#4036 Multi Function Peripheral
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：1.07

発行日：2004年8月5日

作成者：ｺﾆｶﾐﾉﾙﾀﾋﾞｼﾞﾈｽﾃｸﾉﾛｼﾞｰｽﾞ株式会社

＜更新履歴＞

日付	バージョン	承認者	確認者	作成者	担当部署	更新内容
2004/02/27	1.00	廣田	後藤	中山	制御第12開発部	初版
2004/03/30	1.01	廣田	後藤	中山	制御第12開発部	誤植修正など
2004/04/02	1.02	廣田	後藤	中山	制御第12開発部	修正。
2004/04/14	1.03	廣田	後藤	中山	制御第12開発部	所見報告書（ASE001-01～ASE007-01）に対する修正
2004/05/14	1.04	廣田	後藤	中山	制御第12開発部	所見報告書（ASE008-01～ASE013-01）に対する修正
2004/06/25	1.05	廣田	後藤	中山	制御第12開発部	所見報告書（ASE014-01～ASE017-01）に対する修正
2004/08/03	1.06	廣田	後藤	山田	制御第12開発部	所見報告書（ASE018-01～ASE019-01）に対する修正
2004/08/05	1.07	廣田	後藤	中山	制御第12開発部	所見報告書（ASE020-01）に対する修正

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

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

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

1. ST 概説

1.1. ST 識別

・ST名称　：　#4036 Multi Function Peripheral[1] 全体制御ソフトウェア
　　セキュリティターゲット
・STバージョン　：　1.07
・CCバージョン　：　2.1
・作成日　：　2004年8月5日
・作成者　：　コニカミノルタビジネステクノロジーズ株式会社

1.2. TOE 識別

・TOE名称　：　日本名：#4036 Multi Function Peripheral 全体制御ソフトウェア
　　英名　：#4036 Multi Function Peripheral Control Software
・TOEバージョン　：　※ TOEは以下の2つのソフトウェアコンポーネント「Macro System Controller」、「Network Module」から構成され、それぞれにバージョンが存在する。
- Macro System Controller　：　4036-10G0-18-00
- Network Module　：　4036-A0G0-04-00

・TOEの種別　：　ソフトウェア
・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

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適合。

- **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。

[1] #4036 Multi Function Peripheral は、販売商品名「bizhub C350」、「CF2203」、「8022」として消費者に提供される Multi Function Peripheral ある。

- **参考資料**
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 2.1 August 1999 CIMB-99-031
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements Version2.1 August 1999 CCIMB-99-033
  - CCIMB Interpretations-0210
  - 情報技術セキュリティ評価のためのコモンクライテリア パート1：概説と一般モデル 1999年8月 バージョン2.1 CCIMB-99-031（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）
  - 情報技術セキュリティ評価のためのコモンクライテリア パート2：セキュリティ機能要件 1999年8月 バージョン2.1 CCIMB-99-032（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）
  - 情報技術セキュリティ評価のためのコモンクライテリア パート3：セキュリティ保証要件 1999年8月 バージョン2.1 CCIMB-99-033（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）
  - 補足-0210

1.4. ST 概要

#4036 MFP Multi Function Peripheral（以下 MFP とする）とは、コピー、プリント、スキャンの各機能を選択､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。本 ST は、MFP に搭載される制御ソフトウェアの中で、MFP 本体操作パネルからの操作制御処理、ジョブのリソース管理、ジョブのシーケンス制御処理等を実施するソフトウェアコンポーネントである「Macro System Controller」及びクライアント PC からの操作制御処理を実施するソフトウェアコンポーネントである「Network Module」から構成される“ #4036 Multi Function Peripheral 全体制御ソフトウェア ”を評価対象（TOE）として、TOE によって実現されるセキュリティ機能について説明する。

MFP は、一般的なオフィス環境に設置され、ドキュメントのコピー、プリントアウト、スキャンなど、利用方法には様々な形態がある。取り扱われるドキュメントは、機密性の低いものから機密性が高く要求されるものまで幅広い。TOE のセキュリティ機能は、MFP における特定の機能の利用にあたり MFP に取り込まれる機密性の高いドキュメントデータの暴露に対する保護機能を提供する。特定の機能とは以下に示す機能である。

- **親展プリント機能**

  クライアント PC にてパスワードを設定し、MFP に送信して印刷待機状態にあるプリントデータに対して、MFP 本体操作パネルからパスワードを入力して一致した場合に当該プリントデータが印刷される機能。

- **ボックス機能**
  スキャンデータの一時格納領域として設定されるボックスへのアクセスを制御する機能。

- **メモリリコール OFF コピー機能**
  通常、コピーを実行して印刷後には再印刷可能な状態になる当該コピーデータを、印刷終了後自動的に削除する機能。

本 ST は、親展プリント機能、ボックス機能、及びメモリリコール OFF コピー機能において提供される TOE のセキュリティ機能の必要・十分性を記述したドキュメントである。

1.5. 用語

本節では、本 ST で特定の意味をもって使用する用語について解説する。

ジョブ
コピー機能、スキャン機能、プリント機能などの MFP における一連の機能の動作単位。

親展プリント
クライアント PC からの印刷する場合の 1 つの形態。クライアント PC 上のプリンタドライバでパスワードを設定して MFP にプリントデータを送信すると、MFP では印刷が実行されずに待機状態になる。設定したパスワードを MFP に入力すると待機状態が解除されて印刷が実行される。

親展プリントジョブ情報データ
親展プリントとして MFP が受信したプリントデータ。本 ST では保護資産として扱う。

ジョブ ID
親展プリントをはじめてとして MFP における一連のすべてのジョブに付与される管理番号。

ボックス
ハードディスク（HDD）を搭載時、スキャンしたイメージデータを MFP に保管する領域として設定されるディレクトリ。個々の利用者がクライアント PC からのみ名称及びパスワードを設定することが可能である。なお、“ Public ”で示されるボックスは、共同利用されるため、パスワードを設定することはできない。名称変更を行うこともできない。

ボックス識別子
ボックスに設定される名称。

ボックスデータ
ボックスに格納されたイメージデータ。本 ST では保護資産として扱う。

ボックスパスワード

個々のボックスに設定されるパスワード。95 種の ASCII コードが設定可能である。

ボックスユーティリティ

クライアント PC からボックスにアクセスするための専用アプリケーション。本アプリケーションを利用してプレビュー表示、管理者操作によるボックス内データのバックアップ及びリストア操作などが行える。

メモリリコールコピー／メモリリコール OFF コピー

通常、コピーを実行して印刷終了後には再印刷可能な状態になるコピー機能をメモリリコールコピーと呼称する。これに対して、コピーを実行すると、印刷終了後に取り込まれたドキュメントのイメージデータを自動的に削除する機能をメモリリコール OFF コピーと呼称している。

コピージョブ情報データファイル

コピー機能の利用において MFP にスキャンされ取り込まれたイメージデータ。本 ST ではメモリリコール OFF が設定されたコピージョブ情報データを保護資産として扱う。

メモリリコール設定データ

メモリリコールコピーの動作有無を決定するデータ。管理者が設定する。本データを OFF にすると、利用者に提供されるメモリリコール ON コピー／メモリリコール OFF コピーの選択機能が一般ユーザに提供されなくなる。コピーを実行すると、印刷終了後に取り込まれたドキュメントのイメージデータを自動的に削除するメモリリコール OFF コピーとしてコピー機能が動作する。

SMTP サーバ設定データファイル

ボックスデータを E-mail 送信するために必要な MFP 利用環境に設置される SMTP サーバに関する設定情報のデータファイル。MFP に登録される必要があり、ボックスデータを保護するための二次的な資産である。

FTP サーバ設定データファイル

ボックスデータを FTP サーバへ送信するために必要な MFP 利用環境に設置される FTP サーバに関する設定情報のデータファイル。MFP に登録される必要があり、ボックスデータを保護するための二次的な資産である。

管理者モード

認証された管理者にのみ提供される機能群。

管理者モードパスワード

管理者モードに設定されるパスワード。8 桁の数字が設定可能である。

サービスモード

認証されたサービスエンジニアにのみ提供される機能群。

サービスコード

サービスモードに設定されるパスワード。8 桁の数字、“ ＊ ”、“ ＃ ” が設定可能である。

不正使用防止機能

管理者に動作設定管理される機能。本機能が有効になると、ボックス認証機能が動作し、更に管理者機能、親展プリント機能、ボックス機能における各認証機能にて、連続した各不成功認証試行を検出し、不成功認証回数に応じて各認証機能をロックする機能が動作する。

ボックス不正アクセス検出カウント値

不正使用防止機能が動作中にボックスの認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。

親展プリント不正アクセス検出カウント値

不正使用防止機能が動作中に親展プリントの認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。

管理者モード不正アクセス検出カウント値

不正使用防止機能が動作中に管理者の認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。

サービスエンジニア不正アクセス検出カウント値

サービスエンジニアの認証機能において認証試行に失敗した場合、不成功試行回数としてカウントされ保持される値。なお、他の不正アクセス検出カウント値とは異なり、不正使用防止機能の動作設定に依存しない。

アクセス不可状態解除機能

ボックス不正アクセス検出カウント値、親展プリント不正アクセス検出カウント値を 0 クリアする機能。ボックス、親展プリントに対する認証機能がロックした場合、本機能を実行することにより、ロックが解除される。

HDD ロック機能

MFP にて利用される HDD に実装されているセキュリティ機能。HDD にアクセスするためのパスワード（HDD ロックパスワード）が設定可能であり、本機能を使用すると、アクセスする際に HDD ロックパスワードを利用した認証機能が動作する。HDD が設置された MFP であることが認証されない限りアクセスすることはできない。また一定回数の不成功試行が検出されると、それ以降の認証機能をロックし、一切のアクセスを遮断する。

オートリセット機能

設定される一定時間、無操作であることを検出すると、MFP 本体操作パネルからのアクセスであれば、電源を起動した際の基本画面に戻る機能。クライアント PC から管理者モードへのアクセスであれば、接続を遮断する。

オートリセット動作設定データ

オートリセット機能動作を決定する設定可能な時間データ。“ 期限なし ”から、1 分単位で 1～9 分が設定可能。クライアント PC からアクセスする管理者モードに対しては、表 1 の対応表にて示される時間で動作する。

2. TOE 記述

2.1. TOE の種別

TOE である#4036 MFP 全体制御ソフトウェアは、MFP に搭載される#4036 MFP 制御ソフトウェアの一部分を構成するソフトウェア製品であり、具体的にはMFP本体操作パネルからの操作制御、ジョブのリソース管理、ジョブのシーケンス制御等を実施する「Macro System Controller」及びクライアント PC からの操作制御を実施する「Network Module」より構成される。

2.2. MFP の利用環境

想定される一般的な利用環境を図 1 に示す。

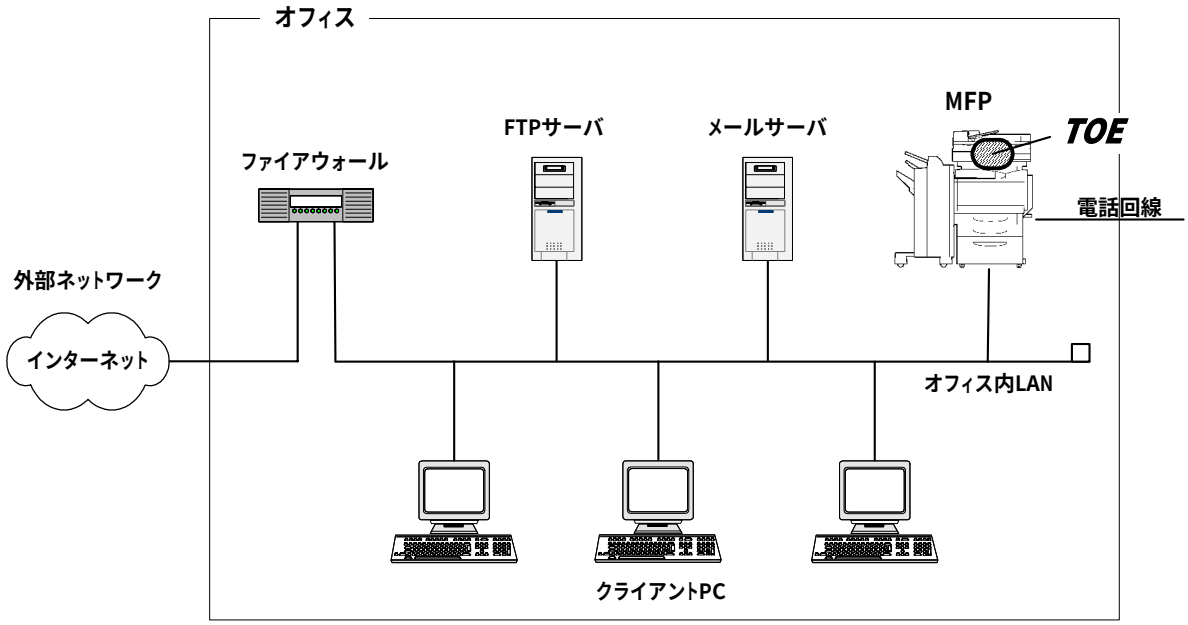

図 1 MFP の利用環境の例

上図に示されるように、MFP は一般的なオフィスに設置される。オフィスは、MFP の利用・運用・保守に関わる者だけが入室することか可能な運用管理体制が敷かれる。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 と接続し、相互にデータ通信を行う。オフィス内 LAN にメールサーバ、FTP サーバが接続される場合は、MFP はこれらを利用してデータ通信を行うことも可能である[2]。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 に対するアクセス要求を遮断するための適切な設定が行われる。またオフィス内 LAN は、スイッチ

[2] ＜補足：メールサーバ、FTP サーバについて＞
MFP を導入するオフィス環境は、メールサーバ、FTP サーバが設置されない場合も想定される。また外部ネットワークへ接続されない場合や電話回線が接続されない場合も想定される。このような場合は、E-mail、FTP などに関係する機能が利用できなくなる。

ングハブ等の利用、オフィスの運用により、MFP とクライアント PC の間の通信データが盗聴されないネットワーク環境が整備されている。MFP に接続される電話回線は、MFP の保守管理を行うサポートセンターとの通信に利用される。

2.3. TOE の利用に関連する者

TOE の利用に関連する利用者の役割を以下に定義する。

- **一般ユーザ**
  MFP が設置されるオフィス内に入室することが可能な、MFP を利用する組織の者。2.5.1 項において記述される一般ユーザ機能を使用することができる。

- **管理者**
  MFP が設置されるオフィス内に入室することが可能な、MFP を利用する組織の者で、且つ MFP の運用管理を行う者。管理者は一般ユーザとして 2.5.1 項において詳細が記述される一般ユーザ機能を使用することができる他、2.5.2 項において記述される管理者機能を使用することができる。

- **サービスエンジニア**
  MFP が設置されるオフィス内に入室することが可能であり、MFP の保守管理を行う者。MFP の印刷エンジン等のマシンメンテナンス（物理的な保守）を行う他、各設定値等を調整するための保守管理機能として提供されるサービスエンジニア機能（2.5.3 項参照）を使用することができる。組織内の人物ではないため、MFP の運用に関わることはない。これら保守作業は管理者の監視の下で実施されるため、不正行為を行うことはない。

- **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。

2.4. TOE の動作環境

2.4.1. TOE のハードウェア環境

TOE のハードウェア環境構成を図 2 に示す。TOE は MFP 制御コントローラの MFP 制御ソフトウェアの中に含まれる。MFP 制御コントローラは、MFP 本体ハードウェアに据え付けられる。MFP 本体ハードウェアには、操作パネルの他に、ネットワークユニットが標準搭載されている。更に MFP 本体ハードウェアには、データコントローラ（遠隔診断機能に必要なハードウェア、後述の 2.5.4 項参照）、HDD ロック機能を有する HDD などが搭載される。

HDD ロック機能とは、HDD 内のデータにアクセスする際、設定するパスワード（HDD ロックパスワード）が必要となる機能である。また HDD ロックパスワードの照合にて不成功試行を検出し、一定回数の不成功試行検出以降、照合機能をロックする機能も持つ。よって HDD が盗難された場合でも不当なアクセスから保護され、機密性が保たれる。

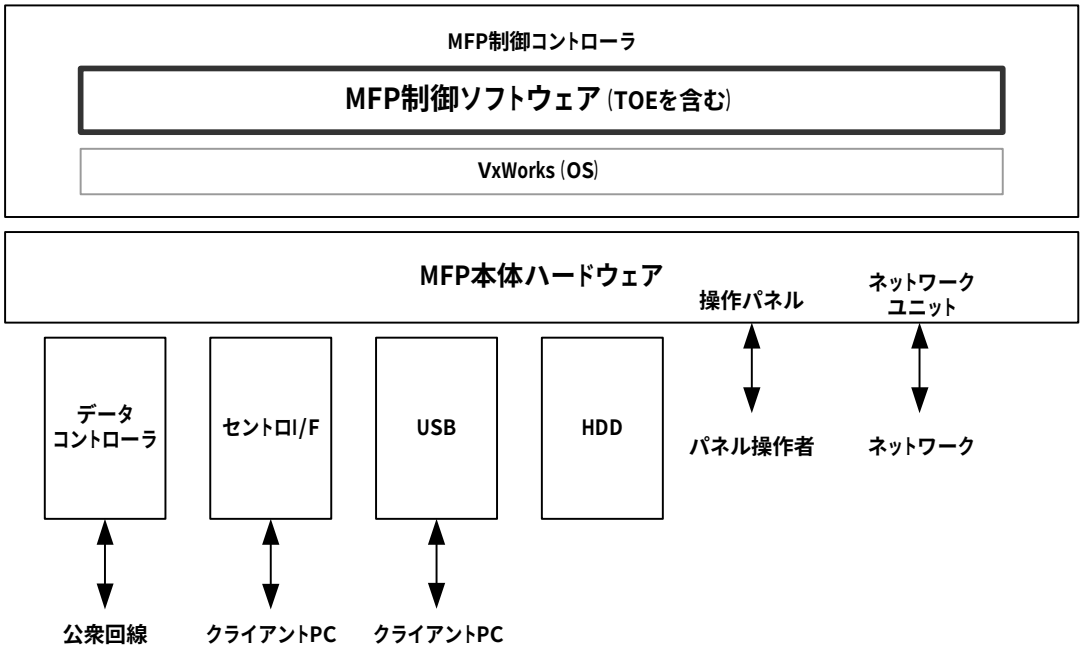

図 2 TOE のハードウェア構成

2.4.2. TOE のソフトウェア環境

TOE である「Macro System Controller」及び「Network Module」は、その他の MFP 制御ソフトウェアコンポーネントと一体となって MFP 本体内部の MFP 制御コントローラで稼動する OS（VxWorks）上で動作する。この MFP 制御ソフトウェアコンポーネントの構成図を図 3 に示す。TOE の物理的領域は、同図にて濃色で示される範囲である。

以下、TOE を始めとして各ソフトウェアコンポーネントが担う動作概要について説明する。

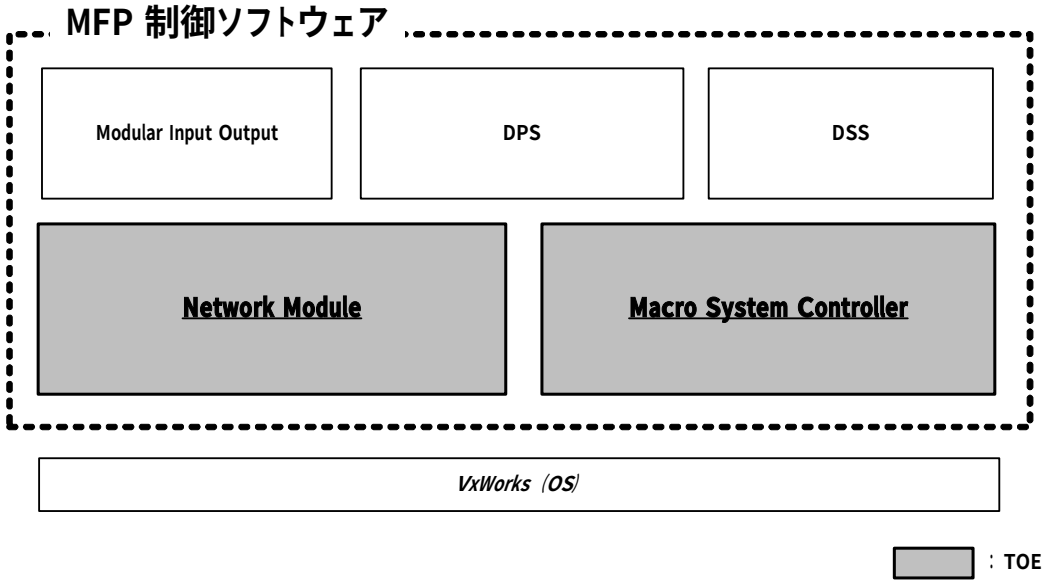

図 3　MFP 制御ソフトウェアの構成と TOE の関係

- *VxWorks（OS）*
  MFP 制御ソフトウェアが動作するために必要な根幹ソフト。オペレーティングシステム。MFP において、ネットワーク機能、ファイルシステム機能、マルチプロセシング処理等のサービスを提供する。

- **Macro System Controller（MSC）**
  TOE。取り込んだイメージデータをジョブとして登録し、ジョブのリソース、起動、シーケンスを管理するモジュール。MFP 本体操作パネルにおける LCD、LED、キー等の入力情報を処理し、処理に応じて他のソフトウェアコンポーネントに通知する。他のソフトウェアコンポーネントからのメッセージを処理してその他のソフトウェアコンポーネントへ通知する、または MFP 本体操作パネルに表示する。

- Modular Input Output（MIO）
  各種の外部インタフェース（ネットワークユニット、セントロ I/F）から受け付けたデータを「DPS」、「DSS」、「Network Module」、「Macro System Controller」で扱うデータに変換するソフトウェアコンポーネント。WWW サーバ機能を実現する。また IP アドレス等ネットワークの諸設定処理を実施する。

- **Network Module（NM）**
  TOE。クライアント PC からの操作要求に対し、「Modular Input Output」からデータを受け付け、処理・制御するソフトウェアコンポーネント。処理に応じて「VxWorks」、または「Macro System Controller」に処理を依頼する。また「VxWorks」、「Macro System Controller」にて処理されたデータを受け付け、「Modular Input Output」に処理を依頼する。

- DPS
  クライアント PC からのプリント受け付け処理を実施するアプリケーションソフトウェアコンポーネント。

- DSS
  スキャンよって取り込まれた画像を E-mail 送信、FTP 送信等の処理を実施するアプリケーションソフトウェアコンポーネント。

よって TOE である「Macro System Controller」及び「Network Module」は、その他の MFP 制御ソフトウェアコンポーネント及び OS と以下の図に示される関係を持つ。同図にて示される TOE の提供する機能内容については次節にて説明する。

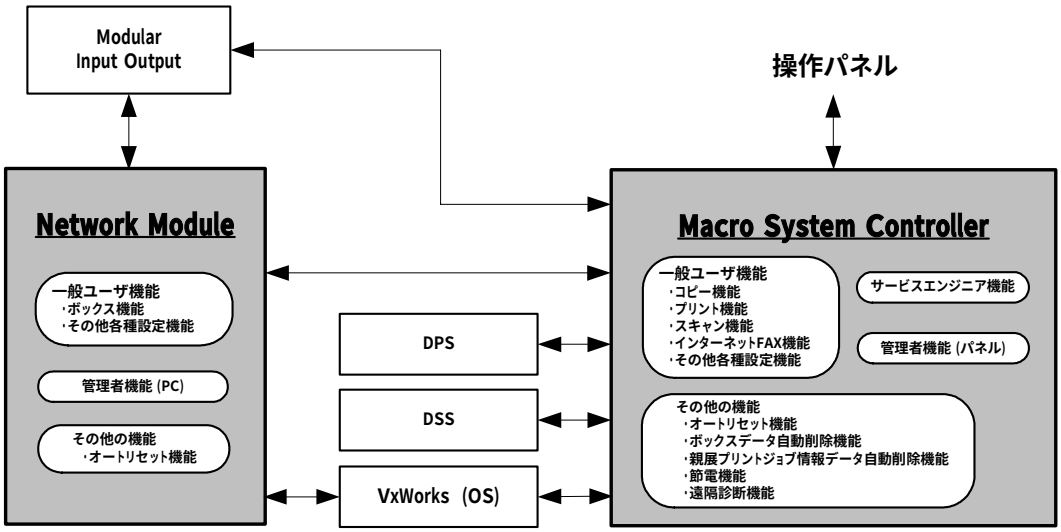

図 4 TOE 動作処理と関係する MFP 制御ソフトウェアコンポーネント

2.5. TOE の提供する機能

一般ユーザ及び管理者は、クライアント PC 及び MFP 本体操作パネルから TOE の搭載される MFP の各種機能を使用する。サービスエンジニアは、MFP 本体操作パネルよりサービスエンジニア向けの機能を使用することができる。以下、一般ユーザ及び管理者が操作する**一般ユーザ機能**、管理者だけが操作することが可能な管理者モードにおける諸機能（**管理者機能（パネル）、管理機能（PC）**）、サービスエンジニア向けの諸機能（**サービスエンジニア機能**）について説明する。

2.5.1. 一般ユーザ機能

(1) コピー機能

MFP 本体操作パネルより、ドキュメントのスキャンを実行すると揮発性メモリにイメージデータを取り込んだ後、イメージデータを印刷する機能。

① メモリリコールコピー
コピーを実行すると、印刷終了後にコピージョブ情報データが印刷可能なジョブとして残り、何度でも再印刷することが可能なコピー機能。

② メモリリコール OFF コピー
コピーを実行すると、印刷終了後にコピージョブ情報データが自動的に削除されるコピー機能。利用者が自動削除を指定して実施される場合と、利用者に設定を委ねず、管理者の設定に基づき自動削除が実施される場合が存在する。

③ 画像蓄積コピー
コピー実行時に画像蓄積を行うことを選択の上でコピーを実行すると、印刷待機状態となるコピー機能。ジョブバインド機能（後述）にて他のジョブと組み合わせて印刷する等の場合にて、本機能は利用される。なお、印刷待機状態となった本ジョブに対する印刷実行操作に対して特にアクセスの制限は設けていない。

(2) プリント機能

クライアント PC のプリンタドライバを使用して、MFP にプリントデータを送信すると、MFP は揮発性メモリに受信したプリントデータを印刷する。プリント機能には、以下に示すプリント方法がある。

① 通常プリント
MFP のメモリに受信したプリントデータをそのまま印刷するプリント機能。

② リプリント
クライアント PC 上で、「リプリント」を指定した場合、プリントデータの印刷を終了後もプリントデータをメモリに蓄積し、再印刷、または印刷仕上げ等の諸設定等を変更した上で何度でも印刷することができるプリント機能。印刷実行操作において特にアクセスの制限は設けていない。

③ 親展プリント
機密性の高いドキュメント等を印刷する場合、クライアント PC のプリンタドライバで「親展」を指定し、パスワードを設定した上で、MFP にプリントデータを送信する。TOE でこのプリントデータを受信すると、親展プリントジョブ情報データとして登録し、印刷待機状態になる。TOE は、MFP 本体操作パネルから入力されるパスワードと親展プリントジョブ情報データのパスワードを照合し、これが一致した場合に待機状態が解除され、印刷が実行される。印刷の終了した親展プリントジョブ情報データは、自動的に削除される。

④ HDD ストアプリント
MFP の HDD にプリントジョブ情報データを保管する機能。MFP 本体操作パネルからの操

作で印刷することができる。印刷実行操作において特にアクセスの制限は設けていない。

(3) **ジョブバインド機能**

メモリリコールされたコピーやリプリント等で印刷待機状態にあるジョブを選択し、順序を設定して 1 つのジョブとして印刷する機能。TOE は、このジョブバインド機能においてジョブの選択、印刷実行の受付処理を行う。

(4) **スキャン機能**

MFP 本体操作パネルからスキャンを実行してイメージをデータとして取り込む機能。スキャンにより揮発性メモリに格納されたイメージデータは、E-mail、FTP などのデータ送信方法があり、スキャンと連動して利用される。またスキャンデータを MFP 外に送信せず、MFP に内蔵される HDD のボックスに保管することも可能である。

(5) インターネット FAX 機能

インターネット FAX（添付される画像形式が規定された E-mail）を受信し、印刷する機能。またスキャン機能によって MFP に取り込んだイメージデータをインターネット FAX として規定される画像圧縮形式の添付ファイルにして E-mail 送信する機能。

(6) **ボックス機能**

クライアント PC よりブラウザを用いて、スキャンされたイメージデータの保管領域であるボックスを HDD に作成（名称、パスワードの新規設定）し、イメージデータ（以降、ボックスデータとする）の格納されたボックス※に対してクライアント PC よりブラウザを用いて以下に示す操作が提供される。

・ボックスデータのクライアント PC へのダウンロード
・ボックスデータの削除
・ボックスの削除
・ボックスの設定変更（名称の変更、パスワードの変更）

※ ボックスには、デフォルトで“Public”と名称が設定されている一般ユーザが共用する保管領域がある。このボックスに対して、パスワード設定、名称変更、ボックス削除等の操作は行えない。

また MFP 本体操作パネルよりボックスに格納されたスキャンデータに対して以下に示す操作が提供される。

・ ボックスデータのクライアント PC への E-mail 送信
・ ボックスデータのクライアント PC への FTP 送信
・ ボックスデータの名称変更
・ ボックスデータの削除

その他、クライアント PC より専用のアプリケーション（ボックスユーティリティ）を用いてボックスに対して以下の操作が提供される。

・ ボックスデータのプレビュー表示
・ ボックスデータの一覧表示（サムネイル付一覧表示）
・ ボックスデータのクライアント PC へのダウンロード
・ ボックスデータの名称変更
・ ボックスデータの削除

(7) **その他各種設定機能**

上記(1)～(6)の機能以外に一般ユーザが扱える機能として、MFP 本体操作パネルからは、印刷における用紙選択、画質選択、倍率等の各種設定を行う複数の機能が存在する。またクライアント PC よりブラウザを利用して操作することができる機能に、MFP のシステム状態（デバイス構成、概要）の閲覧、ジョブ状況の閲覧、スキャン機能における送信方法、宛先の設定等を行う複数の機能が存在する。

2.5.2. 管理者機能

TOE は、管理者だけが操作することが可能な管理者モードにて一般ユーザ機能を管理する管理機能（管理者機能）を提供する。以下、MFP 本体操作パネルから実施可能な管理機能である管理者機能（パネル）、クライアント PC から実施可能な管理機能である管理者機能（PC）について説明する。またクライアント PC より専用アプリケーションであるボックスユーティリティを用いて利用可能な管理機能である管理者機能（ボックスユーティリティ）についても説明する。

(1) **パネル管理者機能**

・管理者モードパスワードの変更機能
・不正使用防止動作設定機能
・アクセス不可状態解除機能（親展プリント、ボックスに対する各不正アクセス検出カウント値を 0 クリアする機能）
・オートリセット機能（後述の 2.5.4 項参照）の動作設定機能
・HDD ロック動作設定機能
・SMTP サーバ、FTP サーバの設定機能
・メモリリコール設定データの設定機能
・管理者向け各種設定機能（親展プリントジョブ情報データの保管期間設定、ネットワークの諸設定、コピー枚数制限の設定、日付時刻の設定など）

(2) PC **管理者機能**

・ボックスデータの削除
・ボックスの削除
・ボックスの設定変更（名称の変更、パスワードの変更）
・オートリセット機能の動作設定
・SMTP サーバ、FTP サーバの設定機能
・メモリリコール設定データの設定機能

・管理者向け各種設定機能（ボックスデータの保管期間設定、親展プリントジョブ情報データの保管期間設定、ネットワークの諸設定、コピー枚数制限の設定、日付時刻の設定など）

(3) **ボックスユーティリティ管理者機能**

・ボックスデータのバックアップ機能

・バックアップされたボックスデータのリストア機能

2.5.3. サービスエンジニア機能

TOE は、MFP 本体操作パネルから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一般ユーザ機能や管理者機能に対する管理機能（サービスエンジニア機能）を提供する。以下、本機能について説明する。

・ROM バージョン表示機能

・管理者モードパスワードの初期化機能

・サービスコードの変更機能

・サービスエンジニア向け各種設定機能（一般ユーザに提供される各設定機能に対する動作設定機能、印刷枚数のカウンタ設定、各機能動作確認、センサチェック、HDD 装着設定、HDD フォーマット等）

2.5.4. その他の機能

一般ユーザ、管理者、及びサービスエンジニアが直接操作することによって動作する機能以外に、各利用者の設定に応じて TOE が自発的に動作する機能が存在する。以下にこの種の代表的な機能を説明する。

(1) オートリセット機能

無操作が継続し、設定された時間を経過すると、自動的に基本画面にリセットされる機能。MFP 本体操作パネルからのアクセス、クライアント PC からの管理者モードへのアクセス中において発動する。発動までの時間（オートリセット設定データ）は、管理者が設定する。（2.5.2 項参照）

(2) ボックスデータ自動削除機能

設定された保管期間を経過したボックスデータを削除する機能。保管期間の設定は、管理者が設定する。（2.5.2 項参照）

(3) 親展プリント自動削除機能

設定された保管時間を経過した親展プリントジョブ情報データを削除する機能。保管時間の設定は、管理者が設定する。（2.5.2 項参照）

(4) パワーセーブ機能

無操作が継続し、設定された時間を経過すると、自動的に印刷エンジン定着部のヒータの温度を調節し、電力消費を抑える以下の機能。本機能が作動すると、印刷待機状態で登録されているジョブは削除される。一般ユーザが本機能の作動開始までの時間を設定する。
・プレヒート機能：印刷エンジン定着部のヒータ温度を低下させる。
・スリープ機能　：印刷エンジン定着部のヒータを消す。

(5) 遠隔診断機能
サポートセンターからのアクセス要求を受け付け、MFP のトラブル発生回数、消耗品の消耗具合を示す値、印刷カウンタ値などの情報をサポートセンターに送信する。また MFP に特定の故障（重大な故障）が発生すると、自動的にサポートセンターへアクセスし、MFP の故障情報を送信する。本機能におけるデータの送受信は、電話回線や E-mail が利用される。

2.6. TOE の提供するセキュリティ機能の詳細

本節は、前節にて述べられた TOE の機能の中で、特に保護対象とする資産（コピージョブ情報データ、親展プリントジョブ情報データ、ボックスデータ）に関係する機能について説明する。

2.6.1. 一般ユーザ機能におけるセキュリティ機能

一般ユーザ機能における以下の機能は、ドキュメントデータの暴露を防止するセキュリティを考慮した機能である。以下に詳細を説明する。

- **メモリリコール OFF 設定による残存コピーデータ保護機能**
  管理者機能にてメモリリコールコピーをしないにした場合、コピー機能の利用にて取り込まれたコピージョブ情報データを印刷終了後、自動的に削除する機能。

- **親展プリントジョブに対する一般ユーザのアクセスを許可する識別認証**
  親展プリントジョブ情報データを印刷する際、当該親展プリントジョブ情報データの正当な利用者である一般ユーザであることを識別認証する機能。認証に 3 回失敗すると、当該親展プリントジョブ情報データに対する認証機能はロックし、アクセスできなくなる。
  認証に成功すると、当該親展プリントジョブ情報データの印刷が開始される。

- **ボックスの作成機能**
  一般ユーザが、名称を指定し、ボックスを作成する機能。

- **ボックスに対する一般ユーザのアクセスを許可する識別認証・アクセス制御機能**
  ボックスにアクセスする際、当該ボックスの正当な利用者である一般ユーザであることを識別認証する機能。認証に 3 回失敗すると、当該ボックスに対する認証機能はロックし、アクセスできなくなる。

認証に成功すると、ボックス内のすべてボックスデータのダウンロードが許可される。(なお、“Public”で示されるボックスは、本セキュリティ機能の対象範囲外である。)

- **アクセスを許可された一般ユーザのボックス管理機能**
  ボックスの正当な利用者である一般ユーザが、当該ボックスの設定（名称、パスワード）を変更する機能。

なお、親展プリントジョブ情報データ、ボックスデータの削除に関係する機能は、以下の理由から脅威が想定されないためセキュリティ機能として考慮しない。

・長期間保管することを目的としていない。
・任意に削除されることによりデータの可用性が落ちるが、原本となるデータや印刷物は各利用者によって管理、保存されているため、これを考慮する必要がない。

2.6.2. 管理者機能におけるセキュリティ機能

管理者機能の中には、保護対象とする資産と関係する管理機能が存在する。これら管理機能を含む管理者機能に対するアクセスは、管理者だけが知り得るパスワードである管理者モードパスワードにより認証された者だけにアクセスが制限されている。この識別認証機能及び認証後に操作可能な保護対象とする資産に関係する管理機能は、セキュリティ機能であり、以下に詳細を説明する。

- **管理者モードに対するアクセスを許可する識別認証機能**
  - MFP 本体操作パネル、またはクライアント PC よりブラウザを用いて管理者モードにアクセスする際、管理者であることを識別認証する機能。認証に 3 回失敗すると、管理者の認証機能はロックし、アクセスすることができなくなる。
  - クライアント PC よりボックスユーティリティを利用してボックスデータのバックアップ機能、リストア機能を実行する際、管理者であることを認証する機能。上記同様、認証に 3 回失敗すると、管理者の認証機能はロックし、アクセスすることができなくなる。

- **管理者モードにおけるセキュリティ関連機能**
  MFP 本体操作パネルから管理者モードにおいて操作することができる以下の機能。
  - 管理者モードパスワードの変更機能
  - 不正使用防止動作設定機能
  - アクセス不可状態解除機能
  - オートリセット機能の動作設定機能
  - SMTP サーバ、FTP サーバの設定機能
  - メモリリコール設定データの設定機能

  クライアント PC から管理者モードにおいて操作することができる以下の機能。
  - ボックスの設定変更機能（名称の変更、パスワードの変更）
  - オートリセット機能の動作設定機能
  - SMTP サーバ、FTP サーバの設定機能

・ メモリリコール設定データの設定機能

2.6.3. サービスエンジニア機能におけるセキュリティ機能

サービスエンジニア機能の中には、保護対象とする資産と関係する管理機能が存在する。これら管理機能を含むサービスモードに対するアクセスは、サービスエンジニアだけが知り得る公開されない秘密情報に加え、サービスエンジニアだけが知り得るパスワードであるサービスコードにより認証された者だけにアクセスが制限されている。この識別認証機能及び認証後に操作可能な保護対象とする資産に関係する管理機能は、セキュリティ機能であり、以下に詳細を説明する。

- **サービスモードへのアクセスを許可する識別認証機能**
  サービスモードにアクセスする際、サービスエンジニアであることを認証する機能。認証に 3 回失敗すると、当該認証機能はロックされ、アクセスすることができなくなる。

- **サービスエンジニア機能におけるセキュリティ関連機能**
  サービスモードにおいて操作することができる以下の機能。
  ・ 管理者モードパスワードの初期化機能
  ・ サービスコードの変更機能

2.6.4. その他の機能におけるセキュリティ機能

オートリセット機能は、無操作状態が継続した場合に MFP 本体パネル基本画面に戻る、またはクライアント PC からの接続であれば接続を遮断する。従って管理者モードへアクセスしている際に誤って離席してしまった場合の補助的なセキュリティ機能として有効である。以下に詳細を説明する。

- **オートリセット機能**
  設定される一定時間、無操作状態が継続した場合にアクセス許可を取り消す機能。本機能の作動時間は、以下の表に示される時間を管理者が設定する。

表 1 オートリセット機能の動作設定と挙動

アクセス状態 / 動作設定時間範囲	MFP 本体操作パネルからアクセスする管理者モードに対する動作	クライアント PC からアクセスする管理者モードに対する動作
動作 OFF	作動しない	10 分後作動
1、2、3、4、5 分	設定通り 1、2、3、4、5 分で作動	5 分固定で作動
6、7、8、9 分	設定通り 6、7、8、9 分で作動	設定通り 6、7、8、9 分で作動

3. TOE セキュリティ環境

本章では、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. 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ついて、悪意を持った行為は行わない。

A.AUTH（パスワードに関する運用条件）

TOE の利用において使用される各パスワードは、そのパスワードの所有者によって漏れることがないよう管理される。

A.HDD（MFP で利用されるハードウェア環境条件）

- TOE が搭載される MFP では、HDD ロック機能を有する HDD だけが利用される。
- HDD ロック機能に利用される HDD ロックパスワードは、その所有者によって漏れることがないよう管理される。

A.NETWORK（MFP のネットワーク接続条件）

- MFP を利用する組織は、TOE が搭載される MFP を設置するオフィス内 LAN において盗聴されないネットワーク環境を構成する。
- 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.PHYSICAL（MFP の設置条件）

TOE が搭載される MFP は、一般ユーザ、管理者、サービスエンジニアだけが入ることが可能な物理的に保護された場所に設置される。

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、TOE の設置及び MFP の保守において課せられた役割として許可される一連の作業について、悪意を持った行為は行わない。

A.SETTING（セキュリティ機能の動作設定条件）

TOE の利用者は、不正使用防止機能が必ず動作する状態で TOE を利用する。

3.2. 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.ACCESS-SECURE-PRINT（親展プリントジョブ情報データの不正な操作）

悪意をもった一般ユーザが、親展プリントジョブ情報データに MFP 本体操作パネルよりアクセスし、他の一般ユーザが送信した親展プリントジョブ情報データを印刷することにより、親展プリントジョブ情報データが不正に暴露される。

T.ACCESS-BOX（ボックスデータの不正な操作）

- 悪意を持った一般ユーザが、作成されたボックスにクライアント PC よりアクセスし、他の一般ユーザが利用するボックスのボックスデータをダウンロード、プレビュー、サムネイル表示することにより、ボックスデータが不正に暴露される。
- 悪意を持った一般ユーザが、作成されたボックスに MFP 本体操作パネルよりアクセスし、他の一般ユーザが利用するボックスのボックスデータを E-mail 送信、FTP 送信することにより、ボックスデータが不正に暴露される。
- 悪意を持った一般ユーザが、クライアント PC より作成されたボックスにアクセスし、ボックスデータをバックアップすることにより、ボックスデータが不正に暴露される。
- 悪意を持った一般ユーザが、クライアント PC よりバックアップされたボックスデータをリストアすることにより、ボックスデータが不正に改ざんされる。

T.ACCESS-COPY-DATA（残存するコピージョブ情報データに対する不正な操作）

悪意を持った一般ユーザが、MFP 本体操作パネルよりアクセスしてコピージョブ情報データを再印刷し、コピージョブ情報データが不正に暴露される。

T.SEND-BOX-DATA（ボックスデータの想定されない宛先への送信）

- 悪意を持った一般ユーザが、MFP 本体操作パネルよりアクセスして MFP が利用する SMTP サーバ、FTP サーバの各設定データを変更することにより、ボックスデータが一般ユーザの意図しないサーバに送信されてしまい、ボックスデータが暴露される。
- 悪意をもった一般ユーザが、クライアント PC よりアクセスして MFP が利用する SMTP サーバ、FTP サーバの各設定データを変更することにより、ボックスデータが一般ユーザの意図しないサーバに送信されてしまい、ボックスデータが暴露される。

3.3. 組織のセキュリティ方針

P.BEHAVIOR-FUNCTION（セキュリティ機能の動作設定機能）

- セキュアな環境では、操作上の便宜を図るために不正使用防止機能を停止することができる。
- セキュアな環境では、操作上の便宜を図るためにメモリリコールコピー機能を動作することができる。

4. セキュリティ対策方針

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

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.ACCESS-ADMIN（管理者が操作する管理機能）

TOE は、管理者だけに管理者機能の操作を実行することを許可する。

O.ACCESS-BOX（ボックスアクセス制御）

- TOE は、正当な利用者である一般ユーザだけに、ボックスデータのダウンロード、プレビュー、サムネイル表示、E-mail 送信、FTP 送信操作を行うことを許可する。
- TOE は、管理者だけにすべてのボックスのボックスデータのダウンロード操作（バックアップ操作）、アップロード操作（リストア操作）を行うことを許可する。

O.ACCESS-SECURE-PRINT（親展プリントジョブアクセス制御）

TOE は、正当な利用者である一般ユーザだけに、親展プリントジョブ情報データの印刷操作を許可する。

O.ACCESS-SERVICE（サービスエンジニアが操作する管理機能）

TOE は、サービスエンジニアだけにサービスエンジニア機能の操作を実行することを許可する。

O.CONTROL-COPY（コピー機能の動作制御）

TOE は、コピー機能の利用において取り込んだコピージョブ情報データを印刷終了後に削除する。

O.I&A-ADMIN（管理者の識別認証）

TOE は、利用者がクライアント PC、または MFP 本体操作パネルより管理者機能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。

O.I&A-SERVICE（サービスエンジニアの識別認証）

TOE は、MFP 本体操作パネルよりサービスエンジニア機能に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。

O.I&A-USER（一般ユーザの識別認証）

TOE は、親展プリントジョブ情報データまたはボックスデータにアクセスする利用者が正当な利用者である一般ユーザであることを識別認証する。

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.FEED-BACK（パスワードのフィードバック）

クライアント PC に利用されるボックスユーティリティは、入力されるボックスパスワード、または管理者モードパスワードに対して保護された適切なフィードバックを提供する。

OE.SECURE-PRINT-QUALITY（親展プリントパスワードの品質尺度）

クライアント PC のプリンタドライバは、親展プリントとして MFP に送信されるプリントデータに対して強度の保証されたパスワードを付加する。

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.AUTH（パスワードの適切な管理、使用法）

- 管理者は、一般ユーザに対して以下に示す運用を実施させる。
  - ・ 一般ユーザは、親展プリントパスワード、ボックスパスワードを秘匿する。
  - ・ 一般ユーザは、親展プリントパスワード、ボックスパスワードに推測可能なものを設定しない。
  - ・ 一般ユーザは、ボックスパスワードの適宜変更を行う。
- MFP を利用する組織の責任者は、管理者に対して以下に示す運用を実施させる。
  - ・ 管理者は、管理者モードパスワードに推測可能なものを設定しない。
  - ・ 管理者は、管理者モードパスワードを秘匿する。
  - ・ 管理者は、管理者モードパスワードの適宜変更を行う。
  - ・ 管理者は、管理者モードパスワードが初期化された際に必ず変更操作を行う。
- MFP を保守管理する組織の責任者は、サービスエンジニアに対して以下に示す運用を実施させる。
  - ・ サービスエンジニアは、サービスコードに推測可能なものを設定しない。
  - ・ サービスエンジニアは、サービスコードを秘匿する。
  - ・ サービスエンジニアは、サービスコードの適宜変更を行う。

OE-N.HDD（MFP で利用される HDD）

- サービスエンジニアは、TOE が搭載される MFP には HDD ロック機能を有する HDD を設置する。
- MFP を利用する組織の責任者は、管理者に対して以下に示す運用を実施させる。
  - ・ 管理者は、HDD ロックパスワードに推測可能なものを設定しない。
  - ・ 管理者は、HDD ロックパスワードを秘匿する。
  - ・ 管理者は、HDD ロックパスワードの適宜変更を行う。

OE-N.NETWORK（MFP の接続するネットワーク環境）

- 管理者は、TOE が搭載される MFP を設置するオフィス LAN において盗聴されないネットワーク環境を実現する機器を設置し、盗聴されないための適切な設定を実施する。
- 管理者は、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の機器を設置し、アクセスを遮断するための適切な設定を実施する。

OE-N.PHYSICAL（MFP の設置環境）

管理者は、物理的に保護されたオフィスに TOE が搭載される MFP を設置し、一般ユーザ、管理者、及びサービスエンジニアだけがそのオフィスに入ることが可能な運用管理を実施する。

OE-N.SERVICE（信頼できるサービスエンジニア）

MFP を保守管理する組織の責任者は、TOE の設置及び 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人物をサービスエンジニアに指定する。

OE-N.SESSION（利用後のセッションの終了）

- 管理者は、一般ユーザに対してボックス機能の利用終了後、そのセッションを必ず終了させる運用を実施する。
- 管理者は、管理者機能の利用終了後、そのセッションを必ず終了させる。
- サービスエンジニアは、サービスエンジニア機能の利用終了後、そのセッションを必ず終了させる。

OE-N.SETTING-1（セキュリティ機能の動作設定１）

- 管理者は、不正使用防止機能を必ず動作させた状態で TOE を運用する。

OE-N.SETTING-2（セキュリティ機能の動作設定２）

- 管理者は、メモリリコールコピー機能が必ず停止した状態で TOE を運用する。

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。

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

TOE に必要とされるセキュリティ機能要件を記述する。全ての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。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。“ イタリック ” 且つ “ ボールド ” 且つ “ アンダーライン ” で示される表記は、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。

5.1.1.1. 利用者データ保護

FDP_ACC.1[1]　　サブセットアクセス制御
FDP_ACC.1.1[1]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。 [割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]： ***「表 2　親展プリントジョブ情報データファイルに対する操作のリスト」に記載*** [割付: *アクセス制御 SFP*]： ***親展プリントジョブアクセス制御***
下位階層　：　なし **依存性**　：　FDP_ACF.1（FDP_ACF.1[1]）

表 2　親展プリントジョブ情報データファイルに対する操作のリスト

サブジェクト	オブジェクト	操作
親展プリントジョブを操作するプロセス	***親展プリントジョブ情報データファイル***	・ ***印刷*** ・ ***登録***

FDP_ACC.1[2]	**サブセットアクセス制御**
FDP_ACC.1.1[2]	
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。 [割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 3　ボックスデータファイルに対する操作のリスト」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[2]）

表 3　ボックスデータファイルに対する操作のリスト

サブジェクト	オブジェクト	操作
ボックスを操作するプロセス	***ボックス***	・ ***ボックス内のボックスデータ読み出し*** ・ ***ボックス内にボックスデータ書き込み*** ・ ***作成***

FDP_ACC.1[3]	**サブセットアクセス制御**
FDP_ACC.1.1[3]	
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。 [割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 4　コピージョブ情報データファイルに対する操作のリスト」に記載*** [割付: *アクセス制御 SFP*]: ***コピージョブアクセス制御***	
下位階層	: なし
依存性	: FDP_ACF.1（FDP_ACF.1[3]）

表 4　コピージョブ情報データファイルに対する操作のリスト

サブジェクト	オブジェクト	操作
コピージョブを操作するプロセス	***コピージョブ情報データファイル***	***削除***

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、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]： ***ジョブ ID***	
[割付: *アクセス制御 **SFP***]： ***親展プリントジョブアクセス制御***	
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*]： ・ ***親展プリントジョブを操作するプロセスは、親展プリントジョブの登録要求を受け付けると、新しく付与される“ジョブ ID”を生成し、これをオブジェクト属性とする親展プリントジョブ情報データファイルを登録する。*** ・ ***一般ユーザが選択した親展プリントジョブの“ジョブ ID”を持つ親展プリントジョブを操作するプロセスは、これと一致する“ジョブ ID”を持つ親展プリントジョブ情報データファイルのみ、印刷操作を許可される。***	
FDP_ACF.1.3[1]	
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。	
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]： ***なし。***	
FDP_ACF.1.4[1]	
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。	
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]： ***なし。***	
下位階層 ： なし **依存性** ： FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3（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、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]： ・ ***ボックス識別子*** ・ ***管理者識別子***	
[割付: *アクセス制御 **SFP***]： ***ボックスアクセス制御***	
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*]： ・ ***“ボックス識別子”を持つボックスを操作するプロセスは、これと一致する“ボックス識別子”を持つボックスが存在しない場合に、この“ボックス識別子”をオブジェクト属性とするボックスの“作成”操作を許可される。*** ・ ***“ボックス識別子”を持つボックスを操作するプロセスは、これと一致する“ボックス識別子”を持つボックスが存在する場合に、この“ボックス識別子”をオブジェクト属性とするボックスの“作成”操作を拒否される。*** ・ ***一般ユーザが選択した“ボックス識別子”を持つボックスを操作するプロセスは、これと一致する“ボックス識別子”を持つボックスのみ、“ボックス内のボックスデータ読み出し”操作を許可される。*** ・ ***“管理者識別子”を持つボックスを操作するプロセスは、すべてのボックスの“ボックス内のボックスデータ読み出し”操作を許可される。*** ・ ***“管理者識別子”を持つボックスを操作するプロセスは、すべてのボックスに対して、“ボックス内にボックスデータ書き込み”操作を許可される。***	
FDP_ACF.1.3[2]	
TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。	
[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]： ***なし。***	
FDP_ACF.1.4[2]	
TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。	

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]: ***なし。***
下位階層 : なし
依存性 : FDP_ACC.1（FDP_ACC.1[2]）、FMT_MSA.3（FMT_MSA.3[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、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]: ***メモリリコール設定データ***
[割付: *アクセス制御 **SFP***]: ***コピージョブアクセス制御***
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*]: ***コピージョブを操作するプロセスは、“メモリリコール設定データ”が“OFF”であるコピージョブ情報データファイルに対して、印刷完了後、削除操作を実行する。***
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（FMT_MSA.3[3]）

5.1.1.2. 識別と認証

FIA_AFL.1[1]	**認証失敗時の取り扱い**
FIA_AFL.1.1[1]	
TSF は、[割付: *認証事象のリスト*]に関して、*[割付: 回数]*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*]： ***親展プリントジョブの正当な利用者である一般ユーザの認証***	
[割付: *回数*]： ***3***	
FIA_AFL.1.2[1]	
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。	
[割付: *アクションのリスト*]： ***以下に示される通常復帰のための操作が実施されない限り、当該親展プリントジョブの正当な利用者である一般ユーザの認証機能をロックする。*** ***＜通常状態復帰のための操作＞*** ***親展プリントジョブに対するアクセス不可状態解除機能を実行する。***	
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、***[割付: 回数]***回の不成功認証試行が生じたときを検出しなければならない。	
[割付: *認証事象のリスト*]： ***ボックスの正当な利用者である一般ユーザの認証***	
[割付: *回数*]： ***3***	
FIA_AFL.1.2[2]	
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。	

[割付: *アクションのリスト*]： ***以下に示される通常復帰のための操作が実施されない限り、当該ボックスの正当な利用者である一般ユーザの認証機能をロックする。*** ***＜通常状態復帰のための操作＞*** ***ボックスに対するアクセス不可状態解除機能を実行する。***
下位階層 ： なし
依存性 ： FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[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、*[割付: 回数]*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*]： ***管理者の認証***	
[割付: *回数*]： ***3***	
FIA_AFL.1.2[3]	
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。	
[割付: *アクションのリスト*]： ***管理者の認証機能をロックする。*** ***＜通常状態復帰のための操作＞*** ***ロック解除のための機能は存在しない。***	
下位階層 ： なし	
依存性 ： FIA_UAU.1（FIA_UAU.2[3]）	

FIA_AFL.1[4]	**認証失敗時の取り扱い**
FIA_AFL.1.1[4]	
TSF は、[割付: *認証事象のリスト*]に関して、***[割付: 回数]***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*]： ***サービスエンジニアの認証***	
[割付: *回数*]： ***3***	

FIA_AFL.1.2[4]
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[割付: *アクションのリスト*]： ***サービスエンジニアの認証機能をロックする。*** ***＜通常状態復帰のための操作＞*** ***ロック解除のための機能は存在しない。***
下位階層 ： なし
依存性 ： FIA_UAU.1（FIA_UAU.2[4]）

FIA_SOS.1[1] **秘密の検証**
FIA_SOS.1.1[1]
TSF は、***ボックスパスワード***が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]： ***最小４桁、最大 64 桁で ASCII コード 0x20 ～ 0x7E（半角英数字、半角記号で 95 種類）***
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、***管理者モードパスワード***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*]： ***8 桁固定で数字（ 0 ～ 9 ）***
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、***サービスコード***が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。

[割付: *定義された品質尺度*]： ***8桁固定で数字（０～９）または“＊”,“＃”***
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***親展プリントジョブの正当な利用者である一般ユーザ***を代行する他の TSF 調停アクションを許可する前に、各***親展プリントジョブの正当な利用者である一般ユーザ***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[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***ボックスの正当な利用者である一般ユーザ***を代行する他の TSF 調停アクションを許可する前に、各***ボックスの正当な利用者である一般ユーザ***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[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***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、***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[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***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、***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 ： なし	
依存性 ： FIA_UID.1（FIA_UID.2[4]）	

FIA_UAU.6	再認証
FIA_UAU.6.1	
TSF は、条件[割付: *再認証が要求される条件のリスト*]のもとで利用者を再認証しなければならない。	
[割付: *再認証が要求される条件のリスト*] ・ ***管理者モードパスワードを改変する。*** ・ ***サービスコードを改変する。***	
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*]: ***管理者モードパスワード、サービスコード、ボックスパスワード、親展プリントパスワードとして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[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]）

FIA_UID.2[1]	アクション前の利用者識別
FIA_UID.2.1[1]	
TSF は、その***親展プリントジョブの正当な利用者である一般ユーザ***を代行する他の TSF 調停アクションを許可する前に、***親展プリントジョブの正当な利用者である一般ユーザ***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[2]	アクション前の利用者識別
FIA_UID.2.1[2]	
TSF は、その***ボックスの正当な利用者である一般ユーザ***を代行する他の TSF 調停アクションを許可する前に、***ボックスの正当な利用者である一般ユーザ***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[3]	**アクション前の利用者識別**
FIA_UID.2.1[3]	
TSF は、その***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***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[4]	**アクション前の利用者識別**
FIA_UID.2.1[4]	
TSF は、その***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、***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

5.1.1.3. セキュリティ管理

FMT_MOF.1	**セキュリティ機能のふるまい管理**
FMT_MOF.1.1	
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。	
[割付: *機能のリスト*]： ***不正使用防止機能***	
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]： ***を動作させる、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[3]）

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*]： ***ボックス識別子***	
[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]： ***改変***	
[割付: *許可された識別された役割*]： ***当該ボックスの正当な利用者である一般ユーザ、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[2]）、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*]： ***メモリリコール設定データ***	
[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]*]： ***デフォルト値変更、問い合わせ***	
[割付: *許可された識別された役割*]： ***管理者***	
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]： ***コピージョブアクセス制御***	
下位階層 ：	なし
依存性 ：	FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1[3]）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1[3]）

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***ジョブID***として、[選択: *制限的*、*許可的*、*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*、*その他の特性*]： ***その他の特性（親展プリントジョブを他のジョブと区別し、一意に識別することが可能な値）***	
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]： ***親展プリントジョブアクセス制御***	
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*]： ***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_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***ボックス識別子***として、[選択: *制限的*、*許可的*、*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*、*その他の特性*]： ***許可的***	
[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[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*]： ***当該ボックスを作成する一般ユーザ***	
下位階層	： なし
依存性	： FMT_MSA.1（FMT_MSA.1[1]）、FMT_SMR.1（FMT_SMR.1[1]）

FMT_MSA.3[3]	**静的属性初期化**
FMT_MSA.3.1[3]	
TSF は、その SFP を実施するために使われる***メモリリコール設定データ***として、[選択: *制限的*、*許可的*、*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*、*その他の特性*]： ***制限的***	
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] ***コピージョブアクセス制御***	
FMT_MSA.3.2[3]	
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*] ***なし***	
下位階層	: なし
依存性	: FMT_MSA.1（FMT_MSA.1[2]）、FMT_SMR.1（なし）

FMT_MTD.1[1]	**TSF データの管理**
FMT_MTD.1.1[1]	
TSF は、[割付: ***TSF データのリスト***]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、*[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。	
[割付: ***TSF データのリスト***]： ・ ***管理者モードパスワード*** ・ ***オートリセット動作設定データ***	
[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]*]： ***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[3]）

FMT_MTD.1[2]	**TSF データの管理**
FMT_MTD.1.1[2]	
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。	
[割付: *TSF データのリスト*]： ・ ***ボックス不正アクセス検出カウント値*** ・ ***親展プリント不正アクセス検出カウント値***	
[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]*]： ***消去***	
[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[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*]： ***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*]： ***当該ボックスの正当な利用者である一般ユーザ、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[4]	**TSF データの管理**
FMT_MTD.1.1[4]	
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。	
[割付: *TSF データのリスト*]： ***サービスコード***	

[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***改変***
[割付:*許可された識別された役割*]： ***サービスエンジニア***
下位階層 ： なし
依存性 ： FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[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*]： ***管理者モードパスワード***
[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（初期値に戻す操作）***
[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[4]）

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*]： ***「表 5　セキュリティ管理機能のリスト」の適用内容欄に記載***
下位階層 ： なし
依存性 ： なし

表 5　セキュリティ管理機能のリスト

N/A：Not Applicable

機能要件コンポーネント	CC パート 2 に記載される管理項目	適用内容
FDP_ACC.1[1]	このコンポーネントについて予見される管理アクティビティはない。	N/A

機能要件 コンポーネント	CC パート 2 に記載される管理項目	適用内容
FDP_ACC.1[2]	このコンポーネントについて予見される管理アクティビティはない。	N/A
FDP_ACC.1[3]	このコンポーネントについて予見される管理アクティビティはない。	N/A
FDP_ACF.1[1]	以下のアクションは FMT の管理機能と考えられる: a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	左記の管理項目に該当する管理機能は存在しない。
FDP_ACF.1[2]	以下のアクションは FMT の管理機能と考えられる: a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	左記の管理項目に該当する管理機能は存在しないが、本要件に関連する事項として以下のセキュリティ管理機能が特定される。 ・ ***ボックス識別子の作成機能*** ・ ***ボックス識別子の改変機能（当該ボックスの正当な利用者である一般ユーザが操作）*** ・ ***ボックス識別子の改変機能（管理者が操作）***
FDP_ACF.1[3]	以下のアクションは FMT の管理機能と考えられる: a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	左記の管理項目に該当する管理機能は存在しないが、本要件に関連する事項として以下のセキュリティ管理機能が特定される。 ・ ***メモリリコール設定データの設定機能***
FIA_AFL.1[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) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	左記の管理項目に該当する管理機能は存在しないが、本要件に関連する事項として以下のセキュリティ管理機能が特定される。 ・ ***不正使用防止機能の動作設定機能*** ・ ***親展プリント不正アクセス検出カウント値を消去するアクセス不可状態解除機能***
FIA_AFL.1[2]	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) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	左記の管理項目に該当する管理機能は存在しないが、本要件に関連する事項として以下のセキュリティ管理機能が特定される。 ・ ***不正使用防止機能の動作設定機能*** ・ ***ボックス不正アクセス検出カウント値を消去するアクセス不可状態解除機能***
FIA_AFL.1[3]	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) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	左記の管理項目に該当する管理機能は存在しないが、本要件に関連する事項として以下のセキュリティ管理機能が特定される。 ・ ***不正使用防止機能の動作設定機能***
FIA_AFL.1[4]	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) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	左記の管理項目に該当する管理機能は存在しない。

機能要件 コンポーネント	CC パート 2 に記載される管理項目	適用内容
FIA_SOS.1[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) 秘密の検証に使用される尺度の管理。	左記の管理項目に該当する管理機能は存在しない。
FIA_SOS.1[2]	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) 秘密の検証に使用される尺度の管理。	左記の管理項目に該当する管理機能は存在しない。
FIA_SOS.1[3]	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) 秘密の検証に使用される尺度の管理。	左記の管理項目に該当する管理機能は存在しない。
FIA_SOS.1[4]	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) 秘密の検証に使用される尺度の管理。	左記の管理項目に該当する管理機能は存在しない。
FIA_UAU.2[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。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	左記の管理項目に該当する管理機能は存在しない。
FIA_UAU.2[2]	以下のアクションは FMT における管理機能と考えられる。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	・ ***ボックスパスワードの改変機能（当該ボックスの正当な利用者である一般ユーザが操作）*** ・ ***ボックスパスワードの改変機能（管理者が操作）*** ・ ***不正使用防止機能の動作設定機能***
FIA_UAU.2[3]	以下のアクションは FMT における管理機能と考えられる。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	・ ***管理者モードパスワードの改変機能*** ・ ***管理者モードパスワードの初期化機能***
FIA_UAU.2[4]	以下のアクションは FMT における管理機能と考えられる。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	・ ***サービスコードの改変機能***
FIA_UAU.6	以下のアクションは FMT における管理機能と考えられる。 許可管理者が再認証を要求できる場合、管理に再認証要求を含める。	左記の管理項目に該当する管理機能は存在しない。
FIA_UAU.7	予見される管理アクティビティはない。	N/A
FIA_UID.2[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;	左記の管理項目に該当する管理機能は存在しない。
FIA_UID.2[2]	以下のアクションは FMT における管理機	・ ***ボックス識別子の作成機能***

機能要件 コンポーネント	CC パート 2 に記載される管理項目	適用内容
	能と考えられる: a) 利用者識別情報の管理;	・ ボックス識別子の改変機能（当該ボックスの正当な利用者である一般ユーザが操作） ・ ボックス識別子の改変機能(管理者が操作)
FIA_UID.2[3]	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;	左記の管理項目に該当する管理機能は存在しない。
FIA_UID.2[4]	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;	左記の管理項目に該当する管理機能は存在しない。
FMT_MOF.1	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MSA.1[1]	以下のアクションは FMT 管理における管理機能と考えられる: a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MSA.1[2]	以下のアクションは FMT 管理における管理機能と考えられる: a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MSA.3[1]	以下のアクションは FMT 管理における管理機能と考えられる: a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MSA.3[2]	以下のアクションは FMT 管理における管理機能と考えられる: a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MSA.3[3]	以下のアクションは FMT 管理における管理機能と考えられる: a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	左記の管理項目に該当する管理機能は存在しない。

機能要件 コンポーネント	CC パート 2 に記載される管理項目	適用内容
FMT_MTD.1[1]	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MTD.1[2]	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MTD.1[3]	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MTD.1[4]	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_MTD.1[5]	以下のアクションは FMT 管理における管理機能と考えられる: a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	左記の管理項目に該当する管理機能は存在しない。
FMT_SMF.1	このコンポーネントに関して予見される管理アクティビティはない。	N/A
FMT_SMR.1[1]	以下のアクションは FMT 管理における管理機能と考えられる: a) 役割の一部をなす利用者のグループの管理。	左記の管理項目に該当する管理機能は存在しない。
FMT_SMR.1[2]	以下のアクションは FMT 管理における管理機能と考えられる: a) 役割の一部をなす利用者のグループの管理。	左記の管理項目に該当する管理機能は存在しない。
FMT_SMR.1[3]	以下のアクションは FMT 管理における管理機能と考えられる: a) 役割の一部をなす利用者のグループの管理。	左記の管理項目に該当する管理機能は存在しない。
FMT_SMR.1[4]	以下のアクションは FMT 管理における管理機能と考えられる: a) 役割の一部をなす利用者のグループの管理。	左記の管理項目に該当する管理機能は存在しない。
FPT_RVM.1	予見される管理アクティビティはない。	N/A
FPT_SEP.1	予見される管理アクティビティはない。	N/A
FTA_SSL.3[1]	以下のアクションは FMT における管理アクティビティと考えられる:	・ ***オートリセット動作設定データの改変機能***

機能要件 コンポーネント	CC パート 2 に記載される管理項目	適用内容
	a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定; b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。	
FTA_SSL.3[2]	以下のアクションは FMT における管理アクティビティと考えられる: a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定; b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。	・ ***オートリセット動作設定データの改変機能***

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*]: ***当該ボックスを作成する一般ユーザ***	
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（適用しない）	

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*]: ***当該ボックスの正当な利用者である一般ユーザ***	
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*]： ***管理者***	
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*]： ***サービスエンジニア***	
FMT_SMR.1.2[4]	
TSF は、利用者を役割に関連づけなければならない。	
下位階層 ： なし	
依存性 ： FIA_UID.1（FIA_UID.2[4]）	

5.1.1.4. TSF の保護

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

FPT_SEP.1	**TSF ドメイン分離**
FPT_SEP.1.1	
TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。	

FPT_SEP.1.2
TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。
下位階層 : なし
依存性 : なし

5.1.1.5. TOE アクセス

FTA_SSL.3[1] **TSF 起動による終了**
FTA_SSL.3.1[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*]: ***パネル管理者機能を操作中、最終操作からオートリセット動作設定データによって決定される時間***
下位階層 : なし
依存性 : なし

FTA_SSL.3[2] **TSF 起動による終了**
FTA_SSL.3.1[2]
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*]: ***PC 管理者機能を操作中、最終操作からオートリセット動作設定データによって決定される時間***
下位階層 : なし
依存性 : なし

5.1.2. 最小セキュリティ機能強度

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

5.1.3. TOE のセキュリティ保証要件

TOE は、一般的なオフィス環境にて利用される商用事務製品であるため、商用事務製品の保証として十分なレベルである EAL3 適合によって必要な TOE セキュリティ保証要件を適用する。下表に適用される TOE のセキュリティ保証要件をまとめる。

表 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

5.2. IT 環境のセキュリティ要件

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。全ての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。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。“ イタリック ” 且つ “ ボールド且つアンダーライン ” で示される表記は、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識別子 “ E ” は、当該機能要件が IT 環境のセキュリティ要件であることを明示するために使用している。また “ ･･･[E1] ”、“ ･･･[E2] ” のように “ E ” の後に付与される番号は当該機能要件が繰り返しされていることを示す。なお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。

5.2.1. IT 環境のセキュリティ機能要件

5.2.1.1. 識別と認証

FIA_SOS.1[E]	**秘密の検証**
FIA_SOS.1.1[E]	
クライアント PC のプリンタドライバは、***親展プリントパスワード***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*]： ***４桁の数字（０～９）***	
下位階層	： なし
依存性	： なし

FIA_UAU.7[E]	**保護された認証フィードバック**
FIA_UAU.7.1[E]	
ボックスユーティリティは、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*]： ***ボックスパスワード、管理者モードパスワードとして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]）

5.2.2. IT 環境のセキュリティ保証要件

IT 環境に対するセキュリティ保証要件は規定しない。

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は、以下に示される表 7、表 8 の通り、前章で記述された TOE セキュリティ機能要件を全て満たしている。

表 7 TOE のセキュリティ機能名称と識別子

識別子	TOE のセキュリティ機能
F.ADMIN-PANEL	パネル管理者モードセキュリティ機能
F.ADMIN-PC	PC 管理者モードセキュリティ機能
F.COPY	残存コピージョブ情報データ保護機能
F.SECURE-PRINT	親展プリントセキュリティ機能
F.SERVICE	サービスモードセキュリティ機能
F.BOX-PANEL	パネルボックスセキュリティ機能
F.BOX-PC	PC ボックスセキュリティ機能
F.BOX-UTILITY-1	ボックスユーティリティセキュリティ機能
F.BOX-UTILITY-2	管理者ボックスユーティリティセキュリティ機能

表 8 TOE 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

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
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]	●	●							●

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
FIA_AFL.1[4]					●				
FIA_SOS.1[1]		●					●		
FIA_SOS.1[2]	●								
FIA_SOS.1[3]					●				
FIA_UAU.2[1]				●					
FIA_UAU.2[2]						●	●	●	
FIA_UAU.2[3]	●	●							●
FIA_UAU.2[4]					●				
FIA_UAU.6	●				●				
FIA_UAU.7	●	●		●	●	●	●	●	●
FIA_UID.2[1]				●					
FIA_UID.2[2]						●	●	●	
FIA_UID.2[3]	●	●							●
FIA_UID.2[4]					●				
FMT_MOF.1	●								
FMT_MSA.1[1]		●					●		
FMT_MSA.1[2]	●	●							
FMT_MSA.3[1]				●					
FMT_MSA.3[2]							●		
FMT_MSA.3[3]			●						
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●								
FMT_MTD.1[3]		●					●		
FMT_MTD.1[4]					●				
FMT_MTD.1[5]					●				
FMT_SMF.1	●	●			●		●		
FMT_SMR.1[1]							●		
FMT_SMR.1[2]							●		
FMT_SMR.1[3]	●	●							
FMT_SMR.1[4]					●				
FPT_RVM.1	●	●		●	●	●	●	●	●
FPT_SEP.1	●	●	●	●	●	●	●	●	●
FTA_SSL.3[1]	●								
FTA_SSL.3[2]		●							

6.1.1. F.ADMIN-PANEL（パネル管理者モードセキュリティ機能）

F.ADMIN-PANEL とは、MFP 本体操作パネルからアクセスする管理者モードにおける管理者識別認証機能、管理者モードパスワード、ボックスパスワード、ボックス識別子を変更するセキュリティ管理機能、不正使用防止機能の動作設定機能、アクセス不可状態解除機能といった一連のセキュリティ機能のことである。

＜管理者モードへのアクセスにおける識別認証機能＞

- 管理者モードへアクセスすることを要求することによってアクセスする利用者を管理者として識別する。
- 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が管理者であることを、8 桁数字の管理者モードパスワードより認証する管理者モードパスワード認証メカニズムを提供する。
- 管理者モードパスワード入力のフィードバックには 1 文字毎に“ ＊ ”を返す。
- 認証に 3 回失敗すると、不正アクセスが行われていると判断し、本認証機能をロックする。（※ロックを解除するための機能は存在しない。）

＜MFP 本体操作パネルからアクセスする管理者モードにおけるセキュリティ管理機能＞

- MFP 本体操作パネルから管理者モードへのアクセスに対して、管理者であることが認証されると、①管理者モードパスワード変更機能、②不正使用防止機能の動作設定機能、③アクセス不可状態解除機能、④オートリセット動作設定データの変更機能、⑤メモリリコール設定データの設定変更機能に対するアクセス及び操作を許可する。

① 管理者モードパスワード変更機能

- 管理者であることを管理者モードパスワードより再認証する管理者モードパスワード認証メカニズムを提供する。
- 再認証の際の管理者モードパスワード入力のフィードバックには、1 文字毎に“ ＊ ”を返す。
- 新規設定される管理者モードパスワードが 8 桁数字であることをチェックし、誤入力を防止するための再入力を受け付け、両者が一致した場合にそのパスワードを管理者モードパスワードとして変更する。
- 再認証のために入力された管理者モードパスワードの誤入力により、管理者モード不正アクセス検出カウント値をカウントする。3 回誤入力が行われると、管理者モードへのアクセス許可を取り消し、以降、管理者モードへアクセスするための認証機能をロックする。

② 不正使用防止機能の動作設定機能

- 「動作する」を選択・実行することにより不正使用防止機能を動作状態にする。
- 「停止する」を選択・実行することにより不正使用防止機能を停止状態にする。

③ アクセス不可状態解除機能

- 各親展プリントジョブの親展プリント不正アクセス検出カウント値を 0 クリアすることに

より、親展プリントジョブの正当な利用者である一般ユーザを認証するための認証機能のロックを解除する。

- 各ボックスのボックス不正アクセス検出カウント値を 0 クリアすることにより、ボックスの正当な利用者である一般ユーザを認証するための認証機能のロックを解除する。

④ オートリセット動作設定データの変更機能

- 「しない」、または 1～9 分の時間範囲でオートリセット機能の動作を設定する。

⑤ メモリリコール設定データの設定変更機能

- 「する」を選択・実行することによりメモリリコール設定データが ON に設定され、メモリリコールコピー機能を動作状態（コピージョブ情報データファイルは削除されず、再印刷可能な状態で残る）にする。
- 「しない」を選択・実行することによりメモリリコール設定データが OFF に設定され、メモリリコールコピー機能を停止状態（コピージョブ情報データファイルは印刷終了後自動削除され、再印刷可能な状態で残らない）にする。

＜MFP 本体操作パネルからアクセスする管理者モードにおいて動作するオートリセット機能＞

・ MFP 本体操作パネルから管理者モードへのアクセスに対して、管理者であることが認証された後、無操作状態がオートリセット動作設定データにより決定される時間経過すると、管理者モードのアクセス許可状態が解除される。
・ 本機能はオートリセット動作設定データにより設定される値通りの時間で動作する。

6.1.2. F.ADMIN-PC（PC 管理者モードセキュリティ機能）

F.ADMIN-PC とは、クライアント PC 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、ボックスパスワード、ボックス識別子を変更するボックス設定管理機能といった一連のセキュリティ機能のことである。

＜管理者モードへのアクセスにおける識別認証機能＞

・ クライアント PC から管理者モードへアクセスすることを要求することによって利用者が管理者として識別する。
・ 管理者モードのアクセス要求に対して、アクセスする利用者が管理者であることを、8 桁数字の管理者モードパスワードより認証する管理者モードパスワード認証メカニズムを提供する。
・ 管理者モードパスワード入力のフィードバックには 1 文字毎に“＊”を返す。
・ 認証に 3 回失敗すると、不正アクセスが行われていると判断し、本認証機能をロックする。（※ロックを解除するための機能は存在しない。）

＜クライアント PC からアクセスする管理者モードにおけるセキュリティ管理機能＞

・ クライアント PC から管理者モードへのアクセスに対して、管理者であることが認証されると、

任意のボックスにおけるボックス識別子、ボックスパスワードを変更する①ボックス設定管理機能、②オートリセット動作設定データの変更機能、③メモリリコール設定データの設定変更機能に対するアクセス及び操作を許可する。

① ボックス設定管理機能

- ボックス識別子の変更は、新しく設定されるボックス識別子の入力を受け付け、同一名称のボックス識別子が登録されていない場合にその名称を当該ボックスのボックス識別子として変更する。
- ボックスパスワードの変更は、新しく設定されるボックスパスワードの入力、誤入力を防止するための再入力を受け付け、両者が一致した場合にそのパスワードを当該ボックスのボックスパスワードとして変更する。
- ボックスパスワードが、4～64 桁且つ ASCII コード 0x20～0x7E（半角英数字、半角記号、計 95 種）であることをチェックする。

② オートリセット動作設定データの変更機能

- 「しない」、または 1～9 分の時間範囲でオートリセット機能の動作を設定する。

③ メモリリコール設定データの設定変更機能

- 「する」を選択・実行することによりメモリリコール設定データが ON に設定され、メモリリコールコピー機能を動作状態（コピージョブ情報データファイルは削除されず、再印刷可能な状態で残る）にする。
- 「しない」を選択・実行することによりメモリリコール設定データが OFF に設定され、メモリリコールコピー機能を停止状態（コピージョブ情報データファイルは印刷終了後自動削除され、再印刷可能な状態で残らない）にする。

＜クライアント PC からアクセスする管理者モードにおいて動作するオートリセット機能＞

・ クライアント PC から管理者モードへのアクセスに対して、管理者であることが認証された後、無操作状態がオートリセット動作設定データにより決定される時間を経過すると、管理者モードのアクセス許可状態が解除される。
・ 本機能は、オートリセット動作設定データが 1～5 分の場合は 5 分、6～9 分の場合は設定値通りの 6～9 分、“ しない ” が設定される場合は 10 分で動作する。

6.1.3. F.COPY（残存コピージョブ情報データ保護機能）

F.COPY とは、MFP 本体操作パネルより実行されるコピー機能において、印刷終了後に取り込んだイメージデータであるコピージョブ情報データを自動的に削除する機能のことである。

・ コピー機能を実行すると、印刷完了後、コピージョブを操作するプロセスにより、メモリリコール設定データが OFF であるコピージョブ情報データが削除される。（※管理者機能にて、メモリリコールコピー機能が停止状態に設定されている場合は、コピージョブ情報データファイルのセ

キュリティ属性であるメモリリコール設定データは必ずOFFになる。）

6.1.4. F.SECURE-PRINT（親展プリントセキュリティ機能）

F.SECURE-PRINTとは、MFP本体操作パネルからの親展プリントジョブ情報データへのアクセスに対して親展プリントジョブ情報データの正当な利用者であることを識別認証し、識別認証後に当該親展プリントジョブ情報データ印刷操作を許可するアクセス制御機能のことである。

＜親展プリントジョブの登録機能＞

・ 親展プリントジョブ情報データファイルの登録は、一般ユーザに提供される。
・ クライアントPCよりプリンタドライバにて設定された親展プリントパスワードと共に送信されてきた親展プリントデータを親展プリントジョブ情報データファイルとしてジョブに一意に識別されるジョブIDを付与して登録する。

＜親展プリントジョブを印刷するための識別認証機能＞

・ MFP本体操作パネルより、印刷待機中の親展プリントジョブが選択されると、選択された親展プリントジョブ情報データにアクセスする者が当該親展プリントジョブの正当な利用者である一般ユーザであることを、4桁数字の親展プリントパスワードより認証する親展プリントパスワード認証メカニズムを提供する。
・ 親展プリントパスワード入力のフィードバックには1文字毎に“＊”を返す。
・ 認証に3回失敗すると不正アクセスが行われていると判断し、当該親展プリントジョブ情報データへ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、F.ADMIN-PANELが提供する親展プリントジョブに対するアクセス不可状態解除機能を実行することにより解除される。

＜親展プリントジョブを印刷するためのアクセス制御機能＞

・ 一般ユーザが当該親展プリントジョブ情報データファイルの正当な利用者であることが認証されると、親展プリントジョブアクセス制御規則に基づき、親展プリントジョブを操作するプロセスに対して、サブジェクト属性と一致する“ジョブID”を持つ親展プリントジョブ情報データファイルの印刷操作が許可される。

6.1.5. F.SERVICE（サービスモードセキュリティ機能）

F.SERVICEとは、MFP本体操作パネルからアクセスするサービスモードにおけるサービスエンジニア識別認証機能、サービスコード変更機能、管理者モードパスワード初期化機能といったサービスモードにおける一連のセキュリティ機能のことである。

＜サービスモードへのアクセスにおける識別認証機能＞

・ サービスモードへのアクセスすることを要求する（サービスエンジニア以外には公開されないサービスモードへの操作手順を実行する）ことによってアクセスする利用者をサービスエンジニア

として識別する。

・ サービスモードへの操作手順を受け付けると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、8 桁の数字、“ ＃ ”、“ ＊ ”からなるパスワード（サービスコード）より認証するサービスコード認証メカニズムを提供する。
・ サービスコード入力のフィードバックには 1 文字毎に“ ＊ ”を返す。
・ 認証に 3 回失敗すると不正アクセスが行われていると判断し、サービスモードへアクセスするための認証機能をロックする。（※ロックを解除するための機能は存在しない。）

＜サービスモードにおけるセキュリティ管理機能＞

・ サービスモードへのアクセスに対して、サービスエンジニアであることが認証されると、サービスモードにおけるセキュリティ管理機能に対するアクセス及び操作を許可する。

① サービスコード変更機能

- サービスコードの変更機能は、サービスモードにて更に公開されない操作手順を入力後、サービスエンジニアであることを再認証するサービスコード認証メカニズムを提供する。
- 再認証の際のサービスコード入力のフィードバックには、1 文字毎に“ ＊ ”を返す。
- 新規設定されるサービスコードが 8 桁数字、“ ＃ ”、“ ＊ ”であることをチェックし、新しく設定されるサービスコードの入力、誤入力を防止するための再入力を受け付け、両者が一致した場合にそのパスワードをサービスコードとして変更する。
- この再認証のために入力されたサービスコードを誤った場合、サービスモードへのアクセス許可を取り消し、サービスエンジニア不正アクセス検出カウント値を 1 つカウントアップする。

② 管理者モードパスワード初期化機能

- 管理者モードパスワード初期化機能を実行すると、管理者モードパスワードをセットアップ時の初期値に設定する。

6.1.6. F.BOX-PANEL（パネルボックスセキュリティ機能）

F.BOX-PANEL とは、一般ユーザの MFP 本体操作パネルからボックスデータへのアクセスに対してボックスデータの正当な利用者であることを識別認証し、ボックスへのアクセスを制御するアクセス制御機能のことである。

＜ボックスへアクセスする際の識別認証機能＞

- アクセス対象とするボックスを選択すると、アクセスする利用者が当該ボックスの正当な利用者である一般ユーザであることを 4～64 桁且つ ASCII コード 0x20～0x7E（半角英数字・半角記号、95 種）からなるボックスパスワードにより認証するボックスパスワード認証メカニズムを提供する。
- ボックスパスワード入力のフィードバックには 1 文字毎に“＊”を返す。
- 認証で 3 回認証試行を失敗すると、以降、アクセス対象としているボックスへ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、F.ADMIN-PANEL が提供するボックスに対するアクセス不可状態解除機能を実行することにより解除する。

＜識別認証後のボックスアクセス制御機能＞

- 一般ユーザが、ボックスの正当な利用者である一般ユーザであると認証されると、ボックスアクセス制御に基づき、ボックスを操作するプロセスに対してサブジェクト属性と一致する“ボックス識別子”を持つボックスの“ボックス内のボックスデータ読み出し”操作が許可される。

（このボックス内のボックスデータ読み出し許可により、MFP 本体操作パネルから E-mail 送信操作、FTP 送信操作が可能となる。）

6.1.7. F.BOX-PC（PC ボックスセキュリティ機能）

F.BOX-PC とは、一般ユーザのクライアント PC からボックスデータへのアクセスに対してボックスデータの正当な利用者であることを識別認証し、ボックスへのアクセスを制御するアクセス制御機能及びボックスを作成・設定管理するセキュリティ機能のことである。

＜ボックス作成機能＞

- ボックス作成機能は、一般ユーザに提供される。
- ボックス作成機能が起動されると、ボックスを操作するプロセスが立ち上がる。
- ボックスを操作するプロセスにより、その一般ユーザが入力したボックス識別子が他のボックスに設定されていない場合、その一般ユーザが入力したボックス識別子を属性とするボックスの作成が行われる。（既に存在する場合は、拒否される。）

＜ボックスへアクセスする際の識別認証機能＞

- アクセス対象とするボックスを選択すると、アクセスする利用者が当該ボックスの正当な利用者

である一般ユーザであることを 4～64 桁且つ ASCII コード 0x20～0x7E（半角英数字・半角記号、95 種）からなるボックスパスワードにより認証するボックスパスワード認証メカニズムを提供する。

・ ボックスパスワード入力のフィードバックには 1 文字毎に“＊”を返す。

・ 認証で 3 回認証試行を失敗すると、以降、アクセス対象としているボックスへ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、F.ADMIN-PANEL が提供するボックスに対するアクセス不可状態解除機能を実行することにより解除する。

＜識別認証後のボックスアクセス制御機能＞

・ 一般ユーザが、ボックスの正当な利用者である一般ユーザであると認証されると、ボックスアクセス制御に基づき、ボックスを操作するプロセスに対してサブジェクト属性と一致する“ボックス識別子”を持つボックスの“ボックス内のボックスデータ読み出し”操作が許可される。

（このボックス内のボックスデータ読み出し許可により、クライアント PC からのダウンロード操作が可能となる。）

＜ボックス設定管理機能＞

・ 識別認証されたボックスの正当な利用者に当該ボックスに対してボックスの設定を変更する機能（ボックス識別子変更、ボックスパスワード変更）を提供する。

・ ボックスパスワードの変更は、新しく設定されるボックスパスワードの入力及び誤入力を防止するための再入力を受け付け、両者が一致した場合にボックスパスワードの変更処理を行う。

・ 新規設定されるボックスパスワードは、4～64 桁且つ ASCII コード 0x20～0x7E（半角英数字・半角記号、95 種）であることをチェックする。

・ 認証で 3 回認証試行を失敗すると、以降、当該ボックスの正当な利用者である一般ユーザの認証機能をロックする。このロック状態は、F.ADMIN-PANEL が提供するボックスに対するアクセス不可状態解除機能を実行することにより解除する。

6.1.8. F.BOX-UTILITY-1（ボックスユーティリティセキュリティ機能）

F.BOX-UTILITY-1 とは、一般ユーザのクライアント PC から専用アプリケーションを利用したボックスデータへのアクセスに対してボックスデータの正当な利用者であること識別認証し、ボックスへのアクセスを制御するアクセス制御機能のことである。

＜ボックスへアクセスする際の識別認証機能＞

・ アクセス対象とするボックスを選択すると、アクセスする利用者が当該ボックスの正当な利用者である一般ユーザであることを 4～64 桁且つ ASCII コード 0x20～0x7E（半角英数字・半角記号、95 種）からなるボックスパスワードにより認証するボックスパスワード認証メカニズムを提供する。

・ 認証で 3 回認証試行を失敗すると、以降、アクセス対象としているボックスへ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、F.ADMIN-PANEL が提供するボックスに対するア

クセス不可状態解除機能を実行することにより解除する。

＜識別認証後のボックスアクセス制御機能＞

・ 一般ユーザが、ボックスの正当な利用者である一般ユーザであると認証されると、ボックスアクセス制御に基づき、ボックスを操作するプロセスに対してサブジェクト属性と一致する“ボックス識別子”を持つボックスの“ボックス内のボックスデータ読み出し”操作が許可される。

（このボックス内のボックスデータ読み出し許可により、クライアント PC からボックスユーティリティを利用してダウンロード操作、プレビュー操作、サムネイル表示操作が可能となる。）

6.1.9. F.BOX-UTILITY-2（管理者ボックスユーティリティセキュリティ機能）

F.BOX-UTILITY-2 とは、管理者のクライアント PC から専用アプリケーションであるボックスユーティリティを利用したボックスへのアクセスに対して管理者を認証する機能のことである。

＜ボックスデータバックアップ操作及びリストア操作における認証機能＞

・ クライアント PC からボックスユーティリティを利用してボックスデータのバックアップ操作、バックアップされたボックスデータのリストア操作を要求する利用者が管理者であることを、8 桁数字の管理者モードパスワードより認証する管理者モードパスワード認証メカニズムを提供する。

・ 認証に 3 回失敗すると、不正アクセスが行われていると判断し、本認証機能をロックする。（※ロックを解除するための機能は存在しない。）

＜認証後のボックスアクセス制御機能（バックアップ操作）＞

・ 管理者であることが認証されると、“管理者識別子”を持つボックスを操作するプロセスに対してすべてのボックスの“ボックス内のボックスデータ読み出し”操作（ボックスデータのバックアップ操作）が許可される。

＜認証後のボックスアクセス制御機能（リストア操作）＞

・ 管理者であることが認証されると、ボックスアクセス制御に基づき、“管理者識別子”を持つボックスを操作するプロセスに対してすべてのボックスに対して“ボックス内にボックスデータ書き込み”操作（バックアップされたボックスデータのリストア操作）が許可される。

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、F.ADMIN-PANEL、F.ADMIN-PC、F.BOX-UTILITY-2 における管理者モードパスワード認証メカニズム、F.SECURE-PRINT における親展プリントパスワード認証メカニズム、及び F.BOX-PANEL、F.BOX-PC、F.BOX-UTILITY-1 におけるボックスパスワード認証メカニズム、F.SERVICE におけるサービスコード認証メカニズムである。機能強度はそれぞれ SOF-基本を満たす。

6.3. 保証手段

表 9 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 9 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	配付説明書
	設置・生成・及び立上げ	ADO_IGS.1	・設置チェックリスト（※和文） ・Installation Checklist（※英文） ※市場における TOE の物理的設置手順は、サービスマニュアル『bizhub C350 サービスマニュアル[セキュリティ機能編]（和文）・bizhub C350 / CF2203 / 8022 Service Manual [Secirity Function]（英文）』に記載されている。
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	・bizhub C350 ユーザーズガイド [セキュリティ機能編] ・・・（※和文） ・bizhub C350 User's Guide [Secirity Function] ・・・（※英文） ・CF2203 User's Guide [Secirity Function] ・・・（※英文） ・8022 User's Guide [Secirity Function] ・・・（※英文） ・bizhub C350 サービスマニュアル [セキュリティ機能編] ・・・（※和文） ・bizhub C350 / CF2203 / 8022 Service Manual [Secirity Function]・・・（※英文）
	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・結果報告書
	独立テスト	ATE_IND.2	TOE を含む MFP 制御ソフトウェア
脆弱性評定	誤使用	AVA_MSU.1	ガイダンス文書に反映

TOE セキュリティ保証要件		コンポーネント	保証手段
	TOE セキュリティ機能強度	AVA_SOF.1	機能強度分析書
	脆弱性分析	AVA_VLA.1	脆弱性分析書

7. PP 主張

本 ST には、適合する PP はない。

8. 根拠

本 ST で規定した内容の正当性について述べる。

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 10 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.AUTH	A.HDD	A.NETWORK	A.PHYSICAL	A.SERVICE	A.SETTING	T.ACCESS-SECURE-PRINT	T.ACCESS-BOX	T.ACCESS-COPY-DATA	T.SEND-BOX-DATA	P.BEHAVIOR-FUNCTION
O.ACCESS-ADMIN								●	●	●		●
O.ACCESS-BOX									●			
O.ACCESS-SECURE-PRINT								●				
O.ACCESS-SERVICE								●	●	●	●	●
O.CONTROL-COPY										●		
O.I&A -ADMIN								●	●	●	●	●
O.I&A -SERVICE								●	●	●	●	●
O.I&A-USER								●	●			

前提・脅威 / セキュリティ対策方針	A.ADMIN	A.AUTH	A.HDD	A.NETWORK	A.PHYSICAL	A.SERVICE	A.SETTING	T.ACCESS-SECURE-PRINT	T.ACCESS-BOX	T.ACCESS-COPY-DATA	T.SEND-BOX-DATA	P.BEHAVIOR-FUNCTION
OE.FEED-BACK									●			
OE.SECURE-PRINT-QUALITY								●				
OE-N.ADMIN	●											
OE-N.AUTH		●										
OE-N.HDD			●									
OE-N.NETWORK				●								
OE-N.PHYSICAL					●							
OE-N.SERVICE						●						
OE-N.SESSION								●	●	●	●	●
OE-N.SETTING-1							●					
OE-N.SETTING-2										●		

8.1.2. 十分性（前提条件）

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、管理者の信頼性が保証される。

  従って本条件は実現される。

- **A.AUTH（パスワードに関する運用条件）**

  本条件は、TOEの利用において使用される各パスワード（親展プリントパスワード、ボックスパスワード、管理者モードパスワード、サービコード）がそのパスワードの利用者より漏洩しないことを想定している。

  OE-N.AUTHは、MFPを利用する組織の責任者が、管理者に対して管理者モード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。

  本セキュリティ対策方針は、管理者が、一般ユーザに対して親展プリントパスワード及びボックス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。

  更に本セキュリティ対策方針は、MFPを保守管理する組織の責任者が、サービスエンジニアに対して、サービスコードに関する運用規則を実施することを規定している。

よってTOEの利用にて使用される各パスワードの扱いは明確にその運用規則が規定されているため、運用上パスワードの漏洩は起こり得ないことが保証される。従って本条件は実現される。

- **A.HDD（MFPで利用するハードウェア環境条件）**

  本条件は、TOEの搭載されるMFPではHDDロック機能をもったHDDだけが利用され、その設定情報であるHDDロックパスワードがその利用者によって漏洩されないこと、すなわち持ち出されるなどして不正にデータ解析が試みられた場合であってもHDD内の資産が保護されることを想定している。

  OE-N.HDDは、サービスエンジニアがTOEの搭載されるMFPでは、HDDロック機能を有するHDDを設置することが規定されており、且つ管理者が適切なHDDロックパスワードを設定、運用管理することを規定している。これより不正にデータ解析が試みられたとしても、HDDロック機能によりデータを読み出すことは不可能であり、保護資産の機密性が確保される。

  従って本条件は実現される。

- **A.NETWORK（MFPのネットワーク接続条件）**

  本条件は、MFPに接続されるネットワーク環境よりオフィス内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上で盗聴されないネットワーク環境を実現するために、スイッチングハブ等の機器を設置する、MFPとクライアントPC間の暗号化を行う等の措置を施し、盗聴されないための適切な環境設定を行うことが規定されており、外部ネットワークからMFPへのアクセスを遮断するための機器を設置し、外部アクセスを遮断するための適切な設定を実施することが規定されている。

  従って本条件は実現される。

  前記にある盗聴されないネットワーク環境とは、具体的に以下に示す方法等により実現することが可能である。

  ① スイッチングハブのみを用いてオフィス内LANを構成し、盗聴行為を禁止するオフィスの運用ポリシーに基づいてオフィス内LAN環境を利用する方法

  ② MFPを特定の機器を介してオフィス内LANと接続し、その機器とオフィス内LAN上のクライアントPCとの間のすべての通信データがIPsec等により暗号化処理される設定を実施する方法

- **A.PHYSICAL（MFPの設置条件）**

  本条件は、TOEの搭載されたMFPが設置される場所は、一般ユーザ、管理者、サービスエンジニアだけが入ることができる物理的に保護された場所であることを想定している。

  OE-N.PHYSICALは、物理的に保護されたオフィスにTOEの搭載されたMFPを設置することを規定している。更に本セキュリティ対策方針は、オフィスに入ることができるのは、一般ユーザ、管理者、及びサービスエンジニアだけに制限する運用管理を実施することを規定しており、これによりTOEは物理的に保護されることが保証される。

  従って本条件は実現される。

- **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がMFPを保守管理する組織において信頼のおける人物をサービスエンジニアに指定するため、サービスエンジニアの信頼性が保証される。
  従って本条件は実現される。

- **A.SETTING（セキュリティ機能の動作設定条件）**
  本条件は、不正使用防止機能が必ず動作することを想定している。
  OE-N.SETTING-1は、TOEの搭載されたMFPの利用において、管理者が不正使用防止機能を動作させる状態にすることが規定されており、これよりセキュリティ管理機能の期待される動作が保証される。
  従って本条件は実現される。

8.1.3. 十分性（脅威）

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.ACCESS-SECURE-PRINT（親展プリントジョブ情報データの不正な操作）**
  本脅威は、親展プリントジョブ情報データに対してMFP本体操作パネルよりアクセスされ、親展プリントジョブ情報データが不正に印刷されてしまう可能性があることを想定している。これに対抗するには、アクセスする利用者に対して正当な利用者であることを検証し、正当な利用者と認められた者以外のアクセス及び操作を制限する必要がある。

  本脅威に対抗するためのセキュリティ対策方針としてO.I&A-USERにより、親展プリントジョブ情報データにアクセスする者が親展プリントジョブの正当な利用者である一般ユーザであることを識別認証することが規定されており、更にO.ACCESS-SECURE-PRINTにより、正当な利用者であることを識別認証された一般ユーザだけがアクセス対象とする親展プリントジョブ情報データの印刷操作を許可することが規定されている。
  この認証機能において機能強度を保つために一定以上のパスワード長が必要であるが、OE.SECURE-PRINT-QUALITYより、クライアントPCにインストールされるプリンタドライバ上にて、親展プリントに設定される親展プリントパスワードとして規定される品質尺度を満たすデータのみ受け付けることが規定されている。

  また親展プリントジョブの正当な利用者である一般ユーザの認証機能における不正アクセスを検出する不正使用防止機能の動作設定機能、及び当該認証機能のロック状態を解除するアクセス不可状態解除機能は管理者モードにて提供されているが、O.I&A-ADMINにより管理者モードにアクセスする利用者が確かに管理者であることを識別認証することが規定されており、更にO.ACCESS-ADMINにより管理者だけが管理者機能の操作を許可される制御が規定され、OE-N.SESSIONによって管理者機能の利用終了後にそのセッションを終了させるという運用が

規定されている。これより、管理者モードにおける親展プリントジョブ情報データに関係するセキュリティ管理機能に対する不正なアクセスから保護される。

更に管理者モードパスワードを初期化する管理機能を有するサービスモードに対する対策としてO.I&A-SERVICEによりサービスモードにアクセスする利用者が確かにサービスエンジニアであることを識別認証することが規定されており、O.ACCESS-SERVICEによりサービスエンジニアだけがサービスモードにおけるセキュリティ関連機能の操作を許可される制御が規定され、OE-N.SESSIONによってサービスモードにおけるセキュリティ管理機能の利用終了後にそのセッションを終了させるという運用が規定されている。

よってこれらセキュリティ対策方針が満たされることにより本脅威に対して十分に対抗することが可能である。

- **T.ACCESS-BOX（ボックスデータへの不正な操作）**

本脅威は、ボックスデータに対してクライアントPCよりアクセスされ、ボックスデータが不正にダウンロードされてしまう可能性があることを想定している。これに対抗するには、アクセスする利用者に対して正当な利用者であることを検証し、正当な利用者と認められた者以外のアクセス及び操作を制限する必要がある。

本脅威に対抗するためのセキュリティ対策方針としてO.I&A-USERにより、ボックスにアクセスする者がボックスの正当な利用者である一般ユーザであることを識別認証することが規定されており、更にO.ACCESS-BOXにより、正当な利用者であることを識別認証された一般ユーザだけがアクセス対象とするボックスにおけるボックスデータのダウンロード操作を許可することが規定されている。更にOE-N.SESSIONは、管理者が一般ユーザに対して、ボックス機能の利用終了後に、そのセッションを必ず終了させる運用を実施することが規定されており、不正アクセスの可能性を軽減している。
ボックスユーティリティを利用したアクセスの場合は、OE.FEED-BACKにより、アクセス時に入力されるボックス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返すことが規定されている。
管理者機能の1つであるボックスデータのバックアップ操作、リストア操作を要求する利用者をO.I&A-ADMINにより、管理者であることを認証することが規定されている。更に、O.ACCESS-ADMINにより、管理者だけが、ボックスデータのバックアップ操作、リストア操作（ダウンロード、アップロード操作）を含む管理者機能を利用することを許可されることが規定されている。この場合もOE.FEED-BACKにより、アクセス時に入力される管理者モード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返すことが規定されている。

管理者機能であるボックスの正当な利用者である一般ユーザの認証機能における不正アクセスを検出する不正使用防止機能の動作設定機能、当該認証機能のロック状態を解除するアクセス不可状態解除機能、ボックスの設定管理機能は管理者モードにて提供されているが、これに対して

ボックスデータのバックアップ操作、リストア操作同様に、O.I&A-ADMINにより管理者モードにアクセスする利用者が確かに管理者であることを識別認証することが規定されており、更にO.ACCESS-ADMINにより管理者だけが管理者機能の操作を許可される制御が規定され、OE-N.SESSIONによって管理者機能の利用終了後にそのセッションを終了させるという運用が規定されている。これより、管理者モードにおけるボックスデータに関係するセキュリティ管理機能に対する不正なアクセスから保護される。

更に管理者モードパスワードを初期化する管理機能を有するサービスモードに対する対策としてO.I&A-SERVICEによりサービスモードにアクセスする利用者が確かにサービスエンジニアであることを識別認証することが規定されており、O.ACCESS-SERVICEによりサービスエンジニアだけがサービスモードにおけるセキュリティ関連機能の操作を許可される制御が規定され、OE-N.SESSIONによってサービスモードにおけるセキュリティ管理機能の利用終了後にそのセッションを終了させるという運用が規定されている。

よってこれらセキュリティ対策方針が満たされることにより本脅威に対して十分に対抗することが可能である。

- **T.ACCESS-COPY-DATA（残存するコピージョブ情報データに対する不正な操作）**

本脅威は、通常利用後に再印刷可能な状態になるコピージョブ情報のデータファイルにアクセスされ、暴露される可能性があることを想定している。これに対抗するには、機密性の高いドキュメント等をコピーする場合、印刷終了後に自動的に削除され、再利用不可能な状態を実現する必要がある。

本脅威に対抗するためのセキュリティ対策方針としてO.CONTROL-COPYは、取り込んだコピージョブ情報データを印刷終了後に削除することを規定しており、且つOE-N.SETTING-2は、管理者がメモリリコールコピー機能を利用しない設定にすることを規定しているため、コピー機能の利用において利用可能な形で残存する可能性のあるコピージョブ情報データに対するセキュリティが保証される。

メモリリコールコピー機能の動作設定機能は、管理者モードにて提供されているが、O.I&A-ADMINにより管理者モードにアクセスする利用者が確かに管理者であることを識別認証することが規定されており、更にO.ACCESS-ADMINにより管理者だけが管理者機能の操作を許可される制御が規定され、OE-N.SESSIONによって管理者機能の利用終了後にそのセッションを終了させるという運用が規定されている。これより、管理者モードにおける親展プリントジョブ情報データに関係するセキュリティ管理機能に対する不正なアクセスから保護される。

更に管理者モードパスワードを初期化する管理機能を有するサービスモードに対する対策としてO.I&A-SERVICEによりサービスモードにアクセスする利用者が確かにサービスエンジニアであることを識別認証することが規定されており、O.ACCESS-SERVICEによりサービスエンジニアだけがサービスモードにおけるセキュリティ関連機能の操作を許可される制御が規定さ

れ、OE-N.SESSIONによってサービスモードにおけるセキュリティ管理機能の利用終了後にそのセッションを終了させるという運用が規定されている。

よってこれらセキュリティ対策方針が満たされることにより本脅威に対して十分に対抗することが可能である。

- **T.SEND-BOX-DATA（ボックスデータの想定されない宛先への送信）**

本脅威は、MFP本体操作パネルより操作することが可能なボックスデータのE-mail送信、FTP送信において、宛先情報として必要となるMFPに登録されているSMTPサーバ、FTPサーバの設定データが変更されることにより、利用者の意図しない宛先にボックスデータが送信されてしまう可能性があることを想定している。これに対抗するには、送信において利用されるSMTPサーバ及びFTPサーバの設定データに対してアクセスする利用者を許可された利用者だけに制限する必要がある。

本脅威に対抗するためのセキュリティ対策方針としてO.I&A-ADMINにより、SMTPサーバ、FTPサーバの設定データ管理機能が提供されている管理者機能にアクセスする利用者を管理者であること識別認証することが規定されている。識別認証された管理者だけがSMTPサーバ、FTPサーバの設定データ管理機能を操作することができる。またOE-N.SESSIONによって管理者機能の利用終了後にそのセッションを終了させるという運用が規定されている。

更に管理者モードパスワードを初期化する管理機能を有するサービスモードに対する対策としてO.I&A-SERVICEによりサービスモードにアクセスする利用者が確かにサービスエンジニアであることを識別認証することが規定されており、O.ACCESS-SERVICEによりサービスエンジニアだけがサービスモードにおけるセキュリティ関連機能の操作を許可される制御が規定され、OE-N.SESSIONによってサービスモードにおけるセキュリティ管理機能の利用終了後にそのセッションを終了させるという運用が規定されている。

よってこれらセキュリティ対策方針が満たされることにより本脅威に対して十分に対抗することが可能である。

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抗するセキュリティ対策方針について以下に説明する。

- **P.BEHAVIOR-FUNCTION（セキュリティ機能の動作設定機能）**

本組織のセキュリティ方針は、セキュアな環境にて利用されるケースに対して操作上の便宜を図るために、不正使用防止機能を停止状態にする、メモリリコールコピー機能を動作状態（メモリリコールOFFコピーで動作しない）にすることが規定されている。これを実現するには、各機能の動作設定機能が提供される必要がある。またセキュリティ構造に大きな影響を及ぼす機能であ

るため、各動作設定機能の管理は信頼できる者に制限される必要がある。

本組織のセキュリティ方針を実現するセキュリティ対策方針は、O.I&A-ADMINにより管理者モードにアクセスする利用者が確かに管理者であることを識別認証することが規定されており、更にO.ACCESS-ADMINにより管理者だけが管理者機能を操作することを許可されることが規定され、OE-N.SESSIONによって管理者機能の利用終了後にそのセッションを終了させるという運用が規定されている。

更に管理者モードパスワードを初期化する管理機能を有するサービスモードに対する対策としてO.I&A-SERVICEによりサービスモードにアクセスする利用者が確かにサービスエンジニアであることを識別認証することが規定されており、O.ACCESS-SERVICEによりサービスエンジニアだけがサービスモードにおけるセキュリティ関連機能の操作を許可される制御が規定され、OE-N.SESSIONによってサービスモードにおけるセキュリティ管理機能の利用終了後にそのセッションを終了させるという運用が規定されている。

よってこの2つのセキュリティ対策方針が満たされることにより、組織のセキュリティ方針を十分実現している。

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 11　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.ACCESS-ADMIN	O.ACCESS-SECURE-PRINT	O.ACCESS-BOX	O.ACCESS-SERVICE	O.CONTROL-COPY	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.FEED-BACK	OE.SECURE-PRINT-QUALITY
FDP_ACC.1[1]		●								
FDP_ACC.1[2]			●							

セキュリティ対策方針 / セキュリティ機能要件	O.ACCESS-ADMIN	O.ACCESS-SECURE-PRINT	O.ACCESS-BOX	O.ACCESS-SERVICE	O.CONTROL-COPY	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.FEED-BACK	OE.SECURE-PRINT-QUALITY
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_SOS.1[1]								●		
FIA_SOS.1[2]						●				
FIA_SOS.1[3]							●			
FIA_UAU.2[1]								●		
FIA_UAU.2[2]								●		
FIA_UAU.2[3]						●				
FIA_UAU.2[4]							●			
FIA_UAU.6	●			●						
FIA_UAU.7						●	●	●		
FIA_UID.2[1]								●		
FIA_UID.2[2]								●		
FIA_UID.2[3]						●				
FIA_UID.2[4]							●			
FMT_MOF.1	●									
FMT_MSA.1[1]	●		●					●		
FMT_MSA.1[2]	●									
FMT_MSA.3[1]		●								
FMT_MSA.3[2]			●					●		
FMT_MSA.3[3]					●					
FMT_MTD.1[1]	●									
FMT_MTD.1[2]	●									
FMT_MTD.1[3]	●							●		
FMT_MTD.1[4]				●						
FMT_MTD.1[5]				●						
FMT_SMF.1	●		●	●				●		

セキュリティ対策方針 / セキュリティ機能要件	O.ACCESS-ADMIN	O.ACCESS-SECURE-PRINT	O.ACCESS-BOX	O.ACCESS-SERVICE	O.CONTROL-COPY	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.FEED-BACK	OE.SECURE-PRINT-QUALITY
FMT_SMR.1[1]			●					●		
FMT_SMR.1[2]			●					●		
FMT_SMR.1[3]	●									
FMT_SMR.1[4]				●						
FPT_RVM.1	＊	＊	＊	＊		＊	＊	＊		
FPT_SEP.1	＊	＊	＊	＊	＊	＊	＊	＊		
FTA_SSL.3[1]	●									
FTA_SSL.3[2]	●									
FIA_SOS.1[E]										●
FIA_UAU.7[E]									●	

※ *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要件であるが、上表“＊”印で示される関連付けられるセキュリティ対策方針より適用される機能要件をサポートする要件として適用される。このサポート関係（相互サポート）については、次々小項にて詳細を説明する。*

8.2.1.2. 十分性

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について以下に説明する。

- **O.ACCESS-ADMIN（管理者が操作する管理機能）**
  本セキュリティ対策方針は、管理者モードにて提供される管理機能に対するアクセスを規定しており、管理者機能を操作することが可能な主体、及び操作対象を規定する必要がある。これに対して以下の機能要件が適用される。

  ＜TSFデータに対する管理者機能＞
  不正使用防止機能は、FMT_MOF.1により管理者だけにその動作設定管理を制限している。

  管理者モードパスワードの変更操作は、FMT_MTD.1[1]、FMT_SMF.1により管理者だけに設定変更操作を制限している。管理者モードパスワードの変更操作は、セキュリティ管理上重要な操作になるため、FIA_UAU.6より利用に際して管理者であることを再認証する。

メモリリコール設定データの変更操作は、FMT_MSA.1[2]、FMT_SMF.1により管理者だけにデフォルト値変更、問い合わせ操作を制限している。

オートリセット動作設定データの変更操作は、FMT_MTD.1[1]、FMT_SMF.1により管理者だけに設定変更操作を制限している。

ボックス不正アクセス検出カウント値、親展プリント不正アクセス検出カウント値は、FMT_MTD.1[2]及びFMT_SMF.1により消去操作を行うことを管理者だけに制限している

ボックス識別子の変更は、FMT_MSA.1[1]、FMT_SMF.1よりボックスの正当な利用者である一般ユーザに加え、管理者も操作可能である。
ボックスパスワードの変更は、FMT_MTD.1[3]及びFMT_SMF.1によりボックスの正当な利用者である一般ユーザに加え、管理者も操作可能である。

FMT_SMR.1[3]により、上記説明されるセキュリティ管理機能を操作することが可能な役割として管理者が存在する。

＜管理者機能のアクセス時間制限＞
管理者機能にアクセス中、設定されるオートリセット動作設定データを越えて無操作状態が継続した場合に、FTA_SSL.3[1]、FTA_SSL.3[2]により管理者機能へのアクセス許可を遮断する。(万が一、管理者機能を利用中のままに放置してしまった場合でもアクセスを制限するため、管理者機能に対する利用制限がより厳しくなる。)

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実現される。

- **O.ACCESS-SECURE-PRINT（親展プリントジョブアクセス制御）**
本セキュリティ対策方針は、親展プリントジョブ情報データの印刷操作を制御することを規定しており、親展プリントジョブ作成時の制御、及び一般ユーザの親展プリントジョブに対するアクセス制御を実施することが必要になる。これに対して以下の機能要件が適用される。

親展プリントジョブの登録要求を受け付けると、FDP_ACC.1[1]及びFDP_ACF.1[1]により、親展プリントジョブを操作するプロセスより“新しく付与されるジョブID”が生成され、これを属性とする親展プリントジョブ情報データファイルを登録するアクセス制御が実施される。
また同機能要件により、親展プリントジョブを操作するプロセスに“一般ユーザが選択した親展プリントジョブのジョブID”が受け渡されると、これと一致する“ジョブID”を持つ親展プリントジョブ情報データを印刷するアクセス制御が実施される。

基本的に上記記載のFDP_ACC.1[1]、FDP_ACF.1[1]により本セキュリティ対策方針は満たされ

る。以下、説明される機能要件は、親展プリントジョブアクセス制御に関係する機能要件である。

セキュリティ属性として利用されるジョブIDのデフォルト値は、FMT_MSA.3[1]より他のジョブと区別され、一意識別される値が与えられる。

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実現される。

- **O.ACCESS-BOX（ボックスアクセス制御）**

本セキュリティ対策方針は、一般ユーザのボックスデータのダウンロード操作を制限することを規定しており、一般ユーザのボックス作成及びボックスへのアクセスを制御する規定が必要になる。これに対して以下の機能要件が適用される。

ボックスへのアクセス制御方針を定義するFDP_ACC.1[2]、FDP_ACF.1[2]により、ボックスを操作するプロセスは、入力した“ボックス識別子”と同じ名称のボックスが存在しない場合、これを属性とするボックスの作成操作を許可されるアクセス制御が実施される。（入力した“ボックス識別子”と同じ名称のボックスが存在する場合、作成操作は拒否される。）
更に同機能要件により、ボックスを操作するプロセスの保持する一般ユーザにより選択された“ボックス識別子”と一致する“ボックス識別子”を持つボックスに対して“ボックス内のボックスデータ読み出し”操作を許可されるアクセス制御が実施される。
また同機能要件は、“管理者識別子”を持つボックスを操作するプロセスが、すべてのボックスの“ボックス内のボックスデータ読み出し”操作が許可されるアクセス制御が実施される。
またすべてのボックスに対して“ボックス内にボックスデータ書き込み”操作を許可される。

基本的に上記記載のFDP_ACC.1[2]、FDP_ACF.1[2]により本セキュリティ対策方針は満たされる。以下、説明される機能要件は、ボックスアクセス制御に関係する機能要件群である。

セキュリティ属性として利用されるボックス識別子のデフォルト値は、FMT_MSA.3[2]より許可的な値であるブランク（NULL）が与えられる。この値は、ボックスを作成する一般ユーザが適切な初期値に設定することが可能である。
FMT_SMR.1[1]により、上記説明されるボックス識別子のブランクを適切な初期値に設定する役割として、当該ボックスを作成する一般ユーザが存在する。

ボックス識別子の変更は、FMT_MSA.1[1]、FMT_SMF.1よりボックスの正当な利用者である一般ユーザが操作可能である。
FMT_SMR.1[2]により、上記説明されるセキュリティ管理機能を操作することが可能な役割としてボックスの正当な利用者である一般ユーザが存在する。

以上、アクセス制御を規定する機能要件に加え、アクセス制御の管理に相当する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実現される。

- **O.ACCESS-SERVICE（サービスエンジニアが操作する管理機能）**
  本セキュリティ対策方針は、サービスモードにて提供されるサービスエンジニア向け管理機能に対するアクセスを規定しており、各セキュリティ管理機能を操作する可能な主体を規定する必要がある。これに対して以下の機能要件が適用される。

  サービスコードの変更操作は、FMT_MTD.1[4]及びFMT_SMF.1によりサービスエンジニアだけに設定変更操作を制限している。サービスコードの変更操作は、セキュリティ管理上重要な操作になるため、FIA_UAU.6より利用に際してサービスエンジニアであることを再認証する。

  管理者モードパスワードを初期化する操作は、FMT_MTD.1[5]及びFMT_SMF.1によりサービスエンジニアだけに制限されている。

  FMT_SMR.1[4]により、上記説明されるセキュリティ管理機能を操作することが可能な役割としてサービスエンジニアが存在する。

  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実現される。

- **O.CONTROL-COPY（コピー機能の動作制御）**
  本セキュリティ対策方針は、コピー機能を利用後にコピージョブ情報データが再印刷されないよう、印刷後に削除することを規定しており、コピージョブ印刷終了後の削除操作の制御が必要となる。これに対して以下の機能要件が適用される。

  FDP_ACC.1[3]、FDP_ACF.1[3]により、コピージョブを操作するプロセスは“メモリリコール設定データ”が“OFF”のコピージョブ情報データファイルに対して、印刷完了後に削除操作を実行するアクセス制御が実施される。

  基本的に上記記載の要件であるFDP_ACC.1[3]、FDP_ACF.1[3]により実現されるコピージョブアクセス制御によって本セキュリティ対策方針は満たされる。以下、説明される本セキュリティ対策方針に対応する機能要件は、コピージョブアクセス制御に寄与する機能要件、またはコピージョブアクセス制御を規定する機能要件を満たすために必要となる主として管理に関係する機能要件群である。

  > コピージョブアクセス制御に利用される属性である“メモリリコール設定データ”は、FMT_MSA.3[3]により、メモリリコールコピーをさせない制限的特性に相当する“OFF”がデフォルト値で与えられる。（この値を上書きする代替の初期値を与える役割は存在しない。）

  以上、コピージョブアクセス制御を規定する機能要件に加え、同アクセス制御の管理に相当する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実現される。

- **O.I&A-ADMIN（管理者の識別認証）**
  本セキュリティ対策方針は、管理者モードへアクセスする利用者が確かに管理者であることを認証することを規定しており、認証における適切な諸条件が必要になる。これに対して以下の機能要件が適用される。

  管理者モードにアクセスする利用者は、FIA_UID.2[3]、FIA_UAU.2[3]により管理者であると識別認証される。認証の際には、FIA_UAU.7により、管理者モードパスワードの入力フィードバックとして1文字データ入力毎に“＊”を返す。また認証において利用される管理者モードパスワードが8桁数字の品質を満たすことがFIA_SOS.1[2]により保証される。
  管理者モードに対するアクセスは、FIA_AFL.1[3]により、3回の管理者認証不成功を不正アクセスと判断し、それ以降の認証機能に対するアクセスをロックすることにより強固に保護される。

  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実現される。

- **O.I&A-SERVICE（サービスエンジニアの識別認証）**
  本セキュリティ対策方針は、サービスモードへアクセスする利用者が確かにサービスエンジニアであることを認証することを規定しており、認証における適切な諸条件が必要になる。これに対して以下の機能要件が適用される。

  サービスモードにアクセスする利用者は、FIA_UID.2[4]、FIA_UAU.2[4]によりサービスエンジニアであると識別認証される。認証の際には、FIA_UAU.7により、サービスコードの入力フィードバックとして1文字データ入力毎に“＊”を返す。また認証において利用されるサービスコードが8桁の数字、“＃”、“＊”の品質をみたすことがFIA_SOS.1[3]により保証される。
  サービスモードに対するアクセスは、FIA_AFL.1[4]により、3回のサービスエンジニア認証不成功を不正アクセスと判断し、それ以降の認証機能に対するアクセスをロックすることにより強固に保護される。

  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実現される。

- **O.I&A-USER（一般ユーザの識別認証）**
  本セキュリティ対策方針は、親展プリントジョブにアクセスする利用者が、親展プリントジョブの正当な利用者である一般ユーザであることを識別認証することを規定している。またボックスデータをダウンロードする利用者が、確かにボックスの正当な利用者である一般ユーザであることを識別認証することを規定しており、識別認証おける適切な諸条件が必要になる。これに対して以下の機能要件が適用される。

  ＜親展プリントジョブに対するアクセスにおける一般ユーザの識別認証＞
  FIA_UID.2[1]、FIA_UAU.2[1]により、アクセスする者が親展プリントジョブの正当な利用者

である一般ユーザであることを識別、認証する。（この認証において使用される親展プリントパスワードの認証強度は、OE.SECURE-PRINT-QUALITYにより保証される。本小項の後述参照。）
親展プリントジョブの正当な利用者である一般ユーザであることの認証において、FIA_UAU.7により、親展プリントパスワードの入力フィードバックとして1文字データ入力毎に“＊”を返す。
FIA_AFL.1[1]により各親展プリントジョブへの3回の不成功認証を不正アクセスと判断し、それ以降の親展プリントジョブの正当な利用者である一般ユーザに対する認証機能をロックする。ロックの解除は、O.ACCESS-ADMINに関連付けられるFMT_MTD.1[2]、FMT_SMF.1により解除可能である。

＜ボックスデータに対するアクセスにおける一般ユーザの識別認証＞
FIA_UID.2[2]、FIA_UAU.2[2]により、ボックスにアクセスする者がボックスの正当な利用者である一般ユーザであることを識別認証する。
上記、FIA_UAU.2[2]による各認証において、FIA_UAU.7により、ボックスパスワードの入力フィードバックとして1文字データ入力毎に“＊”を返す。
また認証において利用されるボックスパスワードが4～64桁の半角英数字、半角記号の品質を満たすことがFIA_SOS.1[1]により保証される。
FIA_AFL.1[2]により各認証において3回の不成功認証を不正アクセスと判断し、それ以降のボックスの正当な利用者である一般ユーザに対する認証機能ををロックする。
このロック状態は、O.ACCESS-ADMINに関連付けられるFMT_MTD.1[2]、FMT_SMF.1により解除可能である。

ボックスの正当な利用者である一般ユーザの識別に利用されるボックス識別子のデフォルト値は、FMT_MSA.3[2]より許可的な値であるブランク（NULL）が与えられる。この値は、ボックスを作成する一般ユーザだけが適切な初期値に設定可能である。
FMT_SMR.1[1]により、上記説明されるボックス識別子のブランクを適切な初期値に設定する役割として、当該ボックスを作成する一般ユーザが存在する。

ボックス識別子の変更は、FMT_MSA.1[1]、FMT_SMF.1よりボックスの正当な利用者である一般ユーザ、管理者が操作可能である。
ボックスパスワードの変更は、FMT_MTD.1[3]及びFMT_SMF.1によりボックスの正当な利用者である一般ユーザ、管理者が操作可能である。
FMT_SMR.1[2]により、上記説明されるセキュリティ管理機能を操作することが可能な役割としてボックスの正当な利用者である一般ユーザが存在する。

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実現される。

- **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、クライアントPC上のボックスユーティリティにおいてボックスパスワード、管理者モードパスワードの入力に対して適切なフィードバックを利用者に提供することを規定している。これに対して以下の機能要件が適用される。

FIA_UAU.7[E]により、クライアントPCのボックスユーティリティは、ボックスパスワード、管理者モードパスワードの入力フィードバックに“＊”を返す。

この機能要件により、本セキュリティ対策方針は実現される。

- **OE.SECURE-PRINT-QUALITY（親展プリントパスワードの品質尺度）**

本セキュリティ対策方針は、IT環境であるクライアントPCのプリンタドライバにおいて親展プリントをTOEの搭載されるMFPにスプールする際、強度の保証されたパスワードを親展プリントジョブ情報データに付加することが規定されている。

これに対してFIA_SOS.1[E]により、クライアントPCのプリンタドライバは、設定される親展プリントパスワードが4桁数字であることを検証する。よって親展プリントをMFPにスプールすると必ず4桁のパスワードが付与されることになる。

この機能要件により、本セキュリティ対策方針は実現される。

8.2.1.3. 相互サポート

(1) 補完性について

直接セキュリティ対策方針と対応関係を持たず、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 12 IT セキュリティ機能要件の相互サポート関係

N/A：Not Applicable

IT セキュリティ機能要件	他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント			
	①迂回防止	②干渉、破壊防止	③非活性化防止	④無効化検出
FDP_ACC.1[1]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACC.1[2]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACC.1[3]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[1]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[2]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[3]	N/A	FPT_SEP.1	N/A	N/A
FIA_AFL.1[1]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[2]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.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[3]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_SOS.1[1]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[2]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[3]	N/A	FPT_SEP.1	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[2]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_UAU.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.6	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[1]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[2]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FMT_MOF.1	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[4]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[5]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMF.1	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[4]	N/A	FPT_SEP.1	N/A	N/A
FPT_RVM.1	N/A	FPT_SEP.1	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A	N/A
FTA_SSL.3[1]	N/A	FPT_SEP.1	N/A	N/A
FTA_SSL.3[2]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[E]	N/A	N/A	N/A	N/A
FIA_UAU.7[E]	N/A	N/A	N/A	N/A

① 迂回防止

TSP 実施機能とは、以下となる。

- 親展プリントジョブに対するアクセス制御機能の動作進行を許可する前に作動すべき機能である親展プリントジョブへアクセスするための識別認証機能（FIA_UID.2[1]、FIA_UAU.2[1]、FIA_UAU.7、FIA_AFL.1[1]により実施される。）
- ボックスデータに対するアクセス制御機能及び一般ユーザが操作するボックスの設定管理（ボックスパスワードの変更、ボックス識別子の変更）の動作進行を許可する前に作動すべき機能であるボックスの正当な利用者である一般ユーザを認証する機能（FIA_UID.2[2]、FIA_UAU.2[2]、FIA_UAU.7、FIA_AFL.1[2]により実施される。）
- 管理者モードにおけるセキュリティ管理機能、ボックスデータに対するアクセス制御機能の動作進行を許可する前に作動すべき機能である管理者を識別認証する機能（FIA_UID.2[3]、FIA_UAU.2[3]、FIA_UAU.7、FIA_AFL.1[3]により実施される。）
- 管理者モードのセキュリティ管理機能の中でも管理者モードパスワード変更機能の動作進行を許可する前に作動すべき機能である管理者再認証機能（FIA_UAU.2[3]、FIA_UAU.6、FIA_UAU.7、FIA_AFL.1[3]により実施される。）
- サービスモードにおけるセキュリティ管理機能の動作進行を許可する前に作動すべき機能であるサービスエンジニアを識別認証する機能（FIA_UID.2[4]、FIA_UAU.2[4]、FIA_UAU.7、FIA_AFL.1[4]により実施される。）
- サービスモードのセキュリティ管理機能の中でもサービスコード変更機能の動作進行を許可する前に作動すべき機能であるサービスエンジニア再認証機能（FIA_UAU.2[4]、FIA_UAU.6、FIA_UAU.7、FIA_AFL.1[4]により実施される。）

以上、TSP 実施機能は、すべて FPT_RVM.1 により必ず呼び出されて成功することがサポートされる。

② 干渉・破壊防止

TOE は、FPT_SEP.1 を実現するため、

- 親展プリントジョブアクセス制御実施中のセキュリティドメイン
- ボックスのセキュリティドメイン
- コピージョブアクセス制御実施中のセキュリティドメイン
- 管理者モードにおけるセキュリティドメイン
- サービスモードにおけるセキュリティドメイン

が保持される。よって信頼されないサブジェクトによる TOE の保護する資源範囲及び TSF の動作範囲であるセキュリティドメインは、干渉・改ざんを受けないことがサポートされる。

③ 非活性化防止

以下の機能要件の動作管理は、FMT_MOF.1 により管理者だけに制限されており、非活性化を狙った攻撃に対する防御を提供している。

- 認証不成功時の検出・ロック（FIA_AFL.1[1]、FIA_AFL.1[2]、FIA_AFL.1[3]）及びボックスへアクセスする際の認証(FIA_UAU.2[2])

④ 無効化検出

無効化検出に関するセキュリティまで考慮しなくても、既に迂回防止や干渉破壊防止などを考慮して適用しているセキュリティ機能要件が存在するため、求められるセキュリティ対策方針を十分に満たすセキュリティ機能要件の構造となっている。従ってセキュリティ機能を無効化する攻撃を検出するためのセキュリティ機能要件を適用しない。

(2) 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
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[1]、FMT_MSA.3[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[3]
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1] ＜補足＞ FIA_UAU.2 は、FIA_UAU.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2] ＜補足＞ FIA_UAU.2 は、FIA_UAU.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[3] ＜補足＞ FIA_UAU.2 は、FIA_UAU.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4] ＜補足＞ FIA_UAU.2 は、FIA_UAU.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[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
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FIA_UAU.6	なし	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1] 、 FIA_UAU.2[2] 、 FIA_UAU.2[3] 、 FIA_UAU.2[4]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[3]
FMT_MSA.1[1]	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1[2] 、 FMT_SMF.1 、 FMT_SMR.1[2] 、 FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1[3]、FMT_SMF.1、FMT_SMR.1[3]
FMT_MSA.3[1]	FMT_MSA.1 FMT_SMR.1	なし ＜①FMT_MSA.1、②FMT_SMR.1 を満たさない理由＞ ①ジョブ ID は、他のジョブと区別するために付与される識別子であり、デフォルト値変更、削除等の操作を可能である必要性がない。またジョブ ID には秘匿性もないため、問い合わせ操作を行う利用者を制限する必要性もない。 ②ジョブ ID は、他のジョブと区別するために付与される識別子であり、代替の初期値に変更する必要性がないため、これに基づいて指定される役割を規定する必要性もない。

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FMT_MSA.3[2]	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1[1]、FMT_SMR.1[1]
FMT_MSA.3[3]	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1[2] ＜FMT_SMR.1 を満たさない理由＞ メモリリコール設定データは、管理者が設定管理しており、コピー機能の利用に伴って生成されるオブジェクトのセキュリティ属性初期値を変更する必要性はない。
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[3]
FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[4]
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	なし ＜FIA_UID.1 を満たさない理由＞ ボックス作成は、任意の一般ユーザに許可されているため、本役割に関連付けられる利用者を識別する必要はない。
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FMT_SMR.1[4]	FIA_UID.1	A_UID.2[4] ＜補足＞ FIA_UID.2 は、FIA_UID.1 の上位コンポーネントになるため、依存性が満たされていることになる。
FPT_RVM.1	なし	N/A
FPT_SEP.1	なし	N/A
FTA_SSL.3[1]	なし	N/A
FTA_SSL.3[2]	なし	N/A
FIA_SOS.1[E]	なし	N/A
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[2]、FIA_UAU.2[3]

以上、(1) 補完性及び(2) IT セキュリティ機能要件の依存性で示される通り、IT セキュリティ要件のセットは、全体として相互サポートする構造となっている。

8.2.2. 最小機能強度根拠

本 TOE の搭載される MFP は、入室管理が実施されている一般的なオフィス環境において設置され、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、3.2 節にて明確化されている TOE の利用者でもある一般利用者及びオフィス内にいる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。

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 14 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-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
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_SOS.1[1]		●					●		
FIA_SOS.1[2]	●								
FIA_SOS.1[3]					●				
FIA_UAU.2[1]				●					
FIA_UAU.2[2]						●	●	●	
FIA_UAU.2[3]	●	●							●
FIA_UAU.2[4]					●				
FIA_UAU.6	●				●				
FIA_UAU.7	●	●		●	●	●	●	●	●
FIA_UID.2[1]				●					
FIA_UID.2[2]						●	●	●	
FIA_UID.2[3]	●	●							●
FIA_UID.2[4]					●				

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
FMT_MOF.1	●								
FMT_MSA.1[1]		●					●		
FMT_MSA.1[2]	●	●							
FMT_MSA.3[1]				●					
FMT_MSA.3[2]							●		
FMT_MSA.3[3]			●						
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●								
FMT_MTD.1[3]		●					●		
FMT_MTD.1[4]					●				
FMT_MTD.1[5]					●				
FMT_SMF.1	●	●			●		●		
FMT_SMR.1[1]							●		
FMT_SMR.1[2]							●		
FMT_SMR.1[3]	●	●							
FMT_SMR.1[4]					●				
FPT_RVM.1	●	●		●	●	●	●	●	●
FPT_SEP.1	●	●	●	●	●	●	●	●	●
FTA_SSL.3[1]	●								
FTA_SSL.3[2]		●							

8.3.1.2. 十分性

TOE セキュリティ機能要件に対する TOE セキュリティ機能について説明する。

- **FDP_ACC.1[1]**

  FDP_ACC.1[1]は、オブジェクトである親展プリントジョブ情報データ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.SECURE-PRINTは、サブジェクト：「親展プリントジョブを操作するプロセス」のオブジェクト：「親展プリントジョブ情報データファイル」に対する操作：「印刷」及び「登録」を制御する「親展プリントジョブアクセス制御」を実施している。

  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ボックスに対して制御されるサブジェクト、操作の関係を規定している。

  F.BOX-PANELは、サブジェクト：「ボックスを操作するプロセス」のオブジェクト：「ボックス」に対する操作：「ボックス内のボックスデータ読み出し」を制御する「ボックスアクセス制御」を実施している。（読み出されたボックスデータは、E-mail送信、またはFTP送信される。）

  F.BOX-PCは、サブジェクト：「ボックスの正当な利用者である一般ユーザを代行するプロセス」のオブジェクト：「ボックスデータファイル」に対する操作：「「ボックス内のボックスデータ読み出し」及び「作成」を制御する「ボックスアクセス制御」を実施している。（読み出しされたボックスデータは、クライアントPCにダウンロードされる。）

  F.BOX-UTILITY-1は、サブジェクト：「ボックスを操作するプロセス」のオブジェクト：「ボックス」に対する操作：「ボックス内のボックスデータ読み出し」を制御する「ボックスアクセス制御」を実施している。（読み出されたボックスデータは、クライアントPCにダウンロードされ、ボックスユーティリティ上で、サムネイル表示、プレビュー表示など様々な形式で表示される。）

  F.BOX-UTILITY-2は、サブジェクト：「ボックスを操作するプロセス」のオブジェクト：「ボックス」に対する操作：「ボックス内のボックスデータ読み出し」及び「ボックス内にボックスデータ書き込み」を制御する「ボックスアクセス制御」を実施している。（すべてのボックスのボックス内ボックスデータが読み出され、クライアントPCにダウンロードされる。またはクライアントPCより任意のボックス内にボックスデータを書き込める。）

  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コピージョブ情報データ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.COPYは、サブジェクト：「コピージョブを操作するプロセス」のオブジェクト：「コピージョブ情報データファイル」に対する操作：「削除」を制御する「コピージョブアクセス制御」を実施している。

  従って本機能要件は満たされる。

- **FDP_ACF.1[1]**

  FDP_ACF.1[1]は、制御されるサブジェクト：「親展プリントジョブを操作するプロセス」、オブジェクト：「親展プリントジョブ情報データファイル」、操作：「印刷」及び「登録」の規則を規定している。

  F.SECURE-PRINTは、親展プリントジョブの登録要求を受け付けると、新しく付与される“ジョブID”を生成し、これを属性とする親展プリントジョブ情報データを登録する。

  また同機能は、識別認証されて一般ユーザが選択した親展プリントジョブの“ジョブID”を持つ親展プリントジョブを操作するプロセスが、これと一致する“ジョブID”を持つ親展プリントジョブ情報データファイルに対して印刷操作が許可される制御を実施している。

  従って本機能要件は満たされる。

- **FDP_ACF.1[2]**

  FDP_ACF.1[2]は、制御されるサブジェクト：「ボックスを操作するプロセス」、オブジェクト：「ボックス」、操作：「ボックス内のボックスデータ読み出し」及び「作成」の規則を規定している。

  F.BOX-PANELは、一般ユーザが選択した“ボックス識別子”を持つボックスを操作するプロセスが、これと一致する“ボックス識別子”を持つボックスに対してボックス内のボックスデータ読み出し操作を許可されるボックスアクセス制御を実施している。

  F.BOX-PCは、以下の3つの規則からなるボックスアクセス制御を実施している。

  - 一般ユーザが選択した“ボックス識別子”を持つボックスを操作するプロセスが、これと一致する“ボックス識別子”を持つボックスに対してボックス内のボックスデータ読み出し操作を許可される。
  - 入力された“ボックス識別子”を持つボックスを操作するプロセスが、これと一致する“ボックス識別子”を持つボックスが存在しない場合、入力された“ボックス識別子”をオブジェクト属性とするボックスの作成操作を許可される。
  - 入力された“ボックス識別子”を持つ、ボックスを操作するプロセスが、これと一致する“ボックス識別子”を持つボックスが存在する場合、入力された“ボックス識別子”をオブジェクト属性とするボックスの作成操作を拒否される制御を実施している。

  F.BOX-UTILITY-1は、一般ユーザが選択した“ボックス識別子”を持つボックスを操作するプロセスが、これと一致する“ボックス識別子”を持つボックスに対してボックス内のボックスデータ読み出し操作を許可されるボックスアクセス制御を実施している。

  F.BOX-UTILITY-2は、以下の2つの規則からなるボックスアクセス制御を実施している。

  - “管理者識別子”を持つボックスを操作するプロセスが、すべてのボックスに対してボックス内のボックスデータ読み出し操作を許可される。
  - “管理者識別子”を持つボックスを操作するプロセスが、すべてのボックスに対してボックス内にボックスデータ書き込み操作を許可される。

  従って本機能要件は満たされる。

- **FDP_ACF.1[3]**

  FDP_ACF.1[3]は、制御されるサブジェクト：「コピージョブを操作するプロセス」、オブジェクト：「コピージョブ情報データファイル」、操作：「削除」の規則を規定している。

  F.COPYは、コピージョブを操作するプロセスにより、メモリリコール設定データがOFFであるコピージョブ情報データファイルを印刷完了後に削除するアクセス制御を実施している。

  従って本機能要件は満たされる。

- **FIA_AFL.1[1]**

  FIA_AFL.1[1]は、親展プリントジョブ情報データに関係する認証事象の一定回数の不成功認証試行が生じた際にその不正アクセスを検出すること、不正アクセスが検出されて何らかのアクションが実行された後に通常復帰するための方法を規定している。

  F.SECURE-PRINTは、親展プリントジョブ情報データに対するアクセスための認証において、

3回の不成功試行を検知した場合に認証機能をロックする。F.ADMIN-PANELの提供するアクセス不可状態解除機能を実行することにより解除される。
従って本機能要件は満たされる。

- **FIA_AFL.1[2]**

  FIA_AFL.1[2]は、ボックスデータに関係する認証事象の一定回数の不成功認証試行が生じた際にその不正アクセスを検出すること、不正アクセスが検出されて何らかのアクションが実行された後に通常復帰するための方法を規定している。
  F.BOX-PANELは、ボックスへのアクセスにおける認証において、3回の不成功試行を検知した場合に各認証機能をロックする。このロック状態は、F.ADMIN-PANELの提供するアクセス不可状態解除機能を実行することにより解除される。
  F.BOX-PCは、ボックスへのアクセスにおける認証において、3回の不成功試行を検知した場合に各認証機能をロックする。このロック状態は、F.ADMIN-PANELの提供するアクセス不可状態解除機能を実行することにより解除される。
  F.BOX-UTILITY-1は、ボックスへのアクセスにおける認証において、3回の不成功試行を検知した場合に各認証機能をロックする。このロック状態は、F.ADMIN-PANELの提供するアクセス不可状態解除機能を実行することにより解除される。
  従って本機能要件は満たされる。

- **FIA_AFL.1[3]**

  FIA_AFL.1[1]は、管理者モードに関係する認証事象の一定回数の不成功認証試行が生じた際にその不正アクセスを検出すること、不正アクセスが検出されて何らかのアクションを実行することを規定している。
  F.ADMIN-PANELは、管理者モードにアクセスするための認証、または管理者モードパスワードの変更機能における再認証において、3回の不成功試行を検知した場合に認証機能をロックする。（管理者モードパスワードの変更機能における再認証の場合は、管理者モードへのアクセスを拒否した上で、管理者モードへアクセスするための認証機能をロックする。）なお、このロック状態を解除するための機能は存在しない。
  F.ADMIN-PCは、管理者モードにアクセスするための認証において、3回の不成功試行を検知した場合に認証機能をロックする。なお、このロック状態を解除するための機能は存在しない。
  F.BOX-UTILITY-2は、ボックスデータのバックアップ操作、リストア操作要求における認証において、3回の不成功試行を検知した場合に認証機能をロックする。なお、このロック状態を解除するための機能は存在しない。
  従って本機能要件は満たされる。

- **FIA_AFL.1[4]**

  FIA_AFL.1[4]は、サービスエンジニアの認証において一定回数の不成功認証試行が生じた際にその不正アクセスを検出すること、不正アクセスが検出されて何らかのアクションを実行することを規定している。
  F.SERVICEは、サービスモードにアクセスするための認証、またはサービスコードの変更機能

における再認証において、3回の不成功試行を検知した場合に認証機能をロックする。（サービスコードの変更機能における再認証の場合は、サービスモードへのアクセスを拒否した上で、サービスモードへアクセスするための認証機能をロックする。）なお、このロック状態を解除するための機能は存在しない。
従って本機能要件は満たされる。

- **FIA_SOS.1[1]**
  FIA_SOS.1[1]は、ボックスパスワードの品質尺度として最小4桁、最大64桁の半角英数字、半角記号を規定している。
  F.BOX-PCは、ボックスパスワードの変更機能にてボックスパスワードの品質尺度に4～64桁且つASCIIコード0x20～0x7E（半角英数字・半角記号、95種）が設定されることをチェックしている。
  F.ADMIN-PCは、ボックスパスワードの変更機能にてボックスパスワードの品質尺度に4～64桁且つASCIIコード0x20～0x7E（半角英数字・半角記号、95種）が設定されることをチェックしている。
  従って本機能要件は満たされる。

- **FIA_SOS.1[2]**
  FIA_SOS.1[2]は、管理者モードパスワードの品質尺度として8桁の数字を規定している。
  F.ADMIN-PANELは、管理者モードパスワードの品質尺度に8桁数字が設定されることをチェックしている。
  従って本機能要件は満たされる。

- **FIA_SOS.1[3]**
  FIA_SOS.1[3]は、サービスコードの品質尺度として8桁で数字、“＊”、“＃”を規定している。
  F.SERVICEは、サービスコードの変更機能にてサービスコードの品質尺度に8桁数字、“＊”、“＃”が設定されることをチェックしている。
  従って本機能要件は満たされる。

- **FIA_UAU.2[1]**
  FIA_UAU.2[1]は、一般ユーザの親展プリントジョブ情報データに対するアクセスにおいて、親展プリントジョブの正当な利用者である一般ユーザを認証することを規定している。
  F.SECURE-PRINTは、親展プリントジョブ情報データに対するアクセスにおいて親展プリントジョブの正当な利用者である一般ユーザを親展プリントパスワードより認証し、認証された親展プリントジョブの正当な利用者である一般ユーザだけに対象としている親展プリントジョブ情報データに対して利用可能な操作の実行を許可している。
  従って本機能要件は満たされる。

- **FIA_UAU.2[2]**
  FIA_UAU.2[2]は、一般ユーザのボックスに対するアクセスにおいて、ボックスの正当な利用者

である一般ユーザを認証することを規定している。
F.BOX-PANELは、ボックスの正当な利用者である一般ユーザをボックスパスワードより認証し、認証されたボックスの正当な利用者である一般ユーザだけに、対象としているボックスへのアクセスを許可している。
F.BOX-PCは、ボックスの正当な利用者である一般ユーザをボックスパスワードより認証し、認証されたボックスの正当な利用者である一般ユーザだけに、対象としているボックスへのアクセスを許可している。
F.BOX-UTILITY-1は、ボックスの正当な利用者である一般ユーザをボックスパスワードより認証し、認証されたボックスの正当な利用者である一般ユーザだけに、対象としているボックスへのアクセスを許可している。
従って本機能要件は満たされる。

- **FIA_UAU.2[3]**

FIA_UAU.2[3]は、管理者機能を利用する前に管理者を認証することを規定している。
F.ADMIIN-PCは、管理者モードに対するアクセスにおいて管理者を認証し、認証された管理者だけに管理者モードに対して利用可能な操作の実行を許可している。
F.ADMIN-PANELは、管理者モードに対するアクセスにおいて管理者を認証し、認証された管理者だけに管理者モードに対して利用可能な操作の実行を許可している。また管理者モードにおけるセキュリティ管理機能である管理者モードパスワード変更機能の実行の前にも管理者を認証（再認証）している。
F.BOX-UTILITY-2は、ボックスデータのバックアップ操作、リストア操作に伴い管理者を認証し、認証された管理者だけバックアップ操作、リストア操作の実行を許可している。
従って本機能要件は満たされる。

- **FIA_UAU.2[4]**

FIA_UAU.2[4]は、サービスエンジニア機能を利用する前にサービスエンジニアを認証することを規定している。
F.SERVICEは、サービスモードに対するアクセスにおいてサービスエンジニアを認証し、認証されたサービスエンジニアだけにサービスモードにおいて利用可能なセキュリティ機能の操作の実行を許可している。またサービスモードにおけるセキュリティ管理機能であるサービスコード変更機能の実行の前にもサービスエンジニアを認証（再認証）している。
従って本機能要件は満たされる。

- **FIA_UAU.6**

FIA_UAU.6は、再認証が必要とされる認証事象について規定している。
F.ADMIN-PANELは、既に管理者モードに対してアクセスを許可された管理者に対してセキュリティ的に重要な機能である管理者モードパスワード変更機能において管理者を再認証し、再認証された管理者だけに管理者モードパスワード変更機能の実行を許可している。
F.SERVICEは、既にサービスモードに対してアクセスを許可されたサービスエンジニアに対してセキュリティ的に重要な機能であるサービスコード変更機能においてサービスエンジニアを

再認証し、再認証されたサービスエンジニアだけにサービスコード変更機能の実行を許可している。
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.SECURE-PRINTは、親展プリントジョブ情報データに対するアクセスにおいて、認証のための文字入力（親展プリントパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.BOX-PANELは、ボックスに対するアクセスにおいて、認証のための文字入力（ボックスパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.BOX-PCは、ボックスに対するアクセスにおいて、認証のための文字入力（ボックスパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.BOX-UTILITY-1は、ボックスに対するアクセスにおいて、認証のための文字入力（ボックスパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.BOX-UTILITY-2は、ボックスデータのバックアップ操作、リストア操作要求におけるアクセスにおいて、認証のための文字入力（管理者モードパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.ADMIN-PANELは、以下の場合に入力される文字のフィードバックとして1文字毎に“＊”を返す。

- 管理者モードに対するMFP本体操作パネルからのアクセスにおける認証機能において入力する文字
- 管理者モードパスワードを変更する際の再認証機能において入力される文字

F.ADMIN-PCは、管理者モードに対するクライアントPCからのアクセスにおいて、認証のための文字入力（管理者モードパスワード）のフィードバックには、1文字毎に“＊”を返す。
F.SERVICEは、以下の場合に入力される文字のフィードバックとして1文字毎に“＊”を返す。

- サービスモードに対するアクセスにおけるサービスコードを用いた認証機能において入力する文字
- サービスコードを変更する際の再認証機能において入力される文字

従って本機能要件は満たされる。

- **FIA_UID.2[1]**

FIA_UID.2[1]は、一般ユーザの親展プリントジョブ情報データに対するアクセスにおいて親展プリントジョブの正当な利用者を識別することを規定している。
F.SECURE-PRINTは、親展プリントジョブ情報データに対するアクセスにおいて親展プリントジョブの名称を基に、一般ユーザが操作対象とする親展プリントジョブを選択することによって親展プリントジョブの正当な利用者である一般ユーザを識別する。
従って本機能要件は満たされる。

- **FIA_UID.2[2]**

FIA_UID.2[2]は、ボックスを扱う一般ユーザをそのボックスの正当な利用者として識別するこ

とを規定している。
F.BOX-PANELは、ボックスデータに対するアクセスにおいて設定されるボックス識別名称を選択することによってボックスの正当な利用者である一般ユーザを識別する。
F.BOX-PCは、ボックスデータに対するアクセスにおいて設定されるボックス識別名称を選択することによってボックスの正当な利用者である一般ユーザを識別する。
F.BOX-UTILITY-1は、ボックスデータに対するアクセスにおいて設定されるボックス識別名称を選択することによってボックスの正当な利用者である一般ユーザを識別する。
従って本機能要件は満たされる。

- **FIA_UID.2[3]**
  FIA_UID.2[3]は、管理者機能を利用する前に利用者を管理者として識別することを規定している。
  F.ADMIN-PANELは、利用者の管理者モードに対するアクセス要求をもってその利用者を管理者として識別する。
  F.ADMIN-PCは、利用者の管理者モードに対するアクセス要求をもってその利用者を管理者として識別する。
  F.BOX-UTILITY-2は、ボックスデータのバックアップ操作、リストア操作の要求をもってその利用者を管理者として識別する。
  従って本機能要件は満たされる。

- **FIA_UID.2[4]**
  FIA_UID.2[4]はサービスエンジンにア機能を利用する前に利用者をサービスエンジニアとして識別することを規定している。
  F.SERVICEは、利用者のサービスモードに対するアクセス要求（公開されない操作手順の実行）をもってその利用者をサービスエンジニアとして識別する。
  従って本機能要件は満たされる。

- **FMT_MOF.1**
  FMT_MOF.1は、管理者が、不正使用防止機能のふるまいを管理することを規定している。
  F.ADMIN-PANELは、不正使用防止機能を動作・停止させる設定管理機能を提供している。
  従って本機能要件は満たされる。

- **FMT_MSA.1[1]**
  FMT_MSA.1[1]は、ボックスアクセス制御において使用されるセキュリティ属性であるボックス識別子の改変操作を“ボックスの正当な利用者である一般ユーザ”と管理者に制限することを規定している。
  F.ADMIN-PCは、管理者モードにてボックス識別子を改変する機能を提供する。
  F.BOX-PCは、ボックスに対してアクセスを許可された正当な利用者である一般ユーザが操作するボックス識別子を改変する機能を提供する。
  従って本機能要件は満たされる。

- **FMT_MSA.1[2]**

  FMT_MSA.1[2]は、コピージョブアクセス制御において使用されるセキュリティ属性であるメモリリコール設定データのデフォルト値変更、問い合わせを管理者に制限することを規定している。
  F.ADMIN-PANELは、メモリリコール設定データを問い合わせ、変更（デフォルト値変更）する機能を提供する。
  F.ADMIN-PCは、管理者モードにてメモリリコール設定データを問い合わせ、変更（デフォルト値変更）する機能を提供する。
  従って本機能要件は満たされる。

- **FMT_MSA.3[1]**

  FMT_MSA.3[1]は、親展プリントアクセス制御において使用されるセキュリティ属性であるジョブIDが生成された際の初期値と初期値を上書きする役割を規定している。
  F.SECURE-PRINTは、親展プリントがMFPにスプールされると他のジョブと区別され、一意に識別することが可能な値を当該親展プリントジョブに付与する。一旦生成されたジョブIDは変更される必要性がないため、ジョブIDを改変する役割は存在しない。
  従って本機能要件は満たされる。

- **FMT_MSA.3[2]**

  FMT_MSA.3は、ボックスアクセス制御において使用されるセキュリティ属性であるボックス識別子が生成される時の許可的なデフォルト値の規定している。またデフォルト値を代替する初期値を設定する役割を、当該ボックスを作成する一般ユーザに制限することを規定している。
  F.BOX-PCは、ボックスの作成機能が起動されると、ボックス識別子のデフォルト値としてブランク（NULL）を提供し、当該ボックスを作成する一般ユーザに対してブランクの代替初期値を設定させるボックス識別子作成機能を提供している。
  従って本機能要件は満たされる。

- **FMT_MSA.3[3]**

  FMT_MSA.3[3]は、コピージョブアクセス制御において使用されるセキュリティ属性であるメモリリコール設定データが生成された際の初期値と初期値を上書きする役割を規定している。
  F.COPYは、コピーの実行において生成されるコピージョブ情報データファイルに対して、制限的特性に相当する“OFF”（メモリリコールしない）にセットされたメモリリコール設定データを付与する。
  従って本機能要件は満たされる。

- **FMT_MTD.1[1]**

  FMT_MTD.1[1]は、管理者モードパスワード、オートリセット動作設定データを改変する役割を規定している。
  F.ADMIN-PANELは、MFP本体操作パネルからアクセスする管理者モードにて管理者モードパスワードを変更する機能を提供している。またオートリセット動作設定データを変更する機能を

提供している。
F.ADMIN-PCは、クライアントPCからアクセスする管理者モードにてオートリセット動作設定データを変更する機能を提供している。
従って本機能要件は満たされる。

- **FMT_MTD.1[2]**
  FMT_MTD.1[2]は、親展プリント不正アクセス検出カウント値、ボックス不正アクセス検出カウント値を消去する役割を規定している。
  F.ADMIN-PANELは、管理者モードにて管理者が操作するアクセス不可状態解除機能を提供している。この機能により、各親展プリントジョブの不正アクセス検出カウント値、または各ユーザボックスの不正アクセス検出カウント値を0クリアする。
  従って本機能要件は満たされる。

- **FMT_MTD.1[3]**
  FMT_MTD.1[3]は、ボックスパスワードを改変する役割を規定している。
  F.ADMIN-PCは、管理者モードにて管理者が操作するボックスパスワードを変更する機能を提供している。
  F.BOX-PCは、ボックスの正当な利用者である一般ユーザが操作するボックスパスワードを変更する機能を提供している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[4]**
  FMT_MTD.1[4]はサービスコードを改変する役割を規定している。
  F.SERVICEは、サービスモードにてサービスエンジニアが操作するサービスコードの変更機能を提供している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[5]**
  FMT_MTD.1[5]は、管理者モードパスワードを初期化する役割を規定している。
  F.SERVICEは、サービスモードにてサービスエンジニアが操作する管理者モードパスワード初期化機能を提供する。本機能が実行されると管理者モードパスワードはセットアップ時の初期値が設定される。

- **FMT_SMF.1**
  FMT_SMF.1は、TOEが提供するセキュリティ管理機能を規定している。
  F.BOX-PCは、ボックスの正当な利用者である一般ユーザがボックスに対して操作する以下のセキュリティ管理機能を提供する。
  - 当該ボックスのボックス識別子の変更機能
  - 当該ボックスのボックスパスワードの変更機能

  またF.BOX-PCは、ボックスの作成において、当該ボックスを作成する一般ユーザに以下のセキ

ュリティ管理機能を提供する。

- ボックス識別子の作成機能

F.ADMIN-PANELは、管理者が管理者モードにて操作する以下のセキュリティ管理機能を提供する。

- 不正使用防止機能の動作設定機能
- 親展プリント不正アクセス検出カウント値を0クリアするアクセス不可状態解除機能
- ボックス不正アクセス検出カウント値を0クリアするアクセス不可状態解除機能
- 管理者モードパスワードを変更する機能
- オートリセット動作設定データの設定管理機能
- メモリリコール設定データの設定管理機能

F.ADMIN-PCは、管理者が管理者モードにて操作する以下のセキュリティ管理機能を提供する。

- 任意のボックスにおけるボックス識別子の変更機能
- 任意のボックスにおけるボックスパスワードの変更機能
- オートリセット動作設定データの設定管理機能
- メモリリコール設定データの設定管理機能

F.SERVICEは、サービスエンジニアがサービスモードにて操作する以下のセキュリティ管理機能を提供する。

- サービスコードを変更する機能
- 管理者モードパスワードの初期化機能

従って本機能要件は満たされる。

- **FMT_SMR.1[1]**

FMT_SMR.1[1]は、役割に「当該ボックスを作成する一般ユーザ」を持つことを規定している。
F.BOX-PCは、ユーザボックスの作成においてユーザボックス作成機能の起動を掛ける利用者を「当該ユーザボックスを作成する一般ユーザ」として認識する。
従って本機能要件は満たされる。

- **FMT_SMR.1[2]**

FMT_SMR.1[2]は、役割に「ユーザボックスの正当な利用者である一般ユーザ」を持つことを規定している。
F.BOX-PCは、当該ユーザボックスへのアクセスに対し、識別認証された利用者を「当該ユーザボックスの正当な利用者である一般ユーザ」として認識する。従って本機能要件は満たされる。

- **FMT_SMR.1[3]**

FMT_SMR.1[3]は、役割に「管理者」を持つことを規定している。
F.ADMIN-PANELは、管理者モードへのアクセスに対し、認証された利用者を「管理者」として認識する。
F.ADMIN-PCは、管理者モードへのアクセスに対し、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[4]**

  FMT_SMR.1[4]は、役割に「サービスエンジニア」を持つことを規定している。
  F.SERVICEは、サービスモードへのアクセスに対し、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。

- **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-PANEL、F.ADMIN-PCは、管理者モードにおけるセキュリティ管理機能が操作可能になる前に、必ず管理者モードにアクセスする利用者が管理者であることを認証する機能が動作する。またF.ADMIN-PANELにて提供される管理者モードパスワード変更機能は、その実行が許可される前に、管理者であることを再認証する機能が動作する。F.BOX-UTILITY-2にて提供されるボックスデータのバックアップ機能及びリストア機能は、操作が許可される前に、管理者であることを認証する機能が動作する。これら認証機能は、各セキュリティ機能の動作進行が許可される前に作動するTSP実施機能であり、必ず動作する仕組みになっている。
  F.SECURE-PRINTは、親展プリントジョブ情報データファイルの印刷が許可される前に必ず、印刷対象となる親展プリントジョブ情報データファイルの正当な利用者である一般ユーザであることを識別、認証する機能が動作する。この識別認証機能は、親展プリントアクセス制御機能が動作して印刷操作が許可される前に作動するTSP実施機能であり、必ず動作する仕組みになっている。
  F.SERVICEは、サービスモードにおけるセキュリティ管理機能が操作可能になる前に必ずサービスモードに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機能が動作する。また同じくF.SERVICEにて提供されるサービスコード変更機能は、その実行が許可される前に、サービスエンジニアであることを再認証する機能が動作する。これら認証機能は、各セキュリティ機能の動作進行が許可される前に作動するTSP実施機能であり、必ず動作する仕組みになっている。
  F.BOX-PANEL、F.BOX-PC、F.BOX-UTILITY-1は、ボックスにアクセスを許可する前に必ず、操作対象であるボックスの正当な利用者である一般ユーザであることを識別、認証する機能が動作する。ボックスへアクセスする際の識別認証機能はボックスアクセス制御機能が動作してボックス内のボックスデータ読み出し操作が許可される前に作動するTSP実施機能であり、必ず動作する仕組みになっている。
  従って識別されるすべてのTOEセキュリティ機能が制御される各機能の動作進行が許可される前に必ず各TSP実施機能を呼び出すため、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-PANELにおいて管理者識別認証後に保持されるセキュリティドメインである管理者モードは、信頼されないサブジェクトから干渉されることはない。
F.ADMIN-PCにおいて管理者識別認証後に保持されるセキュリティドメインである管理者モードは、信頼されないサブジェクトから干渉されることはない。
F.COPYにおいてコピージョブアクセス制御の実行中に保持されるセキュリティドメインは信頼されないサブジェクトから干渉されることはない。
F.SECURE-PRINTにおいて親展プリントジョブの正当な利用者である一般ユーザの認証後に実施される親展プリントジョブアクセス制御の実行中に保持されるセキュリティドメインは信頼されないサブジェクトから干渉されることはない。
F.SERVICEにおいてサービスエンジニア識別認証後に保持されるセキュリティドメインであるサービスモードは、他のサブジェクトからのすべてアクセスを受け付けない。
F.BOX-PANELにおいてボックスアクセス認証後のセキュリティドメインは信頼されないサブジェクトから干渉されることはない。
F.BOX-PCおいてボックスアクセス認証後のセキュリティドメインは信頼されないサブジェクトから干渉されることはない。また複数のユーザからの同一ユーザボックスへのアクセスを受け付けることは許容されているが、それぞれ許可された正当な利用者の保持するセキュリティドメインは分離されており、干渉されることはない。
F.BOX-UTILITY-1においてボックスアクセス認証後のセキュリティドメインは信頼されないサブジェクトから干渉されることはない。また複数のユーザからの同一ユーザボックスへのアクセスを受け付けることは許容されているが、それぞれ許可された正当な利用者の保持するセキュリティドメインは分離されており、干渉されることはない。
F.BOX-UTILITY-2において管理者識別認証後に保持されるセキュリティドメインは、信頼されないサブジェクトから干渉されることはない。
従ってそれぞれのセキュリティドメインが干渉されることがないため、本要件は満たされる。

- **FTA_SSL.3[1]**

FTA_SSL.3[1]は、MFP本体操作パネルよりアクセスする管理者モード接続中のセッション終了を規定している。
F.ADMIN-PANELは、MFP本体操作パネルより管理者モードに接続中、オートリセット動作設定データで決定される時間（設定なし、0～9分）、無操作状態が継続すると自動的に管理者モードへのアクセス許可状態を遮断する。
従って本機能要件は満たされる。

- **FTA_SSL.3[2]**

FTA_SSL.3[2]は、クライアントPCよりアクセスする管理者モード接続中のセッション終了を規定している。
F.ADMIN-PCは、クライアントPCより管理者モードに接続中、オートリセット動作設定データで決定される時間（1～4分の設定：5分、5～9分の設定：設定値、設定なし：10分）、無操作状態が継続すると自動的に管理者モードへのアクセス許可状態を遮断する。
従って本機能要件は満たされる。

8.3.2. TOE セキュリティ機能強度根拠

確率的・順列的メカニズムを有するTOEセキュリティ機能は、①F.ADMIN-PANEL、F.ADMIN-PC、F.BOX-UTILITY-2における管理者モードパスワード認証メカニズム、②F.SECURE-PRINTにおける親展プリントパスワード認証メカニズム、③F.SERVICEにおけるサービスコード認証メカニズム、④F.BOX-PANEL、F.BOX-PC、F.BOX-UTILITY-1におけるボックスパスワード認証メカニズムである。各認証メカニズムは、順に①8桁数字、②4桁数字、③8桁数字・“＃”・“＊”、④4～64桁以上のASCIIコード0x20～0x7E（95種類の文字）をパスワード空間として持ち、不正使用防止機能と共に動作する。（3回の不成功認証試行を以ってアクセスをロックする。（詳細は6.1節に記述。但しサービスコード認証メカニズムは、不正使用防止機能の動作設定に関わらず 3 回の不成功試行を検出しアクセスをロックする。）よって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、8.3.1.2小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 6.3 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、ライフサイクル管理、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。

～ 最終ページ ～