bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221　全体制御ソフトウェア セキュリティターゲット

バージョン：1.03

発行日：2009年8月5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	承認者	確認者	作成者	担当部署	更新内容
2009/01/06	1.00	廣田	出山	渥美	制御第12開発部	初版
2009/06/17	1.01	廣田	多田	渥美	第1オフィスSW開発部	誤植修正
2009/06/22	1.02	廣田	多田	渥美	第1オフィスSW開発部	誤植修正
2009/08/05	1.03	廣田	多田	渥美	第1オフィスSW開発部	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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア セキュリティターゲット
・STバージョン	:	1.03
・作成日	:	2009年8月5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　　渥美 知之

1.2. TOE 参照

・TOE名称	:	日本語名：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア
		英語名　：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software
・TOE識別	:	A11U-0100-G10-06
・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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェアとは、MFP 制御コントローラ上の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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 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 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 全体制御ソフトウェア”である。

TOE は、MFP に保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。また MFP 内に画像データを保存する媒体である HDD が不正に持ち出される等の危険性に対して、不要となったデータを即時に上書き削除する保護機能、及び HDD に搭載される HDD ロック機能を利用する保護機能を提供する。さらに MFP のオプション部品である暗号化基板を取り付けることによって、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**
  MFP を使ってコピー、スキャンなどを行う 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 の動作管理やボックスの管理を行う。（一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される。）

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

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

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

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

1.4.2. TOE の物理的範囲

1.4.2.1. 利用環境

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

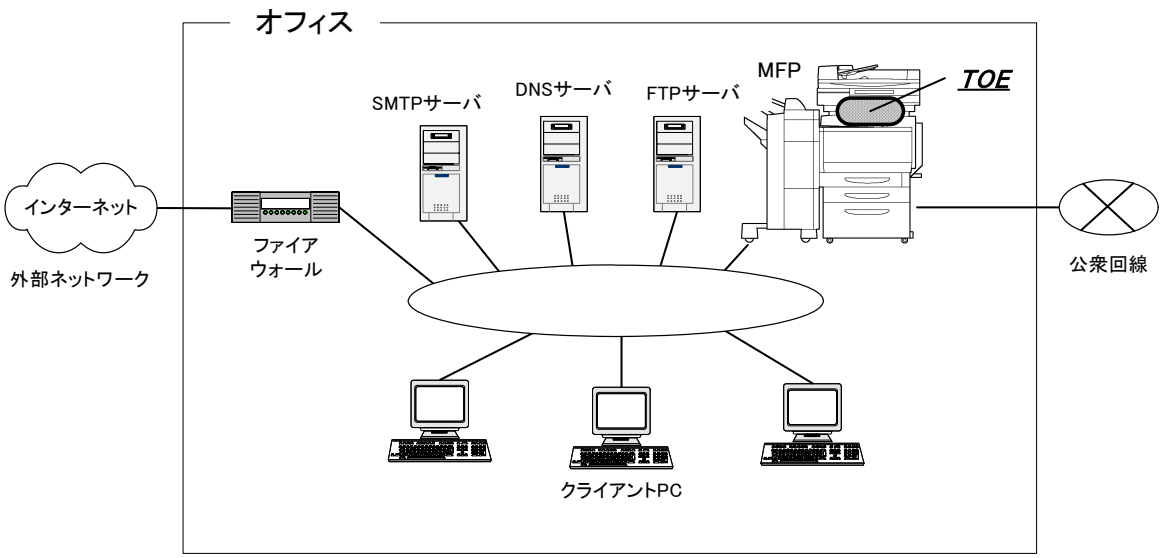

図 1 MFP の利用環境の例

- オフィス内部のネットワークとしてオフィス内 LAN が存在する。
- MFP はオフィス内 LAN を介してクライアント PC と接続され、相互にデータ通信を行える。
- オフィス内 LAN に SMTP サーバ、FTP サーバが接続される場合は、MFP はこれらともデータ通信を行うことが可能。（なお SMTP サーバ、FTP サーバ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。
- オフィス内 LAN は、スイッチングハブ等の利用、盗聴の検知機器の設置などオフィスの運用によって、盗聴されないネットワーク環境が整備されている。
- MFP に接続される公衆回線は、FAX や遠隔サポート機能の通信に利用される。

1.4.2.2. 動作環境

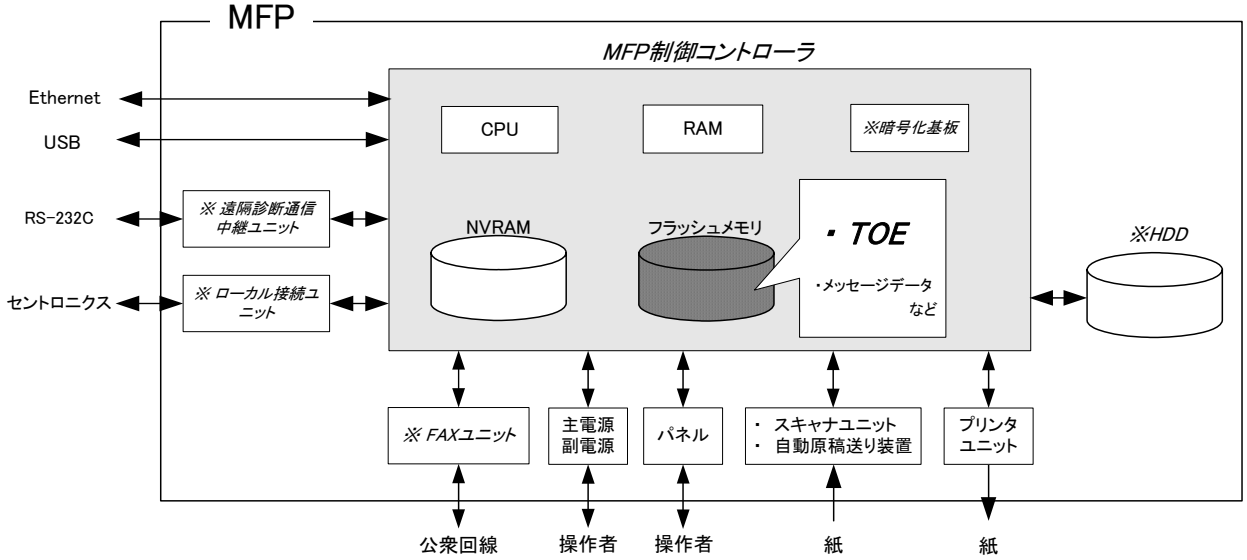

図 2 TOE に関係するハードウェア構成

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 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フラッシュメモリ上に存在し、ロードされる。

以下には図 2 にて示される MFP 制御コントローラ上の特徴的なハードウェア、MFP 制御コントローラとインタ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。

- **フラッシュメモリ**
  TOE である MFP 全体制御ソフトウェアのオブジェクトコードが保管される記憶媒体。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を保管する。

- RAM
  揮発性メモリ。画像データが保管される記憶媒体。

- NVRAM
  不揮発性メモリ。MFP の動作において必要な様々な設定値（管理者パスワード、送信宛先データなど）等が保管される記憶媒体。

- **暗号化基板（※オプションパーツ）**
  HDD に書き込まれるすべてのデータを暗号化するための暗号機能がハード的に実装されている暗号化のための集積回路。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。

- **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。

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

- USB
  ローカル接続によるプリントを行うポート。

- **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。

- HDD（**※オプションパーツ**）
  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、RAM の処理容量を超える画像データがスワップされる領域として利用される。
  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。
  なお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。装着されない場合は、HDD が必要となる機能（1.4.3.3 節のボックス機能）を利用することができない。

- 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。

- **ローカル接続ユニット（※オプションパーツ）**
  クライアント PC とセントロニクスインターフェース（パラレルポート）を使って接続し、ローカル接続でプリント機能を使うためのユニット。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。

- **遠隔診断通信中継ユニット（※オプションパーツ）**
  RS-232C を介して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すれば、故障時などに本インターフェースを介して遠隔診断機能（後述）を使用することができる。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。

1.4.2.3. ガイダンス

- bizhub 350 / 250 / 200　サービスマニュアル　セキュリティ機能編
- bizhub 362 / 282 / 222 / ineo 362 / 282 / 222 / VarioLink 3621 / 2821 / 2221 SERVICE MANUAL SECURITY FUNCTION
- bizhub 350 / 250 / 200 ユーザーズガイド　セキュリティ機能編
- bizhub 362 / 282 / 222 User's Guide [Security Operations]
- ineo 362 / 282 / 222 User's Guide [Security Operations]
- VarioLink 3621 / 2821 / 2221 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、保管された画像ファイルを管理するためのボックス機能、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。（PC からのプリント画像ファイルは、複数の変換処理が行なわれる。）画像ファイルは、印刷用または送信用のデータとして変換され、目的の MFP 制御コントローラ外部のデバイスに転送される。

コピー、プリント、スキャン、FAX などの動作は、ジョブという単位で管理され、パネルからの指示により動作の中止が行える。

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。

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

1.4.3.2. ユーザチョイス機能

主として基本機能の利用において必要となる画質調整（倍率、印刷濃度など）を始めとして、標準レイアウト、省エネ移行時間、オートリセット（一定時間操作を行わないと、操作パネルの表示が基本画面に戻る機能）時間をユーザが自由に設定することができる。

1.4.3.3. ボックス機能

画像ファイルを保管するための領域として、HDD にボックスと呼称されるディレクトリを作成できる。ボックスにはすべてのユーザが利用することが可能な public ボックスと、パスワードを設定して個別、または利用者間でパスワード共用することによって、利用するボックスの 2 つのタイプが存在する。

TOE は、パネル、またはクライアント PC からネットワークを介してネットワークユニットより、ボックス、ボックス内の画像ファイルに対する以下の操作要求を処理する。

- ボックス内の画像ファイルの印刷、送信、クライアント PC からのダウンロード
- ボックス内の画像ファイルの削除
- ボックス内の画像ファイルの保管期間設定（期間経過後は自動的に削除）
- ボックスの名称変更、ボックス ID の変更、パスワードの変更、ボックスの削除など

なお HDD が装着されない場合、ボックスを作成することはできない。

1.4.3.4. 管理者機能

TOE は、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、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。
以下にはセキュリティに関係する機能について例示する。

- ボックスの設定管理
  - ボックス ID の変更
  - ボックスパスワードの変更
- ネットワーク設定管理
  - オフィス内 LAN との接続設定（DNS サーバの設定）
  - SMTP 設定（E-mail 送信にて利用する SMTP サーバの設定）
  - IP アドレス、NetBIOS 名、AppleTalk プリンタ名など
- 廃棄時の上書き削除機能
  - HDD の全データ領域に対して上書き削除を実行する。
  - NVRAM 上の管理者が設定した各種設定値や課金情報なども初期化される。

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- 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
- 認証操作禁止機能の設定
  - 各認証機能における不成功認証の検出する機能
  - 上記の動作モードを選択
  - 不成功認証検出のモードでは、PC からのボックスファイルダウンロード操作時にボックスパスワード照合機能を動作させる。
- 残存情報上書き削除機能（後述）の方式設定
  - 上書きデータ：0x00 ⇒ 0x00 ⇒ 0x00 方式の動作有効と動作無効設定が存在
  - 上記の動作方式を選択
- 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
- 暗号化機能の設定（※暗号化基板を装着時のみ）
  - 動作、停止を選択
  - 動作選択時には、暗号鍵ワードを登録・変更

1.4.3.5. サービスエンジニア機能

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

- 管理者モードパスワードの初期化機能
- 遠隔診断機能（後述）の設定
- トータルクリア機能

- 管理者が設定した各種設定値などを初期化する。

- メモリダンプ機能
  - 故障時などに NVRAM の状態を確認するための機能
  - 管理者パスワードなどの値もダンプによって確認することが可能

1.4.3.6. 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 **残存情報の上書き削除機能**

ジョブの終了、ジョブ管理機能からの削除操作、ボックスに保管される画像ファイルの削除、画像ファイルの保管期間経過による削除などによって、不要になった画像ファイルの上書き削除を行う。上書きされるデータは、0x00 ⇒ 0x00 ⇒ 0x00 の順で行なわれる。

② **遠隔診断機能**

RS-232C を介したモデム接続経由、FAX ユニット経由、E-mail などいくつかの接続方式を利用して、コニカミノルタホールディングス関連会社によって運営される MFP のサポートセンターと通信し、MFP の動作状態、管理者パスワードなどの設定情報、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。遠隔診断機能よりコマンドを受けると Ethernet を介して FTP サーバよりダウンロードし更新することが可能。またコンパクトフラッシュメモリ媒体を接続して行う方法がある。

④ **暗号鍵生成機能**

オプション製品である暗号化基板が MFP 制御コントローラに設置されている場合に、暗号化基板にて HDD のデータ書き込み、読み込みにおいて暗号化・復号処理を実施する。（TOE は、暗復号処理そのものを行わない。）

管理者機能にて本機能の動作設定を行う。動作させる場合は、TOE はパネルにて入力された暗号鍵ワードより暗号鍵を生成する。

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

⑤ **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。

管理者機能にて本機能の動作設定を行う。MFP の起動動作において、MFP 側に設定された HDD ロックパスワードと HDD 側に設定される HDD のパスワードロックを照合し、一致した場合に HDD へのアクセスを許可する。（HDD を持ち出されても、当該 HDD が設置されていた MFP 以外で利用することができない。）

⑥ **暗号化基板の活用**

外部エンティティである暗号化基板は、不正な持ち出し等への対処機能として、暗号鍵ワード

を設定した場合に HDD 内のデータを暗号化する機能が動作する。

1.4.3.7. 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ことが禁止される。また個別には動作設定機能を持たない機能として、機密文書プリントの認証機能の設定が存在するが、セキュリティを強化状態（ID を選択した上でパスワードを入力する動作方式）にする。

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、サービスコ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。

- パスワード規約機能の設定 : 有効
- SNMP（v1、v2、及び v3）による ネットワーク設定変更機能の設定 : 禁止
- 機密文書プリント認証方式の設定 : ファイル ID を指定した後にパスワード照合動作
- 認証操作禁止機能の設定 : 有効（アカウントロック（失敗回数閾値：3 回）状態になる。またボックス認証方式がダウンロード時パスワード照合機能動作方式になる。）
- HDD ロック機能の設定 : 有効（暗号化機能が有効の場合、無効も可）
- 暗号化機能の設定 : 有効（HDD ロック機能が有効の場合、無効も可）
- 残存情報上書き削除機能の設定 : 有効
- トータルクリア機能 : 禁止
- メモリダンプ機能 : 禁止
- 遠隔診断機能 [1] : ・RS232Cモデム接続禁止
  ・FAXユニット接続受信機能禁止
  ・E-mailによる受信機能禁止

[1] ただし、FAX ユニット接続送信機能、E-mail による送信機能は有効である。

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。

- **機密文書プリントファイル**
  - 機密文書プリントによって登録される画像ファイル
- **ボックスファイル**
  - 「Public」以外のボックスに保管される画像ファイル

なお機密文書プリントファイルの印刷においては、万が一不正な MFP が接続された場合に考えられる脅威に備え、MFP の設定（IP アドレスなど）を不正に変更出来ないようにする必要がある。したがって MFP の設定（IP アドレスなど）は副次的な保護資産として考慮する。

複数のジョブの動作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。

- **全ボックスファイル**
  - 「Public」ボックスを含めたボックス内に保管される画像ファイル
- **スワップデータファイル**
  - RAM 領域に収まらないサイズの大きいコピー、PC プリント（機密文書プリントファイルを含む）にて発生する、画像を構成するためのファイル。
- **オーバーレイ画像ファイル**
  - 背景画像ファイル
  - 登録されるこの画像ファイルを背景に設定し、コピーなどが行なえる。
- **HDD 蓄積画像ファイル**
  - PC プリントから HDD に保管し、パネルからの操作で印刷を行うためのファイル
- **残存画像ファイル** [2]
  - 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
- **送信宛先データファイル**
  - E-mail アドレス、電話番号などが含まれるファイル。

[2] 本データは、TOE を設置して、セキュリティ機能が動作する状態において発生しないように制御される資産である。脅威識別には、セキュリティ対策が実施されていなかったと仮定した場合に起こり得る事象として本資産の扱いについて説明している。

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

A.ADMIN（管理者の人的条件）

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

A.SERVICE（サービスエンジニアの人的条件）

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

A.NETWORK（MFP のネットワーク接続条件）

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

A.SECRET（秘密情報に関する運用条件）

TOE の利用において使用される各パスワードや暗号鍵ワードは、各利用者から漏洩しない。

A.SETTING（セキュリティ強化機能の動作設定条件）

- セキュリティ強化機能を有効化した上で、TOE が搭載された MFP を利用する。

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。なお、以下に説明する脅威のうち、HDD 持ち出しに関する T.BRING-OUT-STORAGE、及び HDD が必須となるボックス機能に関する T.ACCESS-BOX は、オプションパーツである HDD を取りつけていない場合は脅威として存在しない。

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、機密文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD残存画像ファイル、送信宛先データファイル、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。[3]

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、全ボックスファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD 蓄積画像ファイル、残存画像ファイルが漏洩する。
・悪意を持った者や悪意を持ったユーザが、MFP 内の HDD を不正にすりかえる。すりかえられた HDD には新たにボックスファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD 蓄積画像ファイル、残存画像ファイルが蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえた HDD を持ち出して解析することにより、これら画像ファイル等が漏洩する。

[3] HDD 未装着の場合、NVRAM 送信宛先データファイル、及び各種パスワードのみ対象となる。

T.ACCESS-BOX（ユーザ機能を利用したボックスへの不正なアクセス）

悪意を持った者や悪意を持ったユーザが、利用を許可されないボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、SMB[4]送信）することにより、ボックスファイルが暴露される。

T.ACCESS-SECURE-PRINT（ユーザ機能を利用した機密文書プリントファイルへの不正なアクセス）

悪意を持った者や悪意を持ったユーザが、利用を許可されない機密文書プリントファイルを印刷することにより、機密文書プリントファイルが暴露される。

T.UNEXPECTED-TRANSMISSION（ネットワーク設定の不正変更）

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

＜ボックスファイル送信に関係するネットワーク設定＞

- SMTP サーバに関する設定
- DNS サーバに関する設定

・悪意を持った者や悪意を持ったユーザが、TOE が導入される MFP に設定される MFP を識別するためのネットワーク設定を変更し、不正な別の MFP などのエンティティにおいて本来 TOE が導入される MFP の設定（NetBIOS 名、AppleTalk プリンタ名、IP アドレスなど）を設定することにより、不正な MFP に機密文書プリントファイルが送付され暴露される。

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

悪意を持った者や悪意を持ったユーザが、セキュリティ強化機能に関係する設定を変更してしまうことにより、ボックスファイル、機密文書プリントファイルが漏洩する可能性が高まる。[5]

3.4. 組織のセキュリティ方針

本 TOE に適用することが想定される組織のセキュリティ方針は存在しない。

[4] Server Message Block の略。Windows でファイル共有、プリンタ共有を実現するプロトコル。
[5] HDD 未装着の場合、機密文書プリントファイルのみ対象となる。

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。

なお HDD が装着されない場合には、不要なセキュリティ対策が存在することになるが、これ以降は、HDD が装着された場合を想定し、最大限必要と考えられる脅威に対するセキュリティ対策、セキュリティ要件について論述することにする。

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.BOX（ボックスアクセス制御）

TOE は、そのボックスの利用を許可されたユーザだけに、そのボックス内のボックスファイルのユーザ機能を許可する。

O.SECURE-PRINT（機密文書プリントファルアクセス制御）

TOE は、その機密文書プリントファイルの利用を許可されたユーザだけに、その機密文書プリントファイルの印刷を許可する。

O.CONFIG（管理機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・SMTP サーバに関係する設定機能
・DNS サーバに関係する設定機能
・MFP のアドレスに関係する設定機能
・HDD ロック機能、暗号化機能の設定機能
・セキュリティ強化機能の設定に関係する機能

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。またユーザ、管理者が設定した送信宛先データを削除する機能、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、暗号鍵ワード）を初期値に戻す機能を提供する。

O.OVERWRITE-FILE（ファイル単位の上書き削除）

TOE は、MFP 内の HDD に書き込まれた画像ファイルが不要になると、削除用データを上書きし、当該画像を復旧不可能にする。

O.CRYPT-KEY（暗号鍵生成）

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

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

TOE は、暗号化基板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。

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.CRYPTO（暗号化機能の利用）

TOE の利用において HDD に保管される画像ファイルの暗号化対策の実施を希望する場合、管理者は暗号化基板のライセンスを購入し、サービスエンジニアと共に暗号化基板の暗号化機能による MFP 内の HDD に書き込まれる画像ファイルの暗号化を行うための設定をする。

OE.LOCK-HDD（HDD ロック機能をもった HDD の利用）

サービスエンジニア及び管理者は、MFP に HDD ロック機能を有する HDD を搭載し、その機能を利用するための設定をする。

OE.FEED-BACK（パスワードのフィードバック）

管理者及びユーザがクライアント PC にて MFP にアクセスするために利用されるブラウザ、PC プリントドライバといったアプリケーションは、入力される機密文書パスワード、ボックスパスワード、管理者パスワードに対して保護された適切なフィードバックを提供する。

OE.ADMIN（信頼できる管理者）

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

OE.SERVICE（サービスエンジニアの保証）

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

OE.NETWORK（MFP の接続するネットワーク環境）

・MFP を利用する組織の責任者は、TOE が搭載される MFP を設置するオフィス LAN において暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を実施する。
・MFP を利用する組織の責任者は、外部ネットワークから TOE が搭載される MFP へのアクセスを遮断するためにファイアウォールなどの機器を設置して、外部からの不正侵入対策を実施する。

OE.SECRET（秘密情報の適切な管理）

管理者は、ユーザに対して以下に示す運用を実施させる。

・機密文書パスワードを秘匿する。

・ボックスパスワードは共同で利用するユーザの間で秘匿する。

・機密文書パスワード、ボックスパスワードに推測可能な値を設定しない。

・ボックスパスワードの適宜変更を行う。

・管理者がボックスパスワードを変更した場合は、速やかに変更させる。

管理者は、以下に示す運用を実施する。

・管理者パスワード、HDD ロックパスワード、暗号鍵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、暗号鍵ワードを秘匿する。

・管理者パスワード、HDD ロックパスワード、暗号鍵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。

・サービスコードに推測可能な値を設定しない。

・サービスコードを秘匿する。

・サービスコ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.SESSION（操作後のセッションの終了）

管理者は、ユーザに対して以下に示す運用を実施させる。

・機密文書プリントファイルに対する機能を操作終了後にログオフ操作を行う。

・ボックスファイルに対する機能を操作終了後にログオフ操作を行う。

管理者は、以下に示す運用を実施する。

・管理者モードの諸機能を操作終了後にログオフ操作を行う。

サービスエンジニアは、以下に示す運用を実施する。

・サービスモードの諸機能を操作終了後にログオフ操作を行う。

OE.SETTING-SECURITY（セキュリティ強化機能の動作設定）

- 管理者は、TOE の運用にあたってセキュリティ強化機能の設定を有効化する。

4.3. セキュリティ対策方針根拠

4.3.1. 必要性

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

表 1 前提条件、脅威に対するセキュリティ対策方針の適合性

前提・脅威 / セキュリティ対策方針	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-BOX	T.ACCESS-SECURE-PRINT	T.UNEXPECTED-TRANSMISSION	T.ACCESS-SETTING
O.BOX								●			
O.SECURE-PRINT									●		
O.CONFIG										●	●
O.OVERWRITE-ALL						●					
O.OVERWRITE-FILE							●				
O.CRYPT-KEY							●				
O.CHECK-HDD							●				
O.CRYPTO-CAPABILITY							●				
O.LOCK-HDD-CAPABILITY							●				
OE.CRYPTO							●				
OE.LOCK-HDD							●				
OE.FEED-BACK								●	●	●	●
OE.ADMIN	●										
OE.SERVICE		●									
OE.NETWORK			●								
OE.SECRET				●							
OE.SESSION								●	●	●	●
OE.SETTING-SECURITY					●						

4.3.2. 前提条件に対する十分性

前提条件に対するセキュリティ対策方針について以下に説明する。

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

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

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

- **A.SECRET（秘密情報に関する運用条件）**
  本条件は、TOE の利用において使用される各パスワード、暗号鍵ワードが各利用者より漏洩しないことを想定している。
  OE.SECRET は、管理者がユーザに対して機密文書パスワード、ボックスパスワードに関する運用規則を実施させることを規定し、管理者が管理者パスワード、HDD ロックパスワード、暗号鍵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サービスコードに関する運用規則を実施することを規定しており、本条件は実現される。

- **A.SETTING（セキュリティ強化機能の動作設定条件）**
  本条件は、セキュリティ強化機能の動作設定条件が満たされることを想定している。
  OE.SETTING-SECURITY は、管理者がセキュリティ強化機能の設定を有効化した上で利用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 内の HDD 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 の全データ領域に削除用のデータを上書きする機能を提供し、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。

O.OVERWRITE-FILE は、TOE が HDD に書き込まれる画像ファイルが不要になると、削除用データを上書きするとしており、HDD 上には利用中である必要最小限のデータが存在することになり、脅威は大幅に軽減される。

また以下の 2 つの対策の少なくともどちらかの対策が、管理者によって選択されるため、脅威の可能性は除去される。

① O.CRYPTO-KEY は、TOE が HDD に書き込まれるデータを暗号化するための暗号鍵を生成し、O.CRYPTO-CAPABILITY により暗号化機能を利用するための動作がサポートされ、OE.CRYPTO により、管理者の設定により暗号化基板による暗号化機能が利用される。

② 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、OE.LOCK-HDD により、管理者により HDD ロック機能を動作させるための設定が行われ HDD ロック機能が動作する。

HDD がすりかえられて、この対策が想定する機能を有さない HDD が設置されることにより、すりかえられた HDD に蓄積される HDD が持ち出されて漏洩する危険性が存在する。これには 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.ACCESS-BOX（ユーザ機能を利用したボックスへの不正なアクセス）**

本脅威は、画像ファイルの保管場所であるボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。

O.BOX によってボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は除去される。

OE.FEED-BACK は、ボックスパスワードの認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、O.BOX は十分サポートされる。

したがって本脅威は十分対抗されている。

- **T.ACCESS-SECURE-PRINT（機密文書プリントファイルへの不正なアクセス）**

本脅威は、機密文書プリントに対して不正な操作が行われてしまう可能性を想定している。

O.SECURE-PRINT によって、機密文書プリントの操作が許可されたユーザだけに制限され、脅威の可能性は除去される。

OE.FEED-BACK は、機密文書プリントへのアクセス認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE.SESSION により操作終了後にはログオフする運用が奨励されるため、O.SECURE-PRINT は十分サポートされている。

したがって本脅威は十分対抗されている。

- **T.UNEXPECTED-TRANSMISSION（ネットワーク設定の不正変更）**

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

  さらに、MFP のアドレスに関係するネットワーク設定を不正に変更された場合に、TOE であると思って利用するユーザが、不正なエンティティにクライアント PC からプリント機能を利用してしまう可能性を想定している。特にオフィス内の他のユーザに対しても秘匿性が要求される機密文書プリントファイルが不正なエンティティに送信されると問題となる。

  これに対して O.CONFIG により、TOE が送信に関係するネットワーク設定を操作する役割を管理者に制限するとしており、本脅威の可能性は除去される。

  OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE.SESSION により操作終了後にはログオフする運用が奨励されるため、O.CONFIG は十分サポートされている。

  したがって本脅威は十分対抗されている。

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

  本脅威はセキュリティに関係する特定の機能設定を変更されることにより、結果的にボックスファイルや機密文書プリントファイルの漏洩に発展する可能性を想定している。

  O.CONFIG により、一連のセキュリティに関連する設定機能を統括するセキュリティ強化機能の設定を管理者だけに許可するとしており、脅威の可能性が除去される。

  OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すアプリケーションを利用するとしており、また OE.SESSION により管理者モード、サービスモードの操作終了後にはログオフする運用が奨励されるため、O.CONFIG は十分サポートされている。

  したがって本脅威は十分対抗されている。

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は適用されていない。

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の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（Functionaly 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**

FIA_EID　アクセス先の承認	1

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 環境エンティティを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*] : ***コニカミノルタ暗号仕様標準***
[割付: *暗号鍵生成アルゴリズム*] : ***コニカミノルタ HDD 暗号鍵生成アルゴリズム***
[割付: *暗号鍵長*] : ***128bit***
下位階層 : なし **依存性** : FCS_CKM.2 or FCS_COP.1（適用しない）、FCS_CKM.4（適用しない）

6.1.1.2. 利用者データ保護

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

表 2　ボックスアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*ボックスファイル*	*・ダウンロード* *・印刷* *・送信（E-mail 送信、FTP 送信、SMB 送信）*

FDP_ACC.1[2]　　サブセットアクセス制御
FDP_ACC.1.1[2]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 3　機密文書プリントファイルアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***機密文書プリントファイルアクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[2]）

表 3　機密文書プリントファイルアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*機密文書プリントファイル*	*印刷*

FDP_ACC.1[3]　　サブセットアクセス制御
FDP_ACC.1.1[3]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 4　管理者モードアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***管理者モードアクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[3]）

表 4 管理者モードアクセス制御 操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*・SMTP サーバグループオブジェクト* *・DNS サーバグループオブジェクト* *・MFP アドレスグループオブジェクト* *・送信宛先データファイルオブジェクト*	*・ 設定*

FDP_ACF.1[1] セキュリティ属性によるアクセス制御
FDP_ACF.1.1[1]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: *＜サブジェクト＞ ＜サブジェクト属性＞* *・利用者を代行するタスク ⇒ ・ボックス属性（ボックス ID）* --- *＜オブジェクト＞ ＜オブジェクト属性＞* *・ボックスファイル ⇒ ・ボックス属性（ボックス ID）*
[割付: *アクセス制御 SFP*]: ***ボックスアクセス制御***
FDP_ACF.1.2[1]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]: ***ボックス属性（ボックス ID）が関連付けられる利用者を代行するタスクは、サブジェクト属性のボックス属性と一致するボックス属性を有するボックスファイルに対して、ダウンロード、印刷、送信（E-mail 送信、FTP 送信、SMB 送信）操作をすることが許可される。***
FDP_ACF.1.3[1]
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]: ***なし。***
FDP_ACF.1.4[1]
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし。***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3（適用しない）

FDP_ACF.1[2] セキュリティ属性によるアクセス制御
FDP_ACF.1.1[2]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、*

SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]： ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　　⇒　・ファイル属性（機密文書内部制御 ID）*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・機密文書プリントファイル　　⇒　・ファイル属性（機密文書内部制御 ID）***
[割付: *アクセス制御 SFP*]： ***機密文書プリントファイルアクセス制御***
FDP_ACF.1.2[2]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]： ***ファイル属性（機密文書内部制御 ID）を持つ利用者を代行するタスクは、ファイル属性（機密文書内部制御 ID）と一致するファイル属性（機密文書内部制御 ID）を持つ機密文書プリントファイルに対して印刷操作を許可される。***
FDP_ACF.1.3[2]
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]： ***なし。***
FDP_ACF.1.4[2]
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]： ***なし。***
下位階層　：　なし 依存性　：　FDP_ACC.1（FDP_ACC.1[2]）、FMT_MSA.3（FMT_MSA.3）

FDP_ACF.1[3]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[3]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]： ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　　⇒　・管理者属性*** --- ***＜オブジェクト＞*** ***・SMTP サーバグループオブジェクト*** ***・DNS サーバグループオブジェクト*** ***・MFPアドレスグループオブジェクト[6]*** ***・送信宛先データファイルオブジェクト*** ***※ オブジェクト属性は、存在しない。***
[割付: *アクセス制御 SFP*]： ***管理者モードアクセス制御***
FDP_ACF.1.2[3]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、*

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

制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]: ***・管理者属性を持つ利用者を代行するタスクだけに、SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクト、送信宛先データファイルオブジェクトを設定操作することが許可される。***
FDP_ACF.1.3[3]
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]: ***なし。***
FDP_ACF.1.4[3]
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし。***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[3]）、FMT_MSA.3（適用しない）

FDP_RIP.1 サブセット残存情報保護
FDP_RIP.1.1
TSF は、以下のオブジェクト[選択: *への資源の割当て、からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト*]。
[選択: *への資源の割当て、からの資源の割当て解除*]: ***からの資源の割当解除***
[割付: *オブジェクトのリスト*]: ***・全ボックスファイル*** ***・スワップデータファイル*** ***・オーバーレイ画像ファイル*** ***・HDD 蓄積画像ファイル***
下位階層 : なし **依存性** : なし

6.1.1.3. 識別と認証

FIA_AFL.1[1] 認証失敗時の取り扱い
FIA_AFL.1.1[1]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*]: ***・サービスモードにアクセスする際の認証*** ***・サービスコ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:正の整数値]：3***
FIA_AFL.1.2[1]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *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＞***

・認証中であれば、サービスモードへの認証状態からログオフし、サービスコードを利用する認証機能をロックする。 ***・認証中でなければ、サービスコードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***TOE の起動処理を行う。***
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:正の整数値]：3***
FIA_AFL.1.2[2]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *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＞*** ***・認証中であれば、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。*** ***・認証中でなければ、管理者パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***TOE の起動処理を行う。***
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*]: ***機密文書プリントファイルにアクセスする際の認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付:正の整数値]：3***
FIA_AFL.1.2[3]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *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＞*** ***当該機密文書プリントファイルへのアクセスを拒否し、当該機密文書プリントファイルに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供されるロック解除機能を実行する。***
下位階層 : なし
依存性 : FIA_UAU.1（FIA_UAU.2[3]）

FIA_AFL.1[4]　　認証失敗時の取り扱い
FIA_AFL.1.1[4]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*]: ***ボックスにアクセスする際の認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付:正の整数値]：3***
FIA_AFL.1.2[4]
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *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＞*** ***当該ボックス及び当該ボックス内のボックスファイルへのアクセスを拒否し、当該ボックスに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***・管理者モード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[4]）

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

FIA_SOS.1[1]　　秘密の検証
FIA_SOS.1.1[1]
TSF は、秘密 ***（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*]: ***・桁数　：8 桁*** ***・文字種：10 文字以上の中から選択可能*** ***・規則　：同一の文字だけで構成されていない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[2]　　秘密の検証

FIA_SOS.1.1[2]
TSF は、秘密 ***（機密文書パスワード、ボックスパスワード）*** 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*** ***・規則　：同一の文字だけで構成されていない。***
下位階層　:　なし
依存性　:　なし

FIA_SOS.1[3]　秘密の検証

FIA_SOS.1.1[3]
TSF は、秘密 ***（HDD ロックパスワード、暗号鍵ワード）*** 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：82 文字以上の中から選択可能*** ***・規則　：同一の文字だけで構成されていない。***
下位階層　:　なし
依存性　:　なし

FIA_SOS.1[4]　秘密の検証

FIA_SOS.1.1[4]
TSF は、秘密 ***（サービスコード）*** 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：12 文字以上の中から選択可能*** ***・規則　：同一の文字だけで構成されていない。***
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 調停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）*** に自分自身を認証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 調停アクションを許可する前に、各利用者 ***（管理者）*** に自分自身を認証することを要求しなければならない。
下位階層　:　FIA_UAU.1
依存性　:　FIA_UID.1（FIA_UID.2[2]）

FIA_UAU.2[3]　　アクション前の利用者認証
FIA_UAU.2.1[3]
TSF は、その利用者 ***(機密文書プリントファイルの利用を許可されたユーザ)*** を代行する他の TSF 調停アクションを許可する前に、各利用者 ***(機密文書プリントファイルの利用を許可されたユーザ)*** に自分自身を認証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[3]）

FIA_UAU.2[4]　　アクション前の利用者認証
FIA_UAU.2.1[4]
TSF は、その利用者 ***(ボックスの利用を許可されたユーザ)*** を代行する他の TSF 調停アクションを許可する前に、各利用者 ***(ボックスの利用を許可されたユーザ)*** に自分自身を認証することを要求しなければならない。
下位階層　：　FIA_UAU.1
依存性　：　FIA_UID.1（FIA_UID.2[4]）

FIA_UAU.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変更する場合*** ***・サービスエンジニアがサービスコードを　変更する場合*** ***・管理者が HDD ロック機能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***
下位階層　：　なし
依存性　：　なし

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

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 調停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)*** に自分自身を識別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 調停アクションを許可する前に各利用者 ***（管理者）*** に自分自身を識別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 ***（機密文書プリントファイルの利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に各利用者 ***（機密文書プリントファイルの利用を許可されたユーザ）*** に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[4]　　アクション前の利用者識別
FIA_UID.2.1[4]
TSF は、その利用者 ***（ボックスの利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に各利用者 ***（ボックスの利用を許可されたユーザ）*** に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_USB.1　　利用者・サブジェクト結合
FIA_USB.1.1
TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: *利用者セキュリティ属性のリスト*]
[割付: *利用者セキュリティ属性のリスト*]： ***・ボックス属性（ボックス ID）*** ***・ファイル属性（機密文書内部制御 ID）*** ***・管理者属性***
FIA_USB.1.2
TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: *属性の最初の関連付けに関する規則*]
[割付: *属性の最初の関連付けに関する規則*]： ***・ボックス属性の場合、ボックスに対するアクセスにおいて認証された際に、利用者を代行するタスクに当該ボックスのボックス ID を関連付ける。*** ***・ファイル属性の場合、機密文書プリントファイルに対するアクセスにおいて認証された際に、利用者を代行するタスクに、当該機密文書プリントファイルの機密文書内部制御 ID を関連付ける。*** ***・管理者属性の場合、管理者として認証された際に、利用者を代行するタスクに管理者属性を関連付ける。***
FIA_USB.1.3
TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: *属性の変更に関する規則*]
[割付: *属性の変更に関する規則*]： ***なし***
下位階層　：　なし
依存性　：　FIA_ATD.1

6.1.1.4. セキュリティ管理

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

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

FMT_MSA.3 静的属性初期化
FMT_MSA.3.1
TSF は、その SFP を実施するために使われるセキュリティ属性（***機密文書内部制御 ID***）として、[選択: *制限的、許可的：から一つのみ選択、[割付：その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[選択: *制限的、許可的：から一つのみ選択、[割付：その他の特性]*] : ***[割付：その他の特性]：一意に識別される***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*] ***機密文書プリントファイルアクセス制御***
FMT_MSA.3.2
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***該当なし***
下位階層 : なし
依存性 : FMT_MSA.1（適用しない）、FMT_SMR.1（FMT_SMR.1[3]）

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*]: ***当該ボックスのボックスパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***・そのボックスの利用を許可されたユーザ*** ***・管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

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*** ***・暗号鍵ワード*** ***・HDD ロックパスワード***
[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***
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[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*]: ***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]*]: ***問い合わせ、[割付: その他の操作]：初期化***
[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*]: ***サービスコード***

[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*]: ***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[5] TSF データの管理

FMT_MTD.1.1[5]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・機密文書パスワード*** ***・ボックスパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***ユーザ***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（適用しない）

FMT_SMF.1 管理機能の特定

FMT_SMF.1.1
TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付： *TSF によって提供されるセキュリティ管理機能のリスト*]。
[割付： *TSF によって提供されるセキュリティ管理機能のリスト*]: ***・管理者によるセキュリティ強化機能の停止機能*** ***・管理者による機密文書不正アクセス検出値の消去機能*** ***・管理者によるボックス不正アクセス検出値の消去機能*** ***・管理者による管理者パスワードの改変機能*** ***・管理者によるボックスパスワードの改変機能*** ***・管理者によるボックス ID 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*** ***・管理者による暗号鍵ワードの改変機能*** ***・管理者による暗号化基板にて実現する暗号化機能を利用するための機能の動作設定機能*** ***・サービスエンジニアによるサービスコードの改変機能*** ***・サービスエンジニアによる管理者パスワードの問い合わせ機能*** ***・サービスエンジニアによる管理者パスワードの初期化機能*** ***・ユーザによるボックスパスワードの登録機能*** ***・ユーザによるボックス ID の登録機能*** ***・ユーザによるボックスの登録機能*** ***・ボックスの利用を許可されたユーザによる当該ボックスのボックスパスワードの改変機能*** ***・ボックスの利用を許可されたユーザによる当該ボックスのボックス ID の改変機能***
下位階層 : なし
依存性 : なし

FMT_SMR.1[1] セキュリティ役割

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

サービスエンジニア
FMT_SMR.1.2[1]
TSF は、利用者を役割に関連づ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づけなければならない。
下位階層　：　なし
依存性　：　FIA_UID.1（FIA_UID.2[2]）

FMT_SMR.1[3]　セキュリティ役割
FMT_SMR.1.1[3]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： *機密文書プリントファイルの利用を許可されたユーザ*
FMT_SMR.1.2[3]
TSF は、利用者を役割に関連付けなければならない。
下位階層　：　なし
依存性　：　FIA_UID.1（FIA_UID.2[3]）

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

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＞* *・機密文書プリントファイル*

・*全ボックスファイル* ・*スワップデータファイル* ・*オーバーレイ画像ファイル* ・***HDD** 蓄積画像ファイル* *＜TSF データ＞* ・***HDD** ロックパスワード* ・*暗号鍵ワード* ・*管理者パスワード* ・*ボックスパスワード*
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　　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 *（**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
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

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*] ***暗号化基板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

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
	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

セキュリティ対策方針 / セキュリティ機能要件	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CRYPT-KEY	O.CHECK-HDD	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	※ set.admin	※ set.service
set.admin	●	●	●								
set.service	●	●	●								
FCS_CKM.1						●					
FDP_ACC.1[1]	●										
FDP_ACC.1[2]		●									
FDP_ACC.1[3]			●								
FDP_ACF.1[1]	●										
FDP_ACF.1[2]		●									
FDP_ACF.1[3]			●								
FDP_RIP.1					●						
FIA_AFL.1[1]											●
FIA_AFL.1[2]										●	
FIA_AFL.1[3]		●									
FIA_AFL.1[4]	●										
FIA_ATD.1	●	●	●								
FIA_SOS.1[1]										●	
FIA_SOS.1[2]	●	●									
FIA_SOS.1[3]			●								
FIA_SOS.1[4]											●
FIA_UAU.2[1]											●
FIA_UAU.2[2]										●	
FIA_UAU.2[3]		●									
FIA_UAU.2[4]	●										
FIA_UAU.6			●							●	●
FIA_UAU.7	●	●								●	●
FIA_UID.2[1]											●
FIA_UID.2[2]										●	
FIA_UID.2[3]		●									

セキュリティ対策方針 / セキュリティ機能要件	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CRYPT-KEY	O.CHECK-HDD	O.CRYPTO-CAPABILITY	O.LOCK-HDD-CAPABILITY	※ set.admin	※ set.service
FIA_UID.2[4]	●										
FIA_USB.1	●	●	●								
FMT_MOF.1			●								
FMT_MSA.1	●										
FMT_MSA.3		●									
FMT_MTD.1[1]	●										
FMT_MTD.1[2]										●	
FMT_MTD.1[3]										●	
FMT_MTD.1[4]											●
FMT_MTD.1[5]	●	●									
FMT_SMF.1	●	●	●							●	●
FMT_SMR.1[1]										●	●
FMT_SMR.1[2]	●		●							●	
FMT_SMR.1[3]		●									
FMT_SMR.1[4]	●										
FAD_RIP.1				●							
FIA_EID.1							●				
FIT_CAP.1[1]								●			
FIT_CAP.1[2]									●		

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

6.2.1.2. 十分性

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

- **O.BOX（ボックスアクセス制御）**

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

＜ボックスアクセス制御＞
ボックス内のボックスファイルを操作するには、そのボックスの利用を許可されたユーザである必要があるが、FIA_UID.2[4]、FIA_UAU.2[4]により、そのボックスの利用を許可されたユーザであることを識別認証される。
FIA_AFL.1[4]により、不成功認証が 3 回に達すると、当該ボックスに対する認証機能をロックする。このロック状態は、TOE の起動、または管理者の解除操作によって解除される。

認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“*”を返し、認証をサポートする。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにボックス ID が関連付けられると、FDP_ACC.1[1]、FDP_ACF.1[1]により、サブジェクト属性のボックス ID と一致するオブジェクト属性を持つボックスファイルに対して、ダウンロード、印刷、送信（E-mail 送信、FTP 送信、SMB 送信）操作が許可される。

＜ボックスの管理＞
FMT_MTD.1[1]により、ボックスパスワードの変更は、管理者及びそのボックスの利用を許可されたユーザだけに許可される。FIA_SOS.1[2]により、ボックスパスワードの品質が検証される。
FMT_MTD.1[5]により、ボックスパスワードの登録はユーザだけに許可される。
また FMT_MSA.1 により、ボックス ID の変更は、管理者及びそのボックスの利用を許可されたユーザだけに許可される。

＜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[2]により管理者、FMT_SMR.1[4]によりそのボックスの利用を許可されたユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

＜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

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

- **O.SECURE-PRINT（機密文書プリントファルアクセス制御）**

本セキュリティ対策方針は、機密文書プリントファイルの印刷をその機密文書プリントファイルの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜機密文書プリントファイルアクセス制御＞
機密文書プリントファイルを印刷するには、その機密文書プリントファイルの利用を許可されたユーザである必要があるが、FIA_UID.2[3]、FIA_UAU.2[3]により、その機密文書プリントファイルの利用を許可されたユーザであることを識別認証される。
FIA_AFL.1[3]により、不成功認証が 3 回に達すると、当該ボックスに対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
認証には、FIA_UAU.7 により、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_ATD.1、FIA_USB.1 により、利用を代行するタスクに機密文書内部制御 ID が関連付けられると、FDP_ACC.1[2]、FDP_ACF.1[2]により、サブジェクト属性の機密文書内部制御 ID と一致するオブジェクト属性を持つ機密文書プリントファイルに対して、印刷操作が許可される。
なお機密文書内部制御 ID は、FMT_MSA.3 より機密文書プリントファイルの登録時に一意に識別される値が与えられている。

＜機密文書パスワード＞
FMT_MTD.1[5]により、認証に利用されるセキュリティ文書パスワードの登録はユーザだけに許

可される。FIA_SOS.1[2]により機密文書プリントパスワードの品質は検証される。

＜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[3]によりユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

＜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

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

- **O.CONFIG（管理機能へのアクセス制限）**

本セキュリティ対策方針は、SMTP サーバに関係する設定、DNS サーバに関係する設定、MFP アドレスに関する設定、セキュリティ強化機能に関係する設定を管理者及びサービスエンジニアに制限しており、一連の設定機能や管理機能に対してアクセスを制限するための諸要件が必要である。

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

＜セキュリティ強化機能の操作制限＞
セキュリティ強化機能を停止設定は、FMT_MOF.1 により、管理者だけに許可される。

＜HDD ロックパスワード、暗号鍵ワードの管理＞
FIA_ATD.1、FIA_USB.1 により利用を代行するタスクに管理者属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、利用者を代行するタスクは、HDD ロックパスワードオブジェクト、暗号鍵ワードオブジェクトに対する設定操作が許可される。FIA_SOS.1[3]により HDD ロックパスワード、暗号鍵ワードの品質が検証される。なお HDD ロックパスワード、暗号鍵ワードが変更される際は、FIA_UAU.6 により、登録済み HDD ロックパスワード、暗号鍵ワードと照合することによって管理者であることを再認証し、再認証された場合に変更が許可される。

＜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[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。

＜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

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

- **O.OVERWRITE-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、NVRAM の管理者パスワードなど初期値に戻すとしており、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。

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

- **O.OVERWRITE-FILE（ファイル単位の上書き削除）**

本セキュリティ対策方針は、HDD に書き込まれて不要となった画像ファイルを抹消するとしており、削除に関係する諸要件が必要である。
FDP_RIP.1 により、対象とする情報（全ボックスファイル、スワップデータファイル、オーバーレイ画像ファイル、HDD 蓄積画像ファイル）が資源からの割当が解除されると、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。

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

- **O.CRYPT-KEY（暗号鍵生成）**

本セキュリティ対策方針は、暗号化基板が設置されている場合に、HDD に書き込むすべての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を利用し、128bit の暗号鍵を生成する。
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。

- **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 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.CRYPTO-CAPABILITY（HDD の暗号化）**

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基板により、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、暗号化基板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。
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.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、HDD ロック機能を解除す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。

以下には、(1)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（set.admin）、(2)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（set.service）のセットをまとめる。

- ***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、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[2]により、不成功認証が 3 回に達すると、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。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される。

＜管理者の認証情報の管理など＞
管理者パスワードは、FIA_SOS.1[1]により品質が検証される。管理者パスワードの変更は、FMT_MTD.1[2]により、管理者に制限される。管理者が管理者パスワードを変更する場合は、FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[2]により、不成功認証が 3 回に達すると、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される。
また管理者のパスワードの問い合わせ、初期化は、FMT_MTD.1[3]によりサービスエンジニアに制限される。

＜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、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[1]により、不成功認証が 3 回に達すると、サービスコ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される。

＜サービスエンジニアの認証情報の管理など＞
サービスコードは、FIA_SOS.1[4]により、品質が検証される。サービスコードの変更は、FMT_MTD.1[4]により、サービスエンジニアに制限される。また FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[1]により、不成功認証が 3 回に達すると、サービスエンジニアの認証状態を解除して、サービスコ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。

なお FPT_RVM.1、FPT_SEP.1 は、直接的にはセキュリティ対策方針と関連付けられないセキュリティ機能要件であるので、上記の十分性の説明に含まれていないが、後述される相互サポートの中で上記の十分性の説明に含まれるセキュリティ機能要件をサポートすることが示されている。この 2 つのセキュリティ機能要件は、2 つのセキュリティ機能要件がそれぞれサポートしているセキュリティ機能要件が対応するセキュリティ対策方針と関連することになるため、結果的にセキュリティ対策方針との対応関係は明らかである。

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_CKM.2 or FCS_COP.1 を適用しない理由＞ 暗号操作は FIT_CAP.1[1]により IT 環境によって行われる。TSF はその能力を利用するのみであり、配布及び暗号操作の必要性はない。 ＜FCS_CKM.4 を適用しない理由＞ 暗号鍵は、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。
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1[1]、 ＜FMT_MSA.3 を適用しない理由＞ 生成されるオブジェクトであるボックスファイルは、識別子であるボックス ID 以外に管理されるべきセキュリティ属性は存在せず、何らかの特性をもったデフォルト値がオブジェクト属性として与えられるという事象を規定する必要性がない。 なおボックスファイルに関連付けられるボックス ID はユーザ操作で指定する値であり、FMT_MSA.3 で想定する事象に該当しない。（ボックスファイル生成時に選択可能なボックスを特定ユーザに対して制限する仕組みは必要ない仕組みであるため。）
FDP_ACF.1[2]	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3
FDP_ACF.1[3]	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1[3] ＜FMT_MSA.3 を適用しない理由＞ オブジェクト属性が存在しないため、本要件を適用する必要性はない。
FDP_RIP.1	なし	N/A
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4]
FIA_ATD.1	なし	N/A
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.6	なし	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1、 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1[1] FMT_SMF.1 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_SMR.1[3] ＜FMT_MSA.1 を適用しない理由＞ 一意に識別される内部制御 ID であり、一度割り当てられた後に変更、削除といった管理を必要としないため。
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]
FMT_MTD.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]
FMT_MTD.1[5]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 ＜FMT_SMR.1 を適用しない理由＞ パスワード登録前の段階では利用者の制限は無い。またパスワード登録後に役割を管理、維持される。この段階における役割の維持の必要性はない。
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[4]
FAD_RIP.1	なし	N/A
FIA_EID.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[1]	なし	N/A
FIT_CAP.1[2]	なし	N/A

6.2.2. IT セキュリティ保証要件根拠

本 TOE は、物理的・人的・接続的に十分なセキュリティを確保した環境に設置され利用されるが、本 TOE を利用する環境において十分な実効性を保証する必要がある。一般的な商用事務製品として機能仕様、上位レベル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.BOX（ボックス機能）	ボックス機能
7.4	F.PRINT（機密文書プリント機能）	機密文書プリント機能
7.5	F.OVERWRITE-FILE（残存情報上書き削除機能）	その他の機能
7.6	F.OVERWRITE-ALL（全領域上書き削除機能）	管理者機能
7.7	F.CRYPT（暗号鍵生成機能）	その他の機能
7.8	F.SUPPORT-CRYPTO（暗号化基板動作サポート機能）	暗号化基板の活用
7.9	F.VALIDATION-HDD（HDD 検証機能）	HDD ロック機能の活用
7.10	F.SUPPORT-HDD（HDD ロック動作サポート機能）	HDD ロック機能の活用
7.11	F.RESET（認証失敗回数リセット機能）	その他の機能

7.1. F.ADMIN（管理者機能）

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

7.1.1. 管理者識別認証機能

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

- 表 9 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パスワード認証メカニズムを提供する。
- 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。
- 認証に成功すると、認証失敗回数をリセットする。
- 管理者パスワードを利用する各認証機能において通算 3 回目となる認証失敗を検知すると、管理者パスワードを利用するすべての認証機能をロックする。（管理者モードへのアクセスを拒否する。
- 認証機能のロックは、F.RESET 機能が動作して解除する。

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

表 9 パスワードに利用されるキャラクタと桁数

対象	桁数	キャラクタ
サービスコード	8 桁	合計 12 文字の中から選択可能 （数字、一部記号）
管理者パスワード	8 桁	合計 10 文字の中から選択可能 （数字）

対象	桁数	キャラクタ
ボックスパスワード 機密文書パスワード	8 桁	合計 92 文字の中から選択可能 （英、数、記号（一部除く））
HDD ロックパスワード 暗号鍵ワード	20 桁	合計 82 文字の中から選択可能 （英、数、記号（一部除く））

7.1.2. 管理者モードにて提供される機能

管理者モードへのアクセス要求において管理者識別認証機能により、管理者として識別認証されると、利用者を代行するタスクに管理者属性が関連づけられ、以下の操作、機能の利用が許可される。
FIA_ATD.1、FIA_USB.1 は上記により実現される。

7.1.2.1. 管理者パスワードの変更

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

- 表 9 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パスワード認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 管理者パスワードを利用する各認証機能において通算 3 回目となる認証失敗を検知すると、パネルからアクセスする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。）
- 認証機能のロックは、F.RESET 機能が動作して解除する。
- 新規設定される管理者パスワードは以下の品質を満たしていることを検証する。
  - 表 9 の管理者パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

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

7.1.2.2. ボックスパスワードの変更

PUBLIC 以外のボックスのボックスパスワードを変更する。新しく設定されるボックスパスワードが以下の
品質を満たしていることを検証する。

- 表 9 のボックスパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

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

7.1.2.3. ボックス ID の変更

ボックスのボックス ID を PUBLIC 以外で未登録のものへ変更する。
以上により FMT_MSA.1、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.2.4. ロックの解除

すべての機密文書**プリント、及びボックス**の認証失敗回数を 0 クリアする。
- アクセスがロックされている機密文書プリントが存在すれば、ロックが解除される。

すべてのボックスの認証失敗回数を 0 クリアする。
- アクセスがロックされているボックスが存在すれば、ロックが解除される。

以上により FIA_AFL.1[3]、FIA_AFL.1[4]、FMT_SMR.1[2]が実現される。

7.1.2.5. ネットワークの設定

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

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

7.1.2.6. HDD ロック機能の動作設定機能

＜**動作**設定 ON＞
OFF から ON にする場合、新しく設定される HDD ロックパスワードが以下の品質を満たしていることを検証する。
- 表 9 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。

＜動作設定 OFF＞
ON から OFF にする。（暗号化機能が ON の場合に限り許可される。）
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ると OFF にする。
- 表 9 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。

＜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 9 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 9 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。

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

7.1.2.7. 暗号化機能の動作設定

暗号化基板オプションが MFP に装着されている場合のみ操作可能。

＜動作設定　ON＞
OFF から ON にする場合、新しく設定される暗号鍵ワードが以下の品質を満たしていることを検証し、F.CRYPT が実行される。
- 表 9 の暗号鍵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。

＜動作設定　OFF＞
ON から OFF にする。（HDD ロック機能が ON の場合に限り許可される。）
現在設定される暗号鍵ワードを使い、管理者であることを再認証されると OFF にする。
- 表 9 に示されるキャラクタからなる暗号鍵ワードを照合する暗号鍵ワード照合メカニズムを提供する。
- 照合では、暗号鍵ワード入力のフィードバックに 1 文字毎“＊”を返す。

＜暗号鍵ワード変更＞
暗号鍵ワードを変更する。現在設定される暗号鍵ワードを使い、管理者であることを再認証され、且つ新規設定される暗号鍵ワードが品質を満たしている場合に変更し、F.CRYPT が実行される。
- 表 9 に示されるキャラクタからなる暗号鍵ワードを照合する暗号鍵ワード照合メカニズムを提供する。
- 照合では、暗号鍵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鍵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 の暗号鍵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]、FIA_UAU.7、FIA_UAU.6、FMT_MTD.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.2.8. 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_MTD.1[2]、FMT_SMF.1、FMT_SMR.1[2]が実現される。

7.1.2.9. セキュリティ強化機能の動作設定

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
  セキュリティ強化機能の有効、無効を設定する機能。
- 全データ領域上書き削除機能
  全データ領域の上書き削除の実行により、セキュリティ強化機能の設定を無効にする。

以上により FMT_MOF.1、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、サービスコ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からなるサービスコードにより認証するサービスコード認証メカニズムを提供する。
- サービスコ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。
- サービスコードを利用する各認証機能において通算 3 回目となる認証失敗を検知すると、サービスコ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。)
- 認証機能のロックは、F.RESET 機能が動作して解除する。

以上により FIA_AFL.1[1]、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。

(1)サービスコードの変更

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からなるサービスコードにより再認証するサービスコード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、サービスコード入力のフィードバックに 1 文字毎“＊”を返す。
- サービスコードを利用する各認証機能において通算 3 回目となる認証失敗を検知すると、パネルからアクセスするサービスモードをログオフし、サービスコ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。)
- 認証機能のロックは、F.RESET 機能が動作して解除する。
- 新規設定されるサービスコードは以下の品質を満たしていることを検証する。
  - 表 9 のサービスコ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_AFL.1[1]、FIA_SOS.1[4]、FIA_UAU.6、FIA_UAU.7、FMT_MTD.1[4]、FMT_SMF.1、FMT_SMR.1[1]が実現される。

(2) 管理者パスワードの初期化

管理者パスワードを初期化する。工場出荷時の初期値に初期化される。

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

7.3. F.BOX（ボックス機能）

F.BOX とは、パネル、またはクライアント PC からボックスに対するアクセスにおいてボックスの利用を許可された者であることを識別認証し、ボックスファイルへの操作を制御するボックスアク

セス制御機能など、ボックスに関係するセキュリティ機能である。

7.3.1. ボックスの登録機能

クライアント PC からのユーザ操作によって、ボックス登録操作が提供される。ボックス ID（未登録のもの)、ボックスパスワードを適切に指定すると指定されたボックスを登録する。

- ボックスパスワードが以下の条件を満たすことを検証する。
  - 表 9 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

  以上により FIA_SOS.1[2]、FMT_MTD.1[5]、FMT_SMF.1 が実現される。

7.3.2. ボックスへのアクセスにおける識別認証機能

個々のボックスへのアクセス要求に対して､アクセスする利用者をそれぞれ当該ボックスの利用を許可されたユーザであることを認証する。

- 表 9 に示されるキャラクタからなるボックスパスワードにより認証するボックスパスワード認証メカニズムを提供する。
- ボックスパスワード入力のフィードバックに 1 文字毎“*”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 当該ボックスに対して、通算 3 回目となる認証失敗を検知すると、当該ボックスに対する認証機能をロックする。
- 認証機能のロックは､F.ADMIN のボックスに対するロック解除機能を実行する､または F.RESET 機能が動作して解除する。

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

(1)パネルからのボックス内のボックスファイルに対するアクセス制御

ユーザを代行するタスクは、そのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、サブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、送信（E-mail 送信、FTP 送信、SMB 送信）操作を行うことを許可される。

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

以下は当該ボックスの利用を許可されたユーザが当該ボックス内のボックスファイル操作において提供される機能であり、クライアント PC からの実行に伴い認証が要求される。

- 表 9 に示されるキャラクタからなるボックスパスワードにより認証するボックスパスワード認証メカニズムを提供する。
- 認証に成功すると、当該ボックスの認証失敗回数をリセットする。
- ボックスパスワードを利用する各認証機能において通算 3 回目となる認証失敗を検知すると、ボックス識別認証ドメインをログオフし、ボックスパスワードを利用するすべての認証機能をロックする。（当該ボックスのボックス識別認証ドメインへのアクセスを拒否する。）
- 認証機能のロックは､F.ADMIN のボックスに対するロック解除機能を実行する､または F.RESET 機能が動作して解除する。

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

(2)クライアント PC からのボックス内のボックスファイルに対するアクセス制御

ユーザを代行するタスクは、そのボックスの「ボックス ID」がボックス属性としてタスクに関連

づけられる。このタスクは、サブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対してダウンロードを行うことを許可される。
以上により FDP_ACC.1[1]、FDP_ACF.1[1]、FIA_ATD.1、FIA_USB.1 が実現される。

(3) クライアント PC からのボックスパスワードの変更
ボックスのボックスパスワードを変更する。
- 新規設定されるボックスパスワードは以下の品質を満たしていることを検証する。
  - 表 9 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

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

(4) クライアント PC からのボックス ID の変更
ボックスのボックス ID を PUBLIC 以外で未登録のものへ変更する。
以上により FMT_MSA.1、FMT_SMF.1、FMT_SMR.1[4]が実現される。

7.4. F.PRINT（機密文書プリント機能）

F.PRINT とは、パネルからの機密文書プリントファイルへのアクセスに対して機密文書プリントファイルの利用を許可されたユーザであることを認証し、認証後に当該機密文書プリントファイルの印刷を許可するアクセス制御機能など機密文書プリントに関係する一連のセキュリティ機能である。

7.4.1. 機密文書パスワードによる認証機能

機密文書プリントファイルへのアクセス要求に対して、アクセスする利用者を当該機密分文書プリントファイルの利用を許可されたユーザであることを認証する。
- 表 9 に示されるキャラクタからなる機密文書パスワードにより認証する機密文書パスワード認証メカニズムを提供する。
- 機密文書パスワード入力のフィードバックに 1 文字毎“*”を返す。
- 当該機密文書プリントファイルに対して、通算 3 回目となる認証失敗を検知すると、当該機密分文書プリントファイルに対する認証機能をロックする。
- ロック状態は、F.ADMIN の機密文書プリントファイルに対するロック解除機能を実行して解除する。

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

7.4.2. 機密文書プリントファイルに対するアクセス制御機能

認証されると、機密文書プリントファイルアクセス制御が動作する。
- 識別認証されたユーザを代行するタスクは、ファイル属性に、認証された機密文書プリントファイルの機密文書 ID を持つ。
- このタスクは、このファイル属性と一致するファイル属性を持つ機密文書プリントファイルに対して印刷を許可される。

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

7.4.3. 機密文書プリントファイルの登録機能

(1) 機密文書パスワードの登録

機密文書プリントファイルの登録要求において、登録される機密文書パスワードが以下の条件を満たすことを検証する。

- 表 9 のボックスパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

(2)機密文書内部制御 ID の付与

機密文書プリントファイルの登録要求において、機密文書パスワードの検証が完了すると、一意に識別される機密文書内部制御 ID を当該機密文書プリントファイルに設定する。

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

7.5. F.OVERWRITE-FILE（残存情報上書き削除機能）

F.OVERWRITE とは、以下の場合においてファイルを削除する際に、一般的な削除（ファイルアクセスのための管理領域の開放）だけではなく、HDD のデータ領域を上書き削除する機能である。

＜残存情報上書き削除が起動する事象＞

- コピー、プリントのジョブ完了。
  - 上書き削除対象：スワップデータファイル
- ユーザ操作による削除。
  - 上書き削除対象：全ボックスファイル、オーバーレイ画像ファイル、HDD 蓄積画像ファイル
- 期限経過による自動削除の起動。
  - 上書き削除対象：全ボックスファイル、スワップデータファイル（機密文書プリントファイルのスワップデータのみが該当する）
- 電源 OFF された際にジョブが実行中であった場合で、電源が ON された場合。
  - 上書き削除対象：スワップデータファイル

削除方式は、「0x00 ⇒ 0x00 ⇒ 0x00」で対象領域を上書する。

以上により FDP_RIP.1 が実現される。

7.6. 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対象は以下の通りである。

＜削除される対象：HDD＞

- 全ボックスファイル
- スワップデータファイル
- オーバーレイ画像ファイル
- HDD 蓄積画像ファイル
- ボックスパスワード

＜削除される対象：NVRAM[7]＞

[7] NVRAM 内のサービスコード、HDD ロックパスワード、暗号鍵ワードも初期化されるが、これら TSF データは削除されずとも返却及び廃棄後に値を確認する手段は存在しないため、削除必須対象物には含まれない。

- 送信宛先データファイル

＜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、書き込む回数など削除方式は、
「0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証」が実行される。
以上により FAD_RIP.1 が実現される。

7.7. F.CRYPT（暗号鍵生成機能）

F.CRYPT とは、米国標準技術局：NIST が、標準（FIPS 180-1）として指定した SHA-1 アルゴリズムを利用し、HDD に書き込まれるすべてのデータを暗号化するための暗号鍵を生成する。
F.ADMIN においてアクセス制限される暗号化機能の動作設定において暗号鍵ワードが決定されると、SHA-1 アルゴリズムを用いて暗号鍵ワードから 128bit 長の暗号鍵を生成する。
以上により FCS_CKM.1 が実現される。

7.8. F.SUPPORT-CRYPTO（暗号化基板動作サポート機能）

F.SUPPORT-CRYPTO とは、TOE から暗号化基板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基板にセットし、暗号化基板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基板にセットし、暗号化基板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。

7.9. 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 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 が実現される。

7.10. 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。

7.11. F.RESET（認証失敗回数リセット機能）

F.RESET とは、管理者認証を始めとした各認証機能においてカウントされる認証失敗回数をリセットする機能である。（ロックの有無と関係しない。）

主電源が ON される、または停電などから復帰した場合など TOE の起動により本機能は動作する。起動すると、以下の認証失敗回数をリセットする。
- 管理者の認証に対する失敗回数
- サービスエンジニアの認証に対する失敗回数
- ボックスの認証に対するボックスそれぞれにおいて保持される失敗回数

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

---以上---