bizhub 42 / bizhub 36 / ineo42 / ineo36 全体制御ソフトウェア A3EW30G0224 A3EW99G0010000 セキュリティターゲット

バージョン：1.05

発行日：2012年01月16日

作成者：コニカミノルタビジネステクノロジーズ株式会社

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2011/6/9	1.00	オフィスHW開発部	永田	太田	津山	初版
2011/10/11	1.01	オフィスHW開発部	永田	太田	津山	モデル名修正、誤植修正
2011/10/17	1.02	オフィスHW開発部	永田	太田	津山	ガイダンスの識別修正
2011/10/25	1.03	オフィスHW開発部	永田	太田	津山	ガイダンスの表記修正
2012/01/11	1.04	オフィスHW開発部	永田	太田	津山	TOEバージョン改訂
2012/01/16	1.05	オフィスHW開発部	永田	太田	津山	ハードウェア構成（FAXユニット）の明確化

—【 目次 】

—【 図目次 】

—【 表目次 】

1. ST 概説

1.1. ST 参照

・ST名称 : bizhub 42 / bizhub 36 / ineo42 / ineo36
全体制御ソフトウェア
A3EW30G0224
A3EW99G0010000
セキュリティターゲット
・STバージョン : 1.05
・作成日 : 2012年01月16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　津山 繁浩

1.2. TOE 参照

・TOE名称 : 日本語名：
bizhub 42 / bizhub 36 / ineo42 / ineo36
全体制御ソフトウェア
英語名 :
bizhub 42 / bizhub 36 / ineo42 / ineo36
Control Software
・TOE識別 : A3EW30G0224（バージョン：「A3EW30G」、リビジョン：「0224」、TOE識別の説明：コントローラーファームウェア）
A3EW99G0010000（バージョン：「A3EW99G」、リビジョン：「0010000」、TOE識別の説明：Boot制御部）
・製造者 : コニカミノルタビジネステクノロジーズ株式会社

1.3. TOE 概要

本節ではTOE種別、TOEの使用方法及び主要なセキュリティ機能について説明する。なお、TOEの動作環境については、「1.4」節に記述する。

1.3.1. TOE の種別

bizhub 42 / bizhub 36 / ineo42 / ineo36 とは、コピー、プリント、スキャン、FAX の各機能で構成されるコニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機である。（以下、これらすべての総称として mfp と呼称する。）TOE が搭載される mfp 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。

TOE である bizhub 42 / bizhub 36 / ineo42 / ineo36 全体制御ソフトウェアとは、mfp 制御コントローラー上のフラッシュメモリと SSD にあって、mfp 全体の動作を統括制御する組み込み型ソフトウェアである。

1.3.2. TOE の使用方法、及び主要なセキュリティ機能

TOE は、mfp 本体のパネルやネットワークから受け付ける操作制御処理、画像データの管理等、

mfp の動作全体を制御する“bizhub 42 / bizhub 36 / ineo42 / ineo36 全体制御ソフトウェア”である。

TOE は、mfp に保存される機密性の高い保護対象資産の暴露に対する保護機能を提供する。他に、TOE は各種上書き消去規格に則った削除方式を有し、HDD のすべてのデータを完全に消去し、mfp を廃棄・リース返却する際に利用することによって mfp を利用する組織の情報漏洩の防止に貢献する。

なお、HDD 内に格納される保護対象資産及び副次的保護対象資産は、外部 IT エンティティであるセキュリティチップ（セキュリティ・アクセラレータ）によって暗号化され、暴露されることが防止される。この外部 IT エンティティが提供する暗号化機能は、保証の対象外である。

1.4. TOE 記述

1.4.1. TOE の利用に関係する人物の役割

TOE が搭載される mfp の利用に関連する人物の役割を以下に定義する。

- **管理者**
  mfp の運用管理を行う mfp の利用者。mfp の動作管理、ユーザーの管理を行う。（一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される。）なお、管理者のアカウントは Built-in アカウントである。

- **サービスエンジニア**
  mfp の保守管理を行う利用者。保守契約が結ばれた場合、mfp の修理、調整等の保守管理を行う。（一般には、コニカミノルタビジネステクノロジーズ株式会社と提携し、mfp の保守サービスを行う販売会社の担当者が想定される。）サービスエンジニアのアカウントは、Built-in アカウントである。

- **ユーザー**
  mfp に登録される mfp の利用者。（一般には、オフィス内の従業員などが想定される。）
  管理者、及びサービスエンジニアは、ユーザーには含まれない。

- **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。

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

1.4.2. TOE の物理的範囲

TOE の物理的範囲は、以下のソフトウェアである。

・コントローラーファームウェア（SSD に存在）

・Boot 制御部（フラッシュメモリに存在）

TOE には OS（VxWorks）が含まれている。

また、mfp には TOE 以外のファームウェアとして、Engine、Panel、Scanner、Fax のファームウェアが存在する。

1.4.2.1. 利用環境

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

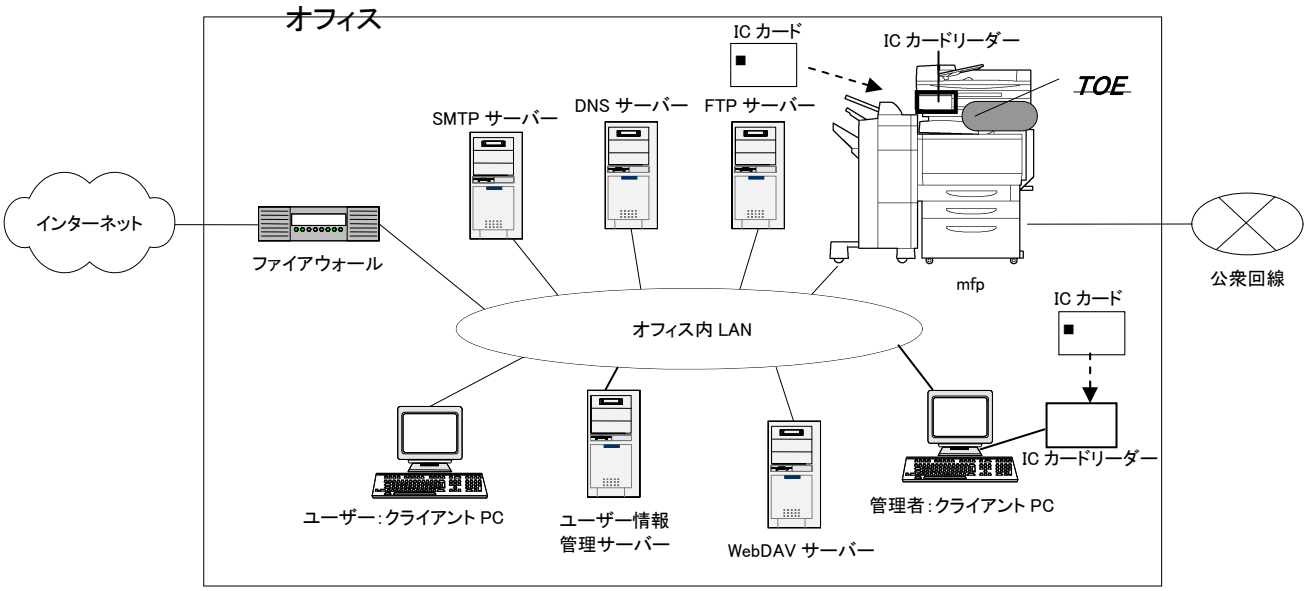

図 1　mfp の利用環境の例

- オフィス内部のネットワークとしてオフィス内 LAN が存在する。
- mfp はオフィス内 LAN を介してクライアント PC と接続され、相互にデータ通信を行える。
- オフィス内 LAN に SMTP サーバー、FTP サーバー、WebDAV サーバーが接続される場合は、mfp はこれらともデータ通信を行うことが可能。（なお SMTP サーバー、FTP サーバー、WebDAV サーバーのドメイン名を設定する場合は、DNS サーバーが必要になる。）
- ユーザーID、ユーザーパスワードをサーバーにて一元管理しているケースも想定する。この場合、ユーザー情報管理サーバーにおけるユーザー登録情報を使って TOE は mfp へのアクセスを制御することが可能。
- ユーザーは、mfp に接続された IC カードリーダーを使用して mfp を利用することができる。この場合、TOE は外部 IT エンティティである IC カードリーダーと連携して mfp の利用を許可する。
- 管理者のクライアント PC に接続された IC カードリーダーは、ユーザーの IC カード情報を読み込む際に使用する。
- オフィス内 LAN が外部ネットワークと接続する場合は、ファイアウォールを介して接続する等の

措置が取られ、外部ネットワークから mfp に対するアクセスを遮断するための適切な設定が行われる。

- オフィス内 LAN は、スイッチングハブ等の利用、盗聴の検知機器の設置などオフィスの運用によって、盗聴されないネットワーク環境が整備されている。
- mfp に接続される公衆回線は、FAX の通信に利用される。
- WebDAV サーバーは、WWW（World Wide Web）でファイルの転送に使われる HTTP（HyperText Transfer Protocol）を拡張し、クライアント PC の Web ブラウザから Web サーバー上のファイルやフォルダを管理できるようにした仕様を持つサーバーである。WebDAV サーバーを利用して、mfp にアクセスすることができるが、Scan to HDD Data、Secure Print Data、及び ID&Print Data にアクセスすることはできない。

1.4.2.2. 動作環境

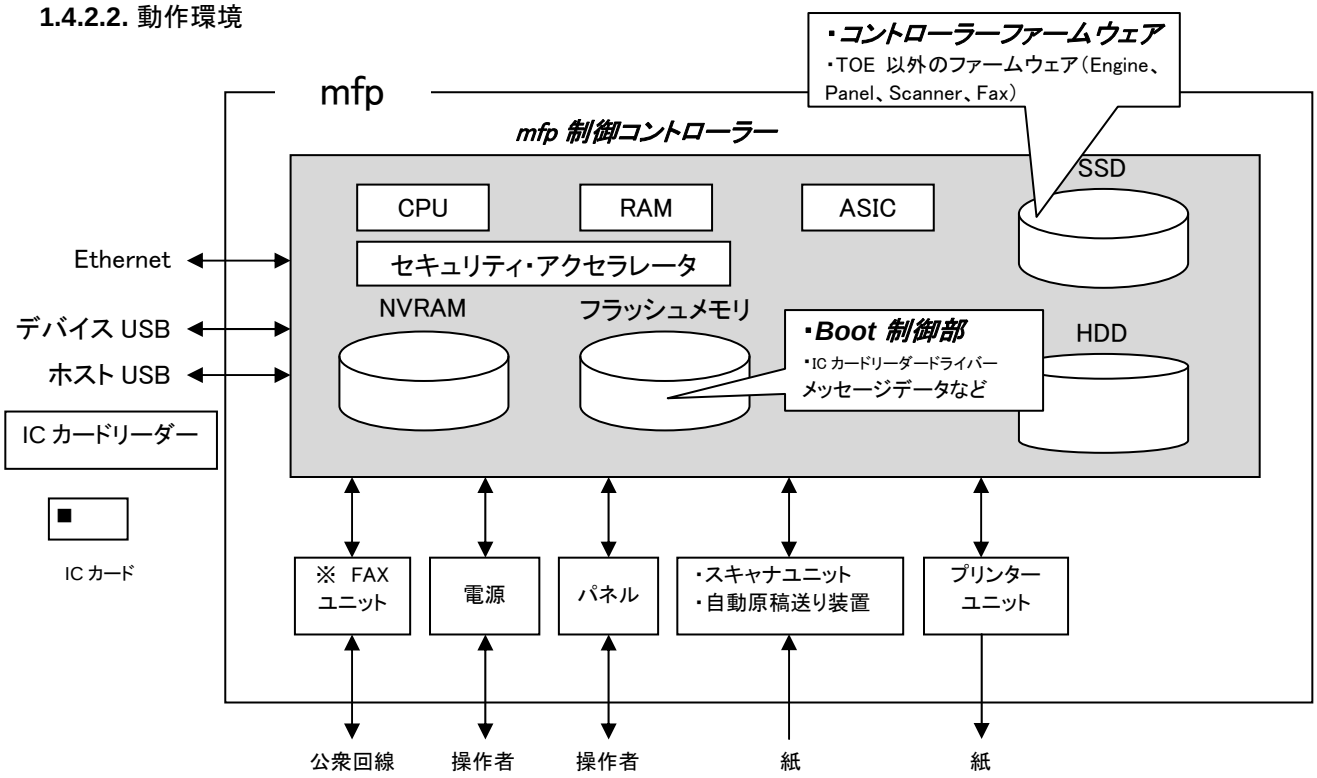

図 2　TOE に関係するハードウェア構成

TOEが動作するために必要なmfp上のハードウェア環境の構成を 図 2 に示す。mfp制御コントローラーはmfp本体内に据え付けられ、TOEはそのmfp制御コントローラー上のフラッシュメモリにBoot制御部、SSDにコントローラーファームウェアが存在し、電源がONになると揮発性RAM（図 2においては、「RAM」と表記）にロードされ動作する。

以下には 図 2 にて示されるmfp制御コントローラー上の特徴的なハードウェア、mfp制御コントローラーとインターフェースを持つハードウェアについて説明する。

- フラッシュメモリ

  TOE である mfp 全体制御ソフトウェアにおける Boot 制御部のオブジェクトコードが保管される記憶媒体。TOE 以外にメッセージデータ、IC カードリーダードライバーなどが保管される。

- HDD（ハードディスクドライブ）

  画像データがファイルとして保管されるほか、ユーザーID、IC カード ID、ユーザーパスワード、

Secure Print パスワードなどが保管される。

- NVRAM
  不揮発性メモリ。TOEの処理に使われるmfpの動作において必要な様々な設定値等が保管される記憶媒体。NVRAMには、管理者パスワード、CE[1]パスワード、SNMPパスワードが保管される。

- セキュリティチップ(セキュリティ・アクセラレータ)
  HDD に書き込まれるデータを暗号化・復号化するための暗号化機能を、mfp 制御コントローラー基板上に実装している。

- パネル
  タッチパネル液晶ディスプレイとテンキーやスタートキー、ストップキー、画面の切り替えキー等を備えた mfp を操作するための専用コントロールデバイス。

- 電源
  mfp を動作させるための電源スイッチ。

- Ethernet
  Ethernet 接続インターフェースデバイス。10BASE-T、100BASE-TX、Gigabit Ethernet をサポート。

- デバイス USB
  mfp 本体の後ろ側にあるローカル接続でプリントするためのポート。

- ホスト USB
  mfp のパネル側にある USB ポート。TOE のアップデート、USB インターフェースに接続した USB メモリからの印刷或いはスキャンしたデータを保存することが可能。なお、この印刷及びスキャンには本 ST に記述される Secure Print、Scan to HDD、及び ID&Print 機能は含まれていない。
  また、IC カードリーダーを接続することによって、ユーザーは IC カードを利用して mfp にアクセスすることが可能。IC カードリーダーは販売の都合により mfp には標準搭載されず、オプションパーツである。

- FAX ユニット（※オプションパーツ）
  公衆回線を介して FAX の送受信に利用されるデバイス。販売上の都合により mfp には標準搭載されず、オプションパーツとして販売される。なお、TOE を搭載する mfp は、FAX 付き mfp と FAX なし mfp の両方を指す。

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

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

[1] Customer Service engineer の略称。また、CE はサービスエンジニアの略称でも使用される。

- SSD（Solid State Drive）
  2GB の Flash Memory Drive である。TOE である mfp 全体制御ソフトウェアにおけるコントローラーファームウェアのオブジェクトコード、画像データ、TOE 以外のファームウェアである Engine、Panel、Scanner、Fax のファームウェアのオブジェクトコードなどが保管される記憶媒体。

- ASIC（Application Specific Integrated Circuit）
  画像処理全般を行うために設計された集積回路。また、画像を印刷するときに画像の展開と色合いの調整等の処理も行う。

- IC カード
  プラスチック製カードに半導体集積回路（IC チップ）を埋め込み、情報を記録できるカード。

- IC カードリーダー
  IC カードを読み取るための機器。

- IC カードリーダードライバー
  IC カードリーダーにアクセスするためのドライバー。

1.4.2.3. ガイダンス

[海外版]
- bizhub 42 / bizhub 36 SERVICE MANUAL SECURITY FUNCTION
- ineo 42 / ineo 36 SERVICE MANUAL SECURITY FUNCTION
- bizhub 42 / bizhub 36 User's Guide [Security Operations]
- ineo 42 / ineo 36 User's Guide [Security Operations]

[日本版]
- サービスマニュアル　セキュリティ機能編 bizhub 36
- ユーザーズガイド　セキュリティ機能編 bizhub 36

1.4.3. TOE の論理的範囲

利用者は、パネルやクライアント PC からネットワークを介して TOE の各種機能を使用する。以下には、基本機能、利用者であるユーザーの識別認証機能、管理者が操作する管理者機能、サービスエンジニアが操作するサービスエンジニア機能､ユーザーには意識されずにバックグラウンドで動作する機能を説明する。

1.4.3.1. 基本機能

mfp には、基本機能としてコピー、プリント、スキャン、FAX といった画像に関するオフィスワークのための一連の機能が存在する。mfp 制御コントローラー外部のデバイスから取得した生データを画像ファイルに変換し、コピー、プリント、スキャンの画像ファイルは HDD に登録し、Fax の画像ファイルは SSD に圧縮して登録する。（クライアント PC からのプリント画像ファイルは、複数の変換処理が行われる。）画像ファイルは、印刷用または送信用のデータとして変換され、目的の mfp 制御コントローラー外部のデバイスに転送される。コピー、プリント、スキャン、Fax の処理において一時的に登録された画像ファイルは、処理終了後論理的に削除する。

コピー、プリント、スキャン、FAX などの動作は、ジョブという単位で管理され、パネルからの

指示により、印字されるジョブであれば仕上がり等の変更、動作の中止が行える。
TOE が提供するセキュリティ機能は、スキャン、及びプリントの一部（Scan to HDD、Secure Print、ID&Print）の制御を行う。
以下は基本機能においてセキュリティと関係する機能である。

- ID&Print 機能
  本機能を管理者が利用設定すると、通常のプリントデータを印刷待機状態で HDD に保管し、パネルからのユーザー識別認証処理、もしくは IC カードリーダーからのユーザー識別処理で印刷を行う機能。利用設定がなくとも、プリントデータに本機能の動作指定がある場合は、管理者による利用設定がある場合と同様に動作する。

- Secure Print 機能（なお、この機能はガイダンス上では「Secured Job」と称す。）
  プリントデータと共に Secure Print パスワードを受信した場合、画像ファイルを印刷待機状態で保管し、パネルからの印刷指示とパスワード入力により印刷を実行する。また、削除指示とパスワード入力により、該当 Secure Print Data の削除を実行する。なお、このデータの一覧表示は、すべてのユーザーに許可される。
  これよりクライアント PC からのプリント行為において、機密性の高いプリントデータが、印刷された状態で他の利用者に盗み見られる可能性や、他の印刷物に紛れ込む可能性を排除する。

- Scan to HDD 機能
  スキャンされた画像データをユーザー情報とともに HDD に保管する。ユーザーは、HDD に保管するとき、Private（秘密）または Public（公開）として画像データを保管することができる。Private として保管された画像データ（Scan to HDD Data）は、クライアント PC からのユーザーID とパスワード入力により、識別認証が成功するとダウンロード、一覧表示、削除が許可される。
  これよりクライアント PC からのダウンロード行為において、機密性の高いスキャンして HDD に保管された画像データが、許可されない利用者に不正アクセスされる可能性を排除する。

1.4.3.2. ユーザー認証機能

TOE は、mfp の利用を mfp に登録された利用者であるユーザーだけに制限することができる。パネル、またはネットワークを介したアクセスにおいて TOE は mfp の利用を許可されたユーザーであることをユーザーID、ユーザーパスワードを使って識別認証する。また、管理者が IC カードリーダードライバーを mfp にインストールすることによって、IC カードを使ってユーザーを識別することができる。（この機能を IC カード機能と称す。）IC カードを利用する場合は、ユーザー認証機能の方式に「本体認証」を設定する。
TOE は、パネルを介したアクセスにおいて、ユーザーID、ユーザーパスワードの識別認証が成功する、もしくは IC カードリーダーを介したアクセスにおいて、IC カード ID の識別が成功すると、ユーザーに対して基本機能などの利用を許可する。ネットワークを介したアクセスにおいては、ユーザーID、ユーザーパスワードの識別認証が成功するとセッション情報が生成されて、セッションを維持している間はセッション情報を使って認証する。ユーザー認証機能は、セキュリティと関係する機能である。
ユーザー認証の方式には、以下に示す 2 つのタイプをサポートしている。

① **本体認証**
mfp 制御コントローラー上の HDD にユーザーID、ユーザーパスワードを登録し、mfp にて認証する方式。またこの他、HDD に個々のユーザーの IC カード ID を登録し、mfp にて識別す

ることも可能である。

② **外部サーバー認証**

mfp本体側でユーザーID及びユーザーパスワードを管理せず、オフィス内LANで接続されるユーザー情報管理サーバー上に登録されるユーザーID及びユーザーパスワードを用いて、mfpにて認証処理を行い、認証する方式。Active Directory[2]、NTLM[3]等といった複数の方式をサポートしているが、本STにおいて想定する外部サーバー認証の方式は、Active Directoryの利用ケースのみとする。

1.4.3.3. 管理者機能

TOE は、認証された管理者だけが操作することが可能な管理者モードにて本体認証の場合におけるユーザーの情報の管理、ネットワークや画質等の各種設定の管理などの機能を提供する。

以下にはセキュリティに関係する機能について説明する。

- 管理者の認証機能
  - パネル、及びネットワークを介したアクセスにおいて、TOE は管理者 ID（“Admin”固定)、管理者パスワードを使って識別認証する。識別認証が成功すると、TOE は管理者に管理機能の利用を許可する。ネットワークを介したアクセスにおいては、管理者 ID、管理者パスワードの識別認証が成功するとセッション情報が生成されて、セッションを維持している間は、セッション情報を使って認証する。管理者は、IC カードを使用して管理機能を利用することができない。
- 管理者パスワードの管理機能
  - パネルを介して、管理者のパスワードを変更する機能。なお、管理者のパスワードは、サービスエンジニアによって変更（初期化）することができる。
- ユーザーの登録管理
  - ユーザーID、ユーザーパスワードの登録・変更、ユーザーの削除
- ネットワーク設定管理
  - IP アドレス、AppleTalk プリンター名などの設定
- HDD の一部のデータのバックアップ及びリストア機能
  - バックアップの対象データは、ユーザーに関わるデータ（ユーザーID、ユーザーパスワード、IC カード ID、など)、Scan to HDD Data である。
  - リストアの対象データは、ユーザーに関わるデータ（ユーザーID、ユーザーパスワード、IC カード ID、など）である。
  - クライアント PC に導入される専用アプリケーションを利用して、バックアップ（データの問い合わせ)、リストアが実行される。なお、Scan to HDD Data は Scan to HDD 機能を利用してバックアップが実行される。
- 全データ上書き消去機能
  - HDD の上書き消去に対して、各種軍用規格（米国国防総省規格等）に則ったデータ消去方式をサポート
  - 全データ上書き消去機能は、パネルを介して起動する。
  - 管理者が選択したデータ消去方法に従い、HDD の全データ領域に対して、上書き消去を行う。

[2] Windows プラットフォームのネットワーク環境にてユーザー情報を一元管理するために Windows Server 2000（それ以降）が提供するディレクトリサービスの方式。

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

- SSD のデータ領域に対して、固定値（0x00）で上書き消去を行う。
- NVRAM のデータ（管理者パスワード、SNMP パスワード、など）に対して、初期化を行う。

- 高信頼チャネル機能
  - クライアント PC と mfp 間で画像ファイル（Scan to HDD Data など）を送受信する際に、SSL または TLS プロトコルを使用して、高信頼チャネルを生成、及び実現する。
- パスワード規約機能
  - パスワード規約機能の設定が“有効”の場合、各種パスワードの有効桁数等、パスワード諸条件をチェックする。
- HDD 論理フォーマット機能
  - パネルを介して、論理フォーマットが実行可能。
  - 論理フォーマットは、HDD を初期化する場合に使用する。

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- ユーザー認証機能の方式設定
  - 本体認証、外部サーバー認証、ユーザー認証停止を選択
  - 本体認証を選択した場合、かつ IC カード機能を使用する場合は、IC カード機能の設定が必要
  - IC カード機能の設定は、IC カード方式に「IC カード」、「IC カード+ユーザーパスワード」、「IC カードを使用しない」を選択
  - 「IC カード」が選択されると、ユーザーID とユーザーパスワードを使用した識別認証の他に、IC カードを使用した識別が可能
  - 「IC カード+ユーザーパスワード」が選択されると、ユーザーID とユーザーパスワードを使用した識別認証の他に、IC カードとユーザーパスワードを使用した識別認証が可能
  - 「IC カードを使用しない」が選択されると、IC カードを使用した識別は行わない
  - 外部サーバー認証が選択されている場合は、IC カード機能を使用することができない
- ユーザーID で特定されない利用者によるアクセスの禁止の設定
  - ユーザーID で特定されない利用者に対して、mfp の利用を禁止する機能の有効、無効を選択
- 認証なしプリントの設定
  - ユーザーID で特定されない利用者に対して、印刷する機能の有効、無効を選択
- パスワード規約機能の設定
  - 各種パスワードの有効桁数等、パスワード諸条件をチェックする機能の動作、禁止を選択
- システムオートリセットの動作設定
  - 設定時間が経過すると、パネル操作を自動的にログアウトする機能の設定
- SNMPv1、v2 によるネットワーク設定変更機能の設定
  - SNMPv1、v2 による MIB の変更操作機能を許可、禁止を選択
- SNMPv3 の書込み操作における認証機能動作設定
  - 認証しない、認証動作のセキュリティレベルを選択
  - 認証動作のセキュリティレベルには、Authentication パスワードのみ、Authentication パスワード且つ Privacy パスワードを設定する場合が存在
- 高信頼チャネル（SSL/TLS 暗号通信）機能の設定
  - サーバー証明書を生成、またはインポート
  - 通信に利用される暗号方式・暗号強度の設定が可能
  - 動作、停止を選択
- 全データ上書き消去機能の動作
  - HDD に対しては、データ消去方法を選択
  - 全データ上書き消去機能を起動
- FTP サーバー機能の設定

- 動作、停止を選択
- FTP サービスは、ユーザー毎の印刷枚数を表すカウンタ情報を管理する機能
- カウンタ情報と共に部門及びユーザー個々の情報も集約管理することが可能
- 動作を選択した場合、FTP サーバーとの通信が可能

- ID&Print 機能の設定
  - ID&Print 機能の有効、無効を選択

1.4.3.4. サービスエンジニア機能

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

- サービスエンジニアの認証機能
  - パネルを介したアクセスにおいて TOE は CE パスワードを使って識別認証する。識別認証が成功すると、TOE はサービスエンジニアにサービスエンジニア機能の利用を許可する。サービスエンジニアは、IC カードを使用してサービスエンジニア機能を利用することができない。
- 管理者パスワードの管理機能
  - 管理者のパスワードを変更する機能（本 ST では、サービスエンジニアが管理者のパスワードを初期化することをパスワードの変更と表現する）

1.4.3.5. その他の機能

TOE はユーザーには意識されないバックグラウンドで処理される機能やファームウェアアップデート更新機能などを提供する。以下に代表的な機能について説明する。

① **遠隔診断機能（CSRC）**
WebDAV の接続方式を利用して、コニカミノルタビジネステクノロジーズ株式会社が管理、運営する mfp のサポートセンターと通信し、mfp の動作状態、印刷数等の機器情報を管理する。また、追加トナーの発送、課金請求、故障診断からサービスエンジニアの派遣などのサービスを提供するために、CSRC による機器情報の管理を行う。

② **ファームウェアアップデート更新機能**
TOE は TOE 自身を更新するための機能を有する。クライアント PC と mfp 間を SSL 通信でつなぎ更新する方法(ファームウェアアップデート更新機能)、USB メモリ等のメモリ媒体を接続して行う方法がある。ファームウェアアップデート更新機能は、セキュリティ強化機能が有効な場合は、その機能を使用することができない。また、USB メモリ等のメモリ媒体を接続した更新機能は、サービスエンジニアのみに提供する。

③ **IC カード機能の活用**
外部 IT エンティティである IC カードリーダードライバーを利用して、TOE はユーザーに mfp へのアクセスを提供する。

以下はその他の機能においてセキュリティと関係する機能である。

- **暗号通信機能**
  TOE はクライアント PC から mfp へ送信するデータ、mfp からダウンロードして受信するデータを SSL/TLS を利用して暗号化することができる。本機能は、管理者機能にて動作設定が行える。

1.4.3.6. セキュリティ強化機能

管理者機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また個別には動作設定機能を持たない機能として、TELNET の機能が存在するが、この機能の利用は禁止される。

以下にセキュリティ強化機能有効時の一連の設定状態をまとめる。なお、セキュリティ強化機能を有効にするためには、高信頼チャネル機能において使用する証明書を登録する、ユーザー認証機能の方式設定を“有効”（本体認証、外部サーバー認証のどちらでも可）にする、パスワード規約機能の設定を“有効”にする事前準備が必要である。また、パスワード規約機能の設定を“有効”にするためには、管理者パスワード、SNMP パスワードを事前にパスワード規約に違反しない値に設定しておく必要がある。
また、セキュリティ強化機能有効には、ファームウェアアップデート更新機能を使用することができない。

- ユーザーID で特定されない利用者によるアクセスの禁止の設定　：有効
- 認証なしプリントの設定　：無効
- ユーザーID 一覧表示　：禁止
- SNMPv1、v2 によるネットワーク設定変更機能の設定：禁止
- SNMPv3 による書き込み操作時認証動作　：有効
- 遠隔診断機能(CSRC)による設定　：禁止
- 高信頼チャネル機能の動作設定　：有効
- ネットワーク経由の管理者パスワード変更　：　禁止

以下の機能はセキュリティ強化機能が有効になるタイミングで以下に示される設定状態になるが、上記の機能群と異なり、個別に設定を変更することが可能である。

- FTP サーバー機能の設定　：禁止

2. 適合主張

2.1. CC 適合主張

本STは、以下の規格に適合する。

情報技術セキュリティ評価のためのコモンクライテリア
パート1：概説と一般モデル　2009年7月　バージョン3.1　改訂第3版（翻訳第1.0版）
パート2：セキュリティ機能コンポーネント　2009年7月　バージョン3.1　改訂第3版（翻訳第1.0版）
パート3：セキュリティ保証コンポーネント　2009年7月　バージョン3.1　改訂第3版（翻訳第1.0版）

- セキュリティ機能要件　：パート2 拡張。
- セキュリティ保証要件　：パート3 適合。

2.2. PP 主張

本 ST が適合する PP はない。

2.3. パッケージ主張

本 ST は、保証パッケージ：EAL3 に適合する。追加する保証コンポーネント機能はない。

2.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model July 2009 Version 3.1 Revision 3 CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components July 2009 Version 3.1 Revision 3 CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components July 2009 Version 3.1 Revision 3 CCMB-2009-07-003
- Common Criteria for Information Technology Security Evaluation Evaluation methodology July 2009 Version 3.1 Revision 3 CCMB-2009-07-004
- 評価方法　2009年7月　バージョン3.1　改訂第3版（翻訳第1.0版）

3. セキュリティ課題定義

本章では、保護対象資産の考え方、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 保護対象資産

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

- Secure Print Data （セキュアプリントファイル）
  Secure Print により HDD 上に登録される画像ファイル
- Scan to HDD Data（スキャンハードディスクファイル）
  Scan to HDD により HDD 上に Private として登録される画像ファイル
  Scan to HDD には、Public として登録される画像ファイル、スキャンした画像データを E-mail で送信する機能（Scan to E-mail）などは含まれない。
- ID&Print Data （ID プリントファイル）
  ID&Print により HDD 上に登録される画像ファイル

ユーザーが意図して mfp の HDD 上に蓄積する Secure Print Data、Scan to HDD Data、ID&Print Data を保護対象として、それ以外の画像ファイルは保護対象とは扱わない。

なお Secure Print Data、ID&Print Data の印刷においては、万が一不正な mfp が接続され、その不正な mfp に登録されてしまった画像が漏洩する脅威に備え、mfp の設定データ（IP アドレスなど）等を不正に変更出来ないようにする必要がある。従って mfp の設定（IP アドレスなど）は副次的な保護資産として考慮する。

また、以下の TSF データを保護対象資産とする。パスワードは暴露及び改ざんから保護し、ユーザー識別情報、IC カード情報、高信頼チャネルの設定データ、及び外部サーバー識別設定データは改ざんから保護する。

- **パスワード**
  NVRAM 上に登録される管理者パスワード、CE パスワード、SNMP パスワード。
  HDD 上に登録されるユーザーパスワード、Secure Print パスワード。
- **ユーザー識別情報**
  HDD 上に登録されるユーザー識別情報。
- **IC カード情報**
  HDD 上に登録されるユーザーの IC カード情報。
- **高信頼チャネルの設定データ**
  NVRAM に保管される高信頼チャネルの設定データ。
- **外部サーバー識別設定データ**
  HDD に保管される外部サーバー識別の設定データ。

一方、mfp をリース返却、廃棄して利用が終了した場合など組織の管轄から保管されるデータが物理的に離れる場合は、組織は HDD、SSD に残存するあらゆるデータ、及び NVRAM に保管されている設定データの漏洩可能性を懸念する。従ってこの場合は以下のデータファイルを保護対象とする。

リース返却、廃棄するなど利用を終了した場合、以下のデータファイルを保護対象とする。

- Secure Print Data （セキュアプリントファイル）
  Secure Print により HDD 上に登録される画像ファイル
- Scan to HDD Data（スキャンハードディスクファイル）
  Scan to HDD により HDD 上に Private として登録される画像ファイル
- ID&Print Data （ID プリントファイル）
  ID&Print により HDD 上に登録される画像ファイル
- 待機状態にあるジョブの画像ファイル
  待機状態にあるジョブの画像ファイルで HDD データ領域に存在する画像ファイル
- 保管画像ファイル
  Secure Print Data、Scan to HDD Data、ID&Print Data 以外に HDD データ領域に保管される画像ファイル
- HDD 残存画像ファイル
  一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、HDD データ領域に残存するファイル
- SSD 画像ファイル
  SSD のデータ領域に保管されるファイル、一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、SSD のデータ領域に残存するファイル
- 画像関連ファイル
  プリント画像ファイル処理において HDD 上に生成されたテンポラリデータファイル
- 送信宛先データファイル
  画像を送信する宛先となる E-mail アドレス、電話番号などが含まれる、SSD 上のデータ領域に保管されるファイル
- 管理者パスワード
  NVRAM に保管される管理者のパスワード
- ユーザー識別情報
  HDD に保管されるユーザーの識別情報
- ユーザーパスワード
  HDD に保管されるユーザーのパスワード
- IC カード情報
  HDD に保管されるユーザーの IC カード情報
- SNMP パスワード
  NVRAM に保管される SNMP のパスワード
- Secure Print パスワード
  HDD に保管される Secure Print のパスワード
- 高信頼チャネルの設定データ
  NVRAM に保管される高信頼チャネルの設定データ
- 外部サーバー識別設定データ
  HDD に保管される外部サーバー識別の設定データ
- mfp の設定データ
  NVRAM に保管される mfp の設定データ
- 残存 TSF データ
  ファイル管理領域の削除だけでは削除されない、HDD データ領域に残存している TSF データ

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

A.ADMIN（管理者の人的条件）

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

A.SERVICE（サービスエンジニアの人的条件）

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

A.NETWORK（mfp のネットワーク接続条件）

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

A.SECRET（秘密情報に関する運用条件）

TOE の利用において使用される各パスワードは、管理者、およびユーザーから漏洩しない。

A.HDD-DATA（HDD データに関する運用条件）

mfp が有する HDD 内の保護対象資産は、HDD から直接解析できない。

3.3. 脅威

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

T.DISCARD-MFP（mfp のリース返却、廃棄）

リース返却、または廃棄となった mfp が回収された場合、悪意を持った者が、mfp 内の HDD、NVRAM、SSD を解析することにより、Secure Print Data、Scan to HDD Data、ID&PrintData、待機状態にあるジョブの画像ファイル、保管画像ファイル、HDD 残存画像ファイル、SSD 画像ファイル、画像関連ファイル、送信宛先データファイル、HDD や NVRAM 上に設定されていたパスワード（管理者パスワード、SNMP パスワード、ユーザー識別情報、ユーザーパスワード、IC カード情報、Secure Print パスワード）、mfp の設定データ、高信頼チャネルの設定データ、外部サーバー識別設定データ、残存 TSF データが漏洩する。

T.ACCESS-DATA（ユーザー機能を利用した Scan to HDD Data への不正なアクセス）

悪意を持った者や悪意を持ったユーザーが、クライアント PC を介して他のユーザーが個人所有する Scan to HDD Data にアクセスし、HDD に保管された Scan to HDD Data をダウンロードすることにより、Scan to HDD Data が暴露される。

T.ACCESS-SECURE-PRINT（ユーザー機能を利用した Secure Print Data、ID&Print Data への不正なアクセス）

悪意を持った者や悪意を持ったユーザーが、パネル、IC カードリーダーを介して利用を許可されない Secure Print Data、ID&Print Data を印刷することにより、Secure Print Data、ID&Print Data が暴露される。

T.UNEXPECTED-TRANSMISSION（想定外対象先への送信）

悪意を持った者や悪意を持ったユーザーが、パネル及びクライアント PC を介して TOE が導入される mfp に設定される mfp を識別するためのネットワーク設定を変更し、不正な別の mfp などのエンティティにおいて本来 TOE が導入される mfp の設定データ（AppleTalk プリンター名（クライアント PC のみ）、IP アドレス（パネル、クライアント PC）など）を設定する。

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

悪意を持った者や悪意を持ったユーザーが、パネルを介してセキュリティ強化機能に関係する設定を変更してしまうことにより、セキュリティ機能が無効化される。

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

悪意を持った者や悪意を持ったユーザーが、クライアント PC を介してバックアップ機能、リストア機能を不正に使用することにより、Scan to HDD Data が漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、mfp の設定（IP アドレスなど）が改ざんされる。

3.4. 組織のセキュリティ方針

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

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

P.COMMUNICATION-DATA（画像ファイルのセキュアな通信）

IT 機器間にて送受信される秘匿性の高い画像ファイル（Secure Print Data、Scan to HDD Data、ID&PrintData）は、正しい相手先に対して信頼されるパスを介して通信する、または暗号化しなければならない。

4. セキュリティ対策方針

本章では、3 章にて識別された前提条件、脅威、組織のセキュリティ方針を受けて、TOE 及び TOE の利用環境にて必要なセキュリティ対策方針について記述する。以下、TOE のセキュリティ対策方針、運用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.REGISTERED-USER（登録ユーザーの利用）

TOE は、管理者によって TOE に登録されたユーザーだけに TOE が搭載された mfp の利用を許可する。

O.SCAN-DATA（Scan to HDD Data アクセス制御）

TOE は、クライアント PC を介して Scan to HDD Data のダウンロードを、管理者、及び許可されたユーザーだけに許可する。

O.SECURE-PRINT（Print Data アクセス制御）

TOE は、パネル、IC カードリーダーを介して Secure Print Data、ID&Print Data の印刷を、許可されたユーザーだけに許可する。

O.CONFIG-A（セキュリティ強化機能の設定に関係する機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・セキュリティ強化機能の設定に関係する機能

O.CONFIG-B（mfp の設定データに関する機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・mfp の設定データに関する機能

O.CONFIG-C（バックアップ機能、リストア機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・バックアップ機能

・リストア機能

O.CONFIG-D（高信頼チャネル機能設定データの設定機能へのアクセス制限）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・高信頼チャネル機能設定データの設定機能

O.OVERWRITE-ALL（全データ上書き消去）

TOE は、mfp 内の HDD 及び SSD のデータ領域に記録されている Secure Print Data、Scan to HDD Data、ID&Print Data、待機状態にあるジョブの画像ファイル、保管画像ファイル、HDD 残存画像ファイル、SSD 画像ファイル、画像関連ファイル、送信宛先データファイル、及びユーザー、管理者が設定した NVRAM 上のパスワード（管理者パスワード、SNMP パスワード）、HDD 上のパスワード（ユーザーパスワード、Secure Print パスワード）、NVRAM 上の mfp の設定データ、高信頼チャネルの設定データ、及び HDD 上の外部サーバー識別設定データ、ユーザー識別情

報、IC カード情報、残存 TSF データを再現できなくする。

O.TRUSTED-PATH（高信頼チャネルの利用）

TOE は、TOE からクライアント PC に送信される以下の画像ファイルを、高信頼チャネルを介して通信する機能を提供する。

＜TOE からクライアント PC 送信される画像ファイル＞

Scan to HDD Data

O.AUTH-CAPABILITY（外部サーバー認証機能を利用するためのサポート動作）

TOE は、ActiveDirectory を用いたユーザー情報管理サーバーの外部サーバー認証によるユーザー識別認証情報を利用するために必要な動作をサポートする。

4.2. 運用環境のセキュリティ対策方針

本節では、TOE の運用環境のセキュリティ対策方針について識別し、説明する。

OE.FEED-BACK（保護された認証フィードバックを行うアプリケーション）

管理者は、管理者またはユーザーがクライアント PC から mfp にアクセスする際には、管理者パスワード、ユーザーパスワード、SNMP パスワードに対して、保護されたフィードバックを提供するアプリケーションを利用させる。

OE.SERVER（ユーザー情報管理サーバーの利用）

管理者は、ユーザーのアカウント管理において、mfp ではなく外部のユーザー情報管理サーバーを利用する場合、Active Directory によるユーザー管理を利用するための設定をする。また、管理者は Active Directory によるユーザーのアカウント情報が漏洩しないように、ユーザー情報管理サーバーに対して適切なアクセス管理を実施する。

OE.SESSION（操作後のセッションの終了）

管理者は、ユーザーに対して以下に示す運用を実施させる。

・クライアント PC を介した Secure Print Data、ID&Print Data の操作、Scan to HDD Data の操作の終了後にログアウト操作を行う。

管理者は、以下に示す運用を実施する。

・クライアント PC を介した管理者モードの諸機能を操作終了後にログアウト操作を行う。

OE.OVERWRITE（全データ上書き消去機能の実行）

管理者は、mfp をリース返却、廃棄するなど利用が終了した場合などユーザーの管轄から保管されるデータが物理的に離れる場合は、全データ上書き消去機能を実行する。

OE.ADMIN（信頼できる管理者）

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

OE.SERVICE（サービスエンジニアの保証）

TOE の保守管理を依頼する場合、mfp を利用する組織の責任者または管理者は、CE と保守契約を締結する。保守契約には、不正な行為をしない旨を明記する。また、保守作業者が正規の保守会社のサービスエンジニアであることを、保守作業の前に管理者が身分証明書を確認して、管理者が

保守作業に立ち会う。

OE.NETWORK（mfp の接続するネットワーク環境）

mfp を利用する組織の責任者は、外部ネットワークから TOE が搭載される mfp へのアクセスを遮断するためにファイアウォールなどの機器を設置して、外部からの不正侵入対策を実施する。

OE.SECRET（秘密情報の適切な管理）

管理者は、ユーザーに対して以下に示す運用を実施させる。

・ユーザーパスワード、Secure Print パスワードを秘匿する。

・ユーザーパスワード、Secure Print パスワードに推測可能な値を設定しない。

・ユーザーパスワードの適宜変更を行う。

・管理者がユーザーパスワードを変更した場合は、速やかに変更させる。

管理者は、以下に示す運用を実施する。

・管理者パスワード、SNMP パスワードに推測可能な値を設定しない。

・管理者パスワード、SNMP パスワードを秘匿する。

・管理者パスワード、SNMP パスワードの適宜変更を行う。

・サービスエンジニアが管理者パスワードを変更した場合は、速やかにパスワードを変更する。

OE.SETTING-SECURITY（セキュリティ強化機能の動作設定）

管理者は、TOE の運用にあたってセキュリティ強化機能の設定を有効化する。

OE. CRPTO-HDD（HDD の暗号化条件）

管理者は、mfp の運用において、外部 IT エンティティであるセキュリティチップ（セキュリティ・アクセラレータ）が提供する暗号化機能を利用する。

OE. CRPTO-NETWORK（ネットワークの暗号化条件）

mfp を利用する組織の責任者は、クライアント PC から TOE に送信される以下の画像ファイルを保護するために、暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を実施する。

＜クライアント PC から TOE に送信される画像ファイル＞

Secure Print Data

ID&Print Data

OE. ICCARD-READER（IC カードリーダーの条件）

mfp において IC カード機能を利用する場合、管理者はガイダンスに記載された IC カードリーダーを使用する。

OE.IC-CARD（IC カードの所有条件）

mfp を利用する組織の責任者は、IC カードに関して以下に示す運用を実施させる。

・mfp を利用する組織の責任者は、組織で利用するために発行した IC カードを、その IC カードの所有が許可される正しいユーザーへ配付する。

・mfp を利用する組織の責任者は、ユーザーに対して IC カードの他人への譲渡、貸与を禁止し、紛失時の届出を徹底させる。

4.3. セキュリティ対策方針根拠

4.3.1. 必要性

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

表 1　前提条件、脅威、組織のセキュリティ方針に対するセキュリティ対策方針の適合性

前提条件・脅威・組織のセキュリティ方針 ＼ セキュリティ対策方針	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.HDD-DATA	T.DISCARD-MFP	T.ACCESS-DATA	T.ACCESS-SECURE-PRINT	T.UNEXPECTED-TRANSMISSION	T.ACCESS-SETTING	T.BACKUP-RESTORE	P.COMMUNICATION-DATA
O.REGISTERED-USER							●	●				
O.SCAN-DATA							●					
O.SECURE-PRINT								●				
O.CONFIG-A										●		
O.CONFIG-B									●			
O.CONFIG-C											●	
O.CONFIG-D												●
O.OVERWRITE-ALL						●						
O.TRUSTED-PATH												●
O.AUTH-CAPABILITY							●	●				
OE.FEED-BACK							●	●	●	●	●	●
OE.SERVER							●	●				
OE.SESSION							●	●	●		●	●
OE.OVERWRITE						●						
OE.SETTING-SECURITY										●		
OE.ADMIN	●											
OE.SERVICE		●										
OE.NETWORK			●									
OE.SECRET				●								
OE. CRPTO-HDD					●							
OE. CRPTO-NETWORK												●
OE. ICCARD-READER							●	●				
OE.IC-CARD							●	●				

4.3.2. 前提条件に対する十分性

前提条件に対するセキュリティ対策方針について以下に説明する。

- **A.ADMIN（管理者の人的条件）**

  本条件は、管理者が悪意を持たないことを想定している。

  OE.ADMIN は、mfp を利用する組織の責任者が 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、管理者の信頼性が充足される。

- **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不正な行為を行なわないことを想定している。

  OE.SERVICE は、TOE を導入する組織は、TOE の保守を担当する組織とサービスエンジニアは不正な行為を行なわない旨を明記した保守契約を締結すること、及び保守作業の前に管理者がサービスエンジニア本人であることを身分証明書で確認すること、管理者が保守作業に立ち会うことを規定しており、本条件は充足される。

- **A.NETWORK（mfp のネットワーク接続条件）**

  本条件は、外部ネットワークから不特定多数の者による攻撃などが行われないことを想定している。

  OE.NETWORK は､外部ネットワークから mfp へのアクセスを遮断するためにファイアウォールなどの機器を設置することにより外部からの不正侵入の防止を規定しており、本条件は充足される。

- **A.SECRET（秘密情報に関する運用条件）**

  本条件は、TOE の利用において使用される各パスワードが管理者、及びユーザーより漏洩しないことを想定している。

  OE.SECRET は、管理者がユーザーに対して Secure Print パスワード、ユーザーパスワードに関する運用規則を実施させることを規定し、管理者が管理者パスワード、SNMP 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おり、本条件は充足される。

- **A.HDD-DATA（HDD データに関する運用条件）**

  本条件は、mfp が有する HDD 内の保護対象資産が、HDD から直接解析できないことを想定している。

  OE.CRPTO-HDD は、管理者が mfp の運用において、外部 IT エンティティであるセキュリティチップ（セキュリティ･アクセラレータ）が提供する暗号化機能を利用することを規定しており、本条件は充足される。

4.3.3. 脅威に対する十分性

脅威に対抗するセキュリティ対策方針について以下に説明する。

- **T.DISCARD-MFP（mfp のリース返却、廃棄）**

本脅威は、TOE を利用する組織から回収された mfp より情報漏洩する可能性を想定している。
O.OVERWRITE-ALL は、TOE が HDD の全データ領域、SSD のデータ領域、及び NVRAM の情報を再現できなくするとしており、mfp が回収される前にこの機能を実行することによって、脅威の可能性は除去される。
OE.OVERWRITE は、管理者が mfp をリース返却、廃棄するなど利用が終了した場合など組織の管轄から保管されるデータが物理的に離れる場合に、全データ上書き消去機能を実行することが要求されるため、T.DISCARD-MFP の脅威の可能性が除去される。
したがって本脅威は十分対抗されている。

- **T.ACCESS-DATA（ユーザー機能を利用したScan to HDD Data への不正なアクセス）**

本脅威は、ユーザー各位が蓄積した Scan to HDD Data に対して、Scan to HDD 機能を利用して不正な操作が行われる可能性を想定している。
O.REGISTERED-USER は、管理者によって TOE に登録されたユーザーだけが、TOE が搭載された mfp を利用することを許可するとしており、さらに O.SCAN-DATA によって HDD 内の Scan to HDD Data のダウンロード操作が、管理者、及び許可されたユーザーだけに制限され、脅威の可能性は軽減される。
なお外部のユーザー情報管理サーバーを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザー情報管理サーバーの外部サーバー認証によるユーザー識別認証情報を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザー管理を利用するための設定が行われ、管理者によって Active Directory によるユーザーのアカウント情報が漏洩しないように、ユーザー情報管理サーバーに対して適切なアクセス管理が行なわれ、ユーザーの識別認証が行われることによって脅威の可能性は軽減される。
また、OE.ICCARD-READER により管理者がガイダンスに記載された IC カードリーダーを使用することによって脅威の可能性は軽減される。
OE.FEED-BACK は、管理者が、管理者またはユーザーがクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用させるとしており、また OE.SESSION によりクライアント PC を介した操作終了後には、ログアウトする運用が要求されるため、T.ACCESS-DATA の脅威の可能性が軽減される。
OE.IC-CARD は、mfp を利用する組織の責任者が、組織で利用するために発行した IC カードを、その IC カードの所有が許可される正しいユーザーへ配付すること、及びユーザーに対して IC カードの他人への譲渡、貸与を禁止し、紛失時の届出を徹底させることが要求されるため、T.ACCESS-DATA の脅威の可能性が軽減される。
したがって本脅威は十分対抗されている。

- **T.ACCESS-SECURE-PRINT（ユーザー機能を利用した Secure Print Data、ID&Print Data への不正なアクセス）**

本脅威は、ユーザー機能を利用した Secure Print Data、ID&Print Data に対して不正な操作が行われてしまう可能性を想定している。
O.REGISTERED-USER は、管理者によって TOE に登録されたユーザーだけが TOE が搭載された mfp を利用することを許可するとしており、さらに O.SECURE-PRINT によって、Secure Print Data、ID&Print Data の操作が許可されたユーザーだけに制限されるため、脅威の可能性は軽減

される。
なお外部のユーザー情報管理サーバーを利用する場合は、O.AUTH-CAPABILITY により Active Directory を用いたユーザー情報管理サーバーの外部サーバー認証によるユーザー識別認証情報を利用するための動作がサポートされ、OE.SERVER より管理者によって Active Directory によるユーザー管理を利用するための設定が行われ、管理者によって Active Directory によるユーザーのアカウント情報が漏洩しないように、ユーザー情報管理サーバーに対して適切なアクセス管理が行なわれ、ユーザーの識別認証が行われることによって脅威の可能性は軽減される。
また、OE.ICCARD-READER により管理者がガイダンスに記載された IC カードリーダーを使用することによって脅威の可能性は軽減される。
OE.FEED-BACK は、管理者が、ユーザーがクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用させるとしており、また OE.SESSION によりクライアント PC を介した操作終了後にはログアウトする運用が要求されるため、T.ACCESS-SECURE-PRINT の脅威の可能性が軽減される。
OE.IC-CARD は、mfp を利用する組織の責任者が、組織で利用するために発行した IC カードを、その IC カードの所有が許可される正しいユーザーへ配付すること、及びユーザーに対して IC カードの他人への譲渡、貸与を禁止し、紛失時の届出を徹底させることが要求されるため、T.ACCESS-DATA の脅威の可能性が軽減される。
したがって本脅威は十分対抗されている。

- **T.UNEXPECTED-TRANSMISSION（想定外対象先への送信）**

本脅威は、mfp のアドレスに関係するネットワーク設定を不正に変更されてしまう可能性を想定している。
これに対して O.CONFIG-B により、TOE が mfp の設定データに関係する設定を操作する役割を管理者に制限するとしており、本脅威の可能性は除去される。
OE.FEED-BACK は、管理者がクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用するとしており、また OE.SESSION によりクライアント PC を介した操作終了後にはログアウトする運用が要求されるため、T.UNEXPECTED-TRANSMISSION の脅威の可能性が除去される。
したがって本脅威は十分対抗されている。

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

本脅威はセキュリティに関係する特定の機能設定を変更されることにより、セキュリティ機能が無効化される可能性を想定している。
O.CONFIG-A により、一連のセキュリティに関連する設定機能を統括するセキュリティ強化機能の設定を管理者だけに許可するとしており、脅威の可能性が除去される。
OE.FEED-BACK は、管理者がクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用するとしており、また OE.SETTING-SECURITY により管理者がセキュリティ強化機能の設定を有効化した上で利用することが要求されるため、T.ACCESS-SETTING の脅威の可能性が除去される。
したがって本脅威は十分対抗されている。

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

本脅威はバックアップ機能、リストア機能が不正に利用されることにより、Scan to HDD Data が漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、mfp の設定（IP アドレスなど）が改ざんされた結果、Secure Print Data、Scan to HDD Data、ID&Print Data が漏洩する可能性を想定している。
O.CONFIG-C により、バックアップ機能、リストア機能の利用を管理者だけに許可するとしてお

り、脅威の可能性が除去される。
OE.FEED-BACK は、管理者がクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用するとしており、またOE.SESSIONによりクライアントPCを介した操作終了後にはログアウトする運用が要求されるため、T.BACKUP-RESTORE の脅威の可能性が除去される。
したがって本脅威は十分対抗されている。

4.3.4. 組織のセキュリティ方針に対する十分性

組織のセキュリティ方針に対応するセキュリティ対策方針について以下に説明する。

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

本組織のセキュリティ方針は、IT 機器間にて送受信される秘匿性の高い画像ファイル（Secure Print Data、Scan to HDD Data、ID&Print Data）について、秘匿性を確保するために、正しい相手先へ信頼されるパスを介した処理を行う、または暗号化すること規定している。
O.TRUSTED-PATH により、TOE からクライアント PC に送信される画像である Scan to HDD Data に対して、TOE からクライアント PC といった画像の送信において正しい相手先との間に高信頼チャネルを提供するため、組織のセキュリティ方針が実現する。また高信頼チャネル機能設定データの設定は、O.CONFIG-D により管理者に制限されている。
OE.CRPTO-NETWORK により mfp を利用する組織の責任者は、クライアント PC から TOE に送信される Secure Print Data、ID&Print Data を保護するために、暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を実施するため、組織のセキュリティ方針をサポートしている。
OE.FEED-BACK は、管理者がクライアント PC から mfp にアクセスする際に、入力されるパスワードに対して、保護されたフィードバックを提供するアプリケーションを利用するとしており、またOE.SESSIONによりクライアントPCを介した操作終了後にはログアウトする運用が要求されるため、組織のセキュリティ方針をサポートしている。
したがって本組織のセキュリティ方針は、達成するために十分である。

5. 拡張コンポーネント定義

5.1. 拡張機能コンポーネント

本 ST では、拡張機能コンポーネントを 3 つ定義する。各セキュリティ機能要件の必要性、ラベリング定義の理由は以下の通りである。

- FAD_RIP.1
  利用者データ及びTSFデータの残存情報を保護することを要求するセキュリティ機能要件である。
  - **拡張の必要性**
    利用者データ及び TSF データの残存情報保護を規定する必要があるが、残存情報保護の観点を説明するセキュリティ機能要件は、利用者データに対する FDP_RIP ファミリしか見当たらない。本要求を満たすセキュリティ機能要件は存在しない。
  - **適用したクラス（FAD）の理由**
    利用者データ及び TSF データの区別なく、双方のデータのセキュリティを説明した要件はない。よって新しいクラスを定義した。
  - **適用したファミリ（FAD_RIP）の理由**
    FDP クラスの FDP_RIP ファミリが説明する内容を利用して、TSF データまで対象を拡張したものであるため、このファミリと同一ラベルを適用した。

- FIT_CAP.1
  TOE が外部 IT エンティティのセキュリティ機能を有効利用するために TOE に必要な能力を規定するためのセキュリティ機能要件である。
  - **拡張の必要性**
    TOE が外部 IT エンティティのセキュリティ機能を利用する場合、外部 IT エンティティのセキュリティ機能が確かにセキュアであることも重要であるが、外部 IT エンティティのセキュリティ機能を正しく使いこなすために TOE 側が提供すべき能力は非常に重要である。しかし本要求のような概念はセキュリティ機能要件には存在しない。
  - **適用したクラス（FIT）の理由**
    CC パート 2 にはない新しい着想であるため、新しいクラスを定義した。
  - **適用したファミリ（FIT_CAP）の理由**
    クラスと同様に CC パート 2 にはない新しい着想であるため、新しいファミリを定義した。

5.1.1. FAD_RIP.1 の定義

- **クラス名**
  FAD：全データの保護
  略称の意味：FAD（Functional requirement for All Data protection）

- **クラスの概要**
  このクラスには、利用者データ、TSF データの区別なく保護することに関連する要件を特定するファミリが含まれる。本件では 1 つのファミリが存在する。

  － 全データの残存情報保護（FAD_RIP）;

- **ファミリのふるまい**
  ファミリ（FAD_RIP）は、削除された情報が二度とアクセスされず、及び別の利用者データ、TSF

データに再割当てされた場合は、リソースに含まれるいかなるデータも無効であることを保証する必要性について扱う。このファミリは、論理的に削除または解放されたが、TOE 内にまだ存在する可能性がある情報に対する保護を要求する。

● コンポーネントのレベル付け

FAD_RIP 全データの残存情報保護	1

FAD_RIP.1：「明示的な消去操作後の全データの残存情報保護」は、TSF によって制御される定義済み利用者データ及び TSF データのサブセットが、明示的な消去操作後において、どの資源のどの残存情報内容も利用できないことを TSF が保証することを要求する。

管理：FAD_RIP.1
予見される管理アクティビティはない。
監査：FAD_RIP.1
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである: a) 最小: 明示的な消去操作を行う利用者識別情報を含む使用

FAD_RIP.1 明示的な消去操作後の全データの残存情報保護
下位階層 : なし **依存性** : なし
FAD_RIP.1.1
TSF は、以下の利用者データ及び TSF データに対する [割付: *明示的な資源の割当て解除要求*] において、資源に割り当てられた以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *利用者データ及び TSF データのリスト*]。

5.1.2. FIT_CAP.1 の定義

- **クラス名**

  FIT：外部 IT エンティティとの連携

  略称の意味：FIT（Functional requirement for IT entities support）

- **クラスの概要**

  このクラスには、外部 IT エンティティが提供するセキュリティサービスの利用に関連する要件を特定するファミリが含まれる。本件では 1 つのファミリが存在する。

  － 外部 IT エンティティを利用するための能力（FIT_CAP）;

- **ファミリのふるまい**

  ファミリ（FIT_CAP）は、外部 IT エンティティのセキュリティ機能を利用するにあたって、TOE に必要となる能力の定義に対応する。

- **コンポーネントのレベル付け**

FIT_CAP　外部 IT エンティティを利用するための能力	1

略称の意味：CAP（**CAP**ability of using IT entities）

FIT_CAP.1：「外部 IT エンティティのセキュリティサービス利用時の能力」は、外部 IT エンティティが提供するセキュリティ機能を正しく利用するための TOE に必要となる能力の具体化に対応する。

管理：FIT_CAP.1
予見される管理アクティビティはない。
監査：FIT_CAP.1
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである: a)　最小:　外部 IT エンティティに対する動作の失敗; b)　基本:　外部 IT エンティティに対するすべての動作の使用（成功、失敗)。

FIT_CAP.1　　外部 IT エンティティのセキュリティサービス利用時の能力
下位階層　:　なし **依存性**　:　なし
FIT_CAP.1.1
TSF は、[割付:*外部 IT エンティティが提供するセキュリティサービス*]に対して、そのサービスを利用するために必要な以下の能力を提供しなければならない：[割付:　*セキュリティサービスの動作に必要な能力のリスト*]。

6. セキュリティ要件

本章では、セキュリティ要件について記述する。

＜ラベル定義について＞

TOE に必要とされるセキュリティ機能要件を記述する。機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用し、ラベルも同一のものを使用する。CC パート 2 に記載されない新しい追加要件は、CC パート 2 と競合しないラベルを新設して識別している。
また、保証要件コンポーネントは、CC パート 3 で規定されているのを直接使用し、ラベルも同一のものを使用する。

＜セキュリティ機能要件“操作”の明示方法＞

以下の記述の中において、イタリック且つボールドで示される表記は、“割付”、または“選択”されていることを示す。アンダーラインで示される原文の直後に括弧書きでイタリック且つボールドで示される表記は、アンダーラインされた原文箇所が“詳細化”されていることを示す。ラベルの後に括弧付けで示される番号は、当該機能要件が“繰り返し”されて使用されていることを示す。

＜依存性の明示方法＞

依存性の欄において括弧付け“( )”された中に示されるラベルは、本 ST にて使用されるセキュリティ機能要件のラベルを示し、複数のセキュリティ機能要件が存在するものはカンマ「,」を使用して羅列する。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。
さらに、セキュリティ保証要件は CC パート 3 で規定されている EAL3 のパッケージを適用しており、EAL に対する保証コンポーネントの追加、または置換などは行なっていない。そのため、本 ST では保証要件の依存性に関する記述は行なわない。

＜用語の定義＞

本章で使用する用語を以下に示す。

表 2 SFR で使用される用語の定義

用語	定義
利用者属性	利用者を一意に特定する属性。
タスク属性	利用者タスクが管理者のタスクであるかユーザーのタスクであるかを特定する属性。
ユーザーID	ユーザーを一意に特定する ID。
ユーザーID の登録	「本体認証」が設定されている場合： 管理者がクライアント PC からユーザーID を登録する。 「外部サーバー認証」が設定されている場合： 外部サーバーがユーザーID を登録する。
ユーザーID の改変	管理者がクライアント PC からユーザーID を改変する。
ユーザーID の削除	管理者がクライアント PC からユーザーID を削除する。
ユーザーID の消去	管理者がパネルから全データ上書き消去機能を使用してユーザーID を消去する。
ユーザーID の問い合わせ	管理者がクライアント PC からユーザーID を問い合わせ（バックアップ）する。
ユーザーID のリストア	管理者がクライアント PC からユーザーID をリストアする。

用語	定義
IC カード ID	IC カードの ID。
IC カード ID の登録	IC カード機能を使用する場合： 管理者がパネル、もしくはクライアント PC から IC カード ID を登録する。
IC カード ID の改変	IC カード機能を使用する場合： 管理者がパネルから IC カード ID を改変する。
IC カード ID の削除	IC カード機能を使用する場合： 管理者がパネル、もしくはクライアント PC から IC カード ID を削除する。
IC カード ID の消去	IC カード機能を使用する場合： 管理者がパネルから全データ上書き消去機能を使用して IC カード ID を消去する。
IC カード ID の問い合わせ	IC カード機能を使用する場合： 管理者がクライアント PC から IC カード ID を問い合わせ（バックアップ）する。
IC カード ID のリストア	IC カード機能を使用する場合： 管理者がクライアント PC から IC カード ID をリストアする。
Scan to HDD Data 属性	Scan to HDD Data の操作を許可されたユーザーを特定する属性。
Secure Print Data 属性	Secure Print Data の操作を許可されたユーザーを特定する属性。
ID&Print Data 属性	ID&Print Data の操作を許可されたユーザーを特定する属性。
CE パスワード	サービスエンジニアのパスワード。
CE パスワードの改変	サービスエンジニアがパネルから CE パスワードを改変する。
管理者パスワード	管理者のパスワード。
管理者パスワードの改変	・管理者がクライアント PC から管理者パスワードを改変する。 ・サービスエンジニアがパネルから管理者パスワードを改変（初期化）する。
管理者パスワードの初期化	管理者がパネルから全データ上書き消去機能を使用して管理者パスワードを初期化する
SNMP パスワード	管理者のパスワード。MIB オブジェクトに対するアクセスを行う場合使用されるパスワード。
SNMP パスワードの改変	管理者がクライアント PC から SNMP パスワードを改変する。
SNMP パスワードの初期化	管理者がパネルから全データ上書き消去機能を使用して SNMP パスワードを初期化する。
ユーザーパスワード	ユーザーのパスワード。
ユーザーパスワードの登録	管理者がクライアント PC からユーザーパスワードを登録する。
ユーザーパスワードのリストア	管理者がクライアント PC からユーザーパスワードをリストアする。
ユーザー自身のユーザーパスワードの改変	管理者及びユーザーがクライアント PC からユーザー自身のユーザーパスワードを改変する。
ユーザーパスワードの問い合わせ	管理者がクライアント PC からユーザーパスワードを問い合わせ（バックアップ）する。
ユーザーパスワードの消去	管理者がパネルから全データ上書き消去機能を使用してユーザーパスワードを消去する。
Secure Print パスワード	Secure Print Data のパスワード。
Secure Print パスワードの登録	ユーザーがクライアント PC から Secure Print Data の印刷指示をした際、Secure Print パスワードを登録する。

用語	定義
Secure Print パスワードの消去	管理者がパネルから全データ上書き消去機能を使用して Secure Print パスワードを消去する。
セッション情報	ユーザー、管理者がネットワーク経由でアクセスした際、識別認証後セッションを維持する情報。
管理者認証	管理者を認証する機能。
ユーザー認証	ユーザーを認証する機能。
外部サーバー	外部認証サーバー。
SNMP パスワード認証機能	SNMP パスワードを使用して管理者を認証する機能。
IC カード機能	IC カード使用してユーザーを識別する機能。
ID&Print 機能	パネルからのユーザー識別認証処理、もしくは IC カードリーダーからのユーザー識別処理で印刷を行う機能。
システムオートリセット時間	パネル操作を自動的にログアウトする時間。
システムオートリセット時間の改変	管理者がパネルからシステムオートリセット時間を改変する。
外部サーバー識別設定データ	外部サーバーを識別するデータ。
外部サーバー識別設定データの改変	管理者がクライアント PC から外部サーバー識別設定データを改変する。
外部サーバー識別設定データの消去	管理者がパネルから全データ上書き消去機能を使用して外部サーバー識別設定データを消去する。
高信頼チャネル設定データ	TOE とクライアント PC との間において、Secure Print Data、及び Scan to HDD Data をセキュアに送受信するために設定するデータ。
ユーザー情報管理サーバー	外部サーバーと同義。
Active Directory	Windows プラットフォームのネットワーク環境にてユーザー情報を一元管理するために Windows Server 2000（それ以降）が提供するディレクトリサービスの方式。
認証情報問い合わせ機能	TSF が外部サーバー（ユーザー情報管理サーバー）に認証情報の問い合わせを行う機能。
認証情報取得機能	TSF が外部サーバー（ユーザー情報管理サーバー）から返される認証情報の取得を行う機能。
Scan to HDD Data	パネルよりユーザーがスキャン機能を利用して、“Private”を選択して HDD に蓄積したデータ。
Scan to HDD Data のダウンロード	ユーザーがクライアント PC から Scan to HDD Data をダウンロードする。
Scan to HDD Data の一覧表示	管理者及びユーザーがクライアント PC から Scan to HDD Data の一覧を表示する。
Scan to HDD Data のバックアップ	管理者がクライアント PC から Scan to HDD Data をバックアップ（ダウンロード）する。
Scan to HDD Data の削除	ユーザーがパネル、クライアント PC から Scan to HDD Data を削除する。 管理者がクライアント PC から Scan to HDD Data を削除する。
Scan to HDD Data の消去	管理者がパネルから全データ上書き消去機能を使用して Scan to HDD Data を消去する。
Secure Print Data	クライアント PC よりユーザーが印刷機能を利用して、Secure Print パスワードを付けて TOE に送信したデータ。
Secure Print Data の一覧表示	ユーザーがパネルから Secure Print Data の一覧を表示する。
Secure Print Data の印刷	ユーザーがパネルから Secure Print Data を印刷する。
Secure Print Data の削除	ユーザーがパネルから Secure Print Data を削除する。

用語	定義
Secure Print Data の消去	管理者がパネルから全データ上書き消去機能を使用して Secure Print Data を消去する。
ID&Print Data	クライアント PC よりユーザーが印刷機能の ID&Print 機能を利用して、TOE に送信したデータ。
ID&Print Data の一覧表示	ユーザーがパネルから ID&Print Data の一覧を表示する。
ID&Print Data の印刷	ユーザーがパネルから ID&Print Data を印刷する。
ID&Print Data の削除	ユーザーがパネルから ID&Print Data を削除する。
ID&Print Data の消去	管理者がパネルから全データ上書き消去機能を使用して ID&Print Data を消去する。
mfp の設定データ	mfp の設定に関係する一連の設定データ（IP アドレス、AppleTalk プリンター名）。
mfp の設定データの設定	管理者がパネル及びクライアント PC から mfp の設定データを設定する。
mfp の設定データの初期化	管理者がパネルから全データ上書き消去機能を使用して mfp の設定データを初期化する。
Secure Print Data の利用を許可されたユーザー	Secure Print Data のパスワードを知っているユーザー。

6.1. セキュリティ機能要件

6.1.1. 利用者データ保護

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

表 3　ユーザーデータアクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者タスク（ユーザーの場合）	*Scan to HDD Data*	*・ダウンロード（ネットワーク経由）* *・一覧表示（パネル経由、ネットワーク経由）* *・削除（パネル経由、ネットワーク経由）*
利用者タスク（管理者の場合）	*Scan to HDD Data*	*・バックアップ（ネットワーク経由）* *・一覧表示（ネットワーク経由）* *・削除（ネットワーク経由）* *・消去（パネル経由）*

FDP_ACC.1[2]　　サブセットアクセス制御
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1[2]）
FDP_ACC.1.1[2]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]: ***「表 4　Print Data アクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***Print Data アクセス制御***

表 4　Print Data アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者タスク（ユーザーの場合）	*Secure Print Data*	*・印刷（パネル経由）* *・削除（パネル経由）* *・一覧表示（パネル経由）*
	ID&Print Data	*・印刷（パネル経由）* *・削除（パネル経由）* *・一覧表示（パネル経由）*
利用者タスク（管理者の場合）	*Secure Print Data*	*・消去（パネル経由）*
	ID&Print Data	*・消去（パネル経由）*

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

表 5　設定管理アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者タスク *（管理者の場合）*	*mfp の設定データ*	*・設定（IP アドレス：パネル経由、ネットワーク経由* *AppleTalk プリンター名：ネットワーク経由）* *・初期化（パネル経由）*

FDP_ACF.1[1]　　セキュリティ属性によるアクセス制御
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.1.1[1]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***利用者タスク　　⇒　・タスク属性*** ***・利用者属性*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***Scan to HDD Data　　⇒　Scan to HDD Data 属性***
[割付: *アクセス制御 SFP*]: ***ユーザーデータアクセス制御***
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を決定するために、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*]: ***＜Scan to HDD Data に対する操作制御＞*** ***・利用者タスクは、サブジェクト属性の利用者属性と一致するオブジェクト属性の Scan to HDD　Data 属性を持つ Scan to HDD Data に対して、ダウンロードすることが許可される。（ネットワーク経由）*** ***・利用者タスクは、サブジェクト属性の利用者属性と一致するオブジェクト属性の Scan to HDD Data 属性を持つ Scan to HDD Data に対して、一覧表示すること、削除することが許可される。（パネル経由、ネットワーク経由）***
FDP_ACF.1.3[1]
TSF は、次の追加規則、[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許可する規則*]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許可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許可する規則*]: ***・利用者タスクは、サブジェクト属性のタスク属性が管理者の場合、Scan to HDD Data の一覧表示、バックアップ（ダウンロード）、削除操作することを許可される。（ネットワーク経由）*** ***・利用者タスクは、サブジェクト属性のタスク属性が管理者の場合、Scan to HDD Data を消去操作することを許可される。（パネル経由）***
FDP_ACF.1.4[1]
TSF は、次の追加規則、[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***

FDP_ACF.1[2]　　セキュリティ属性によるアクセス制御

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.1.1[2]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞　　＜サブジェクト属性＞*** ***利用者タスク　　⇒　・タスク属性*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・Secure Print Data　　⇒　Secure Print Data 属性*** ***・ID&Print Data　　⇒　ID&Print Data 属性***
[割付: *アクセス制御 SFP*]: ***Print Data 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を決定するために、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*]: が ***サブジェクト属性のタスク属性がユーザーの場合*** ***＜Secure Print Data に対する操作制御＞*** ***・利用者タスクは、あらゆる Secure Print Data を一覧表示操作することが許可される。（パネル経由）*** ***・パネル経由で入力された Secure Print パスワードと Secure Print Data 属性が合致して、Secure Print パスワードの認証に成功した利用者タスクは、その Secure Print Data の印刷、削除が許可される。（パネル経由）*** ***＜ID&Print Data に対する操作制御＞*** ***・利用者タスクは、IC カードによって識別された、もしくはパネルによって認証されたユーザーID と合致する ID&Print Data 属性の ID&Print Data を印刷、削除、一覧表示操作することが許可される。（パネル経由）***
FDP_ACF.1.3[2]
TSF は、次の追加規則、[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許可する規則*]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許可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許可する規則*]: ***・利用者タスクは、サブジェクト属性のタスク属性が管理者の場合、あらゆる Secure Print Data、ID&PrintData を消去することが許可される。***
FDP_ACF.1.4[2]
TSF は、次の追加規則、[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

FDP_ACF.1[3]　　セキュリティ属性によるアクセス制御

下位階層　　:　なし
依存性　　:　FDP_ACC.1（FDP_ACC.1[3]）、FMT_MSA.3（適用しない）

FDP_ACF.1.1[3]

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

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

＜サブジェクト＞　　＜サブジェクト属性＞
利用者タスク　　⇒　・タスク属性

＜オブジェクト＞
・mfp の設定データ

※ オブジェクト属性は、存在しない。

[割付: *アクセス制御 SFP*]:
設定管理アクセス制御

FDP_ACF.1.2[3]

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、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*]:

・利用者タスクは、サブジェクト属性のタスク属性が管理者の場合、mfp の設定データを設定することが許可される。（パネル経由、ネットワーク経由）
IP アドレス（パネル、ネットワーク経由）
AppleTalk プリンター名（ネットワーク経由）
・利用者タスクは、サブジェクト属性のタスク属性が管理者の場合、mfp の設定データを初期化することが許可される。（パネル経由）

FDP_ACF.1.3[3]

TSF は、次の追加規則、[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許可する規則*]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許可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許可する規則*]:
なし

FDP_ACF.1.4[3]

TSF は、次の追加規則、[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

6.1.2. 識別と認証

FIA_ATD.1 利用者属性定義
下位階層 : なし 依存性 : なし
FIA_ATD.1.1
TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]
[割付:*セキュリティ属性のリスト*] : ***・タスク属性*** ***・利用者属性***

FIA_SOS.1[1] 秘密の検証
下位階層 : なし 依存性 : なし
FIA_SOS.1.1[1]
TSF は、秘密 ***(管理者パスワード、CE パスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ***・桁数 : 8 桁*** ***・文字種 : 94 文字の中から選択可能*** ***・規則 : (1) 1 つのキャラクターで構成されない。*** ***(2) 変更する場合、変更後の値が現在設定されている値と合致しない。*** ***※ 管理者パスワードはパネル、ネットワーク経由アクセスに適用される。*** ***CE パスワードは、パネル経由アクセスに適用される。***

FIA_SOS.1[2] 秘密の検証
下位階層 : なし 依存性 : なし
FIA_SOS.1.1[2]
TSF は、秘密 ***(SNMP パスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ***・桁数 : 8 桁以上*** ***・文字種 : 90 文字の中から選択可能*** ***・規則 : 1 つのキャラクターで構成されない。***

FIA_SOS.1[3] 秘密の検証
下位階層 : なし 依存性 : なし
FIA_SOS.1.1[3]
TSF は、秘密 ***(ユーザーパスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ***・桁数 : 8 桁以上***

・*文字種：93 文字の中から選択可能*
・*規則　：(1) 1 つのキャラクターで構成されない。*
(2) 変更する場合、変更後の値が現在設定されている値と合致しない。
※　*ユーザーパスワードはパネル、ネットワーク経由アクセスに適用される。*

FIA_SOS.1[4]　　秘密の検証
下位階層　：　なし 依存性　：　なし
FIA_SOS.1.1[4]
TSF は、秘密 ***(Secure Print パスワード)*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : ・*桁数　：8 桁* ・*文字種：93 文字の中から選択可能* ・*規則　：1 つのキャラクターで構成されない。*

FIA_SOS.2　　TSF 秘密生成
下位階層　：　なし 依存性　：　なし
FIA_SOS.2.1
TSF は、[割付: *定義された品質尺度*]に合致する秘密（***セッション情報***）を生成するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*] : *10^{10} 以上（10 種類の空間＊＊10 桁以上）*
FIA_SOS.2.2
TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付: *TSF 機能のリスト*] : ・*管理者認証（ネットワーク経由アクセス）* ・*ユーザー認証（ネットワーク経由アクセス）*

FIA_UAU.2[1]　　アクション前の利用者認証
下位階層　：　FIA_UAU.1 依存性　：　FIA_UID.1（FIA_UID.2[1]）
FIA_UAU.2.1[1]
TSF は、その利用者 ***(サービスエンジニア)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(サービスエンジニア)*** に認証が成功することを要求しなければならない。

FIA_UAU.2[2]　　アクション前の利用者認証
下位階層　：　FIA_UAU.1 依存性　：　FIA_UID.1（FIA_UID.2[2]）
FIA_UAU.2.1[2]
TSF は、その利用者 ***(管理者)*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***(管理者)*** に認証 ***(パネル経由の場合はパスワード認証、ネットワーク経由の場合はパスワード認証とセッションを維持している間のセッション情報認証)*** が成功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**
下位階層	: FIA_UAU.1
依存性	: FIA_UID.1（FIA_UID.2[3]）
FIA_UAU.2.1[3]	
TSF は、その利用者 ***（ユーザー）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（ユーザー）*** に認証 ***（パネル経由の場合はパスワード認証、ネットワーク経由の場合はパスワード認証とセッションを維持している間のセッション情報認証）*** が成功することを要求しなければならない。	

FIA_UAU.2[4]	**アクション前の利用者認証**
下位階層	: FIA_UAU.1
依存性	: FIA_UID.1（FIA_UID.2[4]）
FIA_UAU.2.1[4]	
TSF は、その利用者 ***（Secure Print Data の利用を許可されたユーザー）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（Secure Print Data の利用を許可されたユーザー）*** に認証が成功することを要求しなければならない。	

FIA_UAU.7	**保護された認証フィードバック**
下位階層	: なし
依存性	: FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]）
FIA_UAU.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 ***（操作パネルを操作する利用者）*** に提供しなければならない。	
[割付: *フィードバックのリスト*] : ***入力された文字データ 1 文字毎に隠匿文字の表示***	

FIA_UID.2[1]	**アクション前の利用者識別**
下位階層	: FIA_UID.1
依存性	: なし
FIA_UID.2.1[1]	
TSF は、その利用者 ***（サービスエンジニア）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（サービスエンジニア）*** に識別が成功することを要求しなければならない。	

FIA_UID.2[2]	**アクション前の利用者識別**
下位階層	: FIA_UID.1
依存性	: なし
FIA_UID.2.1[2]	
TSF は、その利用者 ***（管理者）*** を代行する他の TSF 仲介アクションを許可する前に、各利用者 ***（管理者）*** に識別が成功することを要求しなければならない。	

FIA_UID.2[3]	**アクション前の利用者識別**
下位階層	: FIA_UID.1

依存性	: なし
FIA_UID.2.1[3]	
TSF は、その利用者 *（ユーザー）* を代行する他の TSF 仲介アクションを許可する前に、各利用者 *（ユーザー）* に識別 *（パネル経由、及びネットワーク経由の場合はユーザーID 識別、IC カードリーダー経由の場合は IC カード ID 識別）* が成功することを要求しなければならない。	

FIA_UID.2[4]	**アクション前の利用者識別**
下位階層	: FIA_UID.1
依存性	: なし
FIA_UID.2.1[4]	
TSF は、その利用者 *（Secure Print Data の利用を許可されたユーザー）* を代行する他の TSF 仲介アクションを許可する前に、各利用者 *（Secure Print Data の利用を許可されたユーザー）* に識別が成功することを要求しなければならない。	

FIA_UID.2[5]	**アクション前の利用者識別**
下位階層	: FIA_UID.1
依存性	: なし
FIA_UID.2.1[5]	
TSF は、その利用者 *（外部サーバー）* を代行する他の TSF 仲介アクションを許可する前に、各利用者 *（外部サーバー）* に識別が成功することを要求しなければならない。	

FIA_USB.1	**利用者・サブジェクト結合**
下位階層	: なし
依存性	: FIA_ATD.1（FIA_ATD.1）
FIA_USB.1.1	
TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: *利用者セキュリティ属性のリスト*]	
[割付: *利用者セキュリティ属性のリスト*] : ***・タスク属性*** ***・利用者属性***	
FIA_USB.1.2	
TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の最初の関連付けの規則*]	
[割付: *属性の最初の関連付けの規則*] : ***なし***	
FIA_USB.1.3	
TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の変更の規則*]	
[割付: *属性の変更の規則*] : ***なし***	

6.1.3. セキュリティ管理

FMT_MOF.1[1]	**セキュリティ機能のふるまいの管理**
下位階層	: なし
依存性	: FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

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

FMT_MOF.1[2]　　セキュリティ機能のふるまいの管理
下位階層　:　なし 依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MOF.1.1[2]
TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]能力を[割付: *許可された識別された役割*]に制限しなければならない。
[割付: *機能のリスト*]: ***「表 6　セキュリティ機能のふるまいの管理[2]　機能と能力のリスト」に記載***
[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]: ***を停止する、を動作させる、のふるまいを改変する***
[割付: *許可された識別された役割*]: ***管理者***

表 6　セキュリティ機能のふるまいの管理[2]　機能と能力のリスト

機能	能力
ユーザー認証機能	*を停止する、を動作させる、のふるまいを改変する*
SNMP パスワード認証機能	*のふるまいを改変する*
IC カード機能	*を停止する、を動作させる、のふるまいを改変する*
ID&Print 機能	*のふるまいを改変する*

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

FMT_MOF.1[4]　　セキュリティ機能のふるまいの管理
下位階層　:　なし 依存性　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MOF.1.1[4]
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*]: ***全データ上書き消去機能***
[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***
[割付: *許可された識別された役割*]: ***管理者***

FMT_MSA.3[1]　　静的属性初期化
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.3.1[1]
TSF は、その SFP を実施するために使われるセキュリティ属性 ***(Scan to HDD Data 属性)*** に対して[選択: *制限的、許可的、[割付: その他の特性]*: から 1 つのみ選択]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、[割付: その他の特性]*: から 1 つのみ選択]: ***[割付：その他の特性]:*** [割付: *その他の特性*]: ***Scan to HDD Data を登録するユーザーの利用者属性と一致する場合に許可される***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]: ***ユーザーデータアクセス制御***
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***

FMT_MSA.3[2]　　静的属性初期化
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.3.1[2]
TSF は、その SFP を実施するために使われるセキュリティ属性 ***(Secure Print Data 属性、ID&Print Data 属性)*** に対して[選択: *制限的、許可的、[割付: その他の特性]*: から 1 つのみ選択]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、[割付: その他の特性]*: から 1 つのみ選択]: ***[割付：その他の特性]:*** [割付: *その他の特性*]: ***＜Secure Print Data 属性＞*** ***・Secure Print Data として登録したユーザーだけが当該の Secure Print Data を印刷、削除することを許可される。*** ***・mfp に登録されたすべてのユーザーに対して、Secure Print Data を一覧表示することが許可される。*** ***＜ID&Print Data 属性＞*** ***・ID&Print Data として登録したユーザーだけが当該の ID&Print Data を印刷、削除、一覧表示することを許可される。***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]: ***Print Data 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*] ***なし***

FMT_MTD.1[1]　　TSF データの管理
下位階層　：　なし 依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[1]
(ユーザー認証の方式に「本体認証」が選択されている場合、TSF) 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*]： ***ユーザーパスワード***
[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]*]： ***消去、[割付：その他の操作]：*** [割付: *その他の操作*]： ***登録、リストア***
[割付:*許可された識別された役割*]： ***管理者***

FMT_MTD.1[2]　　TSF データの管理
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.1.1[2]
(ユーザー認証の方式に「本体認証」が選択されている場合、TSF) 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*]： ***ユーザー自身のユーザーパスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***改変***
[割付:*許可された識別された役割*]： ***・ユーザー*** ***・管理者***

FMT_MTD.1[3]　　TSF データの管理
下位階層　：　なし 依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[3]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]： ***・ユーザーID*** ***・システムオートリセット時間*** ***・外部サーバー識別設定データ*** ***・SNMP パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]： ***改変***
[割付:*許可された識別された役割*]： ***管理者***

FMT_MTD.1[4]　　TSF データの管理

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.1.1[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*]: ***管理者パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***改変***
[割付:*許可された識別された役割*]: ***・管理者*** ***・サービスエンジニア***

FMT_MTD.1[5] TSF データの管理

下位階層 : なし 依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[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*]: ***・ユーザーパスワード（「本体認証」が設定されている場合）*** ***・ユーザーID*** ***・IC カード ID（IC カード機能を使用している場合）***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***問い合わせ***
[割付:*許可された識別された役割*]: ***管理者***

FMT_MTD.1[6] TSF データの管理

下位階層 : なし 依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[3]）
FMT_MTD.1.1[6]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***Secure Print 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]:*** [割付: *その他の操作*]: ***登録***
[割付:*許可された識別された役割*]: ***ユーザー***

FMT_MTD.1[7] TSF データの管理

下位階層 : なし 依存性 : FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]）
FMT_MTD.1.1[7]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]:

CE 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*]: ***サービスエンジニア***

FMT_MTD.1[8]　　TSF データの管理
下位階層　:　なし **依存性**　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[4]）
FMT_MTD.1.1[8]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ユーザーID***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]:*** [割付: *その他の操作*]: ***登録***
[割付:*許可された識別された役割*]: ***・管理者（「本体認証」が設定されている場合）*** ***・外部サーバー（「外部サーバー認証」が設定されている場合）***

FMT_MTD.1[9]　　TSF データの管理
下位階層　:　なし **依存性**　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[9]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***管理者パスワード***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***[割付：その他の操作]:*** [割付: *その他の操作*]: ***初期化***
[割付:*許可された識別された役割*]: ***管理者***

FMT_MTD.1[10]　　TSF データの管理
下位階層　:　なし **依存性**　:　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[10]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ユーザーID***
[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]: ***削除、消去、[割付：その他の操作]:*** [割付: *その他の操作*]: ***リストア***
[割付:*許可された識別された役割*]:

管理者

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

FMT_MTD.1[12]　　TSF データの管理
下位階層　　：　　なし 依存性　　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[12]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***「表 7　TSFデータの管理[12]　TSFデータと操作のリスト」に記載***
[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：その他の操作]：*** [割付: *その他の操作*]: ***初期化***
[割付:*許可された識別された役割*]: ***管理者***

表 7　TSF データの管理[12]　TSF データと操作のリスト

TSF データ	操作
外部サーバー識別設定データ	*消去*
SNMP パスワード	*初期化*

FMT_MTD.1[13]　　TSF データの管理
下位階層　　：　なし 依存性　　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）
FMT_MTD.1.1[13]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***IC カード ID（IC カード機能を使用している場合）***
[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、削除、消去、[割付：その他の操作]：*** [割付: *その他の操作*]: ***登録、リストア***
[割付:*許可された識別された役割*]:

管理者

FMT_SMF.1　　管理機能の特定
下位階層　　：　なし 依存性　　：　なし
FMT_SMF.1.1
TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]
[割付: *TSF によって提供される管理機能のリスト*] : ***「表 8　セキュリティ管理のリスト」に示す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 8　セキュリティ管理のリスト

機能要件	CC で定義された管理対象	TOE の管理機能
FDP_ACC.1[1]	なし	－
FDP_ACC.1[2]	なし	－
FDP_ACC.1[3]	なし	－
FDP_ACF.1[1]	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。	なし（属性は変更不可のため管理項目はない）
FDP_ACF.1[2]	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。	なし（属性は変更不可のため管理項目はない）
FDP_ACF.1[3]	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。	なし（属性は変更不可のため管理項目はない）
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし（追加のセキュリティ属性はないため管理対象にならない）
FIA_SOS.1[1]	a) 秘密の検証に使用される尺度の管理。	なし（秘密の検証に使用される尺度は固定のため管理対象にならない）
FIA_SOS.1[2]	a) 秘密の検証に使用される尺度の管理。	なし（秘密の検証に使用される尺度は固定のため管理対象にならない）
FIA_SOS.1[3]	a) 秘密の検証に使用される尺度の管理。	なし（秘密の検証に使用される尺度は固定のため管理対象にならない）
FIA_SOS.1[4]	a) 秘密の検証に使用される尺度の管理。	なし（秘密の検証に使用される尺度は固定のため管理対象にならない）
FIA_SOS.2	a) 秘密の生成に使用される尺度の管理。	なし（秘密の生成に使用される尺度は固定のため管理対象にならない）
FIA_UAU.2[1]	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	CE パスワードの管理
FIA_UAU.2[2]	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	管理者パスワード、SNMP パスワードの管理
FIA_UAU.2[3]	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	ユーザーパスワードの管理
FIA_UAU.2[4]	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	Secure Print パスワードの管理

機能要件	CC で定義された管理対象	TOE の管理機能
FIA_UAU.7	なし	－
FIA_UID.2[1]	a) 利用者識別情報の管理。	なし(利用者識別情報は固定のため管理対象にならない)
FIA_UID.2[2]	a) 利用者識別情報の管理。	なし(利用者識別情報は固定のため管理対象にならない)
FIA_UID.2[3]	a) 利用者識別情報の管理。	・ユーザーID の管理 ・IC カード ID の管理
FIA_UID.2[4]	a) 利用者識別情報の管理。	ユーザーID の管理
FIA_UID.2[5]	a) 利用者識別情報の管理。	外部サーバー識別設定データの管理
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	なし(サブジェクトのセキュリティ属性は固定のため管理対象にならない)
	b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる。	
FMT_MOF.1[1]	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;	セキュリティ強化機能の管理
FMT_MOF.1[2]	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;	・ユーザー認証機能の管理 ・IC カード機能の管理 ・ID&Print 機能の管理
FMT_MOF.1[3]	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;	高信頼チャネル機能の管理
FMT_MOF.1[4]	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;	全データ上書き消去機能の管理
FMT_MSA.3[1]	a) 初期値を特定し得る役割のグループを管理すること;	なし （a:役割グループは固定のため管理対象にならない） （b:その他の特性は管理する必要がないため管理対象にならない） （c: セキュリティ属性が特定の値を引き継ぐことがないため管理対象にならない）
	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;	
	c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	
FMT_MSA.3[2]	a) 初期値を特定し得る役割のグループを管理すること;	なし （a:役割グループは固定のため管理対象にならない） （b:その他の特性は管理する必要がないため管理対象にならない） （c: セキュリティ属性が特定の値を引き継ぐことがないため管理対象にならない）
	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;	
	c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	
FMT_MTD.1[1]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[2]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[3]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[4]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）

機能要件	CC で定義された管理対象	TOE の管理機能
FMT_MTD.1[5]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[6]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[7]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[8]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[9]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[10]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[11]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[12]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_MTD.1[13]	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定のため管理対象にならない）
FMT_SMF.1	なし	－
FMT_SMR.1[1]	a) 役割の一部をなす利用者のグループの管理。	なし(役割グループは固定のため管理対象にならない)
FMT_SMR.1[2]	a) 役割の一部をなす利用者のグループの管理。	なし(役割グループは固定のため管理対象にならない)
FMT_SMR.1[3]	a) 役割の一部をなす利用者のグループの管理。	なし(役割グループは固定のため管理対象にならない)
FMT_SMR.1[4]	a) 役割の一部をなす利用者のグループの管理。	なし(役割グループは固定のため管理対象にならない)
FTA_SSL.3	a) 個々の利用者についてロックアウトを生じさせる利用者が非アクティブである時間の特定;	システムオートリセット時間の管理
	b) ロックアウト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;	
	c) セションをロック解除する前に生じるべき事象の管理。	
FTP_ITC.1	a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。	高信頼チャネル機能の管理
FAD_RIP.1	なし	－
FIT_CAP.1	なし	－

FMT_SMR.1[1]　　セキュリティの役割
下位階層　：　なし **依存性**　：　FIA_UID.1（FIA_UID.2[1]）
FMT_SMR.1.1[1]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： ***サービスエンジニア***
FMT_SMR.1.2[1]
TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.1[2]　　セキュリティの役割
下位階層　：　なし **依存性**　：　FIA_UID.1（FIA_UID.2[2]）
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付けなければならない。

FMT_SMR.1[3]　　セキュリティの役割
下位階層　：　なし **依存性**　：　FIA_UID.1（FIA_UID.2[3]）
FMT_SMR.1.1[3]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]： ***ユーザー***
FMT_SMR.1.2[3]
TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.1[4]　　セキュリティの役割
下位階層　：　なし **依存性**　：　FIA_UID.1（FIA_UID.2[5]）
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*]： ***外部サーバー***
FMT_SMR.1.2[4]
TSF は、利用者を役割に関連付けなければならない。

6.1.4. TOE アクセス

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

6.1.5. 高信頼パス/チャネル

FTP_ITC.1　　TSF 間高信頼チャネル
下位階層　　：　なし 依存性　　：　なし
FTP_ITC.1.1
TSF は、それ自身と<u>他の高信頼 IT 製品</u>***（クライアント PC）***間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。
FTP_ITC.1.2
TSF は、[選択: *TSF*、*<u>他の高信頼 IT 製品</u>**（クライアント PC）***]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。
[選択: *TSF*、*<u>他の高信頼 IT 製品</u>**（クライアント PC）***]： ***<u>他の高信頼 IT 製品</u>（クライアント PC）***
FTP_ITC.1.3
TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。
[割付: *高信頼チャネルが要求される機能のリスト*]： ***・Scan to HDD Data のダウンロード***

6.1.6. 拡張：全データの残存情報保護

FAD_RIP.1　　明示的な消去操作後の全データの残存情報保護
下位階層　　：　なし 依存性　　：　なし
FAD_RIP.1.1
TSF は、以下の利用者データ及び TSF データに対する [割付: *明示的な資源の割当て解除要求*] において、資源に割り当てられた以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *利用者データ及び TSF データのリスト*]。
[割付: *明示的な資源の割当て解除要求*]： ***管理者による明示的な消去操作***
[割付: *利用者データのリスト及び TSF データのリスト*]： ***＜利用者データ＞*** ***・Secure Print Data*** ***・Scan to HDD Data*** ***・ID&Print Data*** ***・保管画像ファイル***

・待機状態にあるジョブの画像ファイル ・HDD 残存画像ファイル ・画像関連ファイル ・送信宛先データファイル ・SSD 画像ファイル ・mfp の設定データ（初期化） ＜TSF データ＞ ・管理者パスワード（初期化） ・SNMP パスワード（初期化） ・ユーザーID ・ユーザーパスワード ・IC カード ID ・Secure Print パスワード ・高信頼チャネル設定データ（初期化） ・外部サーバー識別設定データ ・残存 TSF データ

6.1.7. 拡張：外部 IT エンティティを利用するための能力

FIT_CAP.1 外部 IT エンティティのセキュリティサービス利用時の能力
下位階層 : なし 依存性 : なし
FIT_CAP.1.1
TSF は、[割付:*外部 IT エンティティが提供するセキュリティサービス*]に対して、そのサービスを利用するために必要な以下の能力を提供しなければならない：[割付: *セキュリティサービスの動作に必要な能力のリスト*]。
[割付: *外部 IT エンティティが提供するセキュリティサービス*] ***ActiveDirectory を用いたユーザー情報管理サーバーが実現するユーザー識別認証機能***
[割付: *セキュリティサービスの動作に必要な能力のリスト*] ***・識別認証対象のユーザーに対する認証情報問い合わせ機能*** ***・識別認証対象のユーザーに対する認証情報取得機能***

6.2. セキュリティ保証要件

TOE が搭載される mfp 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 9　セキュリティ保証要件

TOEセキュリティ保証要件		コンポーネント
開発	セキュリティアーキテクチャ記述	ADV_ARC.1
	完全な要約を伴う機能仕様	ADV_FSP.3
	アーキテクチャ設計	ADV_TDS.2
ガイダンス文書	利用者操作ガイダンス	AGD_OPE.1
	準備手続き	AGD_PRE.1
ライフサイクルサポート	許可の管理	ALC_CMC.3
	実装表現の CM 範囲	ALC_CMS.3
	配付手続き	ALC_DEL.1
	セキュリティ手段の識別	ALC_DVS.1
	開発者によるライフサイクルモデルの定義	ALC_LCD.1
セキュリティターゲット評価	適合主張	ASE_CCL.1
	拡張コンポーネント定義	ASE_ECD.1
	ST 概説	ASE_INT.1
	セキュリティ対策方針	ASE_OBJ.2
	派生したセキュリティ要件	ASE_REQ.2
	セキュリティ課題定義	ASE_SPD.1
	TOE 要約仕様	ASE_TSS.1
テスト	カバレージの分析	ATE_COV.2
	テスト：基本設計	ATE_DPT.1
	機能テスト	ATE_FUN.1
	独立テスト - サンプル	ATE_IND.2
脆弱性評定	脆弱性分析	AVA_VAN.2

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

6.3.1.1. 必要性

セキュリティ対策方針とセキュリティ機能要件の対応関係を下表に示す。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 10　セキュリティ対策方針に対するセキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.SCAN-DATA	O.SECURE-PRINT	O.CONFIG-A	O.CONFIG-B	O.CONFIG-C	O.CONFIG-D	O.OVERWRITE-ALL	O.TRUSTED-PATH	O.AUTH-CAPABILITY	※ set.admin	※ set.service
set.admin	●	●	●	●	●	●	●	●				
set.service	●	●	●	●	●	●	●	●				
FDP_ACC.1[1]		●				●		●				
FDP_ACC.1[2]			●					●				
FDP_ACC.1[3]					●			●				
FDP_ACF.1[1]		●				●		●				
FDP_ACF.1[2]			●					●				
FDP_ACF.1[3]					●			●				
FIA_ATD.1		●	●		●	●						
FIA_SOS.1[1]											●	●
FIA_SOS.1[2]					●							
FIA_SOS.1[3]	●											
FIA_SOS.1[4]			●									
FIA_SOS.2	●										●	
FIA_UAU.2[1]												●
FIA_UAU.2[2]					●						●	
FIA_UAU.2[3]	●											
FIA_UAU.2[4]			●									
FIA_UAU.7	●		●								●	●
FIA_UID.2[1]												●
FIA_UID.2[2]					●						●	
FIA_UID.2[3]	●											
FIA_UID.2[4]			●									
FIA_UID.2[5]	●											
FIA_USB.1		●	●		●	●						
FMT_MOF.1[1]				●								
FMT_MOF.1[2]	●		●		●							
FMT_MOF.1[3]							●					
FMT_MOF.1[4]				●				●				
FMT_MSA.3[1]		●										
FMT_MSA.3[2]			●									
FMT_MTD.1[1]	●					●		●				
FMT_MTD.1[2]	●					●						
FMT_MTD.1[3]	●				●	●					●	

セキュリティ対策方針 / セキュリティ機能要件	O.REGISTERED-USER	O.SCAN-DATA	O.SECURE-PRINT	O.CONFIG-A	O.CONFIG-B	O.CONFIG-C	O.CONFIG-D	O.OVERWRITE-ALL	O.TRUSTED-PATH	O.AUTH-CAPABILITY	※ set.admin	※ set.service
FMT_MTD.1[4]											●	
FMT_MTD.1[5]						●						
FMT_MTD.1[6]			●									
FMT_MTD.1[7]												●
FMT_MTD.1[8]	●											
FMT_MTD.1[9]								●				
FMT_MTD.1[10]	●					●		●				
FMT_MTD.1[11]								●				
FMT_MTD.1[12]								●				
FMT_MTD.1[13]	●					●		●				
FMT_SMF.1	●		●	●	●	●	●	●			●	●
FMT_SMR.1[1]											●	●
FMT_SMR.1[2]	●		●	●	●	●	●	●			●	
FMT_SMR.1[3]	●		●									
FMT_SMR.1[4]	●											
FTA_SSL.3	●										●	
FTP_ITC.1									●			
FAD_RIP.1								●				
FIT_CAP.1										●		

注) ***set.admin***、***set.service*** は、要件のセットを示しており、「●」が記され対応関係があるとされるセキュリティ対策方針は、縦軸の※ set.admin、※ set.service にて対応付けられる一連の要件セットが、当該セキュリティ対策方針にも対応していることを示す。
「●」の付け方は、以下の通りである。
縦軸のセキュリティ対策方針、set.admin、set.service に対して、対策方針を満たすセキュリティ機能要件に「●」が付けられている。

6.3.1.2. 十分性

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

- **O.REGISTERED-USER（登録ユーザーの利用）**
  本セキュリティ対策方針は、管理者によって TOE に登録されたユーザーだけに TOE が搭載される mfp の利用を制限しており、ユーザーの識別認証に関係して諸要件が必要である。

  ＜ユーザーの識別認証に必要な要件＞
  FIA_UID.2[3]、FIA_UAU.2[3]により、パネル経由でアクセスする利用者、及びネットワーク経由でアクセスする利用者が、登録済みユーザーであることを識別認証する。
  FIA_UID.2[3]により、IC カードリーダー経由でアクセスする利用者が、登録済みユーザーであることを識別する。
  認証には、FIA_UAU.7 により、パネル上の入力文字毎に保護された認証フィードバックとして、隠匿文字を返し、認証をサポートする。
  「本体認証」、「外部サーバー認証」、「認証しない」といったユーザー認証方式の選択は、

FMT_MOF.1[2]により、管理者だけに許可される。また、「本体認証」が選択された場合、「IC カードを使用する」、「IC カード+ユーザーパスワードを使用する」、「IC カードを使用しない」といったICカード方式の選択は、FMT_MOF.1[2]により、管理者だけに許可される。
FMT_SMF.1によりユーザー認証機能の管理、及びICカード機能の管理を管理者に提供する。
FIA_SOS.2により、ネットワークを経由したユーザー認証において利用されるセッション情報が生成されて、そのセッション情報が使用される。

＜識別認証されたユーザーのセッションの管理に必要な要件＞
識別認証されたユーザーのセッションの持続時間は、パネルからログインした場合、識別認証されたユーザーのセッションが、FTA_SSL.3により、非アクティブのままシステムオートリセット時間が経過すると終了することによって、不必要なセッションの継続を悪用する攻撃を困難にしている。システムオートリセット時間の変更は、FMT_MTD.1[3]により管理者に制限される。
FMT_SMF.1によりシステムオートリセット時間の管理を管理者に提供する。

＜ユーザーの識別認証情報の管理に必要な要件＞
FMT_MTD.1[1]により、ユーザー認証の方式に「本体認証」が選択されている場合において、ユーザー登録作業にて行うユーザーパスワードの初期登録は管理者だけに許可される。
またユーザー認証の方式に「本体認証」が選択されている場合、ユーザー登録におけるユーザーIDの登録は、FMT_MTD.1[8]により、及び（ICカード機能が使用される場合）ICカードIDの登録は、FMT_MTD.1[13]により管理者に許可される。
さらにユーザーIDの削除は、FMT_MTD.1[10]により、及びユーザーIDの改変は、FMT_MTD.1[3]により管理者に許可される。ICカードIDの改変及び削除は、FMT_MTD.1[13]により管理者に許可される。
FMT_SMF.1によりユーザーID、ユーザーパスワード、ICカードIDの管理を管理者に提供する。
ユーザー認証方式に「外部サーバー認証」が選択されている場合、FMT_MTD.1[8]により、識別認証されたユーザーは外部サーバーから許可されて自動的に登録される。（これは「外部サーバー」がユーザーIDを登録するということに相当。）この登録の際、FIA_UID.2[5]により、TOEにアクセスする外部サーバーは登録された外部サーバーであることを識別する。この管理行為は、FMT_SMR.1[4]により、役割：外部サーバーとして維持されて、その役割が関連付けられる。
FMT_SMF.1によりユーザーIDの管理を外部サーバーに提供する。
外部サーバー識別設定データの変更は、FMT_MTD.1[3]により管理者だけに制限されている。

FIA_SOS.1[3]により、ユーザーパスワードの品質が検証される。FMT_MTD.1[2]により、ユーザー認証の方式に「本体認証」が選択されている場合、ユーザー自身のユーザーパスワードの変更はユーザー及び管理者に制限される。
FMT_SMF.1によりユーザーパスワードの管理をユーザー及び管理者に提供する。

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

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

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として、FMT_SMR.1[3]によりユーザーとして維持されて、その役割が関連付けられる。

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

- **O.SCAN-DATA（Scan to HDD Data アクセス制御）**

本セキュリティ対策方針は、Scan to HDD Data に対するアクセスを、管理者、及び許可されたユーザーだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜ユーザーデータアクセス制御＞
ユーザーとして識別、もしくは識別認証されると、FIA_ATD.1、FIA_USB.1 により利用者タスクにタスク属性と利用者属性が関連付けられる。FDP_ACC.1[1]、FDP_ACF.1[1]により利用者タスクは、利用者属性を持ち、これと一致する Scan to HDD Data 属性を持つ Scan to HDD Data に対して一覧表示、削除、及びダウンロードが許可される。

＜ユーザーデータの管理＞
Scan to HDD Data のオブジェクト属性は、FMT_MSA.3[1]により、該当データを登録したユーザーID が設定される。

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

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

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

- **O.SECURE-PRINT（Print Data アクセス制御）**

本セキュリティ対策方針は、Secure Print Data、ID&Print Data に対する方針を説明している。まず Secure Print Data についてであるが、Secure Print Data の印刷を、許可されたユーザーだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜Print Data アクセス制御（Secure Print Data のアクセス制御）＞
ユーザーとして識別、もしくは識別認証されると、FIA_ATD.1、FIA_USB.1 により、利用者タスクにタスク属性が関連付けられる。FDP_ACC.1[2]、FDP_ACF.1[2]により、Secure Print Data に対して、印刷、削除、一覧表示操作が許可される。
Secure Print Data を印刷、及び削除するには、その Secure Print Data の利用を許可されたユーザーである必要があるが、FIA_UID.2[4]、FIA_UAU.2[4]により、その Secure Print Data の利用を許可されたユーザーであることを識別認証される。
認証には、FIA_UAU.7 により、パネル上の入力文字毎に保護された認証フィードバックとして、隠匿文字を返し、認証をサポートする。
Secure Print Data のオブジェクト属性は、FMT_MSA.3[2]より Secure Print Data の登録時に Secure Print パスワードが与えられている。

＜Secure Print パスワード＞
FMT_MTD.1[6]により、認証に利用される Secure Print パスワードの登録はユーザーだけに許可される。FIA_SOS.1[4]により Secure Print パスワードの品質は検証される。
FMT_SMF.1 により Secure Print パスワードの管理をユーザーに提供する。

次に ID&Print Data についてであるが、ID&Print Data の印刷を、許可されたユーザーだけに制

限しており、アクセス制御に関係する諸要件が必要である。

＜Print Data アクセス制御（ID&Print Data のアクセス制御）＞
ユーザーとして識別、もしくは識別認証されると、FIA_ATD.1、FIA_USB.1 により、利用者タスクにタスク属性が関連付けられる。FDP_ACC.1[2]、FDP_ACF.1[2]により、利用を許可された ID&Print Data に対して、印刷、削除、一覧表示操作が許可される。
ID&Print Data のオブジェクト属性は、FMT_MSA.3[2]より ID&Print Data の登録時にユーザーID が与えられている。

＜ID&Print Data 機能の動作管理＞
ID&Print Data 機能の動作管理は、FMT_MOF.1[2]により、管理者だけに制限されている。
FMT_SMF.1 により ID&Print 機能の管理を管理者に提供する。

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

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

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として、FMT_SMR.1[3]によりユーザーとして維持されて、その役割が関連付けられる。

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

- **O.CONFIG-A（セキュリティ強化機能の設定に関係する機能へのアクセス制限）**

本セキュリティ対策方針は、セキュリティ強化機能に関係する設定を管理者に制限しており、設定機能に対してアクセスを制限するための諸要件が必要である。

＜セキュリティ強化機能の操作制限＞
セキュリティ強化機能の停止、動作設定は、FMT_MOF.1[1]により、管理者だけに許可される。
また、全データ上書き消去機能によるセキュリティ強化機能の停止設定は、FMT_MOF.1[4]により、管理者だけに許可される。
FMT_SMF.1 によりセキュリティ強化機能の管理、及び全データ上書き消去機能の管理を管理者に提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持されて、その役割が関連付けられる。

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

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

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

- **O.CONFIG-B（mfp の設定データに関する機能へのアクセス制限）**

本セキュリティ対策方針は、mfp の設定データに関係する設定を管理者に制限しており、設定機能に対してアクセスを制限するための諸要件が必要である。

＜mfp の設定データに関係する設定管理＞
FIA_ATD.1、FIA_USB.1 により利用者タスクにタスク属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、利用者タスクは、mfp の設定データに対する設定操作が許可される。

＜MIB オブジェクトに対するアクセスに必要な要件＞
mfp の設定データは、MIB オブジェクトとしても存在するため、SNMP によるアクセスにも制限が必要である。
FIA_UID.2[2]、FIA_UAU.2[2]により、MIB オブジェクトにアクセスする利用者が管理者であることを識別認証する。
FMT_MTD.1[3]により SNMP パスワードの変更は、管理者に制限される。FIA_SOS.1[2]により、SNMP パスワードの品質が検証される。
FMT_SMF.1 により SNMP パスワードの管理を管理者に提供する。
SNMP パスワード認証機能の方式の変更できる役割は、FMT_MOF.1[2]により、管理者だけに制限される。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持されて、その役割が関連付けられる。

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

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

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

- **O.CONFIG-C（バックアップ機能、リストア機能へのアクセス制限）**

本セキュリティ対策方針は、バックアップ機能、リストア機能を管理者に制限しており、管理機能に対してアクセスを制限するための諸要件が必要である。

＜バックアップ、リストア機能の操作制限＞
FIA_ATD.1、FIA_USB.1 により利用者タスクにタスク属性が関連づけられると、利用者タスクは、
・ FDP_ACC.1[1]、FDP_ACF.1[1]により Scan to HDD Data
を対象として、バックアップ（ダウンロード）、削除、及び一覧表示操作が許可される。更に
・ FMT_MTD.1[1]によりユーザーパスワード
（ユーザー認証方式に「本体認証」が選択されている場合）
・ FMT_MTD.1[10]によりユーザーID
・ FMT_MTD.1[13]により IC カード ID（IC カード機能が使用される場合）
を対象データとして管理者だけにリストア操作が許可される。FMT_MTD.1[5]によりユーザーパスワード（「本体認証」が設定されている場合）、ユーザーID、IC カード ID（IC カード機能が

使用される場合）のバックアップ操作（すなわち問い合わせ操作）が管理者だけに許可される。
FMT_SMF.1 によりユーザーID、ユーザーパスワード、IC カード ID の管理を管理者に提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持されて、その役割が関連付けられる。

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

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

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

- **O.CONFIG-D（高信頼チャネル機能設定データの設定機能へのアクセス制限）**

本セキュリティ対策方針は、高信頼チャネル機能に関する設定を管理者に制限しており、設定機能に対してアクセスを制限するための諸要件が必要である。

＜高信頼チャネル機能設定データの操作制限＞
高信頼チャネル機能のふるまいの変更設定、停止、及び動作設定は、FMT_MOF.1[3]により、管理者だけに許可される。
FMT_SMF.1 により高信頼チャネル機能の管理を管理者に提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持されて、その役割が関連付けられる。

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

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

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

- **O.OVERWRITE-ALL（全データ上書き消去）**

本セキュリティ対策方針は、HDD、及び SSD のデータ領域、及び利用者が設定した NVRAM 上の秘匿情報を再現できなくするとしており、再現を不可能にするための諸要件が必要である。

＜全データ上書き消去機能、及び操作制限＞
FAD_RIP.1 、 FMT_MOF.1[4] 、 FMT_MTD.1[1] 、 FMT_MTD.1[9] 、 FMT_MTD.1[10] 、 FMT_MTD.1[11] 、 FMT_MTD.1[12] 、 FMT_MTD.1[13] 、 FDP_ACC.1[1] 、 FDP_ACF.1[1] 、 FDP_ACC.1[2]、FDP_ACF.1[2] 、FDP_ACC.1[3]、FDP_ACF.1[3]により、これら対象とする情報が管理者の全データ上書き操作によって以前のどの情報の内容も利用できなくすることを保証する。
FMT_SMF.1 によりユーザーID、ユーザーパスワード、管理者パスワード、Secure Print パスワ

ード、外部サーバー識別設定データ、SNMP パスワード、IC カード ID、全データ上書き消去機能の管理を管理者に提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持されて、その役割が関連付けられる。

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

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

よって本セキュリティ対策方針は満たされる。

- **O.TRUSTED-PATH（高信頼チャネルの利用）**

本セキュリティ対策方針は、Scan to HDD Data の送信において高信頼チャネルを生成するとしており、高信頼チャネルに関係する要件が必要である。
FTP_ITC.1 は、他の高信頼 IT 製品からの要求に応じて高信頼チャネルを生成するとしており、Scan to HDD Data の送信に適用される。
この機能要件によって本セキュリティ対策方針は満たされる。

- **O.AUTH-CAPABILITY（外部サーバー認証機能を利用するためのサポート動作）**

本セキュリティ対策方針は、TOE が ActiveDirectory を用いたユーザー情報管理サーバーの外部サーバー認証によるユーザー識別認証情報を利用するために必要な動作をサポートするとしており、外部 IT エンティティの動作をサポートすることを規定する諸要件が必要である。
FIT_CAP.1 により、ユーザー情報管理サーバーが実現する ActiveDirectory によるユーザー識別認証機能に対して、識別認証対象のユーザーに対する認証情報問い合わせ機能、識別認証対象のユーザーに対する認証情報取得機能を実現する。
この機能要件によって本セキュリティ対策方針は満たされる。

- ***set.admin*（管理者をセキュアに維持するために必要な要件のセット）**

＜管理者の識別認証＞
FIA_UID.2[2]、FIA_UAU.2[2]により、パネル経由でアクセスする利用者、及びネットワーク経由でアクセスする利用者が管理者であることを識別認証する。
認証には、FIA_UAU.7 により、パネル上の入力文字毎に保護された認証フィードバックとして、隠匿文字を返し、認証をサポートする。

＜識別認証された管理者のセッションの管理＞
識別認証された管理者のセッションの持続時間は、パネルからログインした場合、識別認証された管理者のセッションが、FTA_SSL.3 により、非アクティブのままシステムオートリセット時間が経過すると終了することによって、不必要なセッションの継続を悪用する攻撃を困難にしている。なおシステムオートリセット時間の変更は、FMT_MTD.1[3]により管理者に制限される。
FMT_SMF.1 によりシステムオートリセット時間の管理を管理者に提供する。

＜管理者の認証情報の管理など＞

管理者パスワードは、FIA_SOS.1[1]により品質が検証される。また、FIA_SOS.2 により、ネットワークを経由した管理者認証において利用されるセッション情報が生成されて、そのセッション情報が使用される。管理者パスワードの変更は、FMT_MTD.1[4]により、管理者及びサービスエンジニアに制限される。
FMT_SMF.1 により管理者パスワードの管理を管理者、サービスエンジニアに提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアと FMT_SMR.1[2]により管理者にて維持されて、その役割が関連付けられる。

- ***set.service*（サービスエンジニアをセキュアに維持するために必要な要件のセット）**

＜サービスエンジニアの識別認証＞
FIA_UID.2[1]、FIA_UAU.2[1]により、アクセスする利用者がサービスエンジニアであることを識別認証する。
認証には、FIA_UAU.7 により、パネル上の入力文字毎に保護された認証フィードバックとして、隠匿文字を返し、認証をサポートする。

＜サービスエンジニアの認証情報の管理など＞
CE パスワードは、FIA_SOS.1[1]により、品質が検証される。CE パスワードの変更は、FMT_MTD.1[7]により、サービスエンジニアに制限される。
FMT_SMF.1 により CE パスワードの変更の管理をサービスエンジニアに提供する。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアとして維持されて、その役割が関連付けられる。

6.3.1.3. セキュリティ機能要件の依存性

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　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 を適用しない理由＞ オブジェクト属性が存在しないため、本要件を適用する必要性はない。

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_ATD.1	なし	N/A
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_SOS.2	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FIA_UID.2[5]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MOF.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MSA.3[1]	FMT_MSA.1、 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ Scan to HDD Data のオブジェクト属性は、ユーザーID と常に一致している必要がある。よって保管のタイミングで値が与えられればよく、その他の操作タイミングにてこの属性値が変更される必要性はなく、管理要件は不要である。 ＜FMT_SMR.1＞ FMT_MSA.3.2[1]の割付はなしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MSA.3[2]	FMT_MSA.1、 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ Secure Print Data 属性： Secure Print Data のオブジェクト属性は、Secure Print パスワードであるため、保管のタイミングで値が与えられればよく、その他の操作タイミングにてこの属性値が変更される必要性はなく、管理要件は不要である。 ID&Print Data 属性： ID&Print Data のオブジェクト属性は、ユーザーID であるため、保管のタイミングで値が与えられればよく、その他の操作タイミングにてこの属性値が変更される必要性はなく、管理要件は不要である。

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
		＜FMT_SMR.1＞ FMT_MSA.3.2[2]の割付はなしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2] 、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[5]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[6]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[3]
FMT_MTD.1[7]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]
FMT_MTD.1[8]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MTD.1[9]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[11]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[12]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[13]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[5]
FTA_SSL.3	なし	N/A
FTP_ITC.1	なし	N/A
FAD_RIP.1	なし	N/A
FIT_CAP.1	なし	N/A

6.3.2. セキュリティ保証要件根拠

本 TOE は、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。本 TOE が搭載される mfp は一般的な商用事務製品であるため、機能仕様、TOE 設計に基づくテストが実施されていること、基本的な攻撃能力を持つ攻撃者に対する抵抗力を持つことが必要である。また開発環境の制御、TOE の構成管理、セキュアな配付手続きが取られていることが望まれる。従って十分な保証レベルが提供される EAL3 の選択は妥当である。

なお、保証要件依存性分析は、パッケージである EAL が選択されているため、妥当であるとして詳細は論じない。

7. TOE 要約仕様

TOEのセキュリティ機能要件より導かれるTOEのセキュリティ機能を以下の **表** 12 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 12 TOE のセキュリティ機能名称と識別子の一覧

No.	TOE のセキュリティ機能	
1	F.ADMIN	管理者機能
2	F.ADMIN-SNMP	SNMP 管理者機能
3	F.SERVICE	サービスモード機能
4	F.USERAUTH	ユーザー認証機能
5	F.USERDATA	ユーザーデータ機能
6	F.PRINT	Secure Print 機能、ID&Print 機能
7	F.OVERWRITE-ALL	全データ上書き消去機能
8	F.TRUSTED-PATH	高信頼チャネル機能
9	F.SUPPORT-AUTH	外部サーバー認証動作サポート機能

7.1. F.ADMIN（管理者機能）

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

7.1.1. 管理者識別認証機能

管理者モードへのアクセス要求に対して、アクセスする利用者が管理者であることを識別及び認証する。識別及び認証が成功した場合は管理者モードへのアクセスを許可し、失敗した場合は管理者モードへのアクセスを拒否する。

- ユーザーID が「Admin」であることを識別し、管理者の役割が関連づけられる。
- **表** 13 に示されるキャラクターからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
  - ネットワークからのアクセスに対して管理者認証後は、管理者パスワードとは別のセッション情報を利用した、管理者認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を生成して利用する。
- 操作パネルから入力される管理者パスワードのフィードバックに 1 文字毎隠匿文字を返す。

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

表 13　パスワードに利用されるキャラクターと桁数

対象	桁数	キャラクター
CE パスワード 管理者パスワード	8 桁	最低合計 94 文字の中から選択可能 （英、数、記号） ASCII コード：0x20～0x7e 0x22（”）は選択できない。
ユーザーパスワード	8 桁以上	最低合計 93 文字の中から選択可能 （英、数、記号） ASCII コード：0x20～0x7e 0x20（Space）、0x22（”）は選択できない。
Secure Print パスワード	8 桁	最低合計 93 文字の中から選択可能 （英、数、記号） ASCII コード：0x20～0x7e 0x22（”）、及び 0x2b（+）は選択できない。
SNMP パスワード ・Privacy パスワード ・Authentication パスワード	8 桁以上	最低合計 90 文字の中から選択可能 （英、数、記号） ASCII コード：0x20～0x7e 0x20（Space）、0x22（”）、0x23（#）、0x27（’）、 及び 0x5c（Backslash）は選択できない。

7.1.2. 管理者モードのオートログアウト機能

管理者モードにパネル操作のアクセス中でシステムオートリセット時間以上何らかの操作を受け付けなかった場合は、自動的に管理者モードをログアウトする。

以上により FTA_SSL.3 が実現される。

7.1.3. 管理者モードにて提供される機能

管理者モードへのアクセス要求において管理者識別認証機能により､管理者として識別認証されると、利用者タスクにタスク属性が関連づけられ、その属性が維持される。管理者として識別認証が成功した場合のみ、以下の操作、機能の利用が許可される。

FIA_ATD.1、FIA_USB.1 は上記により実現される。

7.1.3.1. 管理者パスワードの変更

新規設定される管理者パスワードが品質を満たしている場合、変更する。この機能は、パネル操作のみの機能である。

この機能は、管理者の役割を維持する。

新規設定される管理者パスワードは以下の品質を満たしていることを検証する。

- **表** 13 の管理者パスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。
- 現在設定される値と一致しない。

管理者のパスワード変更は、管理者とサービスエンジニアのみに許可する。サービスエンジニアに対する管理者のパスワード変更は、7.3.2 に示す。

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

7.1.3.2. ユーザーの設定

- ユーザー登録（ユーザー認証方式：本体認証において利用されるユーザーのみ）
  クライアント PC 経由でユーザーID を設定し、ユーザーパスワードを登録（「本体認証」が設定されている場合）してユーザーが登録される。
  また、IC カード機能を使用する場合は、パネル経由、もしくはクライアント PC 経由で IC カード ID を設定する。
  新しく設定されるユーザーパスワードは以下の品質を満たしていることを検証する。
  - **表** 13 のユーザーパスワードに示される桁数、キャラクターから構成される。
  - 1 つのキャラクターで構成されない。

  なお、外部サーバー認証を有効にしている場合は、ユーザーパスワード、IC カード ID の登録はできない。

- ユーザー削除（ユーザー認証方式：本体認証、または外部サーバー認証において利用されるユーザー）
  クライアント PC 経由でユーザーID を削除する。

- ユーザーID の変更（ユーザー認証方式：本体認証において利用されるユーザーのみ）
  クライアント PC 経由でユーザーID を変更する。

- IC カード ID の変更（ユーザー認証方式：本体認証、かつ IC カード機能が利用されるユーザーのみ）
  パネル経由で IC カード ID を変更する。

- IC カード ID の削除（ユーザー認証方式：本体認証、かつ IC カード機能が利用されるユーザーのみ）
  パネル経由、もしくはクライアント PC 経由で IC カード ID を削除する。

- ユーザーパスワードの変更（ユーザー認証方式：本体認証において利用されるユーザーのみ）
  クライアント PC 経由でユーザーパスワードを変更する。新しく設定されるユーザーパスワードは以下の品質を満たしていることを検証する。
  - **表** 13 のユーザーパスワードに示される桁数、キャラクターから構成される。
  - 1 つのキャラクターで構成されない。
  - 現在設定される値と一致しない。

  この機能（ユーザーパスワードの変更）は、ユーザーの役割を維持する。

  ユーザーパスワードの変更を除き上記の機能は、管理者のみに許可する。ユーザー自身のユーザーパスワードは、ユーザー自身にも許可する。

以上により FIA_SOS.1[3]、FMT_MTD.1[1]、FMT_MTD.1[2]、FMT_MTD.1[3]、FMT_MTD.1[8]、FMT_MTD.1[10]、FMT_MTD.1[13]、FMT_SMR.1[3]、FMT_SMF.1 が実現される。

7.1.3.3. ユーザー認証機能の設定

ネットワークを介して、ユーザー認証機能における以下の認証方式を設定する。

- 本体認証：mfp 本体側で管理するユーザーパスワードを利用する認証方式
- 外部サーバー認証：ネットワークを介して接続されるユーザー情報管理サーバーにて管理されるユーザーパスワードを利用する認証方式（ActiveDirectory 方式のみ対象）
  - 外部サーバー認証を利用する場合は、ネットワークを介して、外部サーバー識別設定データ（外部サーバーが所属するドメイン名など）を設定する。
- 認証しない：mfp を利用するユーザーを認証しない方式

以下に、ユーザー認証機能におけるセキュリティ機能のふるまいの管理の関係を示す。

- 「を停止する」
  - 「本体認証」、または「外部サーバー認証」から「認証しない」に設定を変更する。
- 「を動作する」
  - 「認証しない」から「本体認証」、または「外部サーバー認証」に設定を変更する。
- 「のふるまいを改変する」
  - 「本体認証」から、「外部サーバー認証」に設定を変更する。または、「外部サーバー認証」から、「本体認証」に設定を変更する。

上記の設定は、管理者のみに許可する。

以上により FMT_MOF.1[2]、FMT_MTD.1[3]、FMT_SMF.1 が実現される。

7.1.3.4. オートログアウト機能の設定

パネルを介して、オートログアウト機能における設定データであるシステムオートリセット時間を以下に示す時間範囲で設定する。

- システムオートリセット時間　　：1～9 分

この設定は、管理者のみに許可する。

以上により FMT_MTD.1[3]、FMT_SMF.1 が実現される。

7.1.3.5. ネットワークの設定

パネル、ネットワークを介して、以下の設定データの設定操作を行う。

- mfp の設定データに関係する一連の設定データ（IP アドレス、AppleTalk プリンター名等）
  ・IP アドレス（パネル、ネットワーク経由の両方から設定可能）
  ・AppleTalk プリンター名（ネットワーク経由のみから設定可能）

この設定は、管理者のみに許可する。

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

7.1.3.6. バックアップ、リストア機能の実行

管理者パスワード、CE パスワードを除いて、HDD に保管される設定データをバックアップ、リストアする。

・ネットワークを介して、ユーザーパスワード（「本体認証」が設定されている場合）、
ユーザーID、IC カード ID（「本体認証」、及び「IC カード」、「IC カード+ユーザーパスワード」

が設定されている場合）をバックアップする。
・ネットワークを介して、Scan to HDD Data をバックアップ（ダウンロード）する。
・ネットワークを介して、ユーザーパスワード（「本体認証」が設定されている場合）、ユーザーID、IC カード ID（「本体認証」、及び「IC カード」、もしくは「IC カード+ユーザーパスワード」が設定されている場合）をリストアする。
・ネットワークを介して、すべての Scan to HDD Data の一覧を表示する。
・ネットワークを介して、Scan to HDD Data を削除する。

上記の機能は、管理者のみに許可する。

以上により FDP_ACC.1[1]、FDP_ACF.1[1]、FMT_MTD.1[1]、FMT_MTD.1[10]、FMT_MTD.1[5] 、FMT_MTD.1[13]、FMT_SMF.1 が実現される。

7.1.3.7. SNMP パスワードの変更

SNMP パスワード（Privacy パスワード、Authentication パスワード）を変更する。新しく設定される SNMP パスワードが以下の品質を満たしていることを検証する。
この機能は、管理者の役割を維持する。
- 表 13 のSNMPパスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。

この変更は、管理者のみに許可する。

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

7.1.3.8. SNMP パスワード認証機能の設定

ネットワークを介して、SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。

この設定は、管理者のみに許可する。

以上により FMT_MOF.1[2]、FMT_SMF.1 が実現される。

7.1.3.9. 高信頼チャネル機能の設定

ネットワークを介して、SSL/TLS による高信頼チャネル機能設定データを設定する。
- 通信暗号強度設定（通信暗号方式の変更）
- 高信頼チャネル機能の動作・停止設定

上記の設定は、管理者のみに許可する。

以上により FMT_MOF.1[3]、FMT_SMF.1 が実現される。

7.1.3.10. セキュリティ強化機能に関連する機能

管理者が操作するセキュリティ強化機能の設定に影響する機能は以下の通り。

- セキュリティ強化機能の動作設定
  パネルを介して、セキュリティ強化機能の有効、無効を設定する機能。
- HDD 論理フォーマット機能
  パネルを介して、HDD にファイルシステムで利用する管理データの初期値を書き込む機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- 全データ上書き消去機能
  パネルを介した、全データ上書き消去の実行により、セキュリティ強化機能の設定を無効にする。

この機能は、管理者のみに許可する。

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

7.1.3.11. 全データ上書き消去機能の管理

全データ上書き消去機能の実行は、パネルを介して管理者のみに制限する。
全データ上書き消去機能の実行によって、消去、初期化されるデータは、「7.7」に記載される。
なお、ユーザーパスワードの消去は、ユーザー認証方式に「本体認証」が選択されている場合に限る。
また、IC カード ID の消去は、ユーザー認証方式に「本体認証」が選択されている場合、かつ IC カード機能が利用される場合に限る。

以上により FDP_ACC.1[1]、FDP_ACF.1[1]、FDP_ACC.1[2]、FDP_ACF.1[2]、FDP_ACC.1[3]、FDP_ACF.1[3]、FMT_MOF.1[4]、FMT_MTD.1[1]、FMT_MTD.1[9]、FMT_MTD.1[10]、FMT_MTD.1[11]、FMT_MTD.1[12]、FMT_MTD.1[13]、FMT_SMF.1 が実現される。

7.1.3.12. IC カード方式の設定

「本体認証」が設定されている場合で且つ、IC カード機能を使用する場合は、ネットワークを介して、IC カード方式を設定する。

- IC カード：IC カードを使用して識別する方式
- IC カード+ユーザーパスワード：IC カードとユーザーパスワードを使用して識別認証する方式
- IC カードを使用しない：IC カード機能を使用しない

上記の設定は、管理者のみに許可する。

以上により FMT_MOF.1[2]、FMT_SMF.1 が実現される。

7.1.3.13. ID&Print 機能の設定

ネットワークを介して、以下の ID&Print 機能の動作モードを設定する。

- ID&Print 自動動作モード（ID&Print 機能が有効）
  クライアント PC より送信されるプリントデータにおいて、通常の印刷設定での印刷要求が行われた場合でも、プリントデータを ID&Print Data として登録する動作モード
- ID&Print 指定動作モード（ID&Print 機能が無効）
  クライアント PC より送信されるプリントデータにおいて、ID&Print Data として登録要求が行われた場合のみ、プリントデータを ID&Print Data として登録する動作モード

上記の設定は、管理者のみに許可する。

以上により FMT_MOF.1[2]、FMT_SMF.1 が実現される。

7.2. F.ADMIN-SNMP（SNMP 管理者機能）

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

7.2.1. SNMP パスワードによる識別認証機能

SNMP を用いてネットワークを介して MIB オブジェクトにアクセスする利用者が管理者であることを SNMP パスワードによって識別認証する。識別及び認証が成功した場合は、管理者の役割が関連づけられ、MIB オブジェクトにアクセスを許可し、失敗した場合は MIB オブジェクトにアクセスを拒否する。

- 管理者を識別するために、SNMP パスワードを使用して識別する。
- **表 13** に示されるキャラクターからなるSNMPパスワードにより認証するSNMP認証メカニズムを提供する。
  - Authentication パスワードのみ、または Privacy パスワード及び Authentication パスワード双方を利用する。
  - SNMP の場合は、別途セッション情報による管理者認証メカニズムを必要とせず、毎回のセッションに SNMP パスワード利用する。

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

7.2.2. SNMP を利用した管理機能

以下に示す操作要求において SNMP パスワードによる識別認証機能により、管理者として識別認証されると、利用者タスクにタスク属性が関連づけられ、その属性が維持される。管理者として識別認証が成功した場合のみ、以下の操作、機能の利用が許可される。

FIA_ATD.1、FIA_USB.1 は上記により実現される。

① ネットワークの設定

ネットワークを介して、以下の設定データの設定操作を行う。

- mfp の設定データに関係する一連の設定データ（IP アドレス、AppleTalk プリンター名等）

この機能は、管理者のみに許可する。

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

② SNMP パスワードの変更

この機能（SNMP パスワードの変更）は、管理者の役割を維持する。

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

- **表 13** のSNMPパスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。

この変更は、管理者のみに許可する。

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

③ SNMP パスワード認証機能の設定

ネットワークを介して、SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。

この設定は、管理者のみに許可する。

以上により FMT_MOF.1[2]、FMT_SMF.1 が実現される。

7.3. F.SERVICE（サービスモード機能）

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

7.3.1. サービスエンジニア識別認証機能

パネルからサービスモードへのアクセス要求に対して、アクセスする利用者をサービスエンジニアであることを識別及び認証する。識別及び認証が成功した場合は、サービスエンジニアの役割が関連づけられ、サービスモードへのアクセスを許可し、失敗した場合はサービスモードへのアクセスを拒否する。

- サービスエンジニアの識別は、サービスモードへのアクセスを要求するための操作を行なった時に識別する。
- **表** 13 に示されるキャラクターからなるCEパスワードにより認証するCE認証メカニズムを提供する。
  - サービスモードの場合はパネルからのアクセスのみになるため、別途セッション情報による CE 認証メカニズムを必要としない。
- 操作パネルから入力される CE パスワードのフィードバックに 1 文字毎隠匿文字を返す。

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

7.3.2. サービスモードにて提供される機能

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

① CE パスワードの変更

この機能（CE パスワード変更）は、サービスエンジニアの役割を維持する。

新規設定されるパスワードが品質を満たしている場合、変更する。

- 新規設定される CE パスワードは以下の品質を満たしていることを検証する。
  - **表** 13 のCEパスワードに示される桁数、キャラクターから構成される。
  - 1 つのキャラクターで構成されない。
  - 現在設定される値と一致しない。

この変更は、サービスエンジニアのみに許可する。

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

② **管理者パスワードの変更**

この機能（管理者パスワード変更）は、管理者の役割を維持する。

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

- **表** 13 の管理者パスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。
- 現在設定される値と一致しない。

管理者のパスワード変更は、管理者とサービスエンジニアのみに許可する。管理者に対する管理者のパスワード変更は、7.1.3.1 に示す。

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

7.4. F.USERAUTH（ユーザー認証機能）

F.USERAUTH とは、mfp の諸機能を利用するにあたって、ユーザーを識別認証する。IC カード機能を使用する場合は、ユーザーを識別する。また識別認証されたユーザーには、F.USERDATA や F.PRINT などの機能の利用を許可する他、本体認証時に mfp 本体にて管理されるユーザーパスワードの管理機能を提供する。

ユーザー機能（F.USERDATA、F.PRINT などの機能の総称）へのアクセス要求においてユーザー識別認証機能により、ユーザーとして識別、もしくは識別認証されると、利用者タスクにタスク属性、利用者属性が関連づけられ、その属性が維持される。ユーザーとして識別認証が成功した場合のみ、以下の操作、機能の利用が許可される。

以上により FIA_ATD.1、FIA_USB.1 が実現される。

7.4.1. ユーザー識別認証機能

Scan to HDD Data、Secure Print Data、及び ID&Print Data へのアクセス要求において、ユーザーであることを識別認証する。識別もしくは識別認証が成功した場合は、ユーザーの役割が関連づけられ、F.USERDATA 及び F.PRINT の利用を許可する。また、失敗した場合は F.USERDATA 及び F.PRINT の利用を拒否する。

設定されているユーザー認証方式、IC カード方式によって、以下の識別処理を行う。

表 14　ユーザー認証方式、IC カード方式による識別

	IC カード方式		
ユーザー認証方式	「IC カード」	「IC カード+ ユーザーパスワード」	「IC カードを使用しない」
「本体認証」	①	②	③
「外部サーバー認証」	④		

- ユーザー認証方式に「本体認証」が設定されている。

①、もしくは②が設定されている場合は、かざされた IC カード ID が HDD に登録されている IC カード ID であることを識別する。識別された IC カード ID によって、ユーザーID を特定する。

③が設定されている場合は、入力されたユーザーID が HDD に登録されているユーザーID であることを識別する。また、①や②が設定されている場合において、ユーザーが IC カードリーダーではなく、パネル経由の識別認証を使用した場合は、入力されたユーザーID が HDD に登録されているユーザーID であることを識別する。

- ユーザー認証方式に「外部サーバー認証」が設定されている。

④が設定されている場合は、入力されたユーザーID が外部サーバーに登録されているユーザーID であることを識別する。

ユーザーの認証は、以下の認証処理を行う。

- **表** 13 に示されるキャラクターからなるユーザーパスワードにより、ユーザーを認証するユーザー認証メカニズムを提供する。
  - ネットワークからのアクセスに対してユーザー認証後は、ユーザーパスワードとは別のセッション情報を利用した、ユーザー認証メカニズムを提供する。
  - プロトコルに応じて、10^{10}以上のセッション情報を生成して利用する。
- 操作パネルから入力されるユーザーパスワードのフィードバックに 1 文字毎隠匿文字を返す。

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

＜ユーザーID の自動登録＞

ユーザー認証方式に「外部サーバー認証」が選択されている場合の機能である。

外部サーバーと接続する場合は、外部サーバー識別設定データを使用して、識別を行う。識別に失敗した場合は、外部サーバーとの接続は行わない。

ユーザーの識別認証が成功した場合は、外部サーバーの役割が関連づけられ、維持される。また、外部サーバーによって、ユーザーの識別認証に伴って利用されたユーザー名をユーザーID として登録する。

以上により FIA_UID.2[5]、FMT_MTD.1[8]、FMT_SMF.1、FMT_SMR.1[4]が実現される。

7.4.2. ユーザー識別認証ドメインにおけるオートログアウト機能

識別認証されたユーザーがアクセス中､システムオートリセット時間以上何らかの操作を受け付けなかった場合、自動的にユーザー識別認証ドメイン（ユーザーの識別認証成功を継続している状態）からログアウトする。この機能は、パネル操作のみである。

以上により FTA_SSL.3 が実現される。

7.4.3. ユーザーパスワードの変更機能

ネットワーク経由で識別認証され､ユーザー識別認証ドメインへのアクセスが許可されると､本人のユーザーパスワードを変更することが許可される。なお外部サーバー認証が有効の場合には､本機能は利用できない。

新規設定されるユーザーパスワードが以下の品質を満たしている場合、変更する。

- **表** 13 のユーザーパスワードに示される桁数、キャラクターから構成される。
- 1 つのキャラクターで構成されない。
- 現在設定される値と一致しない。

この機能は、ユーザーの役割を維持する。

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

7.5. F.USERDATA（ユーザーデータ機能）

F.USERDATA とは、登録ユーザーであると識別、もしくは識別認証されたユーザーに対して、当該ユーザーの Scan to HDD Data の各種操作を許可するアクセス制御機能に関係する一連のセキュリティ機能のことである。

＜Scan to HDD Data の登録＞

- Scan to HDD Data の新規登録操作において、Scan to HDD Data のオブジェクト属性には、登録操作をしたユーザーのユーザーID を設定する。

以上により FMT_MSA.3[1]が実現される。

7.5.1. Scan to HDD 機能

Scan to HDD Data に対するアクセス制御機能

ユーザーの識別認証機能により、タスク属性と利用者属性が利用者タスクに関連づけられる。このタスクは、利用者属性と一致するオブジェクト属性を持つ Scan to HDD Data に対して一覧表示（パネル経由、ネットワーク経由）、ダウンロード（ネットワーク経由）、削除（パネル経由、ネットワーク経由）を行うことを許可される。

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

7.6. F.PRINT（Secure Print 機能、ID&Print 機能）

F.PRINT とは、Secure Print 機能、及び ID&Print 機能におけるセキュリティ機能である。

登録ユーザーであると識別、もしくは識別認証されたユーザーに対して、パネルからの Secure Print Data へのアクセスに対して Secure Print Data の利用を許可されたユーザーであることを認証し、認証後に当該 Secure Print Data の印刷、削除を許可するアクセス制御機能を提供する。

また登録ユーザーであると識別、もしくは識別認証されたユーザーに対して、パネルからの ID&Print Data へのアクセスに対して当該ユーザーが登録した ID&Print Data の印刷、削除を許可するアクセス制御機能を提供する。

7.6.1. Secure Print 機能

Secure Print 機能へのアクセス要求においてユーザー識別認証機能により、ユーザーとして識別、もしくは識別認証されると、利用者タスクにタスク属性が関連づけられ、その属性が維持される。ユーザーとして識別認証が成功した場合のみ、以下の操作、機能の利用が許可される。

以下の機能は、ユーザーのみに許可する。

①Secure Print パスワードによる認証機能

登録ユーザーであることが識別、もしくは識別認証されると、パネルから Secure Print Data へのアクセス要求に対して、アクセスする利用者を当該 Secure Print Data の利用を許可されたユーザーであることを識別認証する。認証に成功した場合は当該 Secure Print Data のアクセスを許可し、認証に失敗した場合は Secure Print Data のアクセスを拒否する。

- Secure Print Data の利用を許可されたユーザーの識別は、ユーザーがパネルを介してアクセスを要求する Secure Print Data の選択操作を行なった時に識別する。
- **表** 13 に示されるキャラクターからなるSecure Printパスワードにより認証するSecure Print

Data認証メカニズムを提供する。なお、Secure Printパスワードが桁数の品質を満たさない、１つのキャラクターで構成されている、文字種の品質を満たさない場合、印刷、削除を許可しない。

- Secure Print の場合はパネルからのアクセスのみになるため、別途セッション情報による Secure Print Data 認証メカニズムを必要としない。
- 操作パネルから入力される Secure Print パスワードのフィードバックに 1 文字毎隠匿文字を返す。

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

② Secure Print Data に対するアクセス制御機能

ユーザーの識別、もしくは識別認証に成功すると、Print Data アクセス制御が動作して、すべての Secure Print Data に対して、一覧表示を許可する。

Secure Print Data の識別認証に成功すると、以下の Print Data アクセス制御が動作する。

- 利用者タスクは、Secure Print Data に対して印刷、削除を許可される。

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

③ Secure Print Data の登録機能

Secure Print Data の登録要求において、登録されたユーザーとして認証されると、Secure Print パスワードを対象となる Secure Print Data と共に登録することを許可する。

以上により FMT_MTD.1[6] 、FMT_SMF.1 が実現される。

- Secure Print パスワードの検証

  登録された Secure Print パスワードが以下の条件を満たすことを検証する。

  ・ 表 13 で示したキャラクターであること

以上により FIA_SOS.1[4]が実現される。

- Secure Print パスワードの付与

  Secure Print Data の登録要求において、Secure Print パスワードの登録に要求される検証が完了すると、Secure Print パスワードを当該 Secure Print Data に設定する。

以上により FMT_MSA.3[2]が実現される。

7.6.2. ID&Print 機能

ID&Print 機能へのアクセス要求においてユーザー識別認証機能により、ユーザーとして識別、もしくは識別認証されると、利用者タスクにタスク属性が関連づけられ、その属性が維持される。ユーザーとして識別認証が成功した場合のみ、以下の操作、機能の利用が許可される。

以下の機能は、ユーザーのみに許可する。

① ID&Print Data に対するアクセス制御機能

ユーザーの識別、もしくは識別認証に成功すると、以下の Print Data アクセス制御が動作する。

- 利用者タスクは、利用者属性と一致するオブジェクト属性を持つ ID&Print Data に対して印刷、削除、一覧表示が許可される。

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

② ID&Print Data の登録機能

ID&Print Data の登録要求において、登録されたユーザーとして認証されると、ID&Print Data が登録される。

➢ ユーザーID の付与

登録するユーザーのユーザーID を ID&Print Data に設定する。

以上により FMT_MSA.3[2]が実現される。

7.7. F.OVERWRITE-ALL（全データ上書き消去機能）

F.OVERWRITE-ALL とは、管理者の明示的な消去操作により、HDD、及び SSD のデータ領域に上書き消去を実行すると共に NVRAM に設定されているパスワード等の設定値を初期化する。消去、または初期化されるべき対象は以下の通りである。

＜消去される対象：HDD＞

- Secure Print Data
- Scan to HDD Data
- ID&Print Data
- 待機状態にあるジョブの画像ファイル
- 保管画像ファイル
- HDD 残存画像ファイル
- 画像関連ファイル
- ユーザーID
- ユーザーパスワード
- IC カード ID
- Secure Print パスワード
- 外部サーバー識別設定データ
- 残存 TSF データ

＜消去される対象：SSD＞

- SSD 画像ファイル
- 送信宛先データファイル

＜初期化される対象：NVRAM＞

- 管理者パスワード
- SNMP パスワード
- 高信頼チャネル設定データ　　・・・初期化状態は何も存在しないので消去される。
- mfp の設定データ

HDDに書き込むデータ、書き込む回数など消去方式は、F.ADMINにおいて設定される全データ上書き消去機能の消去方式（**表 15**）に応じて実行される。また、SSDは固定値（0x00）で上書き消去される。なお、本機能の実行においてセキュリティ強化機能の設定は無効になる。（F.ADMINにおけるセキュリティ強化機能の動作設定の記載参照）

この機能は、管理者のみに許可する。

以上により FAD_RIP.1 が実現される。

表 15　全データの上書き消去のタイプと上書きの方法

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

7.8. F.TRUSTED-PATH（高信頼チャネル機能）

F.TRUSTED-PATH とは、TOE とクライアント PC 間で Scan to HDD Data（TOE からクライアント PC へのダウンロード）を送信する際に、SSL または TLS プロトコルを使用して、高信頼チャネルを生成、及び実現する機能である。
通信は、クライアント PC からの要求により開始する。
以上により FTP_ITC.1 が実現される。

7.9. F.SUPPORT-AUTH（外部サーバー認証動作サポート機能）

F.SUPPORT-AUTH とは、ActiveDirectory によるユーザー情報管理サーバーと連携してユーザー識別認証機能を実現するための機能である。（F.USERAUTH と共に動作する機能である。）
ユーザー認証方式に「外部サーバー認証」が選択されている場合で、ユーザーから識別認証処理が要求されると、ユーザー情報管理サーバーに対して該当ユーザーに対する認証情報の問い合わせを行う。これに対してユーザー情報管理サーバーから返される認証情報を取得し、ユーザーの識別認証処理を実現する。
以上により、FIT_CAP.1 が実現される。