Di3510 シリーズ／Di3510f シリーズ
Multi Function Peripheral　Security Kit
セキュリティターゲット

バージョン：1.18

発行日：2004年6月4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	更新内容
2003/07/31	1.00	石田	橋本	中山	初版作成。
2003/08/28	1.01	石田	橋本	中山	仕様変更反映。
2003/09/02	1.02	石田	橋本	中山	誤植修正。
2003/09/05	1.03	石田	橋本	中山	誤植修正。
2003/09/12	1.04	石田	橋本	中山	誤植修正。
2003/10/06	1.05	石田	橋本	中山	誤植修正。
2003/11/12	1.06	石田	橋本	中山	誤植修正。
2003/11/28	1.07	石田	橋本	中山	所見報告書（ASE001-01～ASE012-01）に対する修正。 誤植修正。
2003/12/12	1.08	石田	橋本	中山	仕様変更反映。 誤植修正。
2003/12/17	1.09	石田	橋本	中山	誤植修正。
2003/12/24	1.10	石田	橋本	中山	誤植修正。
2004/01/08	1.11	石田	橋本	中山	所見報告書（ASE013-01、ASE014-01）に対する修正。 誤植修正。
2004/01/16	1.12	石田	橋本	中山	所見報告書（ASE015-01～ASE019-01）に対する修正。 誤植修正。
2004/02/13	1.13	石田	橋本	中山	所見報告書（ASE020-01～ASE022-01）に対する修正。 誤植修正。
2004/02/26	1.14	石田	橋本	中山	所見報告書（ASE023-01）に対する修正。 誤植修正。
2004/04/02	1.15	石田	橋本	中山	所見報告書（ASE024-01～ASE026-01）に対する修正 誤植修正
2004/04/13	1.16	石田	橋本	中山	UIバージョン変更に伴う修正
2004/05/24	1.17	石田	橋本	中山	所見報告書（ASE027-01）に対する修正 誤植修正
2004/06/04	1.18	石田	橋本	中山	所見報告書（ASE028-01）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　：　Di3510シリーズ／Di3510fシリーズ[1] Multi Function Peripheral Security Kit　セキュリティターゲット
・バージョン　：　1.18
・CCバージョン　：　2.1
・作成日　：　2004年6月4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：Di3510シリーズ／Di3510fシリーズ Multi Function Peripheral Security Kit
英名　：Di3510 Series／Di3510f Series Multi Function Peripheral Security Kit
・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「User Interface」、「Network Module」から構成され、それぞれにバージョンが存在する。
- User Interface　：　4030-20G0-05-00
- Network Module　：　4030-A0G0-03-00

・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。）

[1] 「Di3510 シリーズ」とは、Di1810、Di2010、Di2510、Di3010、Di3510 で識別される Multi Function Peripheral（MFP）のことを示す。また「Di3510f シリーズ」とは、Di1810f、Di2010f、Di2510f、Di3010f、Di3510f で識別される MFP のことを示す。「Di3510 シリーズ」は、FAX 機能をオプション製品としているのに対し、「Di3510f シリーズ」は、FAX 機能が予め搭載されている MFP である。

- **PP参照**

本STは、PP参照を行っていない。

- **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

Multi Function Peripheral（MFP）とは、コピー、プリント、スキャン、FAX の各機能を選択、組み合わせて構成される事務用 IT 機器である。本 ST は、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モノクロ印刷対応の Di3510 シリーズ／Di3510f シリーズ 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を実施するソフトウェアコンポーネントである「User Interface」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“Di3510 シリーズ／Di3510f シリーズ Multi Function Peripheral Security Kit”を評価対象（TOE）とし、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。

Di3510 シリーズ／Di3510f シリーズ 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、スキャン、FAX 送受信など、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。この中で TOE のセキュリティ機能は、Di3510 シリーズ／Di3510f シリーズ MFP の特定の機能の利用にあたって MFP にスプールさ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、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親展プリント機能と、スキャンデータの保存領域として設定されるユーザボック

スへのアクセスを制御するユーザボックス機能のことである。

本 ST は、親展プリント機能及びユーザボックス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、FAX 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。

親展プリントパスワード

親展プリントを行う際、親展プリントに設定するパスワード。（印刷待機状態にある親展プリントに設定されるパスワード。）4 桁の数字が設定可能である。

ユーザボックス

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 ”で示されるユーザボックスは、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。

ユーザボックス識別子

ユーザボックスに設定される名称。

ユーザボックスデータ

ユーザ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。

ユーザボックスパスワード

個々のユーザ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。

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、メンテナンスモード、初期化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。

アクセスチェック機能

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、ユーザ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、ユーザ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。

ユーザボックス不正アクセス検出カウント値

アクセスチェック機能が動作中にユーザ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

アクセスチェック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

アクセスチェック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、アクセスチェック機能の動作設定に依存しない。

ペナルティ解除機能

ユーザ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。ユーザボックス、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。

2. TOE 記述

2.1. TOE の種別

TOE である Di3510 シリーズ／Di3510f シリーズ Multi Function Peripheral Security Kit は、MFP に搭載される 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る。具体的には MFP 本体操作パネルからの操作制御を実施する「User Interface」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。

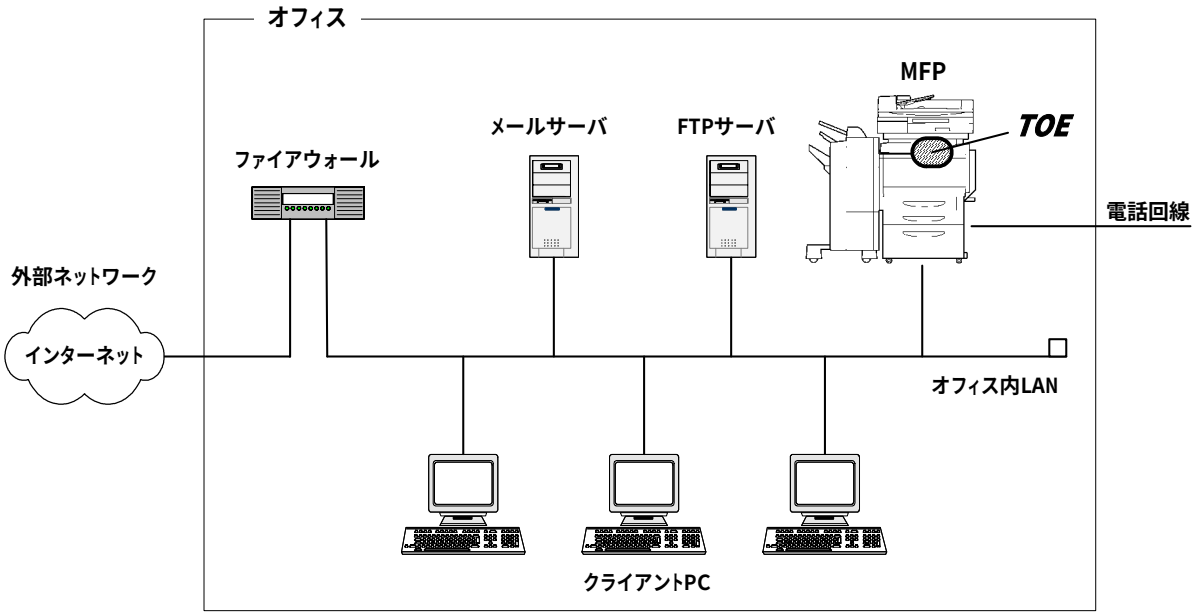

図 1 想定される MFP の利用環境の例

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、FAX に関係する機能が利用できなくなるが、その他の MFP の機能に対して影響はない。TOE のセキュリティ機能の利用に対して、FTP サーバ、メールサーバは必ずしも必要ではなく、外部ネットワークや電話回線に接続される必要性も同様である。

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 は、FAX の送受信及び MFP の保守管理を行うサポートセンターと通信を行うために電話回線に接続される。

2.3. TOE 利用者の役割

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

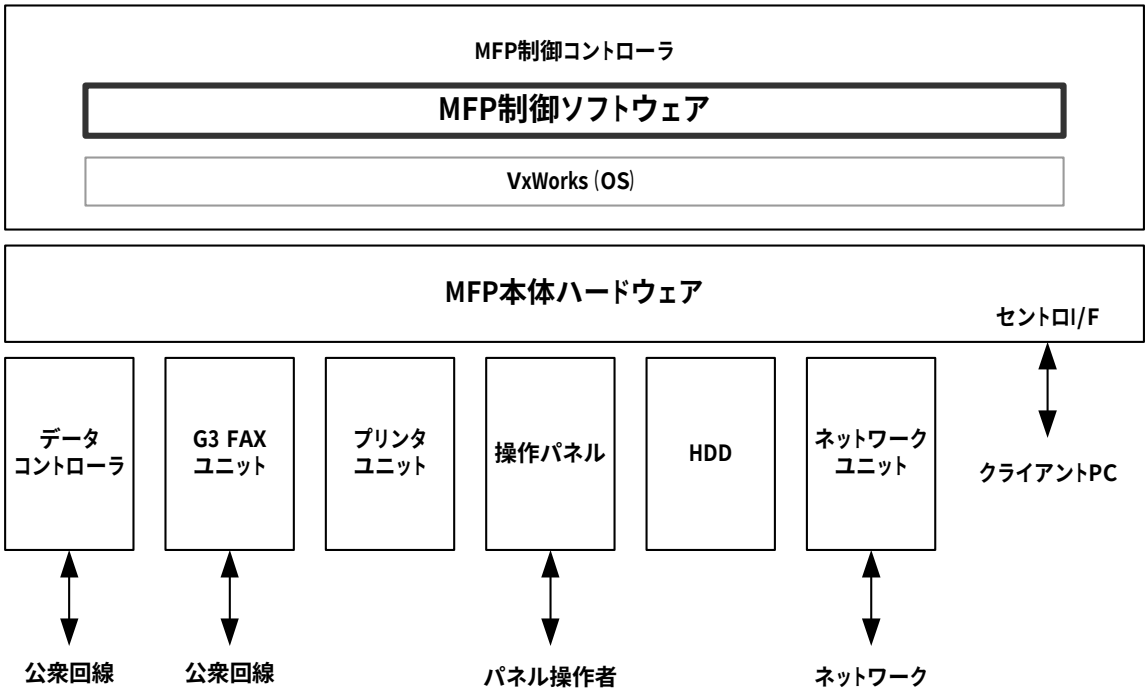

図 2 MFP のハードウェア構成

MFP のハードウェア環境構成を上図に示す。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、クライアント PC と接続するセントロ I/F が標準搭載される。更に MFP 本体ハードウェアには、プリンタユニット、G3 FAX ユニット、データコントローラ（EP-NET に必要なハードウェア）、ハードディスク（HDD）、プリンタユニット搭載時に必要となるネットワークユニットなどが必要になる。

2.4.2. TOE のソフトウェア環境

TOE である「User Interface」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化したオブジェクトコードとして 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。

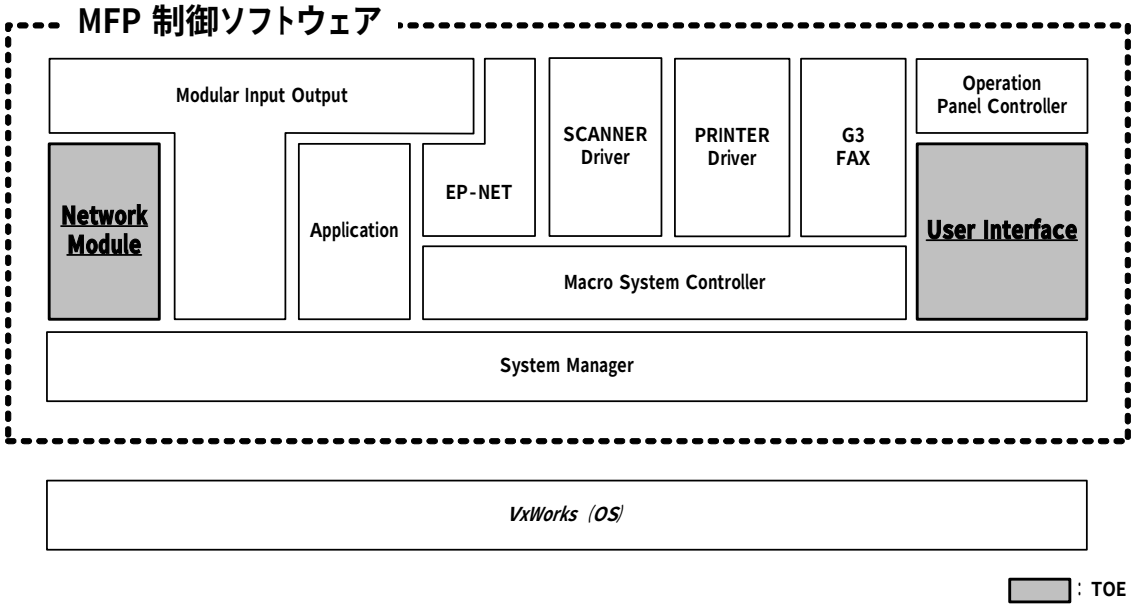

図 3 MFP 制御ソフトウェアコンポーネントの構成

- *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。Di3510 シリーズ／Di3510f シリーズ 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。

- System Manager
  ジョブの登録、起動及びリソースを管理するソフトウェアコンポーネント。

- Operation Panel Cntroller（**通称** OPE）
  MFP 本体操作パネルにおける LCD、LED、キー等のハードウェアを制御するソフトウェアコンポーネント。MFP 本体操作パネルからの入力情報は本ソフトウェアコンポーネントにて処理され、「User Interface」に受け渡される。また「User Interface」の処理結果を受け付け、パネルに表示する。

- **User Interface（通称 UI）**
  本 ST にて評価対象としているソフトウェアコンポーネント。「Operation Panel Controller」からの入力情報を処理し、処理に応じて「System Manager」、「Macro System Controller」、「Network Module」に通知する。また「System Manager」、「Network Module」、「Macro System Controller」からのメッセージを処理して「Operation Panel Controller」へ通知する。

- Modular Input Output（**通称** 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「Application」、「Network Module」、「System Manager」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、DNS サーバ等、ネットワークの諸設定処理を実施する。

- **Network Module（通称 NM）**

  本 ST にて評価対象としているソフトウェアコンポーネント。クライアント PC からの操作要求に対し、「Modular Input Output」がネットワークから受け付けた所定のプロトコル（HTTP、IPP、MIB）によるデータを受け付け、処理・制御する。処理に応じて「VxWorks」、「System Manager」、「Macro System Controller」、「User Interface」に処理を依頼し、「VxWorks」、「System Manager」、「Macro System Controller」、「User Interface」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。

- Macro System Controller（通称 MSC）

  取り込んだ画像データを解析してジョブとして登録するソフトウェアコンポーネント。またコピー、プリント、スキャン、FAX におけるジョブシーケンスの管理を実施する。

- Application

  E-mail 送受信（インターネット FAX 送受信）、FTP 送信、PC からのプリント受け付け処理等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。

- SCANNER Driver

  スキャンにおいて読み取り処理を実施するスキャナデバイスを制御するソフトウェアコンポーネント。

- PRINTER Driver

  印刷においてプリンタデバイスを制御するソフトウェアコンポーネント。（※クライアント PC のプリンタドライバとは異なる。）

- G3 FAX

  G3 規格の FAX 送受信を行うためのソフトウェアコンポーネント。

- EP-NET

  電話回線（公衆回線）または「Modular Input Output」から遠隔診断機能へのアクセスを受け付け、遠隔診断機能を実施するソフトウェアコンポーネント。遠隔診断機能は、電話回線より、サポートセンターからのアクセス要求を受け付ける機能であり、サポートセンターは電話回線を介して、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収集する。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機能も兼ね備えている。また E-mail を利用して同様の機能を実現する E-mail 遠隔診断機能も存在する。

よって TOE である「User Interface」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。

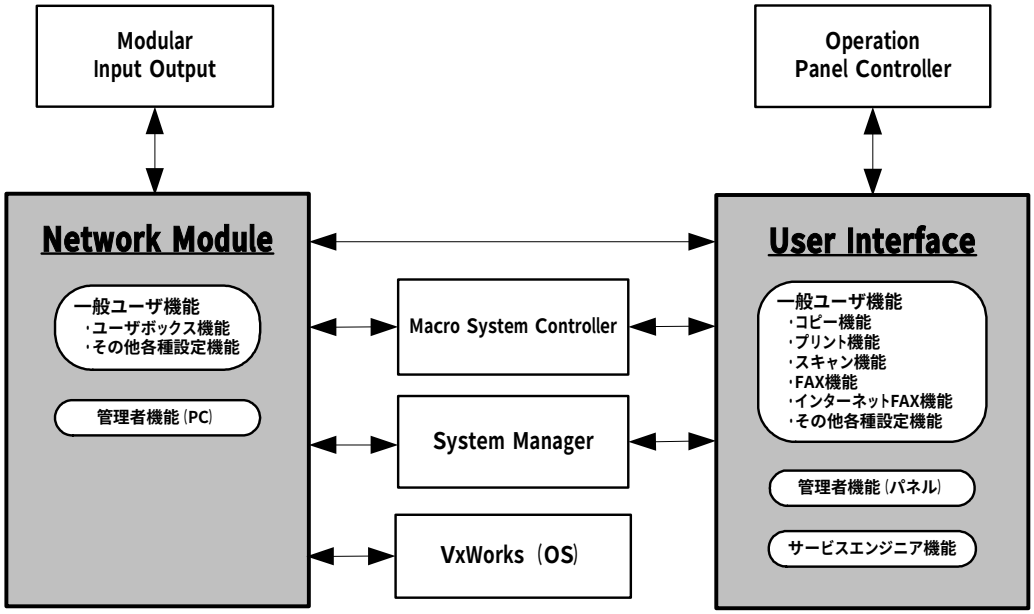

図 4 TOE 動作処理と関係する MFP 制御ソフトウェアコンポーネント

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 の搭載された 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）**、**管理者機能（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

一般ユーザは、MFP としての主機能であるコピー機能、プリント機能、スキャン機能、FAX 機能を利用することができる。TOE はこれら主機能における制御処理の一部を担っている。以下に一般ユーザが扱う一般機能を記述すると共に、各機能において動作する TOE の処理内容について説明する。

(1) **コピー機能**

MFP 本体操作パネルより、スキャンを実行し、スプールされたイメージデータをそのまま印刷する機能。TOE は、このコピー機能において実行受付、実行中処理を示す画面表示、コピーの中断処理受付を行う。

(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。MFP で受信したプリントデータは、「System Manager」によってジョブ ID が付与され、親展プリントジョブ情報データとして登録される。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ジョブ ID で識別される親展プリントジョブの印刷待機解除を「System Manager」に対して通知し、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。

TOE は、上記複数種のプリント機能において、プリントデータを受信中であることを示す画面表示処理、印刷中であることを示す画面表示処理、各画面表示時に実行されるプリント機能の中断処理を行う。親展プリントでは、印刷待機状態のパスワード入力受付、照合処理を行う。

(3) 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。またスキャン時にイメージデータを MFP 外に送信せず、MFP に内蔵される HDD のユーザボックスに保管することも可能である。TOE は、このスキャン機能において実行受付、実行中処理を示す画面表示、スキャンの中断処理受付を行う。

(4) FAX 機能

FAX 用の電話回線から、FAX データを送受信する機能。通常の FAX データ送受信機能に加え、F コードを利用した FAX 機能も対応している。TOE は、この FAX 機能において FAX 送信実行受付、送信処理を示す画面表示、FAX 送信の中断処理を行う。

(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。TOE は、このインターネット FAX 送信時に送信実行受付、送信処理を示す画面表示、送信の中断処理を行う。

(6) **ユーザボックス機能**

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ユーザボックスを作成（名称、及びパスワードの新規設定）し、イメージデータ（以降、ユーザボックスデータとする）の格納されたユーザボックス※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。

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

※ ユーザボックスには、デフォルトで“Public”と名称が設定されているユーザボックスが存在する。“Public”は、一般ユーザが共用する保管領域であるため、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。

(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）に分類して説明する。

(1) **管理者機能（パネル）**

・管理者モードパスワードの変更機能
・アクセスチェック機能の動作状態設定機能
・ペナルティ解除機能（親展プリント、ユーザ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）

・管理者向け各種設定機能（親展プリントジョブの一括削除、ユーザボックスデータの自動削除設定、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) **管理者機能（PC）**

・ユーザボックスデータの削除
・ユーザボックスの削除
・ユーザボックスの設定変更（名称の変更、パスワードの変更）
・管理者向け各種設定機能（ユーザボックス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）

2.5.3. 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、メンテナンスモード、初期化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。

(1) **サービスモード**

・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) **メンテナンスモードモード**

・サービスエンジニア向け各種設定機能（MFP 本体操作パネルの表示調整、等）

(3) **初期化モード**

・サービスエンジニア向け各種設定機能（言語設定、等）

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いて、プリント機能の利用において機密性の高いドキュメントを印刷する際は、親展プリントが有効であり、親展プリントジョブ情報データの暴露防止機能は、セキュリティ機能として位置付けられる。またスキャンしたイメージデータが格納されるユーザボックスにアクセスする

ためには、当該ユーザボックスに設定されるパスワードが必要であり、このアクセスを制御する機能は、ユーザボックスデータの機密性を維持するためのセキュリティ機能として位置付けられる。

以下に一般ユーザ機能の中で、セキュリティ機能として位置付けられる機能について詳細を説明する。

- **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。

- **ユーザボックスの作成機能**

  一般ユーザが、名称を指定し、ユーザボックスを作成する機能。

- **ユーザ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**

  ユーザボックスにアクセスする際、当該ユーザ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、当該ユーザ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、ユーザボックス内のすべてユーザボックスデータのダウンロードが許可される。（なお、“ Public ”で示されるユーザボックスは、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ユーザボックス管理機能**

  ユーザボックスの正当な利用者である一般ユーザが、当該ユーザボックスの設定（名称、パスワード）を変更する機能。

親展プリント機能において、MFP にスプールされ保管状態となる親展プリントジョブ情報データは、機密ドキュメントの印刷時においてセキュリティを維持するために保管される一時的なデータである。つまり本データを長期間 MFP に保管することを目的としていないため、削除操作に対してセキュリティ的な考慮は不要である。また意図せず削除された場合であっても、基本的には元データがクライアント PC に存在するため、可用性が落ちることを考慮する必要がない。

ユーザボックス機能は、印刷物をクライアント PC にて電子データとして取り扱うために利用する機能であり、ユーザボックスデータは、クライアント PC に取り込まれるまで保管される一時的なデータである。ゆえに親展プリント機能と同様、ユーザボックスデータも長期間 MFP に保管することを目的としていないため、削除操作に対してセキュリティ的な考慮は不要である。また意図せず削除された場合であっても、基本的にはユーザボックスデータの元となる印刷物が存在するため、可用性が落ちることを考慮する必要がない。

従って親展プリントジョブ情報データ、ユーザボックスデータの各削除機能に対し、適切な防御機能を想定する必要性はない。

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、当該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
  - アクセスチェック機能の動作状態設定機能
  - ペナルティ解除機能

  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。
  - ユーザボックスの設定変更機能（名称の変更、パスワードの変更）

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

サービスモードにおける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識別認証する機能。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

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.ACCESS-CHECK（アクセスチェック機能の動作設定条件）

MFP の利用者は、アクセスチェック機能が必ず動作する設定状態で MFP を利用する。

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（HDD の保護条件）

管理者がサービスエンジニアに持ち出しを許可した場合を除き、HDD は持ち出されない。

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.SESSION（セッション管理条件）

- 一般ユーザは、ボックス機能の利用終了後、そのセッションを必ず終了する。
- 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する。
- 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、正当な利用者になりすまして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-USER-BOX（ユーザ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、作成されたユーザボックスにクライアント PC よりアクセスし、正当な利用者になりすまして当該ユーザボックスのユーザボックスデータをダウンロードすることにより、ユーザボックスデータが不正に暴露される。

3.3. 組織のセキュリティ方針

P.BEHAVIOR-ACCESS-CHECK（アクセスチェック機能の動作設定機能）

セキュアな環境では、操作性において従来の機種との互換性を維持するために、アクセスチェック機能を停止できる。

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 の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-USER-BOX（ユーザ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、ユーザボックスデータのダウンロード操作を許可する。

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.I&A-ADMIN（管理者の識別認証）

TOE は、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ユーザ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セキュリティ対策方針を IT 環境セキュリティ対策方針、Non-IT 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.ACCESS-SECURE-PRINT（親展プリントジョブアクセス制御）

System Manager 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。

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 環境セキュリティ対策方針

OE-N.ACCESS-CHECK（アクセスチェック機能の動作）

管理者は、アクセスチェック機能を必ず動作させた状態で TOE を運用する。

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）

- 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。
- 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、ユーザ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、ユーザ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、ユーザボックスパスワードの適宜変更を行う。
- 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.MAINTENANCE（MFP の保守管理）

- 管理者は、サービスエンジニア以外の者が保守作業を実施することを許可しない。
- 管理者は、サービスエンジニアが実施する保守作業を必ず管理者立ち会いのもとで実施する運用管理を行うことで、管理者の許可なく HDD が持ち出されることを防止する。

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.STRUCTURE（MFP の HDD 取り付け構造）

TOE が搭載される MFP において利用される HDD は、サービスエンジニア以外の者が取り外すことができない設置構造とする。

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。

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	**サブセットアクセス制御**

FDP_ACC.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 1　ユーザボックスに対する操作のリスト」に記載

[割付: *アクセス制御 **SFP***]：

ユーザ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）

表 1　ユーザボックスに対する操作のリスト

サブジェクト	オブジェクト	操作のリスト
ユーザボックスを操作するプロセス	***ユーザボックス***	***・ ユーザボックス内のユーザボックスデータ読み出し*** ***・ 作成***

FDP_ACF.1	セキュリティ属性によるアクセス制御

FDP_ACF.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*]：

ユーザボックス識別子

[割付: *アクセス制御 SFP*]：

ユーザボックスアクセス制御

FDP_ACF.1.2

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*]：

- ***一般ユーザが選択した“ユーザボックス識別子”を持つユーザボックスを操作するプロセスは、これと一致する“ユーザボックス識別子”を持つユーザボックスのみ、ユーザボックス内のユーザボックスデータ読み出し操作を許可される。***
- ***一般ユーザが入力した“ユーザボックス識別子”を持つユーザボックスを操作するプロセスは、これと一致する“ユーザボックス識別子”を持つユーザボックスが存在しない場合に、一般ユーザが入力した“ユーザボックス識別子”をオブジェクト属性とするユーザボックスの作成操作を許可される。***
- ***一般ユーザが入力した“ユーザボックス識別子”を持つユーザボックスを操作するプロセスは、これと一致する“ユーザボックス識別子”を持つユーザボックスが存在する場合に、一般ユーザが入力した“ユーザボックス識別子”をオブジェクト属性とするユーザボックスの作成操作を拒否される。***

FDP_ACF.1.3

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[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）、FMT_MSA.3（FMT_MSA.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*]：

管理者の認証

[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*]：

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[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*]：

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[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ペナルティ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[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*]：

ユーザ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[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*]：

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、当該ユーザ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をロックする。

＜通常状態復帰のための操作＞

ユーザボックスに対するペナルティ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[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、***ユーザ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***ユーザ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***ユーザ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

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、ユーザ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***ユーザ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、***ユーザ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*]：

アクセスチェック機能

[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[2]）

FMT_MSA.1	**セキュリティ属性の管理**

FMT_MSA.1.1

TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]*]をする能力を[割付: *許可された識別された役割*]に制限するために[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。

[割付: *セキュリティ属性のリスト*]：

ユーザボックス識別子

[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*]：

当該ユーザ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*]：

ユーザ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）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MSA.3	**静的属性初期化**

FMT_MSA.3.1

TSFは、そのSFPを実施するために使われるセキュリティ属性として、[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*]：

ユーザボックスアクセス制御

FMT_MSA.3.2

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

[割付: *許可された識別された役割*]：

当該ユーザ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）、FMT_SMR.1（FMT_SMR.1[4]）

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

[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]：

改変

[割付:*許可された識別された役割*]：

管理者

下位階層 ： なし

依存性 ： FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[2]	**TSF データの管理**

FMT_MTD.1.1[2]

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

[割付: *TSF データのリスト*]：

ユーザ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*]：

当該ユーザ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[1]、FMT_SMR.1[2]）

FMT_MTD.1[3]	**TSF データの管理**

FMT_MTD.1.1[3]

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

[割付: *TSF データのリスト*]：

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[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*]:

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[3]）

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*]:

- ***ユーザ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[2]）

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 2 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 2 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	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	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。 ・ ***ユーザボックス識別子の作成機能*** ・ ***ユーザボックス識別子の改変機能（当該ユーザボックスの正当な利用者である一般ユーザが操作）*** ・ ***ユーザボックス識別子の改変機能（管理者が操作）***
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。 ・ ***アクセスチェック機能の動作設定機能***
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。 ・ ***アクセスチェック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ペナルティ解除機能***
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。 ・ ***アクセスチェック機能の動作設定機能*** ・ ***ユーザボックス不正アクセス検出カウント値を消去するペナルティ解除機能***

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
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。
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_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。	・ ***ユーザボックスパスワードの改変機能（当該ユーザボックスの正当な利用者である一般ユーザが操作）*** ・ ***ユーザボックスパスワードの改変機能（管理者が操作）*** --- 以下は、上記と異なり左記の管理項目に該当する管理機能ではないが、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。 ・ ***アクセスチェック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; 関係する利用者による認証データの管理; 利用者が認証される前にとられるアクションのリストを管理すること。	・ ***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	左記の管理項目に該当する管理機能は存在し

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。 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。	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 における管理機能と考えられる: a) 利用者識別情報の管理;	・ ***ユーザボックス識別子の作成機能*** ・ ***ユーザボックス識別子の改変機能（当該ユーザボックスの正当な利用者である一般ユーザが操作）*** ・ ***ユーザ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	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	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_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。

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[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

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*]：

当該ユーザボックスの正当な利用者である一般ユーザ

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（FIA_UID.1[2]）

FMT_SMR.1[2] セキュリティ役割

FMT_SMR.1.1[2]

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

[割付: *許可された識別された役割*]：

管理者

FMT_SMR.1.2[2]

TSF は、利用者を役割に関連づけなければならない。

下位階層 : なし

依存性 : FIA_UID.1（FIA_UID.2[3]）

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*]：

サービスエンジニア

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[4]）

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*]：

当該ユーザボックスを作成する一般ユーザ

FMT_SMR.1.2[4]

TSF は、利用者を役割に関連づけなければならない。

下位階層 : なし

依存性 : FIA_UID.1（適用しない）

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

5.1.2. 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 3 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。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. 利用者データ保護

FDP_ACC.1[E]	**サブセットアクセス制御**

FDP_ACC.1.1[E]

System Manager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 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[E]）

表 4 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_ACF.1[E]	**セキュリティ属性によるアクセス制御**

FDP_ACF.1.1[E]

System Manager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[E]

System Manager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*]：

- ***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。***
- ***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。***

FDP_ACF.1.3[E]

System Manager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[E]

System Manager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[E]）、FMT_MSA.3（FMT_MSA.3[E]）

5.2.1.2. 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

5.2.1.3. セキュリティ管理

FMT_MSA.3[E]	**静的属性初期化**

FMT_MSA.3.1[E]

System Manager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[E]

System Manager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）

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 5、表 6 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 5 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	管理者モードセキュリティ機能
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.USER-BOX	ユーザボックスセキュリティ機能

表 6 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	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FDP_ACC.1				●
FDP_ACF.1				●
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]				●

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

6.1.1. F.ADMIN（管理者モードセキュリティ機能）

F.ADMIN とは、MFP 本体操作パネルまたはクライアント 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、管理者モードパスワード、ユーザボックスパスワード、ユーザボックス識別子を変更するセキュリティ管理機能、アクセスチェック機能の動作設定機能、ペナルティ解除機能といった管理者モードにおける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。

＜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、任意のユーザボックスにおけるユーザボックス識別子、ユーザボックスパスワードを変更す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。
・ ユーザボックスパスワードの変更は、新しく設定されるユーザ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ユーザボックスのユーザボックスパスワードとして変更する。
・ ユーザ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。

＜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アクセスチェック機能の動作設定機能、③ペナルティ解除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。
- 新しく設定される管理者モードパスワードの入力、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管理者モードパスワードとして変更する。
- 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 アクセスチェック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アクセスチェック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アクセスチェック機能を停止状態にする。

③ ペナルティ解除機能

- 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。
- 各ユーザボックスのユーザ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、ユーザ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。

6.1.2. 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する機能のことである。

＜親展プリントジョブを印刷するための識別認証機能＞

- 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 が提供する親展プリントジョブに対するペナルティ解除機能を実行することにより解除される。

なお、識別認証されると TOE 外エンティティ（IT 環境のソフトウェアコンポーネント）である「System Manager」に当該親展プリントジョブ情報データのジョブ ID 及び認証が成功したこと通知する。（※親展プリントジョブ情報データの印刷は、「System Manager」にて実施される。）

6.1.3. 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、サービスコードを変更機能、管理者モードパスワードを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。

＜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。
- 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。

6.1.4. F.USER-BOX（ユーザボックスセキュリティ機能）

F.USER-BOX とは、一般ユーザのクライアント PC からユーザボックスデータへのアクセスに対してユーザボックスデータの正当な利用者であること識別認証し、ユーザ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ユーザボックスを作成・設定管理するセキュリティ機能のことである。

＜ユーザボックス作成機能＞

・ ユーザボックス作成機能は、一般ユーザに提供される。
・ ユーザボックス作成機能が起動されると、ユーザボックスを操作するプロセスが立ち上がる。
・ ユーザ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ユーザボックス識別子が他のユーザ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ユーザボックス識別子を属性とするユーザ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。）

＜ユーザ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ユーザボックスを選択すると、アクセスする利用者が当該ユーザ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）からなるユーザボックスパスワードにより認証するユーザボックスパスワード認証メカニズムを提供する。
・ ユーザ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ユーザ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 が提供するユーザボックスに対するペナルティ解除機能を実行することにより解除する。

＜識別認証後のユーザボックスアクセス制御機能＞

・ 一般ユーザが、ユーザ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、ユーザボックスアクセス制御機能に基づき、ユーザ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“ユーザボックス識別子”を持つユーザボックスの“ユーザボックス内のユーザボックスデータ読み出し”操作が許可される。

＜ユーザボックス設定管理機能＞

・ 識別認証されたユーザボックスの正当な利用者に当該ユーザボックスに対してユーザボックスの設定を変更する機能（ユーザボックス識別子変更、ユーザボックスパスワード変更）を提供する。
・ ユーザボックスパスワードの変更は、新しく設定されるユーザ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ユーザボックスパスワードの変更処理を行う。
・ 新規設定されるユーザ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、当該ユーザ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 が提供するユーザボックスに対するペナルティ解除機能を実行することにより解除する。

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 における①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②親展プリントパスワード認証メカニズム、F.USER-BOX における③ユーザボックスパスワード認証メカニズム、F.SERVICE が提供する④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 7 で記述した EAL3 の TOE セキュリティ保証要件のコンポーネントを満たす保証手段を下表に示す。

表 7 TOE 保証要件と保証手段の関係

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	CM 能力	ACM_CAP.3	・構成管理計画書 ・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	・セットアップ要領書（※和文：国内向け） ・セットアップ要領書／SETUP INSTRUCTIONS（※和英併記：海外向け） ・設置チェックリスト（※和文） ・Installation Checklist（※英文） ・追加情報／Additional Information（※和英併記）
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	・取扱説明書 セキュリティキット（※和文） Di1810f/Di2510f/Di3010f/Di3510f Di1810/Di2510/Di3010/Di3510 ・USER MANUAL Security Kit（※英文） Di2010f/Di2510f/Di3010f/Di3510f Di2010/Di2510/Di3010/Di3510 ・取扱説明書 PageScope Light（※和文） ・User Manual PageScope Light（※英文） ・サービスマニュアル セキュリティキット(※和文) Di1810f/Di2510f/Di3010f/Di3510f Di1810/Di2510/Di3010/Di3510 ・SERVICE MANUAL Security Kit(※英文) Di2010f/Di2510f/Di3010f/Di3510f Di2010/Di2510/Di3010/Di3510
	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 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、脅威とセキュリティ対策方針の対応関係を下表に示す。セキュリティ対策方針が少なくとも 1 つ以上の前提条件、脅威に対応していることを示している。

表 8　前提条件、脅威に対するセキュリティ対策方針の適合性

前提・脅威 ＼ セキュリティ対策方針	A.ACCESS-CHECK	A.ADMIN	A.AUTH	A.HDD	A.NETWORK	A.PHYSICAL	A.SERVICE	A.SESSION	T.ACCESS-SECURE-PRINT	T.ACCESS-USER-BOX	P.BEHAVIOR-ACCESS-CHECK
O.ACCESS-ADMIN									●	●	●
O.ACCESS-USER-BOX										●	
O.ACCESS-SERVICE									●	●	
O.I&A-ADMIN									●	●	●
O.I&A -SERVICE									●	●	
O.I&A-USER									●	●	
OE.ACCESS-SECURE-PRINT									●		
OE.SECURE-PRINT-QUALITY									●		
OE-N.ACCESS-CHECK	●										
OE-N.ADMIN		●									
OE-N.AUTH			●								
OE-N.MAINTENANCE				●							
OE-N.NETWORK					●						
OE-N.PHYSICAL						●					
OE-N.SERVICE							●				
OE-N.STRUCTURE				●							
OE-N.SESSION								●			

8.1.2. 前提条件に対する十分性

前提条件に対するセキュリティ対策方針について以下に説明する。

- **A.ACCESS-CHECK（アクセスチェック機能の動作設定条件）**
  本条件は、アクセスチェック機能が必ず動作することを想定している。
  OE-N.ACCESS-CHECKは、TOEの搭載されたMFPの利用において、管理者がアクセスチェック機能を動作させる状態にすることが規定されており、これよりアクセスチェック機能の動作が保証される。
  従って本条件は実現される。

- **A.ADMIN（管理者の役割、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、ユーザ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ユーザ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（HDDの保護条件）**
  本条件は、MFP内に設置されるHDDが基本的に持ち出されないこと、及び例外的にサービスエンジニアが持ち出す場合であっても管理者が許可しなければ持ち出すことができないことを想定している。
  HDDが持ち出される危険性は、MFPの保守管理作業において最も高いと考えられるが、OE-N.MAINTENANCEは、MFPを利用する組織がサービスエンジニア以外の者にMFPの保守作業を実施することを許可しないことを規定しており、更にMFPの保守作業に際して必ず管理者が立ち会うことでサービスエンジニアといえども管理者の許可なくHDDを持ち出すことが防止されるため、運用上、HDDが不当に持ち出されないことが保証される。

更にOE-N.STRUCTUERは、構造上、サービスエンジニア以外の者がHDDを取り出すことが出来ないとすることが規定されており、HDDが持ち出されないことを物理的にも保証している。
よって運用・物理的に本事項は対処されており、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の諸条件によりオフィス内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アクセス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。
上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役割、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.SESSION（セッション管理方法）**

本条件は、セッション管理方法として、各々の利用者の各機能の利用終了後に、そのセッションを必ず終了することを規定している。
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し、管理者自身は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ことが規定されており、なりすましの脅威が発生しないことが保証される。
また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にそのセッションを終了させることが規定されており、なりすましの脅威が発生しないことが保証される。
従って本条件は実現される。

8.1.3. 脅威に対する十分性

脅威に対抗するセキュリティ対策方針について以下に説明する。

- **T.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OE.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とあるが、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アクセスチェック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ペナルティ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を操作することを許可されることが規定されている。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は保護される。

  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を操作することを許可されることが規定されている。

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-USER-BOX（ユーザボックスデータへの不正な操作）**

本脅威は、ユーザ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、ユーザ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、ユーザボックスにアクセスする者がユーザ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-USER-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ユーザボックスにおけるユーザ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。

またユーザ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アクセスチェック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ペナルティ解除機能、ユーザ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、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ている。これより、管理者モードにおけるユーザ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は保護される。

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を操作することを許可されることが規定されている。

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-ACCESS-CHECK（アクセスチェック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従来と互換性のある操作性を実現するために、アクセスチェック機能の停止を可能とすることが規定されている。これに実現するには、アクセスチェック機能の動作設定機能が提供される必要がある。また機能強度の大きな影響を及ぼすアクセスチェック機能であるため、その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ている。（アクセスチェック機能の動作設定機能は、管理者機能の1つとして提供されている。）

  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 9　セキュリティ対策方針に対する IT セキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.ACCESS-ADMIN	O.ACCESS-USER-BOX	O.ACCESS-SERVICE	O.I&A -ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.ACCESS-SECURE-PRINT	OE.SECURE-PRINT-QUALITY
FDP_ACC.1		●						
FDP_ACF.1		●						
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	●	●				●		

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-USER-BOX	O.ACCESS-SERVICE	O.I&A -ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.ACCESS-SECURE-PRINT	OE.SECURE-PRINT-QUALITY
FMT_MSA.3		●				●		
FMT_MTD.1[1]	●							
FMT_MTD.1[2]	●					●		
FMT_MTD.1[3]			●					
FMT_MTD.1[4]			●					
FMT_MTD.1[5]	●							
FMT_SMF.1	●	●	●			●		
FMT_SMR.1[1]		●				●		
FMT_SMR.1[2]	●							
FMT_SMR.1[3]			●					
FMT_SMR.1[4]		●				●		
FPT_RVM.1※	＊	＊	＊	＊	＊	＊		
FPT_SEP.1※	＊	＊	＊	＊	＊	＊		
FDP_ACC.1[E]							●	
FDP_ACF.1[E]							●	
FIA_SOS.1[E]								●
FMT_MSA.3[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、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。

アクセスチェック機能は、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。設定される管理者モードパスワードは、FIA_SOS.1[2]により、8桁数字であることを検証する。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。この際、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。更にFIA_AFL.1[1]により、この再認証の不成功も管理者の認証に対する不正アクセスとして不成功回数をカウントするため、管理者モードパスワードの変更操作はより強固に保護される。

ユーザ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[5]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

ユーザボックスパスワードの変更は、FMT_MTD.1[2]及びFMT_SMF.1によりユーザ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。設定されるユーザボックスパスワードはFIA_SOS.1[1]により4～64桁の半角英数字、半角記号であることを検証する。

ユーザボックス識別子の変更は、FMT_MSA.1、FMT_SMF.1よりユーザ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[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管理者が存在する。

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.ACCESS-USER-BOX（ユーザボックスアクセス制御）**

本セキュリティ対策方針は、一般ユーザのユーザ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、一般ユーザのユーザボックス作成及びユーザ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。

ユーザボックスへのアクセス制御方針を定義するFDP_ACC.1、FDP_ACF.1により、ユーザボックスを操作するプロセスは、入力した“ユーザボックス識別子”と同じ名称のユーザボックスが存在しない場合、これを属性とするユーザ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“ユーザボックス識別子”と同じ名称のユーザ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、ユーザボックスの操作するプロセスの保持する“一般ユーザが選択したユーザボックス識別子”と一致する“ユーザボックス識別子”を持つユーザボックスに対して“ユーザボックス内のユーザ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。

基本的に上記記載のFDP_ACC.1、FDP_ACF.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、ユーザ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ユーザボックス識別子のデフォルト値は、FMT_MSA.3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、ユーザ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[4]により、上記説明されるユーザ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、当該ユーザボックスを作成する一般ユーザが存在する。

ユーザボックス識別子の変更は、FMT_MSA.1、FMT_SMF.1よりユーザ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[1]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ユーザ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[3]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。設定されるサービスコードは、FIA_SOS.1[3]により、8桁数字、“＃”、“＊”である。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。この際、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。更にFIA_AFL.1[4]により、この再認証の不成功もサービスエンジニアの認証に対する不正アクセスとして不成功回数をカウントするため、サービスコードの変更操作はより強固に保護される。

管理者モードパスワードを初期化する操作は、FMT_MTD.1[4]及びFMT_SMF.1によりサービスエンジニアだけに制限されている。

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.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。
  管理者モードに対するアクセスは、FIA_AFL.1[1]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-SERCVICE（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。
  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。またユーザボックスデータをダウンロードする利用者が、確かにユーザ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[2]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[5]により解除可能である。

＜ユーザ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、ユーザボックスにアクセスする者がユーザ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、ユーザ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。

FIA_AFL.1[3]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、それ以降のユーザ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[5]により解除可能である。

ユーザ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ユーザボックス識別子のデフォルト値は、FMT_MSA.3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、ユーザ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[4]により、上記説明されるユーザ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、当該ユーザボックスを作成する一般ユーザが存在する。

ユーザボックス識別子の変更は、FMT_MSA.1、FMT_SMF.1よりユーザ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。

ユーザボックスパスワードの変更は、FMT_MTD.1[2]及びFMT_SMF.1によりユーザ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。設定されるユーザボックスパスワードはFIA_SOS.1[1]により4～64桁の半角英数字、半角記号であることを検証する。
FMT_SMR.1[1]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ユーザボックスの正当な利用者が存在する。

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.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、IT環境であるSystem Managerが親展プリントジョブ情報データの印刷操作が制限されることを規定しており、親展プリントジョブが印刷時に実施されるアクセス制御が必要になる。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[E]及びFDP_ACF.1[E]により、System Managerの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。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[E]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。
  印刷時は、FDP_ACC.1[E]及びFDP_ACF.1[E]により、System Managerの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”が受け渡されて、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。

  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.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 10 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	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1	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
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	FMT_MOF.1	N/A
FIA_UAU.2[2]	FPT_RVM.1	FPT_SEP.1	N/A	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	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.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
FDP_ACC.1[E]	N/A	N/A	N/A	N/A
FDP_ACF.1[E]	N/A	N/A	N/A	N/A
FIA_SOS.1[E]	N/A	N/A	N/A	N/A

IT セキュリティ機能要件	他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント			
	①迂回防止	②干渉、破壊防止	③非活性化防止	④無効化検出
FMT_MSA.3[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。

1. 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[2]により実施される。）
2. ユーザ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ユーザボックスの設定管理（ユーザボックスパスワードの変更、ユーザ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ユーザボックス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[3]により実施される。）
3. 管理者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[1]により実施される。）
4. 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[1]により実施される。）
5. 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。）
6. 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、

- 個々のユーザボックスにおける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

認証不成功時の検出・ロック（FIA_AFL.1[1]、FIA_AFL.1[2]、FIA_AFL.1[3]）及びユーザ

ボックスへアクセスする際の認証(FIA_UAU.2[2])の動作の管理は、FMT_MOF.1 により管理者だけに制限しており、FMT_MOF.1 はこれらの動作の非活性化を狙った攻撃に対する防御を提供している。

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 11 IT セキュリティ機能要件コンポーネントの依存関係

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	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1、FMT_MSA.3
FIA_AFL.1[1]	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[2]	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[3]	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[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	なし
FIA_SOS.1[2]	なし	なし
FIA_SOS.1[3]	なし	なし

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	なし
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	なし
FIA_UID.2[2]	なし	なし
FIA_UID.2[3]	なし	なし
FIA_UID.2[4]	なし	なし
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 、 FMT_SMF.1 、 FMT_SMR.1[1] 、 FMT_SMR.1[2]
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1、FMT_SMR.1[4]
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[3]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[3]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_SMF.1	なし	なし

本 ST の機能要件 コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FMT_SMR.1[1]	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[2]	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[3]	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。
FMT_SMR.1[4]	FIA_UID.1	なし ＜FIA_UID.1 を満たさない理由＞ ユーザボックス作成は、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。
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし
FDP_ACC.1[E]	FDP_ACF.1	FDP_ACF.1[E]
FDP_ACF.1[E]	FDP_ACC.1 FMT_MSA.3	FDP_ACF.1[E]、FMT_MSA.3[E]
FIA_SOS.1[E]	なし	なし
FMT_MSA.3[E]	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。

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 の搭載された 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 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 12　TOE セキュリティ機能要件に対する TOE セキュリティ機能の適合性

TOE セキュリティ機能 ＼ TOE セキュリティ機能要件	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
FDP_ACC.1				●
FDP_ACF.1				●
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	●			●
FMT_MSA.3				●
FMT_MTD.1[1]	●			
FMT_MTD.1[2]	●			●

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN	F.SECURE-PRINT	F.SERVICE	F.USER-BOX
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	●	●	●	●

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**

  FDP_ACC.1は、オブジェクト；ユーザ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.USER-BOXは、サブジェクト：「ユーザボックスを操作するプロセス」のオブジェクト：「ユーザボックス」に対する操作：「ユーザボックス内のユーザボックスデータ読み出し」及び「作成」を制御する「ユーザボックスアクセス制御」を実施している。

  従って本機能要件は満たされる。

- **FDP_ACF.1**

  FDP_ACF.1は、制御されるサブジェクト：「ユーザボックスを操作するプロセス」、オブジェクト：「ユーザボックス」、操作：「ユーザボックス内のユーザ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.USER-BOXは、以下の3つの規則からなるユーザボックスアクセス制御を実施している。

  - 選択した“ユーザボックス識別子”を持つユーザボックスを操作するプロセスが、これと一致する“ユーザボックス識別子”を持つユーザボックスに対してユーザボックス内のユーザボックスデータ読み出し操作を許可される。
  - 入力された“ユーザボックス識別子”を持つユーザボックスを操作するプロセスが、これと一致する“ユーザボックス識別子”を持つユーザボックスが存在しない場合、入力された“ユ

ーザボックス識別子 ” をオブジェクト属性とするユーザボックスの作成操作を許可される。

- 入力された “ ユーザボックス識別子 ” を持つ、ユーザボックスを操作するプロセスが、これと一致する “ ユーザボックス識別子 ” を持つユーザボックスが存在する場合、入力された “ ユーザボックス識別子 ” をオブジェクト属性とするユーザボックスの作成操作を拒否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。

- **FIA_AFL.1[1]**

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。

従って本機能要件は満たされる。

- **FIA_AFL.1[2]**

FIA_AFL.1[2]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。このロック状態は、F.ADMINの提供するペナルティ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[3]は、ユーザ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.USER-BOXは、ユーザ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の提供するペナルティ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[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、ユーザ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.USER-BOXは、ユーザボックスパスワードの変更機能にてユーザ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は、ユーザボックスパスワードの変更機能にてユーザ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、一般ユーザのユーザボックスに対するアクセスにおいて、ユーザ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.USER-BOXは、ユーザボックスの正当な利用者である一般ユーザをユーザボックスパスワードより認証し、認証されたユーザボックスの正当な利用者である一般ユーザだけに、対象としているユーザ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.ADMIN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。

  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.USER-BOXは、ユーザ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（ユーザ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.ADMIN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、またはクライアントPC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.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、ユーザボックスを扱う一般ユーザをそのユーザ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.USER-BOXは、ユーザボックスデータに対するアクセスにおいて設定されるユーザボックス識別名称を選択することによってユーザ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。

  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、アクセスチェック機能のふるまいを管理することを規定している。
  F.ADMINは、アクセスチェック機能を動作・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**

  FMT_MSA.1は、ユーザ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ユーザボックス識別子の改変操作を“ユーザ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は、管理者モードにて管理者が操作するユーザボックス識別子を改変する機能を提供する。
  F.USER-BOXは、ユーザ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ユーザボックス識別子を改変する機能を提供する。
  従ってこの2つのTOEセキュリティ機能が動作することにより本機能要件は満たされる。

- **FMT_MSA.3**

  FMT_MSA.3は、ユーザ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ユーザ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ユーザ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.USER-BOXは、ユーザボックスの作成機能が起動されると、ユーザ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、当該ユーザ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ユーザ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_MTD.1[1]**

  FMT_MTD.1[1]は、TSFデータである管理者モードパスワードを改変する役割を規定している。
  F.ADMINは、管理者モードにて管理者が操作する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。
  従って本機能要件は満たされる。

- **FMT_MTD.1[2]**

  FMT_MTD.1[2]は、TSFデータであるユーザ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は、管理者モードにて管理者が操作するユーザボックスパスワードを変更する機能を提供している。

  F.USER-BOXは、ユーザボックスの正当な利用者である一般ユーザが操作するユーザボックスパスワードを変更する機能を提供している。

  従ってこの2つのTOEセキュリティ機能が動作することにより本機能要件は満たされる。

- **FMT_MTD.1[3]**

  FMT_MTD.1[3]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[4]**

  FMT_MTD.1[4]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。

  従って本機能要件は満たされる。

- **FMT_MTD.1[5]**

  FMT_MTD.1[5]は、親展プリント不正アクセス検出カウント値、ユーザ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は、管理者モードにて管理者が操作するペナルティ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_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.USER-BOXは、ユーザボックスの正当な利用者である一般ユーザがユーザ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。

  - 当該ユーザボックスのユーザボックス識別子の変更機能
  - 当該ユーザボックスのユーザボックスパスワードの変更機能

  またF.USER-BOXは、ユーザボックスの作成において、当該ユーザ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。

  - ユーザボックス識別子の作成機能

F.ADMIN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。

- アクセスチェック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クリアするペナルティ解除機能
- ユーザボックス不正アクセス検出カウント値を0クリアするペナルティ解除機能
- 管理者モードパスワードを変更する機能
- 任意のユーザボックスにおけるユーザボックス識別子の変更機能
- 任意のユーザボックスにおけるユーザボックスパスワードの変更機能

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「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.USER-BOX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[2]**

FMT_SMR.1[2]は、役割に「管理者」を持つことを規定している。

F.ADMIN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[3]**

FMT_SMR.1[3]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。

- **FMT_SMR.1[4]**

FMT_SMR.1[4]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.USER-BOX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。

- **FPT_RVM.1**

FPT_RVM.1は、TOEの各セキュリティ機能の動作進行が許可される前に必ずTSP実施機能が必ず呼び出されることをサポートすることを規定している。

F.ADMINは、管理者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識別認証する機能が動作する。また同じくF.ADMIN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。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、親展プリントジョブ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識別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.USER-BOXは、ユーザボックスデータのダウンロード機能及び一般ユーザが操作するセキュリティ管理機能であるユーザボックス識別子、ユーザボックスパスワードを変更する機能は、その実行が許可される前にユーザ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認証する機能が動作する。このユーザボックスに対するアクセスにおける認証機能は、各機能の実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。

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における管理者認証後のセキュリティドメインは、パネルアクセスした場合とクライアントPCからアクセスした場合の2つに分類される。両者とも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.USER-BOXは、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.SERVICEは、サービスコードによる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において、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。

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。

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 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.USER-BOX における ユーザ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、アクセスチェック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、アクセスチェック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 ～