bizhub PRESS 1250 Series

bizhub PRESS 1250 /
bizhub PRESS 1250P /
bizhub PRESS 1052 /
bizhub PRO 951 /
ineo 1250 /
ineo 1052 /
ineo 951

セキュリティターゲット

バージョン：1.12

発行日：2012年7月27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
2011/12/1	1.00	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	初版
2012/1/23	1.01	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・運用環境のセキュリティ対策方針（OE.EQUIPMENT）の追加 ・その他、内部による見直し修正
2012/1/27	1.02	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・BOXデータの削除機能を追加 ・その他、内部による見直し修正
2012/2/2	1.03	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・内部による見直し修正
2012/2/9	1.04	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・TOE識別（コントローラ制御プログラム）の修正
2012/3/3	1.05	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・監査ログのUSB出力の削除 ・OE.SETTING-SECURITYの修正 ・FMT_MSA.3.2の割付の修正 ・TOE識別の修正 ・FPT_TEE.1のアクションの変更
2012/3/8	1.06	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・ASM.SETTINGに関連する修正 ・ASM.SECRETに関連する修正 ・FMT_MSA.3.2に関連する修正 ・FPT_TEE.1のアクションの変更
2012/3/14	1.07	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・TOE名称に関する修正 ・内部による見直し修正
2012/4/11	1.08	開発本部　エレクトロニクス開発センターPPSW開発部	角谷	中神	安加賀	・管理機能（FMT_SMF.1）の修正 ・監査対象事象（FAU_GEN.1）の時刻に関する修正
2012/6/7	1.09	開発本部　PPシステム制御開発センターPPシステム制御開発部	角谷	中神	安加賀	・内部による見直し修正 ・ガイダンス文書に関わる修正 ・管理者パスワードに関わる修正
2012/7/19	1.10	開発本部　PPシステム制御開発センターPPシステム制御開発部	角谷	中神	安加賀	・監査ログに関わる修正
2012/7/26	1.11	開発本部　PPシステム制御開発センターPPシステム制御開発部	角谷	中神	安加賀	・誤記の修正
2012/7/27	1.12	開発本部　PPシステム制御開発センターPPシステム制御開発部	角谷	中神	安加賀	・ガイダンス文書名に関わる修正

—【 目次 】

—【 図目次 】

—【 表目次 】

1. ST 概説

1.1. ST 参照

・ST名称　：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 セキュリティターゲット
・STバージョン　：1.12
・作成日　：2012年7月27日
・作成者　：コニカミノルタビジネステクノロジーズ株式会社

1.2. TOE 参照

・TOE名称　：日本語名：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア
英語名　：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 control software
・TOE識別　：画像制御プログラム（画像制御　I1）：A4EU0Y0-00I1-G00-15
コントローラ制御プログラム(ICコントローラ　P)：A4E-00P1-G00-15
・TOEの種別　：ソフトウェア
・製造者　：コニカミノルタビジネステクノロジーズ株式会社

※bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェアと bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 control software は名称が異なるだけで同一物である。以降 TOE の名称を bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェアと記述する。また、bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 は、以降 bizhub PRESS 1250 シリーズと記述する。

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、TOE の動作環境について説明する。

1.3.1. TOE の種別

TOE である bizhub PRESS 1250 シリーズ 全体制御ソフトウェアとは、コニカミノルタビジネステクノロジーズ株式会社製高速印刷用の大型デジタル複合機（以降、デジタル複合機と記す）「bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951」に搭載され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 を搭載する bizhub PRESS 1250 シリーズは、ネットワーク機能を搭載したデジタル複合機であり、コピー/プリンタなどを活用した機能、bizhub PRESS 1250 シリーズを運用管理するための機能及び bizhub PRESS 1250 シリーズを保守管理するための機能を提供する（以下、これらすべての総称として MFP と呼称する）。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を制御する“bizhub PRESS 1250 シリーズ 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ドキュメントデータの漏洩を防止する。このため、ドキュメントデータを保護するユーザ BOX 機能を提供する。さらには、管理者機能、CE 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やユーザ BOX パスワードの管理を行うための機能を実装する。製品関係者の TOE に対する操作内容は日時と共に監査ログとして格納され、管理者は不正な操作を検出することができる。また、ドキュメントデータを保存する媒体である HDD（ハードディスク装置）には HDD ロック機能を持ったものを採用している。TOE は HDD に対して一定のパスワード規約を満たす HDD ロックパスワードを設定し、起動時に HDD ロックパスワード認証により HDD の正当性を確認し、正当性が確認されない場合は MFP 本体の動作を停止する。

1.4. TOE 記述

1.4.1. TOE の利用に関係する人物の役割

TOE の搭載される MFP の利用に関連する人物の役割を以下に定義する。

- 一般利用者

  一般利用者は、bizhub PRESS 1250 シリーズを導入する組織に在籍し、bizhub PRESS 1250 シリーズのコピー/プリンタなどに関する利用者機能を利用する。特に管理者により TOE に登録されることで、bizhub PRESS 1250 シリーズの HDD（ハードディスク装置）上に存在するユーザ BOX を所有することが出来る（TOE に登録され、ユーザ BOX を所有する一般利用者をユーザと呼称する）。

  一般利用者としては、IT の基礎知識をもっており、公開された情報を使って攻撃はできるが、公開されていない新たな攻撃手法を考案することはできないことを想定する。

- 管理者

  管理者は、bizhub PRESS 1250 シリーズを導入する組織に在籍し、bizhub PRESS 1250 シリーズの運用管理を行う。bizhub PRESS 1250 シリーズが提供する運用管理の機能を利用し、TOE にユーザ BOX の登録を行う。

- 責任者

  責任者は、bizhub PRESS 1250 シリーズを導入する組織に在籍し、管理者を選任する。

- CE[1]

  CE は、bizhub PRESS 1250 シリーズの保守を委託されている企業に在籍する。CE は bizhub PRESS 1250 シリーズが提供する保守管理の機能を利用し、bizhub PRESS 1250 シリーズの保守作業を行う。責任者又は管理者と bizhub PRESS 1250 シリーズの保守契約を締結している。

なお、一般利用者、管理者、責任者、及び CE を製品関係者とする。

[1] Customer service Engineer の略称。

1.4.2. TOE の物理的範囲

1.4.2.1. 利用環境

TOE は、bizhub PRESS 1250 シリーズ 全体制御ソフトウェアである。TOE を搭載する bizhub PRESS 1250 シリーズは、ネットワーク機能を搭載したデジタル複合機であり、コピー/プリンタなどを活用した機能、bizhub PRESS 1250 シリーズを運用管理するための機能及び bizhub PRESS 1250 シリーズ を保守管理するための機能を提供する。bizhub PRESS 1250 シリーズの利用環境として『図 1　bizhub PRESS 1250 シリーズの利用環境の例』に示すオフィスを想定する。

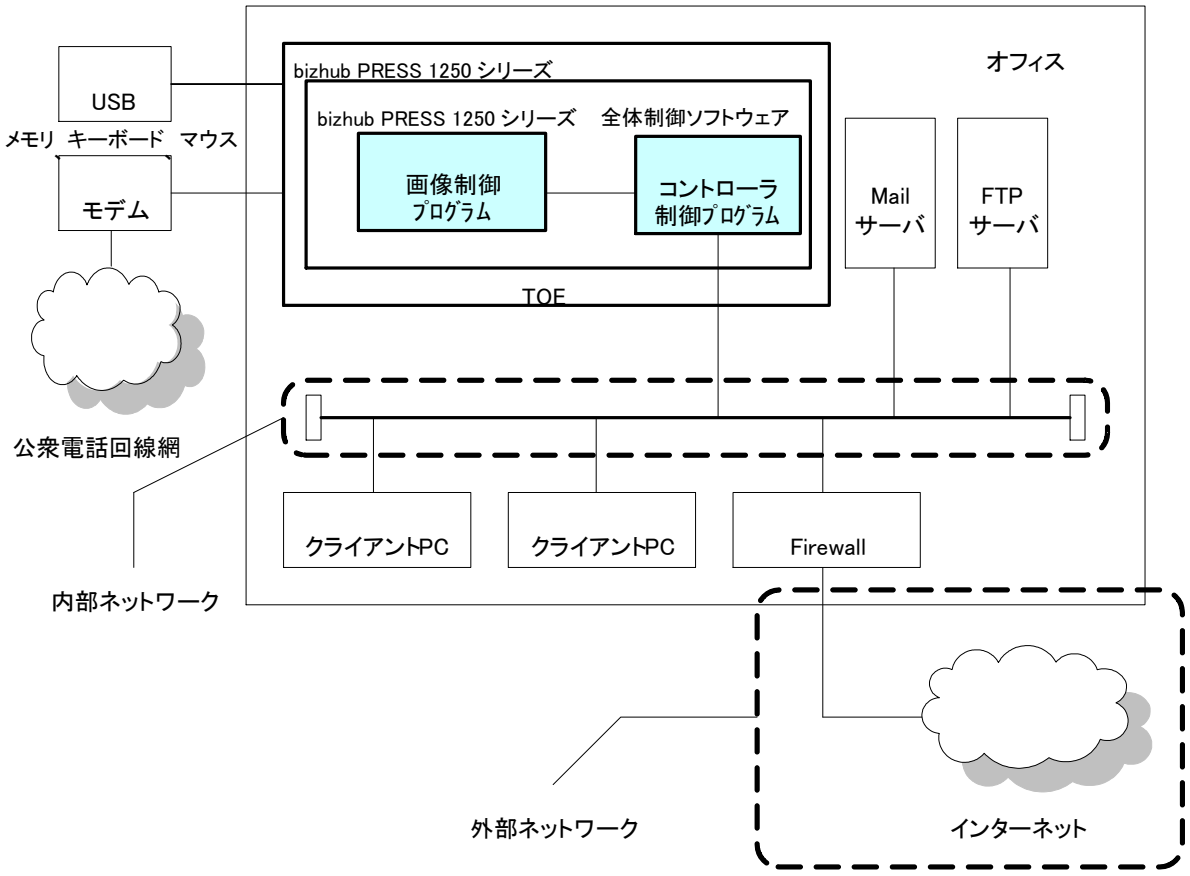
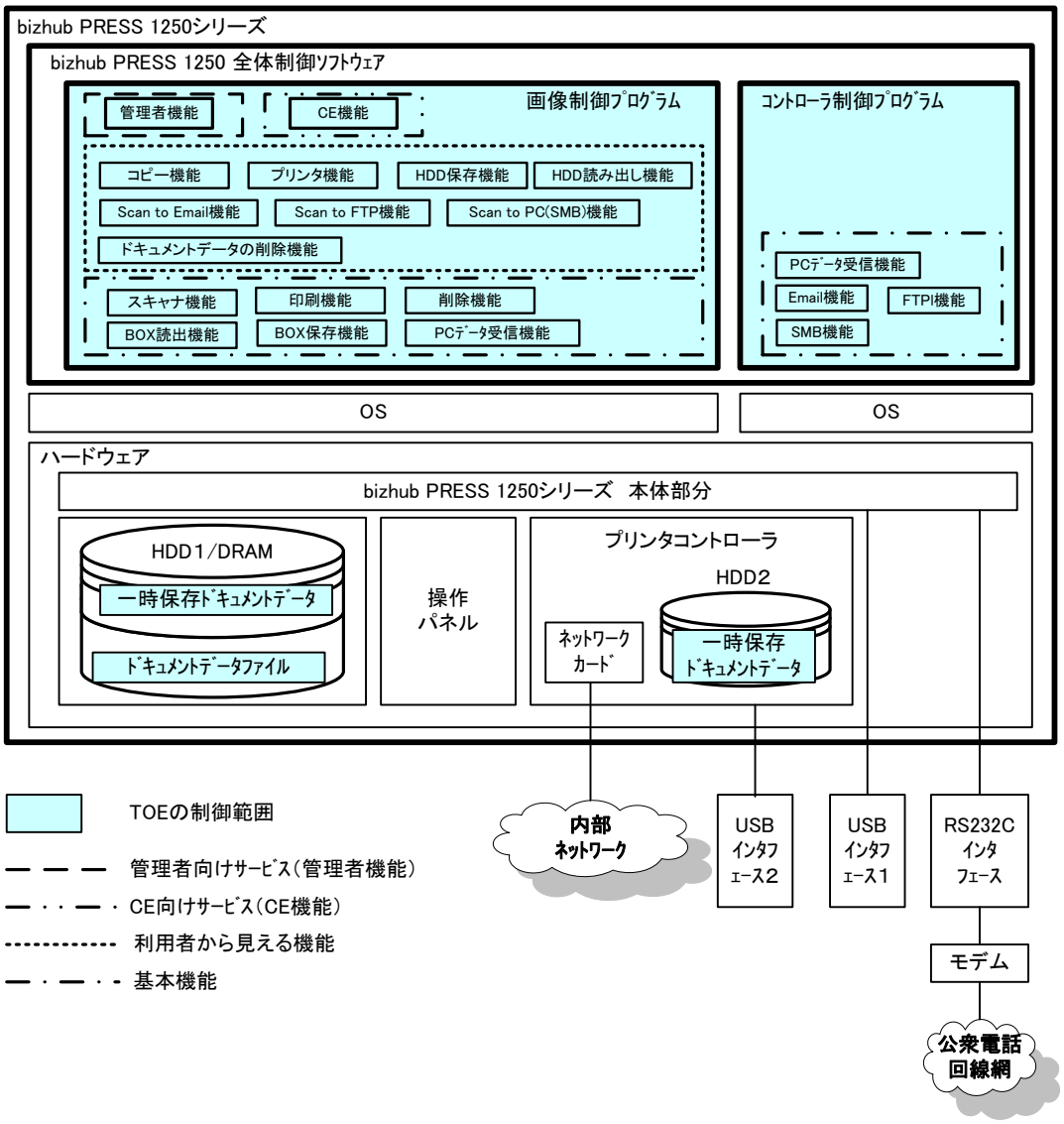


図 1　bizhub PRESS 1250 シリーズの利用環境の例

TOE は、内部ネットワークを経由してドキュメントデータを送受信する機能を持つ。したがって、TOE を搭載する bizhub PRESS 1250 シリーズは、『図 1　bizhub PRESS 1250 シリーズの利用環境の例』に示すように内部ネットワーク及び公衆電話回線網に接続される。内部ネットワークは、一般利用者のクライアント PC、及び bizhub PRESS 1250 シリーズがデータを送信する Mail サーバや FTP サーバと接続する。MFP に接続される公衆回線は、CSRC の通信に利用される。TOE は外部ネットワークとのインタフェースは持たない。オフィス内 LAN が外部ネットワークと接続する場合は、内部ネットワークの各機器を保護するため、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。

1.4.2.2. 動作環境

本 TOE の構成を『図 2　TOE に関係するハードウェア構成』に示す。



※ 図中の「BOX 読出機能」は、「BOX データ読み出し機能」のことを示す。

図 2　TOE に関係するハードウェア構成

bizhub PRESS 1250 シリーズは、ハードウェア、bizhub PRESS 1250 全体制御ソフトウェアから構成される。bizhub PRESS 1250 全体制御ソフトウェアのコンポーネントは、画像制御プログラムとコントローラ制御プログラムから成る。ハードウェアは、bizhub PRESS 1250 シリーズ本体部分、プリンタコントローラ部分、HDD1 部分、DRAM 部分、HDD2 部分、操作パネル及びネットワークカードである。bizhub PRESS 1250 シリーズ本体部分は、紙文書を電子化するためのスキャナ機能と印刷用の紙に文字や図形を印刷する印刷機能を搭載している。プリンタコントローラは PC からの受信データを印刷用の紙に文字や図形を印刷するためのデータ変換を行っている。USB インタフェース 1 は、TOE の設置生成を行う際に保守用のコンピュータと接続するためのインタフェースであり、このインタフェースからドキュメントデータのアクセスはできない。USB インタフェース 2 は、クライアント PC とローカルに接続してプリントするためのインタフェースである。HDD1 部分に

は記憶装置が存在し、ドキュメントの格納と、一時的なドキュメントの格納を行う。HDD2 部分にも記憶装置が存在しドキュメントの一時的な格納を行う。bizhub PRESS 1250 シリーズ全体制御ソフトウェアのコンポーネントである画像制御プログラムは、OS 上で動作する。コントローラ制御プログラムは、OS 上で動作する。OS は、ハードウェア及び bizhub PRESS 1250 シリーズ全体制御ソフトウェアに対するドキュメントデータの入出力を制御する。画像制御プログラムは、管理機能、CE 機能、利用者機能（**表 1** に記述するように、コピー機能、プリンタ機能、Scan to Email 機能、Scan to FTP 機能、Scan to PC(SMB)機能、HDD 保存機能、HDD 読み出し機能、ドキュメントデータの削除機能を指す。）、および基本機能のスキャナ機能、印刷機能、削除機能、BOX 保存機能、BOX データ読み出し機能、PC データ受信機能を制御する。画像制御プログラムの PC データ受信機能は、コントローラ制御プログラムの PC データ受信機能から画像データを受信する機能である。

コントローラ制御プログラムは、Email 機能、FTP 機能、SMB 機能（◆）、および PC データの受信機能からなる基本機能を制御する。コントローラ制御プログラムの PC データ受信機能は、ネットワークカードを介して画像データを受信して、画像制御プログラムの PC データ受信機能に画像データを送信する。

（◆）SMB 機能は、SMB プロトコル（*）により、画像を送信する機能である。

(*) SMB プロトコル （Server Message Block protocol）

Microsoft 系の OS（DOS、Windows など）で利用できる、ファイル・サービスのためのプロトコル。ファイルの共有サービスやプリンタ共有サービス、コンピュータ名のブラウズ、プロセス間通信、メール・スロット機能などを持つ。

HDD1 部分の記憶装置上には、bizhub PRESS 1250 シリーズ全体制御ソフトウェアの動作にともないユーザ BOX が作成される。ユーザ BOX 内にはサブ BOX が作成される。サブ BOX 内にはドキュメントデータを格納したドキュメントデータファイルが存在する。ユーザ BOX は bizhub PRESS 1250 シリーズ上に複数作成することが出来る。ユーザ BOX 内にはサブ BOX が複数存在可能である。ドキュメントデータファイルはユーザ BOX 内のサブ BOX 内に複数存在可能である。TOE の制御範囲は『**図 2　TOE に関係するハードウェア構成**』のハッチのかかった部分である。

bizhub PRESS 1250 シリーズは、製品関係者による操作パネルからの処理要求及び製品関係者によるネットワーク経由の処理要求を受け付け、TOE はその処理要求を実行する。

1.4.2.3. ガイダンス

[日本版]

- bizhub PRESS 1250 / 1052　ユーザーズガイド　コピー編
- bizhub PRESS 1250 / 1052　ユーザーズガイド　POD管理者編
- bizhub PRESS 1250 / 1052　ユーザーズガイド　セキュリティー編
- bizhub PRESS 1250 / 1052　ユーザーズガイド　ネットワークスキャナー編
- bizhub PRESS 1250 / 1250P / 1052　ユーザーズガイド　プリンター編
- bizhub PRESS 1250P　ユーザーズガイド　本体編
- bizhub PRESS 1250P　ユーザーズガイド　セキュリティー編
- bizhub PRO 951　ユーザーズガイド　コピー編
- bizhub PRO 951　ユーザーズガイド　POD管理者編
- bizhub PRO 951　ユーザーズガイド　セキュリティー編
- bizhub PRO 951　ユーザーズガイド　ネットワークスキャナー編
- bizhub PRO 951　ユーザーズガイド　プリンター編
- bizhub PRESS 1250 / 1052　インストールマニュアル
- bizhub PRESS 1250P　インストールマニュアル
- bizhub PRO 951　インストールマニュアル
- bizhub PRESS 1250 / 1250P / 1052 bizhub PRO 951　サービスマニュアル

[海外版]

- bizhub PRESS 1250 / 1052　User's Guide Copier
- bizhub PRESS 1250 / 1052　User's Guide POD Administrator's Reference
- bizhub PRESS 1250 / 1052　User's Guide Security
- bizhub PRESS 1250 / 1052　User's Guide Network Scanner
- bizhub PRESS 1250 / 1250P / 1052　User's Guide Printer
- bizhub PRESS 1250P　User's Guide Main body
- bizhub PRESS 1250P　User's Guide Security
- bizhub PRO 951　User's Guide Copier
- bizhub PRO 951　User's Guide POD Administrator's Reference
- bizhub PRO 951　User's Guide Security
- bizhub PRO 951　User's Guide Network Scanner
- bizhub PRO 951　User's Guide Printer
- bizhub PRESS 1250 / 1052　INSTALLATION MANUAL
- bizhub PRESS 1250P　INSTALLATION MANUAL
- bizhub PRO 951　INSTALLATION MANUAL
- bizhub PRESS 1250 / 1250P / 1052 bizhub PRO 951　SERVICE MANUAL
- ineo 1250 / 1052　User's Guide Copier
- ineo 1250 / 1052　User's Guide POD Administrator's Reference
- ineo 1250 / 1052　User's Guide Security
- ineo 1250 / 1052　User's Guide Network Scanner
- ineo 1250 / 1052　User's Guide Printer
- ineo 951　User's Guide Copier
- ineo 951　User's Guide POD Administrator's Reference
- ineo 951　User's Guide Security
- ineo 951　User's Guide Network Scanner
- ineo 951　User's Guide Printer
- Press 125ppm / Press 105ppm　INSTALLATION MANUAL
- Pro 95ppm　INSTALLATION MANUAL

1.4.3. TOE の論理的範囲

利用者は、パネルから TOE の各種機能を使用する。以下には、基本機能、管理者が操作する管理者機能、サービスエンジニア（以下、CE と呼称）が操作する CE 機能といった代表的な機能について説明する。

1.4.3.1. 基本機能

『表 1　**利用者機能と基本機能の対応**』に示すとおり、利用者機能は基本機能を実施することで実現する。以降、基本機能について説明する。

表 1　利用者機能と基本機能の対応

No	利用者機能	基本機能
1	コピー機能	スキャナ機能と印刷機能
2	プリンタ機能	PC データ受信機能と印刷機能

3	スキャナサービス機能（Scan to Email 機能、Scan to FTP 機能、Scan to PC(SMB)機能）	スキャナ機能と画像データ送信機能 ※画像データ送信機能は「**図 3**」の FTP 機能、Email 機能、SMB 機能のことを示す。
4	HDD 保存機能	スキャナ機能または PC データ受信機能と BOX 保存機能
5	HDD 読み出し機能	BOX データ読み出し機能と印刷機能
6	ドキュメントデータの削除機能	削除機能

『図 3　基本機能の処理概念』に、表 1 で示した利用者機能と基本機能に関連する処理の流れを示す。

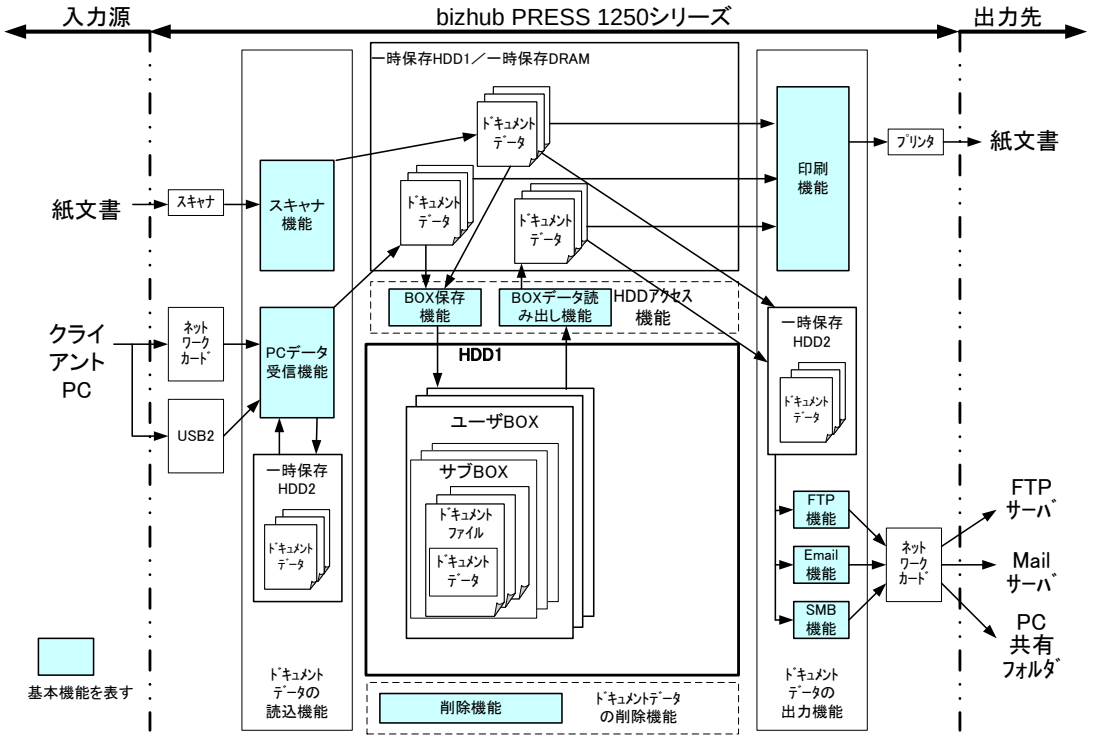


図 3　基本機能の処理概念

『図 3　基本機能の処理概念』に示した機能を以下に述べる。

(1) スキャナ機能

一般利用者により操作パネルから指示された、紙文書の情報をスキャナから取り込みドキュメントデータに変換する機能。変換されたデータは HDD1 または、DRAM に一時保存される。

(2)PC データ受信機能

プリンタコントローラから送られてきたドキュメントデータを一時保存 HDD2 に格納してデータ変換された後に、HDD1、または DRAM に一時保存する機能。

(3)BOX 保存機能

HDD1 に一時保存されたドキュメントデータを、保存する機能。

(4)BOX データ読み出し機能

保存されたドキュメントデータを、HDD1 から読み出す機能。本機能は、ユーザ BOX パスワ

ードで認証された正当なユーザのみに許可される。

(5) 印刷機能
HDD1 または、DRAM に一時保存されたドキュメントデータを印刷する機能。

(6) 画像データ送信機能
スキャナ機能により読み込まれたドキュメントデータを、一時保存 HDD2 に格納して FTP サーバなどに送信する機能。

(7) 削除機能
ユーザ BOX 識別子に関連付けられたユーザ BOX 内のドキュメントデータを削除する機能。

また、以下に TOE が提供するセキュリティ機能を示す。

- 識別認証機能
  TOE はユーザ BOX 識別子、ユーザ BOX パスワードを使ってユーザ BOX の識別認証を行い、識別認証が成功すると、ユーザに対してユーザ BOX パスワードの変更、及び、ユーザ BOX 内の保存ドキュメントデータへのアクセスを許可する。

- アクセス制御機能
  TOE は、ユーザ BOX（保存ドキュメントデータ）へアクセス可能な利用者を制限することができる。アクセス制御機能により、ユーザ BOX パスワードで認証された正当なユーザのみドキュメントデータの読み出しが可能である。

- 監査機能
  TOE は、セキュリティ機能の挙動に関する監査証跡を 1000 件記録することができる。CE・管理者の識別認証に対する失敗/成功、ユーザ BOX の認証に対する成功/失敗、HDD ロックパスワードの変更の成功、セキュリティ強化モードの設定（有効化/停止）の成功、ドキュメントデータの読み出し・印刷、監査ログの読み出し・印刷指示、管理者機能に関する操作が発生した場合に、操作が発生した日時（年月日時分秒）、操作の内容を監査ログとして生成する。

1.4.3.2. 管理者機能

TOE は、認証された管理者だけがパネルから操作することが可能な管理者モードにおいて、セキュリティ強化モード等の各種設定の管理などの機能を提供する。管理者は、管理者機能を使用して、TOE が有する機能の動作設定を行う。管理者機能により、ユーザ BOX パスワードの変更、監査情報の印刷、プリンタ枚数の管理、トラブルシューティング及びトナーの管理など、デジタル複合機の運用に関わる情報を管理する。

以下にはセキュリティに関係する機能について例示する。

- ユーザ BOX の管理
  - ユーザ BOX の登録
  - ユーザ BOX パスワードの登録/変更
- HDD ロック機能の設定
  - HDD ロックパスワード変更

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。

- セキュリティ強化モードの設定
  - 停止

1.4.3.3. CE 機能

TOE は、CE 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機能を提供する。また、CE は公衆回線網に接続したコンピュータから、またはインターネットに接続したコンピュータから、bizhub PRESS 1250 シリーズにアクセスし、ハードウェア保守のため印刷枚数、ジャム回数、トナー切れなどに関する情報の取得を行う（CS Remote Care。以後 CSRC と記述する。「1.4.3.6」参照）。CSRC は、RS232C インタフェースまたは E-Mail インタフェースまたは HTTP インタフェースで行うが、RS232C インタフェース、すなわちモデムとの転送規格は独自通信プロトコルを用いており、E-Mail 及び HTTP には、独自のメッセージ通信プロトコルを用いている。この CSRC は、ドキュメントデータへのインタフェースを持たず、また、セキュリティに関係する機能を実行することもできない。

以下に、セキュリティに関係する代表的な機能を示す。

- 管理者パスワードの登録・変更機能
- CE パスワードの登録・変更機能

以下は、特にセキュリティ機能のふるまいに影響を及ぼす機能の動作設定機能である。

- CE パスワードによる CE の認証の設定
  - 停止を選択

1.4.3.4. その他の機能

TOE は外部エンティティである HDD の HDD ロック機能を有効活用している。以下に代表的な外部エンティティと関係する機能について説明する。

- HDD ロック機能のテスト
  外部エンティティである HDD は、不正な装置接続によるデータ漏洩等への対処機能として、パスワードを設定することにより HDD ロック機能が動作する。TOE は HDD ロック機能を活用し、TOE に接続された HDD（HDD1、2）において HDD ロックパスワードによる認証が成功した場合にのみ起動し、認証が失敗した場合は動作を停止する。

1.4.3.5. セキュリティ強化機能

管理者機能、CE 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。

以下にセキュリティ強化モードが有効化されている場合の一連の設定状態をまとめる。なお、セキュリティ強化モードを有効化するためには、管理者パスワード、CE パスワードを事前にパスワード

規約に違反しない値に設定する等の事前準備が必要である。

- ユーザ識別認証機能 ：有効
- CE 認証機能 ：有効
- パスワード規約機能[2] ：有効
- 監査機能 ：有効
- CSRC 機能（モデム） ：有効
- CSRC 機能（Mail/Http） ：禁止
- USB 経由の TOE 更新機能 ：有効
- ネットワーク管理機能 ：禁止
- インターネット経由 TOE の更新機能 ：禁止
- 不揮発保存機能 ：禁止
- HDD バックアップ/リストア ：禁止
- 設定データ読み込み/保存機能 ：禁止

なお、セキュリティ強化モードが有効の場合、ユーザ BOX 内のドキュメントデータを送信する機能（Email、FTP、SMB）は使用することができない。

1.4.3.6. 用語

本 ST で使用する用語を定義する。

No.	用語	説明
1	ドキュメントデータ	ドキュメントデータは、文字や図形などの情報を電子化したデータである。
2	ユーザ BOX	ユーザ BOX は、ドキュメントデータを格納する個人用のディレクトリである。
3	ユーザ BOX 識別子	ユーザ BOX 識別子は、ユーザ名である。
4	紙文書	紙文書は、文字や図形などの情報を持つ紙媒体の文書である。
5	操作パネル	操作パネルは、bizhub PRESS 1250 シリーズの筐体に付属するタッチパネル式ディスプレイ及び操作ボタンの名称である。
6	内部ネットワーク	内部ネットワークは、bizhub PRESS 1250 シリーズを導入する組織の LAN である。クライアント PC や各種サーバ(例えば Mail サーバや FTP サーバなど)が接続されている。
7	外部ネットワーク	外部ネットワークは、内部ネットワーク(No.6 参照)以外のネットワーク(例えばインターネットなど)である。
8	ＳＭＢ	ＳＭＢとは、Microsoft 系 OS でネットワーク上でコンピュータ同士が通信を行うためのアプリケーションプロトコルである。
9	ユーザ	管理者によりユーザ BOX が TOE に登録され、bizhub PRESS 1250 シリーズの HDD（ハードディスク装置）上にユーザ BOX、

[2] パスワード規約機能が有効である場合は、8 桁未満のユーザパスワード（ユーザ BOX パスワードのこと）の登録/変更が全て拒絶される。

No.	用語	説明
		ドキュメントデータを所有する一般利用者。
10	CSRC	CSRC は、CS Remote Care 機能を実現するアプリケーションである。MFP でトラブルなどが発生した際に、サービス拠点に存在するセンタターミナル PC へ通知するとともに、センタターミナル PC からの要求に応じてカウンタ情報などを通知する。 RS232C インタフェース、E-Mail インタフェース、または HTTP インタフェースで行われるが、セキュリティ強化モードが有効化されている場合は RS232C インタフェース（モデム）経由での利用のみ許可される。
11	ネットワーク管理機能	ネットワーク経由で管理者の識別認証後利用可能となる機能であり、インターネット ISW 機能（インターネットを用いて、外部サーバから、TOE の書き換えを行う機能）、WEB ツール（内部ネットワークを使って、本体の設定情報を取得し、管理者機能を実行する機能）、出力履歴記録機能（本体部分に搭載された NIC 経由で、接続された外部 PC に、出力 JOB 履歴を出力する機能）が存在する。いずれもセキュリティ強化モードが有効化されている場合は使用できない。

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 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 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 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 適合。
- 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、パッケージ：EAL3 に適合する。追加する保証コンポーネントはない。

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 の保護対象となる資産は bizhub PRESS 1250 シリーズのハードディスク（HDD1 および HDD2）に保存されているユーザ BOX 内のドキュメントデータであり、TOE はドキュメントデータの漏洩を防止する。ドキュメントデータは、ユーザのプリント、コピー、スキャンによりハードディスクに保存される。なお、ユーザ BOX を所有しない一般利用者のプリントは、ユーザ BOX には保存されない。

利用者がクライアント PC や紙で所有している MFP 内の HDD 内に保存される以前のドキュメントデータのオリジナルデータについては保護対象外とする。
また、ドキュメントデータに対する処理の過程で DRAM 内に一時的に保存される DRAM 内ドキュメントデータに関しても同様に保護対象外とする。（※DRAM 内に一時的に保存される DRAM 内ドキュメントデータは、外部から DRAM へのアクセスは行えず、電源 OFF と共に DRAM 内一時保存データは消去されるため、データ漏えいの脅威は無い。）

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。

ASM.SECMOD（セキュリティ強化モードの設定条件）
管理者はセキュリティ強化モードを有効化する。

ASM.PLACE（TOE の設置条件）
TOE は、製品関係者のみが利用可能な区画に設置される。

ASM.NET（内部ネットワークの設置条件）
TOE が搭載された bizhub PRESS 1250 シリーズを設置する内部ネットワーク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 bizhub PRESS 1250 シリーズへアクセスできない。

ASM.ADMIN（信頼できる管理者）
管理者は、不正な行為を行わない人物である。

ASM.CE（CE の条件）
CE は、不正な行為を行わない人物である。

ASM.SECRET（秘密情報に関する運用条件）
TOE の利用において、管理者パスワード及び HDD ロックパスワードは、管理者から漏えいしない。又、CE パスワードは CE から漏えいせず、ユーザ BOX パスワードは一般利用者（ユーザ）から漏えいしない。また、各パスワードに対して、推測困難なパスワードが設定される。

ASM.SETTING（セキュリティに関する動作設定条件）

・HDD ロック機能の設定を有効にする。
・CE のログイン認証を有効とする。
・管理者のログイン認証を有効とする。

3.3. 脅威

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

T.ACCESS（ユーザ BOX への不正なアクセス）
一般利用者が、操作パネルから、利用者機能を使うことにより、他の一般利用者の所有するユーザ BOX 内のドキュメントデータを漏洩させる恐れがある。

T.IMPADMIN（CE、管理者へのなりすまし）
一般利用者が、CE 機能インタフェースや管理者機能インタフェースを不正に使用することにより、ユーザ BOX 内のドキュメントデータが漏洩する恐れがある。

3.4. 組織のセキュリティ方針

本節では、TOE の利用及び TOE の利用環境において想定される組織のセキュリティ方針を識別し、説明する。

P.CHECK-HDD（HDD の検証）
TOE は HDD のロックパスワードによって HDD を検証するとともに、HDD のロックパスワードの管理を管理者に制限する。また、TOE は 8～32 桁の半角英大文字、半角英小文字、半角数字のみを HDD ロックパスワードとして受け入れる。

4. セキュリティ対策方針

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

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.IA（利用時の識別と認証）

TOE は、TOE にアクセスを試みる管理者、CE、およびユーザ BOX を所有している一般利用者を識別認証する。一般利用者（ユーザ）は識別認証後に自身のユーザ BOX パスワードを変更できる。

O.ACCESS（ドキュメントデータへのアクセス制限）

TOE は、ユーザ BOX を所有している一般利用者（ユーザ）にのみ、そのユーザ BOX 内のドキュメントデータへの読み出し、印刷を許可する。また、ユーザ BOX を所有している一般利用者及び管理者にのみ、そのユーザ BOX 内のドキュメントデータへの削除を許可する。さらに、ユーザ BOX の登録は管理者のみに許可する。

O.MANAGE（管理機能の提供）

TOE は、管理者だけに以下に示す機能の操作を許可する。

・セキュリティ強化モードの設定に関係する機能

・HDD ロックパスワードの変更

TOE は、管理者、ユーザ BOX を所有している一般利用者（自身のユーザ BOX パスワードのみ）だけに以下に示す機能の操作を許可する。

・ユーザ BOX パスワードの変更機能

TOE は、CE だけに以下に示す機能の操作を許可する。

・CE パスワードの登録・変更機能

・管理者パスワードの登録機能

TOE は、管理者、CE に以下に示す機能の操作を許可する。

・管理者パスワードの変更機能

TOE は、8～32 桁の半角英大文字、半角英小文字、半角数字のみを HDD ロックパスワードとして受け入れる。

O.AUDIT（監査情報の記録）

TOE は、TOE に保護対象資産へのアクセス事象及びそれに関連する事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果を記録する。また、監査情報の参照を管理者に制限する。さらに、TOE は監査記録を出力する領域が既定の容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。

O.CHECK-HDD（HDD の検証）

TOE は、HDD（HDD1 および HDD2）に対する HDD ロックパスワードによる認証が失敗した場合、MFP 本体の動作を停止する。

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を説明する。

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（CE の保証）

・MFP を保守管理する組織の責任者は、TOE の設置、セットアップ及び TOE が搭載される MFP の保守において課せられた役割を忠実に実行するように CE を教育する。
・管理者は、CE による TOE が搭載される MFP のメンテナンス作業に立会う。

OE.PLACE（設置場所の管理）

管理者は製品関係者のみが操作可能な区画に TOE を設置する。

OE.SECOND（セキュリティ強化モードの設定）

管理者は、セキュリティ強化モードを有効化する。

OE.NET（ネットワークの管理）

管理者は、外部ネットワークから TOE が搭載される MFP へのアクセスを遮断するため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.EQUIPMENT（MFP の管理）

管理者は MFP をセキュアな場所に設置し、MFP 及び HDD 等の部品が盗難されないように、及び MFP の内部を解析するような特殊装置などが接続されないように管理する。

OE.SESSION（操作後のセッションの終了）

管理者は、ユーザに対して以下に示す運用を実施させる。
・ユーザ BOX 内のドキュメントデータに対する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。
・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。
CE は、以下に示す運用を実施する。
・サービスモードの諸機能を操作終了後にログアウト操作を行う。

OE.SECRET（秘密情報の適切な管理）

管理者は、以下に示す運用を実施する。
・管理者は、ユーザがユーザ BOX パスワードを他者に漏らさないように教育する。
・管理者パスワード、HDD ロックパスワードを秘匿する。
・管理者パスワード、HDD ロックパスワードの適宜変更を行う。
・管理者は、管理者パスワード、HDD ロックパスワードに推測困難なパスワードを設定する。
CE は以下に示す運用を実施する。
・CE パスワードを秘匿する。
・CE パスワードの適宜変更を行う。
・CE が管理者パスワードを変更した場合は、管理者に速やかに変更させる。
・CE は、CE パスワードに推測困難なパスワードを設定する。

ユーザは以下に示す運用を実施する。

・ユーザは、ユーザ BOX パスワードに推測困難なパスワードを設定する。

OE.SETTING-SECURITY（セキュリティに関する動作設定）

・管理者は、（HDD 1 および HDD2 に対する）HDD ロック機能を「有効」にする。

・管理者は、CE により CE 認証機能を「有効」にさせる。

・管理者は、CE により管理者認証機能を「有効」にさせる。

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 2　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

組織のセキュリティ方針 / 前提 / 脅威 / セキュリティ対策方針	ASM.SECMOD	ASM.PLACE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.SECRET	ASM.SETTING	T.ACCESS	T.IMPADMIN	P.CHECK-HDD
O.IA								●	●	●
O.ACCESS								●		
O.MANAGE								●	●	●
O.AUDIT								●	●	●
O.CHECK-HDD										●
OE.ADMIN				●						
OE.SERVICE					●					
OE.PLACE		●								
OE.SECOND	●									
OE.NET			●							
OE.EQUIPMENT										●
OE.SESSION								●	●	
OE.SECRET						●				
OE.SETTING-SECURITY							●			

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。

- **ASM.SECMOD（セキュリティ強化モードの設定条件）**

  本条件は、管理者がセキュリティ強化モードを有効化することを想定している。
  OE.SECOND は、管理者がセキュリティ強化モードを有効化した上で利用することを規定しており、本条件は実現される。

- **ASM.PLACE（TOE の設置条件）**

  TOE は OE.PLACE によって、製品関係者のみが操作可能な区画に設置される。よって、TOE へのアクセスは製品関係者のみに制限出来る。
  以上に示すように、前提条件 ASM.PLACE は対策方針 OE.PLACE によって実現できる。

- **ASM.NET（内部ネットワークの設置条件）**

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.NET 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、本条件は実現される。

- **ASM.ADMIN（信頼できる管理者）**

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 を利用する組織において信頼のおける人物を管理者に指定するため、管理者の信頼性が実現される。

- **ASM.CE（CE の条件）**

本条件は、CE が悪意を持たないことを想定している。
OE.SERVICE は、MFP を保守管理する組織において CE を教育する。また管理者は、CE の行うメンテナンス作業に立ち会うことが規定されているため、CE の信頼性は確保される。

- **ASM.SECRET（秘密情報に関する運用条件）**

本条件は、TOE の利用において使用される各パスワードが各利用者より漏洩しないこと、及び各パスワードに対して推測困難なパスワードを設定することを想定している。
OE.SECRETは、管理者がユーザに対してユーザBOXパスワードに関する運用規則を実施させることを規定し、管理者が管理者パスワード、HDD ロックパスワードに関する運用規則を実施することを規定している。また、CE が CE パスワードに関する運用規則を実施し、管理者に対して、管理者パスワードに関する運用規則を実施させることを規定しており、本条件は実現される。
また、管理者が管理者パスワード、HDD ロックパスワードを、CE が CE パスワードを、ユーザがユーザ BOX パスワードを推測困難なパスワードの設定を実施することを規定しており、本条件は実現される。

- **ASM.SETTING（セキュリティに関する動作設定条件）**

本条件は、セキュリティに関する動作設定条件を満たす以下の設定が TOE に対して行われていることを想定している。
・管理者による HDD ロック機能の有効化。
・CE 認証機能の有効化。
・管理者認証機能の有効化。

OE.SETTING-SECURITY は、上記全ての項目に対して上記の通りの設定を実施することを規定しており、本条件は実現される。

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.ACCESS：ユーザ BOX への不正なアクセス**

本脅威は、一般利用者が利用者機能を利用することにより、他の一般利用者のユーザ BOX 内のドキュメントデータが漏洩する可能性を想定している。
O.MANAGE により TSF は、O.IA により識別認証された正当な管理者に対してのみ、ユーザ BOX を登録する機能、ユーザ BOX パスワードを変更する機能の使用を許可し、管理者はこの機

能を使ってドキュメントデータを利用可能な一般利用者を決定する。また、セキュリティ強化モードの設定を管理者のみに制限することにより、運用時はセキュリティ強化モードが常に有効な状態が保持され、パスワード規約機能が有効化されることにより、ユーザ BOX のパスワード強度が保証される。TSF は O.IA で識別認証した正当な一般利用者（ユーザ）にのみそのユーザ BOX 内のドキュメントデータの読み出し、印刷を、O.ACCESS により許可する。また、TSF は O.IA で識別認証した正当な一般利用者（ユーザ）、及び管理者にのみそのユーザ BOX 内のドキュメントデータの削除を、O.ACCESS により許可する。

また、TOE は、O.AUDIT により『保護対象となる資産』であるユーザ BOX 内のドキュメントデータへの利用者機能に関する操作を監査情報として記録するため、ドキュメントデータへの不当な操作の検出を可能にする。

さらに、OE.SESSION により CE・管理者の操作終了後は必ずログアウトが実施されること、及びユーザのユーザ BOX の操作終了後は必ずログアウトが実施されることから、MFP 操作者以外の他者が認証状態の MFP を操作することはない。

従って、脅威 T.ACCESS は対策方針 O.IA、O.ACCESS、O.MANAGE、O.AUDIT、及び OE.SESSION により十分対抗されている。

- **T.IMPADMIN：CE、管理者へのなりすまし**

本脅威は、一般利用者が CE・管理者になりすましてドキュメントデータを漏洩させる可能性を想定している。

TSF は CE を O.IA で識別認証する。また、O.MANAGE により識別認証された CE は MFP を管理する組織の責任者により選定された管理者を TOE に登録し、識別認証された管理者に対してのみ、管理機能を使用可能状態にする。

また、TSF は、O.AUDIT により、CE、管理者の識別・認証の失敗、CE、管理者のパスワードの登録/変更を監査情報として記録するため、CE・管理者へのなりすまし操作が行われたことを検出可能にする。

さらに、OE.SESSION により CE・管理者の操作終了後は必ずログアウトが実施されることから、MFP 操作者以外の他者が認証状態の MFP を操作することはない。

従って、脅威 T.IMPADMIN は対策方針 O.IA、O.MANAGE、O.AUDIT、及び OE.SESSION により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を実施するセキュリティ対策方針について以下に説明する。

- **P.CHECK-HDD：HDD の検証**

TSF は O.IA で識別認証された正当な管理者により、O.MANAGE の管理機能で HDD1 および HDD2 の HDD ロックパスワードを変更し管理する。また、O.MANAGE により HDD ロックパスワードは 8～32 桁の半角英大文字、半角英小文字、半角数字のみが受け入れられる。

セキュリティ強化モードの設定を管理者のみに制限することにより、運用時はセキュリティ強化モードが常に有効な状態が保持され、HDD ロック機能が有効化される。また、TSF は、O.AUDIT により、管理者の識別・認証の失敗、セキュリティ強化モードの設定の成功、HDD ロックパスワードの変更の成功を監査情報として記録するため、管理者以外が HDD ロック機能に関わる設定を変更しようと試みたことを検出可能にする。また、O.CHECK-HDD によって HDD1 および HDD2 に対する HDD ロックパスワードによる認証が失敗した場合、MFP 本体の動作を停止する。

OE.EQUIPMENT は、管理者により MFP をセキュアな場所に設置すること、MFP や HDD 等の部品が盗難されないように管理すること、及び MFP の内部を解析するような特殊装置などが接続されないように管理することを示している。

従って、組織のセキュリティ方針 P.CHECK-HDD は対策方針 O.IA、O.MANAGE、O.AUDIT、O.CHECK-HDD、及び OE.EQUIPMENT により達成されている。

5. 拡張コンポーネント定義

本 ST では拡張機能コンポーネントを定義しない。

6. IT セキュリティ要件

本章では、TOE 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。

＜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す。また本 ST にて適用する必要性のない依存性である場合は、同括弧内にて“適用しない”と記述している。

6.1. TOE セキュリティ要件

6.1.1. TOE セキュリティ機能要件

6.1.1.1. 監査

FAU_GEN.1	**監査データ生成**
FAU_GEN.1.1	
TSF は、以下の監査対象事象の監査記録を生成できなければならない： a) 監査機能の起動と終了; b) 監査の[選択：最小、基本、詳細、指定なし：から一つのみ選択]レベルのすべての監査対象事象;及び c) [割付：上記以外の個別に定義した監査対象事象]。	
[選択：最小、基本、詳細、指定なし：から一つのみ選択] ***指定なし***	
[割付：上記以外の個別に定義した監査対象事象] ***以下の監査対象事象*** ***・CE の識別認証時における、識別認証の成功/不成功*** ***・管理者の識別認証時における、識別認証の成功不成功*** ***・ユーザ BOX を所有している一般利用者の識別認証時における、識別認証の成功不成功*** ***・セキュリティ強化モードの設定の成功*** ***・監査ログの印刷指示の成功*** ***・CE パスワードの変更/登録の成功*** ***・CE による管理者パスワードの変更/登録の成功*** ***・管理者による管理者パスワードの変更の成功*** ***・管理者によるユーザ BOX 登録、及びユーザ BOX パスワードの変更/登録の成功*** ***・一般利用者（ユーザ）によるユーザ BOX パスワードの変更の成功*** ***・HDD ロックパスワードの変更の成功*** ***・ユーザ BOX 内のドキュメントデータの読み出し、印刷、削除の成功***	

FAU_GEN.1.2
TSF は、各監査記録において少なくとも以下の情報を記録しなければならない。 a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗); 及び b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報]
[割付: その他の監査関連情報] *なし*
下位階層 : なし
依存性 : FPT_STM.1

表 3 監査対象となる事象

機能要件	CC で定義された監査対象	監査対象事象
FAU_GEN.1	予見される監査対象事象はない。	なし
FAU_STG.1	予見される監査対象事象はない。	なし
FAU_STG.4	基本: 監査格納失敗によってとられるアクション	なし（監査格納失敗時、TOE は停止するため）
FAU_SAR.1	基本: 監査記録からの情報の読み出し。	監査ログの印刷の成功
FAU_SAR.2	基本 :監査記録からの成功しなかった情報読み出し。	なし（管理者のみ利用可能な管理者モードからのみ監査記録へのアクセスが可能なため）
FDP_ACC.1[1]	予見される監査対象事象はない。	なし
FDP_ACC.1[2]	予見される監査対象事象はない。	なし
FDP_ACF.1[1]	最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	ドキュメントデータの読み出し、印刷、削除の成功
FDP_ACF.1[2]	最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	ユーザ BOX の登録の成功
FIA_AFL.1	最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	管理者、CE、ユーザ BOX の認証の不成功が閾値へ到達
FIA_ATD.1	予見される監査対象事象はない。	なし
FIA_SOS.1[1]	最小: TSF による、テストされた秘密の拒否 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。	CE パスワードの登録/変更の成功
FIA_SOS.1[2]	最小: TSF による、テストされた秘密の拒否 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。	管理者パスワードの登録/変更の成功
FIA_SOS.1[3]	最小: TSF による、テストされた秘密の拒否 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。	ユーザ BOX パスワードの登録/変更の成功

機能要件	CC で定義された監査対象	監査対象事象
FIA_SOS.1[4]	最小: TSF による、テストされた秘密の拒否 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。	HDD ロックパスワードの変更の成功
FIA_UAU.2[1]	最小: 認証メカニズムの不成功になった使用 基本: 認証メカニズムのすべての使用。	CE の認証時における、認証の成功及び認証の不成功
FIA_UAU.2[2]	最小: 認証メカニズムの不成功になった使用 基本: 認証メカニズムのすべての使用。	管理者の認証時における、認証の成功及び認証の不成功
FIA_UAU.2[3]	最小: 認証メカニズムの不成功になった使用 基本: 認証メカニズムのすべての使用。	ユーザ BOX の認証時における、認証の成功及び認証の不成功
FIA_UAU.7	予見される監査対象事象はない。	なし
FIA_UID.2[1]	最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	CE の識別時における、識別の成功及び識別の不成功
FIA_UID.2[2]	最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	管理者の識別時における、識別の成功及び識別の不成功
FIA_UID.2[3]	最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	ユーザ BOX の識別時における、識別の成功及び識別の不成功
FIA_USB.1	最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)。	サブジェクトの生成の成功
FMT_MOF.1	基本: TSF の機能のふるまいにおけるすべての改変。	セキュリティ強化モードの停止の成功
FMT_MSA.1	基本: セキュリティ属性の値の改変すべて。	なし（セキュリティ属性の値は常に固定であり、改変できないため）
FMT_MSA.3	基本: 許可的あるいは制限的規則のデフォルト設定の改変。 基本: セキュリティ属性の初期値の改変すべて。	なし（セキュリティ属性の初期値は常に固定であり、改変できないため）
FMT_MTD.1[1]	基本: TSF データの値のすべての改変。	管理者によるユーザ BOX パスワードの登録の成功
FMT_MTD.1[2]	基本: TSF データの値のすべての改変。	管理者によるユーザ BOX パスワードの変更の成功 一般利用者（ユーザ）によるユーザ BOX パスワードの変更の成功
FMT_MTD.1[3]	基本: TSF データの値のすべての改変。	管理者パスワードの変更の成功
FMT_MTD.1[4]	基本: TSF データの値のすべての改変。	CE パスワードの変更の成功
FMT_MTD.1[5]	基本: TSF データの値のすべての改変。	管理者パスワードの登録の成功 CE パスワードの登録の成功
FMT_MTD.1[6]	基本: TSF データの値のすべての改変。	HDD ロックパスワードの変更の成功

機能要件	CC で定義された監査対象	監査対象事象
FMT_SMF.1	最小: 管理機能の使用	セキュリティ強化モードの設定の成功 管理者によるユーザ BOX パスワードの登録/変更の成功 管理者による HDD ロックパスワードの変更の成功 一般利用者（ユーザ）による一般利用者自身のユーザ BOX パスワードの変更の成功 CE による CE パスワードの登録/変更の成功 CE による管理者パスワードの登録/変更の成功
FMT_SMR.1[1]	最小: 役割の一部をなす利用者のグループに対する改変 詳細: 役割の権限の使用すべて。	なし（CE の役割は固定されているため）
FMT_SMR.1[2]	最小: 役割の一部をなす利用者のグループに対する改変 詳細: 役割の権限の使用すべて。	なし（管理者の役割は固定されているため）
FMT_SMR.1[3]	最小: 役割の一部をなす利用者のグループに対する改変 詳細: 役割の権限の使用すべて。	なし（ユーザの役割は固定されているため）
FPT_STM.1	最小: 時間の変更; 詳細: タイムスタンプの提供。	なし(時刻の設定は管理者しか設定できないため不要)
FPT_TEE.1	基本：外部エンティティのテストの実行とテスト結果	なし（HDD ロックパスワード認証が不成功の場合は TOE が起動しないため）

FAU_STG.1　　保護された監査証跡格納
FAU_STG.1.1
TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。
FAU_STG.1.2
TSF は、監査証跡に格納された監査記録への不正な改変を[選択： 防止、検出：から一つのみ選択]できなければならない。
[選択： 防止、検出：から一つのみ選択] *防止*
下位階層　：　なし
依存性　：　FAU_GEN.1

FAU_STG.4　　監査データ損失の防止
FAU_STG.4.1
TSF は、監査証跡が満杯になった場合、[選択： 監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き：から一つのみ選択]及び[割付： 監査格納失敗時にとられるその他のアクション]を行わなければならない。
[選択： 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き：から一つのみ選択] *最も古くに格納された監査記録への上書き*
[割付： 監査格納失敗時にとられるその他のアクション] *なし*
下位階層　：　FAU_STG.3
依存性　：　FAU_STG.1

FAU_SAR.1　　監査レビュー
FAU_SAR.1.1
TSF は、[割付：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。
[割付：許可利用者] ***管理者***
[割付：監査情報のリスト] ***FAU_GEN.1 で規定する『表 3　監査対象となる事象』に示す監査情報***
FAU_SAR.1.2
TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。
下位階層　：　なし
依存性　：　FAU_GEN.1

FAU_SAR.2　　限定監査レビュー
FAU_SAR.2.1
TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。
下位階層　：　なし
依存性　：　FAU_SAR.1

6.1.1.2. 利用者データ保護

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

表 4　ドキュメント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
利用者を代行するタスク	*ドキュメントデータ*	*・ドキュメントデータの読み出し、印刷、削除*

FDP_ACC.1[2]　　サブセットアクセス制御
FDP_ACC.1.1[2]
TSF は、[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]: 「***表 5　ユーザ BOX 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 BOX アクセス制御***
下位階層　:　なし 依存性　:　FDP_ACF.1（FDP_ACF.1[2]）

表 5　ユーザ BOX アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*ユーザ BOX*	*・ユーザ BOX の登録*

FDP_ACF.1[1]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[1]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞*** ***・利用者を代行するタスク*** ***＜サブジェクト属性＞*** ***・ユーザ BOX を所有している一般利用者のユーザ BOX 識別子、管理者*** --- ***＜オブジェクト＞*** ***・ドキュメントデータ*** ***＜オブジェクト属性＞*** ***・ユーザ BOX 識別子***
[割付: *アクセス制御 SFP*]: ***ドキュメント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*]: ***＜ドキュメントデータに対する操作制御＞*** ***・利用者を代行するタスクは、サブジェクト属性のユーザ BOX 識別子（ユーザ名）と一致するドキュメントデータのユーザ BOX 識別子を持つドキュメントデータに対して読み出し、印刷を許可される。*** ***・利用者を代行するタスクは、サブジェクト属性が管理者、もしくはサブジェクト属性のユーザ BOX 識別子（ユーザ名）と一致するドキュメントデータのユーザ BOX 識別子を持つドキュメントデータに対して削除を許可される。***
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*]: ***なし***
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***
下位階層　:　なし 依存性　:　FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3(**適用しない**)

FDP_ACF.1[2]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[2]
TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。
[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]: ***＜サブジェクト＞*** ***・利用者を代行するタスク*** ***＜サブジェクト属性＞*** ***・管理者が登録しようとしているユーザ BOX のユーザ BOX 識別子*** --- ***＜オブジェクト＞*** ***・ユーザ BOX*** ***＜オブジェクト属性＞*** ***・ユーザ BOX 識別子***
[割付: *アクセス制御 SFP*]: ***ユーザ BOX 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*]: ***＜ユーザ BOX に対する操作制御＞*** ***利用者を代行するタスクは、サブジェクト属性のユーザ BOX 識別子が登録されていない場合、そのユーザ BOX 識別子に関連づけられたユーザ BOX の登録を許可される。***
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*]: ***なし***
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***
下位階層　：　なし **依存性**　：　FDP_ACC.1（FDP_ACC.1[2]）、FMT_MSA.3

6.1.1.3. 識別と認証

FIA_AFL.1　　認証失敗時の取り扱い
FIA_AFL.1.1
TSF は、[割付: *認証事象のリスト*]に関して、[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。
[割付: *認証事象のリスト*]: ***管理者、CE 及びユーザ BOX を所有している一般利用者に対する不成功認証***
[選択: *[割付:正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]: ***[割付: 正の整数値]: 1***

FIA_AFL.1.2
不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。
[選択: *に達する、を上回った*]: ***に達する***
[割付: *アクションのリスト*]: ***認証不成功となった管理者、CE 又はユーザ BOX を所有している一般利用者に対して、次の認証試行を 5 秒間実行しない。***
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_ATD.1　利用者属性定義
FIA_ATD.1.1
TSF は、個々の利用者に属する以下のセキュリティ属性のリスト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（ユーザ BOX 識別子、管理者）***
下位階層　:　なし
依存性　:　なし

FIA_SOS.1[1]　秘密の検証
FIA_SOS.1.1[1]
TSF は、秘密 ***（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　：半角英大文字、半角英小文字、半角数字*** ***・規則　：一世代前のパスワードと同一のパスワードを禁止***
下位階層　:　なし
依存性　:　なし

FIA_SOS.1[2]　秘密の検証
FIA_SOS.1.1[2]
TSF は、秘密 ***（管理者パスワード）*** が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。
[割付: *定義された品質尺度*]: ***・桁数　：8 桁*** ***・文字種　：半角英大文字、半角英小文字、半角数字、記号『-^¥@[]:;,./＼!"#$%&'()=~|`{+*}<>?_』*** ***・規則　：一世代前のパスワードと同一のパスワードを禁止***
下位階層　:　なし
依存性　:　なし

FIA_SOS.1[3]　秘密の検証
FIA_SOS.1.1[3]
TSF は、秘密 ***（ユーザ BOX 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～64桁 ・文字種　：半角英大文字、半角英小文字、半角数字 ・規則　：一世代前のパスワードと同一のパスワードを禁止
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[4]　秘密の検証
FIA_SOS.1.1[4]
TSF は、秘密（***HDD ロックパスワード***）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　：8～32 桁 ・文字種：半角英大文字、半角英小文字、半角数字 ・規則　：無し。
下位階層　：　なし
依存性　：　なし

FIA_UAU.2[1]　アクション前の利用者認証
FIA_UAU.2.1[1]
TSF は、その利用者（***CE***）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（***CE***）に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[1]）

FIA_UAU.2[2]　アクション前の利用者認証
FIA_UAU.2.1[2]
TSF は、その利用者（***管理者***）を代行する他の TSF 仲介アクションを許可する前に、各利用者（***管理者***）に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
FIA_UAU.2.1[3]
TSF は、その利用者（***ユーザ BOX を所有している一般利用者***）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（***ユーザ BOX を所有している一般利用者***）に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[3]）

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

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

FIA_UID.2[1]　　アクション前の利用者識別

FIA_UID.2.1[1]

TSF は、その利用者 ***（CE）*** 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 ***（CE）*** に識別が成功することを要求しなければならない。

下位階層	:	FIA_UID.1
依存性	:	なし

FIA_UID.2[2]　　アクション前の利用者識別

FIA_UID.2.1[2]

TSF は、その利用者 ***（管理者）*** を代行する他の TSF 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。

下位階層	:	FIA_UID.1
依存性	:	なし

FIA_UID.2[3]　　アクション前の利用者識別

FIA_UID.2.1[3]

TSF は、その利用者 ***（ユーザ BOX を所有している一般利用者）*** 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 ***（ユーザ BOX を所有している一般利用者）*** に識別が成功することを要求しなければならない。

下位階層	:	FIA_UID.1
依存性	:	なし

FIA_USB.1　　利用者・サブジェクト結合

FIA_USB.1.1

TSF は、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（ユーザ BOX 識別子、管理者）

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*] :

・ユーザ BOX の所有者として認証された際に、利用者を代行するタスクのタスク属性に当該ユーザのユーザ BOX 識別子を関連付ける。

・管理者として認証された際に、利用者を代行するタスクのタスク属性に管理者の属性を関連付ける。

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

下位階層	:	なし
依存性	:	FIA_ATD.1

6.1.1.4. セキュリティ管理

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

FMT_MSA.1　　セキュリティ属性の管理
FMT_MSA.1.1
TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]*] をする能力を[割付: *許可された識別された役割*]に制限するために[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[割付：セキュリティ属性のリスト] ***ユーザ BOX 識別子***
[選択： デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]] ***[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***
[割付：アクセス制御 SFP 、情報フロー制御 SFP] ***ユーザ BOX アクセス制御***
下位階層　:　なし
依存性　:　[FDP_ACC.1、またはFDP_IFC.1]（FDP_ACC.1[2]）、FMT_SMR.1（FMT_SMR.1[2]）、FMT_SMF.1

FMT_MSA.3　　静的属性初期化
FMT_MSA.3.1
TSF は、その SFP を実施するために使われるセキュリティ属性 ***（ユーザ BOX 識別子）*** 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] ***制限的***
[割付：アクセス制御 SFP 、情報フロー制御 SFP] ***ユーザ BOX アクセス制御***
FMT_MSA.3.2
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。
[割付：許可された識別された役割] ***なし***
下位階層　:　なし
依存性　:　FMT_MSA.1、FMT_SMR.1（適用しない）

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

FMT_MTD.1[2]　　TSF データの管理
FMT_MTD.1.1[2]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***ユーザ BOX 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 BOX を所有している一般利用者*** ***・管理者***
下位階層　:　なし
依存性　:　FMT_SMF.1、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

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

FMT_MTD.1[4]　　TSF データの管理
FMT_MTD.1.1[4]
TSF は、[割付: *TSF データのリスト*]を[選択: *デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*]する能力を[割付:*許可された識別された役割*]に制限しなければならない。
[割付: *TSF データのリスト*]: ***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*]: ***CE***
下位階層　:　なし
依存性　:　FMT_SMF.1、FMT_SMR.1（FMT_SMR.1[1]）

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

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

FMT_SMF.1　管理機能の特定
FMT_SMF.1.1
TSF は、以下の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*]: ***・管理者によるセキュリティ強化モードの停止機能*** ***・管理者によるユーザ BOX パスワードの登録機能*** ***・管理者によるユーザ BOX パスワードの改変機能*** ***・管理者による HDD ロックパスワードの改変機能*** ***・ユーザ BOX を所有している一般利用者によるユーザ BOX パスワードの改変機能*** ***・管理者による管理者パスワードの改変機能*** ***・CE による CE パスワードの登録機能*** ***・CE による CE パスワードの改変機能*** ***・CE による管理者パスワードの登録機能*** ***・CE による管理者パスワードの改変機能***
下位階層　:　なし
依存性　:　なし

FMT_SMR.1[1]　　セキュリティの役割
FMT_SMR.1.1[1]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]: ***CE***
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。
下位階層　　:　なし
依存性　　:　FIA_UID.1（FIA_UID.2[1]）

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

FMT_SMR.1[3]　　セキュリティの役割
FMT_SMR.1.1[3]
TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付: *許可された識別された役割*]: ***ユーザ BOX を所有している一般利用者***
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。
下位階層　　:　なし
依存性　　:　FIA_UID.1（FIA_UID.2[3]）

6.1.1.5. TSF の保護

FPT_STM.1　　高信頼タイムスタンプ
FPT_STM.1.1
TSF は、高信頼タイムスタンプを提供できなければならない。
下位階層　　:　なし
依存性　　:　なし

FPT_TEE.1　　外部エンティティのテスト
FPT_TEE.1.1
TSFは、[割付：外部エンティティの特性のリスト]の達成をチェックするために、 [選択：初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、[割付:その他の条件]]時に、テストスイートを実行しなけ

ればならない。
[割付：外部エンティティの特性のリスト] ***TOE に接続された外部エンティティ（HDD）において、HDD ロックパスワードによる認証が成功すること***
[選択：初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、[割付:その他の条件]] ***初期立ち上げ中***
FPT_TEE.1.2
テストに失敗した場合、TSF は[割付：アクション]をとらなければならない。
[割付：アクション] ***MFP 本体の動作を停止する***
下位階層 : なし
依存性 : なし

6.1.2. TOE のセキュリティ保証要件

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

表 6　TOE のセキュリティ保証要件

TOEセキュリティ保証要件		コンポーネント
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

6.2. IT セキュリティ要件根拠

6.2.1. IT セキュリティ機能要件根拠

6.2.1.1. 必要性

セキュリティ対策方針と IT セキュリティ機能要件の対応関係を下表に示す。IT セキュリティ機能要件が少なくとも 1 つ以上のセキュリティ対策方針に対応していることを示している。

表 7　セキュリティ対策方針に対する IT セキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.IA	O.ACCESS	O.MANAGE	O.AUDIT	O.CHECK-HDD
FAU_GEN.1				●	
FAU_STG.1				●	
FAU_STG.4				●	
FAU_SAR.1				●	
FAU_SAR.2				●	
FDP_ACC.1[1]		●			
FDP_ACC.1[2]		●			
FDP_ACF.1[1]		●			
FDP_ACF.1[2]		●			
FIA_AFL.1	●				
FIA_ATD.1		●			
FIA_SOS.1[1]			●		
FIA_SOS.1[2]			●		
FIA_SOS.1[3]	●		●		
FIA_SOS.1[4]			●		
FIA_UAU.2[1]	●				
FIA_UAU.2[2]	●				
FIA_UAU.2[3]	●				
FIA_UAU.7	●				
FIA_UID.2[1]	●				
FIA_UID.2[2]	●				
FIA_UID.2[3]	●				
FIA_USB.1		●			
FMT_MOF.1	●	●	●	●	
FMT_MSA.1		●			
FMT_MSA.3		●			
FMT_MTD.1[1]			●		
FMT_MTD.1[2]	●		●		
FMT_MTD.1[3]			●		
FMT_MTD.1[4]			●		
FMT_MTD.1[5]			●		
FMT_MTD.1[6]			●		
FMT_SMF.1	●	●	●		
FMT_SMR.1[1]			●		
FMT_SMR.1[2]			●		
FMT_SMR.1[3]	●	●			
FPT_STM.1				●	
FPT_TEE.1					●

6.2.1.2. 十分性

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

- **O.IA（利用時の識別と認証）**

  本セキュリティ対策方針は、ユーザ BOX を所有している一般利用者、CE、管理者に対する識別及び認証する機能を要求しており、識別認証に関係する諸要件が必要である。

CE であることを FIA_UID.2[1]で識別し、CE 本人であることを FIA_UAU.2[1]で認証することで、正当な CE の操作であることが確認できる。管理者であることを FIA_UID.2[2]で識別し、管理者本人であることを FIA_UAU.2[2]で認証することで、正当な管理者の操作であることが確認できる。さらに、ユーザ BOX を所有している一般利用者であることを FIA_UID.2[3]で識別し、ユーザ BOX を所有している一般利用者本人であることを FIA_UAU.2[3]で認証することで、正当なユーザ BOX を所有している一般利用者の操作であることが確認できる。

管理者、CE、及びユーザ BOX を所有している一般利用者の認証が不成功となった場合、FIA_AFL.1 により管理者、CE、及びユーザ BOX を所有している一般利用者に対して次の認証の試行を 5 秒間待たせ、不正な利用者が CE、管理者、及びユーザ BOX を所有している一般利用者として識別認証成功するまでの時間を長くする。また、パスワードを秘匿するため、FIA_UAU.7 によりパスワード入力域に入力した字数分のダミー文字(*)を表示する。

識別認証したユーザ BOX を所有する一般利用者に対し、ユーザ BOX パスワードの変更を FMT_MTD.1[2]で許可する。パスワードが変更されることで、不正な利用者から入力したユーザ BOX パスワードが一致する可能性を低くする。

ユーザ BOX パスワードを変更する際、ユーザ BOX パスワードは FIA_SOS.1[3]で指定されたパスワード規則に従っているか検証されている。パスワードの管理を FMT_SMF.1 で特定する。対象のユーザを FMT_SMR.1[3]で維持する。以上の機能は、FMT_MOF.1 により有効に動作する。

従って、対応するセキュリティ機能要件（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.7、FIA_UID.2[1]、FIA_UID.2[2]、FIA_UID.2[3]、FIA_AFL.1、FMT_MTD.1[2]、FIA_SOS.1[3]、FMT_SMF.1、FMT_SMR.1[3]、FMT_MOF.1）により対策方針 O.IA は実現可能である。

- **O.ACCESS（ドキュメントデータへのアクセス制限）**

本セキュリティ対策方針は、ドキュメントデータに対するアクセスを、当該ドキュメントデータを所有するユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

FDP_ACC.1[2]、FDP_ACF.1[2]、FMT_MSA.3、及び FMT_MSA.1 により管理者がユーザ BOX 識別子を登録することでユーザ BOX が作成される。また、FIA_ATD.1、FIA_USB.1 により利用者を代行するタスクのタスク属性にユーザ BOX 識別子、または管理者が関連づけられると、FDP_ACC.1[1]と FDP_ACF.1[1]を使ってユーザ BOX 内のドキュメントデータへのアクセス制御を実現する。さらに、O.ACCESS はドキュメントデータを所有する正当なユーザが所有するドキュメントデータの読み出し操作を行う機能を許可することにより、ドキュメントデータを所有する正当なユーザのみがドキュメントデータを参照可能となる。O.ACCESS はドキュメントデータを所有する正当なユーザが所有するドキュメントデータの削除操作を行う機能を許可する、または管理者にドキュメントデータの削除操作を行う機能を許可することにより、ドキュメントデータを所有する正当なユーザ、または管理者のみがドキュメントデータを削除可能となる。

また、ユーザ BOX を所有している一般利用者は FMT_SMR.1[3]により維持され、ユーザ BOX パスワードの管理を FMT_SMF.1 で特定する。以上の機能は、FMT_MOF.1 により有効に動作する。

従って、対応するセキュリティ機能要件（FIA_ATD.1、FIA_USB.1、FDP_ACC.1[1]、FDP_ACC.1[2]、FDP_ACF.1[1]、FDP_ACF.1[2]、FMT_MSA.3、FMT_MSA.1、FMT_SMR.1[3]、FMT_SMF.1、FMT_MOF.1）により O.ACCESS は実現可能である。

- **O.MANAGE（管理機能の提供）**

本セキュリティ対策方針は、セキュリティ強化モードの設定に関係する機能等を管理者に制限

しており、一連の設定機能や管理機能に対してアクセスを制限するための諸要件が必要である。

CE は管理者のパスワードを FMT_MTD.1[5]により登録出来る。管理者のパスワードを登録することで管理者は TOE に登録され、管理者としての作業が開始できる。CE は CE 自身のパスワードを FMT_MTD.1[5]により登録し、FMT_MTD.1[4]で変更することが出来るため、CE は適当な期間毎に CE や管理者のパスワードを変更することが可能となる。さらに、パスワードが変更されることで、CE および管理者パスワードは FIA_SOS.1[1]、FIA_SOS.1[2]で指定されたパスワード規則に従っていることを検証されているためユーザが入力した CE や管理者のパスワードが一致する可能性を低くする。

CE パスワードおよび管理者のパスワードの管理を FMT_SMF.1 で特定する。管理者、及び CE を FMT_SMR.1[1]、FMT_SMR.1[2]で維持する。以上の機能は、FMT_MOF.1 で有効に動作する状態になる。

FMT_MTD.1[1]により、ユーザ BOX パスワードの登録が管理者にのみ許可されており、FMT_MTD.1[2]により、ユーザ BOX パスワードの変更がユーザ BOX を所有している一般利用者及び管理者にのみ許可されている。ユーザ BOX パスワードを登録、変更する際には、FIA_SOS.1[3]で指定されたパスワード規則に従っているか検証される。

FMT_MTD.1[6]は管理者に、HDD1、2 の HDD ロックパスワードを変更し、管理する機能を提供する。このパスワードは、FIA_SOS.1[4]により指定された規則に従っているか検証されている。

FMT_MTD.1[3]は管理者に管理者自身のパスワードを変更することを許可するため、管理者は適当な期間毎に管理者のパスワードを変更することが可能となる。管理者パスワードを変更する際、パスワードは、FIA_SOS.1[2]で指定されたパスワード規則に従っているか検証されている。

ユーザ BOX パスワードの管理を FMT_SMF.1 で特定する。管理者を FMT_SMR.1[2]で維持する。FMT_MOF.1 により、管理者のみにセキュリティ強化モードの停止を許可する。

従って、対応するセキュリティ機能要件（FMT_MTD.1[2]、FMT_MTD.1[4]、FMT_MTD.1[5]、FMT_MTD.1[6]、FIA_SOS.1[1]、FIA_SOS.1[2]、FMT_SMR.1[1]、FMT_MTD.1[1]、FIA_SOS.1[3]、FIA_SOS.1[4]、FMT_MTD.1[3]、FIA_SOS.1[2]、FMT_SMF.1、FMT_SMR.1[2]、FMT_MOF.1）により O.MANAGE は実現可能である。

- **O.AUDIT（監査情報の記録）**

本セキュリティ対策方針は、監査ログを生成する機能、監査ログへの参照を制限する機能、及び監査データ損失の防止に関わる諸要件が必要である。

必要な監査情報を FPT_STM.1 で信頼できるタイムスタンプと共に FAU_GEN.1 で記録する。監査対象事象には「保護対象となる資産」に対する明白な不正アクセスに関する全ての事象として、ユーザ BOX の識別認証の失敗、ユーザ BOX の登録、ユーザ BOX パスワードの登録/変更、ドキュメントデータの読み出し、印刷、削除に関する操作の履歴が監査ログとして記録されることから、管理者はこの監査ログを参照し、ドキュメントデータに対する不正なアクセスを検出することができる。また、CE・管理者パスワードの登録/変更といった TSF データに対する操作の成功が監査ログに記録され、管理者がこれらの監査ログを参照することにより CE・管理者に対するなりすましを検出することができる。さらに、管理者の識別・認証の失敗、セキュリティ強化モードの設定の成功、HDD ロックパスワードの変更の成功を監査情報として記録するため、管理者以外が HDD ロックパスワードを変更し、当該管理機能を不正に利用しようと試みたことを検出可能にする。

監査格納領域は FAU_STG.1 で保護し、監査格納領域が枯渇した場合に、FAU_STG.4 で古い監査記録領域に対して監査記録の上書きを実施する。監査情報の採取は FMT_MOF.1 により有効に動作する。以上により必要な監査情報は格納される。さらに、管理者以外の監査データ読み出しを FAU_SAR.2 で禁止している。また、監査記録の解釈可能な形での提供を FAU_SAR.1 で実現して

いる。以上により、監査記録の監査は可能となる。

従って、対応するセキュリティ機能要件（FPT_STM.1、 FAU_GEN.1 、FAU_STG.1 、FAU_STG.4 、FMT_MOF.1、 FAU_SAR.2、 FAU_SAR.1）により O.AUDIT は実現可能である。

- **O.CHECK-HDD（HDD の検証）**

本セキュリティ対策方針は、TOE が起動する前に正しい HDD ロックパスワードが設定された HDD が接続されていることを確認するため、TOE が TOE 及び HDD に対して設定された HDD ロックパスワードにより HDD ロック機能をテストするとしており、外部エンティティの動作をテストすることを規定する諸要件が必要である。

FPT_TEE.1 により、TOE 起動時に HDD に対して HDD ロックパスワードを受け渡し、HDD において HDD ロックパスワードによる認証が失敗した場合、MFP 本体の動作を停止する。

従って、対応するセキュリティ機能要件（FPT_TEE.1）により O.HDD-LOCK は実現可能である。

6.2.1.3. IT セキュリティ機能要件の依存性

IT セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 で規定される依存性を満たさない場合、「本 ST における依存関係」の欄にその理由を記述する。

表 8　IT セキュリティ機能要件コンポーネントの依存関係

N/A：Not Applicable

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2
FDP_ACF.1[1]	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1[1] FMT_MSA.3 は、ドキュメントデータが登録されるときに決定するため、不要である。
FDP_ACF.1[2]	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1[2]、FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]
FIA_ATD.1	なし	N/A
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MSA.1	[FDP_ACC.1 または	FDP_ACC.1[2] 、FMT_SMR.1[2]、FMT_SMF.1

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
	FDP_IFC.1] 、FMT_SMR.1、FMT_SMF.1	
FMT_MSA.3	FMT_MSA.1 、FMT_SMR.1	FMT_MSA.1 FMT_SMR.1 は、デフォルト値を上書きする機能が存在しないため、不要である。
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[1]、FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[6]	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]
FPT_STM.1	なし	N/A
FPT_TEE.1	なし	N/A

6.2.2. IT セキュリティ保証要件根拠

本 TOE は、物理的・人的・接続的に十分なセキュリティを確保した環境に設置され利用されるが、本 TOE を利用する環境において十分な実効性を保証する必要がある。一般的な商用事務製品として機能仕様、TOE 設計書に基づくテスト、機能強度分析、脆弱性の探索が実施されている必要があり、また開発環境の制御、TOE の構成管理、セキュアな配付手続きが取られていることが望まれる。従って十分な保証レベルが提供される EAL3 の選択は妥当である。

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

7. TOE 要約仕様

本章では、TOE の要約仕様を記述する。

7.1. TOE 要約仕様

本節では、TOE のセキュリティ機能を説明する。各セキュリティ機能に対応する TOE セキュリティ機能要件が示されているように､本節で説明するセキュリティ機能は、 6.1.1 で記述した TOE セキュリティ機能要件を満たす。

7.1.1. 識別認証

識別認証機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
IA.ADM_ADD 管理者の登録 CE の登録	IA.ADM_ADD は、CE・管理者を TOE に登録する。CE のみが IA.ADM_ADD を操作する。CE は、CE・管理者のパスワードを登録する。IA.ADM_ADD は、CE・管理者登録のインタフェースを提供する。CE・管理者登録のインタフェースは、登録する CE・管理者に対応するパスワードの入力を要求する。 CE が入力する CE・管理者パスワードに対して、以下の規則に従い、許容値を検証する。 ・パスワードは 8 文字とする ・CE パスワードは半角英大文字、半角英小文字、半角数字で構成する ・管理者パスワードは半角英大文字、半角英小文字、半角数字、記号『-^¥@[]:;,./＼!"#$%&'()=~|`{+*}<>?_』で構成する ・パスワードは一世代前のパスワードと同一の値を禁止する 許容値の検証において、規則に従っている場合、CE・管理者を登録する。規則に従っていない場合、登録を拒否する。	FIA_SOS.1[1] FIA_SOS.1[2] FMT_MTD.1[5] FMT_SMF.1 FMT_SMR.1[1]
IA.ADM_AUTH 管理者の識別と認証	IA.ADM_AUTH は、操作者が TOE を利用する前に、TOE に登録した管理者であることを識別し､操作者が管理者本人であることを認証する。 IA.ADM_AUTH は、管理者の識別と認証の前に管理機能の一切の操作を許可しない。管理者の識別と認証のインタフェースは、IA.ADM_ADD で登録、IA_PASS で変更したパスワードの入力を要求する。IA.ADM_AUTH は、管理者の識別と認証のインタフェースの表示により管理者であることを識別し、入力するパスワードを用いて管理者本人であることを認証する。管理者がパスワードを入力する際は、入力したパスワードの代わりにダミー文字(＊)を表示する。 認証不成功時には、5 秒後に管理者の識別と認証のインタフェースを提供する。	FIA_AFL.1 FIA_UAU.2[2] FIA_UAU.7 FIA_UID.2[2]

IA.CE_AUTH CE の識別と認証	IA.CE_AUTH は、操作者が TOE を利用する前に、TOE に登録している CE であることを識別し、操作者が CE 本人であることを認証する。 IA.CE_AUTH は、CE の識別と認証の前に CE 機能の一切の操作を許可しない。IA_PASS で変更したパスワードの入力を要求する。IA.CE_AUTH は CE の識別と認証のインタフェースの表示により CE であることを識別し、入力するパスワードを用いて CE 本人であることを認証する。CE がパスワードを入力する際は、入力したパスワードの代わりにダミー文字(＊)を表示する。 認証不成功時には、5 秒後に CE の識別と認証のインタフェースを提供する。	FIA_AFL.1 FIA_UAU.2[1] FIA_UAU.7 FIA_UID.2[1]
IA.PASS パスワードの変更	IA.PASS は、管理者、CE 及びユーザ BOX の認証情報である管理者のパスワード、CE のパスワード及びユーザ BOX パスワードを変更する。 IA.PASS は、パスワード変更のインタフェースを提供し、新しいパスワードの入力を要求する。利用者により以下のパスワードの変更が可能である。 CE　　：CE のパスワード、管理者のパスワード 管理者　：管理者のパスワード、ユーザ BOX パスワード ユーザ BOX を所有している一般利用者　： 自分自身が所有しているユーザ BOX パスワード CE、管理者、ユーザ BOX を所有している一般利用者が入力するパスワードに対して、以下の規則に従い許容値を検証する。 ・CE 及び管理者パスワードは 8 文字とする ・ユーザ BOX パスワードは 8～64 文字とする ・CE パスワード、ユーザ BOX パスワードは半角英大文字、半角英小文字、半角数字で構成する ・管理者パスワードは半角英大文字、半角英小文字、半角数字、記号『-^¥@[]:;,./＼!"#$%&'()=~|`{+*}<>?_』で構成する ・パスワードは一世代前のパスワードと同一の値を禁止する 許容値の検証において、規則に従っている場合、パスワードを変更する。	FIA_SOS.1[1] FIA_SOS.1[2] FIA_SOS.1[3] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_SMF.1 FMT_SMR.1[1] FMT_SMR.1[2] FMT_SMR.1[3]

7.1.1.1. 対応する SFR の実現方法

FIA_AFL.1

管理者に対しては IA.ADM_AUTH により、CE に対しては IA.CE_AUTH により、認証の不成功時に、それぞれ管理者、CE に対して、次の認証試行を 5 秒間実行しない。

FIA_SOS.1[1]

CE のパスワード登録に対しては IA.ADM_ADD で、CE のパスワード変更に対しては IA.PASS で、パスワード規則に従った許容値の範囲であるか判断する。以上により、IA.PASS を実装することで FIA_SOS.1[1]を実現できる。

FIA_SOS.1[2]

管理者のパスワード登録に対しては IA.ADM_ADD によって、また、管理者および CE によ

る管理者パスワードの変更に対しては IA.PASS により、パスワード規則に従った許容値の範囲であるか判断する。

以上により、IA.ADM_ADD および IA.PASS を実装することで FIA_SOS.1[2]を実現できる。

FIA_SOS.1[3]

ユーザ BOX パスワードの変更に対しては IA.PASS で、パスワード規則に従った許容値の範囲であるか判断する。以上により、IA.PASS を実装することで FIA_SOS.1[3]を実現できる。

FIA_UAU.2[1]

IA.CE_AUTH により、CE の認証を実施する。以上により、IA.CE_AUTH を実装することで FIA_UAU.2[1]を実現する。

FIA_UAU.2[2]

IA.ADM_AUTH により、管理者の認証を実施する。以上により、IA.ADM_AUTH を実装することで FIA_UAU.2[2]を実現する。

FIA_UAU.7

管理者の認証のためのパスワード入力時は IA.ADM_AUTH、CE の認証のためのパスワード入力時は IA.CE_AUTH により、入力したパスワードを入力文字数分のダミー文字(*)で表示する。以上により、IA.ADM_AUTH、IA.CE_AUTH を実装することで FIA_UAU.7 を実現できる。

FIA_UID.2[1]

IA.CE_AUTH により CE の識別を実施する。以上により、IA.CE_AUTH を実装することで FIA_UID.2[1]を実現できる。

FIA_UID.2[2]

管理者に対しては IA.ADM_AUTH で管理者の識別を実施する。以上により、IA.ADM_AUTH を実装することで FIA_UID.2[2]を実現できる。

FMT_MTD.1[2]

ユーザ BOX パスワードの変更を IA.PASS で管理者、自分自身が所有しているユーザ BOX パスワードの変更をユーザ BOX を所有している一般利用者に許可し実行する。以上により、IA.PASS を実装することで FMT_MTD.1[2]を実現できる。

FMT_MTD.1[3]

管理者パスワードの変更を IA.PASS で管理者、CE に許可し実行する。以上により、IA.PASS を実装することで FMT_MTD.1[3]を実現できる。

FMT_MTD.1[4]

CE のパスワードの変更を IA.PASS で CE にのみ許可し実行する。以上により、IA.PASS を実装することで FMT_MTD.1[4]を実現できる。

FMT_MTD.1[5]

CE・管理者のパスワードの登録を IA.ADM_ADD により CE にのみ許可し実行する。

以上により、IA.ADM_ADD を実装することで FMT_MTD.1[5]を実現できる。

FMT_SMF.1

CE 及び管理者のパスワードを管理する機能を IA.ADM_ADD により実装する。管理者、CE 及びユーザ BOX のパスワードを管理する機能を IA.PASS により実装する。以上により、IA.ADM_ADD、IA.PASS を実装することで FMT_SMF.1 を実現できる。

FMT_SMR.1[1]

CE という役割は CE パスワードを管理することで維持される。そこで、CE のパスワードの変更を CE のみに制限することで役割の維持を実現する。この制限は IA.PASS で実装する。以上により、IA.PASS を実装することで FMT_SMR.1[1]を実現できる。

FMT_SMR.1[2]

管理者という役割は管理者パスワードを管理することで維持される。そこで、管理者のパスワードの変更を CE と管理者のみに制限することで役割の維持を実現する。この制限は IA.PASS で実装する。以上により、IA.PASS を実装することで FMT_SMR.1[2]を実現できる。

FMT_SMR.1[3]

ユーザ BOX を所有している一般利用者という役割は当該ユーザ BOX パスワードを管理することで維持される。そこで、ユーザ BOX パスワードの変更を管理者と当該ユーザ BOX を所有している一般利用者のみに制限することで役割の維持を実現する。この制限は IA.PASS で実装する。

以上により、IA.PASS を実装することで FMT_SMR.1[3]を実現できる。

7.1.2. アクセス制御

アクセス制御機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
ACL.USR ユーザ BOX を所有している一般利用者へのアクセスルールと制御	ACL.USR は、IA.ADM_AUTH により認証された管理者のみに、アクセス制御規則に従いユーザ BOX の登録を許可する。また、管理者にドキュメントデータの削除を許可する。 ACL.USR は、ユーザ BOX を所有している一般利用者を識別認証し、本人であることが認証できると、アクセス制御規則に従いユーザ BOX を所有している一般利用者が操作可能な範囲を制限する。 ACL.USR は、ユーザ BOX を所有している一般利用者をユーザ BOX 識別子、ユーザ BOX パスワードを元に識別と認証を行う。ユーザ BOX パスワードを入力する際は、入力したユーザ BOX パスワードの代わりにダミー文字(＊)を表示する。識別認証されると識別認証したユーザ BOX 識別子が示すドキュメントデータに対して以下の操作を許可する。 ・ドキュメントデータの読み出し、印刷、及び削除 識別認証後、ユーザ BOX 識別子と合致するドキュメントデータの内容がパネルに表示され、パネルに表示されたドキュメントデータに対してのみ印刷、削除が許可される（他のユーザ BOX を所有している一般利用者が所有するドキュメントデータは表示されない)。	FDP_ACC.1[1] FDP_ACC.1[2] FDP_ACF.1[1] FDP_ACF.1[2] FIA_AFL.1 FIA_ATD.1 FIA_UAU.2[3] FIA_UAU.7 FIA_UID.2[3] FIA_USB.1 FMT_MSA.3

	また、識別と認証が不成功であった場合、5 秒後に、識別と認証のインタフェースを有効にする。	

7.1.2.1. 対応する SFR の実現方法

FDP_ACC.1[1]

ACL.USR では、ドキュメントデータアクセス制御に基づき、ユーザ BOX を所有している一般利用者に対してのみドキュメントデータの読み出し、印刷を制限する。また、ドキュメントデータアクセス制御に基づき、ユーザ BOX を所有している一般利用者、管理者に対してのみドキュメントデータの削除を制限する。以上により、ACL.USR を実装することで FDP_ACC.1[1]を実現できる。

FDP_ACF.1[1]

ACL.USR では、ドキュメントデータアクセス制御に基づき、ユーザ BOX を所有している一般利用者に対してのみドキュメントデータの読み出し、印刷を制限する。また、ドキュメントデータアクセス制御に基づき、ユーザ BOX を所有している一般利用者、管理者に対してのみドキュメントデータの削除を制限する。以上により、ACL.USR を実装することで FDP_ACF.1[1]を実現できる。

FDP_ACC.1[2]

ACL.USR では、ユーザ BOX アクセス制御に基づき、管理者に対してのみユーザ BOX の登録を制限する。以上により、ACL.USR を実装することで FDP_ACC.1[2]を実現できる。

FDP_ACF.1[2]

ACL.USR では、ユーザ BOX アクセス制御に基づき、管理者に対してのみユーザ BOX の登録を制限する。以上により、ACL.USR を実装することで FDP_ACF.1[2]を実現できる。

FIA_AFL.1

ユーザ BOX に対する認証不成功時に、ユーザ BOX を所有している一般利用者に対して、次の認証試行を 5 秒間実行しない。以上により、ACL.USR を実装することで FIA_AFL.1 を実現する。

FIA_ATD.1

ユーザ BOX の識別認証後、利用者を代行するタスクにユーザ BOX 識別子、または管理者が関連づけられる。以上により、ACL.USR を実装することで FIA_ATD.1 を実現する。

FIA_UAU.2[3]

ACL.USR によりユーザ BOX を所有している一般利用者の認証を実施する。以上により、ACL.USR を実装することで FIA_UAU.2[3]を実現する。

FIA_UAU.7

ユーザ BOX を所有している一般利用者の認証のためのユーザ BOX パスワード入力時は ACL.USR により、入力したユーザ BOX パスワードを入力文字数分のダミー文字(*)で表示する。以上により、ACL.USR を実装することで FIA_UAU.7 を実現できる。

FIA_UID.2[3]

ACL.USR により、ユーザ BOX を所有している一般利用者の識別を実施する。以上により、

ACL.USR を実装することで FIA_UID.2[3]を実現できる。

FIA_USB.1

ユーザ BOX を所有している一般利用者の識別認証後､利用者を代行するタスクにユーザ BOX 識別子が関連づけられる。また、管理者の識別認証後は、利用者を代行するタスクに管理者が関連づけられる。以上により、ACL.USR を実装することで FIA_USB.1 を実現する。

FMT_MSA.3

ACL.USR により、ユーザ BOX の初期化に必要なユーザ BOX へのユーザ BOX 識別子の登録を管理者に許可し実行する。ユーザ BOX 識別子の登録でだれも利用できない制限的な状態でユーザ BOX は作成され、MNG.ADM によるユーザ BOX パスワードを設定することで一般利用者（ユーザ）が利用可能な状態となる。以上により、ACL.USR を実装することで FMT_MSA.3 を実現できる。

7.1.3. 監査

監査機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
AUD.LOG 監査情報の記録	AUD.LOG は、セキュリティ機能の動作に関する監査情報を正確な日付・時刻(年月日時分秒)、操作主体の識別情報、事象の結果情報のリストとして記録する。監査対象となるイベントを以下に示す。 ・監査機能の起動と終了 ・管理者、CE、ユーザ BOX を所有している一般利用者の識別と認証に関する成功不成功 ・CE パスワードの登録の成功 ・管理者パスワード、ユーザ BOX パスワードの登録時の成功 ・管理者、CE のパスワード変更時の成功 ・ユーザ BOX パスワードの変更時の成功 ・ドキュメントデータの読み出し、印刷、削除の成功 ・監査ログの印刷指示の成功 ・セキュリティ強化モードの設定の成功 ・管理者によるユーザ BOX 登録時の成功 ・HDD ロックパスワードの変更の成功	FAU_GEN.1 FPT_STM.1
AUD.MNG 監査領域の管理	AUD.MNG は､監査情報を生成し保存するために監査格納領域を管理する。 監査情報を格納する領域は、リングバッファ形式の記憶領域とする。AUD.MNG は、監査情報の格納領域が枯渇した場合、記憶領域の先頭から監査情報を上書きする。	FAU_STG.4

7.1.3.1. 対応する SFR の実現方法

FAU_GEN.1

セキュリティ機能の動作に関する監査情報として、監査機能の起動/停止、識別認証の成功/不成功、ユーザ BOX 登録の成功、管理者パスワード・CE パスワード・ユーザ BOX パスワード・

HDD ロックパスワードの変更の成功、管理者・ユーザ BOX パスワードの登録の成功、ドキュメントデータの読み出し・印刷、削除の成功、監査ログの印刷指示、セキュリティ強化モードの設定の成功を AUD.LOG により正確な日付・時刻(年月日時分秒)、操作主体の識別情報と共に記録する。以上により、AUD.LOG を実装することで FAU_GEN.1 を実現できる。

FAU_STG.4

監査格納領域が枯渇した場合、AUD.MNG で監査情報を古い格納領域に上書きする。以上により、AUD.MNG を実装することで FAU_STG.4 を実現できる。

FPT_STM.1

必要な監査情報を信頼できるタイムスタンプと共に生成する機能を AUD.LOG で実現する。これにより AUD.LOG を実装することで FPT_STM.1 を実装できる。

7.1.4. 管理支援

管理支援機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
MNG.MODE セキュリティ強化モードの設定	MNG.MODE は、管理者にのみセキュリティ強化モードを停止する機能を許可し実行する。	FMT_MOF.1 FMT_SMF.1
MNG.ADM 管理支援機能(管理者)	MNG.ADM は、管理者に以下の処理を許可し実行する。 ・ユーザ BOX 識別子の登録とユーザ BOX パスワードの登録 ・監査情報の問い合わせ(監査情報の削除機能はない) 管理者が入力するユーザ BOX パスワードに対して、以下の規則に従い、許容値を検証する。 ・パスワードは 8～64 文字とする ・パスワードは半角英大文字、半角英小文字、半角数字で構成する ・パスワードは一世代前のパスワードと同一の値を禁止する 許容値の検証において、規則に従っている場合、登録する。規則に従っていない場合、登録を拒否する。 監査情報の問い合わせでは、事象発生の日付・時刻情報(年月日時分秒)、操作主体の識別情報、事象の結果情報を含み、管理者のみが参照できる形式で印刷する。	FAU_SAR.1 FAU_SAR.2 FAU_STG.1 FIA_SOS.1[3] FMT_MSA.1 FMT_MTD.1[1] FMT_SMF.1 FMT_SMR.1[2]
MNG.HDD HDD ロックパスワード機能	MNG.HDD は、管理者にのみ以下の処理を許可し実行する。 ・HDD ロックパスワードの変更 管理者が入力する HDD ロックパスワードに対して以下の規則に従い、許容値を検証する。 ・パスワードは 8 文字～32 文字とする。 ・パスワードは半角英大文字、半角英小文字、半角数字で構成する。 許容値の検証において、規則に従っている場合、HDD 装置に HDD ロックパスワードを変更する。規則に従っ	FIA_SOS.1[4] FMT_MTD.1[6] FMT_SMF.1 FMT_SMR.1[2]

	ていない場合、変更を拒否する。	

7.1.4.1. 対応する SFR の実現方法

FAU_SAR.1

監査記録を MNG_ADM により管理者が参照できるようにする。以上により、MNG_ADM を実装することで FAU_SAR.1 を実現できる。

FAU_SAR.2

監査記録へのアクセスのインタフェースは管理者モード（管理者の識別認証後にのみアクセス可能）内にのみ存在し、管理者が監査記録を参照できるように MNG.ADM で制限される。以上により、MNG.ADM を実装することで FAU_SAR.2 を実現できる。

FAU_STG.1

監査格納領域内データを管理者のみ読み出し・印刷ができる機能を MNG.ADM で実装する。また、監査格納領域内データに対する削除や改変の機能は提供されない。以上により、MNG.ADM を実装することで FAU_STG.1 を実現できる。

FIA_SOS.1[3]

ユーザ BOX パスワードの登録、変更に対しては MNG_ADM により、パスワード規則に従った許容値の範囲であるか判断する。以上により、MNG_ADM を実装することで FIA_SOS.1[3]を実現できる。

FIA_SOS.1[4]

HDD ロックパスワードの変更に対しては MNG_HDD により、パスワード規則に従った許容値の範囲であるか判断する。以上により、MNG_HDD を実装することで FIA_SOS.1[4]を実現できる。

FMT_MOF.1

TOE のセキュリティ強化モードを停止する機能を MNG.MODE により管理者に対してのみ許可し実行する。以上により、MNG.MODE を実装することで FMT_MOF.1 を実現できる。

FMT_MSA.1

ユーザ BOX 識別子の登録を MNG.ADM により管理者にのみ許可し実行する。以上により、MNG.ADM を実装することで FMT_MSA.1 を実現できる。

FMT_MTD.1[1]

ユーザ BOX パスワードの登録を MNG.ADM により管理者にのみ許可し実行する。以上により、MNG.ADM を実装することで FMT_MTD.1[1]を実現できる。

FMT_MTD.1[6]

HDD ロックパスワードを入力する機能を MNG_HDD で実現する。これにより MNG_HDD の実装で FMT_MTD.1[6]を実装できる。

FMT_SMF.1

セキュリティ強化モードを停止する機能を MNG.MODE で、ユーザ BOX 識別子の登録、ユーザ BOX パスワードの登録によりユーザ BOX を管理する機能を MNG.ADM で、HDD ロックパ

スワードを変更する機能を MNG.HDD で実装する。以上により、MNG.MODE 、MNG.ADM、MNG.HDD を実装することで FMT_SMF.1 を実現できる。

FMT_SMR.1[2]

これは管理者という役割を維持する機能であり、FMT_MTD.1[6]に関連する機能であるが、これは IA.PASS で実現される。

7.1.5. HDD ロック機能のテスト

HDD ロック機能のテストは、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
HDD-LOCK. TEST HDD ロック機能のテスト	HDD-LOCK. TEST は、TOE が TOE に接続された HDD に対して HDD ロック機能のテストを実施するための機能である。TOE 起動時に、TOE は接続された HDD（HDD1、2）に対してロック/アンロック状態の確認を行い、全ての HDD がロック状態であることが確認された場合、HDD ロックパスワードによる解除処理を依頼する（いずれかの HDD がアンロック状態であることが確認された場合はエラー処理により動作を停止する）。HDD ロックパスワードによる解除処理において、TOE は HDD ロックパスワードを全ての HDD に対して送信し、全ての HDD において HDD ロックパスワード認証が成功した場合のみ起動する。HDD ロックパスワードによる解除処理において、いずれかの HDD においてロック解除処理の失敗が確認された場合、MFP 本体の動作を停止する。	FPT_TEE.1

7.1.5.1. 対応する SFR の実現方法

FPT_TEE.1

MFP の起動時に、HDD に対して予め設定された HDD ロックパスワードを受け渡し、HDD の HDD ロック機能によるロック状態を解除するための解除処理を HDD に依頼し、HDD ロックパスワードによる認証に失敗した場合、MFP 本体の動作を停止するため、FPT_TEE.1 を実現できる。

---以上---