
# *bizhub C3850 / bizhub C3350*
# *PKI Card System Control Software*
# *セキュリティターゲット*

バージョン：1.09

発行日：2015年7月24日

作成者：コニカミノルタ株式会社

＜更新履歴＞

| 日付 | Ver | 担当部署 | 承認者 | 確認者 | 作成者 | 更新内容 |
|---|---|---|---|---|---|---|
| 2014/4/30 | 1.00 | 第2OPシステム制御開発部 | 山崎 | 小西 | 津山 | 初版 |
| 2014/8/26 | 1.01 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・S/MIMEに対する見直し修正<br>（暗号強化モードON時にはPSWC使用できない）<br>・Boot制御部の見直し<br>・評価環境を追記<br>・誤植の修正 |
| 2014/9/8 | 1.02 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・TOE名称の変更 |
| 2014/9/26 | 1.03 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・全体の見直し修正 |
| 2014/10/3 | 1.04 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・誤植の修正 |
| 2014/10/23 | 1.05 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・誤植の修正（クライアントPC環境） |
| 2014/11/11 | 1.06 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・誤植の修正 |
| 2014/12/3 | 1.07 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・保護資産の記述、暗号サポートの依存性に関する見直し修正<br>・誤植の修正 |
| 2014/12/22 | 1.08 | 第2OPシステム制御開発部 | 山崎 | 小西 | 戸田 | ・TOEバージョンの修正 |
| 2015/7/24 | 1.09 | 第2OPシステム制御開発部 | 山崎 | 小西 | 田向 | ・ガイダンスの修正 |

## —【 目次 】

## —【 図目次 】



## —【 表目次 】

# 1. ST 概説

## 1.1. ST 参照

・ST名称　：bizhub C3850 / bizhub C3350 PKI Card System Control Software セキュリティターゲット
・STバージョン　：1.09
・作成日　：2015年7月24日
・作成者　：コニカミノルタ株式会社

## 1.2. TOE 参照

・TOE名称　：bizhub C3850 / bizhub C3350 PKI Card System Control Software
・TOE識別　：A3GN30G0213999P（TOE識別の説明：コントローラーファームウェア）
・TOEの種別　：ソフトウェア
・製造者　：コニカミノルタ株式会社

## 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について説明する。なお、TOE の利用環境、動作環境については、「1.4」節に記述する。

### 1.3.1. TOE の種別

TOE である bizhub C3850 / bizhub C3350 PKI Card System Control Software とは、mfp 制御コントローラー上の 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 C3850 / bizhub C3350 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 C3850 / bizhub C3350 PKI Card System Control Software”である。

TOE は、mfp とクライアント PC 間でやりとりされる機密性の高いドキュメントのうち、クライアント PC から mfp へ送信するプリントデータに対して、専用のプリンタドライバー及び IC カードを利用して実現される暗号化プリントを、専用ドライバー（ローダブルドライバー）及び生成する際に利用した IC カードを使い印刷する機能を提供する。また mfp からメール送信するスキャン画像データに対してローダブルドライバー及び IC カードを利用した S/MIME による保護機能を提供する。いずれも IC カードと TOE が連携し、これらセキュリティ機能を実現する。

さらに mfp 内で処理する画像データを一時的に保存する媒体である HDD にアクセスされる等の危険性に対して、HDD に書き込まれる画像データを暗号化することが可能である。他に、TOE は、各種上書き削除規格に則った削除方式により HDD に保存される画像データを含むデータ領域を完全に削除する機能を有し、mfp を利用する組織の情報漏洩の防止に貢献する。

## 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。

- **ユーザー**
  IC カードを所有している 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、ユーザーの管理を行う。（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。

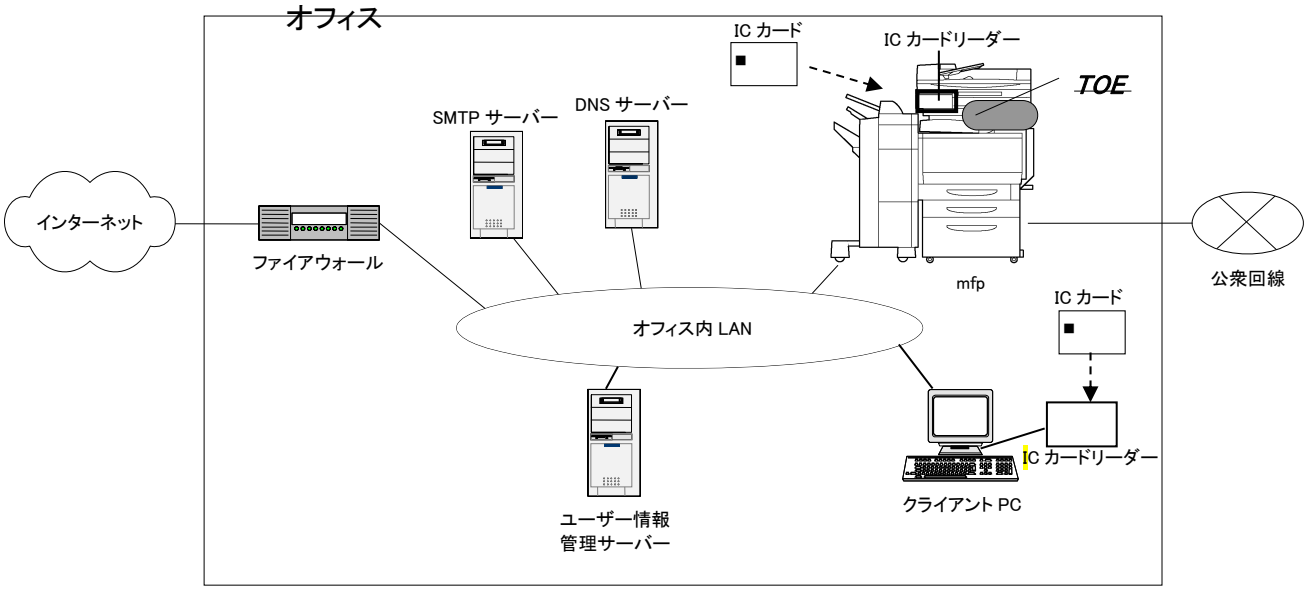


図 1　mfp の利用環境の例

- 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。
- クライアント PC の IC カード、及び IC カードリーダーは、専用プリンタドライバーを利用した mfp への暗号化プリントファイルの送信や、mfp より送信されたスキャン画像データの復号に利用される。
- オフィス内 LAN にはユーザー情報管理サーバーが接続され、IC カードの認証に利用される。
  なお、ユーザー情報管理サーバーは、Active Directory （Kerberos 認証プロトコル）が利用できる Windows Server OS を TOE 評価に使用する。
- オフィス内 LAN には SMTP サーバーが接続され、mfp はこれらともデータ通信を行うことが可能。（なお SMTP サーバー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。）
- 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れる。
- mfp に接続される公衆回線は、FAX の通信に利用される。

#### 1.4.2.2. 動作環境

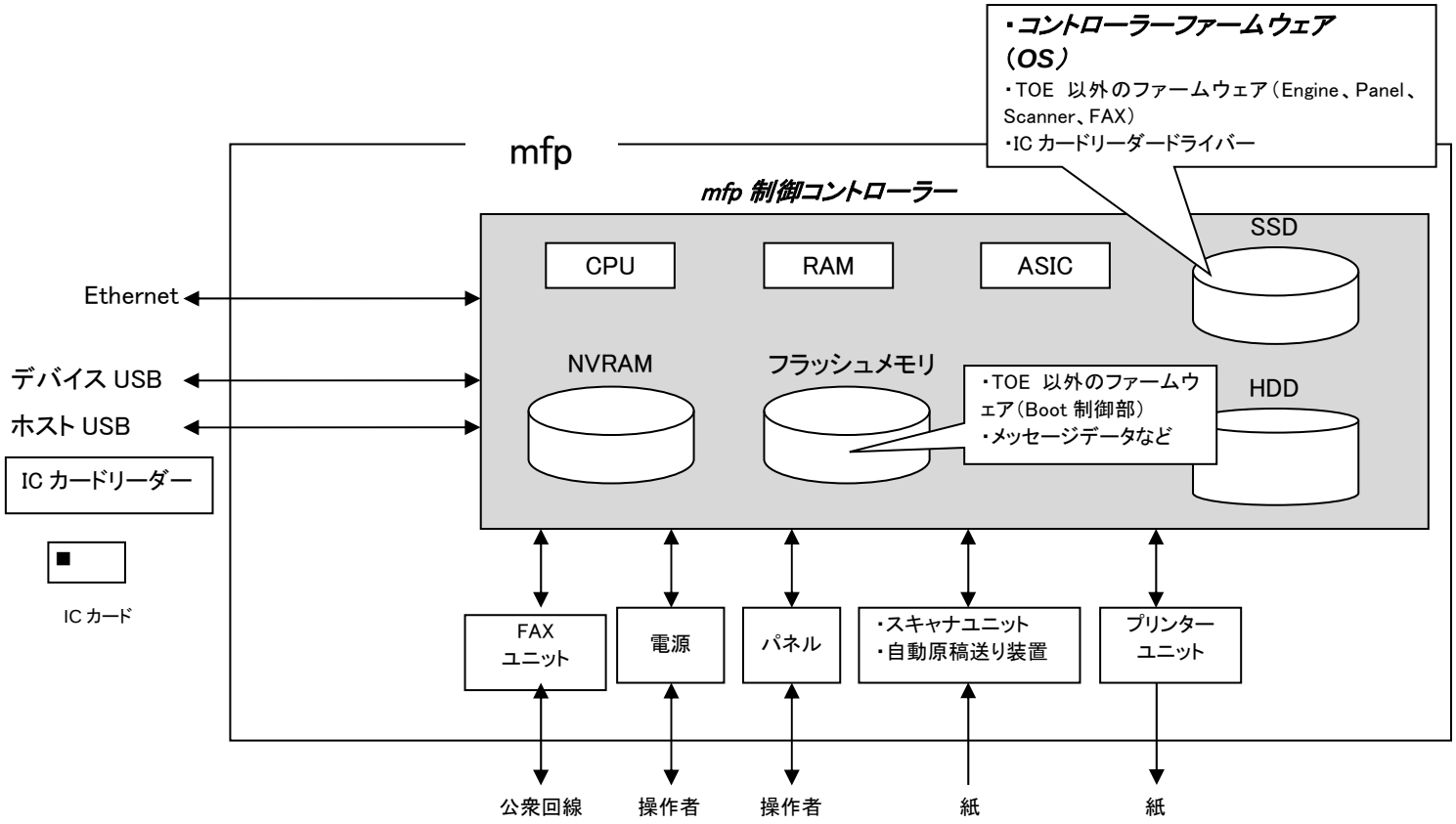


図 2　TOE に関係するハードウェア構成

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 制御コントローラーは mfp 本体内に据え付けられ、TOE はその mfp 制御コントローラー上の SSD にコントローラーファームウェアが存在し、電源が ON になると揮発性 RAM（図 2 においては、「RAM」と表記）にロードされ動作する。

以下には図 2 にて示される mfp 制御コントローラー上の特徴的なハードウェア、mfp 制御コントローラーとインターフェースを持つハードウェアについて説明する。

- RAM
  HDD の暗号化に使用される暗号鍵が保管される。

- SSD
  Flash Memory Drive である。TOE である mfp 全体制御ソフトウェアにおけるコントローラーファームウェアのオブジェクトコード、TOE 以外のファームウェアである Engine、Panel、Scanner、FAX のファームウェアのオブジェクトコード、IC カードリーダードライバーなどが保管される記憶媒体。

- 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管される記憶媒体。NVRAM には、管理者パスワード、CE[1]パスワード、暗号化ワードが保管される。

[1] Customer Service engineer の略称。また、CE はサービスエンジニアの略称でも使用される。

- **フラッシュメモリ**
  TOE 以外の Boot 制御部のオブジェクトコードが保存される記録媒体。
  また、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。

- ASIC
  画像処理全般を行うために設計された集積回路。また、画像を印刷する時に画像の展開と色合いの調整等の処理も行う。

- HDD
  画像データがファイルとして保管される他、IC カード ID などが保管される。すべての画像ファイル、IC カード ID などは、暗号化して保管される。

- **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。

- **プリンターユニット**
  mfp 制御コントローラー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。

- **デバイス USB**
  mfp 本体の後ろ側にあるローカル接続でプリントするためのポート。

- **ホスト USB**
  mfp のパネル側にある USB ポート。TOE のアップデート、USB インターフェースに接続した USB メモリからの印刷あるいはスキャンしたデータを保存することが可能。なお、この印刷及びスキャンには本 ST に記述される暗号化プリント、及び S/MIME 暗号処理機能は含まれていない。
  また、IC カードリーダーを接続することによって、ユーザーは IC カードを利用して mfp にアクセスすることが可能。IC カードリーダーは販売の都合により mfp には標準搭載されず、オプションパーツであるが、本 ST の想定では必須の構成部品である。

- **FAX ユニット**
  公衆回線を介して FAX の送受信の通信に利用される FAX 公衆回線ロを持つデバイス。

- **IC カード**
  Common Access Card（CAC）、及び Personal ID Verification（PIV）の標準仕様をサポートする IC カード。

- IC カードリーダー
  mfp とクライアント PC に接続する IC カードを読み取るための機器。
  使用する機器は AU-211P/Identive SCR-3310/SCR-3310v2 である。

- IC カードリーダードライバー
  IC カードリーダーにアクセスするためのドライバー。
  IC カードリーダードライバーは、IC カードの種類、及び IC カードリーダーに対応したドライバーが必要である。
  なお、mfp 側の TOE 評価には以下のドライバーを使用する。
  IC カードリーダードライバー　A3GN0Y0-A401-G00-00

- FAX ユニット
  公衆回線を介して FAX の送受信に利用される FAX 公衆回線口をもつデバイス。

- クライアント PC 上のソフトウェア
  以下に、TOE 評価で使用するクライアント PC のソフトウェアのバージョンを示す。
  (1) Windows 7 Professional SP1
  (2) Internet Explorer Ver.11
  (3) printer driver：Windows Printer Driver KONICA MINOLTA C3850 Series PCL v1.3.6.0
  (4) ActivClinet v7.0.2.25

#### 1.4.2.3. ガイダンス

[海外版]
- bizhub C3850/C3350 for PKI Card System
  SERVICE MANUAL [SECURITY FUNCTION] Ver. 1.03
- bizhub C3850/C3350 for PKI Card System
  User's Guide [Security Operations] Ver. 1.04

[日本版]
- bizhub C3850/C3350 for PKI Card System
  サービスマニュアル　セキュリティ機能編 Ver. 1.03
- bizhub C3850/C3350 PKIカードシステム
  ユーザーズガイド　セキュリティ機能編 Ver. 1.04

### 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、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､ユーザー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 制御コントローラー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 制御コントローラー外部のデバイスに転送される。また IC カードと連携して各種機能を実現する。

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。

- **暗号化プリント**機能

  クライアント PC より専用のプリンタドライバーから生成された暗号化プリントファイルを受信した場合、暗号化されたまま印刷待機状態で保存する。
  パネルからの印刷指示により IC カードを利用した PKI 処理を経て、暗号化プリントファイルを復号して印刷を実行する。
  これによりクライアント 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。

- Scan To Me 機能

  IC カード所有者が、mfp から IC カードを利用した PKI 処理を経て自身のメールアドレスへスキャン画像を送信する機能であり、以下の 2 つの機能を利用する。

  - S/MIME 暗号化機能

    ユーザーがスキャンした画像ファイルをメールアドレスへ送信する際、スキャン画像を S/MIME メールデータファイルとして暗号化する。
    これにより機密性の高い画像が、通信路上で他の利用者に盗み見られる可能性を排除する。

  - **デジタル署名機能**

    ユーザーがスキャンした画像ファイルをメールアドレスへ送信する際、S/MIME メールデータファイルとして、メールの送信者を証明しメールデータを保証する署名データを付加する。これにより通信路上等で改ざんされたファイルを、誤って受領する可能性を排除する。

#### 1.4.3.2. 管理者機能

TOE は、認証された管理者だけがパネルから操作することが可能な管理者モードにて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。

以下に、セキュリティに関係する代表的な機能を示す。

- システムオートリセットの動作設定
  - アイドル状態で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
- 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
- HDD 暗号化機能の設定
  - HDD 暗号化機能の動作設定
- HDD 暗号化の暗号鍵生成
  - mfp の電源を ON にした時に、暗号化ワードを使用して鍵を生成し、揮発性メモリ（RAM）に保管する。
- 全データ上書き消去機能
  - HDD の上書き消去に対して、各種軍用規格（米国国防総省規格等）に則ったデータ消去方式をサポート
  - 管理者が選択したデータ消去方法に従い、HDD の全データ領域に対して、上書き消去を行う。（HDD 上書き消去機能）
  - NVRAM の管理者パスワード、暗号化ワードに対して、初期化を行う。（NVRAM 初期化機能）
  - 上記、2 つの機能を総称して、全データ上書き消去機能という。
  - 全データ上書き消去機能は、パネルを介して起動する。
- 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
- HDD 論理フォーマット機能
  - パネルを介して、論理フォーマットが実行可能。
  - 論理フォーマットは、HDD を初期化する場合に使用する。
- HDD 暗号化機能
  - HDD 暗号化機能の動作設定が“有効”の場合、HDD に書き込まれるすべての画像ファイルやパスワードなどのデータを暗号化する。
  - HDD 暗号機能を使用する時、管理者は文字列（20 桁）を入力する。その文字列は、暗号化ワードとして NVRAM に保管する。

#### 1.4.3.3. 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。以下に、セキュリティに関係する代表的な機能を示す。

- 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（管理者パスワード、HDD 暗号化機能の設定等の設定データ）に影響を及ぼす機能の動作設定機能である。

#### 1.4.3.4. その他の機能

TOE はユーザー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。

- **ファームウェアアップデート更新機能**
  TOE は TOE 自身を更新するための機能を有する。更新手段は、Ethernet を介して FTP サーバー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。

TOE は外部エンティティである IC カードのセキュリティ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。

- **IC カードの活用**
  外部エンティティである IC カードは、ユーザーの意図に反するデータの暴露への対処機能として、暗号化プリントや E-mail 送信を行う場合に暗号処理や署名処理する機能が動作する。

#### 1.4.3.5. 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、ネットワーク介した TOE の更新機能、ネットワーク設定管理初期化機能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。

- ユーザー：PUBLIC のアクセス　：禁止
- 認証なしプリントの設定　：無効
- ユーザー名一覧表示　：禁止
- パスワード規約機能　：有効
- ボックス管理者機能　：禁止
- SNMP v1/v2c Write 機能　：禁止
- SNMPv3 の利用　：禁止
- HDD 暗号化機能の設定　：有効
- プリントデータキャプチャー機能　：禁止
- ユーザーによる宛先登録変更機能　：禁止
- ネットワークサーバー機能　：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）
  （SHA-256 が有効となる）
- 画像ログ送信　：禁止
- リモートパネル機能　：禁止

以下の機能はセキュリティ強化機能が有効になるタイミングで以下に示される設定状態になるが、上記の機能群と異なり、個別に設定を変更することが可能である。

- FTP サーバー機能の設定　：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 4 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 4 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 4 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 4 CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components Version 3.1 Revision 4 CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components Version 3.1 Revision 4 CCMB-2012-09-003
- Common Methodology for Information Technology Security Evaluation
  Evaluation methodology Version 3.1 Revision 4 CCMB-2012-09-004

# 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、**“ユーザー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。

- **暗号化プリントファイル**
  クライアント PC から専用のプリンタドライバー及び IC カードを使って生成され送信される mfp に蓄積された画像ファイル。
- スキャン画像ファイル
  mfp でその場でスキャンした画像ファイル。ここではスキャンを行った利用者のメールアドレスに E-mail（S/MIME）で送付する運用を想定している。

コピー操作など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。

一方、mfp をリース返却、廃棄して利用が終了した場合など組織の管轄から保管されるデータが物理的に離れる場合は、組織は HDD に残存するあらゆるデータ、及び NVRAM に保管されている設定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。

- **暗号化プリントファイル**
- **スキャン画像ファイル**
- 保存**画像ファイル**
  - 暗号化プリントファイル以外の保存される画像ファイル
- **待機状態にあるジョブの画像ファイル**
  待機状態にあるジョブの画像ファイルで HDD データ領域に存在する画像ファイル
- **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 HDD 上に生成されたテンポラリデータファイル
- **管理者パスワード**
  NVRAM に保管される管理者のパスワード
- **暗号化ワード**
  NVRAM 上に登録される暗号化ワード。

## 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 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。

**A.IC-CARD（IC カードに関する運用条件）**
TOE の利用において使用される IC カードは、正当なユーザーに所有されている。

## 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、暗号化プリントファイル、スキャン画像ファイル、保存画像ファイルが漏洩する。また、悪意を持った者が、mfp 内の NVRAM を解析することにより、管理者パスワード、暗号化ワードが漏洩する。

**T.ACCESS-HDD（HDD 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ーが、mfp に搭載されている HDD に対して不正にアクセスして、HDD に保管されているすべての画像ファイルやパスワードなどのデータが暴露される。

## 3.4. 組織のセキュリティ方針

本 ST では、機密性が考慮される保護対象資産に対するオフィス内 LAN 上のセキュリティ対策として、ファイルの暗号化が要求され、デジタル署名の付加したメールのみ閲覧が許可されるような組織・利用者に対応した TOE セキュリティ環境を想定する。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-CRYPTO（画像ファイルの暗号化通信）**
IT 機器間にて送受信される秘匿性の高い画像ファイル（暗号化プリントファイル、スキャン画像ファイル）は、暗号化されなければならない。

**P.COMMUNICATION-SIGN（画像ファイルの署名）**

秘匿性の高い画像ファイル（スキャン画像ファイル）を含むメールには、デジタル署名が付加されなければならない。

**P.DECRYPT-PRINT（画像ファイルの復号）**

mfp で受信した秘匿性の高い画像ファイル（暗号化プリントファイル）は、そのファイルを生成した利用者だけに印刷することが許可される。

# 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.DECRYPT-PRINT（暗号化プリントファイルの復号）**

TOE は、暗号化プリントファイルの生成に利用した IC カードにのみ、当該暗号化プリントファイルの印刷を許可する。

**O.OVERWRITE-ALL（全データ上書き消去）**

TOE は、mfp 内の HDD のデータ領域に記録されている暗号化プリントファイル、スキャン画像ファイル、待機状態にあるジョブの画像ファイル、保管画像ファイル、HDD 残存画像ファイル、画像関連ファイル、及び管理者が設定した NVRAM 上の管理者パスワード、暗号化ワードを再現できなくする。

**O.CRYPTO-HDD（HDD の暗号化）**

TOE は、mfp の HDD 内に書き込まれるすべての画像ファイルやパスワードなどのデータを保護するため、暗号化ワードを使用して暗号鍵を生成し、画像ファイルやパスワードなどのデータの暗号化及び復号を行う機能を提供する。また、暗号化ワードに対しては、品質を検証する機能を提供する。さらに、HDD 暗号化機能（暗号化ワード）の設定に関係する機能は管理者だけに提供する。

**O.MAIL-CRYPTO（S/MIME の利用、暗号化）**

TOE は、スキャン画像の E-mail 送信において、利用者の要求に応じてスキャン画像を暗号化する。

**O.MAIL-SIGN（S/MIME の利用、署名）**

TOE は、スキャン画像の E-mail 送信において、利用者の要求に応じてデジタル署名処理のために必要な暗号化されたスキャン画像を含む E-mail データのメッセージダイジェストを生成する。

**O.PKI-CAPABILITY（PKI 機能を利用するためのサポート動作）**

TOE は、IC カードリーダー及び IC カードと連携して実現される暗号化プリント機能、Scan To Me 機能を利用するために、ユーザー情報管理サーバ（ActiveDirectory）を利用して IC カードリーダー及び IC カードへの必要な動作をサポートする。

## 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.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）**

TOE の保守管理を依頼する場合、mfp を利用する組織の責任者または管理者は、保守管理を行う会社と保守契約を締結する。保守契約には、不正な行為をしない旨を明記する。また、保守作業者が正規の保守会社のサービスエンジニアであることを、保守作業の前に管理者が身分証明書を確認して、管理者が保守作業に立ち会う。

**OE.CARD-USER（IC カードの利用）**

IC カードの所有者は、暗号化プリントファイルを暗号化する際は、IC カード、及び専用プリンタドライバーを利用し、スキャン画像ファイルを暗号化する際は、IC カードを利用する。

**OE.IC-CARD（IC カードの所有条件）**

mfp を利用する組織の責任者は、IC カード機能を利用する場合、以下に示す運用を実施させる。

・組織で利用するために発行した IC カードを、その IC カードの所有が許可される正しいユーザーへ配付する。

・ユーザーに対して IC カードの他人への譲渡、貸与を禁止し、紛失時の届出を徹底させる。

**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、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.SECRET（秘密情報の適切な管理）**

管理者は、以下に示す運用を実施する。

・管理者パスワード、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、暗号化ワードを秘匿する。

・管理者パスワード、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.SIGN（署名付与の徹底）**

・IC カードの所有者は、機密性の高い画像データを mfp からクライアント PC に送付する際、必ず署名を付加する。

**OE.SETTING-SECURITY（セキュリティ関連設定、維持、操作）**

管理者は、ユーザーに利用させる前に 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、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.DRIVER（専用プリンタドライバーの利用）**

IC カード所有者は、クライアント PC に以下の要件を満たす専用プリンタドライバーを実装する。

・文書の暗号化に用いるランダムな共通鍵の生成をサポートしている。

・IC カード内の公開鍵を用いた共通鍵の暗号化処理をサポートしている。

・SP800-67 に適合した暗号化アルゴリズム、及び鍵長をサポートしている。

## 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<br>前提<br>脅威<br>／<br>セキュリティ対策方針 | A.ADMIN | A.SERVICE | A.NETWORK | A.SECRET | A.IC-CARD | T.DISCARD-mfp | T.ACCESS-HDD | P.COMMUNICATION-CRYPTO | P.COMMUNICATION-SIGN | P.DECRYPT-PRINT |
|---|---|---|---|---|---|---|---|---|---|---|
| O.DECRYPT-PRINT | | | | | | | | | | ● |
| O.OVERWRITE-ALL | | | | | | ● | | | | |
| O.CRYPTO-HDD | | | | | | | ● | | | |
| O.MAIL-CRYPTO | | | | | | | | ● | | |
| O.MAIL-SIGN | | | | | | | | | ● | |
| O.PKI-CAPABILITY | | | | | | | | | ● | ● |
| OE.ADMIN | ● | | | | | | | | | |
| OE.SERVICE | | ● | | | | | | | | |
| OE.CARD-USER | | | | | | | | ● | | |
| OE.IC-CARD | | | | | ● | | | ● | ● | ● |
| OE.NETWORK | | | ● | | | | | | | |
| OE.SECRET | | | | ● | | | | | | |
| OE.SIGN | | | | | | | | | ● | |
| OE.SETTING-SECURITY | | | | | | ● | ● | ● | | |
| OE.DRIVER | | | | | | | | ● | | |

### 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、管理者の信頼性が充足される。

- **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不正な行為を行わないことを想定している。
  OE.SERVICE は、TOE を導入する組織は、TOE の保守を担当する組織は不正な行為を行わない旨を明記した保守契約を締結すること、及び保守作業の前に管理者がサービスエンジニア本人であることを身分証明書で確認すること、管理者が保守作業に立ち会うことを規定しており、本条件は充足される。

- **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れないことを想定している。
  OE.NETWORK は、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、本条件は充足される。

- **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、管理者が管理者パスワード、暗号化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、本条件は充足される。

- **A.IC-CARD（IC カードに関する運用条件）**
  本条件は、TOE の利用において使用される IC カードは正しく運用管理されており、IC カードの所有者は正当なユーザーであることを想定している。
  OE.IC-CARD は、信頼できる PKI 環境により発行された IC カードを用い、組織の責任者は IC カードの配付、回収を適切に行うことを規定している。また組織の責任者が IC カードのユーザーに対して期限切れや紛失時の対応方法等を周知徹底することを規定しており、利用可能な IC カードが組織の責任者が意図しない利用者に所持されることはない。よって IC カードの所有者が正当なユーザーとなるため、本条件は充足される。

### 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、ユーザーから回収された mfp より情報漏洩する可能性を想定している。
  O.OVERWRITE-ALL は、TOE が HDD にある保護資産の画像データ領域、及び NVRAM にあ

る管理者パスワード、暗号化ワードに削除用のデータを上書きする機能を提供する。また、OE.SETTING-SECURITY は、ガイダンスの記載に沿った運用として、mfp が回収される前に TOE が提供する同機能が実行されるため、脅威の可能性は除去される。
従って本脅威は十分対抗されている。

- **T.ACCESS-HDD（HDD への不正なアクセス）**
  本脅威は、mfp の HDD 内に書き込まれるすべての画像ファイルやパスワードなどのデータに対して、HDD に不正にアクセスすることによる暴露の可能性を想定している。
  O.CRYPTO-HDD は、暗号化ワードを使用して暗号鍵を生成し、すべての画像ファイルやパスワードなどのデータを HDD 内に書き込む時は暗号化し、正規に読み出す時は復号するため、脅威の可能性は軽減される。
  また、暗号化ワードに対しては品質を検証するため、脅威の可能性は軽減される。
  従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-CRYPTO（画像ファイルの暗号化通信）**
  本組織のセキュリティ方針は、ネットワーク上に流れる秘匿性の高い画像ファイル（暗号化プリントファイル、スキャン画像ファイル）について、秘匿性を確保するために、暗号化することを想定している。
  O.MAIL-CRYPTO により、mfp からユーザー自身のクライアント PC へメールにて送信されるスキャンした画像ファイルに対して、暗号化する機能を提供する。OE.CARD-USER により、mfp からクライアント PC へ送付する際は IC カード、クライアント PC から mfp に送付する際は IC カードと専用プリンタドライバーを利用することを要求する。また、その際の専用プリンタドライバーは OE.DRIVER により画像データをセキュアに保つものを利用することが要求される。さらに OE.IC-CARD によって IC カードの所有者が正当なユーザーであることを要求する。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なわれる。よって本セキュリティ方針は達成される。

- **P.COMMUNICATION-SIGN（画像ファイルの署名）**
  本組織のセキュリティ方針は、メール（S/MIME）を用いて流れる秘匿性の高い画像ファイル（スキャン画像ファイル）について、署名を付加することを想定している。
  OE.SIGN により、mfp からクライアント PC へメールにて送付されるスキャンした画像ファイルに対して必ず署名が付加される。O.MAIL-SIGN、及び O.PKI-CAPABILITY により、mfp からユーザー自身のクライアント PC へメールにて送信されるスキャンした画像ファイルに対して、IC カードを利用して署名を付加する機能を提供する。さらに OE.IC-CARD によって IC カードの所有者が正当なユーザーであることを要求する。よって本セキュリティ方針は達成される。

- **P. DECRYPT-PRINT（画像ファイルの復号）**
  本組織のセキュリティ方針は、ファイルを生成した利用者（IC カードの所有者）のみが暗号化プリントファイルに対する印刷が行えることを想定している。
  O.DECRYPT-PRINT は、TOE は、その暗号化プリントファイルを生成した IC カードのみに、その暗号化プリントファイルの印刷を許可するとしている。さらに OE.IC-CARD によって IC カードの所有者を正しく管理されることを要求する。
  暗号化プリントファイルの復号処理は外部エンティティである IC カードを利用するが、

O.PKI-CAPABILITY によってその動作がサポートされる。
従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。

# 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 2 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。

- FAD_RIP.1
  利用者データ及びTSFデータの残存情報を保護することを要求するセキュリティ機能要件である。
  - **拡張の必要性**
    利用者データ及び TSF データの残存情報保護を規定する必要があるが、残存情報保護の観点を説明するセキュリティ機能要件は、利用者データに対する FDP_RIP ファミリしか見当たらない。本要求を満たすセキュリティ機能要件は存在しない。
  - **適用したクラス（FAD）の理由**
    利用者データ及び TSF データの区別なく、双方のデータのセキュリティを説明した要件はない。よって新しいクラスを定義した。
  - **適用したファミリ（FAD_RIP）の理由**
    FDP クラスの FDP_RIP ファミリが説明する内容を利用して、TSF データまで対象を拡張したものであるため、このファミリと同一ラベルを適用した。

- FIT_CAP.1
  TOE が外部 IT 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 IT エンティティのセキュリティ機能を利用する場合、外部 IT エンティティ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 IT エンティティ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（FIT_CAP）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. FAD_RIP.1 の定義

- **クラス名**
  FAD：全データの保護
  略称の意味：FAD（Functional requirement for All Data protection）

- **クラスの概要**
  このクラスには、利用者データ、TSF データの区別なく保護すること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。

  － 全データの残存情報保護（FAD_RIP）;

- **ファミリのふるまい**
  ファミリ（FAD_RIP）は、削除された情報が二度とアクセスされず、及び別の利用者データ、TSF

データに再割当てされた場合は、リソースに含まれるいかなるデータも無効であることを保証する必要性について扱う。このファミリは、論理的に削除または解放されたが、TOE 内にまだ存在する可能性がある情報に対する保護を要求する。

- **コンポーネントのレベル付け**

| FAD_RIP　全データの残存情報保護 | 1 |
|---|---|

FAD_RIP.1：「明示的な消去操作後の全データの残存情報保護」は、TSF によって制御される定義済み利用者データ及び TSF データのサブセットが、明示的な消去操作後において、どの資源のどの残存情報内容も利用できないことを TSF が保証することを要求する。

| **管理**：FAD_RIP.1 |
|---|
| 予見される管理アクティビティはない。 |
| **監査**：FAD_RIP.1 |
| セキュリティ監査データ生成(FAU_GEN)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:<br>a) 最小: 明示的な消去操作を行う利用者識別情報を含む使用 |

| **FAD_RIP.1　　明示的な消去操作後の全データの残存情報保護** |
|---|
| **下位階層**　:　なし<br>**依存性**　:　なし |
| FAD_RIP.1.1 |
| **TSF は、以下の利用者データ及び TSF データに対する [割付: *明示的な資源の割当て解除要求*] において、資源に割り当てられた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: *利用者データ及び TSF データのリスト*]。** |

### 5.1.2. FIT_CAP.1 の定義

- **クラス名**

  FIT：外部 IT エンティティとの連携

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

- **クラスの概要**

  このクラスには、外部 IT 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。

  － 外部 IT エンティティを利用するための能力（FIT_CAP）;

- **ファミリのふるまい**

  ファミリ（FIT_CAP）は、外部 IT 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　外部 IT エンティティを利用するための能力 | 1 |
|---|---|

略称の意味：CAP（**CAP**ability of using IT entities）

FIT_CAP.1：「外部 IT エンティティのセキュリティサービス利用時の能力」は、外部 IT 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。

| **管理**：FIT_CAP.1 |
|---|
| 予見される管理アクティビティはない。 |
| **監査**：FIT_CAP.1 |
| セキュリティ監査データ生成(FAU_GEN)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:<br>a) 最小: 外部 IT エンティティに対する動作の失敗;<br>b) 基本: 外部 IT エンティティに対するすべての動作の使用（成功、失敗)。 |

| **FIT_CAP.1　外部 IT エンティティのセキュリティサービス利用時の能力** |
|---|
| **下位階層**　:　なし<br>**依存性**　:　なし |
| FIT_CAP.1.1 |
| **TSF は、[割付:*外部 IT 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以下の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*]。** |

# 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。

＜用語の定義＞

本章で使用する用語を以下に示す。

表 2　SFR で使用される用語の定義

| 用語 | 定義 |
|---|---|
| 暗号化ワード | HDD 暗号鍵生成に使用するワード。 |
| HDD 上書き消去機能 | 管理者が選択したデータ消去方法に従い、パネルから HDD の全データ領域を上書き消去する機能。 |
| NVRAM 初期化機能 | 管理者がパネルから NVRAM の管理者パスワード、暗号化ワードを初期化する機能。 |
| CE パスワード | サービスエンジニアのパスワード。 |
| CE パスワードの改変 | サービスエンジニアがパネルから CE パスワードを改変する。 |
| 管理者パスワード | 管理者のパスワード。 |
| 管理者パスワードの改変 | ・管理者がクライアント PC から管理者パスワードを改変する。<br>・サービスエンジニアがパネルから管理者パスワードを改変（初期化）する。 |
| 管理者パスワードの初期化 | 管理者がパネル、ネットワークから全データ上書き消去機能を使用して管理者パスワードを初期化する |
| 外部サーバー | 外部認証サーバー。 |
| システムオートリセット時間 | パネル操作を自動的にログアウトする時間。 |
| システムオートリセット時間の改変 | 管理者がパネルからシステムオートリセット時間を改変する。 |
| ユーザー情報管理サーバー | 外部サーバーと同義。 |
| Active Directory | Windows プラットフォームのネットワーク環境にてユーザー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。 |
| S/MIME 証明書 | E-Mail から画像ファイルを送信する時に使用する証明書。 |

| 用語 | 定義 |
|---|---|
| S/MIME 暗号処理機能 | スキャンされた画像データを E-mail において暗号化して送信する機能。 |
| 共通鍵の復号機能 | 暗号化プリントファイルを暗号化するために、共通鍵を複合する機能。 |
| メッセージダイジェスト暗号化機能 | S/MIME 機能において、スキャン画像に署名するための暗号化機能。 |

## 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*] :<br>***「表 3　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*] :<br>***「表 3　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*] :<br>***「表 3　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<br>依存性　　:　FCS_CKM.2 or FCS_COP.1（FCS_COP.1（一部事象のみ））、FCS_CKM.4（適用しない） |

表 3　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*<br>*・192 bit*<br>*・168 bit*<br>*・256 bit* |
| *FIPS180-3* | *SHA-256* | *・256bit* |

| **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*] :<br>***「表 4　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*] :<br>***「表 4　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*] :<br>***「表 4　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*] :<br>***「表 4　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 4　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*<br>*・192 bit*<br>*・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*<br>*暗号化プリントファイルの復号* |
| *FIPS 186-2* | *RSA* | *・2048 bit*<br>*・3072 bit*<br>*・4096 bit* | *S/MIME 送信データ暗号化のための共通鍵（暗号鍵）の暗号化* |
| *FIPS 180-2* | *SHA-256* | *N/A* | *メッセージダイジェストの生成* |
| *FIPS PUB 197* | *AES* | *・256 bit* | *・HDD に保管されるすべての画像ファイルやパスワードなどのデータの HDD 書き込み時の暗号化*<br>*・HDD に保管されるすべての画像ファイルやパスワードなどのデータの HDD 読み出し時の復号* |

#### 6.1.1.2. 識別と認証

| **FIA_SOS.1[1]　　秘密の検証** |
|---|
| FIA_SOS.1.1[1] |
| TSF は、秘密 ***（CE 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*]：<br>***・桁数　：12 桁以上 16 桁まで***<br>***・文字種：94 文字の中から選択可能***<br>***・規則　：(1) 1 つのキャラクターで構成されない。***<br>***(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。***<br>***※　CE パスワードは、パネル経由アクセスに適用される。*** |
| 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 ***（管理者パスワード）*** 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*]：<br>***・桁数　：12 桁以上 16 桁まで***<br>***・文字種：94 文字の中から選択可能***<br>***・規則　：(1) 1 つのキャラクターで構成されない。***<br>***(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。***<br>***※　管理者パスワードは、パネル経由アクセスに適用される。*** |
| 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*]：<br>***・桁数　：20 桁***<br>***・文字種：95 文字の中から選択可能***<br>***・規則　：(1)1 つのキャラクターで構成されない。***<br>***(2) 同一文字種のみで構成されない。*** |
| 下位階層　：　なし |
| 依存性　：　なし |

| **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）*** 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.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*]<br>***・サービスエンジニアが CE パスワードを変更する場合***<br>***・管理者が管理者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*]：<br>***入力された文字データ 1 文字毎に秘匿文字の表示*** |
| 下位階層　：　なし |
| 依存性　：　FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[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 ***（IC カード所有者の IC カード）*** 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 ***（IC カード所有者の IC カード）*** 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 |

#### 6.1.1.3. 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*]：<br>***セキュリティ強化設定、HDD 暗号化機能*** |
| [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*]：<br>***を停止する、を動作させる*** |
| [割付: *許可された識別された役割*]：<br>***・管理者*** |
| 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*]：<br>***・HDD 上書き消去機能***<br>***・NVRAM 初期化機能*** |
| [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*]：<br>***を動作させる*** |
| [割付: *許可された識別された役割*]：<br>***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[1]　　TSF データの管理** |
|---|
| FMT_MTD.1.1[1] |
| 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*] :<br>***・システムオートリセット時間***<br>***・パスワード長*** |
| [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]*] :<br>***改変*** |
| [割付:*許可された識別された役割*] :<br>***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] |
| 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*] :<br>***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]*] :<br>***改変*** |
| [割付:*許可された識別された役割*] :<br>***・管理者***<br>***・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[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*] :<br>***・CE 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]*] :<br>***改変*** |
| [割付:*許可された識別された役割*] :<br>***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_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*] :<br>***・管理者による管理者パスワードの改変機能*** |

| |
|---|
| ・管理者によるシステムオートリセット時間の改変機能<br>・管理者による HDD 上書き消去機能、NVRAM 初期化機能<br>・管理者によるセキュリティ強化機能の停止、動作機能<br>・管理者による HDD 暗号化機能の停止、動作機能<br>・管理者によるパスワード長の改変機能<br>・サービスエンジニアによる CE パスワードの改変機能<br>・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 |
| 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*]：<br>*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*]：<br>*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]） |

#### 6.1.1.4. 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*]：<br>*パネルより管理者が操作中、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 |

#### 6.1.1.5. 拡張：全データの残存情報保護

| **FAD_RIP.1　明示的な消去操作後の全データの残存情報保護** |
|---|
| 下位階層　：　なし<br>依存性　：　なし |
| FAD_RIP.1.1 |

| |
|---|
| TSF は、以下の利用者データ及び TSF データに対する [割付: *明示的な資源の割当て解除要求*] において、資源に割り当てられた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: *利用者データ及び TSF データのリスト*]。 |
| [割付: *明示的な資源の割当て解除要求*]:<br>***管理者による明示的な消去操作*** |
| [割付: *利用者データのリスト及び TSF データのリスト*]:<br>***＜利用者データ＞***<br>***・暗号化プリントファイル***<br>***・保管画像ファイル***<br>***・待機状態にあるジョブの画像ファイル***<br>***・HDD 残存画像ファイル***<br>***・画像関連ファイル***<br>***＜TSF データ＞***<br>***・管理者パスワード（初期化）***<br>***・暗号化ワード*** |

#### 6.1.1.6. 拡張：IT 環境エンティティの利用するための能力

| **FIT_CAP.1　　外部 IT エンティティのセキュリティサービス利用時の能力** |
|---|
| 下位階層　　:　なし<br>依存性　　:　なし |
| FIT_CAP.1.1 |
| TSF は、[割付:*外部 IT 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以下の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: *外部 IT エンティティが提供するセキュリティサービス*]<br>***IC カードにて実現する以下の機能***<br>***①暗号化プリントファイルを暗号化する共通鍵の復号機能***<br>***②S/MIME 機能にてスキャン画像に署名するためのメッセージダイジェスト暗号化機能***<br>***③公開鍵を利用するためのサポート機能*** |
| [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*]<br>***・上記①のための暗号化された共通鍵の送付及び暗号化された共通鍵の復号処理の依頼機能***<br>***・上記②のためのメッセージダイジェストの送付及びメッセージダイジェストの暗号化処理の依頼機能***<br>***・上記③のための公開鍵の問い合わせ機能*** |

### 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 5　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 |

| TOEセキュリティ保証要件 | | コンポーネント |
|---|---|---|
| | 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 6　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

| セキュリティ機能要件 ＼ セキュリティ対策方針 | O. DECRYPT-PRINT | O.OVERWRITE-ALL | O.CRYPTO-HDD | O.MAIL-CRYPTO | O.MAIL-SIGN | O.PKI-CAPABILITY | ※ set.admin | ※ set.service |
|---|---|---|---|---|---|---|---|---|
| ***set.admin*** | | ● | ● | ● | | | | |
| ***set.service*** | | ● | ● | ● | | | | |
| FCS_CKM.1 | | | ● | ● | | | | |
| FCS_COP.1 | ● | | ● | ● | ● | | | |
| FIA_SOS.1[1] | | | | | | | | ● |
| FIA_SOS.1[2] | | | | | | | ● | |
| FIA_SOS.1[3] | | | ● | | | | | |
| FIA_UAU.2[1] | | | | | | | | ● |
| FIA_UAU.2[2] | | | | | | | ● | |
| FIA_UAU.6 | | | | | | | ● | ● |
| FIA_UAU.7 | | | | | | | ● | ● |
| FIA_UID.2[1] | | | | | | | | ● |
| FIA_UID.2[2] | | | | | | | ● | |
| FIA_UID.2[3] | | | | | | ● | | |
| FMT_MOF.1[1] | | | ● | ● | | | ● | |
| FMT_MOF.1[2] | | ● | | | | | ● | |
| FMT_MTD.1[1] | | | | | | | ● | |
| FMT_MTD.1[2] | | | | | | | ● | |
| FMT_MTD.1[3] | | | | | | | | ● |
| FMT_SMF.1 | | ● | ● | ● | | | ● | ● |
| FMT_SMR.1[1] | | ● | ● | ● | | | ● | ● |
| FMT_SMR.1[2] | | ● | ● | ● | | | ● | |
| FTA_SSL.3 | | | | | | | ● | |
| FAD_RIP.1 | | ● | ● | | | | | |
| FIT_CAP.1 | | | | | | ● | | |

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.DECRYPT-PRINT（暗号化プリントファイルの復号）**

本セキュリティ対策方針は、暗号化プリントファイルに対する方針を説明している。
O.PKI-CAPABILITY により識別された IC カードを用いて、暗号化プリントファイルに対する印刷操作が行われると、O.PKI-CAPABILITY により IC カードから暗号化プリントファイルを復号するための正しい共通鍵（暗号鍵）が提供され、FCS_COP.1 により暗号化プリントファイルの復号処理が動作する。
よって本セキュリティ対策方針は満たされる。

- **O.OVERWRITE-ALL（全データ上書き消去）**

本セキュリティ対策方針は、HDD の全データ領域、及び利用者が設定した NVRAM 上の秘匿情報を再現できなくするとしており、再現を不可能にするための諸要件が必要である。

＜全データ上書き消去機能、及び操作制限＞
FAD_RIP.1（暗号化ワードを除く）、FMT_MOF.1[2]により、これら対象とする情報が管理者の全データ上書き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。
FMT_SMF.1 により管理者パスワード、HDD 上書き消去機能、NVRAM 初期化機能の管理を管理者に提供する。

＜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、FMT_MOF.1[2]によりそのふるまいが管理される。

＜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

よって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-HDD（HDD の暗号化）**

本セキュリティ対策方針は、HDD 内に書き込まれるすべての画像ファイルやパスワードなどのデータを保護するとしており、暗号化に関係する要件が必要である。
FCS_CKM.1 により、FIPS180-3 の SHA-256 アルゴリズムを利用し、暗号化ワードから暗号鍵（256 bit）を生成する。
なお、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。
FCS_COP.1 により、FIPS PUB 197 の AES（暗号鍵： 256 bit）を利用して HDD 内に書き込まれるすべての画像ファイルやパスワードなどのデータを暗号化する。また同要件により、HDD 内からすべての画像ファイルやパスワードなどのデータを読み出す時に復号する。
HDD 暗号化機能の停止、動作設定は、FMT_MOF.1[1]により管理者だけに許可される。動作設定の際、FIA_SOS.1[3]により、暗号化ワードの品質が検証され、停止設定の際、FAD_RIP.1（暗号化ワード）により、暗号化ワードが削除される。
FMT_SMF.1 により HDD 暗号化機能（暗号化ワード）の管理を管理者に提供する。
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。

＜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と 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、FMT_MOF.1[1]によりそのふるまいが管理される。

- **O. MAIL-CRYPTO（S/MIME の利用、暗号化）**

本セキュリティ対策方針は、mfp を利用してその場でスキャンした画像をメールにてユーザー自身に送信する際に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）を利用してスキャンした画像を暗号化する。（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）を利用してスキャンした画像を暗号化する。（これも同様に S/MIME の送信データになる。）これら共通鍵（暗号鍵）は、O.PKI-CAPABILITY により識別された IC カードを用いて、FCS_COP.1 により、各宛先の S/MIME 証明書の公開鍵（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。
FMT_MOF.1[1]によりセキュリティ強化設定を有効にすることで S/MIME の暗号化方式が 3DES、AES（左記の 2 つは選択可能）、SHA-256 に制限される。
これらの機能要件により本セキュリティ対策方針は満たされる。

＜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と 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、FMT_MOF.1[1]によりそのふるまいが管理される。

- **O. MAIL-SIGN（S/MIME の利用、署名）**

本セキュリティ対策方針は、mfp を利用してその場でスキャンした画像をメールにてユーザー自身に送信する際に署名を付加することを想定したメッセージダイジェストを生成することを規定しており、メッセージダイジェストに関する諸要件が必要である。
FCS_COP.1 により、署名処理に必要であるメッセージダイジェストを、FIPS 180-2 が規定するハッシュ関数（SHA-256）により生成する。
この機能要件により本セキュリティ対策方針は満たされる。

- **O.PKI-CAPABILITY（PKI 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 FIA_UID.2[3]により識別された IC カードにより、その場でスキャンした画像データに対する署名、及び暗号化プリントファイルを復号する共通鍵の復号等の動作を 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 により、IC カードが実現する PKI 機能に対して、スキャンした画像、及び暗号化プリントファイルを PKI 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。

- ***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 文字ごとに秘匿文字を返し、認証をサポートする。

＜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[1]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[2]により、品質が検証される。管理者パスワードの変更は、FMT_MTD.1[2]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。
また、パスワード長の変更は、FMT_MTD.1[1]により管理者に制限される。

＜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、FMT_MOF.1[1]、FMT_MOF.1[2]によりそのふるまいが管理される。

- ***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 文字ごとに秘匿文字を返し、認証をサポートする。

＜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[3]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。

＜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 7　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 |
|---|---|---|
| FCS_CKM.1 | FCS_CKM.2 or FCS_COP.1、FCS_CKM.4、 | FCS_COP.1<br>満たしている事象：擬似乱数生成アルゴリズム、SHA-256 により生成された鍵を操作すること。<br><br>＜FCS_CKM.4 を適用しない理由＞<br>スキャン画像ファイルを暗号化するための暗号鍵、及び HDD の暗号化に使用される暗号鍵は、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。 |
| 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）<br>満たしている事象：S/MIME 送信データの暗号化のための共通鍵を生成すること、及び HDD の暗号化のための暗号鍵を生成すること。<br><br>＜FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 を一部満たしていない理由＞<br>・暗号化プリントファイルの復号を行う共通鍵は FIT_CAP.1 によりインポートするため、鍵生成、外部からのインポートの必要性はない。<br>・S/MIME 送信データの暗号化のための共通鍵の暗号化を行う公開鍵は FIT_CAP.1 によりサポートされるため、鍵生成、外部からのインポートの必要性はない。<br>・メッセージダイジェストの生成に用いるメッセージは生成済みの文書データそのものであるため、鍵生成、外部からのインポートの必要性はない。<br><br>＜FCS_CKM.4 を適用しない理由＞<br>・S/MIME 送信データの暗号化、及び暗号化プリントファイルの復号に用いる鍵は、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なく、自動的に破棄されるため破棄を考慮する必要性はない。<br>・S/MIME 送信データの暗号化のための共通鍵の暗号化を行う公開鍵は公開情報であり、暗号鍵破棄の必要性はない。<br>・HDD の暗号化に使用される暗号鍵は、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。 |
| 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_UAU.2[1] | FIA_UID.1 | FIA_UID.2[1] |
| FIA_UAU.2[2] | FIA_UID.1 | FIA_UID.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_UAU.6 | なし | N/A |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.2[1]、FIA_UAU.2[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 |
| FMT_MOF.1[1] | FMT_SMF.1、FMT_SMR.1 | FMT_SMF.1、FMT_SMR.1[2] |
| FMT_MOF.1[2] | FMT_SMF.1、FMT_SMR.1 | FMT_SMF.1、FMT_SMR.1[2] |
| 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[1]、FMT_SMR.1[2] |
| FMT_MTD.1[3] | FMT_SMF.1、FMT_SMR.1 | FMT_SMF.1 FMT_SMR.1[1] |
| FMT_SMF.1 | 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] |
| FTA_SSL.3 | なし | N/A |
| FAD_RIP.1 | なし | N/A |
| FIT_CAP.1 | 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 8 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 8 TOE のセキュリティ機能名称と識別子の一覧

| 節番号 | TOE のセキュリティ機能 | TOE 論理的範囲との関係 |
|---|---|---|
| 7.1 | F.ADMIN（管理者機能） | 管理者機能 |
| 7.2 | F.SERVICE（サービスモード機能） | サービスエンジニア機能 |
| 7.3 | F.CARD-ID（IC カード識別機能） | 基本機能 |
| 7.4 | F.PRINT（暗号化プリント機能） | 基本機能 |
| 7.5 | F.OVERWRITE-ALL(全データ上書き消去機能) | 管理者機能 |
| 7.6 | F.S/MIME（S/MIME 暗号処理機能） | 基本機能 |
| 7.7 | F.SUPPORT-PKI（PKI サポート機能） | その他の機能 |
| 7.8 | F.CRYPTO-HDD（HDD 暗号化機能） | 基本機能 |

## 7.1. F.ADMIN（管理者機能）

F.ADMIN とは、パネル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。

### 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 9 に示されるキャラクター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。
- 管理者パスワード入力のフィードバックに 1 文字毎秘匿文字を返す。

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

### 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システムオートリセッ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。

表 9 パスワードに利用されるキャラクターと桁数 [2]

| 対象 | 桁数 | キャラクター |
|---|---|---|
| ・管理者パスワード<br>・CE パスワード | 12 以上 16 桁まで | 最低合計 94 文字の中から選択可能<br>（英、数、記号）<br>ASCII コード：0x20～0x7e |

[2] 表 9 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ーが示されているが、除外キャラクターが利用可能なケースは許容される。

| | | |
|---|---|---|
| | | 0x22（”）は選択できない。 |

### 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。
以上により、FMT_SMR.1[2]が実現される。

#### 7.1.3.1. 管理者パスワードの変更

パネルより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 9 に示されるキャラクターからなる管理者パスワードにより再認証する管理者認証メカニズムを提供する。
- 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 文字毎秘匿文字を返す。
- 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 9 の管理者パスワードに示される桁数、キャラクターから構成される。
  - 1 つのキャラクターで構成されない。
  - 現在設定される値と一致しない。

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

#### 7.1.3.2. 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[1]、FMT_SMF.1 が実現される。

#### 7.1.3.3. セキュリティ強化機能、HDD 暗号化機能に関連する機能

＜セキュリティ強化機能＞
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。

- セキュリティ強化機能の動作設定
  パネルを介して、セキュリティ強化機能の有効、無効を設定する機能。
- HDD 論理フォーマット機能
  パネルを介して、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。
- 全データ上書き消去機能
  パネルを介した、全データ上書き消去の実行により、セキュリティ強化機能の設定を無効にする。

この機能は、管理者のみに許可する。
上述の機能により、管理機能であるセキュリティ強化機能の管理機能を提供する。

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

＜HDD 暗号化機能＞
管理者が操作する HDD 暗号化機能の設定は以下の通り。

- HDD 暗号化機能の動作設定
  パネルを介して、暗号化ワードの品質検証と動作を設定する機能、及び暗号化ワードの削除と動作の停止設定する機能。

＜暗号化ワードの品質＞
暗号化ワードの品質尺度は、以下の通りである。

**表 10　暗号化ワードに利用されるキャラクターと桁数**

| 対象 | 桁数 | キャラクター |
|---|---|---|
| 暗号化ワード | 20 桁 | 最低合計 95 文字の中から選択可能<br>（英、数、記号）<br>ASCII コード：0x20～0x7e |

- **表 10** の暗号化ワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。
- 同一文字種のみで構成されない。

暗号化ワードは、登録する時その品質が検証される。
この機能は、管理者のみに許可する。
上述の機能により、管理機能である HDD 暗号化機能の管理機能を提供する。

以上により FIA_SOS.1[3]、FMT_MOF.1[1]、FMT_SMF.1、FAD_RIP.1（暗号化ワード）が実現される。

#### 7.1.3.4. パスワード長の設定

管理者パスワード及び CE パスワードに使用される最小のパスワード長を以下に示す長さの範囲で設定する。

- パスワード長　　：12 桁以上 16 桁まで

現在設定されている管理者パスワード、及び CE パスワードの長さを長くしたい場合は、各パスワードを長くした後、パスワード長の設定を行う。
以上により FMT_MTD.1[1]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

#### 7.1.3.5. 全データ上書き消去機能の管理

全データ上書き消去機能の実行は、パネルを介して管理者のみに制限する。
全データ上書き消去機能の実行によって、消去、初期化されるデータは、「7.5」に記載される。
上述の機能により、管理機能である HDD 上書き消去機能の管理機能、NVRAM 初期化機能の管理機能、管理者パスワードの管理機能を提供する。

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

## 7.2. 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。

### 7.2.1. 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 9 に示されるキャラクターからなる 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。
- CE パスワード入力のフィードバックに 1 文字毎秘匿文字を返す。

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

### 7.2.2. 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、利用者を代行するタスクにサービスエンジニア属性が関連づけられ、以下の機能の利用が許可される。

以上により、FMT_SMR.1[1]が実現される。

#### 7.2.2.1. 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 9 に示されるキャラクターからなる 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。
- 再認証では、CE パスワード入力のフィードバックに 1 文字毎秘匿文字を返す。
- 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 9 の CE パスワードに示される桁数、キャラクターから構成される。
  - 1 つのキャラクターで構成されない。
  - 現在設定される値と一致しない。

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

#### 7.2.2.2. 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 9 の管理者パスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。
- 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[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

### 7.3. F.CARD-ID（IC カード識別機能）

F.CARD-ID とは、暗号化プリント機能、及び Scan To Me 機能を利用する前に mfp に接続されている IC カードを mfp が識別する機能である。

以上により FIA_UID.2[3]が実現される。

### 7.4. F.PRINT（暗号化プリント機能）

F.PRINT とは、暗号化プリント機能におけるセキュリティ機能である。印刷操作に対して、F.SUPPORT-PKI により入手した共通鍵（暗号鍵）により復号処理が動作する。

- 暗号化プリントファイルを復号するための共通鍵（暗号鍵）（168 bit）は、FIPS186-2 で規定される RSA によって復号される。

以上により FCS_COP.1 が実現される。

### 7.5. F.OVERWRITE-ALL（全データ上書き消去機能）

F.OVERWRITE-ALL とは、管理者の明示的な消去操作により、HDD の全データ領域に上書き消去を実行すると共に NVRAM に設定されているパスワード等の設定値を初期化する。消去または初期化するべき対象は以下の通りである。

＜消去される対象：HDD＞

- 暗号化プリントファイル
- 待機状態にあるジョブの画像ファイル
- 保管画像ファイル
- HDD 残存画像ファイル
- 画像関連ファイル

＜初期化される対象：NVRAM＞

- 管理者パスワード

HDD に書き込むデータ、書き込む回数など消去方式は、F.ADMIN において設定される全データ上書き消去機能の消去方式（**表 11**）に応じて実行される。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)

この機能は、管理者のみに許可する。

以上により FAD_RIP.1（暗号化ワードを除く）が実現される。

**表 11　全データの上書き消去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 |
| Mode:5 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF |
| Mode:6 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数 |

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

### 7.6. F.S/MIME（S/MIME 暗号処理機能）

F.S/MIME とは、(その場で) スキャンした画像を S/MIME でユーザー自身に送信する際に、スキャンした画像を暗号化、及び署名する機能である。署名生成は F.SUPPORT-PKI により IC カードが行うが、本機能において署名に用いるメッセージダイジェストを生成する。

＜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、スキャンした画像を暗号化するための共通鍵（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。

＜スキャン画像の暗号化＞

- スキャンした画像は、共通鍵（暗号鍵）(128 bit、192 bit、256 bit）を用いて、FIPS PUB 197 によって規定される AES によって暗号化される。
- スキャンした画像は、共通鍵（暗号鍵）(168 bit）を用いて、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。

＜暗号鍵の暗号化＞

- スキャンした画像を暗号化するための共通鍵 (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 F.SUPPORT-PKI により利用される公開鍵の鍵長は、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。

＜メッセージダイジェスト生成＞

- スキャンした画像は、FIPS 180-2 が規定するハッシュ関数（SHA-256）により、メッセージダイジェストが生成される。
  以上により FCS_COP.1 が実現される。

### 7.7. F.SUPPORT-PKI（PKI サポート機能）

F.SUPPORT-PKI とは、TOE から F.CARD-ID により識別された IC カードを動作させるための機能である。

＜復号処理依頼＞

- 暗号化された共通鍵（暗号鍵）を IC カードに送付し、IC カードにて共通鍵（暗号鍵）の復号処理を行せ、正しく復号した共通鍵（暗号鍵）を受け取る。

＜署名処理依頼＞

- F.S/MIME により生成したメッセージダイジェスト（メッセージのハッシュ値）を IC カードに送付し、署名処理を行わせ、メッセージダイジェストに対する正しい署名を受け取る。

<公開鍵取得依頼>

- IC カードに問い合わせを行い、IC カード内の公開鍵（デジタル証明書）を受け取る。

以上により、FIT_CAP.1 が実現される。

## 7.8. F.CRYPTO-HDD（HDD 暗号化機能）

F.CRYPTO-HDD とは、mfp の HDD 内に画像ファイルやパスワードなどのデータを書き込む時に暗号化するための機能である。

＜HDD 暗号化の暗号鍵生成＞

- 暗号化ワードを使用して、FIPS180-3 によって規定される SHA-256 アルゴリズムを使用し、HDD に書き込まれるすべての画像ファイルやパスワードなどのデータを暗号化、復号するための 256bit 長の暗号鍵を生成する。
  暗号鍵は、mfp の電源を ON にした時、生成される。
  以上により FCS_CKM.1 が実現される。

＜HDD の暗号化、復号＞

- HDD に書き込まれるすべての画像ファイルやパスワードなどのデータを暗号化するための暗号鍵（256 bit）により、FIPS PUB 197 によって規定される AES によって、そのデータを HDD に書き込む時に暗号化される。
- HDD から読み出されるすべての画像ファイルやパスワードなどのデータを復号するための暗号鍵（256 bit）により、FIPS PUB 197 によって規定される AES によって、そのデータを HDD から読み出す時復号される。
  以上により FCS_COP.1 が実現される。

---以上---