFP はこれらともデータ通信を行うことが可能。（なお SMTP サーバ、FTP サーバ、WebDAV サーバのドメイン名を設定する場合は、DNS サービスが必要になる。）
- ユーザ ID、ユーザパスワードをサーバにて一元管理しているケースも想定する。この場合、ユーザ情報管理サーバにおけるユーザ登録情報を使って TOE は MFP へのアクセスを制御することが可能。
- オフィス内 LAN が外部ネットワークと接続する場合は、ファイアウォールを介して接続する等の措置が取られ、外部ネットワークから MFP に対するアクセスを遮断するための適切な設定が行われる。
- オフィス内 LAN は、スイッチングハブ等の利用、盗聴の検知機器の設置などオフィスの運用によって、盗聴されないネットワーク環境が整備されている。
- MFP に接続される公衆回線は、FAX や遠隔診断機能の通信に利用される。

1.4.2.2. 動作環境

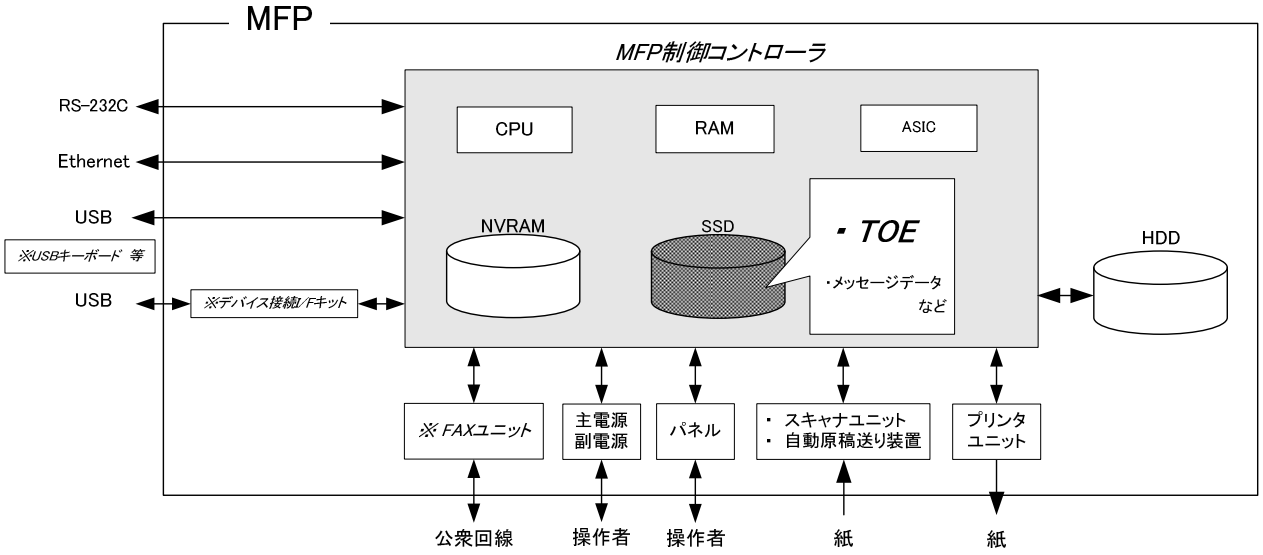

図 2 TOE に関係するハードウェア構成

TOE が動作するために必要な MFP 上のハードウェア環境の構成を図 2 に示す。MFP 制御コントローラは MFP 本体内に据え付けられ、TOE はその MFP 制御コントローラ上の SSD 上に存在し、ロードされる。

以下には図 2 にて示される MFP 制御コントローラ上の特徴的なハードウェア、MFP 制御コントローラとインタフェースを持つハードウェア、及びインタフェースを用いた接続について説明する。

- SSD

  TOE である MFP 全体制御ソフトウェアのオブジェクトコードが**保存**される記憶媒体。TOE の他に、パネルやネットワークからのアクセスに対するレスポンス等で表示するための各国言語メッセージデータ、TOE の処理に使われる MFP の動作において必要な様々な設定値等も保存される。

- NVRAM

  不揮発性メモリ。TOE の処理に使われる MFP の動作において必要な様々な設定値等が保存される記憶媒体。

- ASIC

  HDD に書き込まれるすべてのデータを暗号化するための HDD 暗号化機能を実装した特定利用目的集積回路。

- HDD

  容量 250GB のハードディスクドライブ。画像データがファイルとして保存されるほか、伸張変換などで一時的に画像データ、送信宛先データが保存される領域としても利用される。

- **主電源、副電源**

  MFP を動作させるための電源スイッチ。

- **パネル**
  タッチパネル液晶ディスプレイとテンキーやスタートキー、ストップキー、画面の切り替えキー等を備えた MFP を操作するための専用コントロールデバイス。

- **スキャナユニット／自動原稿送り装置**
  紙から図形、写真を読み取り、電子データに変換するためのデバイス。

- **プリンタユニット**
  MFP 制御コントローラから印刷指示されると、印刷用に変換された画像データを実際に印刷するためのデバイス。

- Ethernet
  10BASE-T、100BASE-TX、Gigabit Ethernet をサポート。

- USB
  外部メモリへの画像のコピー、外部メモリからの画像のコピーやプリント、TOE のアップデートなどを本インタフェースから実施できる。またオプションパーツの接続インタフェースとして対応している。オプションパーツには、Bluetooth 端末から画像のコピーやプリントを行う場合に必要となるデバイス接続 I/F キット、パネル操作でのキー入力を補完する USB キーボード[1]等があり、外部メモリ等を含め使用できるようにする必要がある。

- RS-232C
  D-sub9 ピンを介して、シリアル接続することが可能。故障時などに本インタフェースを介してメンテナンス機能を使用することができる。また公衆回線と接続されるモデムと接続して、遠隔診断機能（後述）を利用することも可能である。

- FAX ユニット（※オプションパーツ）
  公衆回線を介して FAX の送受信や遠隔診断機能（後述）の通信に利用される FAX 公衆回線ロをもつデバイス。販売上の都合により MFP には標準搭載されず、オプションパーツとして販売される。組織が希望する場合に購入するもので、FAX ユニットの搭載は必須ではない。

1.4.2.3. ガイダンス

- bizhub C554 / C454 / C364 / C284 / C224 サービスマニュアル　セキュリティ機能編
- bizhub C554 / C454 / C364 / C284 / C224 / C7828 / C7822 SERVICE MANUAL SECURITY FUNCTION
- ineo+ 554 / 454 / 364 / 284 / 224 SERVICE MANUAL　SECURITY FUNCTION
- bizhub C554 / C454 / C364 / C284 / C224 ユーザーズガイド　セキュリティ機能編
- bizhub C554 / C454 / C364 / C284 / C224 User's Guide [Security Operations]
- bizhub C7828 / C7822 User's Guide [Security Operations]
- ineo+ 554 / 454 / 364 / 284 / 224 User's Guide [Security Operations]

[1]表示言語が英語/フランス語/イタリア語/ドイツ語/スペイン語の場合のみ利用可能。セキュリティ機能には影響しない。

1.4.3. TOE の論理的範囲

利用者は、パネルやクライアント PC からネットワークを介して TOE の各種機能を使用する。以下には、基本機能、保存された画像ファイルを管理するためのボックス機能、利用者であるユーザの識別認証機能、管理者が操作する管理者機能、サービスエンジニアが操作するサービスエンジニア機能、ユーザには意識されずにバックグラウンドで動作する機能といった代表的な機能について説明する。

1.4.3.1. 基本機能

MFP には、基本機能としてコピー、プリント、スキャン、FAX といった画像に関するオフィスワークのための一連の機能が存在し、TOE はこれら機能の動作における中核的な制御を行う。MFP 制御コントローラ外部のデバイスから取得した生データを画像ファイルに変換し、RAM や HDD に保存する。（クライアント PC からのプリント画像ファイルは、複数の変換処理が行われる。）画像ファイルは、印刷用または送信用のデータとして変換され、目的の MFP 制御コントローラ外部のデバイスに転送される。

コピー、プリント、スキャン、FAX などの動作は、ジョブという単位で管理され、パネルからの指示により動作順位の変更、印字されるジョブであれば仕上がり等の変更、動作の中止が行える。

以下は基本機能においてセキュリティと関係する機能である。

- セキュリティ文書機能
  プリントデータと共にセキュリティ文書パスワードを受信した場合、画像ファイルを印刷待機状態で保存し、パネルからの印刷指示とパスワード入力により印刷を実行する。
  これよりクライアント PC からのプリント行為において、機密性の高いプリントデータが、印刷された状態で他の利用者に盗み見られる可能性や、他の印刷物に紛れ込む可能性を排除する。

- 認証＆プリント機能
  本機能を利用者が利用設定すると、通常のプリントデータを印刷待機状態で保存し、パネルからのユーザ認証処理で印刷を行う機能。利用設定がなくとも、プリントデータに本機能の動作指定がある場合は、利用者による利用設定がある場合と同様に動作する。

1.4.3.2. ボックス機能

画像ファイルを保存するための領域として、HDD にボックスと呼称されるディレクトリを作成できる。ボックスには、ユーザが占有する個人ボックス、登録されたユーザが一定数のグループを作って共同利用するための共有ボックス、所属部門のユーザ間で共有するグループボックスといった 3 つのタイプのボックスを設定することができる。個人ボックスは、所有するユーザだけに操作が制限され、共有ボックスは、そのボックスに設定されるパスワードを利用者間で共用することによって、アクセス制御を行っている。グループボックスは、その部門の利用を許可されたユーザだけに操作が制限される。

TOE は、パネル、またはクライアント PC からネットワークを介したネットワークユニットから伝達される操作要求に対して、ボックス、ボックス内の画像ファイルに対する以下の操作要求を処理する。

- ボックス内の画像ファイルの印刷、送信、クライアント PC からのダウンロード
  - 送信方法の 1 つである E-mail においてボックスファイルの暗号化（S/MIME）が可能
- ボックス内の画像ファイルの削除、他のボックスへの移動・コピー、外部メモリへのコピー
- ボックス内の画像ファイルの保存期間設定（期間経過後は自動的に削除）
- ボックスの名称変更、パスワードの変更、ボックスの削除など
- ボックスの属性設定（個人ボックス、共有ボックス、グループボックスの種別変更）

1.4.3.3. ユーザ認証機能

TOE は、MFP を利用する利用者を制限することができる。パネル、またはネットワークを介したアクセスにおいて TOE は MFP の利用を許可されたユーザであることをユーザ ID、ユーザパスワードを使って識別認証する。識別認証が成功すると、TOE はユーザに対して基本機能及びボックス機能などの利用を許可する。

ユーザ認証の方式には、以下に示すいくつかのタイプをサポートしている。

① **本体認証**[2]
MFP 制御コントローラ上の HDD にユーザ ID、ユーザパスワードを登録し、MFP にて認証する方式。

② **外部サーバ認証**
MFP 本体側でユーザ ID 及びユーザパスワードを管理せず、オフィス内 LAN で接続されるユーザ情報管理サーバ上に登録されるユーザ ID 及びユーザパスワードを用いて、MFP にて認証処理を行い、認証する方式。Active Directory[3]、NTLM[4]、NDS 等といった複数の方式をサポートしているが、本 ST において想定する外部サーバ認証の方式は、Active Directory の利用ケースのみとする。

1.4.3.4. 部門認証機能[5]

TOE は、MFP を利用する利用者を部門単位でグルーピングして管理することができる。部門認証には以下に示す方式がある。

① **ユーザ認証連動方式**
ユーザに予め部門 ID を設定し、ユーザの認証時に所属部門の部門 ID と関連づける方式

② **個別認証方式**
各部門 ID に設定される部門パスワードによって認証された場合に当該部門 ID と関連づける方式

1.4.3.5. 管理者機能

TOE は、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、本体認証の場合におけるユーザの情報の管理、ネットワークや画質等の各種設定の管理などの機能を提供する。

---

[2] 管理機能によりユーザが利用停止状態の時は、当該ユーザの認証機能は動作しない。
[3] Windows プラットフォームのネットワーク環境にてユーザ情報を一元管理するために Windows Server 2000（それ以降）が提供するディレクトリサービスの方式。
[4] NT LAN Manager の略。Windows プラットフォームのネットワーク環境にてユーザ情報を一元管理するために Windows NT が提供するディレクトリサービスにおいて利用される認証方式。
[5] 管理機能により部門が利用停止状態の時は、当該部門の認証機能は動作しない。

以下にはセキュリティに関係する機能について例示する。

- ユーザの登録管理
  - ユーザ ID、ユーザパスワードの登録・変更、ユーザの削除、ユーザの利用停止・再開
  - ユーザに対する部門 ID の関連付け変更
- 部門の登録管理
  - 部門 ID、部門パスワードの登録・変更、部門の利用停止・再開
- ボックスの設定管理
  - ボックスパスワードの登録・変更、ユーザ属性の管理
- システムオートリセットの動作設定
  - 設定時間が経過すると、自動的にログアウトする機能の設定
- ネットワーク設定管理
  - オフィス内 LAN との接続設定（DNS サーバの設定）
  - SMTP 設定（E-mail 送信にて利用する SMTP サーバの設定）
  - IP アドレス、NetBIOS 名、AppleTalk プリンタ名など
- NVRAM、SSD 及び HDD のバックアップ及びリストア機能
  - クライアント PC に導入される管理用のバックアップリストア・アプリケーションを利用して、ネットワークを介して実行される。
- HDD の全領域上書き削除機能
  - 各種軍用規格（米国国防総省規格等）に則ったデータ削除方式が存在
  - 起動すると、設定された方式に則り、HDD の全領域に対して上書き削除を実行する。
- HDD のフォーマット機能
  - 論理フォーマットが実行可能。
- 監査ログの閲覧及び削除機能
  - 監査ログをエクスポートし、ログの閲覧やログの削除が実行可能。
- 日時情報設定管理
  - TOE が保持する日時情報を設定。監査対象事象が発生した場合、ここで設定された日時情報が監査ログに記録される。
- FAX 設定管理（※FAX ユニット搭載時）
  - TSI 受信[6]の設定
  - PC-FAX 受信動作における FAX 出力先の設定（ボックス保存、または全ユーザ共通利用領域を設定可能）

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- ユーザ認証機能の方式設定
  - 本体認証、外部サーバ認証、ユーザ認証停止を選択
  - 部門認証機能との組み合わせを設定（ユーザ認証機能連動方式、部門個別認証方式）
- ユーザ：PUBLIC によるアクセスの設定
  - ユーザ ID で特定されない利用者の MFP 利用を許可、禁止を選択
- パスワード規約機能の設定
  - 各種パスワードの有効桁数等、パスワード諸条件をチェックする機能の動作、禁止を選択
- セキュリティ文書の認証方式及び認証操作禁止機能の設定
  - セキュリティ文書の認証に対して認証操作禁止機能が動作するモード、しないモードが存在

[6] Transmitting Subscriber Identification の略。送信者端末識別のこと。TSI 受信とは送信者毎に、**保存**すべきボックスを指定することができる機能である。

- 各認証機能における不成功認証の検出する機能の動作モードも連動
- 上記の動作モードを選択

- SNMPv1、v2 によるネットワーク設定変更機能の設定
  - SNMPv1、v2 による MIB の変更操作機能を許可、禁止を選択
- SNMPv3 の書込み操作における認証機能動作設定
  - 認証しない、認証動作のセキュリティレベルを選択
  - 認証動作のセキュリティレベルには、Authentication パスワードのみ、Authentication パスワード且つ Privacy パスワードを設定する場合が存在
- HDD 暗号化機能の設定
  - 動作、停止を選択
  - 動作選択時には、暗号化ワードを登録・変更
- ボックス一括管理機能の設定
  - ボックスの一括管理機能の許可、禁止を選択
- プリントキャプチャ機能の設定
  - プリント機能の故障時などに MFP が受信するプリントデータを確認するための機能
  - 上記機能を動作、停止を選択
- ネットワーク設定管理リセット機能の設定
  - ネットワーク設定管理リセット機能は、一連の項目を工場出荷値にリセットする。
  - 上記機能を許可、禁止を選択
- 高信頼チャネル（SSL/TLS 暗号通信）機能の設定
  - SSL/TLS サーバ証明書を生成、またはインポート
  - 通信に利用される暗号方式の設定
- 送信宛先データの設定
  - ボックスファイル送信などに利用される送信宛先、送信方法などを設定
  - S/MIME 証明書のインポート
- FTP サーバ機能の設定
  - 動作、停止を選択
- S/MIME 機能の設定
  - S/MIME 証明書自動登録機能の許可、禁止を選択
  - データ暗号化に利用される暗号方式の設定
- 認証&プリント機能の設定
  - 通常の印刷における認証&プリント機能を動作させる、させないを選択
- HDD データ上書き削除機能の設定
  - 削除方式を選択
- 監査ログ満杯時の動作設定
  - 監査ログ満杯時の動作設定を選択

1.4.3.6. サービスエンジニア機能

TOE は、サービスエンジニアだけが操作することが可能なサービスモードにて、管理者の管理、スキャナ・プリントなどのデバイスの微調整等のメンテナンス機能などを提供する。以下はセキュリティに関係する機能について例示する。

- 管理者パスワードの変更機能

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- CE[7]パスワードによるサービスエンジニアの認証の設定
  - 動作、停止を選択
- 遠隔診断機能（後述）の設定
  - 利用、禁止を選択することが可能。
- インターネット経由 TOE 更新機能の設定
  - 利用、禁止を選択することが可能。
- メンテナンス機能の設定
  - 利用、禁止を選択することが可能。
- HDD のフォーマット機能
  - 論理フォーマット、物理フォーマットが実行可能。
- HDD の装着設定
  - HDD をデータ保存領域として利用するには、明示的な装着設定が必要。
- イニシャライズ機能
  - 管理者、ユーザが設定した各種設定値、ユーザが保存したデータを削除する。

1.4.3.7. その他の機能

TOE はユーザには意識されないバックグラウンドで処理される機能や TOE の更新機能などを提供する。以下に代表的な機能について説明する。

- **暗号鍵生成機能**
  ASIC にて HDD へのデータ書き込み、読み込みにおいて暗号化・復号処理を実施する。(TOE は、暗復号処理そのものを行わない。)
  管理者機能にて本機能の動作設定を行う。動作させる場合は、TOE はパネルにて入力された暗号化ワードより暗号鍵を生成する。

- **遠隔診断機能**
  FAX 公衆回線ロや RS-232C を介したモデム接続、E-mail、WebDAV といった接続方式を利用して、コニカミノルタビジネステクノロジーズ株式会社が製造する MFP のサポートセンターと通信し、MFP の動作状態、印刷数等の機器情報を管理する。また必要に応じて適切なサービス（追加トナーの発送、課金請求、故障診断からサービスエンジニアの派遣など）を提供する。

- **TOE の更新機能**
  TOE は TOE 自身を更新するための機能を有する。更新手段は、遠隔診断機能の項目の 1 つとしても存在する他、Ethernet を介して FTP サーバよりダウンロードする方法（インターネット経由 TOE 更新機能)、外部メモリを接続して行う方法がある。

- **暗号通信機能**
  TOE はクライアント PC から MFP へ送信するデータ、MFP からダウンロードして受信するデータを SSL/TLS を利用して暗号化することができる。本機能は、管理者機能にて動作設定が行える。

- **S/MIME 証明書自動登録機能**
  S/MIME 用に各宛先に設定可能な証明書（ITU-T X.509 準拠）を自動登録する機能。メールに証明書が添付されている場合、当該メールのヘッダー情報にてユーザ ID を判別し、証明書を当該ユーザの証明書として登録する。

[7] Customer Service engineer の略称。

- **HDD データ上書き削除機能**
  HDD 上の不要になった画像データ領域に対し、上書き削除を実行する。削除パターンは管理者機能にて設定する。

- **監査ログ機能**
  監査対象事象が発生した場合、監査記録であるログを生成し、HDD に保存する機能。ログに対する操作は管理者のみに制限されており、ログのエクスポート及び削除が実施できる。

TOE は、標準では FAX ユニットが装着されていないため、FAX 公衆回線口が存在せず MFP を経由して内部ネットワークへアクセスされることは無い。但し、FAX ユニットを装着した場合は以下の機能を提供する。

- **FAX ユニット制御機能**
  FAX 公衆回線口から FAX ユニットを通じて、MFP に接続された内部ネットワークへのアクセスを禁止する。

TOE は外部エンティティである ASIC のセキュリティ機能（HDD 暗号化機能）を有効活用している。以下に代表的な外部エンティティと関係する機能について説明する。

- **ASIC の活用**
  外部エンティティである ASIC は、不正な持ち出し等への対処機能として、暗号化ワードを設定した場合に HDD 内のデータを暗号化する機能が動作する。

1.4.3.8. セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更すると警告画面が表示される。また、ネットワークを介した TOE の更新機能、ネットワーク設定管理初期化機能、遠隔診断機能による設定変更などの利用が禁止される、または利用の際に警告画面が表示される。

以下にセキュリティ強化機能有効時の一連の設定状態をまとめる。なお、セキュリティ強化機能を有効にするためには、管理者パスワード、CE パスワードを事前にパスワード規約に違反しない値に設定する等の事前準備が必要である。

- ユーザ認証機能 ：有効（本体認証、外部サーバ認証のどちらでも可）
- ユーザ：PUBLIC のアクセス ：禁止
- ユーザ名一覧表示 ：禁止
- 認証指定なしプリント ：禁止
- プリント簡易認証 ：禁止
- パスワード規約機能 ：有効
- 認証操作禁止機能の設定 ：認証失敗時 5 秒間のパネルのロック且つアカウントロック（失敗回数閾値：1～3 回）
- セキュリティ文書アクセス方式 ：認証操作禁止機能の設定と連動
- ボックス管理者機能 ：禁止
- SNMP v1/v2c Write 機能 ：禁止

- SNMPv3 による WriteUser 認証　：有効
- HDD 暗号化機能の設定　：有効
- プリントデータキャプチャ機能　：禁止
- ユーザによる宛先登録変更機能　：禁止
- SSL 暗号化強度の制限設定　：有効（3DES，AES のみ選択可能となる）
- SSL 対応プロトコル設定　：有効
- 管理者認証の操作禁止解除時間設定　：1～4 分の設定禁止
- CE 認証の操作禁止解除時間設定　：1～4 分の設定禁止
- FTP サーバ機能　：禁止
- S/MIME 証明書の自動取得　：禁止
- S/MIME 暗号化強度の制限設定　：有効（3DES，AES のみ選択可能となる）
- 画像ログ送信　：禁止
- リモートパネル機能　：禁止
- 外部アプリケーション連携　：禁止

2. 適合主張

2.1. CC 適合主張

本STは、以下の規格に適合する。

情報技術セキュリティ評価のためのコモンクライテリア
パート1: 概説と一般モデル バージョン 3.1 改訂第 3 版 ［翻訳第 1.0 版］
パート2: セキュリティ機能コンポーネント バージョン 3.1 改訂第 3 版 ［翻訳第 1.0 版］
パート3: セキュリティ保証コンポーネント バージョン 3.1 改訂第 3 版 ［翻訳第 1.0 版］

- セキュリティ機能要件　：パート2 拡張。
- セキュリティ保証要件　：パート3 適合。

2.2. PP 主張

本 ST が適合する PP はない。

2.3. パッケージ主張

本 ST は、パッケージ：EAL3 に適合する。追加する保証コンポーネントはない。

2.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 3.1 Revision 3 CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components Version 3.1 Revision 3 CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components Version 3.1 Revision 3 CCMB-2009-07-003
- Common Methodology for Information Technology Security Evaluation Evaluation methodology Version 3.1 Revision 3 CCMB-2009-07-004

3. セキュリティ課題定義

本章では、保護対象資産の考え方、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 保護対象資産

TOE のセキュリティコンセプトは、**“ユーザの意図に反して暴露される可能性のあるデータの保護”**である。

MFP を通常の利用方法で使用している場合、利用可能な状態にある以下の画像ファイルを保護対象とする。

- **セキュリティ文書ファイル**
  セキュリティ文書によって保存される画像ファイル
- **認証＆プリントファイル**
  認証&プリント機能を利用してプリントデータが保存される場合に認証&プリントファイルとして保存される画像ファイル
- **ボックスファイル**
  個人ボックス、共有ボックス、グループボックスに保存される画像ファイル

複数のジョブの動作により待機状態として**保存**されるジョブの画像ファイルや、仕上がりの確認のために残り部数の印刷が待機状態となって保存されるジョブの画像ファイル等、上記の対象とする画像ファイル以外は、MFP の通常利用において保護されることが意図されないため、保護資産とは扱わない。

なおセキュリティ文書ファイル、認証&プリントファイルの保存、ボックスファイルの送信においては、万が一不正な MFP やメールサーバなどが接続された場合、不正な MFP 等の接続はなくとも、PC-FAX 受信設定を変更されてしまった場合などに発生する脅威に備え、MFP の設定（IP アドレス、送信宛先データなど）、PC-FAX 受信設定等を不正に変更出来ないようにする必要がある。したがって MFP の設定（IP アドレス、送信宛先データなど）、PC-FAX 受信設定は副次的な保護資産として考慮する。

一方、MFP をリース返却、廃棄するなど利用が終了した場合や HDD が盗難にあった場合などユーザの管轄から**保存**されるデータが物理的に離れてしまった場合は、ユーザは HDD に残存するあらゆるデータの漏洩可能性を懸念する。従ってこの場合は以下のデータファイルを保護対象とする。

- **セキュリティ文書ファイル**
- **認証＆プリントファイル**
- **ボックスファイル**
- **保存画像ファイル**
  - セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル以外の**保存**される画像ファイル
- **HDD 残存画像ファイル**
  - 一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、HDD データ領域に残存するファイル
- **画像関連ファイル**
  - プリント画像ファイル処理において生成されたテンポラリデータファイル

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

A.ADMIN（管理者の人的条件）
管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。

A.SERVICE（サービスエンジニアの人的条件）
サービスエンジニアは、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。

A.NETWORK（MFP のネットワーク接続条件）
・TOE が搭載される MFP を設置するオフィス内 LAN は、盗聴されない。
・TOE が搭載される MFP を設置するオフィス内 LAN が外部ネットワークと接続される場合は、外部ネットワークから MFP へアクセスできない。

A.SECRET（秘密情報に関する運用条件）
TOE の利用において使用される各パスワードや暗号化ワードは、各利用者から漏洩しない。

3.3. 脅威

本節では、TOE の利用及び TOE 利用環境において想定される脅威を識別し、説明する。

T.DISCARD-MFP（MFP のリース返却、廃棄）
リース返却、または廃棄となった MFP が回収された場合、悪意を持った者が、MFP 内の HDD を解析することにより、セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル、保存画像ファイル、HDD 残存画像ファイル、画像関連ファイルが漏洩する。

T.BRING-OUT-STORAGE（HDD の不正な持ち出し）
・悪意を持った者や悪意を持ったユーザが、MFP 内の HDD を不正に持ち出して解析することにより、セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル、保存画像ファイル、HDD 残存画像ファイル、画像関連ファイルが漏洩する。
・悪意を持った者や悪意を持ったユーザが、MFP 内の HDD を不正にすりかえる。すりかえられた HDD には新たにセキュリティ文書ファイル、ボックスファイル、認証&プリントファイル、保存画像ファイル、HDD 残存画像ファイル、画像関連ファイルが蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえた HDD を持ち出して解析することにより、これら画像ファイル等が漏洩する。

T.ACCESS-PRIVATE-BOX（ユーザ機能を利用した個人ボックスへの不正なアクセス）
悪意を持った者や悪意を持ったユーザが、他のユーザが個人所有するボックスにアクセスし、ボックスファイルを操作（コピー、移動、ダウンロード、印刷、送信等）することにより、ボックスファイルが暴露される。

T.ACCESS-PUBLIC-BOX（ユーザ機能を利用した共有ボックスへの不正なアクセス）

悪意を持った者や悪意を持ったユーザが、利用を許可されない共有ボックスにアクセスし、ボックスファイルを操作（コピー、移動、ダウンロード、印刷、送信等）することにより、ボックスファイルが暴露される。

T.ACCESS-GROUP-BOX（ユーザ機能を利用したグループボックスへの不正なアクセス）

悪意を持った者や悪意を持ったユーザが、そのユーザが所属していない部門が所有するグループボックスにアクセスし、ボックスファイルを操作（コピー、移動、ダウンロード、印刷、送信等）することにより、ボックスファイルが暴露される。

T.ACCESS-SECURE-PRINT
（ユーザ機能を利用したセキュリティ文書ファイル、認証&プリントファイルへの不正なアクセス）

・悪意を持った者や悪意を持ったユーザが、利用を許可されないセキュリティ文書ファイルを操作（印刷等）することにより、セキュリティ文書ファイルが暴露される。
・悪意を持った者や悪意を持ったユーザが、他のユーザが保存した認証&プリントファイルを操作（印刷等）することにより、認証&プリントファイルが暴露される。

T.UNEXPECTED-TRANSMISSION（想定外対象先への送受信）

・悪意を持った者や悪意を持ったユーザが、ボックスファイルの送信に関係するネットワーク設定を変更することにより、宛先が正確に設定されていてもボックスファイルがユーザの意図しないエンティティへ送信（E-mail 送信、FTP 送信）されてしまい、ボックスファイルが暴露される。

＜ボックスファイル送信に関係するネットワーク設定＞

- SMTP サーバに関する設定
- DNS サーバに関する設定

・悪意を持った者や悪意を持ったユーザが、TOE が導入される MFP に設定される MFP を識別するためのネットワーク設定を変更し、不正な別の MFP などのエンティティにおいて本来 TOE が導入される MFP の設定（NetBIOS 名、AppleTalk プリンタ名、IP アドレスなど）を設定することにより、セキュリティ文書ファイル、認証&プリントファイルが暴露される。
・悪意を持った者や悪意を持ったユーザが、TSI 受信設定を変更することにより、ボックスファイルが意図しない保存領域に保存されて暴露される。
・悪意を持った者や悪意を持ったユーザが、PC-FAX 受信設定を変更し、共有ボックス等のボックスへの**保存**設定状態から、全ユーザ共通領域に**保存**される設定に変更することにより、ボックスファイルが意図しない保存領域に保存されて暴露される。

※ 本脅威は、PC-FAX 受信設定が、ボックスへの**保存**設定状態を運用として意図している場合のみ発生する脅威である。

T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）

悪意を持った者や悪意を持ったユーザが、セキュリティ強化機能に関係する設定を変更してしまうことにより、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルが漏洩する可能性が高まる。

T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）

悪意を持った者や悪意を持ったユーザが、バックアップ機能、リストア機能を不正に使用することにより、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルが漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、各種設定値が改ざんされる。

3.4. 組織のセキュリティ方針

昨今、オフィス内でもネットワークのセキュアさを要求する組織は多い。本 ST では、オフィス内 LAN 上での盗聴行為等の脅威を想定しないが、オフィス内 LAN 上のセキュリティ対策を希望する組織・利用者に対応した TOE セキュリティ環境を想定する。また、内部ネットワークに存在するクライアント PC およびサーバの蓄積データや内部ネットワークを流れる一般データは保護対象外の資産であるが、FAX 公衆回線ロから MFP を介して内部ネットワークへのアクセスを禁止している組織・利用者に対応した TOE セキュリティ環境を想定する。

また、攻撃者による MFP の不正な利用、保護資産である画像ファイルの漏洩や改竄といった不正な操作のモチベーション低下させたい組織も多い。監査ログ機能は不正な利用や操作の追跡が可能であることから、攻撃者のモチベーションを低下させることが期待される。そこで、同機能を用い MFP を管理することを希望する組織・利用者に対応した TOE セキュリティ環境を想定する。取得するセキュリティに関連するログは２種類である。一つは、すべての認証機能のログを取得する。ユーザや部門の停止状態の確認を除き、MFP の機能を利用するためには、認証に成功する必要があるため、MFP の利用者の不正行為（許可時間外の操作など）を低減することができる。もう一つは、MFP に登録してある保護資産であるボックスファイル、セキュリティ文書ファイル、認証&プリントファイルに関する操作（ジョブ）のログを取得する。ユーザによる保護資産へのアクセスを監視することにより、不正操作を低減することができる。

以下に TOE を利用する組織にて適用されるセキュリティ方針を識別し、説明する。

P.COMMUNICATION-DATA（画像ファイルのセキュアな通信）

IT 機器間にて送受信される秘匿性の高い画像ファイル（セキュリティ文書ファイル、ボックスファイル、認証&プリントファイル）は、組織・利用者が希望する場合において、正しい相手先に対して信頼されるパスを介して通信する、または暗号化しなければならない。

P.REJECT-LINE（公衆回線からのアクセス禁止）

公衆回線網から、MFP の FAX 公衆回線ロを介しての内部ネットワークへのアクセスは禁止しなければならない。

P.AUDIT-LOGGING（監査ログの取得、管理）

全ての認証機能及び監視すべきジョブに関する監査ログを生成維持しなければならない。また、監査ログを開示または改変する権限を保持しない者からは監査ログを保護し、権限を保持する者は監査ログを閲覧できるようにしなければならない。

4. セキュリティ対策方針

本章では、3 章にて識別された前提条件、脅威、組織のセキュリティ方針を受けて、TOE 及び TOE の利用環境にて必要なセキュリティ対策方針について記述する。以下、TOE のセキュリティ対策方針、環境のセキュリティ対策方針に分類して記述する。

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.REGISTERED-USER（許可ユーザの利用）

TOE は、識別認証に成功したユーザだけに TOE の搭載された MFP の利用を許可する。

O.PRIVATE-BOX（個人ボックスアクセス制御）

・TOE は、ユーザだけに、そのユーザが所有する個人ボックスのユーザ機能を許可する。
・TOE は、ユーザだけに、そのユーザが所有する個人ボックス内のボックスファイルのユーザ機能を許可する。

O.PUBLIC-BOX（共有ボックスアクセス制御）

・TOE は、識別認証に成功したユーザだけに、共有ボックスの閲覧操作を許可する。
・TOE は、その共有ボックスの利用を許可されたユーザだけに、その共有ボックスのユーザ機能を許可する。
・TOE は、その共有ボックスの利用を許可されたユーザだけに、その共有ボックス内のボックスファイルのユーザ機能を許可する。

O.GROUP-BOX（グループボックスアクセス制御）

・TOE は、その部門の利用を許可されたユーザだけに、その部門で所有されるグループボックスのユーザ機能を許可する。
・TOE は、その部門の利用を許可されたユーザだけに、その部門で所有されるグループボックス内のボックスファイルのユーザ機能を許可する。

O.SECURE-PRINT（セキュリティ文書ファイル、認証＆プリントファイルアクセス制御）

・TOE は、そのセキュリティ文書ファイルの利用を許可されたユーザだけに、そのセキュリティ文書ファイルのユーザ機能を許可する。
・TOE は、認証&プリントファイルを保存したユーザだけに、当該認証&プリントファイルのユーザ機能を許可する。

O.CONFIG（管理機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・SMTP サーバに関係する設定機能
・DNS サーバに関係する設定機能
・MFP のアドレスに関係する設定機能
・バックアップ機能
・リストア機能
・高信頼チャネル機能設定データの設定機能

・S/MIME 機能で利用する証明書、送信宛先データ等の設定機能
・TSI 受信設定機能
・PC-FAX 受信設定機能
・カウンタ管理機能
・全領域上書き削除機能

TOE は、管理者及びサービスエンジニアだけに以下に示す機能の操作を許可する。
・セキュリティ強化機能の設定に関係する機能

O.OVERWRITE（上書き削除）

TOE は、MFP 内の HDD にある画像データ領域に削除用データを上書きし、あらゆる画像データを復旧不可能にする。

O.CRYPTO-KEY（暗号鍵生成）

TOE は、MFP 内の HDD に書き込まれる画像ファイルを含むすべてのデータを暗号化して保存するための暗号鍵を生成する。

O.TRUSTED-PASS（高信頼チャネルの利用）

TOE は、MFP とクライアント PC の間で送受信される以下の画像ファイルを、高信頼チャネルを介して通信する機能を提供する。
＜MFP からクライアント PC 送信される画像ファイル＞
・ボックスファイル
＜クライアント PC から MFP へ送信される画像ファイル＞
・ボックスファイルとして保存されることになる画像ファイル
・セキュリティ文書ファイルとして保存されることになる画像ファイル
・認証&プリントファイルとして保存されることになる画像ファイル

O.CRYPTO-MAIL（暗号化メールの利用）

TOE は、MFP からメールにて送信されるボックスファイルを、正しい相手先へ暗号化して送信する機能を提供する。

O.FAX-CONTROL（FAX ユニット制御）

TOE は、公衆回線網から FAX 公衆回線ロを通して、当該 MFP が接続されている内部ネットワークへのアクセスを禁止する制御機能を提供する。

O.AUTH-CAPABILITY（ユーザ認証機能を利用するためのサポート動作）

TOE は、ActiveDirectory を用いたユーザ情報管理サーバによるユーザ認証機能を利用するために必要な動作をサポートする。

O.CRYPTO-CAPABILITY（HDD 暗号化機能を利用するためのサポート動作）

TOE は、ASIC による HDD 暗号化機能を利用するために必要な動作をサポートする。

O.AUDIT-LOGGED（監査ログの取得、管理）

TOE は、全ての認証機能及び監視すべきジョブに関する監査ログを生成維持し、監査ログを開示または改変する権限の無い者からは監査ログを保護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

本節では、TOE の運用環境のセキュリティ対策方針を説明する。

OE.FEED-BACK（セキュアなパスワード表示をするアプリケーションの利用）

管理者及びユーザは、クライアント PC にて MFP にアクセスするために利用されるブラウザなどのアプリケーションに、入力されるユーザパスワード、ボックスパスワード、部門パスワード、管理者パスワード、セキュリティ文書パスワード、SNMP パスワードに対して保護された適切なフィードバックを提供するアプリケーションを利用する。

OE.SERVER（ユーザ情報管理サーバの利用）

管理者は、ユーザのアカウント管理において、MFP ではなく外部のユーザ情報管理サーバを利用する場合、Active Directory によるユーザ管理を利用するための設定をする。

OE.SESSION（操作後のセッションの終了）

管理者は、ユーザに対して以下に示す運用を実施させる。

・セキュリティ文書ファイルの操作、認証&プリントファイルの操作、ボックス及びボックスファイルの操作の終了後にログアウト操作を行う。

管理者は、以下に示す運用を実施する。

・管理者モードの諸機能を操作終了後にログアウト操作を行う。

サービスエンジニアは、以下に示す運用を実施する。

・サービスモードの諸機能を操作終了後にログアウト操作を行う。

OE.ADMIN（信頼できる管理者）

MFP を利用する組織の責任者は、TOE が搭載される MFP の運用において課せられた役割を忠実に実行する人物を管理者に指定する。

OE.SERVICE（サービスエンジニアの保証）

・MFP を保守管理する組織の責任者は、TOE の設置、セットアップ及び TOE が搭載される MFP の保守において課せられた役割を忠実に実行するようにサービスエンジニアを教育する。

・管理者は、サービスエンジニアによる TOE が搭載される MFP のメンテナンス作業に立会う。

OE.NETWORK（MFP の接続するネットワーク環境）

・MFP を利用する組織の責任者は、TOE が搭載される MFP を設置するオフィス LAN において暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を実施する。

・MFP を利用する組織の責任者は、外部ネットワークから TOE が搭載される MFP へのアクセスを遮断するためにファイアウォールなどの機器を設置して、外部からの不正侵入対策を実施する。

OE.FAX-UNIT（FAX ユニットの利用）

サービスエンジニアは、MFP にオプションパーツである FAX ユニットを搭載し、FAX ユニットの機能を利用するための設定をする。

OE.SECRET（秘密情報の適切な管理）

管理者は、ユーザに対して以下に示す運用を実施させる。

・ユーザパスワード、セキュリティ文書パスワードを秘匿する。

・ボックスパスワード、部門パスワードは共同で利用するユーザの間で秘匿する。
・ユーザパスワード、セキュリティ文書パスワード、ボックスパスワードに推測可能な値を設定しない。
・ユーザパスワード、ボックスパスワードの適宜変更を行う。
・管理者がユーザパスワード、ボックスパスワードを変更した場合は、速やかに変更させる。

管理者は、以下に示す運用を実施する。
・管理者パスワード、部門パスワード、SNMP パスワード、暗号化ワードに推測可能な値を設定しない。
・管理者パスワード、部門パスワード、SNMP パスワード、暗号化ワードを秘匿する。
・管理者パスワード、部門パスワード、SNMP パスワード、暗号化ワードの適宜変更を行う。

サービスエンジニアは以下に示す運用を実施する。
・CE パスワードに推測可能な値を設定しない。
・CE パスワードを秘匿する。
・CE パスワードの適宜変更を行う。
・サービスエンジニアが管理者パスワードを変更した場合は、管理者に速やかに変更させる。

OE.SETTING-SECURITY（セキュリティ関連設定、維持、操作）

管理者は、ユーザに利用させる前に TOE に対し、セキュリティ強化機能を含むガイダンスの記載に沿った設定を行い、TOE を利用する間は設定が維持されるように運用する。また、管理者は MFP をリース返却、廃棄する際に TOE に対し、ガイダンスの記載に沿って運用する。

OE.AUDIT_STORAGE-PROTECTED（監査ログ保護）

管理者は、信頼できる IT 製品にエクスポートしたログが操作権限を保持しない者からアクセス、削除、改変をされないよう監査ログを保護する。

OE.AUDIT_ACCESS-AUTHORIZED（監査ログへのアクセス権限）

管理者は、信頼できる IT 製品にエクスポートしたログが操作権限を保持する者からのみアクセスできるよう管理する。

OE.AUDIT-REVIEWED（監査ログの精査）

管理者は、セキュリティ侵害や異常状態を検出するために、適切な間隔で監査ログの精査を実施する。

4.3. セキュリティ対策方針根拠

4.3.1. 必要性

前提条件、脅威、及び組織のセキュリティ方針とセキュリティ対策方針の対応関係を下表に示す。セキュリティ対策方針が少なくとも１つ以上の前提条件、脅威、組織のセキュリティ方針に対応していることを示している。

表 1 前提条件、脅威、組織のセキュリティ方針に対するセキュリティ対策方針の適合性

組織のセキュリティ方針 前提 脅威 ／ セキュリティ対策方針	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-PRIVATE-BOX	T.ACCESS-PUBLIC-BOX	T.ACCESS-GROUP-BOX	T.ACCESS-SECURE-PRINT	T.UNEXPECTED-TRANSMISSION	T.ACCESS-SETTING	T.BACKUP-RESTORE	P.COMMUNICATION-DATA	P.REJECT-LINE	P.AUDIT-LOGGING
O.REGISTERED-USER							●	●	●	●						
O.PRIVATE-BOX							●									
O.PUBLIC-BOX								●								
O.GROUP-BOX									●							
O.SECURE-PRINT										●						
O.CONFIG											●	●	●	●		
O.OVERWRITE					●											
O.CRYPTO-KEY						●										
O.TRUSTED-PASS														●		
O.CRYPTO-MAIL														●		
O.FAX-CONTROL															●	
O.CRYPTO-CAPABILITY						●										
O.AUTH-CAPABILITY							●	●	●	●						
O.AUDIT-LOGGED																●
OE.FEED-BACK							●	●	●	●	●	●	●	●		
OE.SERVER							●	●	●	●						
OE.SESSION							●	●	●	●	●	●	●	●		
OE.ADMIN	●															
OE.SERVICE		●														
OE.NETWORK			●													
OE.FAX-UNIT															●	
OE.SECRET				●												
OE.SETTING-SECURITY					●	●	●	●	●	●	●	●	●	●		
OE.AUDIT_STORAGE-PROTECTED																●
OE.AUDIT_ACCESS-AUTHORIZED																●
OE.AUDIT-REVIEWED																●

4.3.2. 前提条件に対する十分性

前提条件に対するセキュリティ対策方針について以下に説明する。

- **A.ADMIN（管理者の人的条件）**
  本条件は、管理者が悪意を持たないことを想定している。
  OE.ADMIN は、MFP を利用する組織が MFP を利用する組織において信頼のおける人物を管理者に指定するため、管理者の信頼性が実現される。

- **A.SERVICE（サービスエンジニアの人的条件）**
  本条件は、サービスエンジニアが悪意を持たないことを想定している。
  OE.SERVICE は、MFP を保守管理する組織においてサービスエンジニアを教育する。また管理者は、サービスエンジニアの行うメンテナンス作業に立ち会うことが規定されているため、サービスエンジニアの信頼性は確保される

- **A.NETWORK（MFP のネットワーク接続条件）**
  本条件は、オフィス内 LAN の盗聴行為、外部ネットワークから不特定多数の者による攻撃などが行われないことを想定している。
  OE.NETWORK は、オフィス内 LAN に暗号化通信を行うための機器や盗聴検知機器を設置するなどにより、盗聴の防止を規定している。また外部ネットワークから MFP へのアクセスを遮断するためにファイアウォールなどの機器を設置することにより外部からの不正侵入の防止を規定しており、本条件は実現される。

- **A.SECRET（秘密情報に関する運用条件）**
  本条件は、TOE の利用において使用される各パスワード、暗号化ワードが各利用者より漏洩しないことを想定している。
  OE.SECRET は、管理者がユーザに対してセキュリティ文書パスワード、ボックスパスワード、ユーザパスワード、部門パスワードに関する運用規則を実施させることを規定し、管理者が管理者パスワード、SNMP パスワード、暗号化ワード、部門パスワードに関する運用規則を実施することを規定している。また、サービスエンジニアが CE パスワードに関する運用規則を実施し、管理者に対して、管理者パスワードに関する運用規則を実施させることを規定しており、本条件は実現される。

4.3.3. 脅威に対する十分性

脅威に対抗するセキュリティ対策方針について以下に説明する。

- **T.DISCARD-MFP（MFP のリース返却、廃棄）**
  本脅威は、ユーザから回収された MFP より情報漏洩する可能性を想定している。
  O.OVERWRITE は、TOE が HDD の画像データ領域に削除用のデータを上書きする機能を提供し、MFP が回収される前に機能が実行されることによって、脅威の可能性は軽減される。また、OE.SETTING-SECURITY は、TOE が提供する HDD の画像データ領域に削除用のデータを上書きする機能の操作を示し、MFP が回収される前に操作が行われることによって、脅威の可能性は軽減される。
  したがって本脅威は十分対抗されている。

- **T.BRING-OUT-STORAGE（HDD の不正な持ち出し）**

  本脅威は、MFP を利用している運用環境から HDD が盗み出される、または不正な HDD が取り付けられて、そこにデータが蓄積されたところで持ち出されることにより、HDD 内の画像データが漏洩する可能性を想定している。

  これに対して O.CRYPTO-KEY は、TOE が HDD に書き込まれるデータを暗号化するための暗号鍵を生成し、O.CRYPTO-CAPABILITY により ASIC での HDD 暗号化機能を利用するための動作がサポートされ、OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれるため、脅威の可能性は軽減される。

  したがって本脅威は十分対抗されている。

- **T.ACCESS-PRIVATE-BOX（ユーザ機能を利用した個人ボックスへの不正なアクセス）**

  本脅威は、ユーザ各位が画像ファイルの**保存**に利用する個人ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

  O.REGISTERED-USER は、TOE が識別認証に成功したユーザだけが、TOE の搭載された MFP を利用することを許可するとしており、さらに O.PRIVATE-BOX によって個人ボックス及び個人ボックス内のボックスファイルの操作が、その所有者であるユーザだけに制限され、脅威の可能性は軽減される。なお外部のユーザ情報管理サーバを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザ情報管理サーバによるユーザ認証機能を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザ管理を利用するための設定が行われ、ユーザの識別認証が行われることによって脅威の可能性は軽減される。

  OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、ユーザの認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後には、ログアウトする運用が要求されるため、O.REGISTERED-USER 及び O.PRIVATE-BOX は十分サポートされている。

  したがって本脅威は十分対抗されている。

- **T.ACCESS-PUBLIC-BOX（ユーザ機能を利用した共有ボックスへの不正なアクセス）**

  本脅威は、ユーザが共有して利用する画像ファイルの**保存**場所である共有ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

  O.REGISTERED-USER は、TOE が識別認証に成功したユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.PUBLIC-BOX によって共有ボックス、共有ボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は軽減される。なお外部のユーザ情報管理サーバを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザ情報管理サーバによるユーザ認証機能を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザ管理を利用するための設定が行われ、ユーザの識別認証が行われることによって脅威の可能性は軽減される。

  OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、ユーザの認証及びボックスの認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.REGISTERED-USER 及び O.PUBLIC-BOX は十分サポートされている。

  したがって本脅威は十分対抗されている。

- **T.ACCESS-GROUP-BOX（ユーザ機能を利用したグループボックスへの不正なアクセス）**

本脅威は、その部門の利用が許可されたユーザが利用する画像ファイルの保存場所であるグループボックスやその中のボックスファイルに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

O.REGISTERED-USER は、TOE が識別認証に成功したユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.GROUP-BOX によってグループボックス、グループボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は軽減される。なお外部のユーザ情報管理サーバを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザ情報管理サーバによるユーザ認証機能を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザ管理を利用するための設定が行われ、ユーザの識別認証が行われることによって脅威の可能性は軽減される。

OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、ユーザの認証及び部門の認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.REGISTERED-USER 及び O.GROUP-BOX は十分サポートされている。

したがって本脅威は十分対抗されている。

- **T.ACCESS-SECURE-PRINT**
  （ユーザ機能を利用したセキュリティ文書ファイル、認証&プリントファイルへの不正なアクセス）

本脅威は、ユーザ機能を利用したセキュリティ文書、及び認証&プリントに対して不正な操作が行われてしまう可能性を想定している。

O.REGISTERED-USER は、TOE が識別認証に成功したユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.SECURE-PRINT によって、セキュリティ文書の操作、及び認証&プリントの操作が許可されたユーザだけに制限されるため、脅威の可能性は軽減される。なお外部のユーザ情報管理サーバを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザ情報管理サーバによるユーザ認証機能を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザ管理を利用するための設定が行われ、ユーザの識別認証が行われることによって脅威の可能性は軽減される。

OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、ユーザの認証及びセキュリティ文書へのアクセス認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.REGISTERED-USER 及び O.SECURE-PRINT は十分サポートされている。

したがって本脅威は十分対抗されている。

- **T.UNEXPECTED-TRANSMISSION（想定外対象先への送受信）**

本脅威は、送信に関係するネットワーク設定を不正に変更された場合に、ボックスファイルを意図しない宛先へ配信してしまう可能性を想定している。これは例えば E-mail の場合、E-mail を中継する SMTP サーバのアドレスを不正に変更される、またはドメイン名の検索によって SMTP サーバのアドレスを利用する場合にドメイン名を問い合わせる DNS サーバのアドレスを不正に変更されることによって、悪意を持つ者がネットワーク環境構成を変えずに、不正に指定されるサーバへボックスファイルが送信されてしまう可能性があることを懸念している。FTP 送信であれば、同様にドメイン名の検索の仕組みを利用する場合があり、E-mail 同様の可能性が懸念され

る。
さらに、MFP のアドレスに関係するネットワーク設定を不正に変更された場合に、TOE であると思って利用するユーザが、不正なエンティティにクライアント PC からプリント機能を利用してしまう可能性を想定している。特にオフィス内の他のユーザに対しても秘匿性が要求されるセキュリティ文書ファイル、認証&プリントファイルが不正なエンティティに送信されると問題となる。
この他に PC-FAX 受信設定、TSI 受信設定は、FAX 受信の場合に発生しうる、意図しないボックスファイルの保存が発生する可能性を想定している。
これに対して O.CONFIG により、TOE が送信に関係するネットワーク設定、PC-FAX 受信設定、TSI 受信設定を操作する役割を管理者に制限するとしており、本脅威の可能性は除去される。
OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、管理者の認証において入力される各種パスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.CONFIG は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）**

本脅威はセキュリティに関係する特定の機能設定を変更されることにより、結果的にボックスファイルやセキュリティ文書ファイル、認証&プリントファイルの漏洩に発展する可能性を想定している。
O.CONFIG により、一連のセキュリティに関連する設定機能を統括するセキュリティ強化機能の設定を管理者及びサービスエンジニアだけに許可するとしており、脅威の可能性が除去される。
OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、管理者の認証において入力される各種パスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により管理者モード、サービスモードの操作終了後にはそれぞれログアウトする運用が要求されるため、O.CONFIG は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）**

本脅威はバックアップ機能、リストア機能が不正に利用されることにより、ボックスファイルやセキュリティ文書ファイル、認証&プリントファイルが漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、各種設定値等が改ざんされた結果、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルが漏洩する可能性を想定している。
O.CONFIG により、バックアップ機能、リストア機能の利用を管理者だけに許可するとしており、脅威の可能性が除去される。
OE.SETTING-SECURITY はセキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行なわれ、OE.FEED-BACK は、管理者の認証において入力される各種パスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.CONFIG をサポートしている。
したがって本脅威は十分対抗されている。

4.3.4. 組織のセキュリティ方針に対する十分性

組織のセキュリティ方針に対応するセキュリティ対策方針について以下に説明する。

- **P.COMMUNICATION-DATA（画像ファイルのセキュアな通信）**

本組織のセキュリティ方針は、ネットワーク上に流れる画像ファイルについて、秘匿性を確保するために、組織・利用者が希望する場合において正しい相手先へ信頼されるパスを介した処理を行う、または暗号化すること規定している。希望に応じて対応できればよいため、すべての通信においてセキュアな通信機能を提供する必要はなく、セキュリティ文書、ボックスファイルを扱うにあたり、MFP と利用者の使うクライアント PC 間で最低限 1 つの手段が提供される必要がある。

O.TRUSTED-PASS により、秘匿性のある画像である、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルに対して、MFP からクライアント PC、またはクライアント PC から MFP といった画像の送受信において正しい相手先に高信頼チャネルを提供するため、組織のセキュリティ方針が実現する。

また O.CRYPTO-MAIL により、MFP からクライアント PC へメールにて送信されるボックスファイルを正しい相手先へ暗号化して送信する機能を提供するとするセキュリティ対策方針により、組織のセキュリティ方針は実現される。

さらに高信頼チャネル機能設定データ、メールによるボックスファイルの暗号化の管理、送信宛先データは、O.CONFIG により管理者に制限されている。また OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により操作終了後にはログアウトする運用が要求されるため、O.CONFIG をサポートしている。また、OE.SETTING-SECURITY によって、セキュリティ強化機能を含むガイダンスの記載に沿った設定とその維持に関する運用が行われる。

したがって本組織のセキュリティ方針は、達成するために十分である。

- **P.REJECT-LINE（公衆回線からのアクセス禁止）**

本組織のセキュリティ方針は、内部ネットワークに存在するクライアント PC およびサーバの蓄積データや内部ネットワークを流れる一般データに対して、MFP に搭載された FAX ユニットの FAX 公衆回線ロを通して、公衆回線網からアクセスされることを禁止している。

これは組織の希望により FAX ユニットを搭載した場合においても、公衆回線網から送付され、MFP の FAX 公衆回線ロを介して内部ネットワークに転送される画像データを除いた通信（遠隔診断機能や不正な操作コマンド）が、内部ネットワークに転送されないことを意味している。

O.FAX-CONTROL により、一般データを含む内部ネットワークに存在するデータに対して、公衆回線から FAX ユニットの FAX 公衆回線ロを経由してのアクセスを禁止している。また OE.FAX-UNIT により、サービスエンジニアによりオプションパーツである FAX ユニットが MFP に搭載され、運用されることが要求されるため、O.FAX-CONTROL をサポートしている。

したがって本組織のセキュリティ方針は実現される。

- **P.AUDIT-LOGGING（監査ログの取得、管理）**

本組織のセキュリティ方針は、すべての認証機能及び監視すべきジョブに関する監査ログを生成維持しなければならない。また、監査ログを開示または改変する権限を保持しない者からは監査ログを保護し、権限を保持する者は監査ログを閲覧できるようにすることを規定している。

O.AUDIT-LOGGED により、すべての認証機能及び監視すべきジョブに関する監査ログを生成維持し、監査ログを開示または改変する権限の無い者からは監査ログを保護する機能を提供することを規定している。また、管理者は OE.AUDIT_STORAGE-PROTECTED により、信頼できる IT

製品にエクスポートしたログが操作権限を保持しない者からアクセス、削除、改変をされないよう監査ログを保護することを、OE.AUDIT_ACCESS-AUTHORIZED により、信頼できる IT 製品にエクスポートしたログが操作権限を保持する者からのみアクセスできるよう管理することを、OE.AUDIT-REVIEWED により、セキュリティ侵害や異常状態を検出するために、適切な間隔で監査ログの精査を実施することを要求されるため、O.AUDIT.LOGGED をサポートしている。
したがって本組織のセキュリティ方針は実現される。

5. 拡張コンポーネント定義

5.1. 拡張機能コンポーネント

本 ST では、拡張機能コンポーネントを 3 つ定義する。各セキュリティ機能要件の必要性、ラベリング定義の理由は以下の通りである。

- FIT_CAP.1

  TOE が IT 環境である外部エンティティのセキュリティ機能を有効利用するために TOE に必要な能力を規定するためのセキュリティ機能要件である。

  - **拡張の必要性**

    TOE が外部のセキュリティ機能を利用する場合、外部のセキュリティ機能が確かにセキュアであることも重要であるが、外部のセキュリティ機能を正しく使いこなすために TOE 側が提供すべき能力は非常に重要である。しかし本要求のような概念はセキュリティ機能要件には存在しない。
  - **適用したクラス（FIT）の理由**

    CC パート 2 にはない新しい着想であるため、新しいクラスを定義した。
  - **適用したファミリ（CAP.1）の理由**

    クラスと同様に CC パート 2 にはない新しい着想であるため、新しいファミリを定義した。

5.1.1. FIT_CAP.1 の定義

- **クラス名**

  FIT：IT 環境エンティティとの連携

  略称の意味：FIT（Functional requirement for IT environment support）

- **クラスのふるまい**

  このクラスには、IT 環境エンティティが提供するセキュリティサービスの利用に関連する要件を特定するファミリが含まれる。本件では 1 つのファミリが存在する。

  － IT 環境エンティティの利用（FIT_CAP）;

- **ファミリのふるまい**

  このファミリは、IT 環境エンティティのセキュリティ機能を利用するにあたって、TOE に必要となる能力の定義に対応する。

- **コンポーネントのレベル付け**

FIT_CAP　IT 環境エンティティの利用するための能力	1

略称の意味：CAP（**CAP**ability of using it environment）

FIT_CAP.1：「IT 環境エンティティのセキュリティサービス利用時の能力」は、IT 環境エンティティが提供するセキュリティ機能を正しく利用するための TOE に必要となる能力の具体化に対応する。

監査：FIT_CAP.1
FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである。 a) 最小　IT 環境エンティティに対する動作の失敗 b) 基本　IT 環境エンティティに対するすべての動作の使用（成功、失敗）
管理：FIT_CAP.1
以下のアクションは FMT における管理機能と考えられる。 予見される管理アクティビティはない。

FIT_CAP.1　IT 環境エンティティのセキュリティサービス利用時の能力
FIT_CAP.1.1
TSF は、[割付: *IT 環境エンティティが提供するセキュリティサービス*]に対して、そのサービスを利用するために必要な能力を提供しなければならない : [割付: *セキュリティサービスの動作に必要な能力のリスト*]。
下位階層　:　なし
依存性　:　なし

6. IT セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

＜ラベル定義について＞

TOE に必要とされるセキュリティ機能要件を記述する。機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用し、ラベルも同一のものを使用する。CC パート 2 に記載されない新しい追加要件は、CC パート 2 と競合しないラベルを新設して識別している。

＜セキュリティ機能要件“操作”の明示方法＞

以下の記述の中において、イタリック且つボールドで示される表記は、“割付”、または“選択”されていることを示す。アンダーラインで示される原文の直後に括弧書きでイタリック且つボールドで示される表記は、アンダーラインされた原文箇所が“詳細化”されていることを示す。ラベルの後に括弧付けで示される番号は、当該機能要件が“繰り返し”されて使用されていることを示す。

＜依存性の明示方法＞

依存性の欄において括弧付け“( )”された中に示されるラベルは、本 ST にて使用されるセキュリティ機能要件のラベルを示す。また本 ST にて適用する必要性のない依存性である場合は、同括弧内にて“適用しない”と記述している。

6.1. TOE セキュリティ要件

6.1.1. TOE セキュリティ機能要件

6.1.1.1. 暗号サポート

FCS_CKM.1　　暗号鍵生成
FCS_CKM.1.1
TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。
[割付: *標準のリスト*] : ***「表 2　暗号鍵生成　標準・アルゴリズム・鍵長の関係」に記載***
[割付: *暗号鍵生成アルゴリズム*] : ***「表 2　暗号鍵生成　標準・アルゴリズム・鍵長の関係」に記載***
[割付: *暗号鍵長*] : ***「表 2　暗号鍵生成　標準・アルゴリズム・鍵長の関係」に記載***
下位階層　　:　なし 依存性　　:　FCS_CKM.2 or FCS_COP.1（FCS_COP.1）、FCS_CKM.4（適用しない）

表 2　暗号鍵生成　標準・アルゴリズム・鍵長の関係

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
FIPS 186-2	***擬似乱数生成アルゴリズム***	***・128 bit*** ***・192 bit*** ***・168 bit*** ***・256 bit***
コニカミノルタ暗号仕様標準	***コニカミノルタ HDD 暗号鍵生成アルゴリズム***	***・128 bit***

FCS_COP.1　　暗号操作
FCS_COP.1.1
TSF は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。
[割付: *標準のリスト*]: ***「表 3　暗号操作　アルゴリズム・鍵長・暗号操作の関係」に記載***
[割付: *暗号アルゴリズム*]: ***「表 3　暗号操作　アルゴリズム・鍵長・暗号操作の関係」に記載***
[割付: *暗号鍵長*]: ***「表 3　暗号操作　アルゴリズム・鍵長・暗号操作の関係」に記載***
[割付: *暗号操作のリスト*]: ***「表 3　暗号操作　アルゴリズム・鍵長・暗号操作の関係」に記載***
下位階層　:　なし 依存性　:　FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1（FCS_CKM.1（一部事象のみ））、FCS_CKM.4（適用しない）

表 3　暗号操作　アルゴリズム・鍵長・暗号操作の関係

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作の内容
FIPS PUB 197	***AES***	***・128 bit ・192 bit ・256 bit***	***S/MIME 送信データの暗号化***
SP800-67	***3-Key-Triple-DES***	***・168 bit***	***S/MIME 送信データの暗号化***
FIPS 186-2	***RSA***	***・1024bit ・2048 bit ・3072 bit ・4096 bit***	***S/MIME 送信データ暗号化のための暗号鍵の暗号化***

6.1.1.2. 利用者データ保護

FDP_ACC.1[1]　　サブセットアクセス制御
FDP_ACC.1.1[1]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 4　ボックスアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***ボックスアクセス制御***
下位階層　:　なし 依存性　:　FDP_ACF.1（FDP_ACF.1[1]）

表 4　ボックスアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	***ボックス***	***・一覧表示***

サブジェクト	オブジェクト	操作
	ボックスファイル	***・印刷*** ***・送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信、WebDAV 送信）*** ***・ダウンロード*** ***・他のボックスへの移動*** ***・他のボックスへのコピー*** ***・外部メモリへのコピー*** ***・バックアップ***

FDP_ACC.1[2]　　サブセットアクセス制御
FDP_ACC.1.1[2]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 5　セキュリティ文書ファイルアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***セキュリティ文書ファイルアクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[2]）

表 5　セキュリティ文書ファイルアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	***セキュリティ文書ファイル***	***・一覧表示*** ***・印刷*** ***・バックアップ***

FDP_ACC.1[3]　　サブセットアクセス制御
FDP_ACC.1.1[3]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 6　設定管理アクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***設定管理アクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[3]）

表 6　設定管理アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	***・SMTP サーバグループオブジェクト*** ***・DNS サーバグループオブジェクト*** ***・MFP アドレスグループオブジェクト*** [8] ***・PC-FAX 受信設定オブジェクト***	***・　設定*** ***・　リストア***

[8] MFP アドレスグループオブジェクトとは、IP アドレス、Appletalk プリンタ名など MFP 本体のアドレスに関する一連のデータのことである。

サブジェクト	オブジェクト	操作
	・送信宛先データオブジェクト	

FDP_ACC.1[4] サブセットアクセス制御

FDP_ACC.1.1[4]

TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]:
「表 7 認証&プリントファイルアクセス制御 操作リスト」に記載

[割付: *アクセス制御 SFP*]:
認証&プリントファイルアクセス制御

下位階層 : なし
依存性 : FDP_ACF.1（FDP_ACF.1[4]）

表 7 認証＆プリントファイルアクセス制御 操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	***認証&プリントファイル***	***・一覧表示*** ***・印刷*** ***・バックアップ***

FDP_ACF.1[1] セキュリティ属性によるアクセス制御

FDP_ACF.1.1[1]

TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]:

＜サブジェクト＞		＜サブジェクト属性＞
・利用者を代行するタスク	⇒	***・ユーザ属性（ユーザ ID）*** ***・所属部門（部門 ID）*** ***・ボックス属性（ボックス ID）*** ***・管理者属性***

＜オブジェクト＞		＜オブジェクト属性＞
・ボックス	⇒	***・ユーザ属性（ユーザ ID or 共有 or 部門 ID）***
・ボックスファイル	⇒	***・ボックス属性（ボックス ID）***

[割付: *アクセス制御 SFP*]:
ボックスアクセス制御

FDP_ACF.1.2[1]

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。

[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]:

＜個人ボックスに対する操作制御＞
利用者を代行するタスクは、サブジェクト属性のユーザ属性（ユーザ ID）と一致するオブジェクト属性のユーザ属性を持つボックスに対して、一覧表示操作をすることが許可される。

＜グループボックスに対する操作制御＞
利用者を代行するタスクは、サブジェクト属性の所属部門（部門 ID）と一致するオブジェクト属性の

所属部門を持つボックスに対して、一覧表示操作をすることが許可される。 *＜共有ボックスに対する操作制御＞* *ユーザ属性（ユーザ ID）が関連づけられる利用者を代行するタスクは、オブジェクト属性のユーザ属性に「共有」が設定されているボックスに対して、一覧表示操作をすることが許可される。* *＜ボックスファイルに対する操作制御＞* *利用者を代行するタスクは、サブジェクト属性のボックス属性（ボックス ID）と一致するオブジェクト属性のボックス属性を持つボックスファイルに対して、印刷、送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信、WebDAV 送信）、ダウンロード、他のボックスへの移動、他のボックスへのコピー、外部メモリへのコピー操作することが許可される。*
FDP_ACF.1.3[1]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]： ***・管理者属性を有する利用者を代行するタスクは、ボックスの一覧表示操作をすることを許可される。*** ***・管理者属性を有する利用者を代行するタスクは、ボックスファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[1]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]： ***なし***
下位階層　：　なし 依存性　：　FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3（FMT_MSA.3[1]、FMT_MSA.3[3]）

FDP_ACF.1[2]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[2]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]： ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　⇒　・ファイル属性（セキュリティ文書内部制御 ID）*** ***・ユーザ属性（ユーザ ID）*** ***・管理者属性*** ***----------*** ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・セキュリティ文書ファイル ⇒　・ファイル属性（セキュリティ文書内部制御 ID）***
[割付: *アクセス制御 SFP*]： ***セキュリティ文書ファイルアクセス制御***
FDP_ACF.1.2[2]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]： ***・ユーザ属性（ユーザ ID）を持つ利用者を代行するタスクは、あらゆるセキュリティ文書ファイルの一覧表示が許可される。*** ***・ファイル属性（セキュリティ文書内部制御 ID）を持つ利用者を代行するタスクは、ファイル属性（セキュリティ文書内部制御 ID）と一致するファイル属性（セキュリティ文書内部制御 ID）を持つセキュリティ文書ファイルに対して印刷操作を許可される。***

FDP_ACF.1.3[2]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]: ***管理者属性を有する利用者を代行するタスクは、セキュリティ文書ファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[2]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[2]）、FMT_MSA.3（FMT_MSA.3[2]）

FDP_ACF.1[3] セキュリティ属性によるアクセス制御

FDP_ACF.1.1[3]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　⇒　・管理者属性*** --- ***＜オブジェクト＞*** ***・SMTP サーバグループオブジェクト*** ***・DNS サーバグループオブジェクト*** ***・MFP アドレスグループオブジェクト*** ***・PC-FAX 受信設定オブジェクト*** ***・送信宛先データオブジェクト*** ***※ オブジェクト属性は、存在しない。***
[割付: *アクセス制御 SFP*]: ***設定管理アクセス制御***
FDP_ACF.1.2[3]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]: ***管理者属性を持つ利用者を代行するタスクは、SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクト、PC-FAX 受信設定オブジェクト、送信宛先データオブジェクトを設定、リストア操作することが許可される。***
FDP_ACF.1.3[3]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]: ***なし***
FDP_ACF.1.4[3]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[3]）、FMT_MSA.3（適用しない）

FDP_ACF.1[4] セキュリティ属性によるアクセス制御

FDP_ACF.1.1[4]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　⇒　・ユーザ属性（ユーザ ID）*** ***・管理者属性*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・認証&プリントファイル　⇒　・ユーザ属性（ユーザ ID）***
[割付: *アクセス制御 SFP*]: ***認証&プリントファイルアクセス制御***
FDP_ACF.1.2[4]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]: ***利用者を代行するタスクは、サブジェクト属性のユーザ属性（ユーザ ID）と一致するオブジェクト属性のユーザ属性を持つ認証&プリントファイルに対して、一覧表示、印刷操作をすることが許可される。***
FDP_ACF.1.3[4]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]: ***管理者属性を有する利用者を代行するタスクは、認証&プリントファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[4]
TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[4]）、FMT_MSA.3（FMT_MSA.3[4]）

FDP_IFC.1 サブセット情報フロー制御

FDP_IFC.1.1
TSF は、[割付: *SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト*]に対して[割付: *情報フロー制御 SFP*]を実施しなければならない。
[割付: *SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト*]: ***＜サブジェクト＞***

・FAX ユニットからの受信 ***＜情報＞*** ***・公衆回線からの受信データ*** ***＜操作＞*** ***・内部ネットワークへ送出する***
[割付: *情報フロー制御 SFP*]: ***FAX 情報フロー制御***
下位階層　:　なし 依存性　:　FDP_IFF.1（FDP_IFF.1）

FDP_IFF.1　　単純セキュリティ属性
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、[割付: *情報フロー制御 SFP*]を実施しなければならない。: [割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性*]
[割付: *情報フロー制御 SFP*]: ***FAX 情報フロー制御***
: [割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性*]: ***＜サブジェクト＞*** ***・FAX ユニットからの受信*** ***＜情報＞*** ***・公衆回線からの受信データ*** ***＜セキュリティ属性＞*** ***・画像データ属性*** ***・画像データ以外のデータ属性***
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: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]。
[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]: ***FAX ユニットから受信した画像データ以外のデータを内部ネットワークへ送出しない。***
FDP_IFF.1.3
TSF は、[割付: *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。
[割付: *追加の情報フロー制御 SFP 規則*]: ***なし***
FDP_IFF.1.4
TSF は、以下の規則、[割付: *セキュリティ属性に基づいて情報フローを明示的に許可する規則*]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。
[割付: *セキュリティ属性に基づいて情報フローを明示的に許可する規則*]: ***なし***
FDP_IFF.1.5
TSF は、以下の規則、[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]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。
[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]: ***なし***
下位階層　:　なし 依存性　:　FDP_IFC.1（FDP_IFC.1）、FMT_MSA.3（適用しない）

FDP_RIP.1　　サブセット情報保護
FDP_RIP.1.1
TSF は、[割付: *オブジェクトのリスト*]のオブジェクト[選択:*への資源の割当て、からの資源の割当て解除*]

において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。
[割付: *オブジェクトのリスト*] : ***・ボックスファイル*** ***・セキュリティ文書ファイル*** ***・認証&プリントファイル*** ***・保存画像ファイル*** ***・HDD 残存画像ファイル*** ***・画像関連ファイル***
[選択: *への資源の割当て、からの資源の割当て解除*] : ***からの資源の割当て解除***
下位階層　　:　なし 依存性　　:　なし

6.1.1.3. 識別と認証

FIA_AFL.1[1]　　認証失敗時の取り扱い
FIA_AFL.1.1[1]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*] : ***・サービスモードにアクセスする際の認証*** ***・CE パスワードを改変する際の再認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] : ***[割付: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[1]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*] : **に達する**
[割付: *アクションのリスト*] : ***＜検出した際のアクション＞*** ***・認証中であれば、サービスモードへの認証状態からログアウトし、CE パスワードを利用する認証機能をロックする。*** ***・認証中でなければ、CE パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***特定操作より CE 認証ロック解除機能を実行する。（特定操作から CE 認証の操作禁止解除時間設定に設定されている時間を経過すると解除処理が行なわれる。）***
下位階層　　:　なし
依存性　　:　FIA_UAU.1（FIA_UAU.2[1]）

FIA_AFL.1[2]　　認証失敗時の取り扱い
FIA_AFL.1.1[2]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*] : ***・管理者モードにアクセスする際の認証*** ***・管理者パスワードを改変する際の再認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] : ***[割付: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[2]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]

をしなければならない。
[選択: *に達する、を上回った*]: **に達する**
[割付: *アクションのリスト*]: ***＜検出した際のアクション＞*** ***・認証中であれば、管理者モードへの認証状態からログアウトし、管理者パスワードを利用する認証機能をロックする。*** ***・認証中でなければ、管理者パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***・TOE の起動処理を行う。（起動処理から管理者認証の操作禁止解除時間設定に設定されている時間を経過後に解除処理が行なわれる。）***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[3]　　認証失敗時の取り扱い
FIA_AFL.1.1[3]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*]: ***・SNMP を利用して MIB オブジェクトへアクセスする際の認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]: ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[3]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*]: **に達する**
[割付: *アクションのリスト*]: ***＜検出した際のアクション＞*** ***MIB オブジェクトへのアクセスを拒否し、SNMP パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[4]　　認証失敗時の取り扱い
FIA_AFL.1.1[4]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*]: ***・ユーザが TOE にアクセスする際の認証*** ***・ユーザがユーザ自身のユーザパスワードを変更する際の再認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]: ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[4]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*]: **に達する**
[割付: *アクションのリスト*]: ***＜検出した際のアクション＞*** ***・認証中であれば、当該ユーザの認証状態からログアウトし、当該ユーザに対する認証機能をロックする。***

・認証中でなければ、ユーザパスワードを利用する認証機能をロックする。 ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.1[1]）

FIA_AFL.1[5]　　認証失敗時の取り扱い
FIA_AFL.1.1[5]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*]: ***セキュリティ文書ファイルにアクセスする際の認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]: ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[5]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*]: **に達する**
[割付: *アクションのリスト*]: ***＜検出した際のアクション＞*** ***当該セキュリティ文書ファイルへのアクセスを拒否し、当該セキュリティ文書ファイルに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[3]）

FIA_AFL.1[6]　　認証失敗時の取り扱い
FIA_AFL.1.1[6]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*]: ***・共有ボックスにアクセスする際の認証*** ***・共有ボックスの利用を許可されたユーザが、当該共有ボックスのボックスパスワードを変更する際の再認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]: ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[6]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*]: **に達する**
[割付: *アクションのリスト*]: ***＜検出した際のアクション＞*** ***・認証中であれば、当該ボックスの認証状態からログアウトし、当該ボックスに対する認証機能をロックする。*** ***・認証中でなければ、ボックスパスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[4]）

FIA_AFL.1[7]　　認証失敗時の取り扱い
FIA_AFL.1.1[7]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*] : ***・部門認証：連動方式においてアクセスするユーザの所属部門が未登録の場合の部門認証*** ***・部門認証：個別認証方式においてアクセスするユーザの部門認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] : ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[7]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*] : **に達する**
[割付: *アクションのリスト*] : ***＜検出した際のアクション＞*** ***当該部門に対する認証機能をロックし、以降当該部門の利用を許可されたユーザの TOE へのアクセスを拒否する。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.1[2]）

FIA_AFL.1[8]　　認証失敗時の取り扱い
FIA_AFL.1.1[8]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]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。
[割付: *認証事象のリスト*] : ***・パネルよりサービスモードにアクセスする際の認証*** ***・パネルより管理者モードにアクセスする際の認証*** ***・パネルよりユーザが TOE にアクセスする際のユーザ認証*** ***・パネルよりユーザが TOE にアクセスする際の部門認証*** ***・パネルよりセキュリティ文書ファイルにアクセスする際の認証*** ***・パネルより共有ボックスにアクセスする際の認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] : ***[割付:正の整数値]：1***
FIA_AFL.1.2[8]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*] : **に達する**
[割付: *アクションのリスト*] : ***＜検出した際のアクション＞*** ***パネルからのすべての入力受付拒否*** ***＜通常復帰のための操作＞*** ***5 秒経過後に自動解除***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.1[1]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.1[2]）

FIA_ATD.1　　利用者属性定義
FIA_ATD.1.1
TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]
[割付:*セキュリティ属性のリスト*] : ***・ユーザ属性（ユーザ ID）*** ***・ボックス属性（ボックス ID）*** ***・ファイル属性（セキュリティ文書内部制御 ID）*** ***・所属部門（部門 ID）*** ***・管理者属性***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[1]　　秘密の検証
FIA_SOS.1.1[1]
TSF は、秘密 ***(ユーザパスワード、管理者パスワード、CE パスワード、セキュリティ文書パスワード、ボックスパスワード、部門パスワード)*** が[割付: *定義された品質尺度*]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。
[割付: *定義された品質尺度*] : ***・桁数　：8 桁以上 64 桁まで*** ***・文字種：94 文字以上の中から選択可能*** ***・規則　：① 同一の文字だけで構成されていない。*** ***② 変更する場合、変更後の値が現在設定されている値と合致しない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[2]　　秘密の検証
FIA_SOS.1.1[2]
TSF は、秘密 ***(SNMP パスワード)*** が[割付: *定義された品質尺度*]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。
[割付: *定義された品質尺度*] : ***・桁数　：8 桁以上 32 桁まで*** ***・文字種：90 文字以上の中から選択可能*** ***・規則　：① 同一の文字だけで構成されていない。*** ***② 変更する場合、変更後の値が現在設定されている値と合致しない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[3]　　秘密の検証
FIA_SOS.1.1[3]
TSF は、秘密 ***(暗号化ワード)*** が[割付: *定義された品質尺度*]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。
[割付: *定義された品質尺度*] : ***・桁数　：20 桁*** ***・文字種：83 文字以上の中から選択可能*** ***・・規則　：① 同一の文字だけで構成されていない。***

② 変更する場合、変更後の値が現在設定されている値と合致しない。
下位階層 : なし
依存性 : なし

FIA_SOS.1[4]　　秘密の検証
FIA_SOS.1.1[4]
TSF は、秘密 ***（セッション情報）*** が[割付: *定義された品質尺度*]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。
[割付: *定義された品質尺度*] : ***10^{10} 以上***
下位階層 : なし
依存性 : なし

FIA_SOS.2　　秘密の検証
FIA_SOS.2.1
TSF は、[割付: *定義された品質尺度*]に合致する秘密（***セッション情報***）を生成するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ***10^{10} 以上***
FIA_SOS.2.2
TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付: *TSF 機能のリスト*] : ***・管理者認証（ネットワーク経由アクセス）*** ***・ユーザ認証（ネットワーク経由アクセス）*** ***・ボックス認証（ネットワーク経由アクセス）***
下位階層 : なし
依存性 : なし

FIA_UAU.1[1]　　認証のタイミング
FIA_UAU.1.1[1]
TSF は、利用者が認証される前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。
[割付: *TSF 仲介アクションのリスト*] : ***ユーザ利用停止状態の確認（ユーザ認証方式：本体認証においてのみ）***
FIA_UAU.1.2[1]
TSF は、その利用者 ***（ユーザ）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（ユーザ）*** に認証が成功することを要求しなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[3]）

FIA_UAU.1[2]　　認証のタイミング
FIA_UAU.1.1[2]
TSF は、利用者が認証される前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。
[割付: *TSF 仲介アクションのリスト*] : ***部門利用停止状態の確認***

FIA_UAU.1.2[2]
TSF は、その利用者 ***(部門の利用を許可されたユーザ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(部門の利用を許可されたユーザ)*** に認証が成功することを要求しなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[3]）

FIA_UAU.2[1] アクション前の利用者認証

FIA_UAU.2.1[1]
TSF は、その利用者 ***(サービスエンジニア)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(サービスエンジニア)*** に認証が成功することを要求しなければならない。
下位階層 : FIA_UAU.1
依存性 : FIA_UID.1（FIA_UID.2[1]）

FIA_UAU.2[2] アクション前の利用者認証

FIA_UAU.2.1[2]
TSF は、その利用者 ***(管理者(管理者パスワードにより認証される利用者、SNMP パスワードによる認証される利用者))*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(管理者(管理者パスワードにより認証される利用者、SNMP パスワードによる認証される利用者))*** に認証が成功することを要求しなければならない。
下位階層 : FIA_UAU.1
依存性 : FIA_UID.1（FIA_UID.2[2]）

FIA_UAU.2[3] アクション前の利用者認証

FIA_UAU.2.1[3]
TSF は、その利用者 ***(セキュリティ文書ファイルの利用を許可されたユーザ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(セキュリティ文書ファイルの利用を許可されたユーザ)*** に認証が成功することを要求しなければならない。
下位階層 : FIA_UAU.1
依存性 : FIA_UID.1（FIA_UID.2[4]）

FIA_UAU.2[4] アクション前の利用者認証

FIA_UAU.2.1[4]
TSF は、その利用者 ***(共有ボックスの利用を許可されたユーザ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(共有ボックスの利用を許可されたユーザ)*** に認証が成功することを要求しなければならない。
下位階層 : FIA_UAU.1
依存性 : FIA_UID.1（FIA_UID.2[5]）

FIA_UAU.6 再認証

FIA_UAU.6.1
TSF は、条件[割付: *再認証が要求される条件のリスト*]のもとで利用者を再認証しなければならない。
[割付: *再認証が要求される条件のリスト*] ***・サービスエンジニアが CE パスワードを変更する場合***

・管理者が管理者パスワードを変更する場合 ***・ユーザがユーザ自身のユーザパスワードを変更する場合*** ***・共有ボックスの利用を許可されたユーザが当該共有ボックスのボックスパスワードを変更する場合***
下位階層　：　なし
依存性　：　なし

FIA_UAU.7　保護された認証フィードバック
FIA_UAU.7.1
TSF は、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。
[割付: *フィードバックのリスト*]: ***入力された文字データ 1 文字毎に“＊”の表示***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.1[1]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.1[2]）

FIA_UID.2[1]　アクション前の利用者識別
FIA_UID.2.1[1]
TSF は、その利用者 ***（サービスエンジニア）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（サービスエンジニア）*** に識別が成功することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[2]　アクション前の利用者識別
FIA_UID.2.1[2]
TSF は、その利用者 ***（管理者）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（管理者）*** に識別が成功することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[3]　アクション前の利用者識別
FIA_UID.2.1[3]
TSF は、その利用者 ***（ユーザ）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（ユーザ）*** に識別が成功することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[4]　アクション前の利用者識別
FIA_UID.2.1[4]
TSF は、その利用者 ***（セキュリティ文書ファイルの利用を許可されたユーザ）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（セキュリティ文書ファイルの利用を許可されたユーザ）*** に識別が成功することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[5]	**アクション前の利用者識別**
FIA_UID.2.1[5]	
TSF は、その利用者 ***(共有ボックスの利用を許可されたユーザ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(共有ボックスの利用を許可されたユーザ)*** に識別が成功することを要求しなければならない。	
下位階層	: FIA_UID.1
依存性	: なし

FIA_UID.2[6]	**アクション前の利用者識別**
FIA_UID.2.1[6]	
TSF は、その利用者 ***(部門の利用を許可されたユーザ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(部門の利用を許可されたユーザ)*** に識別が成功することを要求しなければならない。	
下位階層	: FIA_UID.1
依存性	: なし

FIA_UID.2[7]	**アクション前の利用者識別**
FIA_UID.2.1[7]	
TSF は、その利用者 ***(外部サーバ)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(外部サーバ)*** に識別が成功することを要求しなければならない。	
下位階層	: FIA_UID.1
依存性	: なし

FIA_USB.1	**利用者・サブジェクト結合**
FIA_USB.1.1	
TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: *利用者セキュリティ属性のリスト*]	
[割付: *利用者セキュリティ属性のリスト*] : ***・ユーザ属性（ユーザ ID）*** ***・ボックス属性（ボックス ID）*** ***・ファイル属性（セキュリティ文書内部制御 ID）*** ***・所属部門（部門 ID）*** ***・管理者属性***	
FIA_USB.1.2	
TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の最初の関連付けの規則*]	
[割付: *属性の最初の関連付けの規則*] : ***＜ボックス属性の場合＞*** ***ボックスに対するアクセスにおいて認証された際に、利用者を代行するタスクに当該ボックスのボックス ID を関連付ける。*** ***＜所属部門の場合＞*** ***・部門認証方式が個別認証方式の場合、部門に対するアクセスにおいて認証された際に、利用者を代行するタスクに当該部門の部門 ID を関連付ける。*** ***・部門認証方式がユーザ認証連動方式の場合、ユーザに対するアクセスにおいて認証された際に、利用者を代行するタスクに当該ユーザに設定されている部門 ID を関連づける。*** ***＜ファイル属性の場合＞***	

セキュリティ文書ファイルに対するアクセスにおいて認証された際に、利用者を代行するタスクに、当該セキュリティ文書ファイルのセキュリティ文書内部制御 ID を関連付ける。 ***＜ユーザ属性の場合＞*** ***ユーザとして認証された際に、利用者を代行するタスクに当該ユーザのユーザ ID を関連付ける。*** ***＜管理者属性の場合＞*** ***管理者として認証された際に、利用者を代行するタスクに管理者属性を関連付ける。***
FIA_USB.1.3
TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の変更の規則*]
[割付: *属性の変更の規則*]: ***なし***
下位階層 : なし
依存性 : FIA_ATD.1（FIA_ATD.1）

6.1.1.4. セキュリティ管理

FMT_MOF.1[1] セキュリティ機能のふるまい管理
FMT_MOF.1.1[1]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***セキュリティ強化設定***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***を停止する***
[割付: *許可された識別された役割*]: ***・管理者*** ***・サービスエンジニア***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MOF.1[2] セキュリティ機能のふるまい管理
FMT_MOF.1.1[2]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***・ユーザ認証機能*** ***・S/MIME 機能*** ***・SNMP パスワード認証機能*** ***・認証＆プリント機能*** ***・HDD データ上書き削除機能*** ***・監査ログ機能***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***のふるまいを改変する***
[割付: *許可された識別された役割*]: ***管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MOF.1[3] セキュリティ機能のふるまい管理

FMT_MOF.1.1[3]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***・部門認証機能（管理者用）*** ***・高信頼チャネル機能***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***のふるまいを改変する、を停止する***
[割付: *許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MOF.1[4]　セキュリティ機能のふるまい管理

FMT_MOF.1.1[4]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***・全領域上書き削除機能***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***を動作させる***
[割付: *許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MOF.1[5]　セキュリティ機能のふるまい管理

FMT_MOF.1.1[5]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***・部門認証機能（ユーザ用）***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***のふるまいを改変する***
[割付: *許可された識別された役割*]: ***その部門の利用を許可されたユーザ***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[6]）

FMT_MSA.1[1]　セキュリティ属性の管理

FMT_MSA.1.1[1]
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付: *セキュリティ属性のリスト*]: ***ユーザ自身の「ユーザ ID」が設定されるボックスのユーザ属性***
[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]: ***改変（他のユーザの「ユーザ ID」、または「部門 ID」、または「共有」に改変）***

[割付: *許可された識別された役割*]: ***・ユーザ*** ***・管理者***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]: ***ボックスアクセス制御***
下位階層 : なし
依存性 : FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[1]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

FMT_MSA.1[2] セキュリティ属性の管理
FMT_MSA.1.1[2]
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付: *セキュリティ属性のリスト*]: ***「共有」が設定されるボックスのユーザ属性***
[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]: ***改変（「ユーザ ID」、または「部門 ID」へ改変）***
[割付: *許可された識別された役割*]: ***・その共有ボックスの利用を許可されたユーザ*** ***・管理者***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]: ***ボックスアクセス制御***
下位階層 : なし
依存性 : FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[1]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[4]）

FMT_MSA.1[3] セキュリティ属性の管理
FMT_MSA.1.1[3]
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付: *セキュリティ属性のリスト*]: ***「部門 ID」が設定されるボックスのユーザ属性***
[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]: ***改変（「ユーザ ID」、または「共有」、または他の部門 ID へ改変）***
[割付: *許可された識別された役割*]: ***・その部門の利用を許可されたユーザ*** ***・管理者***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]: ***ボックスアクセス制御***
下位階層 : なし
依存性 : FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[1]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[6]）

FMT_MSA.3[1] 静的属性初期化
FMT_MSA.3.1[1]
TSF は、その SFP を実施するために使われるセキュリティ属性 ***(ボックスのユーザ属性)*** に対して[選択: *制限的、許可的、[割付: その他の特性]: から 1 つのみ選択*]デフォルト値を与える[割付: *アクセス制御 SFP、*

情報フロー制御 SFP]を実施しなければならない。
[選択: *制限的*、*許可的*、*[割付: その他の特性]: から 1 つのみ選択*] : ***[割付：その他の特性]：以下のケースに分類されるボックスの登録状況に応じた*** ***① ユーザ、または管理者の登録操作によるボックスの登録の場合は「共有」*** ***② 未登録ボックスを指定したボックス保存ジョブの動作に伴う個人ボックスの自動ボックス登録の場合は当該ジョブを実行したユーザの「ユーザ ID」***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] : ***ボックスアクセス制御***
FMT_MSA.3.2[1]
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***FMT_MSA.3.1 の「その他の特性」にて示される①のケース：ユーザ、管理者*** ***FMT_MSA.3.1 の「その他の特性」にて示される②のケース：なし***
下位階層　：　なし
依存性　：　FMT_MSA.1（FMT_MSA.1[1]、FMT_MSA.1[2]）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

FMT_MSA.3[2]　静的属性初期化
FMT_MSA.3.1[2]
TSF は、その SFP を実施するために使われるセキュリティ属性 ***（セキュリティ文書内部制御 ID）*** に対して[選択: *制限的*、*許可的*、*[割付: その他の特性]: から 1 つのみ選択*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。
[選択: *制限的*、*許可的*、*[割付: その他の特性]: から 1 つのみ選択*] : ***[割付 ：その他の特性]：一意に識別される***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] : ***セキュリティ文書ファイルアクセス制御***
FMT_MSA.3.2[2]
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***該当なし***
下位階層　：　なし
依存性　：　FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない）

FMT_MSA.3[3]　静的属性初期化
FMT_MSA.3.1[3]
TSF は、その SFP を実施するために使われるセキュリティ属性 ***（ボックスファイルのボックス属性）*** に対して[選択: *制限的*、*許可的*、*[割付: その他の特性]: から 1 つのみ選択*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。
[選択: *制限的*、*許可的*、*[割付: その他の特性]: から 1 つのみ選択*] : ***[割付：その他の特性]：当該ボックスファイルを保存する対象として選択されたボックスのボックス属性の値と一致する***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] : ***ボックスアクセス制御***
FMT_MSA.3.2[3]
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***なし***
下位階層　：　なし

依存性	:	FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない）

FMT_MSA.3[4]　　静的属性初期化
FMT_MSA.3.1[4]
TSF は、その SFP を実施するために使われるセキュリティ属性（***認証&プリントファイルのユーザ属性***）として、[選択: *制限的、許可的：から一つのみ選択*、*[割付：その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。
[選択: *制限的、許可的：から一つのみ選択*、*[割付：その他の特性]*]： ***[割付：その他の特性]：当該認証&プリントファイルを保存する利用者のユーザ属性の値と一致する***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]： ***認証&プリントファイルアクセス制御***
FMT_MSA.3.2[4]
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***なし***
下位階層　: なし
依存性　: FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない）

FMT_MTD.1[1]　　TSF データの管理
FMT_MTD.1.1[1]
（ユーザ認証の方式に「本体認証」が選択されている場合、）TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***ユーザパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]： ***管理者***
下位階層　: なし
依存性　: FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[2]　　TSF データの管理
FMT_MTD.1.1[2]
（ユーザ認証の方式に「本体認証」が選択されている場合、）TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***ユーザ自身のユーザパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***改変***
[割付:*許可された識別された役割*]： ***・ユーザ*** ***・管理者***
下位階層　: なし
依存性　: FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

FMT_MTD.1[3] TSF データの管理
FMT_MTD.1.1[3]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・ユーザ ID*** ***・部門 ID*** ***・部門パスワード*** ***・セキュリティ文書パスワード*** ***・システムオートリセット時間*** ***・認証失敗回数閾値*** ***・外部サーバ認証設定データ*** ***・S/MIME 証明書[9]*** ***・所属部門*** ***・管理者認証の操作禁止解除時間*** ***・暗号化ワード*** ***・SNMP パスワード*** ***・TSI 受信設定データ***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[4] TSF データの管理
FMT_MTD.1.1[4]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***当該ボックスのボックスパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***・その共有ボックスの利用を許可されたユーザ*** ***・管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[4]）

FMT_MTD.1[5] TSF データの管理
FMT_MTD.1.1[5]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ボックスパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]:

[9] 値そのものを改変するのではなく、ユーザ毎に設定可能なデジタル証明書を入れ替える操作を意図している。

[割付：その他の操作]：登録
[割付:*許可された識別された役割*]： ***・ユーザ*** ***・管理者***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

FMT_MTD.1[6]　TSF データの管理

FMT_MTD.1.1[6]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***管理者パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***改変***
[割付:*許可された識別された役割*]： ***・管理者*** ***・サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MTD.1[7]　TSF データの管理

FMT_MTD.1.1[7]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***・SNMP パスワード*** ***・ユーザパスワード*** ***・部門パスワード*** ***・ボックスパスワード*** ***・セキュリティ文書パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***問い合わせ***
[割付:*許可された識別された役割*]： ***管理者***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[8]　TSF データの管理

FMT_MTD.1.1[8]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***セキュリティ文書パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]： ***ユーザ***
下位階層　：　なし

依存性	:	FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[3]）

FMT_MTD.1[9]　TSF データの管理
FMT_MTD.1.1[9]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・CE パスワード*** ***・CE 認証の操作禁止解除時間***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***サービスエンジニア***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]）

FMT_MTD.1[10]　TSF データの管理
FMT_MTD.1.1[10]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ユーザ ID***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***管理者、外部サーバ***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[5]）

FMT_MTD.1[11]　TSF データの管理
FMT_MTD.1.1[11]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・部門 ID*** ***・部門パスワード*** ***・S/MIME 証明書*** ***・TSI 受信設定データ*** ***・外部サーバ認証設定データ***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[12] TSF データの管理
FMT_MTD.1.1[12]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*] : ***ユーザ自身の所属部門***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*] : ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*] : ***管理者、その部門の利用を許可されたユーザ [10]***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[6]）

FMT_MTD.1[13] TSF データの管理
FMT_MTD.1.1[13]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*] : ***ユーザ ID*** ***部門 ID***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*] : ***[割付：その他の操作]：停止、及び再開***
[割付:*許可された識別された役割*] : ***管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[5]）

FMT_MTD.1[14] TSF データの管理
FMT_MTD.1.1[14]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*] : ***監査ログ***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*] : ***問い合わせ、削除***
[割付:*許可された識別された役割*] : ***管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[15] TSF データの管理
FMT_MTD.1.1[15]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: そ*

[10] 所属部門が関連付けられていないユーザで、その部門 ID に対する部門パスワードを管理者からオフラインで知らされたユーザのこと。

の他の操作]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***日時情報***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_SMF.1　　管理機能の特定

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。: [割付: *TSF によって提供される管理機能のリスト*]

[割付: *TSF によって提供される管理機能のリスト*]:

- ***管理者によるセキュリティ強化機能の停止機能***
- ***管理者による認証＆プリント機能の動作設定機能***
- ***管理者によるユーザ認証機能の動作方式設定機能***
- ***管理者による部門認証機能の動作方式設定機能***
- ***管理者による SNMP パスワード認証機能の動作設定機能***
- ***管理者による認証操作禁止機能における認証失敗回数閾値の設定機能***
- ***管理者によるバックアップ機能*** [11]
- ***管理者によるリストア機能*** [12]
- ***管理者による部門 ID の登録機能***
- ***管理者による部門 ID の改変機能***
- ***管理者による部門パスワードの登録機能***
- ***管理者による部門パスワードの改変機能***
- ***管理者によるパネルオートログアウト時間設定機能***
- ***管理者による管理者パスワードの改変機能***
- ***管理者による SNMP パスワードの改変機能***
- ***管理者によるボックスパスワードの登録機能***
- ***管理者によるボックスパスワードの改変機能***
- ***管理者によるボックス登録機能***
- ***管理者によるボックスのユーザ属性の改変機能***
- ***管理者によるユーザ ID の登録機能***
- ***管理者によるユーザの利用停止機能***
- ***管理者によるユーザの利用再開機能***
- ***管理者による部門の利用停止機能***
- ***管理者による部門の利用再開機能***
- ***管理者によるユーザ認証の方式が本体認証の場合におけるユーザパスワードの登録機能***
- ***管理者によるユーザ認証の方式が本体認証の場合におけるユーザパスワードの改変機能***
- ***管理者による S/MIME 証明書登録機能***
- ***管理者による S/MIME 証明書登録変更機能***
- ***管理者による S/MIME 機能の動作設定機能***
- ***管理者による高信頼チャネル機能の動作設定機能***
- ***管理者による所属部門の登録機能***
- ***管理者による所属部門の改変機能***
- ***管理者による管理者認証の操作禁止解除時間の改変機能***
- ***管理者による暗号化ワードの改変機能***
- ***管理者による TSI 受信設定データの改変機能***
- ***管理者による HDD データ上書き削除機能の動作設定機能***

11 バックアップ機能の一部は、TSF データの問い合わせ機能に相当する。

12 リストア機能の一部は、TSF データの改変機能に相当する。

・管理者による全領域上書き削除機能 ・管理者による監査ログの操作機能 ・管理者による監査ログ満杯時の動作設定機能 ・管理者による日時情報の改変機能 ・サービスエンジニアによる CE パスワードの改変機能 ・サービスエンジニアによる管理者パスワードの改変機能 ・サービスエンジニアによるセキュリティ強化機能の停止機能 ・サービスエンジニアによる CE 認証の操作禁止解除時間の改変機能 ・ユーザによるボックスのユーザ属性のデフォルト値上書き機能 ・ユーザによる部門認証の方式がユーザ毎に設定するの場合におけるユーザ自身の部門認証機能の動作方式設定機能 ・ユーザによるユーザ認証の方式が本体認証の場合におけるユーザ自身のユーザパスワードの改変機能 ・ユーザによるボックスパスワードの登録機能 ・ユーザによるボックスのユーザ属性の改変機能 ・その部門の利用を許可されたユーザによる所属部門の登録機能 ・ユーザによるボックス登録機能 ・ユーザによる未登録ボックスを指定したボックス保存ジョブによる個人ボックス自動登録機能 ・ユーザ認証方式が外部サーバ認証の場合における外部サーバによる本体未登録ユーザのユーザ ID 自動登録機能 ・ユーザによるセキュリティ文書ファイル保存に伴うセキュリティ文書パスワードの登録機能 ・共有ボックスの利用を許可されたユーザによる当該ボックスのユーザ属性の改変機能 ・共有ボックスの利用を許可されたユーザによる当該ボックスのボックスパスワードの改変機能 ・グループボックスの利用を許可されたユーザによる当該ボックスのユーザ属性の改変機能
下位階層　：　なし
依存性　：　なし

FMT_SMR.1[1]　セキュリティ役割
FMT_SMR.1.1[1]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： ***サービスエンジニア***
FMT_SMR.1.2[1]
TSF は、利用者を役割に関連付けなければならない。
下位階層　：　なし
依存性　：　FIA_UID.1（FIA_UID.2[1]）

FMT_SMR.1[2]　セキュリティ役割
FMT_SMR.1.1[2]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： ***管理者***
FMT_SMR.1.2[2]
TSF は、利用者を役割に関連付けなければならない。
下位階層　：　なし
依存性　：　FIA_UID.1（FIA_UID.2[2]）

FMT_SMR.1[3]　セキュリティ役割
FMT_SMR.1.1[3]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付: *許可された識別された役割*]: ***ユーザ***
FMT_SMR.1.2[3]
TSF は、利用者を役割に関連付けなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[3]）

FMT_SMR.1[4] セキュリティ役割
FMT_SMR.1.1[4]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]: ***その共有ボックスの利用を許可されたユーザ***
FMT_SMR.1.2[4]
TSF は、利用者を役割に関連付けなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[5]）

FMT_SMR.1[5] セキュリティ役割
FMT_SMR.1.1[5]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]: ***外部サーバ***
FMT_SMR.1.2[5]
TSF は、利用者を役割に関連付けなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[7]）

FMT_SMR.1[6] セキュリティ役割
FMT_SMR.1.1[6]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]: ***その部門の利用を許可されたユーザ***
FMT_SMR.1.2[6]
TSF は、利用者を役割に関連付けなければならない。
下位階層 : なし
依存性 : FIA_UID.1（FIA_UID.2[6]）

6.1.1.5. TOE アクセス

FTA_SSL.3 TSF 起動による終了
FTA_SSL.3.1
TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。
[割付: *利用者が非アクティブである時間間隔*]: ***パネルより管理者、またはユーザが操作中、最終操作からシステムオートリセット時間（1～9 分）によって決定される時間***

下位階層	:	なし
依存性	:	なし

6.1.1.6. 高信頼パス/チャネル

FTP_ITC.1 TSF 間高信頼チャネル
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、[選択: *TSF*、*他の高信頼 IT 製品*]が、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。
[選択: *TSF*、*他の高信頼 IT 製品*] : ***他の高信頼 IT 製品***
FTP_ITC.1.3
TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]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。
[割付: *高信頼チャネルが要求される機能のリスト*] : ***・ボックスファイルのダウンロード*** ***・ボックスファイルとして保存されることになる画像ファイルのアップロード*** ***・セキュリティ文書ファイルになる画像ファイルのアップロード*** ***・認証&プリントファイルになる画像ファイルのアップロード***
下位階層 : なし
依存性 : なし

6.1.1.7. セキュリティ監査

FAU_GEN.1 監査データ生成
FAU_GEN.1.1
TSF は、以下の監査対象事象の監査記録を生成できなければならない: a) 監査機能の起動と終了; b) 監査の[選択: *最小*、*基本*、*詳細*、*指定なし: から 1 つのみ選択*]レベルのすべての監査対象事象;及び c) [割付: *上記以外の個別に定義した監査対象事象*]。
[選択: *最小*、*基本*、*詳細*、*指定なし: から 1 つのみ選択*] : ***指定なし***
[割付: *上記以外の個別に定義した監査対象事象*] : ***「表 8 監査対象事象リスト」に記載***
FAU_GEN.1.2
TSF は、各監査記録において少なくとも以下の情報を記録しなければならない: a) 事象の日付・時刻、事象の種別、サブジェクト識別情報（該当する場合）、事象の結果(成功または失敗);及び b）各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*] 。
[割付: *その他の監査関連情報*] : ***「表 8 監査対象事象リスト」に記載***
下位階層 : なし
依存性 : FPT_STM.1

表 8 監査対象事象リスト

監査事象	関連する機能要件	監査レベル	追加情報
（監視すべき）ジョブの開始と完了	***FDP_ACF.1***	*指定なし*	*ジョブの種類*
すべての認証機能の成功と失敗	***FIA_UAU.2***	*基本*	*なし*

FAU_GEN.2　　利用者識別情報の関連付け

FAU_GEN.2.1

識別された利用者のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

下位階層　：　なし

依存性　：　FAU_GEN.1
FIA_UID.1（FIA_UID.2[1]、FIA_UID.2[2]、FIA_UID.2[3]、FIA_UID.2[4]、FIA_UID.2[5]、FIA_UID.2[6]）

FAU_SAR.1　　監査レビュー

FAU_SAR.1.1

TSF は、[割付: *許可利用者*]が、[割付: *監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付: *許可利用者*]：
管理者

[割付: *監査情報のリスト*]：
「表 8　監査対象事象リスト」に記載される監査ログ

FAU_SAR.1.2

TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

下位階層　：　なし

依存性　：　FAU_GEN.1

FAU_SAR.2　　限定監査レビュー

FAU_SAR.2.1

TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

下位階層　：　なし

依存性　：　FAU_SAR.1

FAU_STG.1　　保護された監査証跡格納

FAU_STG.1.1

TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSF は、監査証跡に格納された監査記録への不正な改変を[選択: *防止*、*検出: から 1 つのみ選択*]できなければならない。

[選択: *防止*、*検出: から 1 つのみ選択*]：
防止

下位階層　：　なし

依存性　：　FAU_GEN.1

FAU_STG.4[1]　　監査データ損失の防止
FAU_STG.4.1[1]
TSF は、監査証跡が満杯になった場合 ***(監査証跡が満杯になった時の動作が「上書き禁止」に設定された状態で、監査証跡が満杯になった場合)***、[選択: *監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択*]及び[割付: *監査格納失敗時にとられるその他のアクション*]を行わなければならない。
[選択: *監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択*]: ***監査事象の無視***
[割付: *監査格納失敗時にとられるその他のアクション*]: ***ジョブの受付停止***
下位階層　:　なし
依存性　:　FAU_STG.1

FAU_STG.4[2]　　監査データ損失の防止
FAU_STG.4.1[2]
TSF は、監査証跡が満杯になった場合 ***(監査証跡が満杯になった時の動作が「上書き許可」に設定された状態で、監査証跡が満杯になった場合)***、[選択: *監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択*]及び[割付: *監査格納失敗時にとられるその他のアクション*]を行わなければならない。
[選択: *監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択*]: ***最も古くに格納された監査記録への上書き***
[割付: *監査格納失敗時にとられるその他のアクション*]: ***なし***
下位階層　:　なし
依存性　:　FAU_STG.1

FPT_STM.1　　タイムスタンプ
FPT_STM.1.1
TSF は、高信頼タイムスタンプを提供できなければならない。
下位階層　:　なし
依存性　:　なし

6.1.1.8. 拡張：IT 環境エンティティの利用するための能力

FIT_CAP.1[1]　　IT 環境エンティティのセキュリティサービス利用時の能力
FIT_CAP.1.1[1]
TSF は、[割付: *IT 環境エンティティが提供するセキュリティサービス*]に対して、そのサービスを利用するために必要な能力を提供しなければならない: [割付: *セキュリティサービスの動作に必要な能力のリスト*]。
[割付: *IT 環境エンティティが提供するセキュリティサービス*] ***ActiveDirectory を用いたユーザ情報管理サーバが実現するユーザ認証機能***
[割付: *セキュリティサービスの動作に必要な能力のリスト*] ***・識別認証対象のユーザに対する認証情報問い合わせ機能***

・識別認証対象のユーザに対する認証情報取得機能
下位階層　：　なし
依存性　：　なし

FIT_CAP.1[2]　IT 環境エンティティのセキュリティサービス利用時の能力
FIT_CAP.1.1[2]
TSF は、[割付: *IT 環境エンティティが提供するセキュリティサービス*]に対して、そのサービスを利用するために必要な能力を提供しなければならない: [割付: *セキュリティサービスの動作に必要な能力のリスト*]。
[割付: *IT 環境エンティティが提供するセキュリティサービス*] ***ASIC が実現する HDD 暗号化機能***
[割付: *セキュリティサービスの動作に必要な能力のリスト*] ***画像ファイルを HDD 暗号化機能で処理させるためのサポート機能***
下位階層　：　なし
依存性　：　なし

6.1.2. TOE のセキュリティ保証要件

TOE は、一般的なオフィス環境にて利用される商用事務製品であるため、商用事務製品の保証として十分なレベルである EAL3 適合によって必要な TOE セキュリティ保証要件を適用する。下表に適用される TOE のセキュリティ保証要件をまとめる。

表 9 TOE のセキュリティ保証要件

TOEセキュリティ保証要件		コンポーネント
開発	セキュリティアーキテクチャ記述	ADV_ARC.1
	完全な要約を伴う機能仕様	ADV_FSP.3
	アーキテクチャ設計	ADV_TDS.2
ガイダンス文書	利用者操作ガイダンス	AGD_OPE.1
	準備手続き	AGD_PRE.1
ライフサイクルサポート	許可の管理	ALC_CMC.3
	実装表現の CM 範囲	ALC_CMS.3
	配付手続き	ALC_DEL.1
	セキュリティ手段の識別	ALC_DVS.1
	開発者によるライフサイクルモデルの定義	ALC_LCD.1
セキュリティターゲット評価	適合主張	ASE_CCL.1
	拡張コンポーネント定義	ASE_ECD.1
	ST 概説	ASE_INT.1
	セキュリティ対策方針	ASE_OBJ.2
	派生したセキュリティ要件	ASE_REQ.2
	セキュリティ課題定義	ASE_SPD.1
	TOE 要約仕様	ASE_TSS.1
テスト	カバレージの分析	ATE_COV.2
	テスト：基本設計	ATE_DPT.1
	機能テスト	ATE_FUN.1
	独立テスト - サンプル	ATE_IND.2
脆弱性評定	脆弱性分析	AVA_VAN.2

6.2. IT セキュリティ要件根拠

6.2.1. IT セキュリティ機能要件根拠

6.2.1.1. 必要性

セキュリティ対策方針と IT セキュリティ機能要件の対応関係を下表に示す。IT セキュリティ機能要件が少なくとも 1 つ以上のセキュリティ対策方針に対応していることを示している。

表 10　セキュリティ対策方針に対する IT セキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	※ set.admin	※ set.service
set.admin	●	●	●	●	●	●										
set.service	●	●	●	●	●	●										
FAU_GEN.1														●		
FAU_GEN.2														●		
FAU_SAR.1														●		
FAU_SAR.2														●		
FAU_STG.1														●		
FAU_STG.4														●		
FCS_CKM.1								●		●						
FCS_COP.1										●						
FDP_ACC.1[1]		●	●	●		●										
FDP_ACC.1[2]					●	●										
FDP_ACC.1[3]						●										
FDP_ACC.1[4]					●	●										
FDP_ACF.1[1]		●	●	●		●										
FDP_ACF.1[2]					●	●										
FDP_ACF.1[3]						●										
FDP_ACF.1[4]					●	●										
FDP_IFC.1											●					
FDP_IFF.1											●					
FDP_RIP.1							●									
FIA_AFL.1[1]																●
FIA_AFL.1[2]															●	
FIA_AFL.1[3]						●										
FIA_AFL.1[4]	●															
FIA_AFL.1[5]					●											
FIA_AFL.1[6]			●													
FIA_AFL.1[7]				●												
FIA_AFL.1[8]	●		●	●	●										●	●
FIA_ATD.1		●	●	●	●	●										
FIA_SOS.1[1]	●		●	●	●	●									●	●
FIA_SOS.1[2]						●										
FIA_SOS.1[3]						●										
FIA_SOS.1[4]	●		●												●	
FIA_SOS.2	●		●												●	

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	※ set.admin	※ set.service
FIA_UAU.2[1]																●
FIA_UAU.2[2]						●									●	
FIA_UAU.1[1]	●															
FIA_UAU.2[3]					●											
FIA_UAU.2[4]			●													
FIA_UAU.1[2]				●												
FIA_UAU.6	●		●			●									●	●
FIA_UAU.7	●		●	●	●										●	●
FIA_UID.2[1]																●
FIA_UID.2[2]						●									●	
FIA_UID.2[3]	●															
FIA_UID.2[4]					●											
FIA_UID.2[5]			●													
FIA_UID.2[6]				●												
FIA_UID.2[7]	●															
FIA_USB.1		●	●	●	●	●										
FMT_MOF.1[1]						●										
FMT_MOF.1[2]	●				●	●										
FMT_MOF.1[3]				●		●										
FMT_MOF.1[4]						●										
FMT_MOF.1[5]				●												
FMT_MSA.1[1]		●				●										
FMT_MSA.1[2]			●			●										
FMT_MSA.1[3]				●		●										
FMT_MSA.3[1]		●	●													
FMT_MSA.3[2]					●											
FMT_MSA.3[3]		●	●	●												
FMT_MSA.3[4]					●											
FMT_MTD.1[1]	●															
FMT_MTD.1[2]	●					●										
FMT_MTD.1[3]	●		●	●	●	●									●	●
FMT_MTD.1[4]			●			●										
FMT_MTD.1[5]			●													
FMT_MTD.1[6]															●	
FMT_MTD.1[7]						●										
FMT_MTD.1[8]					●											
FMT_MTD.1[9]																●
FMT_MTD.1[10]	●															
FMT_MTD.1[11]				●		●										
FMT_MTD.1[12]				●												
FMT_MTD.1[13]	●			●												
FMT_MTD.1[14]						●										
FMT_MTD.1[15]						●										
FMT_SMF.1	●	●	●	●	●	●									●	●
FMT_SMR.1[1]						●									●	●
FMT_SMR.1[2]	●	●	●	●	●	●									●	
FMT_SMR.1[3]	●	●			●											
FMT_SMR.1[4]			●													
FMT_SMR.1[5]	●															

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE	O.CRYPTO-KEY	O.TRUSTED-PASS	O.CRYPTO-MAIL	O.FAX-CONTROL	O.AUTH-CAPABILITY	O.CRYPTO-CAPABILITY	O.AUDIT-LOGGED	※ set.admin	※ set.service
FMT_SMR.1[6]				●												
FPT_STM.1														●		
FTA_SSL.3	●														●	
FTP_ITC.1									●							
FIT_CAP.1[1]												●				
FIT_CAP.1[2]													●			

注) ***set.admin***、***set.service*** は、要件のセットを示しており、「●」が記され対応関係があるとされるセキュリティ対策方針は、縦軸の※ set.admin、※ set.service にて対応付けられる一連の要件セットが、当該セキュリティ対策方針にも対応していることを示す。

6.2.1.2. 十分性

各セキュリティ対策方針に対して適用される IT セキュリティ機能要件について以下に説明する。

- **O.REGISTERED-USER（許可ユーザの利用）**

本セキュリティ対策方針は、識別認証に成功したユーザだけに TOE が搭載される MFP の利用を制限しており、ユーザの識別認証に関係して諸要件が必要である。

＜ユーザの識別認証に必要な要件＞

FIA_UID.2[3]、FIA_UAU.1[1]により、アクセスする利用者が、許可ユーザであることを識別認証する。

認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“*”を返し、認証をサポートする。

FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[4]により不成功認証が 1～3 回に達すると、以降そのユーザに対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。

「本体認証」、「外部サーバ認証」といったユーザ認証方式の選択は、FMT_MOF.1[2]により、管理者だけに許可される。ユーザ認証における不成功認証の試行回数である認証失敗回数の閾値の設定（改変）は、FMT_MTD.1[3]により管理者だけに許可される。

FIA_SOS.1[4]によりネットワークを経由したユーザ認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。

＜識別認証されたユーザのセッションの管理に必要な要件＞

識別認証されたユーザのセッションの持続時間は、パネルからログインした場合は FTA_SSL.3 により、システムオートリセット時間が経過した後、セッションを終了することによって、不必要なセッション接続に伴う攻撃の機会を低減させることに貢献している。

システムオートリセット時間の変更は、FMT_MTD.1[3]により管理者に制限される。

＜ユーザの識別認証情報の管理に必要な要件＞
FMT_MTD.1[1]により、ユーザ認証の方式に「本体認証」が選択されている場合において、ユーザ登録作業にて行うユーザパスワードの初期登録は管理者だけに許可される。
またユーザ認証の方式に「本体認証」が選択されている場合、ユーザ登録におけるユーザ ID の登録、利用停止、及び再開は FMT_MTD.1[10]、FMT_MTD.1[13]により管理者に許可される。なおユーザ認証方式に「外部サーバ認証」が選択されている場合、同要件により、識別認証されたユーザは外部サーバから許可されて自動的に登録される。（これは「外部サーバ」がユーザ ID を登録するということに相当。）この登録の際、FIA_UID.2[7]により、TOE にアクセスする外部サーバは登録された外部サーバであることを識別する。この管理行為は、FMT_SMR.1[5]により、役割：外部サーバとして維持される。更に FMT_SMF.1 によりユーザ ID の登録機能は管理機能として特定される。
外部サーバの設定登録、及び変更操作は FMT_MTD.1[3]、FMT_MTD.1[11]、により管理者だけに制限されている。

FIA_SOS.1[1]により、ユーザパスワードの品質が検証される。FMT_MTD.1[2]により、ユーザ認証の方式に「本体認証」が選択されている場合、ユーザ自身のユーザパスワードの変更はユーザ及び管理者に制限される。なおユーザによってユーザ自身のユーザパスワードを変更する場合は、FIA_UAU.6 により再認証される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[3]によりユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.PRIVATE-BOX（個人ボックスアクセス制御）**

本セキュリティ対策方針は、個人ボックス及び個人ボックス内のボックスファイルのユーザ機能に対するアクセスを、当該ボックスを所有するユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜ボックスアクセス制御（個人ボックス）＞
ユーザとして識別認証されると、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクにユーザ ID が関連付けられる。FDP_ACC.1[1]、FDP_ACF.1[1]により利用者を代行するタスクは、ユーザ ID を持ち、これと一致するユーザ属性を持つボックスの一覧表示操作が許可される。さらにボックスを選択し、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクにボックス ID が関連付けられると、サブジェクト属性のユーザ ID、ボックス ID と一致するオブジェクト属性を持つボックスファイルに対して、印刷、ダウンロード、各送信、移動、コピーの操作が許可される。

＜個人ボックスの管理＞
FMT_MSA.1[1]により、ユーザ自身のユーザ ID が設定されるボックスのユーザ属性の変更操作

は、ユーザ、管理者に許可される。
ボックスの登録は、FMT_MSA.3[1]によりボックスのユーザ属性には共有が指定され、これを変更する初期値を与えるのはユーザ、管理者だけに許可される。また同要件により未登録ボックスを指定したボックスへ**保存**するジョブが実行された場合は、当該ジョブを実行したユーザのユーザ ID が自動的に指定される。
ボックスファイルのボックス属性は、FMT_MSA.3[3]により、**保存**対象として選択されたボックスのボックス属性値と一致する値が設定される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[3]によりユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.PUBLIC-BOX（共有ボックスアクセス制御）**

本セキュリティ対策方針は、共有ボックスの閲覧をすべてのユーザに許可し、共有ボックスの設定、共有ボックス内のボックスファイルのユーザ機能の操作をその共有ボックスの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜ボックスアクセス制御（共有ボックス）＞
ユーザとして識別認証されると、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクにユーザ ID が関連付けられる。FDP_ACC.1[1]、FDP_ACF.1[1]により、ユーザ ID を持つ利用者を代行するタスクは、ユーザ属性に共有が設定されるボックスに対して一覧表示操作が許可される。
共有ボックス内のボックスファイルを操作するには、その共有ボックスの利用を許可されたユーザである必要があるが、FIA_UID.2[5]、FIA_UAU.2[4]により、その共有ボックスの利用を許可されたユーザであることを識別認証される。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[6]により、不成功認証が 1～3 回に達すると、以降その当該ボックスに対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
その共有ボックスの利用を許可されたユーザであることの認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにボックス ID が関連付けられると、FDP_ACC.1[1]、FDP_ACF.1[1]により、サブジェクト属性のボックス ID と一致するオブジェクト属性を持ち、且つボックスのユーザ属性に共有が設定されるボックスファイルに対して、印刷、ダウンロード、各送信、移動、コピーの操作が許可される。
FIA_SOS.1[4]によりネットワークを経由したボックス認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。

＜共有ボックスの管理＞
FMT_MSA.1[2]により、「共有」が設定されるボックスのユーザ属性の変更操作は、その共有ボックスの利用を許可されたユーザ、管理者に許可される。FMT_MTD.1[4]により、ボックスパスワードの変更は、管理者及びその共有ボックスの利用を許可されたユーザだけに許可される。FIA_SOS.1[1]により、ボックスパスワードの品質が検証される。なお共有ボックスの利用を許可されたユーザによって当該共有ボックスのボックスパスワードを変更する場合は、FIA_UAU.6により再認証される。
ボックスの登録は、FMT_MSA.3[1]によりボックスのユーザ属性には共有が指定され、これを変更する初期値を与えるのはユーザ、管理者だけに許可される。FMT_MTD.1[5]により、ボックスパスワードの登録はユーザ、管理者だけに許可される。
ボックスファイルのボックス属性は、FMT_MSA.3[3]により、**保存**対象として選択されたボックスのボックス属性値と一致する値が設定される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[4]によりその共有ボックスの利用を許可されたユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.GROUP-BOX（グループボックスアクセス制御）**

本セキュリティ対策方針は、グループボックスの閲覧を、その部門の利用が許可されたユーザだけに許可する。また利用停止状態でない部門のグループボックスの設定、グループボックス内のボックスファイルのユーザ機能の操作をそのグループボックスの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜ボックスアクセス制御（グループボックス）＞
ユーザとして識別認証されると、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクにユーザ ID が関連付けられる。また部門認証されると、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクに部門 ID が関連付けられる。FDP_ACC.1[1]、FDP_ACF.1[1]により、利用者を代行するタスクは、サブジェクトのセキュリティ属性の所属部門（部門 ID）と一致するユーザ属性が設定されるボックス（グループボックス）に対して一覧表示操作が許可される。
利用停止状態でない部門のグループボックス内のボックスファイルを操作するには、そのグループボックスの利用を許可されたユーザである必要があるが、部門認証方式が「個別認証方式」の場合、FIA_UID.2[6]、FIA_UAU.1[2]により、そのグループボックスの利用を許可されたユーザであることを識別認証される。部門認証方式が「ユーザ認証連動方式」である場合で所属部門が登録されていない場合は、その部門の利用を許可されたユーザであることを、FIA_UID.2[6]、FIA_UAU.1[2]により、識別認証する。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”

を返し、認証をサポートする。
FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[7]により、不成功認証が 1～3 回に達すると、以降その部門に対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
そのグループボックスの利用を許可されたユーザであることの認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにボックス ID が関連付けられると、FDP_ACC.1[1]、FDP_ACF.1[1]により、サブジェクト属性の部門 ID、ボックス ID と一致するオブジェクト属性を持つボックスファイルに対して、印刷、ダウンロード、各送信、移動、コピーの操作が許可される。

＜グループボックスの管理＞
FMT_MSA.1[3]により、「部門 ID」が設定されるボックスのユーザ属性の変更操作は、そのグループボックスの利用を許可されたユーザ、管理者に許可される。
ボックスファイルのボックス属性は、FMT_MSA.3[3]により、保存対象として選択されたボックスのボックス属性値と一致する値が設定される。

＜グループボックスに関係するサブジェクト属性の管理＞
FMT_MTD.1[11]、FMT_MTD.1[13]により、部門 ID 及び部門パスワードの登録、利用停止、及び再開は、管理者だけに制限される。また FMT_MTD.1[3]により、部門 ID 及び部門パスワードの改変は、管理者だけに制限される。ユーザに割り当たられる所属部門の登録は、FMT_MTD.1[12]により管理者及びその部門の利用を許可されたユーザだけに制限される。FIA_SOS.1[1]により、部門パスワードの品質が検証される。

＜部門認証方式の管理＞
FMT_MOF.1[3]により、部門認証機能（管理者用）のふるまい管理、停止操作管理は管理者だけに制限される。
FMT_MOF.1[3]において、管理者が部門認証機能（管理者用）の動作方式を「ユーザが設定する」に選択することによって、部門認証機能の動作方式は、部門認証機能（ユーザ用）の動作方式の選択に委ねられる。FMT_MOF.1[5]により、部門認証機能（ユーザ用）のふるまい管理は、その部門の利用を許可されたユーザ自身も利用できるように制限される。ただし、FMT_MOF.1[5]は FMT_MOF.1[3]のサブセットであり、設定内容が競合することはない。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[6]によりそのグループボックスの利用を許可されたユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.SECURE-PRINT（セキュリティ文書ファイル、認証＆プリントファイルアクセス制御）**

本セキュリティ対策方針は、セキュリティ文書ファイルに対する方針を説明している。
まずセキュリティ文書ファイルについてであるが、セキュリティ文書ファイルの印刷をそのセキュリティ文書ファイルの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜セキュリティ文書ファイルアクセス制御＞
ユーザとして識別認証されると、FIA_ATD.1、FIA_USB.1 により利用を代行するタスクにユーザ ID が関連付けられる。FDP_ACC.1[2]、FDP_ACF.1[2]により、ユーザ ID を持つ利用者を代行するタスクは、あらゆるセキュリティ文書ファイルに対して一覧表示操作が許可される。
セキュリティ文書ファイルを印刷するには、そのセキュリティ文書ファイルの利用を許可されたユーザである必要があるが、FIA_UID.2[4]、FIA_UAU.2[3]により、そのセキュリティ文書ファイルの利用を許可されたユーザであることを識別認証される。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[5]により、不成功認証が 1～3 回に達すると、当該セキュリティ文書ファイルに対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
セキュリティ文書ファイルの利用を許可されたユーザであることの認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにセキュリティ文書内部制御 ID が関連付けられると、FDP_ACC.1[2]、FDP_ACF.1[2]により、サブジェクト属性のセキュリティ文書内部制御 ID と一致するオブジェクト属性を持つセキュリティ文書ファイルに対して、印刷操作が許可される。
なおセキュリティ文書内部制御 ID は、FMT_MSA.3[2]よりセキュリティ文書ファイルの保存時に一意に識別される値が与えられている。

＜セキュリティ文書パスワード＞
FMT_MTD.1[8]により、認証に利用されるセキュリティ文書パスワードの登録はユーザだけに許可される。FIA_SOS.1[1]によりセキュリティ文書パスワードの品質は検証される。

次に認証&プリントファイルについてであるが、認証&プリントファイルの印刷をその認証&プリントファイルを保存したユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜認証&プリントファイルアクセス制御＞
FDP_ACC.1[4]、FDP_ACF.1[4]により、ユーザ ID を持つ利用者を代行するタスクは、そのユーザ ID と一致するユーザ属性を有する認証&プリントファイルに対して一覧表示、印刷操作が許可される。
なお認証&プリントファイルに設定されるユーザ属性は、FMT_MSA.3[4]により、当該ファイルが保存される際、保存する利用者のユーザ ID が設定される。

＜認証&プリント機能の動作管理＞
この動作モードの管理は、FMT_MOF.1[2]により、管理者だけに制限されている。

＜管理者をセキュアに維持するために必要な要件＞

⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[3]によりユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.CONFIG（管理機能へのアクセス制限）**

本セキュリティ対策方針は、SMTP サーバに関係する設定、DNS サーバに関係する設定、セキュリティ強化機能に関係する設定、バックアップ機能、リストア機能等を管理者に制限しており、一連の設定機能や管理機能に対してアクセスを制限するための諸要件が必要である。

＜ネットワークの設定管理＞
利用を代行するタスクに管理者属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、利用者を代行するタスクは、SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクト、PC-FAX 受信設定オブジェクト、送信宛先データオブジェクトに対する設定操作が許可される。

＜バックアップ、リストア機能の操作制限＞
FIA_ATD.1、FIA_USB.1 により利用を代行するタスクに管理者属性が関連づけられると、利用者を代行するタスクは、

- FDP_ACC.1[1]、FDP_ACF.1[1]によりボックスファイル
- FDP_ACC.1[2]、FDP_ACF.1[2]によりセキュリティ文書ファイル
- FDP_ACC.1[4]、FDP_ACF.1[4]により認証&プリントファイル

を対象として、バックアップ操作が許可される。また

- FDP_ACC.1[3]、FDP_ACF.1[3]により SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクト、PC-FAX 動作設定オブジェクト、送信宛先データオブジェクト

を対象として、リストア操作を許可される。更に

- FMT_MOF.1[1]によりセキュリティ強化設定データ
- FMT_MOF.1[2]により、ユーザ認証機能の動作設定データ、S/MIME 機能における暗号強度設定データ、SNMP パスワード認証機能の動作設定データ
- FMT_MOF.1[3]により高信頼チャネル機能設定データ、暗号化ワード、部門認証機能の動作設定データ
- FMT_MSA.1[1]、FMT_MSA.1[2]、FMT_MSA.1[3]によりボックスのユーザ属性
- FMT_MTD.1[2]によりユーザパスワード
- FMT_MTD.1[3]によりユーザ ID、SNMP パスワード、システムオートリセット時間、認証失敗回数閾値、セキュリティ文書パスワード、外部サーバ認証設定データ、部門 ID、部門パスワード、S/MIME 証明書、所属部門、管理者認証の操作禁止解除時間、TSI 受信設定データ
- FMT_MTD.1[4]によりボックスパスワード

を対象データとして管理者だけにリストア操作（すなわち改変操作）が許可される。

FMT_MTD.1[7]により SNMP パスワード、ユーザパスワード、ボックスパスワード、セキュリティ文書パスワード、部門パスワードのバックアップ操作（すなわち問い合わせ操作）が管理者だけに許可される。

＜セキュリティ強化機能の操作制限＞
セキュリティ強化機能の停止設定は、FMT_MOF.1[1]により、管理者及びサービスエンジニアだけに許可される。

＜暗号化ワードの管理＞
FMT_MTD.1[3]により、暗号化ワードに対する改変操作が管理者だけに許可される。
FIA_SOS.1[3]により暗号化ワードの品質が検証される。

＜MIB オブジェクトに対するアクセスに必要な要件＞
SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクトは、MIB オブジェクトとしても存在するため、SNMP によるアクセスにも制限が必要である。
FIA_UID.2[2]、FIA_UAU.2[2]により、MIB オブジェクトにアクセスする利用者が管理者であることを識別認証する。
FIA_AFL.1[3]により、不成功認証が 1～3 回に達すると、MIB オブジェクトにアクセスするための認証機能をロックする。このロック状態は、管理者によるロック解除操作によって解除される。
SNMP パスワード利用した管理者認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに制限される。
FMT_MTD.1[3]により SNMP パスワードの変更は、管理者に制限される。FIA_SOS.1[2]により、SNMP パスワードの品質が検証される。
SNMP パスワード認証機能の方式は、FMT_MOF.1[2]により、管理者だけに制限される。

＜高信頼チャネル機能設定データの操作制限＞
高信頼チャネル機能のふるまい及び停止設定は、FMT_MOF.1[3]により、管理者だけに許可される。

＜S/MIME 機能のための操作制限＞
S/MIME 証明書の登録は、FMT_MTD.1[11]により管理者だけに許可され、登録される S/MIME 証明書の変更は、FMT_MTD.1[3]により管理者だけに許可される。また送信宛先データの設定は、FDP_ACC.1[3]、及び FDP_ACF.1[3]により管理者だけに許可される。S/MIME 機能のふるまいは、FMT_MOF.1[2]により、管理者だけに許可される。

＜FAX 機能のための操作制限＞
TSI 受信において格納されるボックス（TSI 受信設定）の登録は、FMT_MTD.1[11]により管理者だけに許可され、登録された TSI 受信設定の変更は、FMT_MTD.1[3]により管理者だけに許可される。また PC-FAX 受信時に保存する領域の設定（PC-FAX 受信設定）は、FDP_ACC.1[3]、及び FDP_ACF.1[3]により管理者だけに許可される。

＜HDD データ上書き削除機能の消去方式の操作制限＞
HDD **データ上書き削除機能**の消去方式は、FMT_MOF.1[2]により、管理者だけに操作が制限される。

＜全領域上書き削除機能の操作制限＞
全領域上書き削除機能の起動は、FMT_MOF.1[4]により、管理者だけに許可される。

＜監査ログの操作制限＞
監査ログの問い合わせ及び削除操作は、FMT_MTD.1[14]により、管理者だけに許可される。

＜監査ログ満杯時の動作設定の操作制限＞
監査ログ満杯時の動作設定の操作は、FMT_MOF.1[2]により、管理者だけに許可される。

＜日時情報の操作制限＞
日時情報の改変は、FMT_MTD.1[15]により、管理者だけに許可される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニア、FMT_SMR.1[2]により管理者として維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.OVERWRITE（上書き削除）**
  本セキュリティ対策方針は、HDD のすべての画像データ領域を抹消する、削除に関係する諸要件が必要である。
  FDP_RIP.1 により、これら対象とする情報が消去操作によって以前のどの情報の内容も利用できなくすることを保証する。
  よって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-KEY（暗号鍵生成）**
  本セキュリティ対策方針は、HDD に書き込むすべてのデータを ASIC を利用して暗号化するために必要な暗号鍵を生成するとしており、暗号鍵生成に関係する諸要件が必要である。
  FCS_CKM.1 により、コニカミノルタ暗号仕様標準に従ったコニカミノルタ HDD 暗号鍵生成アルゴリズムを利用し、128bit の暗号鍵を生成する。なお、暗号鍵は電源 ON で揮発性メモリである RAM 上に作成され、電源 OFF により消失する。
  この機能要件によって本セキュリティ対策方針は満たされる。

- **O.TRUSTED-PASS（高信頼チャネルの利用）**
  本セキュリティ対策方針は、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルの送受信において高信頼チャネルを生成するとしており、高信頼チャネルに関係する要件が必要である。
  FTP_ITC.1 は、他の高信頼 IT 製品からの要求に応じて高信頼チャネルを生成するとしており、ボックスファイル、セキュリティ文書ファイル、認証&プリントファイルの送受信に適用される。

この機能要件によって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-MAIL（暗号化メールの利用）**

本セキュリティ対策方針は、ボックスファイルをメールにて送信する際にボックスファイルを暗号化することを規定しており、暗号に関する諸要件が必要である。
FCS_CKM.1 により、FIPS 186-2 に従った擬似乱数生成アルゴリズムを利用し、暗号鍵（128 bit、または 168 bit、または 192 bit、または 256 bit）を生成する。
FCS_COP.1 により、FIPS PUB 197 の AES（暗号鍵：128 bit、または 192 bit、または 256 bit）を利用してボックスファイルを暗号化する。（これは S/MIME の送信データになる。）また同要件により SP800-67 の 3-Key-Triple-DES（暗号鍵：168 bit）を利用してボックスファイルを暗号化する。（これも同様に S/MIME の送信データになる。）これら暗号鍵は、FCS_COP.1 により、各宛先の S/MIME 証明書の公開鍵（1024bit、または 2048 bit、または 3072 bit、または 4096 bit）を使用して FIPS 186-2 の RSA により暗号化される。
これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O. FAX-CONTROL（FAX ユニット制御）**

本セキュリティ対策方針は、公衆回線網から FAX 公衆回線ロを通して、当該 MFP が接続されている内部ネットワークへのアクセスを禁止することを規定している。これは公衆回線網から送付され、MFP を介して内部ネットワークに転送される画像データを除いた通信（遠隔診断機能や不正な操作コマンド）が、内部ネットワークに転送されないことを意味しており、FAX ユニットのフロー制御に関する諸要件が必要である。
FDP_IFC.1、及び FDP_IFF.1 により、公衆回線からの受信機能が受信した画像データ以外のデータを内部ネットワークに送出しないというフロー制御を実現する
この機能要件によって本セキュリティ対策方針は満たされる。

- **O.AUTH-CAPABILITY（ユーザ認証機能を利用するためのサポート動作）**

本セキュリティ対策方針は、TOE 外のエンティティであるユーザ情報管理サーバを利用したユーザ認証機能を TOE がサポートするとしており、外部エンティティの動作をサポートすることを規定する諸要件が必要である。
FIT_CAP.1[1]により、ユーザ情報管理サーバが実現する ActiveDirectory によるユーザ認証機能に対して、識別認証対象のユーザに対する認証情報問い合わせ機能、識別認証対象のユーザに対する認証情報取得機能を実現する。
この機能要件によって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-CAPABILITY（HDD 暗号化機能を利用するためのサポート動作）**

本セキュリティ対策方針は、TOE 外のエンティティである ASIC により、HDD 内に保存されるデータを暗号化するための動作を TOE がサポートするとしており、外部エンティティの動作をサポートすることを規定する諸要件が必要である。
FIT_CAP.1[2]により、ASIC が実現する HDD 暗号化機能に対して、HDD のすべてのデータを HDD 暗号化機能で処理させるためのサポート機能を実現する。
この機能要件によって本セキュリティ対策方針は満たされる。

- **O.AUDIT-LOGGED（監査ログの取得、管理）**

本セキュリティ対策方針は、すべての認証機能及び監視すべきジョブに関する監査ログを生成維持し、監査ログを開示または改変する権限の無い者からは監査ログを保護するとしており、監査ログに関する要件が必要である。

FAU_GEN.1,FAU_GEN.2 により、すべての認証機能及び監視すべきジョブに関する監査ログを生成する機能を、FAU_SAR.1,FAU_SAR.2, FAU_STG.1, FAU_STG.4[1], FAU_STG.4[2]により、監査ログを開示または改変する権限の無い者からは監査ログを保護する機能を実現する。監査情報に必要なユーザ情報と日時情報を提供するために FIA_UID.2[1]、FIA_UID.2[2]、FIA_UID.2[3]、FIA_UID.2[4]、FIA_UID.2[5]、FIA_UID.2[6]と FPT_STM.1 によってサポートされる。
この機能要件によって本セキュリティ対策方針は満たされる。

- ***set.admin*（管理者をセキュアに維持するために必要な要件のセット）**

＜管理者の識別認証＞
FIA_UID.2[2]、FIA_UAU.2[2]により、アクセスする利用者が管理者であることを識別認証する。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[2]により、不成功認証が 1～3 回に達すると、認証中であればログアウトし、以降管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除機能が実行され、管理者認証の操作禁止解除時間が経過後に解除される。
管理者認証における不成功認証の試行回数である認証失敗回数の閾値の設定及び管理者認証の操作禁止解除時間の変更は、FMT_MTD.1[3]により、管理者だけに許可される。

＜識別認証された管理者のセッションの管理＞
識別認証された管理者のセッションの持続時間は、パネルからログインした場合は FTA_SSL.3 により、システムオートリセット時間が経過した後、セッションを終了することによって、不必要なセッション接続に伴う攻撃の機会を低減させることに貢献している。なおシステムオートリセット時間の変更は、FMT_MTD.1[3]により管理者に制限される。

＜管理者の認証情報の管理など＞
管理者パスワードは、FIA_SOS.1[1]により品質が検証される。また FIA_SOS.1[4]によりネットワークを経由した管理者認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。管理者パスワードの変更は、FMT_MTD.1[6]により、管理者及びサービスエンジニアに制限される。管理者が管理者パスワードを変更する場合は、FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[2]により、不成功認証が 1～3 回に達すると、認証中であればログアウトし、以降管理者の認証状態を解除し、管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除機能が実行され、管理者認証の操作禁止解除時間が経過後に解除される。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアと FMT_SMR.1[2]により管理者にて維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

- ***set.service*（サービスエンジニアをセキュアに維持するために必要な要件のセット）**

＜サービスエンジニアの識別認証＞
FIA_UID.2[1]、FIA_UAU.2[1]により、アクセスする利用者がサービスエンジニアであることを識別認証する。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”

を返し、認証をサポートする。
FIA_AFL.1[8]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[1]により、不成功認証が 1～3 回に達すると、認証中であればログアウトし、CE パスワードを利用するすべての認証機能をロックする。このロック状態は、CE 認証機能ロック解除機能が実行されて、CE 認証の操作禁止解除時間を経過すると解除される。
サービスエンジニア認証における不成功認証の試行回数である認証失敗回数の閾値の設定は FMT_MTD.1[3]により管理者だけに許可される。CE 認証の操作禁止解除時間の設定は、FMT_MTD.1[9]により、サービスエンジニアだけに許可される。

＜サービスエンジニアの認証情報の管理など＞
CE パスワードは、FIA_SOS.1[1]により、品質が検証される。CE パスワードの変更は、FMT_MTD.1[9]により、サービスエンジニアに制限される。また FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[1]により、不成功認証が 1～3 回に達すると、サービスエンジニアの認証状態を解除して、CE パスワードを利用するすべての認証機能をロックする。このロック状態は、CE 認証機能ロック解除機能が実行されて、CE 認証の操作禁止解除時間を経過すると解除される。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

6.2.1.3. IT セキュリティ機能要件の依存性

IT セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 で規定される依存性を満たさない場合、「本 ST における依存関係」の欄にその理由を記述する。

表 11 IT セキュリティ機能要件コンポーネントの依存関係

N/A : Not Applicable

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2[1]、FIA_UID.2[2]、FIA_UID.2[3] FIA_UID.2[4]、FIA_UID.2[5]、FIA_UID.2[6]
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1、 FCS_CKM.4、	FCS_COP.1（一部事象のみ） ＜FCS_CKM.2 or FCS_COP.1 を一部満たしていない理由＞ ・コニカミノルタ HDD 暗号鍵生成アルゴリズムにより生成された鍵を用いた暗号操作は FIT_CAP.1[1]により IT 環境によって行われる。TSF はその能力を利用するのみであり、配布及び暗号操作の必要性はない。 ＜FCS_CKM.4 を適用しない理由＞ ・暗号鍵は、一時的に揮発性のある記憶領域に存在する

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
		が、外部からアクセスする必要が無く自動的に破棄されるため、破棄を考慮する必要性はない。
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2、FCS_CKM.4、	FCS_CKM.1（一部事象のみ)、 満たしている事象：S/MIME 通信にて添付ファイルを暗号化するための暗号鍵を生成すること。 ＜FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 を一部満たしていない理由＞ ・S/MIME のデータ暗号化のための暗号鍵を暗号化するための公開鍵を TSF の制御範囲外よりインポートするため、FDP_ITC.1 の適用が妥当と考えられるが、S/MIME 証明書は､管理者の操作によって登録される。その際、信頼されないチャネルを経由する、しない等の考慮は不要であり、セキュリティ要件を適用する必然性がない。(A.NETWORK が成立する条件下での利用) ・またインポートされる暗号鍵の属性情報は、アクセス制御等に利用されるセキュリティ属性に相当せず、属性の初期化等に関係しないため､適用の必要性はない。 ・FMT_MTD.1[11]にて TSF データの登録として、表現されており、インポート操作を行う対象は適切な役割に割り振られている。 ・結果、鍵管理相当の事象は依存性で示されるセキュリティ要件ではなく他のセキュリティ要件を用いて説明されているため、本依存性が満たされなくとも問題ない。 ＜FCS_CKM.4 を適用しない理由＞ 暗号鍵は、一時的に揮発性のある記憶領域に存在するが、外部からアクセスする必要が無く自動的に破棄されるため、破棄を考慮する必要性はない。
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACC.1[4]	FDP_ACF.1	FDP_ACF.1[4]
FDP_ACF.1[1]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[1]、 FMT_MSA.3[1]、FMT_MSA.3[3]
FDP_ACF.1[2]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3[2]
FDP_ACF.1[3]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[3] ＜FMT_MSA.3 を適用しない理由＞ オブジェクト属性が存在しないため、本要件を適用する必要性はない。
FDP_ACF.1[4]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[4] FMT_MSA.3[4]
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1、 FMT_MSA.3	FDP_IFC.1 ＜FMT_MSA.3 を適用しない理由＞ セキュリティ属性は外部にて初期化されるため、本要件を適用する必要性はない
FDP_RIP.1	なし	N/A
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.1[1]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[7]	FIA_UAU.1	FIA_UAU.1[2]
FIA_AFL.1[8]	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.1[1]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.1[2]
FIA_ATD.1	なし	N/A
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_SOS.2	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.1[1]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[5]
FIA_UAU.1[2]	FIA_UID.1	FIA_UID.2[6]
FIA_UAU.6	なし	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.1[1]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.1[2]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FIA_UID.2[5]	なし	N/A
FIA_UID.2[6]	なし	N/A
FIA_UID.2[7]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1[1]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MOF.1[4]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MOF.1[5]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[6]
FMT_MSA.1[1]	FDP_ACC.1 or FDP_IFC.1、FMT_SMF.1、FMT_SMR.1	FDP_ACC.1[1]、FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1、FMT_SMF.1、FMT_SMR.1	FDP_ACC.1[1]、FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MSA.1[3]	FDP_ACC.1 or FDP_IFC.1、FMT_SMF.1、FMT_SMR.1	FDP_ACC.1[1]、FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[6]
FMT_MSA.3[1]	FMT_MSA.1、FMT_SMR.1	FMT_MSA.1[1]、FMT_MSA.1[2]、FMT_SMR.1[3]
FMT_MSA.3[2]	FMT_MSA.1、FMT_SMR.1	両者とも適用しない

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
		＜FMT_MSA.1 を適用しない理由＞ 一意に識別される内部制御 ID であり、一度割り当てられた後に変更、削除といった管理を必要としないため。 ＜FMT_SMR.1＞ FMT_MSA.3.2[2] の割付は該当なしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MSA.3[3]	FMT_MSA.1、 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ ボックスファイルのボックス属性は、ボックスと常に一致している必要がある。よって**保存**のタイミングで値が与えられればよく、その他の操作タイミングにてこの属性値が変更される必要性はなく、管理要件は不要である。 ＜FMT_SMR.1＞ FMT_MSA.3.2[3] の割付は該当なしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MSA.3[4]	FMT_MSA.1、 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ 認証&プリントは、保存した本人だけがアクセスすることができる印刷物であることがコンセプトであり、他のユーザに譲渡することを想定していない。したがって、保存のタイミング以外の操作においてこの属性が値変更される必要性はなく、管理要件は不要である。 ＜FMT_SMR.1＞ FMT_MSA.3.2[4] の割付は該当なしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2] 、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[6]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[7]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[8]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[3]
FMT_MTD.1[9]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]、FMT_SMR.1[5]
FMT_MTD.1[11]	FMT_SMF.1	FMT_SMF.1

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
	FMT_SMR.1	FMT_SMR.1[2]
FMT_MTD.1[12]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2] FMT_SMR.1[6]
FMT_MTD.1[13]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[14]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[15]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[5]
FMT_SMR.1[5]	FIA_UID.1	FIA_UID.2[7]
FMT_SMR.1[6]	FIA_UID.1	FIA_UID.2[6]
FPT_STM.1	なし	N/A
FTA_SSL.3	なし	N/A
FTP_ITC.1	なし	N/A
FIT_CAP.1[1]	なし	N/A
FIT_CAP.1[2]	なし	N/A

6.2.2. IT セキュリティ保証要件根拠

本 TOE は、物理的・人的・接続的に十分なセキュリティを確保した環境に設置され利用されるが、本 TOE を利用する環境において十分な実効性を保証する必要がある。一般的な商用事務製品として機能仕様、TOE 設計書に基づくテスト、機能強度分析、脆弱性の探索が実施されている必要があり、また開発環境の制御、TOE の構成管理、セキュアな配付手続きが取られていることが望まれる。従って十分な保証レベルが提供される EAL3 の選択は妥当である。

なお、保証要件依存性分析は、パッケージである EAL が選択されているため、妥当であるとして詳細は論じない。

7. TOE 要約仕様

TOEのセキュリティ機能要件より導かれるTOEのセキュリティ機能を以下の表 12にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 12 TOE のセキュリティ機能名称と識別子の一覧

No.	TOE のセキュリティ機能	
1	F.ADMIN	管理者機能
2	F.ADMIN-SNMP	SNMP 管理者機能
3	F.SERVICE	サービスモード機能
4	F.USER	ユーザ機能
5	F.BOX	ボックス機能
6	F.PRINT	セキュリティ文書機能、認証&プリント機能
7	F.CRYPTO	暗号鍵生成機能
8	F.RESET	認証失敗回数リセット機能
9	F.TRUSTED-PASS	高信頼チャネル機能
10	F.S/MIME	S/MIME 暗号処理機能
11	F.FAX-CONTROL	FAX ユニット制御機能
12	F.SUPPORT-AUTH	外部サーバ認証動作サポート機能
13	F.SUPPORT-CRYPTO	ASIC サポート機能
14	F.OVERWRITE	HDD データ上書き削除機能
15	F. AUDIT-LOGGED	監査ログ機能

7.1. F.ADMIN（管理者機能）

F.ADMIN とは、パネルやネットワークからアクセスする管理者モードにおける管理者識別認証機能、管理者パスワードの変更やロックされたボックスのロック解除などのセキュリティ管理機能といった管理者が操作する一連のセキュリティ機能である。（なお、すべての機能がパネル及びネットワークの双方から実行可能な機能ということではない。）

7.1.1. 管理者識別認証機能

管理者モードへのアクセス要求に対して、アクセスする利用者を管理者であることを識別及び認証する。

- 表 13 に示されるキャラクタからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
  - ネットワークからのアクセスに対して管理者認証後は、管理者パスワードとは別のセッション情報を利用した、管理者認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- 管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 管理者パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、管理

者パスワードを利用するすべての認証機能をロックする。(管理者モードへのアクセスを拒否する。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作して解除する。

以上により FIA_AFL.1[2]、FIA_AFL.1[8]、FIA_SOS.1[4]、FIA_SOS.2、FIA_UAU.2[2]、FIA_UAU.7、FIA_UID.2[2]が実現される。

表 13 パスワードに利用されるキャラクタと桁数 [13]

対象	桁数	キャラクタ
ユーザパスワード CE パスワード 管理者パスワード 部門パスワード ボックスパスワード	8～64 桁	最低合計 161 文字の中から選択可能 （英、数、記号（一部除く）、特殊文字（一部除く））
暗号化ワード	20 桁	最低合計 83 文字の中から選択可能 （英、数、記号（一部除く））
セキュリティ文書パスワード	8～64 桁	最低合計 94 文字の中から選択可能 （英、数、記号（一部除く））
SNMP パスワード ・Privacy パスワード ・Authentication パスワード	8～32 桁	最低合計 90 文字の中から選択可能 （英、数、記号（一部除く））

7.1.2. 管理者モードのオートログアウト機能

パネルから管理者モードにアクセス中でパネルオートログアウト時間以上何らかの操作を受け付けなかった場合は、自動的に管理者モードをログアウトする。

以上により FTA_SSL.3 が実現される。

7.1.3. 管理者モードにて提供される機能

管理者モードへのアクセス要求において管理者識別認証機能により、管理者として識別認証されると、利用者を代行するタスクに管理者属性が関連づけられ、以下の操作、機能の利用が許可される。

FIA_ATD.1、FIA_USB.1 は上記により実現される。

7.1.3.1. 管理者パスワードの変更

管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、パスワードを変更する。

- 表 13 に示されるキャラクタからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。

管理者パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、アクセスする管理者モードをログアウトし、管理者パスワードを利用するすべての認証機能をロック

[13] 表 13 は、セキュリティ仕様として最小のパスワード空間を示すものである。よってパスワード種に応じていくつか除外されているキャラクタが示されているが、除外キャラクタが利用可能なケースは許容される。

する。（管理者モードへのアクセスを拒否する。）
- 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。

- 認証機能のロックは、F.RESET が動作して解除する。
- 新規設定される管理者パスワードは以下の品質を満たしていることを検証する。
  - 表 13 の管理者パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_AFL.1[2]、FIA_SOS.1[1]、FIA_UAU.6、FIA_UAU.7、FMT_MTD.1[6]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.2. ユーザの設定

- ユーザ登録（ユーザ認証方式：本体認証において利用されるユーザのみ）
  ユーザ ID（ユーザ名と認証サーバ情報 [14]から構成されるが、本体認証時はユーザ名のみの登録。）を設定し、ユーザパスワードを登録してユーザが登録される。新しく設定されるユーザパスワードは以下の品質を満たしていることを検証する。
  - 表 13 のユーザパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

  なお、外部サーバ認証を有効にしている場合は、ユーザパスワードの登録はできない。
  また所属部門（部門 ID）を登録し、関連付けする。（予め部門設定が必要。）

- ユーザパスワードの変更（ユーザ認証方式：本体認証において利用されるユーザのみ）
  ユーザパスワードを変更する。新しく設定されるユーザパスワードは以下の品質を満たしていることを検証する。
  - 表 13 のユーザパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

- ユーザ削除
  ユーザ ID、ユーザパスワードを削除する。
  - 当該ユーザが所有する個人ボックスが存在した場合、それら個人ボックスを、ユーザ属性：共有の共有ボックスに設定するか削除するかを選択する。

- ユーザの利用停止・再開（ユーザ認証方式：本体認証においてのみ有効）
  ユーザ ID を指定し、ユーザを利用停止、もしくは利用停止状態のユーザを再開する。利用停止状態のユーザは識別認証されなくなり、識別認証以降のユーザ機能が利用不可となる。

- 所属部門の変更
  ユーザに関連付けられる所属部門を変更する。

以上により FIA_SOS.1[1]、FMT_MTD.1[1]、FMT_MTD.1[2]、FMT_MTD.1[3]、FMT_MTD.1[10]、FMT_MTD.1[12]、FMT_MTD.1[13]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

---

[14] ユーザ認証機能の方式にて、外部サーバ認証（ここでは ActiveDirectory 方式のみ適用可）を利用する場合に設定される外部サーバ認証設定データと関連する。ユーザ情報管理サーバが複数存在する場合にも対応しているため、外部サーバ認証設定データには、認証サーバ情報が複数含まれるケースがある。

7.1.3.3. ボックスの設定

- ボックスの登録
  管理者属性が関連付けられていると、ボックスの一覧表示が許可される。一覧から選択した未登録ボックス ID に対して、ユーザ属性を選定して、個人ボックス、グループボックス、共有ボックスを登録する。登録する際、ボックスのユーザ属性にはデフォルト値として「共有」が指定されるが、「ユーザ ID」、「部門 ID」を選択することも可能。
  - 個人ボックスの場合は、登録される任意のユーザ ID を指定する。
  - 共有ボックスの場合は、登録されるボックスパスワードが以下の条件を満たすことを検証する。
    - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
    - 1 つのキャラクタで構成されない。
  - グループボックスの場合、登録される任意の部門 ID を指定する。

- ボックスパスワードの変更
  - 共有ボックスに設定されるボックスパスワードを変更する。
  - 新しく設定されるボックスパスワードは以下の品質を満たしていることを検証する。
    - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
    - 1 つのキャラクタで構成されない。
    - 現在設定される値と一致しない。

- ボックスのユーザ属性の変更
  - 個人ボックスのユーザ属性を登録されている別のユーザ、または部門に指定する。
  - グループボックスのユーザ属性を登録されているユーザ、または別の部門に指定する。
  - 共有ボックスのユーザ属性を登録されているユーザ、または部門に指定する。
  - 個人ボックス、グループボックスのユーザ属性を共有に指定する。
    - 同時にボックスパスワードが登録されていなければ、登録が必須となり、上記のボックスパスワードの変更と同様の処理が行われる。

以上により FDP_ACC.1[1]、FDP_ACF.1[1]、FIA_SOS.1[1]、FMT_MSA.1[1]、FMT_MSA.1[2]、FMT_MSA.1[3]、FMT_MSA.3[1]、FMT_MTD.1[4]、FMT_MTD.1[5]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.4. ロックの解除

- 各ユーザの認証失敗回数を 0 クリアする。
  - アクセスがロックされているユーザがあれば、ロックが解除される。
- 各セキュリティ文書パスワードの認証失敗回数を 0 クリアする。
  - アクセスがロックされているセキュリティ文書パスワードがあれば、ロックが解除される。
- 各ボックスの認証失敗回数を 0 クリアする。
  - アクセスがロックされているボックスがあれば、ロックが解除される。
- 各部門の認証失敗回数を 0 クリアする。
  - アクセスがロックされている部門があれば、ロックが解除される。
- SNMP パスワードによる認証失敗回数を 0 クリアする。
  - MIB オブジェクトへのアクセスがロックされていれば、ロックが解除される。

以上により FIA_AFL.1[3]、FIA_AFL.1[4]、FIA_AFL.1[5]、FIA_AFL.1[6]、FIA_AFL.1[7]が実

現される。

7.1.3.5. ユーザ認証機能の設定

ユーザ認証機能における以下の認証方式を設定する。

- 本体認証：MFP 本体側で管理するユーザパスワードを利用する認証方式
- 外部サーバ認証：ネットワークを介して接続されるユーザ情報管理サーバにて管理されるユーザパスワードを利用する認証方式（ActiveDirectory 方式のみ対象）
  - 外部サーバ認証を利用する場合は、外部サーバ認証設定データ（外部サーバが所属するドメイン名など、複数の認証サーバ情報を含む）を設定する。

ユーザ認証機能と組み合わせて利用される部門認証機能における以下の認証方式を設定する。

- 部門認証機能（管理者用）：連動方式
  ユーザ ID に予め関連付けられている部門 ID を利用する方式
- 部門認証機能（管理者用）：個別認証方式
  ユーザ ID に予め関連付けられている部門 ID を利用せず、アクセス時に部門 ID と部門パスワードによって認証する方式
- 部門認証機能（管理者用）：利用しない
  ユーザ ID による認証機能だけを利用し、部門情報による識別認証を行わない。
- 部門認証機能（管理者用）：ユーザが設定する
  登録ユーザ自身が、ユーザ認証と部門認証を連動させるか否かの設定を設ける。

以上により FMT_MOF.1[2]、FMT_MOF.1[3]、FMT_MTD.1[3]、FMT_MTD.1[11]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.6. 不正アクセス関係の設定

- **不正アクセス検出閾値の設定**
  認証操作禁止機能における不正アクセス検出閾値を 1～3 回間で設定する。
- **管理者認証の操作禁止解除時間の設定**
  管理者認証の操作禁止解除時間を 5～60 分で設定する。

以上により FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.7. オートログアウト機能の設定

オートログアウト機能における設定データであるシステムオートリセット時間を以下に示す時間範囲で設定する。

- システムオートリセット時間　　：1～9 分

以上により FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.8. ネットワークの設定

以下の設定データの設定操作を行う。

- SMTP サーバに関係する一連の設定データ（IP アドレス、ポート番号等）
- DNS サーバに関係する一連の設定データ（IP アドレス、ポート番号等）
- MFP アドレスに関係する一連の設定データ（IP アドレス、NetBIOS 名、AppleTalk プリンタ名等）

以上により FDP_ACC.1[3]、FDP_ACF.1[3]が実現される。

7.1.3.9. バックアップ、リストア機能の実行

管理者パスワード、CE パスワード、暗号化ワードを除いて、NVRAM、SSD 及び HDD に**保存**されるあらゆる設定データをバックアップ、リストアする。セキュリティに関係する対象としては、秘匿性、完全性の関係より以下の分類にて示されるものが対象となっている。

＜タイプ A　バックアップ・リストア制限されるべき対象＞
- SNMP パスワード
- ユーザパスワード
- 部門パスワード
- セキュリティ文書パスワード
- ボックスパスワード

＜タイプ B　リストアが制限されるべき対象＞
- SMTP サーバ設定に関係する一連のデータ
- DNS サーバ設定に関係する一連のデータ
- MFP アドレス設定に関係する一連のデータ
- SNMP パスワード認証機能の動作設定データ
- セキュリティ強化機能の設定データ
- ユーザ認証機能の動作方式設定データ
- 部門認証機能の動作設定データ
- 認証操作禁止機能の認証失敗回数閾値
- システムオートリセット時間
- ユーザ ID
- ボックスのユーザ属性
- 部門 ID
- S/MIME 証明書
- 送信宛先データ
- S/MIME 機能における暗号化強度設定データ
- SSL 証明書
- 所属部門
- 管理者認証の操作禁止解除時間
- PC-FAX 受信設定
- TSI 受信設定データ
- 外部サーバ認証設定データ

＜タイプ C　バックアップが制限されるべき対象＞
- セキュリティ文書ファイル
- ボックスファイル
- 認証&プリントファイル

以上により FDP_ACC.1[1]、FDP_ACC.1[2]、FDP_ACC.1[3]、FDP_ACC.1[4]、FDP_ACF.1[1]、FDP_ACF.1[2]、FDP_ACF.1[3]、FDP_ACF.1[4]、FMT_MOF.1[1]、FMT_MOF.1[2]、FMT_MOF.1[3]、FMT_MSA.1[1] 、 FMT_MSA.1[2] 、 FMT_MSA.1[3] 、 FMT_MTD.1[2] 、 FMT_MTD.1[3] 、 FMT_MTD.1[4]、FMT_MTD.1[7]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.10. HDD 暗号化機能の動作設定

＜暗号化ワード変更＞
暗号化ワードを変更する。新規設定される暗号化ワードが品質を満たしている場合に変更し、F.CRYPTO が実行される。

- 新規設定される暗号化ワードは以下の品質を満たしていることを検証する。
  - 表 13 の暗号化ワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_SOS.1[3]、FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.11. SNMP パスワードの変更

SNMP パスワード（Privacy パスワード、Authentication パスワード）を変更する。新規設定されるパスワードが品質を満たしている場合、変更する。

- 新しく設定される SNMP パスワードが以下の品質を満たしていることを検証する。
  - 表 13 の SNMP パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_SOS.1[2]、FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.12. SNMP パスワード認証機能の設定

SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。
以上により FMT_MOF.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.13. 部門の設定

- 部門登録
  部門 ID を設定し、部門パスワードを登録して部門が登録される。新しく設定される部門パスワードは以下の品質を満たしていることを検証する。
  - 表 13 の部門パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

- 部門 ID、部門パスワードの変更
  部門 ID、部門パスワードを変更する。新しく設定される部門パスワードは以下の品質を満たしていることを検証する。
  - 表 13 の部門パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

- 部門削除
  部門 ID、部門パスワードを削除する。
  - 当該部門 ID のグループボックスが存在した場合、それらグループボックスを、ユーザ属性：

共有の共有ボックスに設定するか削除するかを選択する。

- 部門の利用停止・再開
  部門 ID を指定し、部門を利用停止、もしくは利用停止状態の部門を再開する。利用停止状態の部門は識別認証されなくなり、部門の識別認証を必要とするユーザ機能が利用不可となる。

以上により FIA_SOS.1[1]、FMT_MSA.1[3]、FMT_MTD.1[3]、FMT_MTD.1[11]、FMT_MTD.1[13]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.14. 高信頼チャネル機能の設定

SSL/TLS による高信頼チャネル機能設定データを設定する。

- 通信暗号強度設定（通信暗号方式の変更）
- 高信頼チャネル機能の動作・停止設定

以上により FMT_MOF.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.15. S/MIME 送信機能の設定

ボックスファイルを S/MIME 送信する際に利用される設定データを設定する。

- 送信宛先データ（e-mail アドレス）
- S/MIME 証明書の登録、変更
- S/MIME 機能における暗号化強度の設定

以上により FDP_ACC.1[3]、FDP_ACF.1[3]、FMT_MOF.1[2]、FMT_MTD.1[3]、FMT_MTD.1[11]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.16. FAX の設定

以下の FAX に関連する設定データを設定する。

- PC-FAX 受信設定
  - PC-FAX の動作は、FAX 送信時に指定される情報に基づき、個々のボックスに保存するモードと、全ユーザ共通利用する領域に保存するモードが存在する。
- TSI 受信設定
  - 送信者端末識別情報として、発信者の電話番号とボックスを関連付け、TSI 受信において格納されるボックスを設定する。

以上により FDP_ACC.1[3]、FDP_ACF.1[3]、FMT_MTD.1[3]、FMT_MTD.1[11]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.17. セキュリティ強化機能に関連する機能

管理者が操作するセキュリティ強化機能の設定に影響する機能は以下の通り。（※バックアップ・リストア機能の影響については、「7.1.3.9」にて説明済み）

- セキュリティ強化機能の動作設定
  セキュリティ強化機能の有効、無効を設定する機能。

セキュリティ強化機能の動作設定以外にも、HDD 論理フォーマット機能や全領域上書き削除機能等を実行することで、セキュリティ強化機能の設定を無効にすることができる。これらの操作は

全て管理者に限定されている。

以上により FMT_MOF.1[1]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.18. パスワード初期化機能に関連する機能

管理者が操作するパスワードの初期化に関係する機能は以下の通り。

- 全領域上書き削除機能
  全領域の上書き削除の実行により、管理者パスワード、SNMP パスワードを工場出荷の初期値に設定する。
  以上により FMT_MTD.1[3]、FMT_MTD.1[6]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.19. 認証＆プリント機能の動作設定

以下に示す認証&プリント機能の動作モードを設定する。

- 認証&プリント自動動作モード
  PC より送信されるプリントファイルにおいて、通常の印刷設定での印刷要求が行われた場合でも、プリントファイルを認証&プリントファイルとして保存する動作モード
- 認証&プリント指定動作モード
  PC より送信されるプリントファイルにおいて、認証&プリントファイルとして保存要求が行われた場合のみ、プリントファイルを認証&プリントとして保存する動作モード
  以上により FMT_MOF.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.20. HDD データ上書き削除機能の動作設定

HDD **データ上書き削除機能**における消去方式を「Mode1」または「Mode2」に設定する。(「Mode1」「Mode2」の詳細は**表 15** 参照)
以上により FMT_MOF.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.21. 監査ログ機能に関連する機能

- 監査ログの閲覧及び削除
  監査ログ機能で取得した監査ログをエクスポートする。(エクスポートの際に監査ログは消去される。)また、エクスポート操作による削除とは別に、監査ログ消去操作があり、どちらも管理者のみが操作できる。
- 監査ログ満杯時の動作設定
  監査ログ満杯時の動作を、最も古い監査ログから順に上書きする「上書き許可」設定、またはジョブの受付を停止する「上書き禁止」設定のどちらかを設定する。(デフォルトは上書き禁止)

以上により FMT_MOF.1[2]、FMT_MTD.1[14]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.22. 日時情報の設定

- 日時情報を設定する。日時情報は管理者のみが設定できる。
  年(00～37)、月(01～12)、日(01～31)、時(00～23)、分(00～59)の各値が括弧内の値以外の場合、設定を確定できない。また、管理者が設定した MFP 内の時刻機能及び NTP サーバの

時刻情報を参照する。

以上により FMT_MTD.1[15]、FMT_SMF.1、FMT_SMR.1[2]、FPT_STM.1 が実現される。

7.1.3.23. 全領域上書き削除機能

全領域上書き削除機能とは、HDD のデータ領域に上書き削除を実行すると共に NVRAM 及び SSD に設定されているパスワード等の設置値を初期化する。削除、または初期化されるべき対象は以下の通りである。

＜削除される対象：HDD＞
- セキュリティ文書ファイル
- ボックスファイル
- 認証&プリントファイル
- 保存画像ファイル
- HDD 残存画像ファイル
- 画像関連ファイル
- 送信宛先データファイル
- ユーザ ID
- ユーザパスワード
- ボックスパスワード
- セキュリティ文書パスワード
- 部門 ID
- 部門パスワード
- S/MIME 証明書
- SSL 証明書

＜初期化される対象：NVRAM・SSD＞
- 管理者パスワード
- SNMP パスワード
- 暗号化ワード　　・・・暗号化ワードが消去され、HDD 暗号化機能の動作設定が OFF になる。

HDD に書き込むデータ、書き込む回数など削除方式は、F.ADMIN において設定される全領域上書き削除機能の消去方式（**表 15**）に応じて実行される。HDD 暗号化機能は動作設定が OFF されることによって、設定されていた暗号化ワードが利用できなくなる。なお、本機能の実行においてセキュリティ強化機能の設定は無効になる。（F.ADMIN におけるセキュリティ強化機能の動作設定の記載参照）

以上により、FDP_RIP.1、FMT_MOF.1[4]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

表 14　全領域の上書き削除のタイプと上書きの方法

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	乱数 ⇒ 乱数 ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
Mode:4	乱数 ⇒ 0x00 ⇒ 0xFF

方式	上書きされるデータタイプとその順序
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

7.2. F.ADMIN-SNMP（SNMP 管理者機能）

F.ADMIN-SNMP とは、クライアント PC から SNMP を利用してネットワークを介したアクセスにおいて管理者を識別認証し、識別認証された管理者だけにネットワークの設定機能の操作を許可するセキュリティ機能である。

7.2.1. SNMP パスワードによる識別認証機能

SNMPを用いてネットワークを介してMIBオブジェクトにアクセスする利用者が管理者であることをSNMPパスワードによって識別認証する。

- 表 13 に示されるキャラクタからなる SNMP パスワードにより認証する SNMP 認証メカニズムを提供する。
  - Authentication パスワードのみ、または Privacy パスワード及び Authentication パスワード双方を利用する。
  - SNMP の場合は、別途セッション情報による管理者認証メカニズムを必要とせず、毎回のセッションに SNMP パスワード利用する。
- 認証に成功すると、認証失敗回数をリセットする。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に成功した場合に認証失敗回数をリセットする。
- SNMP パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、SNMP パスワードを利用するすべての認証機能をロックする。（MIB オブジェクトへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に失敗した場合でも 1 回の失敗として検知する。
- ロック状態は、F.ADMIN の MIB オブジェクトに対するロック解除機能が実行されることによって解除される。

以上により FIA_AFL.1[3]、FIA_UAU.2[2]、FIA_UID.2[2]が実現される。

7.2.2. SNMP を利用した管理機能

SNMP パスワードにより管理者であることが識別認証されると、MIB オブジェクトへのアクセスが許可され、以下に示す設定データの設定操作を行うことが許可される。

① ネットワークの設定

以下の設定データの設定操作を行う。

- SMTP サーバに関係する設定データ（IP アドレス、ポート番号等）
- DNS サーバに関係する設定データ（IP アドレス、ポート番号等）
- MFP アドレスに関係する一連の設定データ（IP アドレス、NetBIOS 名、AppleTalk プリンタ名等）

以上により FDP_ACC.1[3]、FDP_ACF.1[3]が実現される。

② SNMP パスワードの変更

SNMP パスワード（Privacy パスワード、Authentication パスワード）を変更する。新しく設定される SNMP パスワードが以下の品質を満たしていることを検証する。

- 表 13 の SNMP パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。
- 現在設定される値と一致しない。

以上により FIA_SOS.1[2]、FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

③ SNMP パスワード認証機能の設定

SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。

以上により FMT_MOF.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.3. F.SERVICE（サービスモード機能）

F.SERVICE とは、パネルからアクセスするサービスモードにおけるサービスエンジニア識別認証機能、CE パスワードの変更や管理者パスワードの変更などのセキュリティ管理機能といったサービスエンジニアが操作する一連のセキュリティ機能である。

7.3.1. サービスエンジニア識別認証機能

パネルからサービスモードへのアクセス要求に対して、アクセスする利用者をサービスエンジニアであることを識別及び認証する。

- 表 13 に示されるキャラクタからなる CE パスワードにより認証する CE 認証メカニズムを提供する。
  - サービスモードの場合はパネルからのアクセスのみになるため、別途セッション情報による CE 認証メカニズムを必要としない。
- CE パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからの入力を 5 秒間受け付けない。
- CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、CE パスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作して解除する。

以上により FIA_AFL.1[1]、FIA_AFL.1[8]、FIA_UAU.2[1]、FIA_UAU.7、FIA_UID.2[1]が実現される。

7.3.2. サービスモードにて提供される機能

サービスモードへのアクセス要求においてサービスエンジニア識別認証機能により、サービスエンジニアとして識別認証されると、以下の機能の利用が許可される。

7.3.2.1. CE パスワードの変更

サービスエンジニアであることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

- 表 13に示されるキャラクタからなるCEパスワードにより再認証するCE認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、CE パスワード入力のフィードバックに 1 文字毎“*”を返す。

CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、パネルからアクセスするサービスモードをログアウトし、CE パスワードを利用するすべての認証機能をロックする。(サービスモードへのアクセスを拒否する。)

  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。

- 認証機能のロックは、F.RESET が動作して解除する。
- 新規設定される CE パスワードは以下の品質を満たしていることを検証する。
  - 表 13 の CE パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_AFL.1[1]、FIA_SOS.1[1]、FIA_UAU.6、FIA_UAU.7、FMT_MTD.1[9]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.3.2.2. 管理者パスワードの変更

管理者パスワードを変更する。新規設定される管理者パスワードは以下の品質を満たしていることを検証する。

- 表 13 の管理者パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。
- 現在設定される値と一致しない。

以上により FIA_SOS.1[1]、FMT_MTD.1[6]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.3.2.3. CE 認証の操作禁止解除時間の設定

CE 認証の操作禁止解除時間を 5～60 分で設定する

以上により FMT_MTD.1[9]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.3.2.4. セキュリティ強化機能に関連する機能

サービスエンジニアが操作するセキュリティ強化機能の設定に影響する機能は以下の通り。

- HDD 論理フォーマット機能
  HDD にファイルシステムで利用する管理データの初期値を書き込む機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- HDD 物理フォーマット機能
  HDD にトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- イニシャライズ機能
  NVRAM 及び SSD に書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、セキュリティ強化機能の設定を無効にする。

以上により FMT_MOF.1[1]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.4. F.USER（ユーザ機能）

F.USER とは、MFP の諸機能を利用するにあたって、ユーザを識別認証する。また識別認証されたユーザには、F.BOX や F.PRINT などの機能の利用を許可する他、本体認証時に MFP 本体にて管理されるユーザパスワードの管理機能を提供する。

7.4.1. ユーザ認証機能

＜部門認証：連動方式のユーザ識別認証＞

ボックスへのアクセス要求、セキュリティ文書ファイルの保存要求において、許可ユーザであることを識別認証する。識別認証されたユーザには、ユーザ ID 以外に予め設定される当該ユーザ ID に対する所属部門（部門 ID）が関連付けられ、F.BOX および F.PRINT の利用を許可する。

- ユーザパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該ユーザに対して、通算 1～3 回目となる認証失敗を検知すると、当該ユーザに対する認証機能をロックする。
  - 失敗回数閾値は、認証操作禁止機能の動作設定にて管理者が指定する。
- 認証機能のロックは、F.ADMIN において当該ユーザに対するロック解除機能が実行されることによって解除される。

以上により FIA_AFL.1[4]、FIA_AFL.1[8]、FIA_ATD.1、FIA_UAU.1[1]、FIA_UAU.7、FIA_UID.2[3]、FIA_USB.1 が実現される。

＜部門認証：連動方式において所属部門が登録されていない場合の所属部門登録機能＞

- ユーザ識別認証後、部門認証が要求される。
- 部門認証に成功すると、成功した部門 ID が所属部門として登録される。（これにより FMT_MTD.1[12]、FMT_SMF.1、FMT_SMR.1[6]が実現される。）
  （部門認証の詳細は、下段の＜部門認証：個別認証方式のユーザ識別認証＞において説明される箇条書き部の処理と同様。）

＜部門認証：個別認証方式のユーザ識別認証＞

ボックスへのアクセス要求、セキュリティ文書ファイルの保存要求において、許可ユーザであることを識別認証する。ユーザ認証の詳細は、部門認証：連動方式のユーザ識別認証と同様である。パネルからのアクセスの場合、ユーザ識別認証されたユーザには、部門認証が要求され、部門認証に成功するとユーザ ID に所属部門が関連づけられ、F.BOX および F.PRINT の利用を許可する。

- 表 13 に示されるキャラクタからなる部門パスワードにより、部門を認証する部門認証メカニズムを提供する。
- 部門パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該部門に対して、通算 1～3 回目となる認証失敗を検知すると、当該部門に対する認証機能をロックする。
  - 失敗回数閾値は、認証操作禁止機能の動作設定にて管理者が指定する。

- 認証機能のロックは、F.ADMIN において当該部門に対してロック解除機能が実行されることによって解除される。

以上により FIA_AFL.1[7]、FIA_AFL.1[8]、FIA_ATD.1、FIA_UAU.1[2]、FIA_UAU.7、FIA_UID.2[6]、FIA_USB.1 が実現される。

ネットワークからのアクセスの場合、ユーザ認証後に部門を認証するのではなく、ユーザ及び部門を 1 つのシーケンス内で処理する。認証されると、ユーザ ID と部門 ID は関連付けられ、部門認証：連動方式のユーザ識別認証と同じセッション情報より、ユーザ ID、部門 ID を判定する。

- 表 13 に示されるキャラクタからなるユーザパスワードにより、ユーザを認証するユーザ認証メカニズムを提供する。
  - ネットワークからのアクセスに対してユーザ認証後は、ユーザパスワードとは別のセッション情報を利用した、ユーザ認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。

以上により FIA_ATD.1、FIA_SOS.1[4]、FIA_SOS.2、FIA_USB.1 が実現される。

＜部門認証：利用しない場合のユーザ識別認証＞

ボックスへのアクセス要求、セキュリティ文書ファイルの保存要求において、許可ユーザであることを識別認証する。ユーザ認証の詳細は、部門認証：連動方式のユーザ識別認証と同様である。ユーザ識別認証されたユーザには、F.BOX および F.PRINT の利用を許可する。

以上により FIA_AFL.1[4]、FIA_AFL.1[8]、FIA_ATD.1、FIA_UAU.1[1]、FIA_UAU.7、FIA_UID.2[3]、FIA_USB.1 が実現される。

＜ユーザ ID の自動登録＞

ユーザ認証方式に「外部サーバ認証」が選択されている場合、識別認証されたユーザは、識別認証に伴って利用されたユーザ名、認証サーバ情報と合わせてユーザ ID として登録する。

以上により FIA_UID.2[7]、FMT_MTD.1[10]、FMT_SMF.1、FMT_SMR.1[5]が実現される。

7.4.2. 部門認証機能の動作方式設定機能

ユーザ認証機能と組み合わせて利用される部門認証機能における以下の認証方式を設定する。

- 部門認証機能（ユーザ用）：連動方式
  ユーザ ID に予め関連付けられている部門 ID を利用する方式
- 部門認証機能（ユーザ用）：個別認証方式
  ユーザ ID に予め関連付けられている部門 ID を利用せず、アクセス時に部門 ID と部門パスワードによって認証する方式

以上により FMT_MOF.1[5]、FMT_SMF.1、FMT_SMR.1[6]が実現される。

7.4.3. ユーザ識別認証ドメインにおけるオートログアウト機能

識別認証されたユーザがパネルからアクセス中、パネルオートログアウト時間以上何らかの操作を受け付けなかった場合、自動的にユーザ識別認証ドメインからログアウトする。

以上により FTA_SSL.3 が実現される。

7.4.4. ユーザパスワードの変更機能

識別認証され、ユーザ識別認証ドメインへのアクセスが許可されると、本人のユーザパスワードを変更することが許可される。なお外部サーバ認証が有効の場合には、本機能は利用できない。

ユーザであることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

- 表 13 に示されるキャラクタからなるユーザパスワードにより認証するユーザ認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、パネルからのアクセスの場合、ユーザパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 当該ユーザに対するユーザパスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、当該ユーザのユーザパスワードを利用するすべての認証機能をロックする。（ユーザのログインを拒否する。ユーザパスワードの変更操作を拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.ADMIN において当該ユーザに対するロック解除機能が実行されることによって解除される。
- 新規設定されるユーザパスワードが以下の品質を満たしている場合、変更する。
  - 表 13 のユーザパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_AFL.1[4]、FIA_SOS.1[1]、FIA_UAU.6、FIA_UAU.7、FMT_MTD.1[2]、FMT_SMF.1、FMT_SMR.1[3]が実現される。

7.5. F.BOX（ボックス機能）

F.BOX とは、許可ユーザであると識別認証されたユーザに対して、そのユーザの個人ボックスの操作、管理を許可する。部門認証を利用している場合、当該ユーザの所属部門に関連付けられるグループボックスの操作、管理を許可する。共有ボックスへのアクセスに対して共有ボックスの利用を許可されたユーザであることを認証し、認証後に当該ボックス、ボックスファイルの各種操作を許可するアクセス制御機能などボックスに関係する一連のセキュリティ機能のことである。

＜ユーザ操作によるボックスの登録＞

選択した未登録ボックス ID に対して、ユーザ属性を選定して、個人ボックス、グループボックス、または共有ボックスを登録する。登録する際、ボックスのユーザ属性にはデフォルト値として「共有」が指定されるが、「ユーザ ID」または「部門 ID」を選択することも可能。

- 個人ボックスの場合は、登録される任意のユーザ ID を指定する。
- 共有ボックスの場合は、登録されるボックスパスワードが以下の条件を満たすことを検証する。
  - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- グループボックスの場合、登録される任意の部門 ID を指定する。

以上により FIA_SOS.1[1]、FMT_MSA.3[1]、FMT_MTD.1[5]、FMT_SMF.1、FMT_SMR.1[3]が実現される。

＜ボックスの自動登録＞

- プリントジョブにおけるボックス保存操作において、指定したボックスが未登録である場合、ユーザ属性に当該ジョブを操作するユーザのユーザ ID が設定される個人ボックスを自動的に登録

する。
以上により FMT_MSA.3[1]、FMT_SMF.1 が実現される。

＜ボックスファイルの保存＞
- ボックスファイルの新規保存操作、移動またコピー操作において、ボックスファイルのボックス属性には、保存対象として指定したボックスと同値のボックス ID を設定する。

以上により FMT_MSA.3[3]が実現される。

7.5.1. 個人ボックス機能

7.5.1.1. 個人ボックスに対するアクセス制御機能

識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザ ID」を持つ。このタスクは、このユーザ属性と一致するユーザ属性を持つ個人ボックスの一覧表示操作が許可される。
以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。

7.5.1.2. 個人ボックス内のボックスファイルに対するアクセス制御機能

操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、ボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、E-mail 送信（S/MIME 送信を含む）、FTP 送信、FAX 送信、SMB 送信、WebDAV 送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー、外部メモリへのコピー操作を行うことを許可される。
以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。

7.5.1.3. 個人ボックスのユーザ属性変更

ユーザ属性を変更することができる。
- 他の登録ユーザを指定すると、他のユーザが管理する個人ボックスになる。
- 共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。この場合は、ボックスパスワードが以下の条件を満たすことを検証する。
  - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 部門 ID を指定すると、当該部門の利用を許可されたユーザがアクセス可能なグループボックスになる。

以上により FIA_SOS.1[1]、FMT_MSA.1[1]、FMT_SMF.1、FMT_SMR.1[3]が実現される。

7.5.2. 共有ボックス機能

許可ユーザとして識別認証されると、識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザ ID」を持つ。このタスクは、ユーザ属性に共有が設定される共有ボックスの一覧表示操作が許可される。個々の共有ボックスの操作仕様は以下の通りである。
（上記により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。）

7.5.2.1. 共有ボックスへのアクセスにおける認証機能

個々の共有ボックスへのアクセス要求に対して、上記の検証機能の動作後、アクセスする利用者をそれぞれ当該共有ボックスの利用を許可されたユーザであることを認証する。

- 表 13 に示されるキャラクタからなるボックスパスワードにより認証するボックス認証メカニズムを提供する。
- ネットワークからのアクセスに対してボックス認証後は、ボックスパスワードとは別のセッション情報を利用した、ボックス認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- ボックスパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
  - パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 当該共有ボックスに対して、通算 1～3 回目となる認証失敗を検知すると、当該共有ボックスに対する認証機能をロックする。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.ADMIN の共有ボックスに対するロック解除機能が実行されることによって解除される。

以上により FIA_AFL.1[6]、FIA_AFL.1[8]、FIA_SOS.1[4]、FIA_SOS.2、FIA_UAU.2[4]、FIA_UAU.7、FIA_UID.2[5]が実現される。

以下は当該共有ボックスの利用を許可されたユーザが当該ボックスのボックス識別認証ドメインにおいて提供される機能である。

7.5.2.2. 共有ボックス内のボックスファイルに対するアクセス制御

ユーザを代行するタスクは、ユーザ属性に加えてそのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、サブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、E-mail 送信（S/MIME 送信を含む）、FTP 送信、FAX 送信、SMB 送信、WebDAV 送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー、外部メモリへのコピー操作を行うことを許可される。

以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。

7.5.2.3. 共有ボックスのユーザ属性変更

当該ボックスのユーザ属性を変更することができる。

- 登録ユーザを指定し、登録ユーザの個人ボックスに変更する。
- 部門 ID を指定し、当該部門の利用が許可されたユーザがアクセス可能なグループボックスにする。

以上により FMT_MSA.1[2]、FMT_SMF.1、FMT_SMR.1[4]が実現される。

7.5.2.4. 共有ボックスパスワードの変更

共有ボックスのボックスパスワードを変更する。当該共有ボックスの利用を許可されたユーザであることを再認証され、且つ新しく設定されるボックスパスワードが以下の品質を満たしている場合、変更する。

- 表 13 に示されるキャラクタからなるボックスパスワードにより認証するボックス認証メカニズ

ムを提供する。

- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、パネルからのアクセスの場合、ボックスパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 当該共有ボックスに対するボックスパスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、当該共有ボックスのボックスパスワードを利用するすべての認証機能をロックする。(当該共有ボックスへのログインを拒否する。当該共有ボックスのボックスパスワード変更操作を拒否する。)
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.ADMIN の共有ボックスに対するロック解除機能が実行されることによって解除される。
- 新規設定されるボックスパスワードが以下の品質を満たしている場合、変更する。
  - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

以上により FIA_AFL.1[6]、FIA_SOS.1[1]、FIA_UAU.6、FIA_UAU.7、FMT_MTD.1[4]、FMT_SMF.1、FMT_SMR.1[4]が実現される。

7.5.3. グループボックス機能

7.5.3.1. グループボックスに対するアクセス制御機能

識別認証されたユーザを代行するタスクは、識別認証されたユーザと関連づけられた所属部門として「部門 ID」を持つ。このタスクは、この部門 ID と一致するユーザ属性を持つグループボックスの一覧表示操作が許可される。

以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。

7.5.3.2. グループボックス内のボックスファイルに対するアクセス制御機能

操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、サブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、E-mail 送信 (S/MIME 送信を含む)、FTP 送信、FAX 送信、SMB 送信、WebDAV 送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー、外部メモリへのコピー操作を行うことを許可される。

以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACF.1[1]が実現される。

7.5.3.3. グループボックスのユーザ属性変更

ユーザ属性を変更することができる。

- 他の部門 ID を指定すると、他の部門所属のユーザがアクセス可能なグループボックスになる。
- 共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。この場合は、ボックスパスワードが以下の条件を満たすことを検証する。
  - 表 13 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 登録ユーザを指定し、登録ユーザの個人ボックスに変更する。

以上により FIA_SOS.1[1]、FMT_MSA.1[3]、FMT_SMF.1、FMT_SMR.1[6]が実現される。

7.6. F.PRINT（セキュリティ文書機能、認証＆プリント機能）

F.PRINT とは、セキュリティ文書機能、及び認証&プリント機能におけるにおけるセキュリティ機能である。

許可ユーザであると識別認証されたユーザに対して、パネルからのセキュリティ文書ファイルへのアクセスに対してセキュリティ文書ファイルの利用を許可されたユーザであることを認証し、認証後に当該セキュリティ文書ファイルの一覧表示、印刷を許可するアクセス制御機能を提供する。

また許可ユーザであると識別認証されたユーザに対して、パネルからの認証&プリントファイルへのアクセスに対して当該ユーザが保存した認証&プリントファイルだけを一覧表示、印刷操作を許可するアクセス制御機能を提供する。

7.6.1. セキュリティ文書機能

7.6.1.1. セキュリティ文書パスワードによる認証機能

許可ユーザであることが識別認証されると、パネルからセキュリティ文書ファイルへのアクセス要求に対して、アクセスする利用者を当該セキュリティ文書ファイルの利用を許可されたユーザであることを認証する。

- 表 13 に示されるキャラクタからなるセキュリティ文書パスワードにより認証するセキュリティ文書認証メカニズムを提供する。
- セキュリティ文書の場合はパネルからのアクセスのみになるため、別途セッション情報によるセキュリティ文書認証メカニズムを必要としない。
- セキュリティ文書パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該セキュリティ文書ファイルに対して、通算 1～3 回目となる認証失敗を検知すると、当該セキュリティ文書ファイルに対する認証機能をロックする。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- ロック状態は、F.ADMIN において当該セキュリティ文書ファイルに対してロック解除機能が実行されることによって解除される。

以上により FIA_AFL.1[5]、FIA_AFL.1[8]、FIA_UAU.2[3]、FIA_UAU.7、FIA_UID.2[4]が実現される。

7.6.1.2. セキュリティ文書ファイルに対するアクセス制御機能

認証されると、セキュリティ文書ファイルアクセス制御が動作する。

- 識別認証されたユーザを代行するタスクは、ファイル属性に、認証されたセキュリティ文書ファイルのセキュリティ文書内部制御 ID を持つ。
- このタスクは、このファイル属性と一致するファイル属性を持つセキュリティ文書ファイルに対して印刷を許可される。

以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[2]、FDP_ACF.1[2]が実現される。

7.6.1.3. セキュリティ文書ファイルの登録機能

セキュリティ文書ファイルの保存要求において、許可されたユーザとして認証されると、セキュリティ文書パスワードを対象となるセキュリティ文書ファイルと共に登録することを許可する。

- **セキュリティ文書パスワードの登録**
  登録されるセキュリティ文書パスワードが以下の条件を満たすことを検証する。
  - 表 13 のセキュリティ文書パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

- **セキュリティ文書内部制御 ID の付与**
  セキュリティ文書ファイルの保存要求において、セキュリティ文書パスワードの検証が完了すると、一意に識別されるセキュリティ文書内部制御 ID を当該セキュリティ文書ファイルに設定する。

以上により FIA_SOS.1[1]、FMT_MSA.3[2]、FMT_MTD.1[8]、FMT_SMF.1、FMT_SMR.1[3]が実現される。

7.6.2. 認証＆プリント機能

7.6.2.1. 認証＆プリントファイルの登録機能

認証&プリントファイルの保存要求において、許可されたユーザとして認証されると認証&プリントファイルが保存される。

- 保存する利用者のユーザ ID を当該認証&プリントファイルのユーザ属性として設定する。

以上により FMT_MSA.3[4]が実現される。

7.6.2.2. 認証＆プリントファイルに対するアクセス制御機能

認証されると、認証&プリントファイルアクセス制御が動作する。

- 識別認証されたユーザを代行するタスクは、ユーザ属性としてユーザ ID を持つ。
- このタスクは、このユーザ属性と一致するユーザ属性を持つ認証&プリントファイルに対して一覧表示、印刷操作を許可される。

以上により FIA_ATD.1、FIA_USB.1、FDP_ACC.1[4]、FDP_ACF.1[4]が実現される。

7.7. F.CRYPTO（暗号鍵生成機能）

F.CRYPTO とは、コニカミノルタ暗号仕様標準によって規定されるコニカミノルタ HDD 暗号鍵生成アルゴリズムを利用し、HDD に書き込まれるすべてのデータを暗号化するための暗号鍵を生成する。

F.ADMIN においてアクセス制限される HDD 暗号化機能の動作設定において暗号化ワードが決定されると、コニカミノルタ HDD 暗号鍵生成アルゴリズムを用いて暗号化ワードから 128bit 長の暗号鍵を生成する。

以上により FCS_CKM.1 が実現される。

7.8. F.RESET（認証失敗回数リセット機能）

F.RESET とは、管理者認証、CE 認証においてアカウントロックした場合にカウントした認証失敗回数をリセットして、ロックを解除する機能である。

① CE 認証機能ロック解除処理機能

特定操作により実行され、CE 認証の操作禁止解除時間後に CE 認証の失敗回数を 0 クリアすることによりロックを解除する。

以上により FIA_AFL.1[1]が実現される。

② 管理者認証機能ロック解除処理機能

主電源の OFF/ON より実行され、管理者認証の操作禁止解除時間後に管理者認証の失敗回数を 0 クリアすることによりロックを解除する。

以上により FIA_AFL.1[2]が実現される。

7.9. F.TRUSTED-PASS（高信頼チャネル機能）

F.TRUSTED-PASS とは、クライアント PC と MFP 間で以下の画像ファイルを送受信する際に、SSL または TLS プロトコルを使用して、高信頼チャネルを生成、及び実現する機能である。

- ボックスファイル（MFP からクライアント PC へのダウンロード）
- ボックスファイルとして保存されることになる画像ファイル（クライアント PC から MFP へのアップロード）
- セキュリティ文書ファイルとして保存されることになる画像ファイル（クライアント PC から MFP へのアップロード）
- 認証&プリントファイルとして保存されることになる画像ファイル（PC から MFP へのアップロード）

以上により FTP_ITC.1 が実現される。

7.10. F.S/MIME（S/MIME 暗号処理機能）

F.S/MIME とは、ボックスファイルを S/MIME として送信する際に、ボックスファイルを暗号化するための機能である。

＜ボックスファイル暗号鍵生成＞

- FIPS 186-2 が規定する擬似乱数生成アルゴリズムより、ボックスファイルを暗号化するための暗号鍵を生成する。（暗号鍵長は、128 bit、168 bit、192 bit、256 bit のいずれかである。）

以上により FCS_CKM.1 が実現される。

＜ボックスファイル暗号化＞

- ボックスファイルを暗号化するための暗号鍵（128 bit、192 bit、256 bit）により、FIPS PUB 197 によって規定される AES によって暗号化される。
- ボックスファイルを暗号化するための暗号鍵（168 bit）により、SP800-67 によって規定される 3-Key-Triple-DES によって暗号化される

以上により FCS_COP.1 が実現される。

＜ボックスファイル暗号鍵の暗号化＞

- ボックスファイルを暗号化するための暗号鍵は、FIPS 186-2 が規定する RSA により、暗号化される。
- この際利用される暗号鍵の鍵長は、1024bit、2048 bit、3072 bit、4096 bit のいずれかである。

以上により FCS_COP.1 が実現される。

7.11. F.FAX-CONTROL（FAX ユニット制御機能）

F.FAX-CONTROL とは、FAX ユニットを通じて、MFP に接続された内部ネットワークへのアクセスを、TOE が制御することにより禁止する機能である。

TOE は、公衆回線網から受け渡されるデータを内部 LAN に受け渡す機能を制御する。TOE の制御により公衆回線から内部ネットワークへのアクセス（画像データを除くデータの転送）の禁止を実現する。

以上により、FDP_IFC.1、及び FDP_IFF.1 が実現される。

7.12. F.SUPPORT-AUTH（外部サーバ認証動作サポート機能）

F.SUPPORT-AUTH とは、ActiveDirectory によるユーザ情報管理サーバと連携してユーザ認証機能を実現するための機能である。（F.USER と共に動作する機能である。）

ユーザ認証方式に「外部サーバ認証」が選択されている場合で、ユーザから識別認証処理が要求されると、ユーザ情報管理サーバに対して該当ユーザに対する認証情報の問い合わせを行う。これに対してユーザ情報管理サーバから返される認証情報を取得し、ユーザの識別認証処理を実現する。

以上により、FIT_CAP.1[1]が実現される。

7.13. F.SUPPORT-CRYPTO（ASIC サポート機能）

F.SUPPORT-CRYPTO とは、TOE から ASIC による HDD 暗号化機能を動作させるための機能である。

HDD に書き込まれるすべてのデータに対して、F.CRYPTO により生成された暗号鍵を ASIC にセットし、ASIC にて暗号化処理を行わせる。また HDD から読み出される暗号化されたデータに対して、同じく F.CRYPTO により生成された暗号鍵を ASIC にセットし、ASIC にて復号処理を行わせる。

以上により、FIT_CAP.1[2]が実現される。

7.14. F.OVERWRITE（HDD データ上書き削除機能）

F.OVERWRITE とは、HDD 上の不要になった画像データが再利用されないように、データ領域に対し、上書き削除を実行する。

- 上書き削除の対象となる画像データは以下の通りである。
  - ボックスファイル

- セキュリティ文書ファイル
- 認証&プリントファイル
- 保存画像ファイル
- HDD 残存画像ファイル
- 画像関連ファイル

● 上書き削除の実施タイミングは以下の通りである。
- プリントやスキャンなどのジョブの完了、停止時
- 削除操作などによって、データの保持が不要になった時
- 意図しない電源オフの後、電源オン時に残存情報が存在する時

● HDD に書き込むデータ、書き込む回数など削除方式は、F.ADMIN において設定される HDD データ上書き削除機能の消去方式（**表 15**）に応じて実行される。

以上により FDP_RIP.1 が実現される。

表 15 一時データ上書き削除のタイプと上書きの方法

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	0x00 ⇒ 0xFF ⇒ 0x61 ⇒ 検証

7.15. F. AUDIT-LOGGED（監査ログ機能）

F. AUDIT-LOGGED とは、セキュリティ関連の監査対象事象が発生した際、監査記録であるログを生成する機能である。以下の事象の記録を生成する。

① スタートアップ/シャットダウン
MFP の起動と終了、監査ログ機能の ON/PFF の記録を取得する。

② （監視すべき）ジョブの開始と完了
MFP に登録してある保護資産であるボックスファイル、セキュリティ文書ファイル、認証&プリントファイルに関する操作のログを取得する。これら操作が監視すべきジョブであり、その開始と完了のタイミングの記録を取得する。

- ボックスファイル
  ボックスファイルに関するジョブは以下の通り。以下のジョブの記録を取得する。
  - ✧ パネルジョブ
    （操作パネルからのコピー、スキャン、ボックスモードでのボックス保存操作）
  - ✧ ドライバー・ネットワーク経由ボックス保存ジョブ
    （プリンタドライバ及びネットワーク経由からのボックス保存）
  - ✧ USB・Bluetooth 経由ボックス保存ジョブ
    （USB と Bluetooth 経由のボックス保存操作）
  - ✧ FAX 受信ボックス保存ジョブ
    （FAX 受信経由のボックス保存操作）
  - ✧ ボックス出力ジョブ
    （操作パネルからのボックスモードでの印刷、操作パネル及びネットワークからのボックスモードでの送信操作）
- セキュリティ文書ファイル、認証&プリントファイル
  セキュリティ文書ファイル、認証&プリントファイルに関するジョブは以下の通り。以

下のジョブの記録を取得する。

- ✧ ドライバー・ネットワーク経由ボックス保存ジョブ
  （プリンタドライバ及びネットワーク経由からのボックス保存操作）
- ✧ ボックス出力ジョブ
  （操作パネルからの印刷操作）

③ すべての認証機能の成功と失敗

- ➢ 管理者・CE 識別認証
- ➢ ユーザ認証、部門認証
- ➢ 共有ボックス認証
- ➢ セキュリティ文書アクセス認証

また、ログ取得項目として「日時情報」「ユーザ ID」「ジョブ名（ジョブタイプ）」「結果」が記録される。日時情報は F.ADMIN で管理者が設定する日時情報が記録される。また、管理者はネットワーク経由でログファイルをエクスポートすることができ、エクスポートした際にログは削除される。管理者以外のユーザはログのエクスポート及び削除の操作を実施することができない。また、監査記録が満杯になった場合、最も古い監査ログから順に上書きするか、TOE の動作を禁止する。F.ADMIN の設定に応じて動作する。

以上により、FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4 が実現される。

---以上---