bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)

# *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：1.10

発行日：2006年9月8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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

**＜更新履歴＞**

| 日付 | Ver | 担当部署 | 承認者 | 確認者 | 作成者 | 更新内容 |
|---|---|---|---|---|---|---|
| 2005/09/12 | 1.00 | 制御第12開発部 | 多田 | 橋本 | 加藤 | 初版 |
| 2006/04/04 | 1.01 | 制御第12開発部 | 多田 | 橋本 | 加藤 | 仕様改訂に伴う変更 |
| 2006/05/11 | 1.02 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・TOE識別を明示<br>・TOEのVer変更、誤植修正 |
| 2006/06/02 | 1.03 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・サービスの諸機能がセキュリティ的に一切不要となったため、3章以降の関係記載をすべて削除<br>・TOEの識別方法を再度変更<br>・SNMPv1のWrite権限が強化モードで禁止される説明を追加（2章）<br>・オートログアウト機能をセキュリティ機能としての位置付けから変更（通常機能） |
| 2006/06/05 | 1.04 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・遠隔診断機能の詳細修正（サービスの諸機能復帰）<br>・誤植修正 |
| 2006/06/13 | 1.05 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・保証手段となるガイダンス系ドキュメントの識別不備修正<br>・オートリセット機能をセキュリティ対象外に変更 |
| 2006/06/28 | 1.06 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・基本機能説明修正（2章）<br>・セキュリティ強化機能の説明修正（2章）<br>・完全上書削除、ファイル単位の上書削除の対策内容が入れ違いになっていたため修正（4章）<br>・セキュリティ強化機能を停止する役割を修正（5章） |
| 2006/07/05 | 1.07 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・FIA_SOS.1[1]とITセキュリティ機能との不要なマッピング修正（8章）<br>・FIA_UAU.7の不要な依存性であるFIA_UAU.2[4]を削除修正（5章、8章）<br>・存在しないFIA_UAU.2[5]の誤植修正<br>・T.DISCARD-MFP、T.BRING-OUT-STORAGEの表現修正<br>・残存画像ファイルについて捕捉説明追加。（3章） |
| 2006/07/18 | 1.08 | 制御第12開発部 | 多田 | 橋本 | 加藤 | ・NVRAMの説明追加<br>・オートリセット機能に関する説明追加<br>・ST概説一部修正<br>・表12の誤植修正（FIA_SOS.1要件の対応関係）<br>・依存性が適用されないケースの説明追加（ボックス、機密文書プリントにおけるFMT_MSA.3が適用されない理由、HDDロック機能の要件における識別要件の必要性）<br>・TOEのセキュリティ要件であるFIA_UAU.7の動作がMFPのパネル処理のみに適用されることを各所で説明（TOE記述、根拠など）<br>・表9の修正（ログオフの運用に関する根拠説明の対応不備）<br>・FIA_AFL.1要件の選択操作の記載不備修正<br>・保護資産の説明を追加。（送信宛先データとMFPアドレスが異なる対象であることを明確化）<br>・HDDなしの場合における脅威補足説明を追加<br>・サービスエンジニアに対するログオフ運用対策をST上積極的に謳う必要性がなくなったため、削除。関係箇所修正。<br>・競合要件が存在しないことの実証根拠を追加。<br>・その他誤植修正など |
| 2006/09/02 | 1.09 | 制御12開発部 | 多田 | 橋本 | 加藤 | ・機密文書プリントの静的属性初期化の依存性なしを依存性ありに変更（FMT_MSA.3を追加）<br>・サービスモードへのアクセスを拒否するという表現が、サービスエンジニアの認証状態にあることを正確に表現できていなかったため、表現修正。<br>・記載不備修正<br>- HDDロックパスワードの条件の根拠記載不備<br>- 機密文書プリントのロック解除条件の根拠記載不備<br>- その他誤植 |
| 2006/09/08 | 1.10 | 制御12開発部 | 多田 | 橋本 | 加藤 | ・拡張要件をパート2に沿って監査、管理項目を追加<br>・ボックスに関する再認証は認証であるため、「再」を削除<br>・全領域削除機能においてセキュリティ強化機能設定が関係することの補足説明を追加 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

## ―【 目次 】――――――――――――――――――――――――――――――――――――



Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

## ―【 図目次 】――――――――――――――――――――――――――――――――――――



## ―【 表目次 】――――――――――――――――――――――――――――――――――――



Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 1. ST 概説

## 1.1. ST 識別

・ST名称 ： bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)
**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 ： 1.10
・CCバージョン ： 2.1、CCIMB Interpretations-0407
・作成日 ： 2006年9月8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　　加藤 知和

## 1.2. TOE 識別

・TOE名称 ： 日本名：bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)
全体制御ソフトウェア
英名　：bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)
Control Software
・TOE識別 ： 4040-0100-G10-25-000
・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. CC 適合主張

本STが対象とするTOEは、以下に適合する。

- **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。

- **評価保証レベル**
EAL3適合。（追加する保証コンポーネントはない。）

- **PP参照**
本STは、PP参照を行っていない。

- **補足**
CCIMB Interpretations-0407を適用する。

- **参考資料**
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 2.1 August 1999 CIMB-99-031
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements Version2.1 August 1999 CCIMB-99-033

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- CCIMB Interpretations-0407
- **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** 1999年8月 **バージョン**2.1 CCIMB-99-031（**平成**13**年**1**月翻訳第**1.2**版 情報処理振興事業協会 セキュリティセンター**）
- **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2：セキュリティ機能要件** 1999**年**8**月 バージョン**2.1 CCIMB-99-032（**平成**13**年**1**月翻訳第**1.2**版 情報処理振興事業協会 セキュリティセンター**）**
- **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3：セキュリティ保証要件** 1999**年**8**月 バージョン**2.1 CCIMB-99-033（**平成**13**年**1**月翻訳第**1.2**版 情報処理振興事業協会 セキュリティセンター**）**
- **補足**-0210 **第**2**版** [1]（**平成**16**年**8**月 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室**）**
- **補足**-0407（**平成**16**年**8**月 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室**）**

## 1.4. ST **概要**

bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1)**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。）本** ST **では、**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 / ineo 350 / ineo 250 (Ver.1) **全体制御ソフトウェア”を評価対象（以下** TOE **とする）として、**TOE **が提供するセキュリティ機能について説明する。**

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、**HDD **が備える不正アクセス防止機能（**HDD **ロック機能）を利用する仕組みを有し、また不要となったデータを即時に上書き削除するといった保護機能を提供する。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。**

**本** ST **は、これら** TOE **のセキュリティ機能の必要・十分性を記述したドキュメントである。**

[1] CCIMB Interpretations-0407 **の翻訳は、補足**-0407 **と補足**-0210 **第** 2 **版で示される。**

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 2. TOE 記述

## 2.1. TOE の種別

TOE である bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) 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。

## 2.2. MFP の利用環境

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。

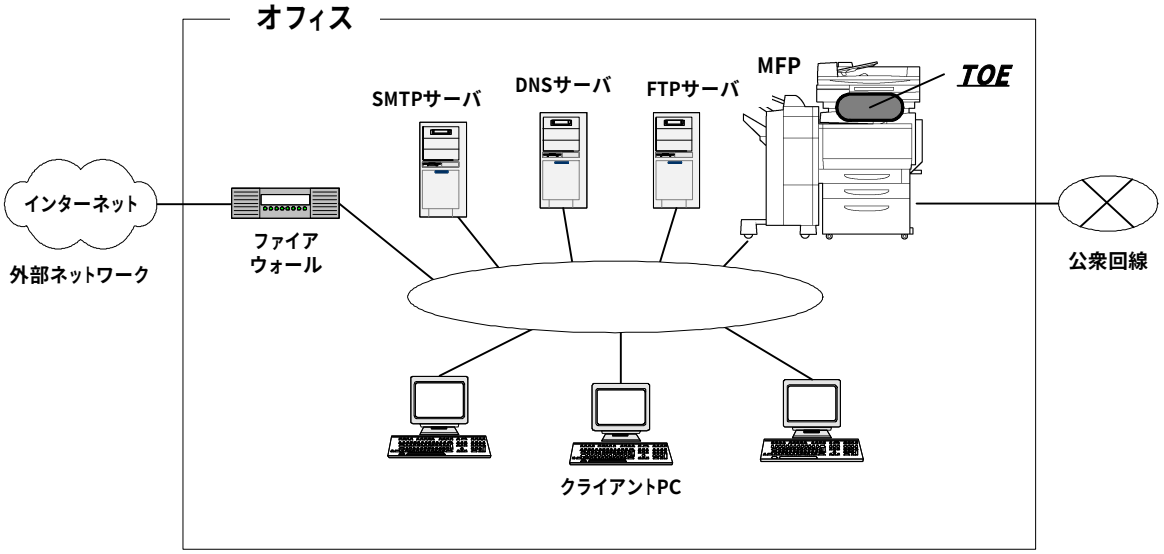


**図 1 MFP の利用環境の例**

- 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

## 2.3. TOE の動作環境構成

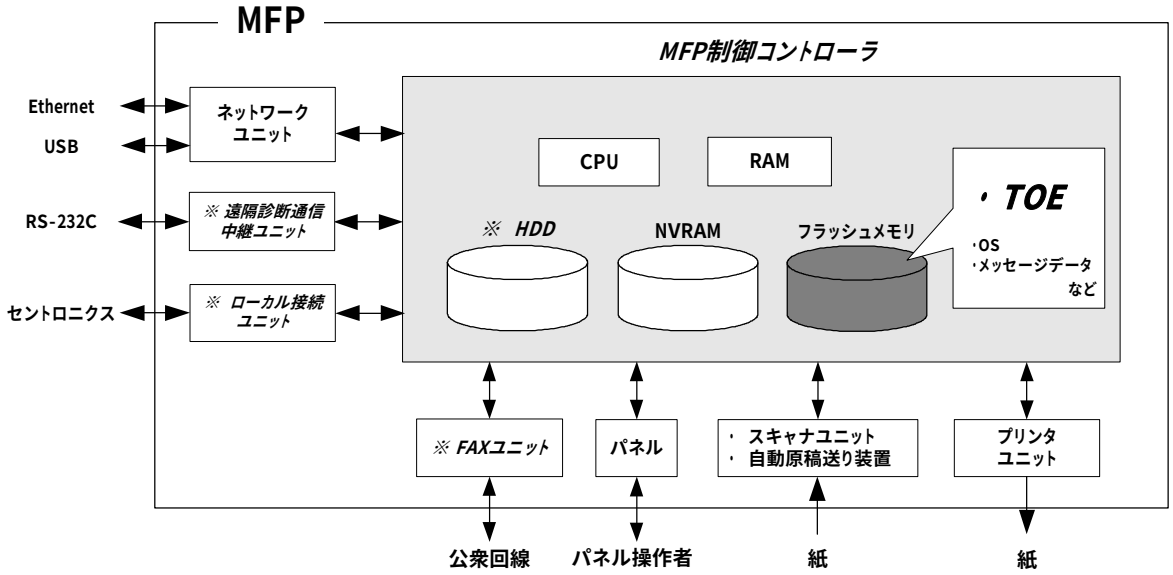


**図 2 TOE に関係するハードウェア構成**

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や OS（VxWorks）なども保管される。

- 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。

- **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。

- **ネットワークユニット**
  Ethernet 接続インターフェースデバイス。10BASE-T、100BASE-TX をサポート。また USB ポートは PC とローカル接続でプリント機能を使うためのポートとして搭載される。

- **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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- **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。

## 2.4. 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。）

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- 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。

## 2.5. TOE の機能

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。

### 2.5.1. 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 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。

### 2.5.2. 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

### 2.5.3. 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、固定のボックス名「Public」と付けられたすべてのユーザが利用することが可能なボックスと、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、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。

### 2.5.4. 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
  - ボックスパスワードの変更
- ネットワーク設定管理
  - IP アドレスなど
- 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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

### 2.5.5. 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

### 2.5.6. 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 **HDD ロック機能**
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。）

③ **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。

④ **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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

### 2.5.7. 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（ID 及びパスワードを同時に検索して一致したファイルの印刷許可する動作方式と、ID を選択した上でパスワードを入力する動作方式）が存在するが、セキュリティを強化状態（後者の動作方式）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
- SNMPv1 のネットワーク設定変更機能　：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
- 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
- 管理者パスワード初期化機能　：禁止
- 遠隔診断機能 [2]　：・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

[2] 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 3. TOE セキュリティ環境

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. 保護対象資産の考え方

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** [3]
  - 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**
  - 画像を送信する宛先となる E-mail アドレス、電話番号などが含まれるファイル。

[3] 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

## 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が有効化した上で、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。

**T.DISCARD-MFP（MFP のリース返却、廃棄）**
・リース返却、または廃棄となった MFP が回収された場合、悪意を持った者が、MFP 内の HDD を取り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。
・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 を動作させることによって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を知ってしまうかもしれない。

**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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

**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.ACCESS-NET-SETTING（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、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（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。

**＜※ 捕捉：HDD が装着されない場合＞**
以下の脅威について考慮する必要はない。（脅威は存在しない。）
・T.BRING-OUT-STORAGE
・T.ACCESS-BOX

以下の脅威は、NVRAM に保管されるデータである、送信宛先データファイル、各種パスワードを考慮する必要がある。
・T.DISCARD-MFP

以下の脅威は、HDD の装着有無を問わず、利用可能な機能である機密文書プリントファイルのみ考慮する必要がある。
・T.ACCESS-SETTING

## 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 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。

・MFP のアドレスに関係する設定機能

・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。

・TOE は、ユーザが設定した個人情報や企業情報の一部となる電話番号や E-mail アドレスなどの送信宛先データを削除する機能、管理者パスワード、HDD ロックパス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.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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

## 4.2. 環境のセキュリティ対策方針

本節では、TOE の利用環境における環境のセキュリティ対策方針を IT 環境のセキュリティ対策方針、Non-IT の環境のセキュリティ対策方針で識別し、説明する。

### 4.2.1. IT 環境のセキュリティ対策方針

**OE.LOCK-HDD（HDD のアクセス制御）**
MFP 内に設置される HDD は、設置された MFP からだけのデータの読み出しを許可する。

**OE.FEED-BACK（パスワードのフィードバック）**
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。

### 4.2.2. Non-IT 環境のセキュリティ対策方針

**OE-N.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-N.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-N.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-N.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。
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。

**OE-N.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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

**OE-N.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 ロックパスワードを秘匿する。**

**・管理者パスワード、HDD ロックパス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。**

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境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 及び IT 環境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。また各要件の対象が TOE、IT 環境のどちらであるか明示するため、IT 環境において必要とされる要件のラベルの後には[E]を付ける。

**＜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。（なお、繰り返しは TOE 要件、IT 環境要件でそれぞれ分離して付与する。）

**＜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。

## 5.1. TOE セキュリティ要件

### 5.1.1. TOE セキュリティ機能要件

#### 5.1.1.1. 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*]：<br>***「表 1　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*]：<br>***ボックスアクセス制御*** |
| **下位階層**　：　なし<br>**依存性**　：　FDP_ACF.1（FDP_ACF.1[1]） |

**表 1　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*** |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 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*]：<br>***「表 2 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*]：<br>***機密文書プリントファイルアクセス制御*** | |
| **下位階層** ： なし<br>**依存性** ： FDP_ACF.1（FDP_ACF.1[2]） | |

**表 2 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*]：<br>***「表 3 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*]：<br>***管理モードアクセス制御*** | |
| **下位階層** ： なし<br>**依存性** ： FDP_ACF.1（FDP_ACF.1[3]） | |

**表 3 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*** | ***・HDD ロックパスワードオブジェクト***<br>***・MFP アドレスグループオブジェクト*** | ***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*]：<br>***＜サブジェクト＞ ＜サブジェクト属性＞***<br>***・利用者を代行するタスク ⇒ ・ボックス属性（ボックス ID）***<br>---<br>***＜オブジェクト＞ ＜オブジェクト属性＞***<br>***・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*]：<br>***ボックスアクセス制御*** | |
| FDP_ACF.1.2[1] | |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| |
|---|
| 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*]:<br>***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*]:<br>***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*]:<br>***なし。*** |
| **下位階層** : なし<br>**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*]:<br>***＜サブジェクト＞ ＜サブジェクト属性＞***<br>***・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）***<br>---<br>***＜オブジェクト＞ ＜オブジェクト属性＞***<br>***・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*]:<br>***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*]:<br>***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*]:<br>***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*]: |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| |
|---|
| ***なし。*** |
| **下位階層　：　なし**<br>**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*]：<br>***＜サブジェクト＞　　＜サブジェクト属性＞***<br>***・利用者を代行するタスク　　⇒　・管理者属性***<br>---<br>***＜オブジェクト＞***<br>***・HDD ロックパスワードオブジェクト***<br>***・MFP アドレスグループオブジェクト*** [4] |
| [割付: *アクセス制御 SFP*]：<br>***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、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*]：<br>***管理者属性を持つ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、MFP アドレスグループ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*]：<br>***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*]：<br>***なし。*** |
| **下位階層　：　なし**<br>**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*]：<br>***からの資源の割当解除*** |
| [割付: *オブジェクトのリスト*]：<br>***・全ボックスファイル*** |

[4] 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| |
|---|
| ***・スワップデータファイル***<br>***・オーバーレイ画像ファイル***<br>***・HDD 蓄積画像ファイル*** |
| **下位階層　：　なし**<br>**依存性　：　なし** |

#### 5.1.1.2. 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*]：<br>***・サービスモードにアクセスする際の認証***<br>***・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]」*]<br>***[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に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。 |
| [割付: *アクションのリスト*]：<br>***＜検出した際のアクション＞***<br>***・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。***<br>***・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。***<br>***＜通常復帰のための操作＞***<br>***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*]：<br>***・管理者モードにアクセスする際の認証***<br>***・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]」*]<br>***[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に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。 |
| [割付: *アクションのリスト*]：<br>***＜検出した際のアクション＞***<br>***・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。***<br>***・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。***<br>***＜通常復帰のための操作＞***<br>***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]）** |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 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*]：<br>***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]」*]<br>***[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に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。 | |
| [割付: *アクションのリスト*]：<br>***＜検出した際のアクション＞***<br>***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。***<br>***＜通常復帰のための操作＞***<br>***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*]：<br>***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]」*]<br>***[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に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。 | |
| [割付: *アクションのリスト*]：<br>***＜検出した際のアクション＞***<br>***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。***<br>***＜通常復帰のための操作＞***<br>***・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。***<br>***・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*]：<br>***・ボックス属性（ボックス ID）***<br>***・ファイル属性（機密文書内部制御 ID）*** | |
| **下位階層** | ： なし |
| **依存性** | ： なし |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 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*]：<br>***・桁数　：8 桁***<br>***・文字種：数字***<br>***・規則　：同種の文字列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*]：<br>***・桁数　：8 桁***<br>***・文字種：ASCII コード（0x20 ～ 0x7E、ただし 0x22、0x2B、0x5E を除く）***<br>***・規則　：同種の文字列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）*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。 | |
| [割付: *定義された品質尺度*]：<br>***・桁数　：20 桁***<br>***・文字種：ASCII コード（0x20 ～ 0x7E、ただし 0x20、0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D、0x5E を除く）***<br>***・規則　：同種の文字列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*]：<br>***・桁数　：8 桁***<br>***・文字種：数字、#、 **<br>***・規則　：同種の文字列だけで構成されていない。*** | |
| **下位階層** | **：　なし** |
| **依存性** | **：　なし** |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 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*]<br>***・管理者が管理者パスワードを改変する場合***<br>***・サービスエンジニアがサービスコードを改変する場合***<br>***・管理者が HDD ロック機能の設定を変更する場合*** | |
| **下位階層** | ： なし |
| **依存性** | ： なし |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| FIA_UAU.7 | **保護された認証フィードバック** |
|---|---|
| FIA_UAU.7.1 | |
| TSF は、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。 | |
| [割付: *フィードバックのリスト*]：<br>***入力された文字データ１文字毎に“＊”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_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 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| FIA_USB.1 | 利用者・サブジェクト結合 |
|---|---|
| FIA_USB.1.1 | |
| TSF は、適切な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。 | |
| **下位階層** | : なし |
| **依存性** | : FIA_ATD.1 |

#### 5.1.1.3. 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*]:<br>***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*]:<br>***を停止する*** | |
| [割付: *許可された識別された役割*]:<br>***管理者*** | |
| **下位階層** | : なし |
| **依存性** | : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]） |

| FMT_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]*]:<br>***[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*]<br>***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*]<br>***該当なし*** | |
| **下位階層** | : なし |
| **依存性** | : FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない） |

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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| |
|---|
| [割付:*許可された識別された役割*]：<br>***・そのボックスの利用を許可されたユーザ***<br>***・管理者*** |
| **下位階層　：　なし** |
| **依存性　：**　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_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*]：<br>***管理者パスワード*** |
| [選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]：<br>***改変*** |
| [割付:*許可された識別された役割*]：<br>***管理者*** |
| **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*]：<br>***管理者パスワード*** |
| [選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]：<br>***問い合わせ*** |
| [割付:*許可された識別された役割*]：<br>***サービスエンジニア*** |
| **下位階層　：　なし** |
| **依存性　：**　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]） |

| **FMT_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*]：<br>***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]*]：<br>***改変*** |
| [割付:*許可された識別された役割*]：<br>***サービスエンジニア*** |
| **下位階層　：　なし** |
| **依存性　：**　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]） |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| **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*]：<br>***・管理者によるセキュリティ強化機能の停止機能***<br>***・管理者による機密文書不正アクセス検出値の消去機能***<br>***・管理者によるボックス不正アクセス検出値の消去機能***<br>***・管理者による管理者パスワードの改変機能***<br>***・管理者によるボックスパスワードの改変機能***<br>***・サービスエンジニアによるサービスコードの改変機能***<br>***・サービスエンジニアによる管理者パスワードの問い合わせ機能***<br>***・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*** |
| **下位階層　：**　なし |
| **依存性　：**　なし |

| **FMT_SMR.1[1]　　セキュリティ役割** |
|---|
| FMT_SMR.1.1[1] |
| TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。 |
| [割付: *許可された識別された役割*]：<br>***サービスエンジニア*** |
| FMT_SMR.1.2[1] |
| TSF は、利用者を役割に関連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*]：<br>***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*]：<br>***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]） |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

#### 5.1.1.4. TSF の保護

| FPT_RVM.1 | TSP の非バイパス性 |
|---|---|
| FPT_RVM.1.1 | |
| TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。 | |
| **下位階層** | : なし |
| **依存性** | : なし |

| FPT_SEP.1 | TSF ドメイン分離 |
|---|---|
| FPT_SEP.1.1 | |
| TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。 | |
| FPT_SEP.1.2 | |
| TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。 | |
| **下位階層** | : なし |
| **依存性** | : なし |

#### 5.1.1.5. 拡張要件：アクセス先の識別と承認

| FIA_NEW.1 | TOE からのアクセス対象となる利用者の識別と承認 |
|---|---|
| FIA_NEW.1.1 | |
| TSF は、TOE から利用者（*HDD*）に対してアクションする前に、その利用者の識別に成功することを要求しなければならない。 | |
| FIA_NEW.1.2 | |
| TSF は、利用者の識別に失敗した場合、TOE から利用者（*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 |

| **監査：**FIA_NEW.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。<br>a) 最小 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用<br>b) 基本 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用 |
| **管理：**FIA_NEW.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。<br>a) 利用者識別情報の管理 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

#### 5.1.1.6. 拡張要件：明示的な消去操作後の残存情報保護

| FNEW_RIP.1 | 明示的な消去操作後の利用者データと TSF データの残存情報保護 |
|---|---|
| FNEW_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*]：<br>***＜オブジェクト＞***<br>***・全ボックスファイル***<br>***・スワップデータファイル***<br>***・オーバーレイ画像ファイル***<br>***・HDD 蓄積画像ファイル***<br>***・送信宛先データファイル***<br>***・HDD ロックパスワードオブジェクト***<br>***＜TSF データ＞***<br>***・管理者パスワード***<br>***・ボックスパスワード*** | |
| **下位階層** ： なし<br>**依存性** ： なし | |

| **監査：**FNEW_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：**FNEW_RIP.1 |
| 予見される管理アクティビティはない。 |

### 5.1.2. 最小セキュリティ機能強度

TOE の最小機能強度レベルは、SOF-基本である。確率的・順列的メカニズムを利用する TOE セキュリティ機能要件は、FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.6、FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]、FIA_SOS.1[4]である。

### 5.1.3. 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 |
|---|---|---|
| 構成管理 | CM 能力 | ACM_CAP.3 |
| | CM 範囲 | ACM_SCP.1 |
| 配付と運用 | 配付 | ADO_DEL.1 |
| | 設置・生成・及び立上げ | ADO_IGS.1 |
| 開発 | 機能仕様 | ADV_FSP.1 |
| | 上位レベル設計 | ADV_HLD.2 |
| | 表現対応 | ADV_RCR.1 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| TOEセキュリティ保証要件 | | コンポーネント |
|---|---|---|
| ガイダンス文書 | 管理者ガイダンス | AGD_ADM.1 |
| | 利用者ガイダンス | AGD_USR.1 |
| ライフサイクルサポート | 開発セキュリティ | ALC_DVS.1 |
| テスト | カバレージ | ATE_COV.2 |
| | 深さ | ATE_DPT.1 |
| | 機能テスト | ATE_FUN.1 |
| | 独立テスト | ATE_IND.2 |
| 脆弱性評定 | 誤使用 | AVA_MSU.1 |
| | TOE セキュリティ機能強度 | AVA_SOF.1 |
| | 脆弱性分析 | AVA_VLA.1 |

## 5.2. IT 環境のセキュリティ要件

#### 5.2.1.1. 識別と認証

| FIA_AFL.1[E] 認証失敗時の取り扱い |
|---|
| FIA_AFL.1.1[E] |
| TSF*（HDD）*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*]：<br>***HDD にアクセスする際の HDD ロック機能による認証*** |
| [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]*」]<br>***[割付:正の整数値]：5*** |
| FIA_AFL.1.2[E] |
| 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。 |
| [割付: *アクションのリスト*]：<br>***＜検出した際のアクション＞***<br>***HDD へのデータの読み込み及び書き込みを拒否する。***<br>***＜通常復帰のための操作＞***<br>***HDD への通電 OFF（電源 OFF）*** |
| **下位階層** ： なし |
| **依存性** ： FIA_UAU.1（FIA_UAU.2[E]） |

| FIA_UAU.2[E] アクション前の利用者認証 |
|---|
| FIA_UAU.2.1[E] |
| TSF*（HDD）*は、その利用者*（HDD が設置された MFP 本体）*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*（HDD が設置された MFP 本体）*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（適用しない） |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 6. TOE 要約仕様

## 6.1. TOE セキュリティ機能

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 5 にて一覧を示す。仕様詳細は、後述の項にて説明する。

**表 5 TOE のセキュリティ機能名称と識別子の一覧**

| No. | TOE のセキュリティ機能 | |
|---|---|---|
| 1 | F.ADMIN | 管理者機能 |
| 2 | F.SERVICE | サービスモード機能 |
| 3 | F.BOX | ボックス機能 |
| 4 | F.PRINT | 機密文書プリント機能 |
| 5 | F.OVERWRITE-FILE | 残存情報上書き削除機能 |
| 6 | F.OVERWRITE-ALL | 全領域上書き削除機能 |
| 7 | F.HDD | HDD 検証機能 |
| 8 | F.RESET | 認証失敗回数リセット機能 |

### 6.1.1. 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。）

#### 6.1.1.1. 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 6 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。

**表 6 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 文字が選択可能<br>・数字：0 ～ 9、#、* |
| 管理者パスワード | 8 桁 | 合計 10 文字が選択可能<br>・数字：0 ～ 9 |
| ボックスパスワード | 8 桁 | 合計 92 文字が選択可能<br>ASCII コード（0x20 ～ 0x7E、ただし 0x22、0x5E、0x2B を |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 対象 | 桁数 | キャラクタ |
|---|---|---|
| 機密文書パスワード | | 除く）<br>・数字：0 ～ 9<br>・英字：大文字、小文字<br>・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、_、`、{、|、}、~、*SPACE* |
| HDD ロックパスワード | 20 桁 | 合計 82 文字が選択可能<br>ASCII コード（0x20 ～ 0x7E、ただし 0x20、x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D、0x5E を除く）<br>・数字：0 ～ 9<br>・英字：大文字、小文字<br>・記号：!、 #、 $、 %、 &、 ’ 、 *、 +、 -、.、 /、 =、 ?、 @、 _、 `、 {、 |、 }、 ~ |

#### 6.1.1.2. 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権限が関連づけられ、以下の操作、機能の利用が許可される。

**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 6 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、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 6 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。

**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 6 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。

**③ ロックの解除**

すべての機密文書プリントの認証失敗回数を 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

**④ 全領域上書き削除機能の設定と実行**
全領域の上書き削除を実行する。（F.OVERWRITE-ALL を実行する。）

**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。
- MFP アドレスに関係する一連の設定データ（IP アドレス等）

**⑥ HDD ロック機能のパスワード設定機能**
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 6 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 6 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。

**⑦ 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。
- 全領域上書き削除機能
  全領域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。

### 6.1.2. 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。

#### 6.1.2.1. 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 6 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。

#### 6.1.2.2. 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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

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 6 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少なくとも通算 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 6 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。

② 管理者パスワードの送信

MFP の装置情報を FAX ユニット経由、または E-mail で MFP のサポートセンターへ送信する。

- 発信される装置情報の中には、セキュリティ情報、秘匿性のある管理者パスワードを含む。（管理者パスワードの問い合わせ機能に相当する。）

### 6.1.3. F.BOX（ボックス機能）

F.BOX とは、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。

#### 6.1.3.1. ボックスの登録機能

ユーザ操作によって、ボックス登録操作が提供される。ボックス名、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。

- ボックス名は、既登録済みのボックス名がないことを検証する。
- 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 6 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。

#### 6.1.3.2. 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 6 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、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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

機能が動作して解除する。

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のボックス識別認証ドメインにおいて提供される機能であり、すべて実行に伴い認証が要求される。

- 表 6 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。

**① 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「ボックス名」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操作を行うことを許可される。

**② 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。

- 表 6 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再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。
- 再認証に成功すると、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。
- 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 6 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。

### 6.1.4. 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。

#### 6.1.4.1. 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 6 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- 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。

#### 6.1.4.2. 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内部制御 ID を持つ。
- このタスクは、このファイル属性と一致するファイル属性を持つ機密文書プリントファイルに対して印刷を許可される。

#### 6.1.4.3. 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 6 の機密文書パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

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。

### 6.1.5. F.OVERWRITE-FILE（残存情報上書き削除機能）

F.OVERWRITE-FILE 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 [5]。
  - 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。本機能の動作の結果、残存画像ファイルは発生しない。

[5] ジョブ完了とは、コピーなどで印刷を終えて正常終了する、またはユーザ操作によって中止操作された場合を意図している。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

### 6.1.6. 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 に設定されている送信宛先データファイルを削除する。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＞
- 送信宛先データファイル
- HDD ロックパスワード

＜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。

なお、本機能の実行においてセキュリティ強化機能の設定は、無効になる。（F.ADMIN におけるセキュリティ強化機能の動作設定の記載参照）

### 6.1.7. F.HDD（HDD 検証機能）

F.HDD とは、HDD に対して HDD ロックパスワードを設定している場合、HDD のステータスをチェックし、HDD のロックパスワードが設定されていなければ、不正な HDD が設置されているとして読み込み、書き込み操作を許可しない。HDD ロックパスワードが確かに設定されていると確認された場合のみ 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。

### 6.1.8. 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

## 6.2. TOE セキュリティ機能強度

確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りであり、機能強度はそれぞれ SOF-基本を満たす。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

① F.ADMIN が提供する管理者パスワード認証メカニズム、HDD ロックパスワード照合メカニズム
② F.SERVICE が提供するサービスコード認証メカニズム
③ F.PRINT が提供する機密文書パスワード認証メカニズム
④ F.BOX が提供するボックスパスワード認証メカニズム

## 6.3. TOE セキュリティ機能と機能要件の対応関係

TOE のセキュリティ機能と TOE セキュリティ機能要件との対応関係は 8.3 の表 12 に示す。表 12 は TOE のセキュリティ機能が少なくとも 1 つ以上の TOE セキュリティ機能要件に対応していることが示される。

## 6.4. 保証手段

表 7 で記述した EAL3 の TOE セキュリティ保証要件のコンポーネントを満たす保証手段を下表に示す。

**表 7 TOE 保証要件と保証手段の関係**

| TOE セキュリティ保証要件 | | コンポーネント | 保証手段 |
|---|---|---|---|
| 構成管理 | CM 能力 | ACM_CAP.3 | ・構成管理計画書<br>・構成リスト<br>・CM 記録 |
| | CM 範囲 | ACM_SCP.1 | |
| 配付と運用 | 配付 | ADO_DEL.1 | 配付説明書 |
| | 設置・生成・及び立上げ | ADO_IGS.1 | ・サービスマニュアル<br>bizhub 200 / 250 / 350 サービスマニュアル[セキュリティ機能編] 2006.06(和文)、bizhub 200 / 250 / 350 ineo 250 / 350 Service Manual [Security Function] 2006.06（英文）<br>・ユーザーズガイド<br>bizhub 200 / 250 / 350 ユーザーズガイド[セキュリティ機能編] 2006.06（和文）、bizhub 200 / 250 / 350 User's Guide [Security Operations] 2006.06（英文）、ineo 250 / 350 User's Guide [Security Operations] 2006.06（英文） |
| 開発 | 機能仕様 | ADV_FSP.1 | セキュリティ機能仕様書 |
| | 上位レベル設計 | ADV_HLD.2 | セキュリティ上位レベル設計書 |
| | 表現対応 | ADV_RCR.1 | 表現対応分析書 |
| ガイダンス文書 | 管理者ガイダンス | AGD_ADM.1 | ・サービスマニュアル<br>bizhub 200 / 250 / 350 サービスマニュアル[セキュリティ機能編] 2006.06(和文)、bizhub 200 / 250 / 350 ineo 250 / 350 Service Manual |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| TOE セキュリティ保証要件 | | コンポーネント | 保証手段 |
|---|---|---|---|
| | 利用者ガイダンス | AGD_USR.1 | [Security Function] 2006.06（英文）<br>・ユーザーズガイド<br>bizhub 200 / 250 / 350 ユーザーズガイド[セキュリティ機能編] 2006.06（和文）、bizhub 200 / 250 / 350 User's Guide [Security Operations] 2006.06（英文）、ineo 250 / 350 User's Guide [Security Operations] 2006.06（英文） |
| ライフサイクルサポート | 開発セキュリティ | ALC_DVS.1 | 開発セキュリティ説明書 |
| テスト | カバレージ | ATE_COV.2 | カバレージ分析書 |
| | 深さ | ATE_DPT.1 | 深さ分析書 |
| | 機能テスト | ATE_FUN.1 | テスト仕様・結果報告書 |
| | 独立テスト | ATE_IND.2 | TOE を含む MFP 制御ソフトウェア |
| 脆弱性評定 | 誤使用 | AVA_MSU.1 | ※特にドキュメントはなし<br>（ガイダンス文書証拠に要求事項反映） |
| | TOE セキュリティ機能強度 | AVA_SOF.1 | 脆弱性分析書 |
| | 脆弱性分析 | AVA_VLA.1 | |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 7. PP 主張

本 ST には、適合する PP はない。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

# 8. 根拠

## 8.1. セキュリティ対策方針根拠

### 8.1.1. 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、脅威に対応していることを示している。

**表 8 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.ACCESS-NET-SETTING | T.ACCESS-SETTING |
|---|---|---|---|---|---|---|---|---|---|---|---|
| O.BOX | | | | | | | | ● | | | |
| O.SECURE-PRINT | | | | | | | | | ● | | |
| O.CONFIG | | | | | | | | | | ● | ● |
| O.OVERWRITE-ALL | | | | | | ● | | | | | |
| O.OVERWRITE-FILE | | | | | | | ● | | | | |
| O.CHECK-HDD | | | | | | | ● | | | | |
| OE.LOCK-HDD | | | | | | | ● | | | | |
| OE.FEED-BACK | | | | | | | | ● | ● | ● | ● |
| OE-N.ADMIN | ● | | | | | | | | | | |
| OE-N.SERVICE | | ● | | | | | | | | | |
| OE-N.NETWORK | | | ● | | | | | | | | |
| OE-N.SECRET | | | | ● | | | | | | | |
| OE-N.SESSION | | | | | | | | | ● | ● | ● |
| OE-N.SETTING-SECURITY | | | | | ● | | | | | | |

### 8.1.2. 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-N.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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- **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-N.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-N.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が各利用者より漏洩しないことを想定している。
  OE-N.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-N.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。

### 8.1.3. 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。
  OE.LOCK-HDD は、HDD の機能として、MFP に設置される HDD が設置された MFP 以外からはデータを読み出しすることを許可しないため、脅威の可能性は除去される。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

上記において、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-N.SESSION により操作終了後にはログオフする運用が要求されるため、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.ACCESS-NET-SETTING（ネットワーク設定の不正変更）**
  本脅威は、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 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-N.SESSION により操作終了後にはログオフする運用が要求されるため、O.CONFIG は十分サポートされている。
  したがって本脅威は十分対抗されている。

- **T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）**
  本脅威はセキュリティに関係する特定の機能設定を変更されることにより、結果的にボックスファイルや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としており、また OE-N.SESSION により管理者モードの操作終了後にはそれぞれログオフする運用が要求されるため、O.CONFIG は十分サポートされている。
  したがって本脅威は十分対抗されている。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

#### 8.1.4. 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。

## 8.2. IT セキュリティ要件根拠

### 8.2.1. IT セキュリティ機能要件根拠

#### 8.2.1.1. 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 9 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.CHECK-HDD | OE.LOCK-HDD | OE.FEED-BACK | ※ set.admin | ※ set.service |
|---|---|---|---|---|---|---|---|---|---|---|
| set.admin | ● | ● | ● | | | | | | | |
| set.service | ● | ● | ● | | | | | | | |
| 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] | ● | | | | | | | | | |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 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.CHECK-HDD | OE.LOCK-HDD | OE.FEED-BACK | ※ set.admin | ※ set.service |
|---|---|---|---|---|---|---|---|---|---|---|
| FIA_UAU.6 | | | ● | | | | | | ● | ● |
| FIA_UAU.7 | | ● | | | | | | | ● | ● |
| FIA_UID.2[1] | | | | | | | | | | ● |
| FIA_UID.2[2] | | | | | | | | | ● | |
| FIA_UID.2[3] | | ● | | | | | | | | |
| FIA_UID.2[4] | ● | | | | | | | | | |
| FIA_USB.1 | ● | ● | | | | | | | | |
| FMT_MOF.1 | | | ● | | | | | | | |
| FMT_MSA.3 | | ● | | | | | | | | |
| 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] | ● | | ● | | | | | | ● | |
| FMT_SMR.1[3] | ● | | | | | | | | | |
| FPT_RVM.1 | ● | ● | ● | | | ● | | | | |
| FPT_SEP.1 | ● | ● | ● | | | | | | | |
| FNEW_RIP.1 | | | | ● | | | | | | |
| FIA_NEW.1 | | | | | | ● | | | | |
| FIA_AFL.1[E] | | | | | | | ● | | | |
| FIA_UAU.2[E] | | | | | | | ● | | | |
| FIA_UAU.7[E] | | | | | | | | ● | | |

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。

#### 8.2.1.2. 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

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

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。
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。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[3]により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、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＞
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。

＜管理者をセキュアに維持するために必要な要件＞

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

⇒ 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、ネットワークの設定を管理者、セキュリティ強化機能に関係する設定を管理者に制限しており、一連の設定機能や管理機能に対してアクセスを制限するための諸要件が必要である。

  ＜ネットワークの設定管理＞
  利用を代行するタスクに管理者属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、利用者を代行するタスクは、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 ロックパスワードの管理＞
  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、HDD ロックパス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 ロックパスワードの品質が検証される。なお HDD ロックパス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。
  FNEW_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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- **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.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_NEW.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。

- **OE.LOCK-HDD（HDD のアクセス制御）**
  本セキュリティ対策方針は、TOE のセキュリティ維持に必要な IT 環境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としており、TOE が設置された正当な MFP であることを検証する諸要件が必要である。
  FIA_UAU.2[E]により HDD は、HDD にアクセスするエンティティを、HDD が設置された MFP であることを認証する。
  FIA_AFL.1[E]により、不成功認証が 5 回に達すると、HDD へのデータ読み込み、書き込み関する一切のアクセスを拒否する。
  これら複数の機能要件が組み合わさることにより、本セキュリティ対策方針は満たされる。

- **OE.FEED-BACK（パスワードのフィードバック）**
  本セキュリティ対策方針は、TOE のセキュリティ維持に必要な IT 環境のエンティティであるアプリケーション（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）は、入力される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としている。
  FIA_UAU.7[E]によりアプリケーションは、入力された文字データ一文字毎に“＊”を表示する。
  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、パネルに保護されたフィードバックとして入力毎 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。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

＜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、パネルに保護されたフィードバックとして入力毎 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。

#### 8.2.1.3. 明示された IT セキュリティ機能要件の必要性

本 ST では、拡張要件として FNEW_RIP.1 と FIA_NEW.1 を挙げている。これら要件を提示する必要性、及びこれら要件を保証する上で適用している保証要件の妥当性について以下に記述する。

- **拡張要件：FNEW_RIP.1 の必要性**
  FNEW_RIP.1 は、残存情報保護という観点では FDP_RIP.1 が最も近い要件に相当するが、要件

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

は利用者データだけでなく、TSF データの保護を規定する必要があるため、利用者データ保護のクラスに存在する当該機能要件では不適切であり、拡張要件が必要である。
**＜要件識別構造の妥当性＞**
本要件は、該当するクラスが存在しないため、TSF データと利用者データの区分のない統合されたデータ保護クラスということで、FNEW という新しいクラスを設け、残存情報保護を示す FDP クラスの RIP ファミリと同一のファミリ名を付与し、識別を明確化した。
予見される管理アクティビティはないとしているが、情報の再利用不可とするタイミングは要件において具体的に規定しているなど、特に可変的に扱われるパラメタなどは本要件において推察されない。また予見される監査アクティビティに利用者識別と共に実行の記録が残されていることが示されている。

- **拡張要件：FIA_NEW.1 の必要性**
  FIA_NEW.1 は、識別という観点では FIA_UID.1 や FIA_UID.2 が最も近い要件に相当するが、HDD の検証行為は、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、当該機能要件では不適切であり、拡張要件が必要である。
  **＜要件識別構造の妥当性＞**
  本要件は、識別要件の 1 つであるため、FIA クラスの中に追加されるファミリとして NEW というファミリを設定し、識別を明確化した。
  管理において予見されるアクティビティとして、FIA_UID 要件と同様の管理項目が想定されている。また監査において予見されるアクティビティにも、FIA_UID 要件と同様の監査項目が想定されている。

#### 8.2.1.4. 明示された IT セキュリティ機能要件の保証妥当性

2 つの明示された機能要件（FNEW_RIP.1、FIA_NEW.1）は、CC パート 2 に規定される機能要件の概念を大幅に拡張したものではなく、新規性の高い内容ではない。つまり本機能要件を正確に評価するにあたり、特別に TSP モデルを提示するといった必要性や、潜在的な隠れチャネルの可能性等が想定されるものではない。

従って、EAL3 の保証要件のセットによって十分にこれら機能要件が示す機能の妥当性を保証することが可能であり、特別な保証要件や、EAL4 以上から求められる保証要件を必要としない。

#### 8.2.1.5. 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 10　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 |
|---|---|---|
| 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、<br>FMT_MSA.3 | FDP_ACC.1[1]、 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 本 ST の機能要件コンポーネント | CC パート 2 の依存性 | 本 ST における依存関係 |
|---|---|---|
| | | ＜FMT_MSA.3 を適用しない理由＞<br>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。<br>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、<br>FMT_MSA.3 | FDP_ACC.1[2]<br>FMT_MSA.3 |
| FDP_ACF.1[3] | FDP_ACC.1、<br>FMT_MSA.3 | FDP_ACC.1[3]<br><br>＜FMT_MSA.3 を適用しない理由＞<br>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] |
| 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_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、<br>FMT_SMR.1 | FMT_SMF.1、<br>FMT_SMR.1[2] |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | 両者とも適用しない<br><br>＜FMT_MSA.1 を適用しない理由＞<br>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。<br>＜FMT_SMR.1＞<br>FMT_MSA.3.2 の割付は該当なしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。 |
| FMT_MTD.1[1] | FMT_SMF.1、 | FMT_SMF.1、 |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| 本 ST の機能要件コンポーネント | CC パート 2 の依存性 | 本 ST における依存関係 |
|---|---|---|
| | FMT_SMR.1 | FMT_SMR.1[2]、FMT_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_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[4] |
| FPT_RVM.1 | なし | N/A |
| FPT_SEP.1 | なし | N/A |
| FNEW_RIP.1 | なし | N/A |
| FIA_NEW.1 | なし | N/A |
| FIA_AFL.1[E] | FIA_UAU.1 | FIA_UAU.2[E] |
| FIA_UAU.2[E] | FIA_UID.1 | 適用しない<br><br>＜FIA_UID.1 を適用しない理由＞<br>MFP 内に設置される HDD へのアクセスを規定するものである。HDD へのアクセスは一般的な IDE インターフェースを介してなされるものであるため、複数のアクセスルートはない。<br>つまり複数の利用者がアクセスする場合に必要となる利用者に応じた認証情報は本処理には不要であり、アクセスするエンティティの識別の必要性はない。 |
| FIA_UAU.7[E] | FIA_UAU.1 | FIA_UAU.2[2]、FIA_UAU.2[4] |

### 8.2.1.6. IT セキュリティ機能要件の相互サポート関係

機能要件の依存関係の分析には明示されない他のセキュリティ機能要件を有効に動作させるための IT セキュリティ機能要件を下表に示す。

**表 11 IT セキュリティ機能要件の相互サポート関係**

N/A：Not Applicable

| IT セキュリティ機能要件 | 他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント | | | |
|---|---|---|---|---|
| | ①迂回防止 | ②干渉、破壊防止 | ③非活性化防止 | ④無効化検出 |
| FDP_ACC.1[1] | N/A | N/A | N/A | N/A |
| FDP_ACC.1[2] | N/A | N/A | FMT_MOF.1 | N/A |
| FDP_ACC.1[3] | N/A | N/A | N/A | N/A |
| FDP_ACF.1[1] | FIA_UAU.2[4] | FPT_SEP.1 | N/A | N/A |
| FDP_ACF.1[2] | FIA_UAU.2[3] | FPT_SEP.1 | FMT_MOF.1 | N/A |
| FDP_ACF.1[3] | FIA_UAU.2[2] | FPT_SEP.1 | N/A | N/A |
| FDP_RIP.1 | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_AFL.1[1] | N/A | N/A | FMT_MOF.1 | N/A |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| IT セキュリティ機能要件 | 他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント | | | |
|---|---|---|---|---|
| | ①迂回防止 | ②干渉、破壊防止 | ③非活性化防止 | ④無効化検出 |
| FIA_AFL.1[2] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_AFL.1[3] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_AFL.1[4] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_ATD.1 | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_SOS.1[1] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_SOS.1[2] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_SOS.1[3] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_SOS.1[4] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_UAU.2[1] | FPT_RVM.1 | FMT_MTD.1[4] | N/A | N/A |
| FIA_UAU.2[2] | FPT_RVM.1 | FMT_MTD.1[2]<br>FMT_MTD.1[3] | N/A | N/A |
| FIA_UAU.2[3] | FPT_RVM.1 | N/A | FMT_MOF.1 | N/A |
| FIA_UAU.2[4] | FPT_RVM.1 | FMT_MTD.1[1] | FMT_MOF.1 | N/A |
| FIA_UAU.6 | N/A | N/A | N/A | N/A |
| FIA_UAU.7 | N/A | N/A | N/A | N/A |
| FIA_UID.2[1] | N/A | N/A | N/A | N/A |
| FIA_UID.2[2] | N/A | N/A | N/A | N/A |
| FIA_UID.2[3] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_UID.2[4] | N/A | N/A | FMT_MOF.1 | N/A |
| FIA_USB.1 | N/A | N/A | FMT_MOF.1 | N/A |
| FMT_MOF.1 | N/A | N/A | N/A | N/A |
| FMT_MSA.3 | N/A | N/A | N/A | N/A |
| FMT_MTD.1[1] | N/A | N/A | N/A | N/A |
| FMT_MTD.1[2] | N/A | N/A | N/A | N/A |
| FMT_MTD.1[3] | N/A | N/A | N/A | N/A |
| FMT_MTD.1[4] | N/A | N/A | N/A | N/A |
| FMT_SMF.1 | N/A | N/A | N/A | N/A |
| FMT_SMR.1[1] | N/A | N/A | N/A | N/A |
| FMT_SMR.1[2] | N/A | N/A | N/A | N/A |
| FMT_SMR.1[3] | N/A | N/A | N/A | N/A |
| FPT_RVM.1 | N/A | N/A | N/A | N/A |
| FPT_SEP.1 | N/A | N/A | N/A | N/A |
| FIA_NEW.1 | FPT_RVM.1 | N/A | FMT_MOF.1 | N/A |
| FNEW_RIP.1 | N/A | N/A | N/A | N/A |
| FIA_AFL.1[E] | N/A | N/A | N/A | N/A |
| FIA_UAU.2[E] | N/A | N/A | N/A | N/A |
| FIA_UAU.7[E] | N/A | N/A | N/A | N/A |

**① 迂回防止**

**＜サービスエンジニアに関係する機能要件のバイパス防止＞**

**サービスエンジニアの認証を規定する** FIA_UAU.2[1]**は、**FPT_RVM.1 **によって必ず呼び出されるため、バイパス防止がサポートされる。**

**＜管理者に関係する機能要件のバイパス防止＞**

**管理者モードアクセス制御を規定する** FDP_ACF.1[3]**は、管理者の識別認証を規定する** FIA_UAU.2[2]**によってバイパス防止がサポートされる。**

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

さらに FIA_UAU.2[2]は FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜ボックスに関係する機能要件のバイパス防止＞
ボックスアクセス制御を規定する FDP_ACF.1[1]は、ボックスの利用を許可されたユーザであることの認証を規定する FIA_UAU.2[4]によってバイパス防止がサポートされる。
さらにボックスの利用を許可されたユーザであることの認証を規定する FIA_UAU.2[4]は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜機密文書プリントに関係する機能要件のバイパス防止＞
機密文書プリントファイルアクセス制御を規定する FDP_ACF.1[2]は、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する FIA_UAU.2[3]によってバイパス防止がサポートされる。
さらに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の認証を規定する FIA_UAU.2[3]は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜HDD の正当性検証のバイパス防止＞
HDD の正当性を検証する FIA_NEW.1 は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

② **干渉・破壊防止**
＜ボックスアクセス制御の維持＞
FPT_SEP.1 により、ボックスアクセス制御で想定されている認証されたボックスの利用を許可されたユーザだけがボックスファイルの操作が可能であり、FDP_ACF.1[1]は他の不正なサブジェクトによる干渉・破壊防止がサポートされる。

＜機密文書プリントファイルアクセス制御の維持＞
FPT_SEP.1 により機密文書プリントファイルアクセス制御で想定されている認証された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が機密文書プリントファイルの操作が可能であり、FDP_ACF.1[2]は他の不正なサブジェクトによる干渉・破壊防止がサポートされる。

＜管理者モードアクセス制御の維持＞
FPT_SEP.1 により管理者モードアクセス制御で想定されている認証された管理者を代行するサブジェクトだけが、管理者モードアクセス制御にて規定されるオブジェクトの操作が可能であり、FDP_ACF.1[3]は他の不正なサブジェクトによる不正な干渉・破壊防止がサポートされる。

＜サービスコードの管理＞
サービスコードの改変操作は FMT_MTD.1[4]によりサービスエンジニアだけに許可している。これより FIA_UAU.2[1]の不正な干渉・破壊防止がサポートされる。

＜管理者パスワードの管理＞
管理者パスワードの改変操作は FMT_MTD.1[2]により管理者に制限される。また問い合わせ操作は FMT_MTD.1[3]によりサービスエンジニアだけに許可している。これより FIA_UAU.2[2]の不正な干渉・破壊防止がサポートされる。

＜ボックスパスワードの管理＞

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

ボックスパスワードの改変操作はFMT_MTD.1[1]によりボックスの利用を許可されたユーザ及び管理者だけに許可している。これより FIA_UAU.2[4]の不正な干渉・破壊防止がサポートされる。

③ **非活性化防止**

＜セキュリティ強化機能の維持＞

FMT_MOF.1 により、セキュリティ強化機能の動作設定が管理者だけに許可されている。セキュリティ強化機能は、パスワード規約機能（FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]、FIA_SOS.1[4]）、機密文書プリントの認証方式（FIA_UAU.2[3]、FIA_UID.2[3]、FDP_ACC.1[2]、FDP_ACF.1[2]、FIA_ATD.1、FIA_USB.1）、ボックスアクセスにおける識別認証（FIA_UAU.2[4]、FIA_UID.2[4]）認証操作禁止機能（FIA_AFL.1[1]、FIA_AFL.1[2]、FIA_AFL.1[3]、FIA_AFL.1[4]）、残存情報上書き削除機能（FDP_RIP.1）といったTOEのセキュリティ機能の実行を強制させる機能であり、非活性化防止がサポートされる。

④ **無効化検出**

特に無効化検出をサポートする要件は存在しない。[6]

### 8.2.2. 最小機能強度根拠

本TOEの搭載されるMFPは、外部とのネットワーク接続において適切な管理が実施されているオフィス内部LANに接続される。よってインターネットを介して不特定多数の者に直接攻撃されるような可能性はなく、3.3節にて明確化されているTOEの利用者であるユーザ及びTOEの利用者ではないオフィス内に入ることが可能な人物をエージェントとした脅威に対抗する強度レベルを有すれば良い。従って本TOEは、攻撃者のレベルとして低レベルを想定したセキュリティ対策方針を規定しており、最小機能強度としてSOF-基本の選択は妥当である。

### 8.2.3. 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。

#### 8.2.3.1. IT セキュリティ機能要件のセット一貫性根拠

以下に競合可能性のあるITセキュリティ要件が存在しない論拠を示す。

＜IT セキュリティ機能要件＞

- アクセス制御要件（FDP_ACC.1 など）の繰り返しにより、複数のアクセス制御方針を立てているが、①ボックス、②機密文書プリント、③HDD ロックパスワード及び MFP アドレスに関するアクセス制御を規定している。つまりこれらは同一の制御対象を複数のポリシーでカバーし合う

[6] 相互サポート分析の中で示されないが、各認証機能の無効化を狙った攻撃に対しては、それぞれ対応するFIA_AFL.1要件がサポートしており、本TOEのセキュリティ対策方針を維持するにあたって十分である。（なお、依存性分析にて本内容は明示されている。）

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

ものではないため、競合するものではない。

- 保護資産の削除を規定した FDP_RIP.1、拡張要件として FNEW_RIP.1 を適用しているが、不正削除の可能性に関する脅威は、機密性重視のコンセプトより、本件では対象としておらず、したがって競合するデータ削除保護に関する要件は全く選択されていない。
- 依存性による要件間の関係、相互サポートによる相関関係、TOE セキュリティ対策方針に対するセキュリティ機能要件妥当性の各種分析より、競合可能性が示唆される構造は存在しない。

＜IT セキュリティ保証要件＞

- 保証パッケージである EAL を利用している。すなわちセキュリティ保証要件が競合する可能性は、本 ST とは関係なく、存在しないことが確認されている。

## 8.3. TOE 要約仕様根拠

### 8.3.1. TOE セキュリティ機能根拠

#### 8.3.1.1. 必要性

TOE のセキュリティ機能と TOE セキュリティ機能要件との適合性を下表に示す。TOE のセキュリティ機能が少なくとも 1 つ以上の TOE セキュリティ機能要件に対応していることを示している。

表 12　TOE セキュリティ機能要件に対する TOE セキュリティ機能の適合性

| TOE セキュリティ機能 / TOE セキュリティ機能要件 | F.ADMIN | F.SERVICE | F.BOX | F.PRINT | F.OVERWRITE-FILE | F.OVERWRITE-ALL | F.HDD | F.RESET |
|---|---|---|---|---|---|---|---|---|
| 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] | | ● | | | | | | |

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

| TOE セキュリティ機能 / TOE セキュリティ機能要件 | F.ADMIN | F.SERVICE | F.BOX | F.PRINT | F.OVERWRITE-FILE | F.OVERWRITE-ALL | F.HDD | F.RESET |
|---|---|---|---|---|---|---|---|---|
| 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] | | | | ● | | | | |
| FIA_UID.2[4] | | | ● | | | | | |
| FIA_USB.1 | | | ● | ● | | | | |
| FMT_MOF.1 | ● | | | | | | | |
| FMT_MSA.3 | | | | ● | | | | |
| 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] | ● | | | | | | | |
| FMT_SMR.1[3] | | | ● | | | | | |
| FPT_RVM.1 | ● | ● | ● | ● | | | ● | |
| FPT_SEP.1 | ● | ● | ● | ● | | | | |
| FNEW_RIP.1 | | | | | | ● | | |
| FIA_NEW.1 | | | | | | | ● | |

#### 8.3.1.2. 十分性

**各 TOE セキュリティ機能要件に対して適用される TOE セキュリティ機能について以下に説明する。**

- **FDP_ACC.1[1]**

  FDP_ACC.1[1]**は、オブジェクトであるボックス、ボックスファイルに対して制御されるサブジェクト、操作の関係を規定している。**
  F.BOX **は、利用者を代行するタスクが、ボックスファイルをダウンロードするためのボックスアクセス制御を実施する。**
  **従って本機能要件は満たされる。**

- **FDP_ACC.1[2]**

  FDP_ACC.1[2]**は、オブジェクトである機密文書プリントファイルに対して制御されるサブジェクト、操作の関係を規定している。**
  F.PRINT **は、利用者を代行するタスクが、機密文書プリントファイルを印刷するための機密文書**

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

プリントファイル制御を実施する。
従って本機能要件は満たされる。

- FDP_ACC.1[3]

FDP_ACC.1[3]は、オブジェクトである HDD ロックパスワードオブジェクト、MFP アドレスグループオブジェクトに対して制御されるサブジェクト、操作の関係を規定している。
F.ADMIN は、利用者を代行するタスクが、HDD ロックパスワードオブジェクト、MFP アドレスグループオブジェクトを、設定する管理者モードアクセス制御を実施する。
従って本機能要件は満たされる。

- FDP_ACF.1[1]

FDP_ACF.1[1]は、オブジェクトであるボックス、ボックスファイルに対して制御されるサブジェクト、操作の関係の規則を規定している。
F.BOX は、以下の規則が適用されるボックスアクセス制御を実施する。

- ボックスの利用が許可されたユーザに対して、選択した共有ボックス内のボックスファイルのダウンロード操作を許可する。

従って本機能要件は満たされる。

- FDP_ACF.1[2]

FDP_ACF.1[2]は、オブジェクトである機密文書プリントファイルに対して制御されるサブジェクト、操作の関係の規則を規定している。
F.PRINT は、以下の規則が適用される機密文書プリントファイルアクセス制御を実施する。

- 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対して、選択した機密文書プリントファイルの印刷操作を許可する。

従って本機能要件は満たされる。

- FDP_ACF.1[3]

FDP_ACF.1[3]は、オブジェクトである HDD ロックパスワードオブジェクト、MFP アドレスグループオブジェクトに対して制御されるサブジェクト、操作の関係の規則を規定している。
F.ADMIN は、以下の規則が適用される管理者モードアクセス制御を実施する。

- 管理者に対して HDD ロックパスワードオブジェクト、MFP アドレスグループオブジェクトの設定操作を許可する。

従って本機能要件は満たされる。

- FDP_RIP.1

FDP_RIP.1 は、資源（HDD）からの割当解除された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 蓄積画像ファイルの保護を規定している。
F.OVERWRITE-FILE は、ジョブの実行完了時や削除操作された場合に、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 蓄積画像ファイルを削除方式に則り上書き処理を行う。
従って本機能要件は満たされる。

- FIA_AFL.1[1]

FIA_AFL.1[1]は、サービスエンジニアの認証に対する不成功認証時アクションを規定している。
F.SERVICE は、サービスモードへのアクセス、サービスコードの変更の際に行うサービスエンジニアの認証において、失敗回数閾値（3 回）の認証失敗を検知すると、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て、認証機能をロックする。認証中でなければ、認証機能を

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

ロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。
従って本機能要件は満たされる。

- FIA_AFL.1[2]

FIA_AFL.1[2]は、管理者の認証に対する不成功認証時アクションを規定している。
F.ADMIN は、管理者モードへのアクセス、管理者パスワードの変更の際に行う管理者の認証において、失敗回数閾値（3 回）の認証失敗を検知すると、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て、認証機能をロックする。認証中でなければ、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。
従って本機能要件は満たされる。

- FIA_AFL.1[3]

FIA_AFL.1[3]は、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の認証に対する不成功認証時アクションを規定している。
F.PRINT は、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の認証において、失敗回数閾値（3 回）の認証失敗を検知すると当該機密文書プリントファイルへのアクセスを拒否して、認証機能をロックする。
F.ADMIN は、管理者モード内にて提供するロック解除機能によりこのロック状態を解除する。
従って本機能要件は満たされる。

- FIA_AFL.1[4]

FIA_AFL.1[4]は、ボックスの利用を許可されたユーザであることの認証に対する不成功認証時アクションを規定している。
F.BOX は、ボックスへのアクセス、ボックスのパスワード変更の際に行う認証において、失敗回数閾値（3 回）の認証失敗を検知すると当該ボックスへのアクセスを拒否して、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。また F.ADMIN は、管理者モード内にて提供するロック解除機能によりこのロック状態を解除する。
従って本機能要件は満たされる。

- FIA_ATD.1

FIA_ATD.1 は、利用者に関係付けられるセキュリティ属性を規定している。
F.BOX は、利用者を代行するタスクに対してボックス ID を関係付ける。
F.PRINT は、利用者を代行するタスクに対して機密文書内部制御 ID を関係付ける。
従って本機能要件は満たされる。

- FIA_SOS.1[1]

FIA_SOS.1[1]は、管理者パスワードの品質を規定している。
F.ADMIN は、管理者パスワードの品質として 8 桁の数字で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

- FIA_SOS.1[2]

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

FIA_SOS.1[2]は、機密文書パスワード、ボックスパスワードの品質を規定している。
F.ADMIN は、ボックスパスワードの品質として 8 桁の合計 92 文字の ASCII コード（0x20 ～ 0x7E、ただし 0x22、0x2B、0x5E を除く）で、同一キャラクタから構成されないことを検証する。
F.BOX は、ボックスパスワードの品質として 8 桁の合計 92 文字の ASCII コード（0x20 ～ 0x7E、ただし 0x22、0x2B、0x5E を除く）で、同一キャラクタから構成されないことを検証する。
F.PRINT は、機密文書パスワードの品質として 8 桁の合計 92 文字の ASCII コード（0x20 ～ 0x7E、ただし 0x22、0x2B、0x5E を除く）で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

- FIA_SOS.1[3]

FIA_SOS.1[3]は、HDD ロックパスワードの品質を規定している。
F.ADMIN は、HDD ロックパスワードの品質として 20 桁の合計 82 文字の ASCII コード（0x20 ～ 0x7E、ただし 0x20、0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D、0x5E を除く）で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

- FIA_SOS.1[4]

FIA_SOS.1[4]は、サービスコードの品質を規定している。
F.SERVICE は、サービスコード、の品質として 8 桁の数字、#、*で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

- FIA_UAU.2[1]

FIA_UAU.2[1]は、サービスエンジニアの認証を規定している。
F.SERVICE は、サービスコードを使ってサービスモードへ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認証する。
従って本機能要件は満たされる。

- FIA_UAU.2[2]

FIA_UAU.2[2]は、管理者の認証を規定している。
F.ADMIN は、管理者パスワードを使って管理者モードへアクセスする利用者が管理者であることを認証する。
従って本機能要件は満たされる。

- FIA_UAU.2[3]

FIA_UAU.2[3]は、機密文書プリントファイルの利用を許可されたユーザの認証を規定している。
F.PRINT は、各機密文書プリントファイルに対して設定される機密文書パスワードを使っ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する。
従って本機能要件は満たされる。

- FIA_UAU.2[4]

FIA_UAU.2[4]は、ボックスの利用を許可されたユーザの認証を規定している。
F.BOX は、各ボックスに対して設定されるボックスパスワードを使って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。
従って本機能要件は満たされる。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- FIA_UAU.6

  FIA_UAU.6 は、パスワードの変更といった重要な操作の際の再認証を規定している。
  F.ADMIN は、管理者パスワードの変更操作において管理者を再認証する。また HDD ロックパスワードの変更操作に伴い、既登録済みの HDD ロックパスワードの照合によって各秘密情報を知り得る管理者であることを再認証する。
  F.SERVICE は、サービスコードの変更操作においてサービスエンジニアを再認証する。
  従って本機能要件は満たされる。

- FIA_UAU.7

  FIA_UAU.7 は、認証中のフィードバックに“＊”を返すことを規定している。
  F.ADMIN は、管理者の認証、再認証においてパネルにて入力される管理者パスワードに対して 1 文字毎に“＊”返し、管理者パスワードのダイレクト表示を防止する。
  F.SERVICE は、サービスエンジニアの認証、再認証においてパネルにて入力されるサービスコードに対して 1 文字毎に“＊”返し、サービスコードのダイレクト表示を防止する。
  F.PRINT は、機密文書プリントファイルの利用を許可されたユーザのであることの認証においてパネルにて入力される機密文書パスワードに対して 1 文字毎に“＊”返し、機密文書パスワードのダイレクト表示を防止する。
  従って本機能要件は満たされる。

- FIA_UID.2[1]

  FIA_UID.2[1]は、サービスエンジニアの識別を規定している。
  F.SERVICE は、サービスモードへアクセスする利用者がサービスエンジニアであると識別する。
  従って本機能要件は満たされる。

- FIA_UID.2[2]

  FIA_UID.2[2]は、管理者の認証を規定している。
  F.ADMIN は、管理者モードへアクセスする利用者が管理者であると識別する。
  従って本機能要件は満たされる。

- FIA_UID.2[3]

  FIA_UID.2[3]は、機密文書プリントファイルの利用を許可されたユーザの識別を規定している。
  F.PRINT は、操作対象として機密文書プリントファイルを選択することにより、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と識別する。
  従って本機能要件は満たされる。

- FIA_UID.2[4]

  FIA_UID.2[4]は、ボックスの利用を許可されたユーザの識別を規定している。
  F.BOX は、操作対象としてボックスを選択することにより、ボックスの利用を許可されたユーザであると識別する。
  従って本機能要件は満たされる。

- FIA_USB.1

  FIA_USB.1 は、利用者を代行するサブジェクトへのセキュリティ属性関連付けを規定している。
  F.PRINT は、利用者を代行するタスクに“機密文書内部制御 ID”を関連付ける。
  F.BOX は、利用者を代行するタスクに“ボックス ID”を関連付ける。
  従って本機能要件は満たされる。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

- FMT_MOF.1

  FMT_MOF.1 は、セキュリティ強化機能のふるまい管理を規定している。
  F.ADMIN は、管理者モードにおいてセキュリティ強化機能の設定機能を提供しており、当該機能の停止操作が管理されている。全領域上書き削除機能も実行に伴いセキュリティ強化設定を無効とするが、F.ADMIN により管理者だけに操作が許可される。
  従って本機能要件は満たされる。

- FMT_MSA.3

  FMT_MSA.3 は、機密文書プリントファイルの登録時に設定される機密文書内部制御 ID を規定している。
  F.PRINT は、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付与する。
  従って本機能要件は満たされる。

- FMT_MTD.1[1]

  FMT_MTD.1[1]は、ボックスパスワードの管理を規定している。
  F.ADMIN は、管理者モードにてボックスに設定されるボックスパスワードの変更操作を許可している。
  F.BOX は、ボックスの利用を許可されたユーザに対して、当該ボックスのボックスパスワードの変更操作を許可している。
  従って本機能要件は満たされる。

- FMT_MTD.1[2]

  FMT_MTD.1[2]は、管理者パスワードの管理を規定している。
  F.ADMIN は、管理者モードにて管理者パスワードの変更操作を許可している。
  従って本機能要件は満たされる。

- FMT_MTD.1[3]

  FMT_MTD.1[3]は、管理者パスワードの管理を規定している。
  F.SERVICE は、サービスモードにて FAX ユニットを介して、または E-mail で管理者パスワードを送信する機能（管理者パスワードの問い合わせに相当する）を許可している。
  従って本機能要件は満たされる。

- FMT_MTD.1[4]

  FMT_MTD.1[4]は、サービスコードの管理を規定している。
  F.SERVICE は、サービスモードにてサービスコードの変更操作を許可している。
  従って本機能要件は満たされる。

- FMT_SMF.1

  FMT_SMF.1 は、セキュリティ管理機能を特定している。
  F.ADMIN は、以下のセキュリティ管理機能を提供する。
  - セキュリティ強化機能の停止機能
  - 管理者パスワードの変更機能
  - ボックスパスワードの変更機能
  - ロック解除機能

    以下の認証機能に対して提供する。
    ・ボックスへのアクセスにおける認証機能

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

・機密文書プリントへのアクセスにおける認証機能

F.SERVICE は、以下のセキュリティ管理機能を提供する。

- サービスコードの変更機能
- 管理者パスワードの問い合わせ機能

F.BOX は、以下のセキュリティ管理機能を提供する。

- ボックスパスワードの変更機能

従って本機能要件は満たされる。

- FMT_SMR.1[1]

FMT_SMR.1[1]は、役割：サービスエンジニアを規定している。
F.SERVICE は、サービスコードにより認証された利用者をサービスエンジニアとして認識する。
従って本機能要件は満たされる。

- FMT_SMR.1[2]

FMT_SMR.1[2]は、役割：管理者を規定している。
F.ADMIN は、管理者パスワードにより認証された利用者を管理者として認識する。
従って本機能要件は満たされる。

- FMT_SMR.1[3]

FMT_SMR.1[3]は、役割：そのボックスの利用を許可されたユーザを規定している。
F.BOX は、ボックスパスワードにより認証された利用者をそのボックスの利用を許可されたユーザとして認識する。
従って本機能要件は満たされる。

- FPT_RVM.1

FPT_RVM.1 は、TOE の各セキュリティ機能の動作進行が許可される前に、必ず TSP 実施機能が必ず呼び出されることをサポートすることを規定している。
F.ADMIN は､管理者だけが扱える諸機能の利用が許可される前に､動作することが必須である“ 管理者認証機能 ” を必ず起動する。
F.SERVICE は、サービスエンジニアだけが扱える諸機能の利用が許可される前に、動作することが必須である “ サービスエンジニア認証機能 ” を必ず起動する。
F.BOX は、ボックスの利用を許可されたユーザだけが扱える諸機能の利用が許可される前に、動作することが必須である “ ボックスパスワードによる認証機能 ” を必ず起動する。
F.PRINT は、機密文書の利用を許可されたユーザだけが扱える諸機能の利用が許可される前に、動作することが必須である “ 機密文書パスワードによる認証機能 ” を必ず起動する。
F.HDD は、HDD ロック機能の動作時において HDD の書き込みが許可される前に、動作することが必須である “ HDD の正当性検証機能 ” を必ず起動する。
従って本機能要件は満たされる。

- FPT_SEP.1

FPT_SEP.1 は、信頼されないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間を分離することを規定している。
F.ADMIN は､管理者だけが操作することを許可される諸機能が提供される管理者認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
F.BOX は、ボックスパスワードによる認証により、ボックスの利用を許可されたユーザだけが操作することを許可される諸機能が提供されるボックス認証ドメインを保持し、許可されないサブ

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

ジェクトによる干渉行為を許可しない。
F.PRINT は、機密文書パスワードによる認証により、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が操作することを許可される諸機能が提供される機密文書プリントファイル認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。
F.SERVICE は、サービスエンジニアだけが操作することを許可される諸機能が提供されるサービスエンジニア認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。

- FNEW_RIP.1
  FNEW_RIP.1 は、明示的な消去操作において対象となるオブジェクト及び TSF データが復旧できないことを規定している。
  F.OVERWRITE-ALL は、HDD の全データ領域に対して上書き削除を行うことによって、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を削除する。また NVRAM の管理者パスワードを初期値に戻し、送信宛先データファイル、HDD ロックパスワードを削除する。
  従って本機能要件は満たされる。

- FIA_NEW.1
  FIA_NEW.1 は、TSF から利用者に対してアクションする前に利用者の識別を規定している。
  F.HDD は、HDD ロックパスワードを設定している場合に、HDD のステータスをチェックし HDD ロックパスワードが設定されていなければ、HDD への書き込み、読み込み処理を行なわない。HDD ロックパスワードが確かに設定されていると確認された場合のみ HDD への読み込み、書き込みを許可する。
  従って本機能要件は満たされる。

### 8.3.2. TOE セキュリティ機能強度根拠

確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りである。

① F.ADMIN が提供する管理者パスワード認証メカニズム
② F.SERVICE が提供するサービスコード認証メカニズム
③ F.PRINT が提供する機密文書パスワード認証メカニズム
④ F.BOX が提供するボックスパスワード認証メカニズム
⑤ F.ADMIN が提供する HDD ロックパスワード照合メカニズム

①は 8 桁 10 種類のキャラクタ、②は 8 桁 12 種類のキャラクタ、③及び④は 8 桁 92 種のキャラクタ、⑤は 20 桁 82 種のキャラクタから構成される秘密を利用する。このうち①～④は、認証操作禁止機能の動作によって、連続 3 回の不成功認証により認証機能はロックする。

従って 6.2 節にて主張される通り、これらメカニズムの機能強度は SOF-基本を十分満たしており、5.1.2 項にてセキュリティ機能強度主張される TOE セキュリティ機能要件に対して主張される最小機能強度：SOF-基本と一貫している。

### 8.3.3. 相互サポートする TOE セキュリティ機能

TOE 要約仕様で識別される IT セキュリティ機能が組み合わさることにより満たされる TOE セキュリティ機能要件は、8.3.1 項に記述される各根拠記述にて述べられる通りである。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.

### 8.3.4. 保証手段根拠

評価保証レベル EAL3 において必要なドキュメントは 6.4 節において説明される保証手段に示されたドキュメント資料により網羅されている。これら保証手段として提示されているドキュメントに従った開発、テストの実施、脆弱性の分析、開発環境の管理、構成管理、配付手続きが実施され、適切なガイダンス文書が作成されることにより、TOE セキュリティ保証要件が満たされる。

## 8.4. PP 主張根拠

本 ST が参照する PP はない。

Copyright © 2006 KONICA MINOLTA BUSINESS TECHNOLOGIES, INC., All Rights Reserved.