bizhub 501 / bizhub 421 / bizhub 361
PKI Card System Control Software
A0R50Y0-0100-GR0-20
A0R50Y0-1D00-G00-11

セキュリティターゲット

バージョン：1.06

発行日：2009年8月6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
2009/1/27	1.00	制御第11開発部	山崎	角谷	小田	初版
2009/3/12	1.01	制御第11開発部	山崎	角谷	小田	A.SETTINGへの内容修正 FMT_MOF.1[2]、FMT_MOF.1[3]の内容修正 FMT_MOF.1[4]の追加 完全上書き削除機能の修正 その他誤植修正
2009/6/3	1.02	第１電子情報技術開発部	飯塚	角谷	小田	組織変更に伴い更新履歴の部署名と承認者を変更 FIA_SOS.1[2]の追加に伴う修正 FIA_UID.2[3]、F.CARD-IDの追加に伴う修正 その他誤植修正
2009/6/26	1.03	第１電子情報技術開発部	飯塚	角谷	小田	A.SETTING、OE.SETTING-SECURITYの内容修正 認証失敗回数の記述修正 FMT_MTD.1[4]、FMT_MOF.1［2］、FMT_SMF.1の内容修正 その他誤植修正
2009/7/3	1.04	第１電子情報技術開発部	飯塚	角谷	小田	T.BRING-OUT-CFの内容修正 その他誤植修正
2009/7/8	1.05	第１電子情報技術開発部	飯塚	角谷	小田	主要なセキュリティ機能の記述追記 1.4.2.2. 動作環境の記述修正 その他誤植修正
2009/8/6	1.06	第１電子情報技術開発部	飯塚	角谷	小田	管理者パスワードの入力可能桁数の表記修正 その他誤植修正

—【 目次 】

—【 図目次 】

—【 表目次 】

1. ST 概説

1.1. ST 参照

・ST名称 : bizhub 501 / bizhub 421 / bizhub 361 PKI Card System Control Software
A0R50Y0-0100-GR0-20 A0R50Y0-1D00-G00-11セキュリティターゲット
・STバージョン : 1.06
・作成日 : 2009年8月6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 小田 昭彦

1.2. TOE 参照

・TOE名称 : bizhub 501 / bizhub 421 / bizhub 361 PKI Card System Control Software
・TOE識別 : A0R50Y0-0100-GR0-20 （システム制御部）
A0R50Y0-1D00-G00-11 （BIOS制御部）
・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 501 / bizhub 421 / bizhub 361 PKI Card System Control Software とは、MFP 制御コントローラ上のコンパクトフラッシュメモリ及びフラッシュメモリにあって、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 501 / bizhub 421 / bizhub 361 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 501 / bizhub 421 / bizhub 361 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で、かつ、クライアント PC から MFP へ送信されるプリントデータのうち専用のプリンタドライバ及び IC カードを利用して暗号化プリントファイルとして生成されたものを、専用ドライバ（ローダブルドライバ）及び生成する際に利用した IC カードを使い MFP において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を、ローダブルドライバ及び IC カードを利用して S/MIME により保護する機能を提供する。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。

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、あるいは、すりかえられる等の危険性に対して、HDD に搭載される HDD ロック機能、及び HDD 検証機能を活用すること、CF が不正に持ち出されすりかえられて不正な TOE で動作させられることにより機密情報が漏洩する危険性に対して CF に搭載される CF ロック機能、及び CF 検証機能を活用すること、さらに

は、オプションで提供される暗号化キットを利用し、HDD に書き込まれる画像データを暗号化することにより、機密情報が漏洩することを防止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を有し、HDD のすべてのデータを完全に削除し、MFP を廃棄・リース返却する際に利用することによって 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**
  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。

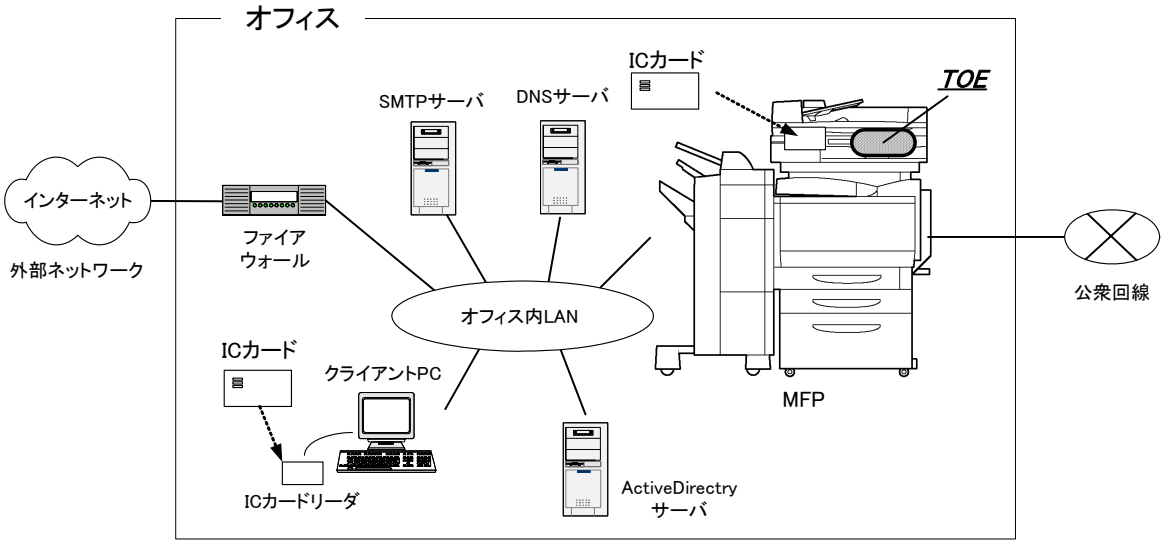


図 1　MFP の利用環境の例

- 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。
- クライアント PC の IC カード、及び IC カードリーダは、専用プリンタドライバを利用した 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 ActiveDirectory サーバが接続され、IC カードの認証に利用される。
- オフィス内 LAN には SMTP サーバが接続され、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われる。
- MFP に接続される公衆回線は、FAX や遠隔サポート機能の通信に利用される。

1.4.2.2. 動作環境

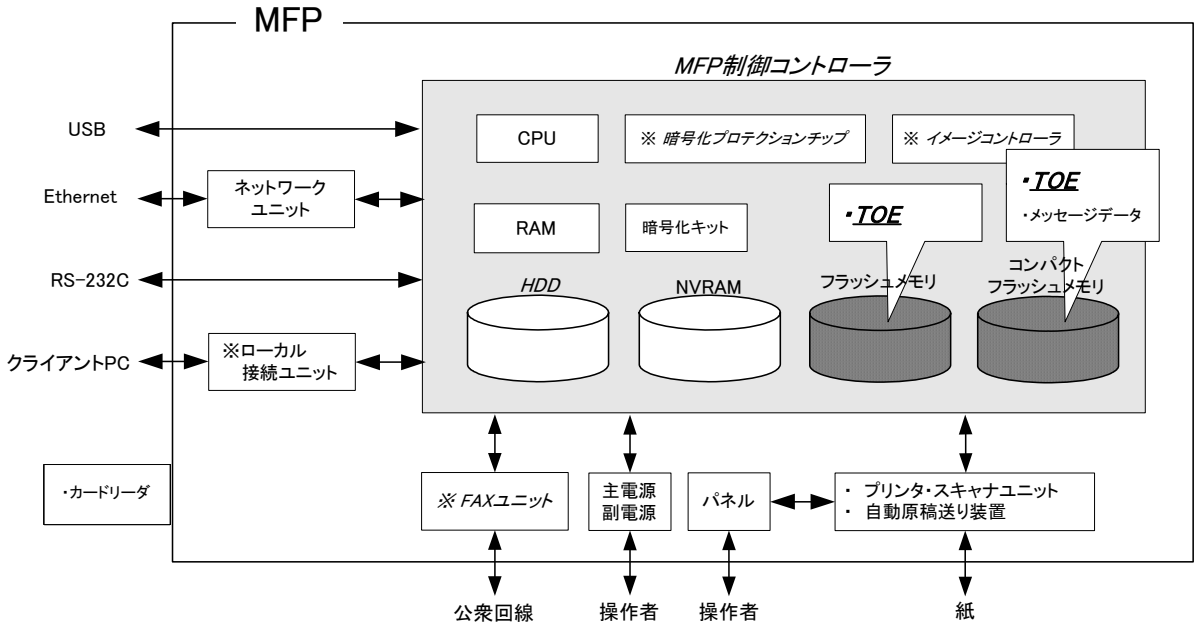


図 2 TOE に関係するハードウェア構成

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 TOE に関係するハードウェア構成 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コンパクトフラッシュメモリにシステム制御部、フラッシュメモリに BIOS 制御部が存在し、主電源が ON になると RAM にロードされ動作する。

以下には 図 2 TOE に関係するハードウェア構成 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ーフェースを持つハードウェア、及び RS-232C を用いた接続について説明する。

- **コンパクトフラッシュメモリ（以降、CF と略称を利用）**

  TOE である MFP PKI Card System Control Software におけるシステム制御部のオブジェクトコードが保管される記憶媒体。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などで表示するための各国言語メッセージデータも保管される。

  また 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。セキュリティ上関連するデータとしては、各種設定値がこれにふくまれるが、管理者パスワード、CE パスワード、HDD ロックパスワード、暗号化ワード、CF ロックパスワードは含まれない。

  特徴的な機能として、パスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（CF ロック機能）が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。

- **フラッシュメモリ**

  TOE である MFP PKI Card System Control Software における BIOS 制御部のオブジェクトコードが保管される記憶媒体。

- HDD

  容量 60GB 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管されるほか、伸張変換などで一時的に画像データが保管される領域としても利用される。また、IC カードにアクセスするための専用ドライバもここに保存される。

特徴的な機能として、パスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（HDD ロック機能）が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。

- 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管される記憶媒体。

- **暗号化キット、暗号化プロテクションチップ（※オプション）**
  HDD に書き込まれる画像データを暗号化するための暗号化機能が MFP 制御コントローラ上のハードウェアである暗号化キットに実装されている。暗号化機能を動作させるためにはオプション購入の暗号化プロテクションチップが必要。

- **イメージコントローラ（※オプションパーツ）**
  MFP 制御コントローラとビデオバスで接続される画像変換処理のためのコントローラ。販売上の都合により MFP には標準搭載されず、オプションパーツであるが、本 ST の想定では必須の構成部品である。

- **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。

- **主電源、副電源**
  MFP を動作させるための電源スイッチ。

- **ネットワークユニット**
  Ethernet 接続インタフェースデバイス。10BASE-T、100BASE-TX、Gigabit Ethernet をサポート。

- **ローカル接続ユニット（※オプション）**
  クライアント PC と USB を使って接続するためのデバイス。プリント機能に利用される。

- USB
  ローカル接続でプリントするために利用される他には、IC カードに対応したカードリーダを接続するために使用する。カードリーダは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（※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。

- **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。

- RS-232C
  シリアル接続することが可能。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。

- 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。

1.4.2.3. ガイダンス

- bizhub 501/421/361 for PKI Card System SERVICE MANUAL　SECURITY FUNCTION
- bizhub 501/421/361 for PKI Card System User's Guide [Security Operations]

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 に登録する。（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。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。

以下は基本機能で提供されるセキュリティ機能である。

- 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管する。
  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 カード所有者が以下の機能を利用して、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。

  - S/MIME 暗号化機能
    ユーザ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
  - 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
- HDD の完全上書き削除機能
  - 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。
- HDD ロック機能の設定
  - 動作、停止を選択
  - 動作選択時には、HDD ロックパスワード登録・変更
- CF ロック機能の設定
  - 動作、停止を選択
  - 動作選択時には、CF ロックパスワード登録・変更
- 暗号化機能の設定（※暗号化プロテクションチップを装着時のみ）
  - 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
- S/MIME 処理に適用される暗号方式の設定
- S/MIME 処理に適用される署名に用いるメッセージダイジェスト方式の設定
- S/MIME 処理に適用される署名付与設定
- 認証操作禁止設定
  - 各種パスワードを入力した際に認証機能の強度を高める機能
  - パスワード誤入力時に５秒間の認証停止、一定回数以上の失敗時に認証禁止する
  - 上記の動作タイプの設定が行える

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 ロック機能の設定、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。

- CE[1]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
  - 物理フォーマットが実行可能。
- 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、ユーザが保管したデータを削除する。

1.4.3.4. 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。

① **暗号鍵生成機能**

オプション製品である暗号化プロテクションチップが MFP 制御コントローラに設置されている場合に、暗号化キットにて HDD の画像データ書き込み、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。

② **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 等の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。

③ **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）、USB メモリ等のメモリ媒体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 HDD、CF、暗号化キット、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。

- **HDD ロック機能の活用**

  外部エンティティである HDD は、不正な持ち出し等への対処機能として、パスワードを設定した場合に HDD ロック機能が動作する。

[1] Customer service Engineer の略称。

- **CF ロック機能の活用**
  外部エンティティである CF は、不正な持ち出し等への対処機能として、パスワードを設定した場合に CF ロック機能が動作する。

- **暗号化キットの活用**
  外部エンティティである暗号化キットは、不正な持ち出し等への対処機能として、オプションの暗号化プロテクションチップを購入しパスワードを設定した場合に、HDD に書き込まれる画像ファイルに対して暗号化処理機能が動作する。

- **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。

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

- 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 September 2006 Version 3.1 Revision 1 CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components September 2007 Version 3.1 Revision 2 CCMB-2007-09-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components September 2007 Version 3.1 Revision 2 CCMB-2007-09-003
- Common Criteria for Information Technology Security Evaluation Evaluation methodology September 2007 Version 3.1 Revision 2 CCMB-2007-09-004

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 に蓄積された暗号化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管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管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管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。

- **暗号化プリントファイル**
- **スキャン画像ファイル**
- **オンメモリ画像ファイル**
  - 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**
  - 暗号化プリントファイル以外の保管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**
  - 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 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、正当なユーザに所有されている。

A.SETTING（セキュリティに関する動作設定条件）
・管理者のパスワードを連続で一定回数間違った場合に管理者認証操作を禁止する。
・遠隔診断機能を利用不可とする。
・インターネット経由 TOE 更新機能を利用不可とする。
・メンテナンス機能を利用不可とする。
・HDD ロック機能の設定を有効にする。
・CF ロック機能の設定を有効にする。
・暗号化機能を利用する場合は、暗号化機能の設定を有効にする。
・サービスエンジニアのログイン認証を有効とする。
・パネル以外からの管理者機能による設定を不可とする。

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、NVRAM 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、オンメモリ画像ファイル、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、設定されていた各種パスワード等の秘匿情報が漏洩する。

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、暗号化プリントファイル、スキャン画像ファイル、オンメモリ画像ファイル、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、設定されていた各種パスワード等が漏洩する。

・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 には新たに暗号化プリントファイル､スキャン画像ファイル､オンメモリ画像ファイル、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、設定されていた各種パスワード等が蓄積され､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.BRING-OUT-CF（コンパクトフラッシュメモリの不正な持ち出し）

悪意を持った者や悪意を持ったユーザが、MFP 内のコンパクトフラッシュメモリを不正に持ち出し、内容が書き換えられる、あるいは、コンパクトフラッシュがすりかえられることにより、異なるシステム制御部のオブジェクトコード等の不正な TOE で動作させられ、暗号化プリントファイル等の保護資産が漏洩する。

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、署名を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（完全上書き削除）
TOE は、MFP 内の HDD のすべての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。また管理者が設定した秘匿性のある NVRAM 上のパスワード（管理者パスワード、HDD ロックパスワード、CF ロックパスワード、暗号化ワード）設定値を初期化する機能を提供する。

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暗号化して保存するための暗号鍵を生成する。

O.CHECK-HDD（HDD の正当性確認）
TOE は、正しい HDD が設置されていることを検証する。

O.CHECK-CF（CF の正当性確認）
TOE は、正しい CF が設置されていることを検証する。

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.CRYPTO-CAPABILITY（暗号化機能を利用するためのサポート動作）
TOE は、暗号化キットによる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.LOCK-HDD-CAPABILITY（HDD ロック機能を利用するためのサポート動作）
TOE は、HDD による HDD ロック機能を利用するために必要な動作をサポートする。

O.LOCK-CF-CAPABILITY（CF ロック機能を利用するためのサポート動作）
TOE は、CF による CF ロック機能を利用するために必要な動作をサポートする。

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

TOE は、カードリーダ及び IC カードと連携して実現される暗号化プリントファイル機能、Scan To Me 機能を利用するために、ActiveDirectory を利用してカードリーダ及び 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）

・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.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、及び専用ドライバを利用し、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、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利用者へ配付する。
・MFP を利用する組織の責任者は、利用者に対して 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。
・管理者パスワードに 8 桁以上の値を設定する。
・管理者パスワード、HDD ロックパスワード、CF ロックパスワード、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、HDD ロックパスワード、CF ロックパスワード、暗号化ワードを秘匿する。
・管理者パスワード、HDD ロックパスワード、CF ロックパスワード、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。
・管理者パスワードを変更する場合、8 桁以上の値を設定する。
・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。
・管理者は、デジタル署名付与方法設定を、強制的もしくは任意に署名を付加する設定にする。

OE.SETTING-SECURITY（セキュリティに関する動作設定）

・管理者は、認証操作禁止機能の設定を「有効」（認証操作禁止）にする。
・サービスエンジニアは、遠隔診断機能を「禁止」にする。
・サービスエンジニアは、インターネット経由 TOE 更新機能を「禁止」にする。
・サービスエンジニアは、メンテナンス機能を「禁止」にする。
・管理者は、HDD ロック機能を「有効」にする。
・管理者は、CF ロック機能を「有効」にする。
・暗号化機能を利用する場合、管理者が暗号化機能を「有効」にする。[2]
・サービスエンジニアは、サービスエンジニア認証機能を「有効」にする。
・管理者は、ネットワーク経由の管理者機能による設定を「禁止」にする。

OE.DRIVER（専用ドライバの利用）

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ドライバを実装する。
・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。

[2] 暗号化機能の利用にはオプションの暗号化プロテクションチップの購入（サービスエンジニアによる MFP への装着）が必要。

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	A.IC-CARD	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.BRING-OUT-CF	P.COMMUNICATION-CRYPTO	P.COMMUNICATION-SIGN	P.DECRYPT-PRINT
O.DECRYPT-PRINT												●
O.OVERWRITE-ALL							●					
O.CRYPTO-KEY								●				
O.CHECK-HDD								●				
O.CHECK-CF									●			
O.MAIL-CRYPTO										●		
O.MAIL-SIGN											●	
O.CRYPTO-CAPABILITY								●				
O.LOCK-HDD-CAPABILITY								●				
O.LOCK-CF-CAPABILITY									●			
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、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、管理者が管理者パスワード、暗号化ワード、HDD ロックパスワード、CF ロック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。

- **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となるため、本条件は実現される。

A.SETTING（セキュリティに関する動作設定条件）

本条件は、セキュリティに関する動作設定条件を満たす以下の設定が TOE に対して行われていることを想定している。

・管理者に対するパスワードロックの有効化。
・サービスエンジニアの遠隔診断の禁止。
・サービスエンジニアのインターネット経由 TOE 更新の禁止。
・サービスエンジニアのメンテナンス機能の禁止。
・管理者による HDD ロック機能の有効化。
・管理者による CF ロック機能の有効化。
・暗号化機能を利用する場合の、管理者による暗号化機能の有効化。
・サービスエンジニア認証機能の有効化。
・ネットワーク経由の管理者機能による設定機能の禁止。

OE.SETTING-SECURITY は、上記全ての項目に対して上記の通りの設定を実施す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-ALL は、TOE が HDD の全領域に削除用のデータを上書きする機能を提供し、NVRAM の情報を初期化するとしており、MFP が回収される前にこの機能を実行することによって、脅威の可能性は除去される。
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.LOCK-HDD-CAPABILITYによりHDDロック機能を利用するための動作がサポートされ、HDD ロック機能が動作することによって脅威の可能性は軽減される。また暗号化プロテクションチップを装着している場合、O.CRYPTO-KEY は、TOE が HDD に書き込まれる画像データを暗号化するための暗号鍵を生成し、O.CRYPTO－CAPABILITY により暗号化プロテクテクションチップでの暗号化機能を利用するための動作がサポートされるため、脅威の可能性は軽減される。
HDD がすりかえられて、HDD ロック機能をもたない HDD が設置されることにより、持ち出されて漏洩する危険性が存在するが、O.CHECK-HDD により、TOE によって設置されている HDD の正当性が検証されるため、すりかえられた HDD にはデータを書き込むことはない。したがって脅威の可能性は除去される。
したがって本脅威は十分対抗されている。

- **T.BRING-OUT-CF（コンパクトフラッシュメモリの不正な持ち出し）**

本脅威はコンパクトフラッシュメモリが持ち出され、異なる TOE 及び情報に書き換えられて設置されることによって不正な操作が行われる可能性を想定している。
O.LOCK-CF-CAPABILITY により CF ロック機能を利用するための動作がサポートされ、CF ロック機能が動作することによって脅威の可能性は軽減される。
CF がすりかえられて、CF ロック機能を有さない、もしくは CF ロック機能を動作させない CF が設置されることにより、セキュリティに関連する設定値が脆弱な状態で動作する危険性が存在する。これに対しては、O.CHECK-CF により、TOE によって設置されている CF の正当性が検証されるため、すりかえられた CF で動作することはない。したがって脅威の可能性は除去される。
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-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 カードと専用ドライバを利用することを要求する。また、その際の専用ドライバは 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.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 カードの所有者が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。
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。

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。

- 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**

    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.1 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（RIP）の理由**

    FDP クラスの当該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。

- FIA_EID.1

  TOE から外部エンティティへアクセスする際の条件を規定するセキュリティ機能要件である。

  - **拡張の必要性**

    TOE が外部エンティティからアクセスされる行為を承認するのではなく、TOE 自らが外部エンティティに対して発動する行為への承認であり、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（FIA）の理由**

    外部エンティティを識別することを規定しているため、識別認証の各種セキュリティ機能要件をまとめる FIA クラスが最適である。
  - **適用したファミリ（EID）の理由**

    本要求内容は、既存ファミリに対して内容を拡張したものには該当しないと判断される。よって新しいファミリを定義した。

- 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. 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。

  － 全データ残存情報保護（FAD_RIP）;

- **ファミリのふるまい**

  このファミリは、削除された情報が二度とアクセスされず、及び新しく作成したオブジェクト、TSF データがアクセス可能にするべきではない情報を含まないようにする必要性に対応する。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オブジェクトのサブセットが、資源の割当てあるいは割当て解除において、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。

監査：FAD_RIP.1
明示的な消去操作を行う利用者識別情報を含む使用
管理：FAD_RIP.1
予見される管理アクティビティはない。

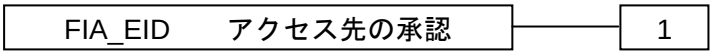
FAD_RIP.1　　明示的な消去操作後の全データの残存情報保護
FAD_RIP.1.1
TSF は、以下のオブジェクト及び TSF データに対する明示的な消去操作において、資源に割り当てられた以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト及び TSF データのリスト*]。
下位階層　：　なし **依存性**　：　なし

5.1.2. FIA_EID.1 の定義

- **ファミリのふるまい**

  このファミリは、TOE 外の IT 環境エンティティがセキュリティ機能を提供する場合、IT 環境エンティティが不正にすりかえられていないことを確認する必要性に対応する。
  このファミリは IT 環境エンティティの正当性の検証を要求する。

- **コンポーネントのレベル付け**



略称の意味：EID（**E**xternal entity **ID**entification）

FIA_EID.1：「TOE からのアクセス対象となる IT 環境エンティティの識別」は、IT 環境エンティティに対してアクションを発動する前に IT 環境エンティティの正当性検証（ここでは識別）に成功することを要求する。

監査：FIA_EID.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　提供される IT 環境エンティティ識別情報を含む、IT 環境エンティティ識別メカニズムの不成功使用 b) 基本　提供される IT 環境エンティティ識別情報を含む、IT 環境エンティティ識別メカニズムのすべての使用
管理：FIA_EID.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。 a)　IT 環境エンティティ識別情報の管理

FIA_EID.1　　TOE からのアクセス対象となる IT 環境エンティティの識別
FIA_EID.1.1
TSF は、TOE から IT 環境エンティティに対してアクションする前に、その IT 環境エンティティの識別に成功することを要求しなければならない。
FIA_EID.1.2
TSF は、IT 環境エンティティの識別に失敗した場合、TOE から IT 環境エンティティに対するアクションの起動を停止しなければならない。
下位階層　：　なし
依存性　：　なし

5.1.3. 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（一部事象のみ））、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（SHA256）*	*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* *暗号化プリントファイルの復号*
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共通鍵（暗号鍵）の暗号化*
FIPS 180-2	*SHA-1*	*N/A*	*メッセージダイジェストの生成*
FIPS 180-2	*SHA-256*	*N/A*	*メッセージダイジェストの生成*

6.1.1.2. 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]：1～5 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に[選択: *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: *達する、を上回った*]: **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＞*** ***・認証状態であれば、サービスモードへの認証状態からログオフし、CE パスワードを利用する認証機能をロックする。*** ***・認証状態でなければ、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 認証ロック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]：1～5 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に[選択: *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: *達する、を上回った*]: **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＞*** ***・認証状態であれば、管理者モードへの認証状態からログオフし、管理者パスワードを利用する認証機能をロックする。*** ***・認証状態でなければ、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＞*** ***・サービスモード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。（起動処理から管理者認証ロック時間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*]: ***・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***
[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[3]
不成功の認証試行が定義した回数に[選択: *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: *達する、を上回った*]: **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_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*]： ***・桁数　：8 桁*** ***・文字種：92 文字以上の中から選択可能***	
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*]： ***文字種：92 文字以上の中から選択可能***	
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 ***（HDD ロックパスワード、CF ロックパスワード、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 同種の文字列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_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*]

- ***管理者が管理者パスワードを改変する場合***
- ***サービスエンジニアが CE パスワードを改変する場合***
- ***管理者が HDD ロックの設定を変更する場合***
- ***管理者が暗号化機能の設定を変更する場合***
- ***管理者が CF ロックの設定を変更する場合***

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_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*] : ***・遠隔診断機能*** ***・インターネット経由 TOE 更新機能*** ***・メンテナンス機能*** ***・HDD のフォーマット機能（物理フォーマット）*** ***・イニシャライズ機能***
[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*] : ***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_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*] : ***・完全上書き削除機能*** ***・ネットワーク経由の管理機能*** ***・HDD のフォーマット機能（論理フォーマット）***
[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*] : ***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[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*] : ***・デジタル署名付与*** ***・認証操作禁止*** ***・HDD ロック機能*** ***・CF ロック機能*** ***・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*] : ***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*]: ***サービスエンジニア認証機能***
[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*]: ***を停止する***
[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[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*]: ***・パネルオートログオフ時間*** ***・認証失敗回数閾値*** ***・S/MIME 暗号化強度（暗号アルゴリズム）*** ***・S/MIME メッセージダイジェスト方式*** ***・管理者認証ロック時間*** ***・HDD ロックパスワード*** ***・CF ロックパスワード*** ***・暗号化ワード***
[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***
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*]: ***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[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*]: ***・CE パスワード*** ***・CE 認証ロック時間***
[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[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*]: ***・暗号化ワード***
[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_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*]: ***・管理者による管理者パスワードの改変機能*** ***・管理者による管理者認証ロック時間の改変機能*** ***・管理者によるパネルオートログオフ時間の改変機能*** ***・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改変機能*** ***・管理者による S/MIME 暗号化強度（暗号アルゴリズム）の改変機能*** ***・管理者による S/MIME メッセージダイジェスト方式の改変機能*** ***・管理者による暗号化ワードの登録機能*** ***・管理者による暗号化ワードの改変機能*** ***・管理者による HDD ロックパスワードの改変機能*** ***・管理者による CF ロックパスワードの改変機能*** ***・管理者による全領域上書き削除機能*** ***・管理者によるデジタル署名付与機能*** ***・管理者による認証操作禁止機能*** ***・管理者による暗号化設定機能*** ***・管理者によるネットワーク経由の管理機能*** ***・管理者による HDD のフォーマット機能（論理フォーマット）*** ***・サービスエンジニアによるサービスエンジニア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 CE 認証ロック時間の改変機能*** ***・サービスエンジニアによるサービスエンジニア認証設定機能*** ***・サービスエンジニアによる遠隔診断機能*** ***・サービスエンジニアによるインターネット経由 TOE 更新機能*** ***・サービスエンジニアによるメンテナンス機能***

・サービスエンジニアによる HDD のフォーマット機能（物理フォーマット） *・サービスエンジニアによるイニシャライズ機能*
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]）

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*]: ***パネルより管理者が操作中、最終操作からパネルオートログオフ時間（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
FAD_RIP.1.1
TSF は、以下のオブジェクト及び TSF データに対する明示的な消去操作において、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: *オブジェクトのリスト及び TSF データのリスト*]。
[割付: *オブジェクトのリスト及び TSF データのリスト*]: ***＜オブジェクト＞*** ***・暗号化プリントファイル***

・*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* ＜*TSF データ*＞ ・*暗号化ワード* ・*HDD ロックパスワード* ・*CF ロックパスワード* ・*管理者パスワード*
下位階層　：　なし 依存性　：　なし

6.1.1.6. 拡張：アクセス先の承認

FIA_EID.1[1]　TOE からのアクセス対象となる IT 環境エンティティの識別
FIA_EID.1.1[1]
TSF は、TOE から IT 環境エンティティ *（HDD）* に対してアクションする前に、その IT 環境エンティティ（*HDD*）の識別に成功することを要求しなければならない。
FIA_EID.1.2[1]
TSF は、IT 環境エンティティ *（HDD）* の識別に失敗した場合、TOE から IT 環境エンティティ *（HDD）* に対するアクションの起動を停止しなければならない。
下位階層　：　なし
依存性　：　なし

FIA_EID.1[2]　TOE からのアクセス対象となる IT 環境エンティティの識別
FIA_EID.1.1[2]
TSF は、TOE から IT 環境エンティティ *（CF）* に対してアクションする前に、その IT 環境エンティティ（*CF*）の識別に成功することを要求しなければならない。
FIA_EID.1.2[2]
TSF は、IT 環境エンティティ *（CF）* の識別に失敗した場合、TOE から IT 環境エンティティ *（CF）* に対するアクションの起動を停止しなければならない。
下位階層　：　なし
依存性　：　なし

6.1.1.7. 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*] ***暗号化キットが実現する暗号化機能***
[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

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*] ***HDD が実現する HDD ロック機能***
[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*] ***・HDD ロックパスワードの変更するためのサポート機能*** ***・HDD ロック機能を解除するためのサポート機能***
下位階層 : なし
依存性 : なし

FIT_CAP.1[3]	**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[3]
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*] ***IC カードにて実現する以下の機能*** ***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*** ***② S/MIME 機能にてスキャン画像を署名するためのメッセージダイジェスト暗号化機能*** ***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*] ***・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*** ***・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*** ***・上記③のための公開鍵の問い合わせ機能***
下位階層 : なし
依存性 : なし

FIT_CAP.1[4]	**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[4]
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*] ***CF が実現する CF ロック機能***
[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*] ***・CF ロックパスワードの変更するためのサポート機能*** ***・CF ロック機能を解除す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 4 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

TOEセキュリティ保証要件		コンポーネント
	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 5　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. DECRYPT-PRINT	O.OVERWRITE-ALL	O.CRYPTO-KEY	O.CHECK-HDD	O.CHECK-CF	O.MAIL-CRYPTO	O.MAIL-SIGN	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.LOCK-CF-CAPABILITY	O.PKI-CAPABILITY	※ set.admin	※ set.service
set.admin						●	●	●	●	●			
set.service						●	●	●	●	●			
FCS_CKM.1			●			●							
FCS_COP.1	●					●	●						
FIA_AFL.1[1]													●
FIA_AFL.1[2]												●	
FIA_AFL.1[3]												●	●

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-KEY	O.CHECK-HDD	O.CHECK-CF	O.MAIL-CRYPTO	O.MAIL-SIGN	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	O.LOCK-CF-CAPABILITY	O.PKI-CAPABILITY	※ set.admin	※ set.service
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_MOF.1[3]												●	
FMT_MOF.1[4]													●
FMT_MTD.1[1]						●	●	●	●	●		●	●
FMT_MTD.1[2]												●	
FMT_MTD.1[3]													●
FMT_MTD.1[4]								●					
FMT_SMF.1						●	●					●	●
FMT_SMR.1[1]												●	●
FMT_SMR.1[2]						●	●					●	
FTA_SSL.3												●	
FAD_RIP.1		●											
FIA_EID.1[1]				●									
FIA_EID.1[2]					●								
FIT_CAP.1[1]								●					
FIT_CAP.1[2]									●				
FIT_CAP.1[3]											●		
FIT_CAP.1[4]										●			

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（完全上書き削除）**

  本セキュリティ対策方針は、HDD のすべてのデータ領域を抹消し、利用者が設定した NVRAM 上の秘匿情報を初期化するとしており、削除に関係する諸要件が必要である。
  FAD_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、暗号化プロテクションチップが設置されている場合に、HDD に書き込む画像データを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 暗号鍵生成メカニズム（SHA256）を利用し、128bit の暗号鍵を生成する。
  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.CHECK-HDD（HDD の正当性確認）**

  本セキュリティ対策方針は、不正な HDD が紛れ込んでいないことを確認するため、HDD の正当性を検証するとしており、TOE からの外部エンティティの検証に関係する諸要件が必要である。
  FIA_EID.1[1]により、TOE から HDD へのアクションの前に HDD を識別し、識別に失敗した場合は、予定されていたアクションを停止する。
  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.CHECK-CF（CF の正当性確認）**

  本セキュリティ対策方針は、不正な CF が紛れ込んでいないことを確認するため、CF の正当性を検証するとしており、TOE からの外部エンティティの検証に関係する諸要件が必要である。
  FIA_EID.1[2]により、TOE から CF へのアクションの前に CF を識別し、識別に失敗した場合は、予定されていたアクションを停止する。
  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. 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（1024bit、または 2048 bit、または 3072 bit、または 4096 bit）である FIPS 186-2 の RSA により暗号化される。
  また暗号アルゴリズムの設定は FMT_MTD.1[1]により管理者に限定される。
  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、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。

- **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。
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、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-1、もしくは SHA-256）により生成する。
またメッセージダイジェスト方式の設定は FMT_MTD.1[1]により管理者に限定される。
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。

＜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。

- **O.CRYPTO-CAPABILITY（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暗号化キットにより、HDD 内に保管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[1]により、暗号化キットが実現する暗号化機能に対して、画像ファイルを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。また暗号化に用いる暗号化ワードは、FIA_SOS.1[3]により品質が検証され、FMT_MTD.1[1]、及び FMT_MTD.1[4]により設定はその管理者に限定される。
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。

＜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。

- **O.LOCK-HDD-CAPABILITY（HDD ロック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 HDD により、設置された MFP 以外からの不正なアクセスを拒否するための動作を 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、HDD が実現する HDD ロック機能に対して、HDD ロックパスワードを変更するためのサポート機能を実現する。HDD ロックパスワードは、FIA_SOS.1[3]により品質が検証され、FMT_MTD.1[1]によりその設定は管理者に限定される。
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。

＜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。

- **O.LOCK-CF-CAPABILITY（CF ロック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 CF により、設置された MFP 以外からの不正なアクセスを拒否するための動作を 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[4]により、CF が実現する CF ロック機能に対して、CF ロックパスワードを変更するためのサポート機能を実現する。CF ロックパスワードは、FIA_SOS.1[3]により品質が検証され、FMT_MTD.1[1]によりその設定は管理者に限定される。
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。

＜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。

- **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の暗号化と署名、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[3]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“＊”を返し、認証をサポートする。

  FIA_AFL.1[3]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、連続して不成功認証が上限値（1～5 回）に達すると、認証状態であればログオフし、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、管理者認証ロック時間が経過後に解除される。またサービスエンジニアによる管理者認証機能のロック解除機能の動作によって解除される。

  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ロック時間は、FMT_MTD.1[1]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、パネルオートログオフ時間が経過した後、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。なおパネルオートログオフ時間の変更は、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。この再認証において、FIA_AFL.1[2]により、連続して不成功認証が上限値（1～5 回）に達すると、認証状態であればログオフし、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、管理者認証ロック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、FMT_MOF.1[2]、及び FMT_MOF.1[3]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“＊”を返し、認証をサポートする。

  FIA_AFL.1[3]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、連続して不成功認証が上限値（1～5 回）に達すると、認証状態であればログオフし、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 認証ロック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[1]により管理者だけに許可される。CE 認証ロック時間の設定は、FMT_MTD.1[3]

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[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。この再認証において、FIA_AFL.1[1]により、連続して不成功認証が上限値（1～5 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 認証ロック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、FMT_MOF.1[1]、及び FMT_MOF.1[4]**によりそのふるまいが管理される。**

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 6 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（一部事象のみ） 満たしている事象：擬似乱数生成アルゴリズムにより生成された鍵を操作すること ＜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 暗号化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、配付及び暗号操作の必要性はない。 ＜FCS_CKM.4 を適用しない理由＞ ・擬似乱数生成アルゴリズムにより生成された鍵は、一時的に揮発性のある記憶領域に存在すると考えられるが、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。 ・コニカミノルタ HDD 暗号化暗号鍵生成アルゴリズムにより生成された鍵は、保管されるデータのために定常的に保管される。また保管媒体への任意のアクセスは困難であり、暗号鍵破棄の必要性はない。
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 送信データを暗号化するための共通鍵を生成すること。 ＜FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 を一部満たしていない理由＞ ・暗号化プリントファイルの復号を行う共通鍵は

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
		FIT_CAP.1[3]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。 ・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[3]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。 ・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。 ＜FCS_CKM.4 を適用しない理由＞ ・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、メッセージダイジェストの生成に用いる鍵は、一時的に揮発性のある記憶領域に存在すると考えられるが、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。 ・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。
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]
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]
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[1]
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[1]
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_MTD.1[4]	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]
FTA_SSL.3	なし	N/A
FAD_RIP.1	なし	N/A
FIA_EID.1[1]	なし	N/A
FIA_EID.1[2]	なし	N/A
FIT_CAP.1[1]	なし	N/A

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
FIT_CAP.1[2]	なし	N/A
FIT_CAP.1[3]	なし	N/A
FIT_CAP.1[4]	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 7 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 7 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（全領域上書き削除機能）	管理者機能
7.6	F.CRYPTO（暗号鍵生成機能）	その他の機能
7.7	F.VALIDATION-HDD（HDD 検証機能）	その他の機能
7.8	F.VALIDATION-CF（CF 検証機能）	その他の機能
7.9	F.RESET（認証失敗回数リセット機能）	管理者機能、サービスエンジニア機能
7.10	F.S/MIME（S/MIME 暗号処理機能）	基本機能
7.11	F.SUPPORT-CRYPTO（暗号化キット動作サポート機能）	その他の機能
7.12	F.SUPPORT-HDD（HDD ロック動作サポート機能）	その他の機能
7.13	F.SUPPORT-CF（CF ロック動作サポート機能）	その他の機能
7.14	F.SUPPORT-PKI（PKI サポート機能）	その他の機能

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 8 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。
- 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。
- 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連続して 1～5 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 が動作する、または F.SERVICE における管理者認証機能のロック解除機能が実行されて解除する。

以上により FIA_AFL.1[2]、FIA_AFL.1[3]、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オフ機能

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オフ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オフする。

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。

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た場合、変更する。

- 表 8 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再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、パネルからのアクセスの場合、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連続して1～5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管理者モードをログオフし、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。(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 が動作する、または F.SERVICE における管理者認証機能のロック解除機能が実行されて解除する。
- 新規設定される管理者パスワードは表 8 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ていることを検証する。

以上により FIA_SOS.1[2]、FIA_AFL.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. 不正アクセス関係の設定

- **不正アクセス検出の設定**
  認証操作禁止機能の有効、及び無効を設定する。
- **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 1～5 回間で設定する。
- **管理者認証ロック時間の設定**
  管理者認証ロック時間を 1～60 分で設定する。

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

7.1.3.3. オートログオフ機能の設定

オートログオフ機能における設定データであるパネルオートログオフ時間を以下に示す時間範囲で設定する。

- パネルオートログオフ時間　　：1～9 分

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

7.1.3.4. HDD ロック機能の設定機能

＜HDD ロックパスワード変更＞
HDD ロックパスワードを変更する。現在設定される HDD ロックパスワードを使い、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、変更する。

- 表 8 に示されるキャラクタからなる HDD ロックパスワードを照合する HDD ロックパスワード照合メカニズムを提供する。
- 照合では、HDD ロックパスワード入力のフィードバックに 1 文字毎“*”を返す。
- 新規設定される HDD ロック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 8 の HDD ロック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[3]、FIA_UAU.7、FIA_UAU.6、FMT_MTD.1[1]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

表 8 パスワードに利用されるキャラクタと桁数 [3]

対象	桁数	キャラクタ
・管理者パスワード	（0～8 桁）	最低合計 92 文字の中から選択可能
・CE パスワード	8 桁	最低合計 92 文字の中から選択可能
・HDD ロックパスワード	20 桁	最低合計 83 文字の中から選択可能
・CF ロックパスワード	20 桁	最低合計 84 文字の中から選択可能
・暗号化ワード	20 桁	最低合計 84 文字の中から選択可能

7.1.3.5. CF ロック機能の設定機能

＜CF ロックパスワード変更＞
CF ロックパスワードを変更する。現在設定される CF ロックパスワードを使い、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、変更する。

- 表 8 に示されるキャラクタからなる CF ロックパスワードを照合する CF ロックパスワード照合メカニズムを提供する。
- 照合では、CF ロックパスワード入力のフィードバックに 1 文字毎“*”を返す。
- 新規設定される CF ロック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 8 の CF ロック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[3]、FIA_UAU.7、FIA_UAU.6、FMT_MTD.1[1]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.6. 暗号化機能の動作設定

（※暗号化プロテクションチップが MFP に装着されている場合のみ操作可）
＜動作設定 ON＞
OFF から ON にする場合、新しく設定される暗号化ワードが以下の品質を満たしていることを検証

[3] 表 8 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。

し、F.CRYPTO が実行される。
- 表 8 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。

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

＜暗号化ワード変更、動作設定 OFF＞
暗号化ワードを変更、動作設定を OFF にする。現在設定される暗号化ワードを使い、管理者であることを再認証された場合に許可される。暗号化ワードを変更する場合は、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。
- 表 8 に示されるキャラクタからなる暗号化ワードを照合する暗号化ワード照合メカニズムを提供する。
- 照合では、暗号化ワード入力のフィードバックに 1 文字毎“*”を返す。
- 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 8 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_MOF.1[3]、FIA_UAU.7、FIA_UAU.6、FMT_MTD.1[1]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.3.7. S/MIME 送信機能の設定

管理者が操作する S/MIME 機能に関係する機能は以下の通り。
- デジタル署名付与の設定
  S/MIME 機能利用時のデジタル署名を常に有効、送信時選択、及び常に無効から選択可能
- S/MIME 暗号化強度（暗号アルゴリズム）の変更
- S/MIME メッセージダイジェストの方式のアルゴリズム変更

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

7.1.3.8. 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、管理者パスワードを工場出荷の初期値に設定する。

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

7.1.3.9. セキュリティに関する動作設定機能

管理者が操作するセキュリティに関する動作設定機能は以下の通り。
- ネットワークからの管理者機能の有効、及び無効化設定
  ネットワークからの管理者機能を有効化することにより、ネットワーク経由での管理者機能が利用可能となる。
- 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。
- 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、HDD 上のファイルシステムで利用する管理データの値が初期化される。

以上により FMT_MOF.1[2]、FMT_SMF.1、FMT_SMR.1[2]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 8 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。
- 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連続して 1～5 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[3]、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、以下の機能の利用が許可される。

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 8 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、パネルからのアクセスの場合、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連続して 1～5 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オフし、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 パスワードは表 8 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ていることを検証する。

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

7.2.2.3. 管理者認証機能のロックの解除

管理者認証失敗回数を 0 クリアする。

- アクセスがロックされていれば、ロックが解除される。

以上により FIA_AFL.1[2]が実現される。

7.2.2.4. CE 認証ロック時間の設定

CE 認証ロック時間を 1～60 分で設定する
以上により FMT_MTD.1[3]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.2.2.5. サービスエンジニア認証機能の設定

サービスエンジニア認証機能の有効、無効を設定する。
以上により FMT_MOF.1[4]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

7.2.2.6. TSF データに影響する機能の管理

サービスエンジニアが操作する他の TSF データに影響する機能は以下の通り。

- 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。
- イニシャライズ機能
  NVRAM 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。
- メンテナンス機能
  RC-232C を介したシリアル接続を行い故障時等のメンテナンスを行う機能。
- 遠隔診断機能
  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機能。
- インターネット経由 TOE 更新機能
  Ethernet を介して TOE をダウンロードする機能。

以上により FMT_MOF.1[1]、FMT_SMF.1、FMT_SMR.1[1]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、SP800-67 によって規定される 3-Key-Triple-DES 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（全領域上書き削除機能）

F.OVERWRITE-ALL とは、HDD のデータ領域に上書き削除を実行すると共に 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＞

- 暗号化プリントファイル
- 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 ロック機能の動作設定（OFF）　・・・HDD ロックパスワードが消去される。
- CF ロック機能の動作設定（OFF）　・・・CF ロックパスワードが消去される。
- 暗号化機能の動作設定（OFF）　・・・暗号化ワードが消去される。

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 9**）に応じて実行される。HDD ロック機能、CF ロック機能、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 HDD ロックパスワード、CF ロックパスワード、暗号化ワードが利用できなくなる。

以上により FAD_RIP.1 が実現される。

表 9　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
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

7.6. 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（SHA256）を利用し、HDD に書き込まれる画像データを暗号化するための暗号鍵を生成する。コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA256）とは、FIPS 180-2 が規定する SHA256 を利用して暗号鍵を生成するアルゴリズムである。

F.ADMIN においてアクセス制限される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（SHA256）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。

7.7. F.VALIDATION-HDD（HDD 検証機能）

F.VALIDATION-HDD とは、HDD に HDD ロックパスワードを設定している場合において、不正な HDD が設置されていないことを検証し、正当性が確認された場合だけ HDD への読み込み、書き込みを許可するチェック機能である。

HDD に HDD ロックパスワードが設定されている場合、TOE 起動時の HDD 動作確認において、HDD のステータス確認を行う。ステータス確認の結果、HDD ロックパスワードが確かに設定されていることが返された場合は、HDD へのアクセスを許可し、HDD ロックパスワードが設定されていないことが返された場合は、不正な可能性があるため HDD へのアクセスを拒否する。

以上により FIA_EID.1[1]が実現される。

7.8. F.VALIDATION-CF（CF 検証機能）

F.VALIDATION-CF とは、CF に CF ロックパスワードを設定している場合において、不正な CF が設置されていないことを検証し、正当性が確認された場合だけ CF への読み込み、書き込みを許可するチェック機能である。

CF に CF ロックパスワードが設定されている場合、TOE 起動時の CF 動作確認において、CF のステータス確認を行う。ステータス確認の結果、CF ロックパスワードが確かに設定されていることが返された場合は、CF へのアクセスを許可し、CF ロックパスワードが設定されていないことが返された場合は、不正な可能性があるため CF へのアクセスを拒否する。

以上により FIA_EID.1[2]が実現される。

7.9. 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 認証ロック時間後に 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、管理者認証ロック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。

7.10. 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、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。

＜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-1、もしくは 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。

7.11. F.SUPPORT-CRYPTO（暗号化キット動作サポート機能）

F.SUPPORT-CRYPTO とは、TOE から暗号化キットによる暗号化機能を動作させるための機能である。

HDD に書き込まれる画像ファイルに対して、F.CRYPTO により生成された暗号鍵を暗号化キットにセットし、暗号化キット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画像ファイルに対して、同じく F.CRYPTO により生成された暗号鍵を暗号化キットにセットし、暗号化キットにて復号処理を行わせる。

以上により、FIT_CAP.1[1]が実現される。

7.12. F.SUPPORT-HDD（HDD ロック動作サポート機能）

F.SUPPORT-HDD とは、TOE から HDD による HDD ロック機能を動作させるための機能である。

＜HDD のロック状態を解除処理＞
MFP の起動時に、HDD の HDD ロック機能によるロック状態を解除するための解除処理を行う。
- HDD に対して、NVRAM に保管されている HDD ロックパスワードを用いて解除処理要求を実施する。

＜HDD ロックパスワードの変更に基づく処理＞
F.ADMIN からの、HDD ロックパスワードの変更処理要求を行う。
- HDD に対して、NVRAM に保管されている HDD ロックパスワードと新しい HDD ロックパスワードを用いて変更処理要求を実施する。

以上により、FIT_CAP.1[2]が実現される。

7.13. F.SUPPORT-CF（CF ロック動作サポート機能）

F.SUPPORT-CF とは、TOE から CF による CF ロック機能を動作させるための機能である。

＜CF のロック状態を解除処理＞
MFP の起動時に、CF の CF ロック機能によるロック状態を解除するための解除処理を行う。
- CF に対して、NVRAM に保管されている CF ロックパスワードを用いて解除処理要求を実施する。

＜CF ロックパスワードの変更に基づく処理＞
F.ADMIN からの、CF ロックパスワードの変更処理要求を行う。
- CF に対して、NVRAM に保管されている CF ロックパスワードと新しい CF ロックパスワードを用いて変更処理要求を実施する。

以上により、FIT_CAP.1[4]が実現される。

7.14. 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）の復号処理を行わせ、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[3]が実現される。

---以上---