bizhub C650 / ineo+ 650 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：1.06

発行日：2007年8月24日

作成者：コニカミノルタビジネステクノロジーズ株式会社

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2007/01/22	1.00	制御第12開発部	廣田	中島	吉田	初版 ～bizhub C450系との差異について（20～30%変更）～ ・組織のセキュリティ方針追加、概念説明 - 高信頼チャネル機能の追加 - S/MIME機能の追加 ・部門制御の概念を追加 ・ユーザー意性の概念変更（外部サーバ認証考慮） ・向上した認証機能のロック処理の仕様を反映 ・セキュリティ強化条件追加、修正反映 ・CCv2.3対応 ・ハード環境構成の変更対応
2007/02/28	1.01	制御第12開発部	廣田	中島	吉田	・誤植対応（内部レビュー）
2007/06/20	1.02	制御第12開発部	廣田	中島	吉田	・誤植対応
2007/07/05	1.03	制御第12開発部	廣田	中島	吉田	・誤植対応
2007/07/20	1.04	制御第12開発部	廣田	中島	吉田	・誤植対応
2007/08/02	1.05	制御第12開発部	廣田	中島	吉田	・管理者ユーザモード反映 ・誤植対応 ・用語修正（機密文書⇒セキュリティ文書）
2007/08/24	1.06	制御第12開発部	廣田	中島	吉田	・誤植対応

—【 目次 】

—【 図目次 】

—【 表目次 】

1. ST 概説

1.1. ST 識別

・ST名称 : bizhub C650 / ineo+ 650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 : 1.06
・CCバージョン : 2.3
・作成日 : 2007年8月24日
・作成者 : コニカミノルタビジネステクノロジーズ株式会社　吉田 英一

1.2. TOE 識別

・TOE名称 : 日本名：
bizhub C650 / ineo+ 650 全体制御ソフトウェア
英名 :
bizhub C650 / ineo+ 650 Control Software
・TOE識別 : A00H0Y0-0100-GM0-00
・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**
補足-0512（Interpratations-0512）を適用する。

- **参考資料**
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model 2005 Version 2.3 CCMB-2005-08-001
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements 2005 Version 2.3 CCMB-2005-08-002
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements 2005 Version 2.3 CCMB-2005-08-003
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-001 （平成17年12月翻訳第1.0版 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）
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-002 （平成17年12月翻訳第1.0版 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）
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-003 （平成17年12月翻訳第1.0版 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-0512（平成17年12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 C650、ineo+ 650 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 C650 / ineo+ 650 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、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。

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。

2. TOE 記述

2.1. TOE の種別

TOE である bizhub C650 / ineo+ 650 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。

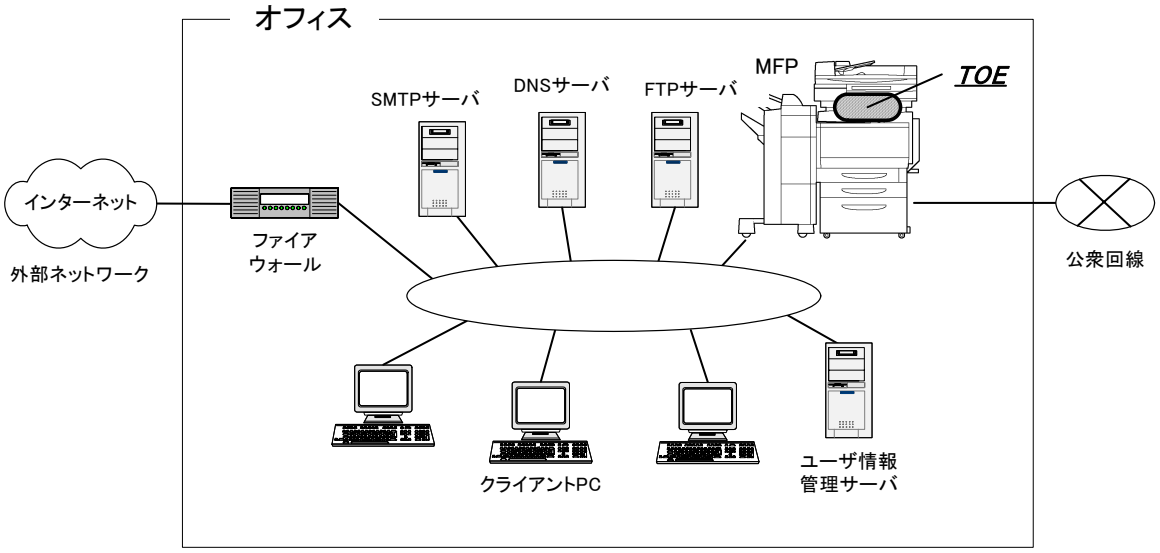

図 1 MFP の利用環境の例

- 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。)
- ユーザ ID、ユーザパスワードをサーバにて一元管理しているケースも想定する。この場合、ユーザ情報管理サーバにおけるユーザ登録情報を使って TOE は MFP へのアクセスを制御することが可能。
- オフィス内 LAN が外部ネットワークと接続する場合は、ファイアウォールを介して接続する等の措置が取られ、外部ネットワークから MFP に対するアクセスを遮断するための適切な設定が行われる。
- オフィス内 LAN は、スイッチングハブ等の利用、盗聴の検知機器の設置などオフィスの運用によって、盗聴されないネットワーク環境が整備されている。
- MFP に接続される公衆回線は、FAX や遠隔サポート機能の通信に利用される。

2.3. TOE の動作環境構成

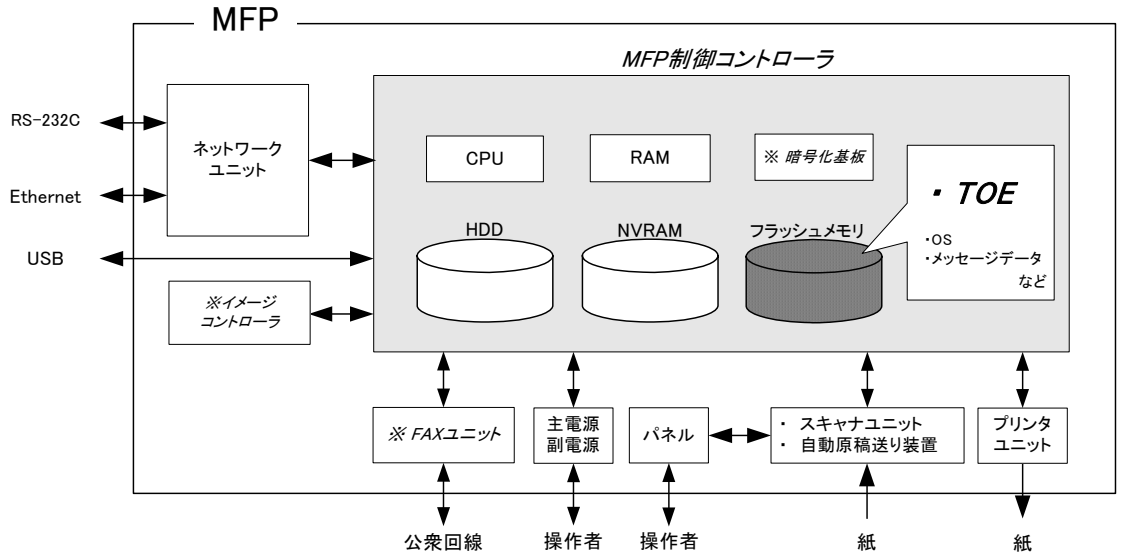

図 2 TOE に関係するハードウェア構成

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。

- HDD

  容量 60GB のハードディスクドライブ。画像データがファイルとして保管されるほか、伸張変換などで一時的に画像データ、送信宛先データが保管される領域としても利用される。
  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。

- NVRAM

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

- 暗号化基板（※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。

- **主電源**
  MFP を動作させるための電源スイッチ。

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

- USB
  ローカル接続でプリントすためのポート。MFP 制御コントローラに対して直接接続されるインタフェースを持つ。

- **イメージコントローラ（※オプションパーツ）**
  MFP 制御コントローラとビデオバスで接続される Fiery 等のコントローラ。

- FAX ユニット（※オプションパーツ）
  公衆回線を介して FAX の送受信や遠隔診断機能（後述）の通信に利用されるデバイス。販売上の都合により MFP には標準搭載されず、オプションパーツとして販売される。

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

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

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

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

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

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

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

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

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

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、利用者であるユーザの識別認証機能、管理者が操作する管理者機能、サービスエンジニアが操作するサービスエンジニア機能、ユーザには意識されずにバックグラウンドで動作する機能といった代表的な機能について説明する。

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圧縮変換し、RAM や HDD に登録する。(PC からのプリント画像ファイルは、複数の変換処理を行なった後に圧縮変換される。)圧縮変換された画像ファイルは、印刷用または送信用のデータとして伸張変換され、目的の MFP 制御コントローラ外部のデバイスに転送される。

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

以下は基本機能においてセキュリティと関係する機能である。

- セキュリティ文書プリント機能
  プリントデータと共にセキュリティ文書パスワードを受信した場合、画像ファイルを印刷待機状態で保管し、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. 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、ユーザが占有する個人ボックス、登録されたユーザが一定数のグループを作って共同利用するための共有ボックス、所属部門のユーザ間で共有するグループボックスといった 3 つのタイプのボックスを設定することができる。個人ボックスは、所有するユーザだけに操作が制限され、共有ボックスは、そのボックスに設定されるパスワードを利用者間で共用することによって、アクセス制御を行っている。グループボックスは、その部門の利用を許可されたユーザだけに操作が制限される。

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

- ボックス内の画像ファイルの印刷、送信、クライアント PC からのダウンロード
  - 送信方法の 1 つである E-mail においてボックスファイルの暗号化（S/MIME）が可能
- ボックス内の画像ファイルの削除、他のボックスへの移動・コピー
- 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
- ボックスの属性設定（個人ボックス、共有ボックス、グループボックスの種別変更）

2.5.3. ユーザ認証機能

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

ユーザ認証の方式には、以下に示すいくつかのタイプをサポートしている。

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

② **外部サーバ認証**
MFP本体側でユーザID及びユーザパスワードを管理せず、オフィス内LANで接続されるユーザ情報管理サーバ上に登録されるユーザID及びユーザパスワードを用いて、MFPにて認証処理を行い、認証する方式。Active Directory[1]、NTLM[2]、NDS等といった複数の方式をサポートしているが、本STにおいて想定する外部サーバ認証の方式は、Active Directoryの利用ケースのみとする。

[1] Windows プラットフォームのネットワーク環境にてユーザ情報を一元管理するために Windows Server 2000（それ以降）が提供するディレクトリサービスの方式。
[2] NT LAN Manager の略。Windows プラットフォームのネットワーク環境にてユーザ情報を一元管理するために Windows NT が提供するディレクトリサービスにおいて利用される認証方式。

2.5.4. 部門認証機能

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

① **ユーザ認証連動方式**
ユーザに予め部門 ID を設定し、ユーザの認証時に所属部門の部門 ID と関連づける方式
② **個別認証方式**
各部門 ID に設定される部門パスワードによって認証された場合に当該部門 ID と関連づける方式

2.5.5. 管理者機能

TOE は、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、本体認証の場合におけるユーザの情報の管理、ネットワークや画質等の各種設定の管理などの機能を提供する。
以下にはセキュリティに関係する機能について例示する。

- ユーザの登録管理
  - ユーザ ID、ユーザパスワードの登録・変更、ユーザの削除
  - ユーザに対する部門 ID の関連付け変更
- 部門の登録管理
  - 部門 ID、部門パスワードの登録・変更
- ボックスの設定管理
  - ボックスパスワードの登録・変更、ユーザ属性の管理
- オートシステムリセットの動作設定
  - 設定時間が経過すると、自動的にログアウトする機能の設定
- ネットワーク設定管理
  - オフィス内 LAN との接続設定（DNS サーバの設定）
  - SMTP 設定（E-mail 送信にて利用する SMTP サーバの設定）
  - IP アドレス、NetBIOS 名、AppleTalk プリンタ名など
- NVRAM、HDD のバックアップ及びリストア機能
  - クライアント PC に導入される管理用の専用アプリケーションを利用して、ネットワークを介して実行される。
- HDD の完全上書き削除機能
  - 各種軍用規格などに則ったデータ削除方式が存在
  - 起動すると、設定された方式に則り、HDD の全領域に対して上書き削除を実行する。
- HDD のフォーマット機能
  - 論理フォーマットが実行可能。

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- ユーザ認証機能の方式設定
  - 本体認証、外部サーバ認証、ユーザ認証停止を選択
  - 部門認証機能との組み合わせを設定（ユーザ認証機能連動方式、部門個別認証方式）
- ユーザ：PUBLIC によるアクセスの設定
  - ユーザ ID で特定されない利用者の MFP 利用を許可、禁止を選択

- パスワード規約機能の設定
  - 各種パスワードの有効桁数等、パスワード諸条件をチェックする機能の動作、禁止を選択
- セキュリティ文書プリントの認証方式及び認証操作禁止機能の設定
  - セキュリティ文書プリントの認証に対して認証操作禁止機能が動作するモード、しないモードが存在
  - 各認証機能における不成功認証の検出する機能の動作モードも連動
  - 上記の動作モードを選択
- SNMPv1、v2 によるネットワーク設定変更機能の設定
  - SNMPv1、v2 による MIB の変更操作機能を許可、禁止を選択
- 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、暗号化ワードを登録・変更
- ボックス一括管理機能の設定
  - ボックスの一括管理機能を許可、禁止を選択
- プリントキャプチャ機能の設定
  - プリント機能の故障時などに MFP が受信するプリントデータを確認するための機能
  - 上記機能を動作、停止を選択
- ネットワーク設定管理リセット機能の設定
  - ネットワーク設定管理リセット機能は、一連の項目を工場出荷値にリセットする。
  - 上記機能を許可、禁止を選択
- 高信頼チャネル（SSL/TLS 暗号通信）機能の設定
  - SSL/TLS サーバ証明書を生成、またはインポート
  - 通信に利用される暗号方式の設定
- 送信宛先データの設定
  - ボックスファイル送信などに利用される送信宛先、送信方法などを設定
  - S/MIME 証明書のインポート
  - データ暗号化に利用される暗号方式の設定

2.5.6. サービスエンジニア機能

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

- 管理者パスワードの変更機能

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- CE[3]パスワードによるサービスエンジニアの認証の設定
  - 動作、停止を選択
- 遠隔診断機能（後述）の設定
  - 利用、禁止を選択することが可能。

[3] Customer Service engineer の略称。

- インターネット経由 TOE 更新機能の設定
  - 利用、禁止を選択することが可能。
- メンテナンス機能の設定
  - 利用、禁止を選択することが可能。
- HDD のフォーマット機能
  - 論理フォーマット、物理フォーマットが実行可能。
- HDD の装着設定
  - HDD をデータ保管領域として利用するには、明示的な装着設定が必要。
  - 装着設定を行うと論理フォーマットが実施される。
- イニシャライズ機能
  - 管理者、ユーザが設定した各種設定値、ユーザが保管したデータを削除する。

2.5.7. その他の機能

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

① **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化ワードより暗号鍵を生成する。

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**

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

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。更新手段は、遠隔診断機能の項目の 1 つとしても存在する他、Ethernet を介して FTP サーバよりダウンロードする方法(インターネット経由 TOE 更新機能)、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。

⑤ **暗号通信機能**

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

⑥ S/MIME 証明書自動登録機能
S/MIME 用に各宛先に設定可能な証明書（ITU-T X.509 準拠）を自動登録する機能。メールに証明書が添付されている場合、当該メールのヘッダー情報にてユーザ ID を判別し、証明書を当該ユーザの証明書として登録する。

2.5.8. セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また個別には動作設定機能を持たない機能として、ネットワーク設定のリセット機能、ネットワーク介した TOE の更新機能が存在するが、これら機能の利用は禁止される。

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

- ユーザ識別認証機能の設定 ：有効（本体認証、外部サーバ認証のどちらでも可）
- ユーザ：PUBLIC のアクセスの設定 ：禁止
- サービスエンジニア認証機能の設定 ：有効
- パスワード規約機能の設定 ：有効
- セキュリティ文書プリントの認証方式の設定 ：認証操作禁止機能有効方式（連動してパネルにおける
  認証失敗時 5 秒間のパネルのロック、且つアカウントロック（失敗回数閾値：1～3 回）状態にもなる。）
- ボックス一括管理機能の設定 ：禁止
- SNMPv1、v2 によるネットワーク設定変更機能の設定
  ：禁止
- 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）
- プリントキャプチャ機能の設定 ：禁止
- メンテナンス機能の設定 ：禁止
- 遠隔診断機能 ：禁止
- ネットワーク設定管理リセット機能 ：禁止
- インターネット経由 TOE の更新機能 ：禁止
- ユーザによる送信宛先データの設定機能 ：禁止
- 高信頼チャネル機能の動作設定 ：有効

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

TOE のセキュリティコンセプトは、**“ユーザの意図に反して暴露される可能性のあるデータの保護”**である。MFP を通常の利用方法で使用している場合、利用可能な状態にある以下の画像ファイルを保護対象とする。

- **セキュリティ文書プリントファイル（セキュリティ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（個人ボックス、共有ボックス、グループボックスに保管される画像ファイル）**

複数のジョブの動作により待機状態として保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。

なおセキュリティ文書プリントファイルの印刷、ボックスファイルの送信においては、万が一不正な MFP やメールサーバなどが接続された場合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。

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

- **セキュリティ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**
  - 待機状態にあるジョブの画像ファイル
- **保管画像ファイル**
  - セキュリティ文書プリントファイル、ボックスファイル以外の保管される画像ファイル
- **残存画像ファイル**
  - 一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、HDD データ領域に残存するファイル
- **画像関連ファイル**
  - プリント画像ファイル処理において生成されたテンポラリデータファイル
- **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。

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

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

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

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

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

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。

A.SERVER（オフィス内 LAN に接続されるユーザ情報管理サーバの管理条件）
ユーザ認証方式に外部サーバ認証を利用する場合、TOE が搭載される MFP を設置するオフィス内 LAN に接続されるユーザ情報管理サーバは、アカウントの管理、アクセス制御、パッチ適用などが適切に実施されている。

3.3. 脅威

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

T.DISCARD-MFP（MFP のリース返却、廃棄）
リース返却、または廃棄となった MFP が回収された場合、悪意を持った者が、MFP 内の HDD や NVRAM を解析することにより、セキュリティ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、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等の秘匿情報が漏洩する。

T.BRING-OUT-STORAGE（HDD の不正な持ち出し）
・悪意を持った者や悪意を持ったユーザが、MFP 内の HDD を不正に持ち出して解析することにより、セキュリティ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、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が漏洩する。
・悪意を持った者や悪意を持ったユーザが、MFP 内の HDD を不正にすりかえる。すりかえられた HDD には新たにセキュリティ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、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえた HDD を持ち出して解析することにより、これら画像ファイル等が漏洩する。

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

悪意を持った者や悪意を持ったユーザが、他のユーザが個人所有するボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX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-PUBLIC-BOX（ユーザ機能を利用した共有ボックスへの不正なアクセス）

悪意を持った者や悪意を持ったユーザが、利用を許可されない共有ボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail 送信、FTP 送信、FAX 送信、SMB 送信）、他のボックスへ移動・コピーすることにより、ボックスファイルが暴露される。

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

悪意を持った者や悪意を持ったユーザが、そのユーザが所属していない部門が所有するグループボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail 送信、FTP 送信、FAX 送信、SMB 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セキュリティ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セキュリティ文書プリントファイルを印刷することにより、セキュリティ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、ボックスファイルの送信に関係するネットワーク設定を変更することにより、宛先が正確に設定されていてもボックスファイルがユーザの意図しないエンティティへ送信（E-mail 送信、FTP 送信）されてしまい、ボックスファイルが暴露される。

＜ボックスファイル送信に関係するネットワーク設定＞

- SMTP サーバに関する設定
- DNS サーバに関する設定

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

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、セキュリティ文書プリントファイルが漏洩する可能性が高まる。

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

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

[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。

3.4. 組織のセキュリティ方針

昨今、オフィス内でもネットワークのセキュアさを要求する組織は多い。本 ST では、オフィス内 LAN 上での盗聴行為等の脅威を想定しないが、オフィス内 LAN 上のセキュリティ対策が要求される組織にも対応した TOE セキュリティ環境を想定する。特に前項にて示した機密性が考慮される保護対象資産に対するセキュアな通信に対応する。

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

P.COMMUNICATION-DATA（画像ファイルのセキュアな通信）

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

4. セキュリティ対策方針

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

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.REGISTERED-USER（登録ユーザの利用）

TOE は、登録されたユーザだけに TOE の搭載された MFP の利用を許可する。

O.PRIVATE-BOX（個人ボックスアクセス制御）

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

O.PUBLIC-BOX（共有ボックスアクセス制御）

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

O.GROUP-BOX（グループボックスアクセス制御）

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

O.SECURE-PRINT（セキュリティ文書プリントファルアクセス制御）

TOE は、そのセキュリティ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、そのセキュリティ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
・バックアップ機能
・リストア機能
・高信頼チャネル機能設定データの設定機能
・S/MIME 機能で利用する証明書、送信宛先データ等の設定機能

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

O.OVERWRITE-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、管理者が設定した秘匿性のある NVRAM 上のパスワード（管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号化ワード）の設定値を初期化する機能を提供する。

O.CRYPTO-KEY（暗号鍵生成）

TOE は、MFP 内の HDD に書き込まれる画像ファイルを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.TRUSTED-PASS（高信頼チャネルの利用）

TOE は、MFP と PC の間で送受信される以下の画像ファイルを、高信頼チャネルを介して通信する機能を提供する。

＜MFP から PC 送信される画像ファイル＞

・ボックスファイル

＜PC から MFP へ送信される画像ファイル＞

・ボックスファイルとして保存されることになる画像ファイル

・セキュリティ文書プリントファイルとして保存されることになる画像ファイル

O.CRYPTO-MAIL（暗号化メールの利用）

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

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.CRYPTO（HDD の暗号化）

MFP 内に設置される暗号化基板は、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 HDD に保管する。

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 だけのデータの読み出しを受け付ける。

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などのアプリケーションは、入力されるユーザパスワード、ボックスパスワード、部門パスワード、管理者パスワード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.SECRET（秘密情報の適切な管理）

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

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

サービスエンジニアは以下に示す運用を実施する。
・CE パスワードに推測可能な値を設定しない。
・CE パスワードを秘匿する。
・CE パスワードの適宜変更を行う。
・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-N.SERVER（セキュアなユーザ情報管理サーバ）

MFP を利用する組織の責任者は、ユーザ情報管理サーバに対してアカウント管理、パッチの適用を行い、適切なアクセス制御を実施させる等、ユーザ情報管理サーバをセキュアに管理する。

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。

・セキュリティ文書プリントファイルの操作、ボックス及びボックスファイルの操作の終了後にログオフ操作を行う。

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-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。

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. 暗号サポート

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

表 1　暗号鍵生成　標準・アルゴリズム・鍵長の関係

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
FIPS 186	***擬似乱数生成アルゴリズム***	***・128 bit*** ***・192 bit*** ***・168 bit*** ***・256 bit***
コニカミノルタ暗号仕様標準	***コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）***	***128 bit***

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

表 2　暗号操作　アルゴリズム・鍵長・暗号操作の関係

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作の内容
FIPS PUB 197	*AES*	*・128 bit* *・192 bit* *・256 bit*	*S/MIME 送信データの暗号化*
SP800-67	*3-Key-Triple-DES*	*・168 bit*	*S/MIME 送信データの暗号化*
FIPS 186-1	*RSA*	*・1024bit* *・2048 bit* *・3072 bit* *・4096 bit*	*S/MIME 送信データ暗号化のための暗号鍵の暗号化*

5.1.1.2. 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 3　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 3　ボックスアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*ボックス*	*・一覧表示*
	ボックスファイル	*・印刷* *・送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信）* *・ダウンロード* *・他のボックスへの移動* *・他のボックスへのコピー* *・バックアップ*

FDP_ACC.1[2]　　サブセットアクセス制御
FDP_ACC.1.1[2]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*] : ***「表 4　セキュリティ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*] : ***セキュリティ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 4　セキュリティ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	*セキュリティ文書プリントファイル*	*・一覧表示* *・印刷* *・バックアップ*

FDP_ACC.1[3]　　サブセットアクセス制御
FDP_ACC.1.1[3]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*] : ***「表 5　設定管理アクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*] : ***設定管理アクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[3]）

表 5　設定管理アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*・HDD ロックパスワードオブジェクト* *・暗号化ワードオブジェクト*	*・　設定*
	・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* [5]	*・　設定* *・　リストア*

[5] 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。

FDP_ACF.1[1] セキュリティ属性によるアクセス制御

FDP_ACF.1.1[1]

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

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

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

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

＜個人ボックスに対する操作制御＞

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

＜個人ボックス内のボックスファイルに対する操作制御＞

利用者を代行するタスクは、サブジェクト属性のユーザ属性（ユーザ ID）、ボックス属性（ボックス ID）と一致するオブジェクト属性のユーザ属性、ボックス属性を持つボックスファイルに対して、印刷、送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信）、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作することが許可される。

＜グループボックスに対する操作制御＞

利用者を代行するタスクは、サブジェクト属性の所属部門（部門 ID）と一致するオブジェクト属性の所属部門を持つボックスに対して、一覧表示操作をすることが許可される。

＜グループボックス内のボックスファイルに対する操作制御＞

利用者を代行するタスクは、サブジェクト属性の所属部門（ユーザ ID）、ボックス属性（ボックス ID）と一致するオブジェクト属性のユーザ属性、ボックス属性を持つボックスファイルに対して、印刷、送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信）、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作することが許可される。

＜共有ボックスに対する操作制御＞

ユーザ属性（ユーザ ID）が関連づけられる利用者を代行するタスクは、オブジェクト属性のユーザ属性に「共有」が設定されているボックスに対して、一覧表示操作をすることが許可される。

＜共有ボックス内のボックスファイルに対する操作制御＞

ユーザ属性（ユーザ ID）とボックス属性（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、オブジェクト属性のユーザ属性に「共有」が設定され、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、印刷、送信（E-mail 送信、FTP 送信、SMB 送信、FAX 送信）、ダウンロード、他のボックスへの移動、他のボックスへのコピー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*]: ***・管理者属性を有する利用者を代行するタスクは、ボックスの一覧表示操作をすることを許可される。*** ***・管理者属性を有する利用者を代行するタスクは、ボックスファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[1]
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし。***
下位階層 : なし **依存性** : FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3（FMT_MSA.3[1]）

FDP_ACF.1[2] セキュリティ属性によるアクセス制御

FDP_ACF.1.1[2]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞ ＜サブジェクト属性＞*** ***・利用者を代行するタスク ⇒ ・ファイル属性（セキュリティ文書内部制御 ID）*** ***・ユーザ属性（ユーザ ID）*** ***・管理者属性*** --- ***＜オブジェクト＞ ＜オブジェクト属性＞*** ***・セキュリティ文書プリントファイル ⇒ ・ファイル属性（セキュリティ文書内部制御 ID）***
[割付: *アクセス制御 SFP*]: ***セキュリティ文書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*]: ***・ユーザ属性（ユーザ ID）を持つ利用者を代行するタスクは、あらゆるセキュリティ文書プリントファイルの一覧表示が許可される。*** ***・ユーザ属性（ユーザ ID）とファイル属性（セキュリティ文書内部制御 ID）を持つ利用者を代行するタスクは、ファイル属性（セキュリティ文書内部制御 ID）と一致するファイル属性（セキュリティ文書内部制御 ID）を持つセキュリティ文書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*]: ***管理者属性を有する利用者を代行するタスクは、セキュリティ文書プリントファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[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[2]）

FDP_ACF.1[3]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[3]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***・利用者を代行するタスク　　⇒　・管理者属性*** ***・CE 属性*** --- ***＜オブジェクト＞*** ***・HDD ロックパスワードオブジェクト*** ***・暗号化ワードオブジェクト*** ***・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***
[割付: *アクセス制御 SFP*]: ***設定管理アクセス制御***
FDP_ACF.1.2[3]
TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。
[割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]: ***・管理者属性を持つ利用者を代行するタスクは、HDD ロックパスワードオブジェクト、暗号化ワードオブジェクトを設定操作することが許可される。*** ***・管理者属性を持つ利用者を代行するタスクは、SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクトを設定、リストア操作することが許可される。*** ***・CE 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、暗号化ワードオブジェクトを設定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）

5.1.1.3. 識別と認証

FIA_AFL.1[1] 認証失敗時の取り扱い
FIA_AFL.1.1[1]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*] : ***・サービスモードにアクセスする際の認証*** ***・CE パスワードを改変する際の再認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[1]
不成功の認証試行が定義した回数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*] : ***＜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、CE パスワードを利用する認証機能をロックする。*** ***・認証中でなければ、CE パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***特定操作より CE 認証ロック解除機能を実行する。(特定操作から CE 認証ロック時間を経過すると解除処理が行なわれる。)***
下位階層 : なし
依存性 : FIA_UAU.1 (FIA_UAU.2[1])

FIA_AFL.1[2] 認証失敗時の取り扱い
FIA_AFL.1.1[2]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*] : ***・管理者モードにアクセスする際の認証*** ***・管理者パスワードを改変する際の再認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[2]
不成功の認証試行が定義した回数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*] : ***＜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＞*** ***・サービスモード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。(起動処理から管理者認証ロック時間後に解除処理が行なわれる。)***
下位階層 : なし
依存性 : FIA_UAU.1 (FIA_UAU.2[2])

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

FIA_AFL.1[4]　　認証失敗時の取り扱い
FIA_AFL.1.1[4]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]*」]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*] : ***ユーザが TOE にアクセスする際の認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]*」] ***[割付: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[4]
不成功の認証試行が定義した回数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*] : ***＜検出した際のアクション＞*** ***認証中であれば、当該ユーザの認証状態からログオフし、当該ユーザに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***管理者モード内にて提供される認証失敗回数の消去機能を実行する。***
下位階層　　:　なし
依存性　　:　FIA_UAU.1（FIA_UAU.2[3]）

FIA_AFL.1[5]　　認証失敗時の取り扱い
FIA_AFL.1.1[5]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]*」]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*] : ***セキュリティ文書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: 許容可能な値の範囲] : 1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[5]
不成功の認証試行が定義した回数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*] :

＜検出した際のアクション＞ *当該セキュリティ文書プリントファイルへのアクセスを拒否し、当該セキュリティ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認証失敗回数の消去機能を実行する。*
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[4]）

FIA_AFL.1[6]　　認証失敗時の取り扱い
FIA_AFL.1.1[6]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*]: ***共有ボックスにアクセスする際の認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[6]
不成功の認証試行が定義した回数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*]: *＜検出した際のアクション＞* *当該ボックスへの認証状態であればログオフし、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認証失敗回数の消去機能を実行する。*
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[5]）

FIA_AFL.1[7]　　認証失敗時の取り扱い
FIA_AFL.1.1[7]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*]: ***・部門認証：連動方式においてアクセスするユーザの所属部門が未登録の場合の部門認証*** ***・部門認証：個別認証方式においてアクセスするユーザの部門認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[7]
不成功の認証試行が定義した回数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*]: *＜検出した際のアクション＞* *当該部門に対する認証機能をロックし、以降当該部門の利用を許可されたユーザの TOE へのアクセスを拒否する。* *＜通常復帰のための操作＞* *管理者モード内にて提供される認証失敗回数の消去機能を実行する。*
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[6]）

FIA_AFL.1[8]　　認証失敗時の取り扱い
FIA_AFL.1.1[8]
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*] : ***・サービスモードにアクセスする際の認証*** ***・パネルより管理者モードにアクセスする際の認証*** ***・パネルよりユーザが TOE にアクセスする際のユーザ認証*** ***・パネルよりユーザが TOE にアクセスする際の部門認証*** ***・セキュリティ文書プリントファイルにアクセスする際の認証*** ***・パネルより共有ボックスにアクセスする際の認証***
[選択: *[割付:正の整数値], 「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」*] ***[割付:正の整数値]：1***
FIA_AFL.1.2[8]
不成功の認証試行が定義した回数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*] : ***＜検出した際のアクション＞*** ***パネルからのすべての入力受付拒否*** ***＜通常復帰のための操作＞*** ***5 秒経過後に自動解除***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.2[5]、FIA_UAU.2[6]）

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（セキュリティ文書内部制御 ID）*** ***・所属部門（部門 ID）***
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、CE パスワード）*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ***・桁数　：8 桁*** ***・文字種：ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）*** ***・規則　：① 同種の文字列だけで構成されていない。　② 現在設定されている値と合致しない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[2]　　秘密の検証
FIA_SOS.1.1[2]
TSF は、秘密 ***(SNMP パスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]: ***・桁数　：8 桁以上*** ***・文字種：ASCII コード（0x20 ～ 0x7E）***
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 ***(ユーザパスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]: ***・桁数　：8 桁以上*** ***・文字種：ASCII コード（0x20 ～ 0x7E）*** ***・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 ***(HDD ロックパスワード、暗号化ワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]: ***・桁数　：20 桁*** ***・文字種：ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く）*** ***・規則　：① 同種の文字列だけで構成されていない。　② 現在設定されている値と合致しない。***
下位階層　　:　なし
依存性　　:　なし

FIA_SOS.1[5]　　秘密の検証
FIA_SOS.1.1[5]
TSF は、秘密 ***(セキュリティ文書パスワード)*** 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：ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く）*** ***・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[6]　　秘密の検証
FIA_SOS.1.1[6]
TSF は、秘密 ***（セッション情報）*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]： ***10^{10} 以上***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[7]　　秘密の検証
FIA_SOS.1.1[7]
TSF は、秘密 ***（ボックスパスワード、部門パスワード）*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]： ***・桁数　：8 桁*** ***・文字種：ASCII コード（0x21 ～ 0x7E）*** ***・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.2　　秘密の検証
FIA_SOS.2.1
TSF は、[割付: *定義された品質尺度*]に合致する秘密（***セッション情報***）を生成するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]： ***10^{10} 以上***
FIA_SOS.2.2
TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付: *TSF 機能のリスト*]： ***・管理者認証（ネットワーク経由アクセス）*** ***・ユーザ認証（ネットワーク経由アクセス）*** ***・ボックス認証（ネットワーク経由アクセス）***
下位階層　：　なし
依存性　：　なし

FIA_UAU.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 ***（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 ***（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 ***（セキュリティ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 ***（セキュリティ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[4]）

FIA_UAU.2[5] アクション前の利用者認証

FIA_UAU.2.1[5]
TSF は、その利用者 ***（共有ボックスの利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に、各利用者 ***（共有ボックスの利用を許可されたユーザ）*** に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[5]）

FIA_UAU.2[6] アクション前の利用者認証

FIA_UAU.2.1[6]
TSF は、その利用者 ***（部門の利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に、各利用者 ***（部門の利用を許可されたユーザ）*** に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[6]）

FIA_UAU.6 再認証

FIA_UAU.6.1
TSF は、条件[割付: *再認証が要求される条件のリスト*]のもとで利用者を再認証しなければならない。
[割付: *再認証が要求される条件のリスト*] ***・管理者が管理者パスワードを改変する場合*** ***・サービスエンジニアが CE パスワードを改変する場合*** ***・管理者が HDD ロックの設定を変更する場合*** ***・管理者が暗号化機能の設定を変更する場合***
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_UAU.2[5]）

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 ***（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 ***（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 ***（セキュリティ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 ***（セキュリティ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[5] アクション前の利用者識別

FIA_UID.2.1[5]
TSF は、その利用者 ***（共有ボックスの利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に各利用者 ***（共有ボックスの利用を許可されたユーザ）*** に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[6]　　アクション前の利用者識別

FIA_UID.2.1[6]
TSF は、その利用者 ***（部門の利用を許可されたユーザ）*** を代行する他の TSF 調停アクションを許可する前に各利用者 ***（部門の利用を許可されたユーザ）*** に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[7]　　アクション前の利用者識別

FIA_UID.2.1[7]
TSF は、その利用者 ***（外部サーバ）*** を代行する他の TSF 調停アクションを許可する前に各利用者 ***（外部サーバ）*** 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（セキュリティ文書内部制御 ID）*** ***・所属部門（部門 ID）***
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。*** ***＜所属部門の場合＞*** ***・部門認証方式が個別認証方式の場合、部門に対するアクセスにおいて認証された際に、利用者を代行するタスクに当該部門の部門 ID を関連付ける。*** ***・部門認証方式がユーザ認証連動方式の場合、ユーザに対するアクセスにおいて認証された際に、利用者を代行するタスクに当該ユーザに設定されている部門 ID を関連づける。*** ***＜ファイル属性の場合＞*** ***セキュリティ文書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、当該セキュリティ文書プリントファイルのセキュリティ文書内部制御 ID 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

5.1.1.4. セキュリティ管理

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

FMT_MOF.1[2]　　セキュリティ機能のふるまい管理
FMT_MOF.1.1[2]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***・ユーザ認証機能*** ***・高信頼チャネル機能*** ***・S/MIME 機能*** ***・SNMP パスワード認証機能***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***のふるまいを改変する***
[割付: *許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

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

FMT_MSA.1[1]　　セキュリティ属性の管理
FMT_MSA.1.1[1]
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限するために[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*]: ***ユーザ自身の「ユーザ ID」が設定されるボックスのユーザ属性***
[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*[割付: その他の操作]*]: ***改変（他のユーザの「ユーザ ID」、または「部門 ID」、または「共有」に改変）***
[割付: *許可された識別された役割*]: ***・ユーザ*** ***・管理者***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]: ***ボックスアクセス制御***
下位階層　：　なし
依存性　：　FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[1]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

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

FMT_MSA.1[3]　　セキュリティ属性の管理
FMT_MSA.1.1[3]
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限するために[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*]: ***「部門 ID」が設定されるボックスのユーザ属性***
[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*[割付: その他の操作]*]: ***改変（「ユーザ ID」、または「共有」、または他の部門 ID へ改変）***
[割付: *許可された識別された役割*]: ***・その部門の利用を許可されたユーザ*** ***・管理者***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]: ***ボックスアクセス制御***

下位階層	:	なし
依存性	:	FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[1]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[6]）

FMT_MSA.3[1] 静的属性初期化

FMT_MSA.3.1[1]

TSF は、その SFP を実施するために使われるセキュリティ属性（***ボックスのユーザ属性***）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]：以下のケースに分類されるボックスの登録状況に応じた
① ユーザ、または管理者の登録操作によるボックスの登録の場合は「共有」
② 未登録ボックスを指定したボックス保管ジョブの動作に伴う自動ボックス登録の場合は当該ジョブを実行したユーザの「ユーザ ID」

[割付: *アクセス制御 SFP、情報フロー制御 SFP*]:
ボックスアクセス制御

FMT_MSA.3.2[1]

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付: *許可された識別された役割*]
FMT_MSA.3.1 の「その他の特性」にて示される①のケース：ユーザ
FMT_MSA.3.1 の「その他の特性」にて示される②のケース：なし

下位階層	:	なし
依存性	:	FMT_MSA.1（FMT_MSA.1[1]、FMT_MSA.1[2]）、FMT_SMR.1（FMT_SMR.1[3]）

FMT_MSA.3[2] 静的属性初期化

FMT_MSA.3.1[2]

TSF は、その SFP を実施するために使われるセキュリティ属性（***セキュリティ文書内部制御 ID***）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*]:
セキュリティ文書プリントファイルアクセス制御

FMT_MSA.3.2[2]

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付: *許可された識別された役割*]
該当なし

下位階層	:	なし
依存性	:	FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない）

FMT_MTD.1[1] TSF データの管理

FMT_MTD.1.1[1]

（ユーザ認証の方式に「本体認証」が選択されている場合、）TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。

[割付: *TSF データのリスト*]:
ユーザパスワード

[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***管理者***
下位階層 : なし
依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

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

FMT_MTD.1[3] TSF データの管理
FMT_MTD.1.1[3]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・ユーザ ID*** ***・部門 ID*** ***・部門パスワード*** ***・SNMP パスワード*** ***・セキュリティ文書パスワード*** ***・パネルオートログオフ時間*** ***・認証失敗回数閾値*** ***・外部サーバ認証設定データ*** ***・S/MIME証明書[6]*** ***・送信宛先データ*** ***・高信頼チャネル機能設定データ*** ***・所属部門*** ***・管理者認証ロック時間***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***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]）

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

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

FMT_MTD.1[5]　　TSF データの管理
FMT_MTD.1.1[5]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*] : ***ボックスパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*] : ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*] : ***・ユーザ*** ***・管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

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

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

FMT_MTD.1[8]　　TSF データの管理
FMT_MTD.1.1[8]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***セキュリティ文書パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***ユーザ***
下位階層　　:　なし
依存性　　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[3]）

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

FMT_MTD.1[10]　　TSF データの管理
FMT_MTD.1.1[10]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: そ*

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

FMT_MTD.1[11]　TSF データの管理

FMT_MTD.1.1[11]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***管理者パスワード、SNMP 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]：初期化***
[割付:*許可された識別された役割*]: ***管理者、サービスエンジニア***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MTD.1[12]　TSF データの管理

FMT_MTD.1.1[12]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***・部門 ID*** ***・部門パスワード*** ***・S/MIME 証明書*** ***・送信宛先データ*** ***・高信頼チャネル機能設定データ***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]: ***管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[13]　TSF データの管理

FMT_MTD.1.1[13]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ユーザ自身の所属部門***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]：登録***
[割付:*許可された識別された役割*]:

管理者、その部門の利用を許可されたユーザ [7]		
下位階層	:	なし
依存性	:	FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[6]）

FMT_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*
- *管理者によるユーザ認証機能の動作方式設定機能*
- *管理者による部門認証機能の動作方式設定機能*
- *管理者による SNMP パスワード認証機能の動作設定機能*
- *管理者による認証操作禁止機能における認証失敗回数閾値の設定機能*
- *管理者によるバックアップ機能 [8]*
- *管理者によるリストア機能 [9]*
- *管理者による部門 ID の登録機能*
- *管理者による部門 ID の改変機能*
- *管理者による部門パスワードの登録機能*
- *管理者による部門パスワードの改変機能*
- *管理者によるパネルオートログオフ時間設定機能*
- *管理者による SNMP 認証失敗回数の消去機能*
- *管理者によるユーザ認証失敗回数の消去機能*
- *管理者によるセキュリティ文書認証失敗回数の消去機能*
- *管理者によるボックス認証失敗回数の消去機能*
- *管理者による部門認証失敗回数の消去機能*
- *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 SNMP パスワードの改変機能*
- *管理者によるボックスパスワードの登録機能*
- *管理者によるボックスパスワードの改変機能*
- *管理者によるボックス登録機能（但し、ユーザ属性が「共有」の登録のみ）*
- *管理者によるボックスのユーザ属性の改変機能*
- *管理者によるユーザ ID の登録機能*
- *管理者によるユーザ認証の方式が本体認証の場合におけるユーザパスワードの登録機能*
- *管理者によるユーザ認証の方式が本体認証の場合におけるユーザパスワードの改変機能*
- *管理者による管理者パスワードの初期化機能*
- *管理者による SNMP パスワードの初期化機能*
- *管理者による S/MIME 証明書登録機能*
- *管理者による S/MIME 証明書登録変更機能*
- *管理者による S/MIME 機能の動作設定機能*
- *管理者による送信宛先データの登録機能*
- *管理者による送信宛先データの改変機能*
- *管理者による高信頼チャネル機能設定データの登録機能*
- *管理者による高信頼チャネル機能設定データの改変機能*
- *管理者による高信頼チャネル機能の動作設定機能*
- *管理者による所属部門の登録機能*
- *管理者による所属部門の改変機能*
- *管理者による管理者認証ロック時間の改変機能*
- *サービスエンジニアによるサービスエンジニアパスワードの改変機能*
- *サービスエンジニアによる管理者パスワードの改変機能*
- *サービスエンジニアによるセキュリティ強化機能の停止機能*

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

[8] バックアップ機能の一部は、TSF データの問い合わせ機能に相当する。

[9] リストア機能の一部は、TSF データの改変機能に相当する。

・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 ・サービスエンジニアによる SNMP パスワードの初期化機能 ・サービスエンジニアによる管理者認証失敗回数の消去機能 ・サービスエンジニアによる CE 認証ロック時間の改変機能 ・ユーザによるボックスのユーザ属性のデフォルト値を上書き機能 ・ユーザによるユーザ認証の方式が本体認証の場合におけるユーザ自身のユーザパスワードの改変機能 ・ユーザによるボックスパスワードの登録機能 ・ユーザによるボックスのユーザ属性の改変機能 ・その部門の利用を許可されたユーザによる所属部門の登録機能 ・ユーザによるボックス登録機能 ・ユーザによる未登録ボックスを指定したボックス保管ジョブによる個人ボックス自動登録機能 ・ユーザ認証方式が外部サーバ認証の場合における外部サーバによる本体未登録ユーザのユーザ ID 自動登録機能 ・ユーザによるセキュリティ文書プリントファイル登録に伴うセキュリティ文書パスワードの登録機能 ・共有ボックスの利用を許可されたユーザによる当該ボックスのユーザ属性の改変機能 ・共有ボックスの利用を許可されたユーザによる当該ボックスのボックスパスワードの改変機能 ・グループボックスの利用を許可されたユーザによる当該ボックスのユーザ属性の改変機能
下位階層　：　なし
依存性　：　なし

FMT_SMR.1[1]　セキュリティ役割
FMT_SMR.1.1[1]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： ***サービスエンジニア***
FMT_SMR.1.2[1]
TSF は、利用者を役割に関連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*]： ***ユーザ***
FMT_SMR.1.2[3]
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[3]）

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

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

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

5.1.1.5. 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

5.1.1.6. TOE アクセス

FTA_SSL.3　　TSF 起動による終了
FTA_SSL.3.1
TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。
[割付: *利用者が非アクティブである時間間隔*]： ***パネルより管理者、またはユーザが操作中、最終操作からパネルオートログオフ時間（1～9 分）によって決定される時間***
下位階層　：　なし
依存性　：　なし

5.1.1.7. 高信頼パス/チャネル

FTP_ITC.1　　TSF 間高信頼チャネル
FTP_ITC.1.1
TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。
FTP_ITC.1.2
TSF は、[選択: *TSF*、*リモート高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。
[選択: *TSF*、*リモート高信頼 IT 製品*]： ***リモート高信頼 IT 製品***
FTP_ITC.1.3
TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。
[割付: *高信頼チャネルが要求される機能のリスト*]： ***・ボックスファイルのダウンロード*** ***・ボックスファイルとして保管されることになる画像ファイルのアップロード*** ***・セキュリティ文書プリントファイルになる画像ファイルのアップロード***
下位階層　：　なし
依存性　：　なし

5.1.1.8. 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。 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 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。 a) 利用者識別情報の管理

5.1.1.9. 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*]： *＜オブジェクト＞* *・ボックスファイル* *・セキュリティ文書プリントファイル* *・オンメモリ画像ファイル* *・保管画像ファイル* *・残存画像ファイル* *・画像関連ファイル* *・送信宛先データファイル* *・HDD ロックパスワードオブジェクト* *・暗号化ワードオブジェクト* *＜TSF データ＞* *・管理者パスワード* *・SNMP パスワード* *・ユーザ ID* *・ユーザパスワード* *・ボックスパスワード* *・セキュリティ文書パスワード* *・部門 ID* *・部門パスワード* *・S/MIME 証明書* *・高信頼チャネル設定データ*	

・残存TSFデータ [10]
下位階層 : なし 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.2[5]、FIA_UAU.2[6]、FIA_UAU.6、FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]、FIA_SOS.1[4]、FIA_SOS.1[5]、FIA_SOS.1[6]、FIA_SOS.1[7]、FIA_SOS.2 である。

なお FCS_CKM.1 の暗号鍵生成アルゴリズム、FCS_COP.1 の暗号アルゴリズムは、最小機能強度主張の対象には含まない。

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 6 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
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

[10] ファイル管理領域の削除だけでは削除されない、HDD データ領域に残存している TSF データ

5.2. IT 環境のセキュリティ要件

5.2.1.1. 暗号サポート

FCS_COP.1[E]　　暗号操作
FCS_COP.1.1[E]
TSF ***（暗号化基板）*** は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。
[割付: *標準のリスト*] : ***FIPS PUB 197***
[割付: *暗号アルゴリズム*] : ***AES***
[割付: *暗号鍵長*] : ***128bit***
[割付: *暗号操作のリスト*] : ***・HDD に書き込まれるすべてのデータの暗号化*** ***・HDD から読み出されるすべてのデータの復号***
下位階層　:　なし 依存性　:　FDP_ITC.1 or FCS_CKM.1（FCS_CKM.1）、FCS_CKM.4（適用しない）、FMT_MSA.2（適用しない）

5.2.1.2. 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*] : ***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]」*] ***[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*] : ***＜検出した際のアクション＞*** ***HDD へのデータの読み込み及び書き込みを拒否する。*** ***＜通常復帰のための操作＞*** ***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）

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*]: ***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[3]、FIA_UAU.2[5]）

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 7 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 7 TOE のセキュリティ機能名称と識別子の一覧

No.	TOE のセキュリティ機能	
1	F.ADMIN	管理者機能
2	F.ADMIN-SNMP	SNMP 管理者機能
3	F.SERVICE	サービスモード機能
4	F.USER	ユーザ機能
5	F.BOX	ボックス機能
6	F.PRINT	セキュリティ文書プリント機能
7	F.OVERWRITE-ALL	全領域上書き削除機能
8	F.CRYPTO	暗号鍵生成機能
9	F.HDD	HDD 検証機能
10	F.RESET	認証失敗回数リセット機能
11	F.TRUSTED-PASS	高信頼チャネル機能
12	F.S/MIME	S/MIME 暗号処理機能

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 8 に示されるキャラクタからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
  - ネットワークからのアクセスに対して管理者認証後は、管理者パスワードとは別のセッション情報を利用した、管理者認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- 管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 管理者パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、管理者パスワードを利用するすべての認証機能をロックする。（管理者モードへのアクセスを拒否する。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作する、または F.SERVICE における管理者認証機能のロッ

ク解除機能が実行されて解除する。

表 8 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
CE パスワード 管理者パスワード	8 桁	合計 92 文字が選択可能 ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~
セキュリティ文書パスワード	8 桁	合計 93 文字が選択可能 ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、*SPACE*
HDD ロックパスワード 暗号化ワード	20 桁	合計 83 文字が選択可能 ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、 #、 $、 %、 &、’ 、 *、 +、 -、.、 /、 =、 ?、 @、 ^、 _、 `、 {、 |、 }、 ~
SNMP パスワード ・Privacy パスワード ・Authentication パスワード ユーザパスワード	8 桁以上	合計 95 文字が選択可能 ASCII コード（0x20 ～ 0x7E） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、”、+、*SPACE*
部門パスワード ボックスパスワード	8 桁	

6.1.1.2. 管理者モードのオートログオフ機能

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

6.1.1.3. 管理者モードにて提供される機能

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

① 管理者パスワードの変更

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

- 表 8 に示されるキャラクタからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、パネルからのアクセスの場合、管理者パスワード入力のフィードバックに 1 文字

毎“＊”を返す。

- 管理者パスワードを利用する各認証機能において通算1～3回目となる認証失敗を検知すると、パネルからアクセスする管理者モードをログオフし、管理者パスワードを利用するすべての認証機能をロックする。(管理者モードへのアクセスを拒否する。)
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作する、または F.SERVICE における管理者認証機能のロック解除機能が実行されて解除する。
- 新規設定される管理者パスワードは以下の品質を満たしていることを検証する。
  - 表 8 の管理者パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

② ユーザの設定

- ユーザ登録（ユーザ認証方式：本体認証において利用されるユーザのみ)
  ユーザID（ユーザ名と認証サーバ情報 [11]から構成されるが、本体認証時はユーザ名のみの登録。）を設定し、ユーザパスワードを登録してユーザが登録される。新しく設定されるユーザパスワードは以下の品質を満たしていることを検証する。
  - 表 8 のユーザパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

  なお、外部サーバ認証を有効にしている場合は、ユーザパスワードの登録はできない。
  また所属部門（部門 ID）を登録し、関連付けする。(予め部門設定が必要。)
- ユーザパスワードの変更（ユーザ認証方式：本体認証において利用されるユーザのみ)
  ユーザパスワードを変更する。新しく設定されるユーザパスワードは以下の品質を満たしていることを検証する。
  - 表 8 のユーザパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- ユーザ削除
  ユーザ ID、ユーザパスワードを削除する。
  - 当該ユーザが所有する個人ボックスが存在した場合、それら個人ボックスは、ユーザ属性：共有の共有ボックスに自動設定される。
- 所属部門の変更
  ユーザに関連付けられる所属部門を変更する。

③ ボックスの設定

- **ボックスの登録**
  選択した未登録ボックス ID に対して、ユーザ属性を選定して、個人ボックス、または共有ボックスを登録する。登録する際、ボックスのユーザ属性にはデフォルト値として「共有」が指定されるが、「ユーザ ID」を選択することも可能。
  - 個人ボックスの場合は、登録される任意のユーザ ID を指定する。
  - 共有ボックスの場合は、登録されるボックスパスワードが以下の条件を満たすことを検証する。
    - ✧ 表 8 のボックスパスワードに示される桁数、キャラクタから構成される。
    - ✧ 1 つのキャラクタで構成されない。
  - グループボックスの場合、登録される任意の部門 ID を指定する。

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

➢ **ボックスパスワードの変更**
- 共有ボックスに設定されるボックスパスワードを変更する。
- 新しく設定されるボックスパスワードは以下の品質を満たしていることを検証する。
  - ✧ 表 8 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。

➢ **ボックスのユーザ属性の変更**
- 個人ボックスのユーザ属性を登録された別のユーザ、または部門を指定する。
- グループボックスのユーザ属性を登録されたユーザ、または別の部門を指定する。
- 共有ボックスのユーザ属性を登録されたユーザ、または部門を指定する。
- 個人ボックス、グループボックスのユーザ属性を共有に指定する。
  - ✧ 同時にボックスパスワードの登録が必要となり、上記のボックスパスワードの変更と同様の処理が行われる。

④ ロックの解除

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

⑤ ユーザ認証機能の設定

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

ユーザ認証機能と組み合わせて利用される部門認証機能における以下の認証方式を設定する。
➢ 部門認証機能：連動方式
ユーザ ID に予め関連付けられている部門 ID を利用する方式
➢ 部門認証機能：個別認証方式
ユーザ ID に予め関連付けられている部門 ID を利用せず、アクセス時に部門 ID と部門パスワードによって認証する方式
➢ 部門認証機能：利用しない
ユーザ ID による認証機能だけを利用し、部門情報による識別認証を行わない。

⑥ 不正アクセス検出閾値の設定

認証操作禁止機能における不正アクセス検出閾値を 1～3 回間で設定する。

⑦ 全領域上書き削除機能の設定と実行

以下の表に示される消去方式を選択し、HDD のデータ領域の上書き削除および NVRAM の初期化を実行する。（F.OVERWRITE-ALL を実行する。）

表 9 全領域の上書き削除のタイプと上書きの方法

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	乱数 ⇒ 乱数 ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
Mode:4	乱数 ⇒ 0x00 ⇒ 0xFF
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

⑧ オートログオフ機能の設定

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

- パネルオートログオフ時間 ：1～9 分

⑨ 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）

⑩ バックアップ、リストア機能の実行

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

＜タイプ A バックアップ・リストア制限されるべき対象＞

- SNMP パスワード
- ユーザパスワード
- 部門パスワード
- セキュリティ文書パスワード
- ボックスパスワード

＜タイプ B リストアが制限されるべき対象＞

- SMTP サーバ設定に関係する一連のデータ
- DNS サーバ設定に関係する一連のデータ
- MFP アドレス設定に関係する一連のデータ
- セキュリティ強化機能の設定データ
- ユーザ認証機能の動作方式設定データ
- 認証操作禁止機能の認証失敗回数閾値
- パネルオートログオフ時間
- ユーザ ID
- ボックスのユーザ属性
- 部門 ID

- S/MIME 証明書
- 送信宛先データ
- S/MIME 機能における暗号化強度設定データ
- 高信頼チャネル機能設定データ
- 所属部門
- CE 認証ロック時間
- 管理者認証ロック時間

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

⑪ 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 8 のHDDロックパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

＜HDD ロックパスワード変更＞

HDD ロックパスワードを変更する。現在設定される HDD ロックパスワードを使い、管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。
- 表 8 に示されるキャラクタからなるHDDロックパスワードを照合するHDDロックパスワード照合メカニズムを提供する。
- 照合では、HDD ロックパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 新規設定される HDD ロックパスワードは以下の品質を満たしていることを検証する。
  - 表 8 のHDDロックパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

⑫ 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）

＜動作設定　ON＞

OFF から ON にする場合、新しく設定される暗号化ワードが以下の品質を満たしていることを検証し、F.CRYPTO が実行される。
- 表 8 の暗号化ワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

＜暗号化ワード変更＞

暗号化ワードを変更する。現在設定される暗号化ワードを使い、管理者であることを再認証され、且つ新規設定される暗号化ワードが品質を満たしている場合に変更し、F.CRYPTO が実行される。
- 表 8 に示されるキャラクタからなる暗号化ワードを照合する暗号化ワード照合メカニズムを提供する。
- 照合では、暗号化ワード入力のフィードバックに 1 文字毎“＊”を返す。
- 新規設定される暗号化ワードは以下の品質を満たしていることを検証する。
  - 表 8 の暗号化ワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

⑬ セキュリティ強化機能に関連する機能

管理者が操作するセキュリティ強化機能の設定に影響する機能は以下の通り。(※バックアップ・リストア機能の影響については、⑩にて説明済み)

- セキュリティ強化機能の動作設定
  セキュリティ強化機能の有効、無効を設定する機能。
- HDD 論理フォーマット機能
  HDD に OS のシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- 全領域上書き削除機能
  全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。

⑭ SNMP パスワードの変更

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

- 表 8 のSNMPパスワードに示される桁数、キャラクタから構成される。

⑮ SNMP パスワード認証機能の設定

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

⑯ 部門の設定

- 部門登録
  部門 ID を設定し、部門パスワードを登録して部門が登録される。新しく設定される部門パスワードは以下の品質を満たしていることを検証する。
  - 表 8 の部門パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 部門 ID、部門パスワードの変更
  部門 ID、部門パスワードを変更する。新しく設定される部門パスワードは以下の品質を満たしていることを検証する。
  - 表 8 の部門パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 部門削除
  部門 ID、部門パスワードを削除する。
  - 当該部門 ID のグループボックスが存在した場合、それらグループボックスは、ユーザ属性:共有の共有ボックスに自動設定される。

⑰ 管理者認証ロック時間の設定

管理者認証ロック時間を 1～60 分で設定する。

⑱ 高信頼チャネル機能の設定

SSL/TLS による高信頼チャネル機能の設定データを設定する。

- 通信暗号強度設定(利用可能する通信暗号方式の変更)

⑲ S/MIME 送信機能の設定

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

- 送信宛先データ(e-mail アドレス)

- S/MIME 証明書の登録、変更
- 暗号化強度の設定

6.1.2. F.ADMIN-SNMP（SNMP 管理者機能）

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

6.1.2.1. SNMP パスワードによる識別認証機能

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

- 表 8 に示されるキャラクタからなるSNMPパスワードにより認証するSNMP認証メカニズムを提供する。
  - Authentication パスワードのみ、または Privacy パスワード及び Authentication パスワード双方を利用する。
  - SNMP の場合は、別途セッション情報による管理者認証メカニズムを必要とせず、毎回のセッションに SNMP パスワード利用する。
- 認証に成功すると、認証失敗回数をリセットする。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に成功した場合に認証失敗回数をリセットする。
- SNMP パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、SNMP パスワードを利用するすべての認証機能をロックする。（MIB オブジェクトへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に失敗した場合でも 1 回の失敗として検知する。
- ロック状態は、F.ADMIN の MIB オブジェクトに対するロック解除機能が実行されることによって解除される。

6.1.2.2. SNMP を利用した管理機能

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

① ネットワークの設定

以下の設定データの設定操作を行う。

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

② SNMP パスワードの変更

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

- 表 8 のSNMPパスワードに示される桁数、キャラクタから構成される。

③ SNMP パスワード認証機能の設定

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

6.1.3. F.SERVICE（サービスモード機能）

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

6.1.3.1. サービスエンジニア識別認証機能

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

- 表 8 に示されるキャラクタからなるCEパスワードにより認証するCE認証メカニズムを提供する。
  - サービスモードの場合はパネルからのアクセスのみになるため、別途セッション情報による CE 認証メカニズムを必要としない。
- CE パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからの入力を 5 秒間受け付けない。
- CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、CE パスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作して解除する。

6.1.3.2. サービスモードにて提供される機能

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

① CE パスワードの変更

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

- 表 8 に示されるキャラクタからなるCEパスワードにより再認証するCE認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、パネルからのアクセスの場合、CE パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、パネルからアクセスするサービスモードをログオフし、CE パスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET が動作して解除する。
- 新規設定される CE パスワードは以下の品質を満たしていることを検証する。

- 表 8 のCEパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。
- 現在設定される値と一致しない。

② 管理者パスワードの変更

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

- 表 8 の管理者パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。
- 現在設定される値と一致しない。

③ セキュリティ強化機能に関連する機能

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

- HDD 論理フォーマット機能
  HDD に OS のシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- HDD 物理フォーマット機能
  HDD にトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- HDD 装着設定機能
  搭載された HDD を有効化するための機能。この HDD 装着設定を無効化することにより、セキュリティ強化機能の設定を無効にする。
- イニシャライズ機能
  NVRAM に書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、セキュリティ強化機能の設定を無効にする。

④ パスワード初期化機能に関連する機能

サービスエンジニア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。

- イニシャライズ機能
  NVRAM に書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、管理者パスワード、SNMP パスワードを工場出荷の初期値に設定する。HDD ロック機能、暗号化機能の動作設定をいずれも OFF にする。(動作設定が OFF されることにより、設定されていた HDD ロックパスワード、暗号化ワードを再度利用することができなくなる。)
- HDD 物理フォーマット機能
  HDD にトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、HDD ロック機能を OFF にする。(動作設定が OFF されることにより、設定されていた HDD ロックパスワードを再度利用することができなくなる。)

⑤ 管理者認証機能のロックの解除

管理者認証失敗回数を 0 クリアする。

- アクセスがロックされてれば、ロックが解除される。

⑥ CE 認証ロック時間の設定

CE 認証ロック時間を 1～60 分で設定する

6.1.4. F.USER（ユーザ機能）

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

6.1.4.1. ユーザ識別認証機能

＜部門認証：連動方式のユーザ識別認証＞

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

- 表 8 に示されるキャラクタからなるユーザパスワードにより、ユーザを認証するユーザ認証メカニズムを提供する。
  - ネットワークからのアクセスに対してユーザ認証後は、ユーザパスワードとは別のセッション情報を利用した、ユーザ認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- ユーザパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該ユーザに対して、通算 1～3 回目となる認証失敗を検知すると、当該ユーザに対する認証機能をロックする。
  - 失敗回数閾値は、認証操作禁止機能の動作設定にて管理者が指定する。
- 認証機能のロックは、F.ADMIN において当該ユーザに対するロック解除機能が実行されることによって解除される。

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

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

＜部門認証：個別認証方式のユーザ識別認証＞

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

- 表 8 に示されるキャラクタからなる部門パスワードにより、部門を認証する部門認証メカニズムを提供する。
- 部門パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該部門に対して、通算 1～3 回目となる認証失敗を検知すると、当該部門に対する認証機能をロックする。
  - 失敗回数閾値は、認証操作禁止機能の動作設定にて管理者が指定する。

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

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

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

6.1.4.2. ユーザ識別認証ドメインにおけるオートログオフ機能

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

6.1.4.3. ユーザパスワードの変更機能

識別認証され、ユーザ識別認証ドメインへのアクセスが許可されると、本人のユーザパスワードを変更することが許可される。なお外部サーバ認証が有効の場合には、本機能は利用できない。
新規設定されるユーザパスワードが以下の品質を満たしている場合、変更する。

- 表 8 のユーザパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

6.1.5. F.BOX（ボックス機能）

F.BOX とは、登録ユーザであると識別認証されたユーザに対して、そのユーザの個人ボックスの操作、管理を許可し、共有ボックスへのアクセスに対して共有ボックスの利用を許可されたユーザであることを認証し、認証後に当該ボックス、ボックスファイルの各種操作を許可するアクセス制御機能などボックスに関係する一連のセキュリティ機能のことである。

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

- 個人ボックスの場合は、登録される任意のユーザ ID を指定する。
- 共有ボックスの場合は、登録されるボックスパスワードが以下の条件を満たすことを検証する。
  - 表 8 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- グループボックスの場合、登録される任意の部門 ID を指定する。

＜ボックスの自動登録＞

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

6.1.5.1. 個人ボックス機能

① 個人ボックスに対するアクセス制御機能

識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザ ID」を持つ。このタスクは、このユーザ属性と一致するユーザ属性を持つ個人ボックスの一覧表示操作が許可される。

② 個人ボックス内のボックスファイルに対するアクセス制御機能

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

③ 個人ボックスのユーザ属性変更

ユーザ属性を変更することができる。

- 他の登録ユーザを指定すると、他のユーザが管理する個人ボックスになる。
- 共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。この場合は、ボックスパスワードが以下の条件を満たすことを検証する。
  - 表 8 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 部門 ID を指定すると、当該部門の利用を許可されたユーザがアクセス可能なグループボックスになる。

6.1.5.2. 共有ボックス機能

登録ユーザとして識別認証されると、識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザ ID」を持つ。このタスクは、ユーザ属性に共有が設定される共有ボックスの一覧表示操作が許可される。個々の共有ボックスの操作仕様は以下の通りである。

- 共有ボックスへのアクセスにおける認証機能

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

- 表 8 に示されるキャラクタからなるボックスパスワードにより認証するボックス認証メカニズムを提供する。
  - ネットワークからのアクセスに対してボックス認証後は、ボックスパスワードとは別のセッション情報を利用した、ボックス認証メカニズムを提供する。
- プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- ボックスパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 当該共有ボックスに対して、通算 1～3 回目となる認証失敗を検知すると、当該共有ボックスに対する認証機能をロックする。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.ADMIN の共有ボックスに対するロック解除機能が実行されることによって解除される。

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

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

- **共有ボックスのユーザ属性変更**
  当該ボックスのユーザ属性を変更することができる。
  - 登録ユーザを指定し、登録ユーザの個人ボックスに変更する。
  - 部門 ID を指定し、当該部門の利用が許可されたユーザがアクセス可能なグループボックスにする。

- **共有ボックスパスワードの変更**
  共有ボックスのボックスパスワードを変更する。新しく設定されるボックスパスワードが以下の品質を満たしている場合、変更する。
  - 表 8 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。

6.1.5.3. グループボックス機能

① グループボックスに対するアクセス制御機能
識別認証されたユーザを代行するタスクは、識別認証されたユーザと関連づけられた所属部門として「部門 ID」を持つ。このタスクは、この部門 ID と一致するユーザ属性を持つグループボックスの一覧表示操作が許可される。

② グループボックス内のボックスファイルに対するアクセス制御機能
操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、このユーザ属性及びボックス属性と一致するユーザ属性、ボックス属性を持つボックスファイルに対して印刷、E-mail 送信（S/MIME 送信を含む)、FTP 送信、FAX 送信、SMB 送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

③ グループボックスのユーザ属性変更
ユーザ属性を変更することができる。
- 他の部門 ID を指定すると、他の部門所属のユーザがアクセス可能なグループボックスになる。
- 共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。この場合は、ボックスパスワードが以下の条件を満たすことを検証する。
  - 表 8 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
- 登録ユーザを指定し、登録ユーザの個人ボックスに変更する。

6.1.6. F.PRINT（セキュリティ文書プリント機能）

F.PRINT とは、登録ユーザであると識別認証されたユーザに対して、パネルからのセキュリティ文書プリントファイルへのアクセスに対してセキュリティ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、認証後に当該セキュリティ文書プリントファイルの一覧表示、印刷を許可するアクセス制御機能などセキュリティ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。

6.1.6.1. セキュリティ文書パスワードによる認証機能

登録ユーザであることが識別認証されると、パネルからセキュリティ文書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セキュリティ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 8 に示されるキャラクタからなるセキュリティ文書パスワードにより認証するセキュリティ文書認証メカニズムを提供する。
  - セキュリティ文書プリントの場合はパネルからのアクセスのみになるため、別途セッション情報によるセキュリティ文書認証メカニズムを必要としない。
- セキュリティ文書パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- 認証に失敗すると、パネルからのアクセスを 5 秒間受け付けない。
- 当該セキュリティ文書プリントファイルに対して、通算 1～3 回目となる認証失敗を検知すると、当該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。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- ロック状態は、F.ADMIN において当該セキュリティ文書プリントファイルに対してロック解除機能が実行されることによって解除される。

6.1.6.2. セキュリティ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、セキュリティ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、認証されたセキュリティ文書プリントファイルのセキュリティ文書内部制御 ID を持つ。
- このタスクは、このファイル属性と一致するファイル属性を持つセキュリティ文書プリントファイルに対して印刷を許可される。

6.1.6.3. セキュリティ文書プリントファイルの登録機能

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

① セキュリティ文書パスワードの登録

登録されるセキュリティ文書パスワードが以下の条件を満たすことを検証する。

- 表 8 のセキュリティ文書パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

② セキュリティ文書内部制御 ID の付与

セキュリティ文書プリントファイルの登録要求において、セキュリティ文書パスワードの検証が

完了すると、一意に識別されるセキュリティ文書内部制御 ID を当該セキュリティ文書プリントファイルに設定する。

6.1.7. F.OVERWRITE-ALL（全領域上書き削除機能）

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

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

＜初期化される対象：NVRAM＞
- 管理者パスワード
- SNMP パスワード
- HDD ロック機能の動作設定（OFF）　・・・HDD ロックパスワードが消去される。
- 暗号化機能の動作設定（OFF）　・・・暗号化ワードが消去される。
- 高信頼チャネル設定データ　・・・初期化状態は何も存在しないので消去される。

HDDに書き込むデータ、書き込む回数など削除方式は、F.ADMINにおいて設定される全領域上書き削除機能の消去方式（**表 9**）に応じて実行される。HDDロック機能及び暗号化機能は動作設定がOFFされることによって、設定されていたHDDロックパスワード、暗号化ワードが利用できなくなる。なお、本機能の実行においてセキュリティ強化機能の設定は無効になる。（F.ADMINにおけるセキュリティ強化機能の動作設定の記載参照）

6.1.8. F.CRYPTO（暗号鍵生成機能）

F.CRYPTO とは、コニカミノルタ暗号仕様標準によって規定されるコニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）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。コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）とは、FIPS 180-1 が規定する SHA-1 を利用して暗号鍵を生成するアルゴリズムである。

F.ADMIN においてアクセス制限される暗号化機能の動作設定において暗号化ワードが決定され

ると、コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）を用いて暗号化ワードから 128bit 長の暗号鍵を生成する。

6.1.9. F.HDD（HDD 検証機能）

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

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

6.1.10. F.RESET（認証失敗回数リセット機能）

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

① CE 認証機能ロック解除処理機能

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

② 管理者認証機能ロック解除処理機能

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

6.1.11. F.TRUSTED-PASS（高信頼チャネル機能）

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

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

6.1.12. F.S/MIME（S/MIME 暗号処理機能）

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

＜ボックスファイル暗号鍵生成＞

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

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

＜ボックスファイル暗号鍵の暗号化＞
- ボックスファイルを暗号化するための暗号鍵は、FIPS 186 -1 が規定する RSA により、暗号化される。
- この際利用される暗号鍵の鍵長は、1024bit、2048 bit、3072 bit、4096 bit のいずれかである。

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。

① F.ADMIN が提供する管理者認証メカニズム、HDD ロックパスワード照合メカニズム、暗号化ワード照合メカニズム
② F.SERVICE が提供する CE 認証メカニズム
③ F.PRINT が提供するセキュリティ文書認証メカニズム
④ F.BOX が提供するボックス認証メカニズム
⑤ F.ADMIN-SNMP が提供する SNMP 認証メカニズム
⑥ F.USER が提供するユーザ認証メカニズム、部門認証メカニズム

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 表 15 に示す。表 15 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 10 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 10 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 ・構成リスト ・CM 記録
	CM 範囲	ACM_SCP.1	
配付と運用	配付	ADO_DEL.1	配付/運用説明書
	設置・生成・及び立上げ	ADO_IGS.1	・サービスマニュアル [セキュリティ機能編] bizhub C650 ・Service Manual [Security Function] bizhub C650

TOE セキュリティ保証要件		コンポーネント	保証手段
			ineo+ 650 ・ユーザーズガイド [セキュリティ機能編] bizhub C650 ・User's Guide [Security Operations] bizhub C650 ・User's Guide [Security Operations] ineo+ 650
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 [セキュリティ機能編] bizhub C650 ・Service Manual [Security Function] bizhub C650 ineo+ 650 ・ユーザーズガイド [セキュリティ機能編] bizhub C650 ・User's Guide [Security Operations] bizhub C650 ・User's Guide [Security Operations] ineo+ 650
	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	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	テスト仕様書（結果報告を含む）
	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 （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	

7. PP 主張

本 ST には、適合する PP はない。

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 11 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	A.SERVER	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-PRIVATE-BOX	T.ACCESS-PUBLIC-BOX	T.ACCESS-GROUP-BOX	T.ACCESS-SECURE-PRINT	T.ACCESS-NET-SETTING	T.ACCESS-SETTING	T.BACKUP-RESTORE	P.COMMUNICATION-DATA
O.REGISTERED-USER									●	●	●	●				
O.PRIVATE-BOX									●							
O.PUBLIC-BOX										●						
O.GROUP-BOX											●					
O.SECURE-PRINT												●				
O.CONFIG													●	●	●	●
O.OVERWRITE-ALL							●									
O.CRYPTO-KEY								●								
O.CHECK-HDD								●								
O.TRUSTED-PASS																●
O.CRYPTO-MAIL																●
OE.CRYPTO								●								
OE.LOCK-HDD								●								
OE.FEED-BACK									●	●	●	●	●	●	●	●
OE-N.ADMIN	●															
OE-N.SERVICE		●														
OE-N.NETWORK			●													
OE-N.SECRET				●												
OE-N.SERVER						●										
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。

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

- **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。

- **A.SERVER（オフィス内 LAN に接続されるユーザ情報管理サーバの管理条件）**
  本条件は、ユーザ認証の方式に「外部サーバ認証」が利用される際に必要なユーザ情報管理サーバがセキュアに管理されていることを想定している。
  OE-N.SERVER は、組織の責任者は、ユーザ情報管理サーバに対して、パッチ適用、アカウント管理、アクセス制御などセキュリティを保つために必要なサーバ管理を実施させ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 より情報漏洩する可能性を想定している。
O.OVERWRITE-ALL は、TOE が HDD の全領域に削除用のデータを上書きする機能を提供し、NVRAM の情報を初期化するとしており、MFP が回収される前にこの機能を実行することによって、脅威の可能性は除去される。
したがって本脅威は十分対抗されている。

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

本脅威は、MFP を利用している運用環境から HDD が盗み出される、または不正な HDD が取り付けられて、そこにデータが蓄積されたところで持ち出されることにより、HDD 内の画像データが漏洩する可能性を想定している。
これに対して以下の 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、OE.CRYPTO により、暗号化基板がデータを暗号化する。
② 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。

上記において、②のみが選択された場合は、HDD がすりかえられて、②の機能を持たない HDD が設置されることにより、持ち出されて漏洩する危険性が存在する。これに対しては、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-PRIVATE-BOX（ユーザ機能を利用した個人ボックスへの不正なアクセス）**

本脅威は、ユーザ各位が画像ファイルの保管に利用する個人ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。
O.REGISTERED-USER は、TOE が登録されたユーザだけが、TOE の搭載された MFP を利用することを許可するとしており、さらに O.PRIVATE-BOX によって個人ボックス及び個人ボックス内のボックスファイルの操作が、その所有者であるユーザだけに制限され、脅威の可能性は除去される。
OE.FEED-BACK は、ユーザの認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、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.REGISTERED-USER 及び O.PRIVATE-BOX は十分サポートされている。
したがって本脅威は十分対抗されている。

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

本脅威は、ユーザが共有して利用する画像ファイルの保管場所である共有ボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。
O.REGISTERED-USER は、TOE が登録されたユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.PUBLIC-BOX によって共有ボックス、共有ボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は除去される。
OE.FEED-BACK は、ユーザの認証及びボックスの認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、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.REGISTERED-USER 及び O.PUBLIC-BOX は十分サポートされている。
したがって本脅威は十分対抗されている。

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

本脅威は、その部門の利用が許可されたユーザが利用する画像ファイルの保管場所であるグループボックスやその中のボックスファイルに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。
O.REGISTERED-USER は、TOE が登録されたユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.GROUP-BOX によってグループボックス、グループボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は除去される。
OE.FEED-BACK は、ユーザの認証及び部門の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、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.REGISTERED-USER 及び O.GROUP-BOX は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-SECURE-PRINT（セキュリティ文書プリントファイルへの不正なアクセス）**

本脅威は、セキュリティ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.REGISTERED-USER は、TOE が登録されたユーザだけが TOE の搭載された MFP を利用することを許可するとしており、さらに O.SECURE-PRINT によって、セキュリティ文書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、ユーザの認証及びセキュリティ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.REGISTERED-USER 及び O.SECURE-PRINT は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-NET-SETTING（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 PC からプリント機能を利用してしまう可能性を想定している。特にオフィス内の他のユーザに対しても秘匿性が要求されるセキュリティ文書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セキュリティ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及びサービスエンジニアだけに許可するとしており、脅威の可能性が除去される。
OE.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、サービス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。

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

本脅威はバックアップ機能、リストア機能が不正に利用されることにより、ボックスファイルやセキュリティ文書プリントファイルが漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、各種設定値等が改ざんされた結果、ボックスファイル、セキュリティ文書プリントファイルを想定している。
O.CONFIG により、バックアップ機能、リストア機能の利用を管理者だけに許可するとしており、脅威の可能性が除去される。
OE.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 をサポートしている。
したがって本脅威は十分対抗されている。

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に対応するセキュリティ対策方針について以下に説明する。

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

本組織のセキュリティ方針は、ネットワーク上に流れる画像ファイルについて、秘匿性を確保するために、正しい相手先へ信頼されるパスを介した処理を行う、または暗号化すること規定している。
O.TRUSTED-PASS により、秘匿性のある画像である、ボックスファイル、セキュリティ文書プリントファイルに対して、MFP から PC、または PC から MFP といった画像の送受信において正しい相手先に高信頼チャネルを提供するため、組織のセキュリティ方針が実現する。
また O.CRYPTO-MAIL により、MFP から PC へメールにて送信されるボックスファイルを正しい相手先へ暗号化して送信する機能を提供するとするセキュリティ対策方針により、組織のセキュリティ方針は実現される。
さらに高信頼チャネル機能設定データ、メールによるボックスファイルの暗号化の管理、送信宛先データは、O.CONFIG により管理者に制限されている。また OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、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 をサポートしている。
したがって本組織のセキュリティ方針は、達成するために十分である。

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 12 セキュリティ対策方針に対する IT セキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPTO-KEY	O.CHECK-HDD	O.TRUSTED-PASS	O.CRYPTO-MAIL	OE.CRYPTO	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
set.admin	●	●	●	●	●	●										
set.service	●	●	●	●	●	●										
FCS_CKM.1								●			●					
FCS_COP.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]						●										
FIA_AFL.1[1]																●
FIA_AFL.1[2]															●	
FIA_AFL.1[3]						●										
FIA_AFL.1[4]	●															
FIA_AFL.1[5]					●											
FIA_AFL.1[6]			●													
FIA_AFL.1[7]				●												
FIA_AFL.1[8]	●		●	●	●										●	●
FIA_ATD.1		●	●	●	●											
FIA_SOS.1[1]															●	●
FIA_SOS.1[2]						●										
FIA_SOS.1[3]	●															
FIA_SOS.1[4]						●										
FIA_SOS.1[5]					●											
FIA_SOS.1[6]	●		●												●	
FIA_SOS.1[7]			●	●												
FIA_SOS.2	●		●												●	
FIA_UAU.2[1]																●
FIA_UAU.2[2]						●									●	
FIA_UAU.2[3]	●															
FIA_UAU.2[4]					●											
FIA_UAU.2[5]			●													
FIA_UAU.2[6]				●												
FIA_UAU.6						●									●	●
FIA_UAU.7	●		●	●	●										●	●
FIA_UID.2[1]																●

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-BOX	O.GROUP-BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPTO-KEY	O.CHECK-HDD	O.TRUSTED-PASS	O.CRYPTO-MAIL	OE.CRYPTO	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
FIA_UID.2[2]						●									●	
FIA_UID.2[3]	●															
FIA_UID.2[4]					●											
FIA_UID.2[5]			●													
FIA_UID.2[6]				●												
FIA_UID.2[7]	●															
FIA_USB.1		●	●	●	●											
FMT_MOF.1[1]						●										
FMT_MOF.1[2]	●					●										
FMT_MOF.1[3]				●												
FMT_MSA.1[1]		●				●										
FMT_MSA.1[2]			●			●										
FMT_MSA.1[3]				●		●										
FMT_MSA.3[1]		●	●													
FMT_MSA.3[2]					●											
FMT_MTD.1[1]	●															
FMT_MTD.1[2]	●					●										
FMT_MTD.1[3]	●		●	●	●	●									●	●
FMT_MTD.1[4]			●			●										
FMT_MTD.1[5]			●													
FMT_MTD.1[6]															●	
FMT_MTD.1[7]						●										
FMT_MTD.1[8]					●											
FMT_MTD.1[9]																●
FMT_MTD.1[10]	●															
FMT_MTD.1[11]						●									●	
FMT_MTD.1[12]				●		●										
FMT_MTD.1[13]				●												
FMT_SMF.1	●	●	●	●	●	●									●	●
FMT_SMR.1[1]						●									●	●
FMT_SMR.1[2]	●	●	●	●	●	●									●	
FMT_SMR.1[3]	●	●			●											
FMT_SMR.1[4]			●													
FMT_SMR.1[5]	●															
FMT_SMR.1[6]				●												
FPT_RVM.1	●	●	●	●	●	●			●						●	●
FPT_SEP.1	●	●	●	●	●	●									●	●
FTA_SSL.3	●														●	
FTP_ITC.1										●						
FNEW_RIP.1							●									
FIA_NEW.1									●							
FCS_COP.1[E]												●				
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.REGISTERED-USER（登録ユーザの利用）**

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

＜ユーザの識別認証に必要な要件＞
FIA_UID.2[3]、FIA_UAU.2[3]により、アクセスする利用者が、登録済みユーザであることを識別認証する。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[4]により、不成功認証が 1～3 回に達すると、以降そのユーザに対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
「本体認証」、「外部サーバ認証」といたユーザ認証方式の選択は、FMT_MOF.1[2]により、管理者だけに許可される。ユーザ認証における不成功認証の試行回数である認証失敗回数の閾値の設定（改変）は、FMT_MTD.1[3]により管理者だけに許可される。
FIA_SOS.1[6]によりネットワークを経由したユーザ認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。

＜識別認証されたユーザのセッションの管理に必要な要件＞
識別認証されたユーザのセッションの持続時間は、パネルからログインした場合は FTA_SSL.3 により、パネルオートログオフ時間が経過した後、セッションを終了することによって、不必要なセッション接続に伴う攻撃の機会を低減させることに貢献している。
パネルオートログオフ時間の変更は、FMT_MTD.1[3]により管理者に制限される。

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

FIA_SOS.1[3]により、ユーザパスワードの品質が検証される。FMT_MTD.1[2]により、ユーザ認証の方式に「本体認証」が選択されている場合、ユーザ自身のユーザパスワードの変更はユーザ及び管理者に制限される。

＜管理者をセキュアに維持するために必要な要件＞

⇒ set.admin 参照

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

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

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

- **O.PRIVATE-BOX（個人ボックスアクセス制御）**

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

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

＜個人ボックスの管理＞
FMT_MSA.1[1]により、ユーザ自身のユーザ ID が設定されるボックスのユーザ属性の変更操作は、ユーザ、管理者に許可される。
ボックスの登録は、FMT_MSA.3[1]によりボックスのユーザ属性には共有が指定され、これを変更する初期値を与えるのはユーザだけに許可される。また同要件により未登録ボックスを指定したボックスへ保管するジョブが実行された場合は、当該ジョブを実行したユーザのユーザ ID が自動的に指定される。

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

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

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

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

- **O.PUBLIC-BOX（共有ボックスアクセス制御）**

本セキュリティ対策方針は、共有ボックスの閲覧をすべてのユーザに許可し、共有ボックスの設定、共有ボックス内のボックスファイルのユーザ機能の操作をその共有ボックスの利用を許可さ

れたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

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

＜共有ボックスの管理＞
FMT_MSA.1[2]により、「共有」が設定されるボックスのユーザ属性の変更操作は、その共有ボックスの利用を許可されたユーザに許可される。FMT_MTD.1[4]により、ボックスパスワードの変更は、管理者及びその共有ボックスの利用を許可されたユーザだけに許可される。FIA_SOS.1[7]により、ボックスパスワードの品質が検証される。
ボックスの登録は、FMT_MSA.3[1]によりボックスのユーザ属性には共有が指定され、これを変更する初期値を与えるのはユーザだけに許可される。また同要件により未登録ボックスを指定したボックスへ保管するジョブが実行された場合は、当該ジョブを実行したユーザのユーザ ID が自動的に指定される。FMT_MTD.1[5]により、ボックスパスワードの登録はユーザ、管理者だけに許可される。

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

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

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

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

- **O.GROUP-BOX（グループボックスアクセス制御）**

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

＜ボックスアクセス制御（グループボックス）＞
FDP_ACC.1[1]、FDP_ACF.1[1]により、利用者を代行するタスクは、サブジェクトのセキュリティ属性の所属部門（部門 ID）と一致するユーザ属性が設定されるボックス（グループボックス）に対して一覧表示操作が許可される。
グループボックス内のボックスファイルを操作するには、そのグループボックスの利用を許可されたユーザである必要があるが、部門認証方式が「個別認証方式」の場合、FIA_UID.2[6]、FIA_UAU.2[6]により、そのグループボックスの利用を許可されたユーザであることを識別認証される。部門認証方式が「ユーザ認証連動方式」である場合で所属部門が登録されていない場合は、その部門の利用を許可されたユーザであることを、FIA_UID.2[6]、FIA_UAU.2[6]により、識別認証する。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[7]により、不成功認証が 1～3 回に達すると、以降その部門に対する認証機能をロックする。このロック状態は、管理者の解除操作によって解除される。
そのグループボックスの利用を許可されたユーザであることの認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにボックス ID が関連付けられると、FDP_ACC.1[1]、FDP_ACF.1[1]により、サブジェクト属性の部門 ID、ボックス ID と一致するオブジェクト属性を持つボックスファイルに対して、印刷、ダウンロード、各送信、移動、コピーの操作が許可される。

＜グループボックスの管理に必要な要件＞
FMT_MSA.1[3]により、「部門 ID」が設定されるボックスのユーザ属性の変更操作は、そのグループボックスの利用を許可されたユーザに許可される。

＜グループボックスに関係するサブジェクト属性の管理に必要な要件＞
FMT_MTD.1[12]により、部門 ID 及び部門パスワードの登録は、管理者だけに制限される。また FMT_MTD.1[3]により、部門 ID 及び部門パスワードの改変は、管理者だけに制限される。ユーザに割り当たられる所属部門の登録は、FMT_MTD.1[13]により管理者及びその部門の利用を許可されたユーザだけに制限される。FIA_SOS.1[7]により、部門パスワードの品質が検証される。

＜部門認証方式の管理＞
FMT_MOF.1[3]により、部門認証機能のふるまい管理、停止操作管理は管理者だけに制限される。

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

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

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

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

- **O.SECURE-PRINT（セキュリティ文書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、セキュリティ文書プリントファイルの印刷をそのセキュリティ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。

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

＜セキュリティ文書パスワード＞
FMT_MTD.1[8]により、認証に利用されるセキュリティ文書パスワードの登録はユーザだけに許可される。FIA_SOS.1[5]によりセキュリティ文書パスワードの品質は検証される。

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

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

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

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

- **O.CONFIG（管理機能へのアクセス制限）**

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

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

＜バックアップ、リストア機能の操作制限＞
利用を代行するタスクに管理者属性が関連づけられると、利用者を代行するタスクは、
- FDP_ACC.1[1]、FDP_ACF.1[1]によりボックスファイル
- FDP_ACC.1[2]、FDP_ACF.1[2]によりセキュリティ文書プリントファイル

を対象として、バックアップ操作が許可される。また
- FDP_ACC.1[3]、FDP_ACF.1[3]により暗号化ワードオブジェクト、HDD ロックパスワードオブジェクト、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

を対象として、リストア操作を許可される。更に
- FMT_MOF.1[1]によりセキュリティ強化設定データ
- FMT_MSA.1[1]及び FMT_MSA.1[2]によりボックスのユーザ属性
- FMT_MTD.1[2]によりユーザパスワード
- FMT_MTD.1[3]によりユーザ ID、SNMP パスワード、パネルオードログオフ時間、認証失敗回数、セキュリティ文書パスワード、外部サーバ認証設定データ、部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データ、所属部門、CE 認証ロック時間、管理者認証ロック時間
- FMT_MTD.1[4]によりボックスパスワード

を対象データとして管理者だけにリストア操作（すなわち改変操作）が許可される。FMT_MTD.1[7]により SNMP パスワード、ユーザパスワード、ボックスパスワード、セキュリティ文書パスワード、部門パスワードのバックアップ操作（すなわち問い合わせ操作）が管理者だけに許可される。

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

＜HDD ロックパスワード、暗号化ワードの管理＞
利用者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、暗号化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[4]により HDD ロックパスワード及び暗号化ワードの品質が検証される。なお HDD ロックパスワードや暗号化ワードが変更される際は、FIA_UAU.6 により、それぞれ既登録済み HDD ロックパスワード、暗号化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。
また利用者を代行するタスクに CE 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、暗号化ワードオブジェ

クトに対する設定操作が許可される。

＜MIB オブジェクトに対するアクセスに必要な要件＞
SMTP サーバグループオブジェクト、DNS サーバグループオブジェクト、MFP アドレスグループオブジェクトは、MIB オブジェクトとしても存在するため、SNMP によるアクセスにも制限が必要である。
FIA_UID.2[2]、FIA_UAU.2[2]により、MIB オブジェクトにアクセスする利用者が管理者であることを識別認証する。
FIA_AFL.1[3]により、不成功認証が 1～3 回に達すると、MIB オブジェクトにアクセスするための認証機能をロックする。このロック状態は、管理者によるロック解除操作によって解除される。
SNMP パスワード利用した管理者認証における不成功認証の試行回数である認証失敗回数の閾値の設定は、FMT_MTD.1[3]により、管理者だけに制限される。
FMT_MTD.1[3]により SNMP パスワードの変更は、管理者に制限される。FIA_SOS.1[2]により、SNMP パスワードの品質が検証される。
SNMP パスワードの初期化は、FMT_MTD.1[11]により、管理者、サービスエンジニアだけに制限される。
SNMP パスワード認証機能の方式は、FMT_MOF.1[2]により、管理者だけに制限される。

＜高信頼チャネル機能設定データの操作制限＞
高信頼チャネル機能設定データの登録は、FMT_MTD.1[12]により、管理者だけに許可される。高信頼チャネル機能設定データの改変は、FMT_MTD.1[3]により、管理者だけに許可される。高信頼チャネル機能のふるまいは、FMT_MOF.1[2]により、管理者だけに許可される。

＜S/MIME 機能のための操作制限＞
S/MIME 証明書、送信宛先データの登録は、FMT_MTD.1[12]により、管理者だけに許可される。また登録される S/MIME 証明書、送信宛先データの変更は、FMT_MTD.1[3]により、管理者だけに許可される。S/MIME 機能のふるまいは、FMT_MOF.1[2]により、管理者だけに許可される。

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

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

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

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

- **O.OVERWRITE-ALL（完全上書き削除）**

本セキュリティ対策方針は、HDD のすべてのデータ領域を抹消し、利用者が設定した NVRAM 上の秘匿情報を初期化するとしており、削除に関係する諸要件が必要である。
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。
よって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-KEY（暗号鍵生成）**

本セキュリティ対策方針は、暗号化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（SHA-1）を利用し、128bit の暗号鍵を生成する。なおコニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）とは、一般標準で認められたアルゴリズムではないが、FIPS 180-1 で指定される SHA-1 を使ったアルゴリズムであるため、128bit のエントロピーを損ねることのない、強度十分なアルゴリズムであり、セキュリティ対策方針が求める強度レベルを損ねることはない。（本アルゴリズムに関する説明は、6 章 TOE 要約仕様参照）

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.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。

- **O.TRUSTED-PASS（高信頼チャネルの利用）**

本セキュリティ対策方針は、ボックスファイル、セキュリティ文書プリントファイル等の送受信において高信頼チャネルを生成するとしており、高信頼チャネルに関係する要件が必要である。

FTP_ITC.1 は、リモート高信頼 IT 製品からの要求に応じて高信頼チャネルを生成するとしており、ボックスファイル、セキュリティ文書プリントファイル等の送受信に適用される。

この機能要件によって本セキュリティ対策方針は満たされる。

- **O.CRYPTO-MAIL（暗号化メールの利用）**

本セキュリティ対策方針は、ボックスファイルをメールにて送信する際にボックスファイルを暗号化することを規定しており、暗号に関する諸要件が必要である。

FCS_CKM.1 により、FIPS 186 に従った擬似乱数生成アルゴリズムを利用し、暗号鍵（128 bit、または 168 bit、または 192 bit、または 256 bit）を生成する。

FCS_COP.1 により、FIPS PUB 197 の AES（暗号鍵：128 bit、または 192 bit、または 256 bit）を利用してボックスファイルを暗号化する。（これは S/MIME の送信データになる。）また同要件により SP800-67 の 3-Key-Triple-DES（暗号鍵：168 bit）を利用してボックスファイルを暗号化する。（これも同様に S/MIME の送信データになる。）これら暗号鍵は、FCS_COP.1 により、各宛先の S/MIME 証明書の公開鍵（1024bit、または 2048 bit、または 3072 bit、または 4096 bit）である FIPS 186-1 の RSA により暗号化される。

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

- **OE.CRYPTO（HDD の暗号化）**

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としており、暗号に関係する諸要件が必要である。

FCS_COP.1[E]により、暗号化基板は FIPS PUB 197 に準拠する AES を使って 128bit の暗号鍵より HDD に書き込まれるすべてのデータの暗号化、復号処理を行う。

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、入力されるユーザパスワード、ボックスパスワード、管理者パスワード、部門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ー文字毎に“＊”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に入力毎 1 文字ごとに“＊”を返し、認証をサポートする。

  FIA_AFL.1[8]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[2]により、不成功認証が 1～3 回に達すると、認証中であればログオフし、以降管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除機能が実行され、管理者認証ロック時間が経過後に解除される。

  管理者認証における不成功認証の試行回数である認証失敗回数の閾値の設定及び管理者認証ロック時間は、FMT_MTD.1[3]により、管理者だけに許可される。

  ＜識別認証された管理者のセッションの管理＞

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

  ＜管理者の認証情報の管理など＞

  管理者パスワードは、FIA_SOS.1[1]により品質が検証される。また FIA_SOS.[6]によりネットワークを経由した管理者認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。管理者パスワードの変更は、FMT_MTD.1[6]により、管理者及びサービスエンジニアに制限される。管理者が管理者パスワードを変更する場合は、FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[2]に

より、不成功認証が 1～3 回に達すると、認証中であればログオフし、以降管理者の認証状態を解除し、管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除機能が実行され、管理者認証ロック時間が経過後に解除される。
また管理者パスワードの初期化は FMT_MTD.1[11]により管理者、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に入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[8]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[1]により、不成功認証が 1～3 回に達すると、認証中であればログオフし、CE パスワードを利用するすべての認証機能をロックする。このロック状態は、シークレットロック解除機能が実行されて、CE 認証ロック時間を経過すると解除される。
サービスエンジニア認証における不成功認証の試行回数である認証失敗回数の閾値の設定は FMT_MTD.1[3]により管理者だけに許可される。CE 認証ロック時間の設定は、FMT_MTD.1[9]により、サービスエンジニアだけに許可される。

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

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

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を想定するものではない。

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 13 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、 FMT_MSA.2	FCS_COP.1、FCS_COP.1[E] ＜①FCS_CKM.4、②FMT_MSA.2 を適用しない理由＞ ① 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。 ② 本 TOE には、暗号鍵に対して管理されるべきセキュリティ属性をもたないため、セキュアなセキュリティ属性を規定する必要はない。
FCS_COP.1	FCS_CKM.1 or FDP_ITC.1、 FCS_CKM.4、 FMT_MSA.2	FCS_CKM.1（一部事象のみ）、 満たしている事象：S/MIME 通信にて添付ファイルを暗号化するための暗号鍵を生成すること。 ＜FCS_CKM.1 or FDP_ITC.1 を一部満たしていない理由＞ ・S/MIME のデータ暗号化のための暗号鍵を暗号化するための公開鍵を TSC 外よりインポートするため、FDP_ITC.1 の適用が妥当と考えられるが、S/MIME 証明書は、管理者の操作によって登録される。その際、信頼されないチャネルを経由する、しない等の考慮は不要であり、セキュリティ要件を適用する必然性がない。（A.NETWORK が成立する条件下での利用） ・またインポートされる暗号鍵の属性情報は、アクセス制御等に利用されるセキュリティ属性に相当せず、属性の初期化等に関係せず、適用が難しい。 ・FMT_MTD.1[12]にて TSF データの登録として、表現されており、インポート操作を行う対象は適切な役割に割り振られている。 ・結果、鍵管理相当の事象は依存性で示されるセキュリティ要件ではなく他のセキュリティ要件を用いて説明されているため、本依存性が満たされなくとも問題ない。 ＜FCS_CKM.4 を適用しない理由＞ 暗号鍵は、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。 ＜FMT_MSA.2 を適用しない理由＞ 送信の都度生成される 3-Key-Triple-DES の暗号鍵は、暗号鍵に対して管理されるべきセキュリティ属性をもたないため、セキュアなセキュリティ属性を規定する必要はない。
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]

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_ACF.1[1]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[1]、 FMT_MSA.3[1]
FDP_ACF.1[2]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3[2]
FDP_ACF.1[3]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[3] ＜FMT_MSA.3 を適用しない理由＞ オブジェクト属性が存在しないため、本要件を適用する必要性はない。
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[2]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[5]
FIA_AFL.1[7]	FIA_UAU.1	FIA_UAU.2[6]
FIA_AFL.1[8]	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、 FIA_UAU.2[4]、FIA_UAU.2[5]、FIA_UAU.2[6]
FIA_ATD.1	なし	N/A
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_SOS.1[5]	なし	N/A
FIA_SOS.1[6]	なし	N/A
FIA_SOS.1[7]	なし	N/A
FIA_SOS.2	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.2[5]	FIA_UID.1	FIA_UID.2[5]
FIA_UAU.2[6]	FIA_UID.1	FIA_UID.2[6]
FIA_UAU.6	なし	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、 FIA_UAU.2[4]、FIA_UAU.2[5]、FIA_UAU.2[6]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FIA_UID.2[5]	なし	N/A
FIA_UID.2[6]	なし	N/A
FIA_UID.2[7]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MSA.1[1]	FDP_ACC.1 or FDP_IFC.1、 FMT_SMF.1、 FMT_SMR.1	FDP_ACC.1[1]、 FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1、	FDP_ACC.1[1]、

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MSA.1[3]	FDP_ACC.1 or FDP_IFC.1、 FMT_SMF.1、 FMT_SMR.1	FDP_ACC.1[1]、 FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[6]
FMT_MSA.3[1]	FMT_MSA.1、 FMT_SMR.1	FMT_MSA.1[1]、FMT_MSA.1[2]、 FMT_SMR.1[3]
FMT_MSA.3[2]	FMT_MSA.1、 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ 一意に識別される内部制御 ID であり、一度割り当てられた後に変更、削除といった管理を必要としないため。 ＜FMT_SMR.1＞ FMT_MSA.3.2[2] の割付は該当なしである。 FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2] 、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[6]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[7]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[8]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[3]
FMT_MTD.1[9]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]、FMT_SMR.1[5]
FMT_MTD.1[11]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1] FMT_SMR.1[2]
FMT_MTD.1[12]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[13]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2] FMT_SMR.1[6]
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[5]
FMT_SMR.1[5]	FIA_UID.1	FIA_UID.2[7]
FMT_SMR.1[6]	FIA_UID.1	FIA_UID.2[6]
FPT_RVM.1	なし	N/A
FPT_SEP.1	なし	N/A
FTA_SSL.3	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
FTP_ITC.1	なし	N/A
FNEW_RIP.1	なし	N/A
FIA_NEW.1	なし	N/A
FCS_COP.1[E]	FDP_ITC.1 or FCS_CKM.1、FCS_CKM.4、FMT_MSA.2	FCS_CKM.1 ＜①FCS_CKM.4、②FMT_MSA.2 を適用しない理由＞ ① 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。 ② 本 TOE には、暗号鍵に対して管理されるべきセキュリティ属性をもたないため、セキュアなセキュリティ属性を規定する必要はない。
FIA_AFL.1[E]	FIA_UAU.1	FIA_UAU.2[E]
FIA_UAU.2[E]	FIA_UID.1	適用しない ＜FIA_UID.1 を適用しない理由＞ 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。 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[3]、FIA_UAU.2[5]

8.2.1.6. IT セキュリティ機能要件の相互サポート関係

機能要件の依存性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 14 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
FCS_CKM.1	N/A	FMT_MTD.1[3] FMT_MTD.1[12]	FMT_MOF.1[1]	N/A
FCS_COP.1	N/A	FMT_MTD.1[3] FMT_MTD.1[12]	N/A	N/A
FDP_ACC.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACF.1[1]	FIA_UAU.2[2] FIA_UAU.2[3] FIA_UAU.2[5] FIA_UAU.2[6]	FMT_MSA.1[1] FMT_MSA.1[2] FMT_MSA.1[3] FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[2]	FIA_UAU.2[2] FIA_UAU.2[3] FIA_UAU.2[4] FIA_UAU.2[6]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[3]	FIA_UAU.2[1] FIA_UAU.2[2]	FPT_SEP.1	FMT_MOF.1[1]	N/A

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[1]	N/A	FMT_MTD.1[9]	FMT_MOF.1[1]	N/A
FIA_AFL.1[2]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_AFL.1[3]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_AFL.1[4]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_AFL.1[5]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_AFL.1[6]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_AFL.1[7]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[8]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_ATD.1	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[6]	N/A	N/A	N/A	N/A
FIA_SOS.1[7]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.2	N/A	N/A	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FMT_MTD.1[9]	FMT_MOF.1[1]	N/A
FIA_UAU.2[2]	FPT_RVM.1	FMT_MTD.1[3] FMT_MTD.1[6] FMT_MTD.1[7] FMT_MTD.1[11]	FMT_MOF.1[1]	N/A
FIA_UAU.2[3]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[7]	FMT_MOF.1[1]	N/A
FIA_UAU.2[4]	FPT_RVM.1	FMT_MTD.1[3] FMT_MTD.1[7] FMT_MTD.1[8]	FMT_MOF.1[1]	N/A
FIA_UAU.2[5]	FPT_RVM.1	FMT_MTD.1[4] FMT_MTD.1[5] FMT_MTD.1[7]	FMT_MOF.1[1]	N/A
FIA_UAU.2[6]	FPT_RVM.1	FMT_MTD.1[3] FMT_MTD.1[7] FMT_MTD.1[12]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.6	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UAU.7	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[3]	N/A	FMT_MTD.1[10]	FMT_MOF.1[1]	N/A
FIA_UID.2[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[6]	N/A	FMT_MTD.1[3] FMT_MTD.1[12]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[7]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FIA_USB.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[1]	N/A	N/A	N/A	N/A
FMT_MOF.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[3]	N/A	N/A	N/A	N/A
FMT_MSA.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MSA.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MSA.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MSA.3[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MSA.3[2]	N/A	N/A	FMT_MOF.1[1]	N/A

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
FMT_MTD.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[6]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[7]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[8]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[9]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[10]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[11]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[12]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[13]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMF.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[6]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FPT_RVM.1	N/A	N/A	FMT_MOF.1[1]	N/A
FPT_SEP.1	N/A	N/A	FMT_MOF.1[1]	N/A
FTA_SSL.3	N/A	FMT_MTD.1[3]	FMT_MOF.1[1]	N/A
FTP_ITC.1	N/A	FMT_MTD.1[3] FMT_MTD.1[12]	FMT_MOF.1[1]	N/A
FIA_NEW.1	FPT_RVM.1	N/A	FMT_MOF.1[1]	N/A
FNEW_RIP.1	N/A	N/A	N/A	N/A
FCS_COP.1[E]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_AFL.1[E]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UAU.2[E]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UAU.7[E]	N/A	N/A	FMT_MOF.1[1]	N/A

① **迂回防止**

＜管理者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]、セキュリティ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]、設定管理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。

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。

＜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＞

設定管理アクセス制御を規定する FDP_ACF.1[3]は、サービスエンジニアの識別認証を規定する FIA_UAU.2[1]によってバイパス防止がサポートされる。

さらに 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。

＜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、ユーザの認証を規定する FIA_UAU.2[3]、部門認証を規定する FIA_UAU.2[6]によってバイパス防止がサポートされる。共有ボックスに

対するアクセスの場合は、FIA_UAU.2[5]も FDP_ACF.1[1]のバイパス防止に貢献する。
さらにユーザの認証を規定する FIA_UAU.2[3]、部門認証を規定する FIA_UAU.2[6]、共有ボックスの利用を許可されたユーザであることの認証を規定する FIA_UAU.2[5]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。

＜セキュリティ文書プリントに関係する機能要件のバイパス防止＞
セキュリティ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、ユーザの認証を規定する FIA_UAU.2[3]、部門認証を規定する FIA_UAU.2[6]、セキュリティ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[4]によってバイパス防止がサポートされる。
さらにユーザの認証を規定する FIA_UAU.2[3]、部門認証を規定する FIA_UAU.2[6]、セキュリティ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[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。

＜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＞
ボックスのセキュリティ属性であるユーザ属性は、「共有」が設定されている場合は、FMT_MSA.1[2]によりボックスの利用を許可された利用者及び管理者だけに改変を許可している。「ユーザ ID」が設定されている場合は、FMT_MSA.1[1]によりそのユーザと管理者だけに改変を許可している。「部門 ID」が設定されている場合は、FMT_MSA.1[3]により、その部門の利用を許可されたユーザと管理者だけに改変を許可している。また 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ユーザ、認証された管理者、認証された共有ボックスの利用を許可されたユーザの 3 つのタイプのサブジェクトだけがボックス、ボックスファイルの操作が可能である。
以上、4 つの要件によって 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。

＜セキュリティ文書プリントファイルアクセス制御の維持＞
FPT_SEP.1 によりセキュリティ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ユーザ、認証された管理者、認証されたセキュリティ文書プリントファイルの利用を許可されたユーザの 3 つのタイプのサブジェクトだけがセキュリティ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。

＜設定管理アクセス制御の維持＞
FPT_SEP.1 により設定管理アクセス制御で想定されている認証された管理者、認証されたサービスエンジニアを代行するサブジェクトだけが、設定管理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。

＜CE パスワードの管理＞
CE パスワードの改変操作は FMT_MTD.1[9]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[6]により管理者及びサービスエンジニアだけに許可している。管理者パスワードの初期化は、FMT_MTD.1[11]により管理者、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。

＜SNMP パスワードの管理＞
SNMP パスワードの改変操作は FMT_MTD.1[3]により管理者、問い合わせ操作は FMT_MTD.1[7]により管理者、初期化操作は FMT_MTD.1[11]により管理者、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。

＜ユーザパスワードの管理＞
ユーザパスワードの登録は FMT_MTD.1[1]により管理者､改変操作は FMT_MTD.1[2]により管理者及びそのユーザ、問い合わせ操作は FMT_MTD.1[7]により管理者だけに許可している。これより FIA_UAU.2[3]の不正な干渉・破壊防止がサポートされる。

＜部門パスワードの管理＞
部門パスワードの登録は FMT_MTD.1[12]により管理者、改変操作は FMT_MTD.1[3]により管理者及、問い合わせ操作は FMT_MTD.1[7]により管理者だけに許可している。これより FIA_UAU.2[6]の不正な干渉・破壊防止がサポートされる。

＜セキュリティ文書パスワードの管理＞
セキュリティ文書パスワードの登録は FMT_MTD.1[8]によりユーザだけに許可、問い合わせ操作は FMT_MTD.1[7]により管理者だけに許可､改変は FMT_MTD.1[3]により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。

＜ボックスパスワードの管理＞
ボックスパスワードの登録は、FMT_MTD.1[5]によりユーザ及び管理者、改変操作は FMT_MTD.1[4]により共有ボックスの利用を許可されたユーザ及び管理者、問い合わせ操作は FMT_MTD.1[7]により管理者だけに許可している。これより FIA_UAU.2[5]の不正な干渉・破壊防止がサポートされる。

＜ユーザ ID の管理＞
ユーザ ID の登録は、FMT_MTD.1[10]により管理者だけに限定され、外部サーバ認証利用時にはユーザ認証されたことをもって MFP に登録されていないユーザは自動的に登録される。また改変は FMT_MTD.1[3]により管理者だけに許可している。これより FIA_UID.2[3]の不正な干渉・破壊防止がサポートされる。

＜部門 ID、所属部門の管理＞
部門 ID の登録は、FMT_MTD.1[12]により管理者だけに限定される。また改変操作は FMT_MTD.1[3]により管理者だけに許可している。
また所属部門の改変操作は FMT_MTD.1[3]により管理者だけに許可している。
これより FIA_UID.2[6]の不正な干渉・破壊防止がサポートされる。

＜外部サーバ認証設定データの管理＞
外部サーバ認証時に利用する外部サーバ認証設定データの設定は､FMT_MTD.1[10]により管理者だけに許可している。これより FIA_UID.2[7]の不正な干渉・破壊防止がサポートされる。

＜オートログオフ時間の管理＞
パネルオートログオフ時間の改変操作は、FMT_MTD.1[3]により管理者だけに許可している。これより FTA_SSL.3 の不正な干渉・破壊防止がサポートされる。

＜認証失敗回数閾値の管理＞
サービスエンジニア認証、管理者認証、ユーザ認証、セキュリティ文書プリント認証、ボックス認証、MIB オブジェクトアクセスにおける認証といったすべての認証行為において設定される認証回数失敗閾値の改変操作は、FMT_MTD.1[3]により管理者だけに許可している。これより FIA_AFL.1[1]、FIA_AFL.1[2]、FIA_AFL.1[3]、FIA_AFL.1[4]、FIA_AFL.1[5]、FIA_AFL.1[6]、FIA_AFL.1[7]の不正な干渉・破壊防止がサポートされる。

＜高信頼チャネル機能の管理＞
高信頼チャネル機能設定データの登録は、FMT_MTD.1[12]により管理者だけに限定される。また改変操作は FMT_MTD.1[3]により管理者だけに許可している。これより FTP_ITC.1 の不正な干渉・破壊防止がサポートされる。

＜CE 認証ロック時間の管理＞
CE 認証ロック時間の設定は、FMT_MTD.1[9]によりサービスエンジニアだけに許可している。これより FIA_AFL.1[2]の不正な干渉・破壊防止がサポートされる。

＜管理者認証ロック時間の管理＞
管理者認証ロック時間の設定は、FMT_MTD.1[3]によりサービスエンジニアだけに許可している。これより FIA_AFL.1[1]の不正な干渉・破壊防止がサポートされる。

＜S/MIME 証明書の管理＞
S/MIME 証明書の登録は、FMT_MTD.1[12]により管理者だけに限定される。また改変操作は FMT_MTD.1[3]により管理者だけに許可している。これより FCS_CKM.1、FCS_COP.1 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[1]により、セキュリティ強化機能の動作設定が管理者及びサービスエンジニアだけに許可されている。セキュリティ強化機能は、多くの TOE のセキュリティ構造に影響するものであり、FCS_COP.1、FMT_MOF.1[1]、FMT_MOF.1[3]、FIA_SOS.1[6]、FIA_SOS.2、FNEW_RIP.1 を除く TOE のセキュリティ要件によって実現されるすべてのセキュリティ機能の非活性化防止がサポートされる。

＜部門認証機能の維持＞
FMT_MOF.1[3]により、部門認証機能の動作設定（停止操作の管理）が管理者に許可されており、部門認証に関係する FIA_UID.2[6]、FIA_UAU.2[6]、FIA_AFL.1[7]、FMT_SMR.1[6]の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。[12]

[12] 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

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。

8.2.4. 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セキュリティ文書プリント、③MFP アドレスなど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。

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。）

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 15 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.ADMIN-SNMP	F.SERVICE	F.USER	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPTO	F.HDD	F.RESET	F.TRUSTED-PASS	F.S/MIME
FCS_CKM.1								●				●
FCS_COP.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]	●	●	●									
FIA_AFL.1[1]			●							●		
FIA_AFL.1[2]	●		●							●		
FIA_AFL.1[3]	●	●										
FIA_AFL.1[4]	●			●								
FIA_AFL.1[5]	●					●						
FIA_AFL.1[6]	●				●							
FIA_AFL.1[7]	●			●								
FIA_AFL.1[8]	●		●	●	●	●						
FIA_ATD.1				●	●	●						
FIA_SOS.1[1]	●		●									
FIA_SOS.1[2]	●	●										
FIA_SOS.1[3]	●			●								
FIA_SOS.1[4]	●											
FIA_SOS.1[5]						●						
FIA_SOS.1[6]	●			●	●							
FIA_SOS.1[7]	●				●							
FIA_SOS.2	●			●	●							
FIA_UAU.2[1]			●									
FIA_UAU.2[2]	●	●										
FIA_UAU.2[3]				●								
FIA_UAU.2[4]						●						
FIA_UAU.2[5]					●							
FIA_UAU.2[6]				●								
FIA_UAU.6	●		●									
FIA_UAU.7	●		●	●	●	●						

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.USER	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPTO	F.HDD	F.RESET	F.TRUSTED-PASS	F.S/MIME
FIA_UID.2[1]			●									
FIA_UID.2[2]	●	●										
FIA_UID.2[3]				●								
FIA_UID.2[4]						●						
FIA_UID.2[5]					●							
FIA_UID.2[6]				●								
FIA_UID.2[7]				●								
FIA_USB.1				●	●	●						
FMT_MOF.1[1]	●		●									
FMT_MOF.1[2]	●	●										
FMT_MOF.1[3]	●											
FMT_MSA.1[1]	●				●							
FMT_MSA.1[2]	●				●							
FMT_MSA.1[3]	●				●							
FMT_MSA.3[1]	●				●							
FMT_MSA.3[2]						●						
FMT_MTD.1[1]	●											
FMT_MTD.1[2]	●			●								
FMT_MTD.1[3]	●	●										
FMT_MTD.1[4]	●				●							
FMT_MTD.1[5]	●				●							
FMT_MTD.1[6]	●		●									
FMT_MTD.1[7]	●											
FMT_MTD.1[8]						●						
FMT_MTD.1[9]			●									
FMT_MTD.1[10]	●			●								
FMT_MTD.1[11]	●		●									
FMT_MTD.1[12]	●											
FMT_MTD.1[13]	●			●								
FMT_SMF.1	●	●	●	●	●	●						
FMT_SMR.1[1]			●									
FMT_SMR.1[2]	●	●										
FMT_SMR.1[3]				●	●	●						
FMT_SMR.1[4]					●							
FMT_SMR.1[5]				●								
FMT_SMR.1[6]				●								
FPT_RVM.1	●	●	●	●	●	●			●			
FPT_SEP.1	●	●	●	●	●	●						
FTA_SSL.3	●			●								
FTP_ITC.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。

- **FCS_CKM.1**

  FCS_CKM.1 は、HDD の暗号化、S/MIME 機能の利用に伴い生成される暗号鍵の諸条件を規定している。
  F.CRYPTO は、コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）を利用して 128bit の暗号鍵を生成する。
  F.S/MIME は、擬似乱数生成アルゴリズムを利用して AES 用にて利用される 128bit、または 192bit、または 256bit の暗号鍵を生成する。また 3-Key-Triple-DES の場合は同様に擬似乱数生成アルゴリズムを利用して 168bit の暗号鍵を生成する。
  従って本機能要件は満たされる。

- **FCS_COP.1**

  FCS_COP.1 は、HDD の暗号化に伴い生成される暗号鍵の諸条件を規定している。
  F.SMIME は、S/MIME 機能において、データの暗号化に 168bit の暗号鍵より 3-Key-Triple-DES を利用して暗号化する。または 128bit、または 192bit、または 256bit の暗号鍵より AES を利用して暗号化する。データの暗号化に用いられる暗号鍵は、1024bit、または 2048bit、または 3072bit、または 4096bit の暗号鍵より RSA を利用して暗号化する。
  従って本機能要件は満たされる。

- **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.ADMIN は、利用者を代行するタスクが、ボックスの一覧表示、ボックスファイルをバックアップするためのボックスアクセス制御を実施する。
  F.BOX は、利用者を代行するタスクが、ボックスの一覧表示、ボックスファイルを印刷、送信、ダウンロード、移動、コピー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セキュリティ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.ADMIN は、利用者を代行するタスクが、セキュリティ文書プリントファイルをバックアップするためのセキュリティ文書プリントファイルアクセス制御を実施する。
  F.PRINT は、利用者を代行するタスクが、セキュリティ文書プリントファイルを一覧表示、印刷するためのセキュリティ文書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、暗号化ワードオブジェクト、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、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しては、設定、リストアする設定管理アクセス制御を実施する。
F.ADMIN-SNMP は、利用者を代行するタスクが、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を設定する設定管理アクセス制御を実施する。
F.SERVICE 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、暗号化ワードオブジェクトを設定する設定管理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.ADMIN 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。
- 管理者に対して、ボックスの設定に際してボックスの一覧表示操作を許可する。
- 管理者に対してボックスファイルのバックアップ操作を許可する。

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。
- ユーザに対して、ユーザ ID と一致するオブジェクト属性を持つボックス（個人ボックス）の一覧表示を許可する。
- ユーザに対して、選択した個人ボックス内のボックスファイルの印刷、送信、ダウンロード、移動、コピー操作を許可する。
- ユーザに対して、共有が設定されるボックス（共有ボックス）の一覧表示操作を許可する。
- 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印刷、送信、ダウンロード、移動、コピー操作を許可する。
- ユーザに対して、部門 ID と一致するオブジェクト属性を持つボックス（グループボックス）の一覧表示を許可する。
- ユーザに対して、選択したグループボックス内のボックスファイルの印刷、送信、ダウンロード、移動、コピー操作を許可する。

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セキュリティ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.ADMIN は、以下の規則が適用されるセキュリティ文書プリントファイルアクセス制御を実施する。
- 管理者に対してセキュリティ文書プリントファイルのバックアップ操作を許可する。

F.PRINT は、以下の規則が適用されるセキュリティ文書プリントファイルアクセス制御を実施する。
- ユーザに対して、セキュリティ文書プリントファイルの一覧表示操作を許可する。
- セキュリティ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、選択したセキュリティ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、暗号化ワードオブジェクト、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設定管理アクセス制御を実施する。

- 管理者に対して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の設定、リストア操作を許可する。

F.ADMIN-SNMPは、以下の規則が適用される設定管理アクセス制御を実施する。

- 管理者に対して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の設定操作を許可する。

F.SERVICEは、以下の規則が適用される設定管理アクセス制御を実施する。

- サービスエンジニアに対してHDDロックパスワードオブジェクト、暗号化ワードオブジェクトの設定操作（初期化操作）を許可する。

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、CEパスワ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、管理者が設定する失敗回数閾値（1～3回）の認証失敗を検知するとサービスモード認証状態であればログオフし、認証機能をロックする。
F.RESETは、シークレットロック解除機能の実行後に電源OFF/ONによるTOEの起動により、CE認証ロック時間後、失敗回数をクリアして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、管理者が設定する失敗回数閾値（1～3回）の認証失敗を検知すると管理者モード認証状態であればログオフし、認証機能をロックする。
F.RESETは、電源OFF/ONによるTOEの起動より、管理者認証ロック時間後、失敗回数をクリアしてロック状態を解除する。
また F.SERVICE は、サービスモード内にて提供するロック解除機能により認証失敗回数をクリアして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、SNMPを利用してMIBオブジェクトへアクセスする際の管理者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-SNMPは、MIBオブジェクトへのアクセスの際に行うSNMPパスワードを利用した認証において、管理者が設定する失敗回数閾値（1～3回）の認証失敗を検知するとMIBオブジェクト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認証失敗回数をクリアして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、ユーザ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.USER は、ユーザのアクセス、ユーザによるユーザ自身のパスワード変更の際に行うユーザの認証において、管理者が設定する失敗回数閾値（1～3回）の認証失敗を検知すると認証状態であればログオフし、以降当該ユーザの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認証失敗回数をクリアして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[5]**

FIA_AFL.1[5]は、セキュリティ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、セキュリティ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、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると当該セキュリティ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認証失敗回数をクリアして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[6]**

FIA_AFL.1[6]は、共有ボックスの利用を許可されたユーザであることの認証に対する不成功認証時アクションを規定している。
F.BOX は、共有ボックスへのアクセス、共有ボックスのパスワード変更の際に行う認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると認証状態であればログオフし、当該ボックスの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認証失敗回数をクリアして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[7]**

FIA_AFL.1[7]は、部門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.USER は、ユーザのアクセスの際に部門の認証が動作する場合において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると、以降当該部門の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認証失敗回数をクリアして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[8]**

FIA_AFL.1[8]は、パネルにおける各種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の際に行うサービスエンジニアの認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
F.ADMIN は、管理者モードへのアクセスの際に行う管理者の認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
F.USER は、パネルからのユーザのアクセスの際に行うユーザの認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。またパネルからの部門認証処理において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
F.BOX は、パネルからの共有ボックスへのアクセスの際に行う認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
F.PRINT は、セキュリティ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、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
これら一連の動作解除は、5 秒後に自動的に解除する。
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セキュリティ文書内部制御 ID を関係付ける。
F.USER は、利用者を代行するタスクに対して、所属部門（部門 ID）を関連付ける。
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、CE 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 桁の合計 92 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されない、且つ現下で設定されている値と一致しないことを検証する。
F.SERVICE は、CE パスワード、管理者パスワードの品質として 8 桁の合計 92 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されない、且つ現下で設定されている値と一致し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]**

FIA_SOS.1[2]は、SNMP パスワードの品質を規定している。
F.ADMIN は、SNMP パスワード（Privacy パスワード、Authentication パスワード）の品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）であることを検証する。
同様にして F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication パスワード）の品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）であることを検証する。
従って本機能要件は満たされる。

- **FIA_SOS.1[3]**

FIA_SOS.1[3]は、ユーザパスワードの品質を規定している。
F.ADMIN は、ユーザパスワードの品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）で、先頭から 8 桁が同一キャラクタから構成されないことを検証する。
F.USER は、ユーザパスワードの品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）で、先頭から 8 桁が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、HDD ロックパスワード、暗号化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、暗号化ワードの品質として 20 桁の合計 83 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く）で、同一キャラクタから構成されない、且つ現下で設定されている値と一致し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[5]**

FIA_SOS.1[5]は、セキュリティ文書パスワードの品質を規定している。
F.PRINT は、セキュリティ文書パスワードの品質として 8 桁の合計 93 文種の ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B 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[6]**

  FIA_SOS.1[6]は、セッション情報の品質を規定している。
  F.ADMIN は、セッション情報の品質として、10^{10} 以上の空間品質であることを検証する。
  F.BOX は、セッション情報の品質として、10^{10} 以上の空間品質であることを検証する。
  F.USER は、セッション情報の品質として、10^{10} 以上の空間品質であることを検証する。
  従って本機能要件は満たされる。

- **FIA_SOS.1[7]**

  FIA_SOS.1[7]は、部門パスワード、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、部門パスワードの品質として 8 桁の合計 95 文種の ASCII コード（0x20 ～ 0x7E）で、先頭から 8 桁が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 95 文種の ASCII コード（0x20 ～ 0x7E）で、先頭から 8 桁が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.2**

  FIA_SOS.2 は、セッション情報の生成とその品質を規定している。
  F.ADMIN は、管理者認証のセッション情報に 10^{10} 以上の空間品質である秘密を生成する。
  F.BOX は、ボックス認証のセッション情報に 10^{10} 以上の空間品質である秘密を生成する。
  F.USER は、ユーザ認証のセッション情報に 10^{10} 以上の空間品質である秘密を生成する。
  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、CE パスワ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。
  F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication パスワード）を使って MIB オブジェクトにアクセスする利用者が管理者であることを認証する。
  従って本機能要件は満たされる。

- **FIA_UAU.2[3]**

  FIA_UAU.2[3]は、ユーザの認証を規定している。
  F.USER は、各ユーザに対して設定されるユーザパスワードを使って登録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、セキュリティ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、各セキュリティ文書プリントファイルに対して設定されるセキュリティ文書パスワードを使ってセキュリティ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[5]**

FIA_UAU.2[5]は、共有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共有ボックスの利用を許可されたユーザであることを認証する。
従って本機能要件は満たされる。

- **FIA_UAU.2[6]**

FIA_UAU.2[6]は、部門の認証を規定している。
F.USER は、部門認証機能の方式が、個別認証方式である場合、各部門に対して設定される部門パスワードを使ってその部門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.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、暗号化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、暗号化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、CE パスワ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 CE パスワードに対して 1 文字毎に“*”返し、CE パスワードのダイレクト表示を防止する。
F.PRINT は、セキュリティ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セキュリティ文書パスワードに対して 1 文字毎に“*”返し、セキュリティ文書パスワードのダイレクト表示を防止する。
F.USER は、ユーザの認証においてパネルにて入力されるユーザパスワードに対して 1 文字毎に“*”返し、ユーザパスワードのダイレクト表示を防止する。また部門認証においてパネルにて入力される部門パスワードに対して 1 文字毎に“*”返し、部門パスワードのダイレクト表示を防止する。
F.BOX は、共有ボックスの利用を許可されたユーザであることの認証においてパネル入力されるボックスパスワードに対して 1 文字毎に“*”返し、ボックス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。
F.ADMIN-SNMP は、MIB オブジェクトに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、ユーザの識別を規定している。
F.USERは､各ユーザに対して設定されるユーザIDより登録されたユーザであることを識別する。
従って本機能要件は満たされる。

- **FIA_UID.2[4]**

FIA_UID.2[4]は、セキュリティ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、操作対象としてセキュリティ文書プリントファイルを選択することにより、セキュリティ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[5]**

FIA_UID.2[5]は、共有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、共有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_UID.2[6]**

FIA_UID.2[6]は、部門の識別を規定している。
F.USER は、部門認証機能の方式が個別認証方式である場合、各部門に対して設定される部門 ID より登録済みの部門であることを識別する。
従って本機能要件は満たされる。

- **FIA_UID.2[7]**

FIA_UID.2[7]は、外部サーバの識別を規定している。
F.USER は、ユーザ認証方式に外部サーバ認証が選択されている場合、ユーザ情報の問い合わせにアクセスする外部サーバを識別する。
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セキュリティ文書プリントファイルへのアクセスに対して認証された際に、当該セキュリティ文書プリントファイルの“セキュリティ文書内部制御 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、またはボックスファイルへのアクセスに対して認証された際に、当該ボックス、または当該ボックスファイルの“ボックス ID”を関連付ける。
F.USER は、利用者を代行するタスクに、部門認証方式が個別認証方式の場合は部門認証に成功した際、部門認証方式が連動方式の場合はユーザ認証した際に、“部門 ID”を関連付ける。
従って本機能要件は満たされる。

- **FMT_MOF.1[1]**

FMT_MOF.1[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。またバックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にセキュリティ強化機能を停止設定させることが可能であるが、F.ADMIN は管理者だけにバックアップ、リストア操作を許可している。HDD 論理フォーマット、全領域の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。
F.SERVICE は、サービスモードにおいて実行に伴いセキュリティ強化機能を無効とする HDD 論理フォーマット機能、HDD 物理フォーマット機能、HDD 装着設定機能、イニシャライズ機能を提供しており、セキュリティ強化機能の停止操作が管理されている。
従って本機能要件は満たされる。

- **FMT_MOF.1[2]**

FMT_MOF.1[2]は、高信頼チャネル機能、S/MIME 機能、ユーザ認証機能、及び SNMP パスワード認証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ユーザ認証機能の設定機能、高信頼チャネル機能の暗号方式設定機能、S/MIME 機能の暗号方式設定機能を提供しており、各機能の動作モードの設定を許可している。
F.ADMIN-SNMP は、SNMP パスワードによって認証された管理者に SNMP パスワード認証機能の設定機能の操作を許可している。
従って本機能要件は満たされる。

- **FMT_MOF.1[3]**

FMT_MOF.1[3]は、部門認証機能のふるまい管理、停止操作管理を規定している。
F.ADMIN は、管理者モードにおいて部門認証機能の設定機能を提供しており、各機能の動作モードの設定や部門認証の停止機能の操作を許可している。
従って本機能要件は満たされる。

- **FMT_MSA.1[1]**

FMT_MSA.1[1]は、ボックスのユーザ属性（ユーザ ID が設定されている場合）の管理を規定している。
F.ADMIN は､管理者モードにおいてボックスに設定されるユーザ属性の変更操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスのユーザ属性を改変させることが可能である。
さらに登録ユーザの削除操作によって当該ユーザが個人ボックスを所有していた場合、当該ボックスは共有ボックスに変更される。
F.BOX は、認証されたユーザに対して、ボックスのユーザ属性に当該ユーザのユーザ ID が設定されるボックスのユーザ属性を変更することを許可している。
従って本機能要件は満たされる。

- **FMT_MSA.1[2]**

FMT_MSA.1[2]は、ボックスのユーザ属性（共有が設定されている場合）の管理を規定している。
F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスのユーザ属性を改変させることが可能である。
F.BOX は、共有ボックスの利用を許可されたユーザとして認証されたユーザに対して、共有が設

定されるボックスのユーザ属性を変更することを許可している。
従って本機能要件は満たされる。

- **FMT_MSA.1[3]**

FMT_MSA.1[3]は、ボックスのユーザ属性（部門 ID が設定されている場合）の管理を規定している。
F.ADMIN は､管理者モードにおいてボックスに設定されるユーザ属性の変更操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスのユーザ属性を改変させることが可能である。
さらに登録ユーザの削除操作によって当該ユーザがグループボックスを所有していた場合、当該ボックスは共有ボックスに変更される。
F.BOX は、認証されたユーザに対して、ボックスのユーザ属性に当該ユーザの部門 ID が設定され、認証されたユーザの所属部門と一致するグループボックスのユーザ属性を変更することを許可している。
従って本機能要件は満たされる。

- **FMT_MSA.3[1]**

FMT_MSA.3[1]は、ボックスが生成される際に付与されるセキュリティ属性であるユーザ属性のデフォルト値などを規定している。
F.ADMIN は、管理者モードにおいて実施されるボックスの登録操作において、ボックスのユーザ属性に「共有」がデフォルト値として設定される。これをユーザは任意の値（登録されるユーザのユーザ ID、または部門 ID）に変更することを許可する。
F.BOX は、認証されたユーザが実施するボックスの登録操作において、ボックスのユーザ属性に「共有」がデフォルト値として設定される。これをユーザは任意の値（登録されるユーザのユーザ ID、または部門 ID）に変更することを許可する。
また未登録ボックスを指定したボックスへ保管するジョブが実行された場合は、当該ジョブを実行したユーザの「ユーザ ID」がデフォルト値として設定され、未登録ボックスを指定したボックスへ保管する。(未登録ボックス指定のケースは、デフォルト値を変更する初期値を設定するタイミングがない存在せず、ユーザ属性を変更することはできない。)
従って本機能要件は満たされる。

- **FMT_MSA.3[2]**

FMT_MSA.3[2]は、セキュリティ文書プリントファイルの登録時に設定されるセキュリティ文書内部制御 ID を規定している。
F.PRINT は、セキュリティ文書プリントファイルの登録時に、一意に識別されるセキュリティ文書内部制御 ID を当該セキュリティ文書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、ユーザパスワードの管理を規定している。
F.ADMIN は、ユーザ認証の方式に「本体認証」が選択されている場合、管理者モードにてユーザ登録に伴うユーザパスワードの登録操作を提供している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的ユーザパスワードを登録させることが可能である。

従って本機能要件は満たされる。

- **FMT_MTD.1[2]**

FMT_MTD.1[2]は、ユーザパスワードの管理を規定している。
F.ADMIN は、ユーザ認証の方式に「本体認証」が選択されている場合、管理者モードにて登録されたユーザパスワードの変更を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にユーザパスワードを改変させることが可能である。
F.USER は、ユーザ認証の方式に本体認証が選択されている場合、認証されたユーザに対して、ユーザ自身の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、ユーザ ID、SNMP パスワード、パネルオートログオフ時間、認証失敗回数閾値、外部サーバ認証設定データ、セキュリティ文書パスワード、部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データ、所属部門、管理者認証ロック時間の管理を規定している。
F.ADMIN は、管理者モードにて、SNMP パスワードの変更、パネルオートログオフ時間の変更、認証失敗回数閾値、外部サーバ認証設定データ、部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データ、所属部門、管理者認証ロック時間の変更操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にユーザ ID、SNMP パスワード、パネルオートログオフ時間、認証失敗回数閾値、セキュリティ文書パスワード、外部サーバ認証設定データ、部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データ、所属部門、管理者認証ロック時間を改変させることが可能である。
F.ADMIN-SNMP は、SNMP パスワードによって認証された管理者に SNMP 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[4]**

FMT_MTD.1[4]は、ボックスパスワードの管理を規定している。
F.ADMIN は、管理者モードにて共有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。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスパスワードを改変させることが可能である。
F.BOX は、共有ボックスの利用を許可されたユーザとして認証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[5]**

FMT_MTD.1[5]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の登録操作、すなわち共有ボックスに設定されるボックスパスワードの登録操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスパスワードを登録させることが可能である。
F.BOX は、認証されたユーザに対して、ボックスの登録操作、すなわち共有ボックスに設定され

るボックスパスワードの登録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[6]**
  FMT_MTD.1[6]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。CE 認証ロック時間はバックアップ/リストア操作にて結果的に変更操作が可能である。
  F.SERVICE は、サービス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[7]**
  FMT_MTD.1[7]は、SNMP パスワード、ユーザパスワード、ボックスパスワード、セキュリティ文書パスワード、部門パスワードの管理を規定している。
  F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータから、SNMP パスワード、ユーザパスワード、ボックスパスワード、セキュリティ文書パスワード、部門パスワードを閲覧することが可能である。
  従って本機能要件は満たされる。

- **FMT_MTD.1[8]**
  FMT_MTD.1[8]は、セキュリティ文書パスワードの管理を規定している。
  F.PRINT は、セキュリティ文書プリントファイルの登録に伴い、ユーザにセキュリティ文書パスワードの登録を許可している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[9]**
  FMT_MTD.1[9]は、CE パスワード、CE 認証ロック時間の管理を規定している。
  F.SERVICE は、サービスモードにて CE パスワード、CE 認証ロック時間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[10]**
  FMT_MTD.1[10]は、ユーザ ID の管理を規定している。
  F.ADMIN は、管理者モードにてユーザ ID の登録操作を許可する。
  F.USER はユーザ認証方式に「外部サーバ認証」が選択されている場合においてユーザ認証に成功したユーザが MFP 本体に登録されていない場合、認証されたユーザのユーザ ID を登録する。（外部サーバによって登録されることと同等。）
  従って本機能要件は満たされる。

- **FMT_MTD.1[11]**
  FMT_MTD.1[11]は、管理者パスワード及び SNMP パスワードの管理を規定している。
  F.ADMIN は、管理者モードにて全領域上書削除機能の実行に伴って実行される管理者パスワード及び SNMP パスワードの初期化操作を許可する。
  F.SERVICE は、サービスモードにてイニシャライズ機能の実行に伴って実行される管理者パスワード、SNMP パスワードの初期化操作を許可する。
  従って本機能要件は満たされる。

- **FMT_MTD.1[12]**

FMT_MTD.1[12]は、部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データの管理を規定している。
F.ADMIN は、管理者モードにて部門 ID、部門パスワード、S/MIME 証明書、送信宛先データ、高信頼チャネル機能設定データの登録操作を許可する。
従って本機能要件は満たされる。

- **FMT_MTD.1[13]**

FMT_MTD.1[13]は、所属部門の管理を規定している。
F.ADMIN は、管理者モードにてユーザに関連づけられる所属部門の登録設定操作を許可する。
F.USER は、部門認証によってその部門の利用を許可された利用者であると認証された場合に、その認証成功処理をもって所属部門が当該部門であると設定する。
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。

- ユーザ認証機能の動作設定機能
- 部門認証機能の動作設定機能
- 高信頼チャネル機能の動作設定（暗号方式設定等）
- S/MIME 機能の動作設定（暗号方式設定等）
- 認証失敗回数閾値の設定機能
- バックアップ、リストア機能
  結果的に以下に示す TSF データの問い合わせ機能に相当する。
  ・SNMP パスワード
  ・ユーザパスワード
  ・ボックスパスワード
  ・セキュリティ文書パスワード
  ・部門パスワード
  また以下に示す TSF データの改変機能に相当する。
  ・SNMP パスワード
  ・ユーザパスワード
  ・ボックスパスワード
  ・セキュリティ文書パスワード
  ・部門パスワード
  ・ユーザ ID
  ・ボックスのユーザ属性
  ・パネルオートログオフ時間
  ・セキュリティ強化機能の動作設定データ
  ・認証操作禁止機能の認証失敗回数閾値
  ・部門 ID
  ・S/MIME 証明書
  ・送信宛先データ
  ・高信頼チャネル機能設定データ
  ・所属部門
  ・CE 認証ロック時間
  ・管理者認証ロック時間
- セキュリティ強化機能の停止機能

・セキュリティ強化機能の動作設定機能
・HDD 論理フォーマット機能
- ボックスのユーザ属性の登録・変更機能
- 管理者パスワードの変更機能
- ボックスパスワードの登録・変更機能
- ユーザ ID の登録機能
- ユーザ認証「本体認証」時のユーザパスワードの登録・変更機能
- SNMP パスワード（Privacy パスワード、Authentication パスワード）の変更機能
- SNMP パスワード認証機能の動作設定機能
- パネルオートログオフ時間の設定機能
- 部門 ID、部門パスワードの登録・変更機能
- S/MIME 証明書の登録・変更機能
- 送信宛先データの登録・変更機能
- 高信頼チャネル機能設定データの登録・変更機能
- ユーザに関連づけられる所属部門の登録・変更機能
- 管理者認証ロック時間の変更機能
- ロック解除機能

以下の認証機能に対して提供する。
・MIB オブジェクトへのアクセスにおける認証機能
・共有ボックスへのアクセスにおける認証機能
・セキュリティ文書プリントへのアクセスにおける認証機能
・ユーザ認証機能
・部門認証機能

F.ADMIN-SNMP は、以下のセキュリティ管理機能を提供する。
- SNMP パスワード（Privacy パスワード、Authentication パスワード）の変更機能
- SNMP パスワード認証機能の動作設定機能

F.SERVICE は、以下のセキュリティ管理機能を提供する。
- CE パスワードの変更機能
- 管理者認証のロック解除機能
- CE 認証ロック時間の変更機能
- 管理者パスワードの変更機能
- 管理者パスワードの初期化機能
  ・イニシャライズ機能
- SNMP パスワード（Privacy パスワード、Authentication パスワード）の初期化機能
  ・イニシャライズ機能
- セキュリティ強化機能の停止機能
  ・HDD 論理フォーマット機能
  ・HDD 物理フォーマット機能
  ・HDD 装着設定機能
  ・イニシャライズ機能

F.USER は、以下のセキュリティ管理機能を提供する。
- ユーザ認証方式が本体認証の場合におけるユーザ自身のユーザパスワードの変更機能
- ユーザ認証方式が外部サーバ認証の場合における外部サーバによる MFP 未登録ユーザのユーザ ID 自動登録機能
- 部門認証方式が、連動方式にて所属部門が登録されていない場合における所属部門の登録機能

F.BOX は、以下のセキュリティ管理機能を提供する。
- ボックスのユーザ属性変更機能

・ユーザによる個人ボックスの変更（ユーザ ID ⇒ 共有 or 他のユーザ ID or 部門 ID）
・共有ボックスの利用を許可されたユーザによる共有ボックスの変更（共有 ⇒ ユーザ ID or 部門 ID）
・グループボックスの利用を許可されたユーザによるグループボックスの変更（部門 ID ⇒ 共有 or ユーザ ID or 他の部門 ID）

- ボックスのユーザ属性デフォルト値上書き機能
- ボックスパスワードの登録・変更機能
- ユーザによる未登録ボックスを指定したボックス保管ジョブによる個人ボックス自動登録

F.PRINT は、以下のセキュリティ管理機能を提供する。

- セキュリティ文書パスワードの登録機能

F.ADMIN により、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
  ・全領域上書き削除機能
- 管理者パスワードの初期化機能
  ・全領域上書き削除機能
- SNMP パスワード（Privacy パスワード、Authentication パスワード）の初期化機能
  ・全領域上書き削除機能

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、CE パスワ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。
F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication 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：ユーザを規定している。
F.USER は、ユーザパスワードにより認証された利用者をユーザとして認識する。
F.USER においてユーザと認識された利用者は、F.BOX、F.PRINT にも継承されて、同様にユーザとして認識される。
従って本機能要件は満たされる。

- **FMT_SMR.1[4]**

FMT_SMR.1[4]は、役割：その共有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共有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。

- **FMT_SMR.1[5]**

FMT_SMR.1[5]は、役割：外部サーバを規定している。
F.USER は、外部サーバ認証時に、ユーザ情報の問い合わせ先を外部サーバとして認識する。

従って本機能要件は満たされる。

- **FMT_SMR.1[6]**

  FMT_SMR.1[6]は、役割：その部門の利用を許可されたユーザを規定している。
  F.USER は、部門認証方式が連動方式である場合、ユーザ認証されると当該ユーザの所属部門より、その部門の利用を許可されたユーザとして認識する。部門認証方式が個別認証方式である場合、部門認証されるとその部門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.ADMIN-SNMP は、管理者だけが扱えるネットワーク設定機能など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.USER は、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“ユーザ認証機能”を必ず起動する。部門認証方式が個別認証方式である場合、または連動方式でも所属部門が登録されていないユーザのアクセスの場合、“部門認証機能”を必ず起動する。
  F.BOX は、共有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、セキュリティ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“セキュリティ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.ADMIN-SNMP は、SNMP パスワードより認証された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.USER は、認証された各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ユーザ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、共有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、許可されないサブジェクトによる干渉行為を許可しない。
  F.PRINT は、セキュリティ文書パスワードによる認証により、セキュリティ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セキュリティ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。
従って本機能要件は満たされる。

- **FTA_SSL.3**

FTA_SSL.3 は、パネルからアクセスする管理者に対するセッションの強制終了を規定している。
F.ADMIN は、パネルから管理者がアクセスしている場合に、最終操作からパネルオートログオフ時間が経過すると自動的にログオフして、管理者認証ドメインへのアクセスを拒否する。
F.USER は、パネルからユーザがアクセスしている場合に、最終操作からパネルオートログオフ時間が経過すると自動的にログオフして、ユーザ認証ドメインへのアクセスを拒否する。
従って本機能要件は満たされる。

- **FTP_ITC.1**

FTP_ITC.1 は、高信頼チャネルを規定している。
F.TRUSTED-PASS は、高信頼 IT 製品からの要求に応じて、SSL/TLS による高信頼チャネルを生成し、セキュリティ文書プリントファイル、ボックスファイル、ボックスファイルになる画像ファイルの通信データをセキュアに保護する。
従って本機能要件は満たされる。

- **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、指定された上書き削除方式に則り、HDD の全領域に対して上書き削除を行うことによって、ボックスファイル、セキュリティ文書プリントファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、ユーザ ID、ユーザパスワード、ボックスパスワード、セキュリティ文書パスワード、残存 TSF データ、部門 ID、部門パスワード、S/MIME 証明書を削除する。
また NVRAM の管理者パスワード、SNMP パスワードを初期化し、HDD ロック機能、暗号化機能の動作設定を OFF にする。さらに、高信頼チャネル機能設定データを消去する。
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。
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 が提供する管理者認証メカニズム
② F.SERVICE が提供する CE 認証メカニズム
③ F.PRINT が提供するセキュリティ文書認証メカニズム
④ F.BOX が提供するボックス認証メカニズム
⑤ F.ADMIN-SNMP が提供する SNMP 認証メカニズム

⑥ F.USER が提供するユーザ認証メカニズム
⑦ F.ADMIN が提供する HDD ロックパスワード照合メカニズム
⑧ F.ADMIN が提供する暗号化ワード照合メカニズム
⑨ F.USER が提供する部門認証メカニズム

①、②は 8 桁 92 種のキャラクタ、③は 8 桁 93 種のキャラクタ、⑤、⑥は 8 桁以上 95 種のキャラクタ、④、⑨は 8 桁 95 種のキャラクタ、⑦、⑧は 20 桁 83 種のキャラクタから構成されるパスワードを利用する。このうち①～⑥、⑨は、認証操作禁止機能の動作によって、最大でも連続 3 回の不成功認証により認証機能はロックする。

なお①、④、⑥については、ネットワークからのアクセスにおいてセッション情報を秘密に利用する。これら秘密は 10^{10} 以上の値を TOE が生成して利用する。また外部より与えられた 10^{10} 以上の値のセッション情報を利用する。

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。

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。