Multi functional printer (digital copier) bizhub PRO 1050 Series セキュリティターゲット 第10版

2004 年 12 月 21 日

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 －

改訂版数	改訂内容	承認者	審査者	作成者
1	・ 新規作成	2004/4/15 牛尾 勝	2004/4/15 安田 和夫	2004/4/15 横堀 潤
2	・ 基本処理概念図の修正	2004/5/20 牛尾 勝	2004/5/20 安田 和夫	2004/5/20 横堀 潤
3	・ 評価指摘事項による是正	2004/6/7 牛尾 勝	2004/6/7 安田 和夫	2004/6/7 横堀 潤
4	・ 評価指摘事項による是正２	2004/7/24 牛尾 勝	2004/7/24 安田 和夫	2004/7/24 横堀 潤
5	・ 評価指摘事項による是正３	2004/9/17 牛尾 勝	2004/9/17 安田 和夫	2004/9/17 横堀 潤
6	・ 評価指摘事項による是正４	2004/10/4 牛尾 勝	2004/10/4 安田 和夫	2004/10/4 横堀 潤
7	・ 評価指摘事項による是正５	2004/10/6 牛尾 勝	2004/10/6 安田 和夫	2004/10/6 横堀 潤
8	・ 評価指摘事項による是正６	2004/10/12 牛尾 勝	2004/10/12 安田 和夫	2004/10/12 横堀 潤
9	・ 評価指摘事項による是正７	2004/11/29 牛尾 勝	2004/11/29 安田 和夫	2004/11/29 横堀 潤
10	・ 評価指摘事項による是正 8	2004/12/21 牛尾 勝	2004/12/21 安田 和夫	2004/12/21 横堀 潤

- 目次 -

－ 図目次 －

- 表目次 -

1. ST 概説

1.1. ST 識別

1.1.1. ST の識別と管理

名称: Multi functional printer(digital copier) bizhub PRO 1050　Series セキュリティターゲット

バージョン: 第1.0版

作成日: 2004 年 12 月 21 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

1.1.2. TOE の識別と管理

名称: 日本 : bizhub PRO 1050 全体制御ソフトウェア

・本ソフトウェアは以下の二つのコンポーネントで構成される。

画像制御プログラム（画像制御 I1）

コントローラ制御プログラム(IP コントローラ P1)

海外 : bizhub PRO 1050 control software

・本ソフトウェアは以下の二つのコンポーネントで構成される。

Image Control Program(Image Control I1)

Controller Control Program(IP Control P1)

注）Image Control Program は画像制御プログラムの、Controller Control Program はコントローラ制御プログラムの英語名称であり、それぞれ名称が異なるだけで、同一物である。

バージョン:

画像制御プログラム（画像制御 I1） :11-0000

コントローラ制御プログラム（IP コントローラ P1） :10-0000

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

bizhub PRO 1050 全体制御ソフトウェアと bizhub PRO 1050 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 PRO 1050 全体制御ソフトウェアと記述する。

1.1.3. 使用する CC のバージョン

JIS X 5070:2000

注）日本語訳は以下の資料を利用する。

- 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 2.1 1999 年 8 月 CCIMB-99-031
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2:セキュリティ機能要件 バージョ

ン 2.1 1999 年 8 月 CCIMB-99-032

- 情報技術セキュリティ評価のためのコモンクライテリア パート 3:セキュリティ保証要件 バージョン 2.1 1999 年 8 月 CCIMB-99-033

1.2. ST 概要

本 ST は、コニカミノルタビジネステクノロジーズ株式会社製デジタル複合機「bizhub PRO 1050 シリーズ」(以降 bizhub PRO 1050 シリーズと記述する)に搭載する「bizhub PRO 1050 全体制御ソフトウェア」について記述している。

bizhub PRO 1050 全体制御ソフトウェアは、コピー/プリンタなどを活用した機能において、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 機能および各種管理機能を実装し、文書を保管する HDD(ハードディスク装置)には機密性の高いものを採用している。

1.3. CC 適合

パート 2 拡張

パート 3 適合

EAL3 適合

1.4. 参考資料

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 1999 Version 2.1 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 1999 Version 2.1 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 1999 Version 2.1 CCIMB-99-033
- Common Criteria CCIMB Interpretations-0210
- Common Criteria 補足-0210
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 99/12

2. TOE 記述

2.1. TOE 種別

ネットワーク機能を搭載したデジタル複合機のソフトウェア製品

2.2. 用語説明

No.	用語	説明
1	ユーザ BOX	ユーザ BOX は、ドキュメントデータ(No.2 参照)を格納するディレクトリである。
2	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。
3	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。
4	操作パネル	操作パネルは、bizhub PRO 1050 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。
5	内部ネットワーク	内部ネットワークは、bizhub PRO 1050 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。
6	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.5 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。
7	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。

2.3. TOE 概要

TOE は、bizhub PRO 1050 全体制御ソフトウェア全体である。TOE を搭載する bizhub PRO 1050 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 PRO 1050 シリーズを運用管理するための機能及び bizhub PRO 1050 シリーズを保守管理するための機能を提供する。bizhub PRO 1050 シリーズの利用環境として『図 2.1 bizhub PRO 1050 シリーズの利用環境』に示すオフィスを想定する。

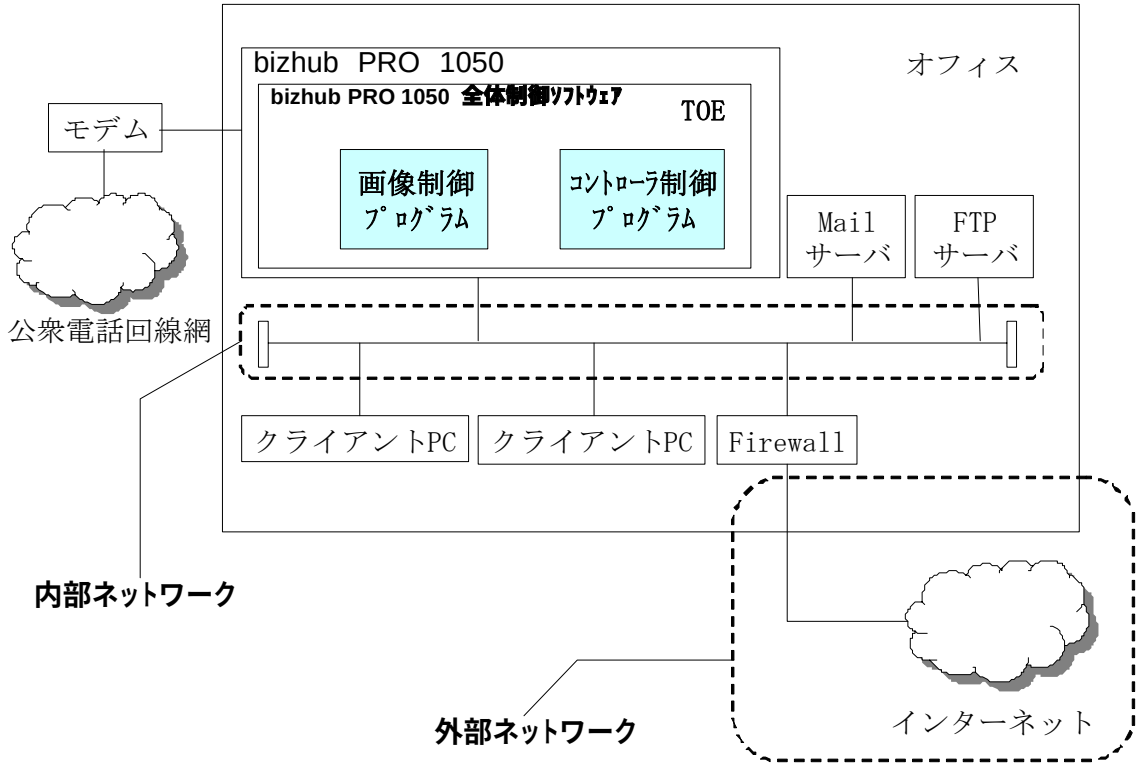

図 2.1 bizhub PRO 1050 シリーズの利用環境

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 PRO 1050 シリーズは、『図 2.1 bizhub PRO 1050 シリーズの利用環境』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 PRO 1050 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。TOE は外部ネットワークとのインタフェースは持たない。内部ネットワークの各機器を保護するため、外部ネットワークとの接続を行う場合は Firewall を介して接続する。

2.4. bizhub PRO 1050 シリーズの関連者と役割

bizhub PRO 1050 シリーズの関連者と役割を以下に示す。

- 一般利用者

  一般利用者は、bizhub PRO 1050 シリーズを導入する組織に在籍し、bizhub PRO 1050 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 TOE に登録することで、bizhub PRO 1050 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。

  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 PRO 1050 シリーズを導入する組織に在籍し、bizhub PRO 1050 シリーズの運

用管理を行う。bizhub PRO 1050 シリーズが提供する運用管理の機能を利用する。

- 責任者

  責任者は、bizhub PRO 1050 シリーズを導入する組織に在籍し、管理者を選任する。

- CE

  CE は、bizhub PRO 1050 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 PRO 1050 シリーズが提供する保守管理の機能を利用し、bizhub PRO 1050 シリーズの保守作業を行う。責任者又は管理者と bizhub PRO 1050 シリーズの保守契約を締結している。

なお、一般利用者、管理者及び CE を製品関係者とする。

2.5. TOE の構成

本 TOE の構成を『図 2.2 TOE の構成』に示す。

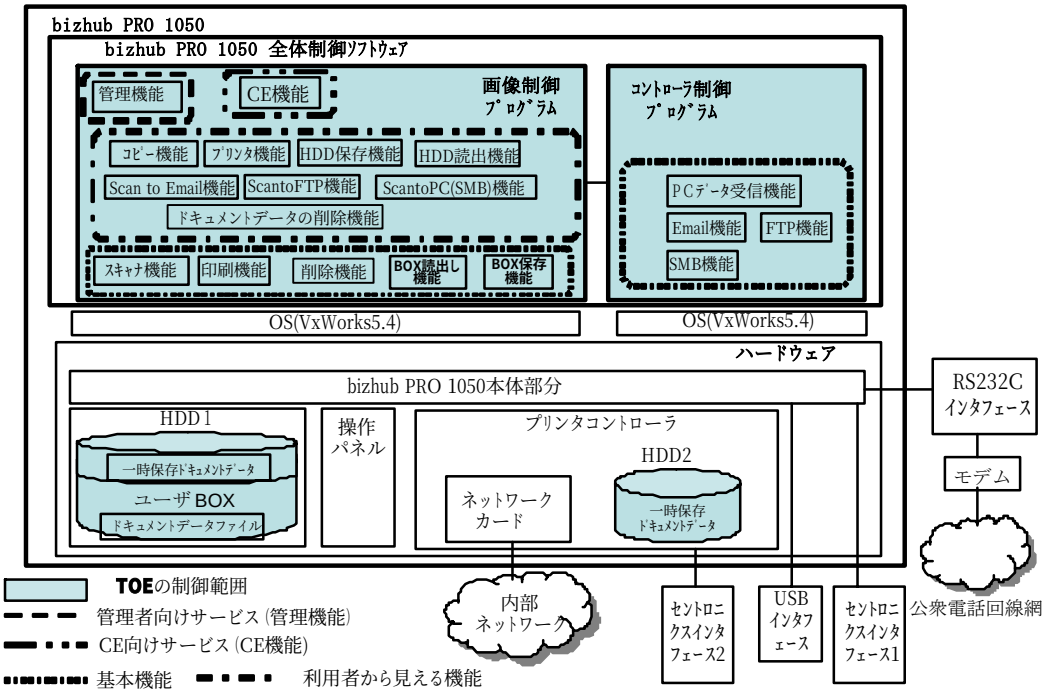

図 2.2 TOE の構成

bizhub PRO 1050 シリーズは、ハードウェア、bizhub PRO 1050 全体制御ソフトウェアから構成される。bizhub PRO 1050 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 PRO 1050 シリーズ本体部分、プリンタコントローラ部分、HDD1 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 PRO 1050 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 インタフェースとセントロニクスインタフェース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。セントロニクスインタフェース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。OS には、VxWorks 5.4 を使用する。bizhub PRO 1050 全体制御ソフトウェアは、OS(VxWorks 5.4)上で動作する。OS は、ハードウェア及び bizhub PRO 1050 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 2.1 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。）から PC データ受信機能、Email 機能、FTP 機能、SMB 機能を除く部分、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 読み出し機能を制御する。

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。

（◆）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 PRO 1050 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 PRO 1050 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 2.2 TOE の構成』のハッチのかかった部分である。

bizhub PRO 1050 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。

2.6. bizhub PRO 1050 全体制御ソフトウェアの機能構成

bizhub PRO 1050 全体制御ソフトウェアは以下の機能を有する。

2.6.1. 基本機能

スキャナから入力されたドキュメントデータは一旦 DRAM 及び HDD1 の一時保存領域に格納され、またクライアント PC からのドキュメントデータは一時保存 HDD2 に格納されデータ変換された後に、一旦 DRAM 及び HDD1 の一時保存領域に格納され、HDD1 内のユーザ BOX、プリンタ、及び一時保存 HDD2 経由で FTP サーバ、Mail サーバ、PC 共用フォルダへ出力される。HDD1内のユーザ BOX のドキュメントデータは一旦DRAM及びHDD1内の一時保存領域に格納され、プリンタに出力される。一時保存DRAMに一時格納されたデータは、電源の OFF と共に消える。一時保存 HDD1／一時保存 DRAM は、一時格納する領域である。

基本機能は、ドキュメントデータの操作をする機能である。ユーザ BOX はユーザ BOX 識別子で識別され、さらに各ユーザ BOX の所有者の正当性を確認するためにユーザ BOX 毎にユーザ BOX パスワードが設定される。正当なユーザ BOX の所有者はそのユーザBOX内のすべてのドキュメントデータをアクセスできる。基本機能の概念を『図 2.3 基本機能の処理概念』に示す。

サブBOXはユーザBOX内に作成され、サブBOXの中にドキュメントデータをまとめて格納する。

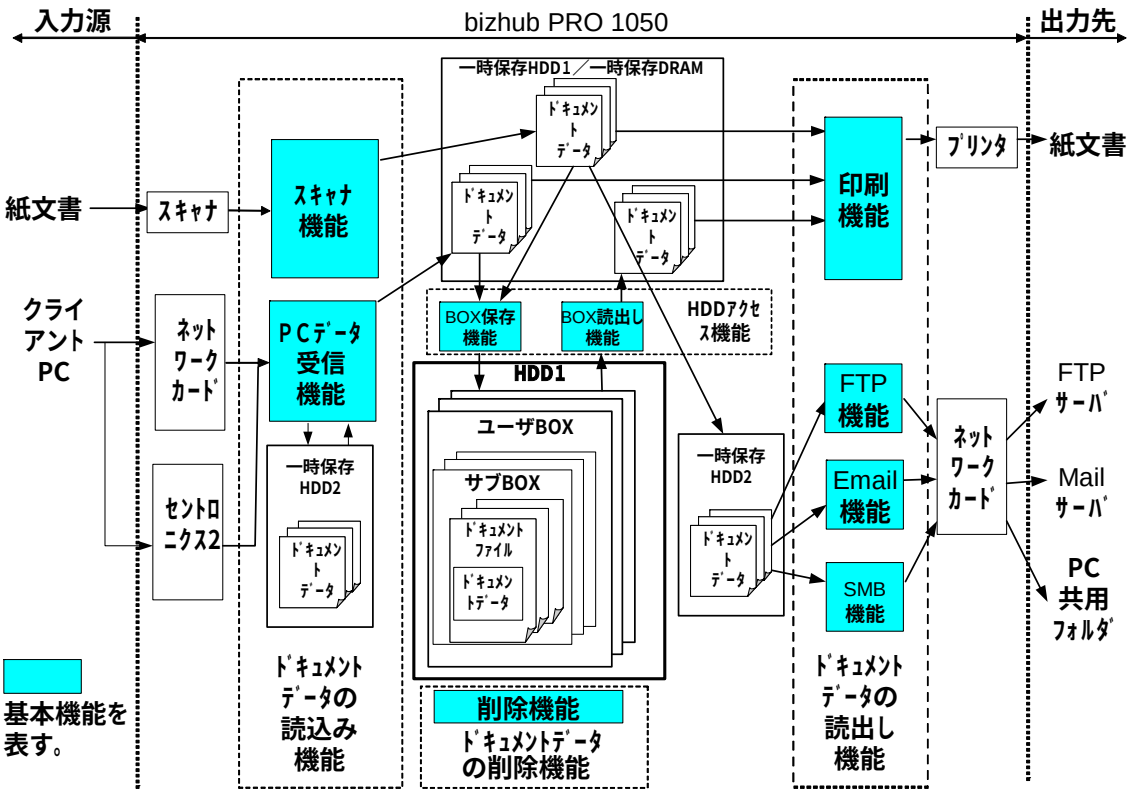

図 2.3 基本機能の処理概念

『表 2.1 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 2.1 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	Scan to Email 機能	スキャナ機能と Email 機能
4	Scan to FTP 機能	スキャナ機能と FTP 機能
5	Scan to PC（SMB）機能	スキャナ機能と SMB 機能
6	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
7	HDD 読出し機能	BOX 読出し機能と印刷機能
8	ドキュメントデータの削除機能	削除機能

『図 2.3 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して、一時保存 HDD1 または、一時保存 DRAM に格納する機能。

(2) PC データ受信機能

一般利用者により、クライアント PC から内部ネットワーク、またはセントロニクス経由で指示されたドキュメントデータを、一時保存 HDD2に格納し、データ変換した後、一時保存 HDD1、または一時保存 DRAM に格納する機能。

(3)BOX 保存機能

一時保存 HDD1 または、一時保存 DRAM に一時格納されたドキュメントデータを、ユーザ BOX 内に追加格納する機能。

(4)BOX 読出し機能

ユーザ BOX 内のドキュメントデータを、一時保存 HDD1 または、一時保存 DRAM に一時読出しする機能。本読み出し機能は、ユーザBOXパスワードで認証された正当な一般利用者のみに許可される。

(5) 印刷機能

一時保存 HDD1 または、一時保存 DRAM に一時格納されたドキュメントデータを印刷する機能。

(6) Email 機能

一時保存 HDD1 または、一時保存 DRAM に一時格納された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 を経由してメールに添付し Mail サーバに送信する機能。

(7) FTP 機能

一時保存 HDD1 または、一時保存 DRAM に一時格納された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 を経由して FTP サーバに送信する機能。

(8)SMB 機能

一時保存 HDD1 または、一時保存 DRAM に一時格納された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 を経由して内部ネットワークに接続されている PC の共有フォルダに送信する機能。

(9)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。

2.6.2. 管理機能

管理機能は、識別と認証が成功した場合のみ管理者に利用を許可する。本機能は操作パネルからのみ利用できる。管理者は、管理機能を使用して、TOE のネットワーク情報の設定、TOE が有する機能の動作設定を行う。また、管理機能は、ユーザ BOX の作成/属性変更/削除、監査情報の印刷、HDD1、HDD2 の初期化処理(データの初期化、不正データ読み出し防止のためのパスワード設定)、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。

2.6.3. CE 機能

CE 機能は、識別と認証が成功した場合のみ以下の機能の利用を CE に許可する。

- サービス設定モード

  CE は、操作パネルから操作しサービス設定モードの機能を利用し管理者のパスワード登録と変更を実施する。

- CSRC(CS Remote Care)

  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 PRO 1050 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。CSRC は、RS232C インタフェースまたは E-Mail インタフェースで行われる。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ロルを用いている。E-Mail には、独自のメッセージ通信プロトコルを用いており、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ない。

2.7. 保護対象となる資産

TOE の保護対象となる資産は bizhub PRO 1050 のハードディスク(HDD1 および HDD2)に格納される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のオリジナルデータは、利用者がクライアントPCや紙で所有しているので、TOEはドキュメントデータの削除に対する防止は行わない。

3. TOE セキュリティ環境

3.1. 前提条件

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 は、ドキュメントデータの漏洩が発生しない内部ネットワークに接続される。

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.USR　　一般利用者の管理

一般利用者は利用者自身のユーザBOXパスワードを漏らさない。

3.2. 脅威

T.ACCESS　　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.HDDACCESS　HDD への不正なアクセス

- 一般利用者が不正な装置を HDD1に接続する事により、HDD1 内のドキュメントデータを漏洩させる恐れがある。
- 一般利用者が不正な装置を HDD2 に接続する事により、HDD2 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してドキュメントデータを漏洩する恐れがある。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

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 又はユーザ BOX を所有している一般利用者を識別認証する。

O.MANAGE 管理機能の提供

TOE は、管理者にユーザ BOX をセキュアに管理する機能、およびドキュメントデータを格納する HDD をセキュアに管理する機能（HDD ロックパスワードを管理・設定する機能）を提供する。

O.CE CE 機能の提供

TOE は、CE が管理機能を管理者に使用可能状態にする機能を提供する。

O.DATAACCESS 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を許可する。

O.AUDIT 監査情報の記録

TOE は、『保護対象となる資産』へのアクセス機能に関連する事象を監査情報として記録する。また、監査情報の参照を管理者のみに制限する。

4.2. 環境のセキュリティ対策方針

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.NET ネットワークの管理

管理者は、通信がセキュアに行われる機器を利用して、ドキュメントデータが漏洩しない、ファイアウォールで保護された内部ネットワーク環境にTOEを接続する。

OE.USR 一般利用者の教育

管理者は、一般利用者がユーザ BOX パスワードを他者に漏らさないように教育する。

OE.ADMIN 管理者の条件

責任者は、不正を行わない人物を管理者として選任する。

OE.HDD　　HDD の保護

ドキュメントデータを格納するための HDD1 および HDD2 は、HDD ロックパスワードで不正なアクセスを防止する。

OE.CE　　CE の保証

責任者又は管理者は、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。

5. IT セキュリティ要件

5.1.　TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

FIA_UID.2　　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　:「利用者」→ 管理者、CE 及びユーザBOXを所有している一般利用者

依存性:なし

FIA_UAU.2　　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を認証することを要求しなければならない。

詳細化　：「利用者」→ 管理者、CE 及びユーザBOXを所有している一般利用者

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.7　　保護された認証フィードバック

下位階層：なし

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]

- 操作者が入力するパスワード文字数分のダミー文字(*)

依存性：FIA_UAU.1 認証のタイミング

FIA_AFL.1　　認証失敗時の取り扱い

下位階層：なし

FIA_AFL.1.1

TSFは、[割付：認証事象のリスト]に関して、[割付：回数]回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト]

- 管理者、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

[割付：回数]

- 1

FIA_AFL.1.2

不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：アクションのリスト]をしなければならない。

[割付：アクションのリスト]

- 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。

依存性：FIA_UAU.1 認証のタイミング

FIA_SOS.1[1]　　秘密の検証

下位階層:なし

FIA_SOS.1.1

TSF は、秘密が[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]

- パスワードの品質尺度を以下のように定義する。

  パスワード長:8 から 64 文字

  構成文字種　:半角英大文字、半角英小文字、半角数字

  許容条件　　:一世代前のパスワードと同一のパスワードを禁止

詳細化 :「秘密」→

「ユーザ BOX パスワード」

依存性:なし

FIA_SOS.1[2]　　秘密の検証

下位階層:なし

FIA_SOS.1.1

TSF は、秘密が[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]

- パスワードの品質尺度を以下のように定義する。

  パスワード長: 8 文字

  構成文字種　:半角英大文字、半角英小文字、半角数字

  許容条件　　:一世代前のパスワードと同一のパスワードを禁止

詳細化 :「秘密」→

「管理者のパスワード」及び「CE のパスワード」

依存性:なし

FDP_ACC.1[1]　サブセットアクセス制御

下位階層：なし

FDP_ACC.1.1

TSFは、[割付：サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付：アクセス制御SFP]を実施しなければならない。

[割付：サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

- サブジェクト：利用者受付機能１ ： ユーザBOXを所有している一般利用者のユーザBOXへのアクセスの依頼を受け付けるプロセス
- オブジェクト：ユーザ BOX
- 操作：
  1)ユーザ BOX 内のドキュメントデータの読み出し

[割付：アクセス制御SFP]

- アクセス制御方針1

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1[2]　サブセットアクセス制御

下位階層：なし

FDP_ACC.1.1

TSFは、[割付：サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付：アクセス制御SFP]を実施しなければならない。

[割付：サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

- サブジェクト：利用者受付機能２ ： 管理者のユーザ BOX へのアクセスの依頼を受け付けるプロセス
- オブジェクト：ユーザ BOX
- 操作：
  1)ユーザ BOX の作成

[割付：アクセス制御SFP]

- アクセス制御方針2

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

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

FDP_ACF.1.1

TSFは、[割付：セキュリティ属性、名前付けされたセキュリティ属性のグループ]に基づいて、オブジェクトに対して、[割付：アクセス制御SFP]を実施しなければならない。

[割付：セキュリティ属性、名前付けされたセキュリティ属性のグループ]

- セキュリティ属性：ユーザBOX識別子
- 名前付けされたセキュリティ属性のグループ：なし

[割付：アクセス制御SFP]

- アクセス制御方針1

FDP_ACF.1.2

TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：［割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則］。

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

以下で特定されるユーザBOX内のドキュメントデータの読み出しを許可する。

・利用者受付機能1に関連付けられたユーザBOX識別子とユーザBOXに関連付けられたユーザBOX識別子が一致する。

FDP_ACF.1.3

TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない：［割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則］。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]

- なし

FDP_ACF.1.4

TSFは、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

- なし

依存性：FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

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

FDP_ACF.1.1

TSFは、[割付：セキュリティ属性、名前付けされたセキュリティ属性のグループ]に基づいて、オブジェクトに対して、[割付：アクセス制御SFP]を実施しなければならない。

[割付：セキュリティ属性、名前付けされたセキュリティ属性のグループ]

- セキュリティ属性：ユーザBOX識別子
- 名前付けされたセキュリティ属性のグループ：なし

[割付：アクセス制御SFP]

- アクセス制御方針2

FDP_ACF.1.2

TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：［割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則］。

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

下記を実行する。

・利用者受付機能2に関連付けられたユーザ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の作成を許可する。

FDP_ACF.1.3

TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない：［割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則］。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]

- なし

FDP_ACF.1.4

TSFは、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

- なし

依存性：FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FAU_GEN.1　　監査データの生成

下位階層:なし

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]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]

- 指定なし

[割付:上記以外の個別に定義した監査対象事象]

- 監査の対象を『表 5.1 監査対象となる事象』に記す。

表 5.1 監査対象となる事象

機能コンポーネント	監査情報
FIA_UID.2	管理者、CE、ユーザ BOX を所有している一般利用者の識別時における、識別の成功及び識別の不成功
FIA_UAU.2	管理者、CE、ユーザ BOX を所有している一般利用者の認証時における、認証の成功及び認証の不成功
FIA_AFL.1	管理者、CE、ユーザ BOX を所有している一般利用者の認証の不成功が閾値へ到達
FIA_SOS.1[1]	テストされた認証情報の拒否または受入れ
FIA_SOS.1[2]	テストされた認証情報の拒否または受入れ
FDP_SOS.1	テストされた認証情報の拒否または受入れ
FDP_ACF.1[1]	オブジェクトに対する操作の実行における成功及び不成功の要求
FDP_ACF.1[2]	オブジェクトに対する操作の実行における成功及び不成功の要求
FMT_SMF.1	管理機能の使用
FDP_MTD.1	管理者データの値の改変

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、事象の結果(成功又は失敗); 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

依存性:FPT_STM.1 高信頼タイムスタンプ

FAU_STG.1　　保護された監査証跡格納

下位階層：なし

FAU_STG.1.1

TSFは、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、監査記録の改変を[選択: 防止、検出]できねばならない。

[選択: 防止、検出]

- 防止

依存性:FAU_GEN.1 監査データ生成

FAU_STG.4　　監査データ損失の防止

下位階層:FAU_STG.3

FAU_STG.4.1

TSF は、監査証跡が満杯になった場合、[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]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]を行わねばならない。

[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]

- 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

依存性:FAU_STG.1 保護された監査証跡格納

FAU_SAR.1　　監査レビュー

下位階層：なし

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 5.1 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。

依存性：FAU_GEN.1 監査データ生成

FAU_SAR.2　　監査レビューの制限

下位階層:なし

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。

依存性:FAU_SAR.1 監査レビュー

FMT_MTD.1[1]　TSF データの管理

下位階層：なし

FMT_MTD.1.1

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

[割付：TSFデータのリスト]

- 管理者のパスワード

[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、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

依存性：FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1[2]　TSF データの管理

下位階層:なし

FMT_MTD.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]

- CE のパスワード

[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:その他の操作]
なし

[割付:許可された識別された役割]

- CE

依存性:FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1[3]　TSF データの管理

下位階層：なし

FMT_MTD.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]]
改変

[割付：その他の操作]
なし

[割付：許可された識別された役割]

- 管理者

依存性：FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1[4]　TSF データの管理

下位階層:なし

FMT_MTD.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]]
その他の操作

[割付:その他の操作]

- ユーザ BOX を所有している一般利用者自身のユーザ BOX パスワードに対してのみ改変

[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役割

依存性:FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1[5]　TSF データの管理

下位階層:なし

FMT_MTD.1.1

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

[割付:TSFデータのリスト]

- 管理者パスワード

[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

依存性:FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

FMT_MSA.1　　セキュリティ属性の管理

下位階層:なし

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]]

- 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]

- アクセス制御方針 2

依存性:[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MSA.3　　静的属性初期化

下位階層：なし

FMT_MSA.3.1

TSFは、そのSFPを実施するために使われるセキュリティ属性として[選択：制限的、許可的、その他の特性]デフォルト値を与える[割付： アクセス制御SFP、情報制御フローSFP]を実施しなければならない。

[選択：制限的、許可的、その他の特性]

- 制限的

[割付：アクセス制御SFP 、情報フロー制御SFP]

- アクセス制御方針 2

詳細化 ：「セキュリティ属性」→「ユーザ BOX 識別子」

FMT_MSA.3.2

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

[割付：許可された識別された役割]

- 管理者

依存性：FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティ役割

FMT_SMR.1　　セキュリティ役割

下位階層：なし

FMT_SMR.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]

- 管理者
- CE
- ユーザBOXを所有している一般利用者役割

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性:FIA_UID.1 識別のタイミング

FMT_MOF.1　　セキュリティ機能のふるまいの管理

下位階層:なし

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]

- 機能1、機能2、機能3　および　機能4
  - 機能1:　パスワードの長さチェック機能
  - 機能2:　HDDの識別・認証機能
  - 機能3:　監査情報の記録機能
  - 機能4:　識別・認証機能

[選択:のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

を動作させる、を停止する

[割付:許可された識別された役割]

- 管理者

依存性:FMT_SMR.1　セキュリティ役割

FMT_SMF.1　管理機能の特定

FMT_SMF.1　　管理機能の特定

下位階層:なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付:TSF によって提供されるセキュリティ管理機能のリスト]

[割付:TSF によって提供されるセキュリティ管理機能のリスト]

- 『表 5.2 管理要件項目一覧』に示す

表 5.2 管理要件項目一覧

機能要件	管理要件	管理項目
FIA_UID.2	利用者識別情報の管理	ユーザ BOX 識別子
FIA_UAU.2	CE による認証データの管理	管理者のパスワード
	管理者による認証データの管理	ユーザ BOX パスワード
	このデータに関係する利用者による認証データの管理	管理者のパスワード CE のパスワード ユーザ BOX パスワード
FIA_UAU.7	なし	
FIA_SOS.1[1]	秘密の検証に使用される尺度の管理	秘密の検証に使用される尺度は変更不可であるため、管理項目はない
FIA_SOS.1[2]	秘密の検証に使用される尺度の管理	秘密の検証に使用される尺度は変更不可であるため、管理項目はない
FDP_SOS.1	IT 環境の秘密の検証に使用される尺度の管理	IT 環境の秘密の検証に使用される尺度は変更不可であるため、管理項目はない
FIA_AFL.1	不成功の認証試行に対する閾値の管理	閾値は固定であり、変更不可であるため、管理項目はない
	認証失敗の事象においてとられるアクションの管理	アクションは固定であり、変更不可であるため、管理項目はない
FDP_ACC.1[1]	なし	
FDP_ACC.1[2]	なし	
FDP_ACF.1[1]	明示的なアクセスまたは拒否に基づく決定に	ユーザ BOX 識別子

機能要件	管理要件	管理項目
	使われる属性の管理	
FDP_ACF.1[2]	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	ユーザ BOX 識別子
FAU_GEN.1	なし	
FAU_STG.1	なし	
FAU_STG.4	監査格納失敗時に取られるアクションの維持	監査格納失敗時に取られるアクションは変更不可であるため、管理項目はない
FAU_SAR.1	監査記録に対して読み出し権のある使用者グループの維持(削除、改変、追加)	監査記録に対して読み出し権を所有するのは管理者だけであり、変更不可であるため、管理項目はない
FAU_SAR.2	なし	
FMT_MTD.1[1]	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	CE 役割は一人に固定されているため、管理項目はない。
FMT_MTD.1[2]	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	CE 役割は一人に固定されているため、管理項目はない。
FMT_MTD.1[3]	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	管理者役割は一人に固定されているため、管理項目はない。
FMT_MTD.1[4]	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	ユーザ BOX を所有している一般利用者役割は固定されているため、管理項目はない。
FMT_MTD.1[5]	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	管理者役割は一人に固定されているため、管理項目はない。
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること	管理者役割は一人に固定されているため、管理項目はない。
FMT_MSA.3	初期値を特定できる役割グループを管理すること	管理者役割は一人に固定されているため、管理項目はない。
	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	デフォルト値は固定であるため、管理項目はない
FMT_SMR.1	役割の一部をなす利用者のグループの管理	CE、管理者、ユーザ BOX を所有している一般利用者役割は固定されているため、管理項目はない。
FMT_MOF.1	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	管理者役割は一人に固定されているため、管理項目はない。
FMT_SMF.1	なし	

機能要件	管理要件	管理項目
FMT_RVM.1	なし	
FDP_MTD.1	管理者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	管理者役割は一人に固定されているため、管理項目はない。

依存性:なし

FPT_RVM.1　　TSP の非バイパス性

下位階層:なし

FPT_RVM.1.1

TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性:なし

本 ST では、CCPart2 を参照せずに新規に TOE セキュリティ機能要件（FDP_MTD.1　管理者データの管理、FDP_SOS.1　IT　環境の秘密の検証）を作成し、使用している。管理者データとは、管理者のみがアクセスできる、IT 環境のセキュリティ機能の制御データである。

FDP_MTD.1　　管理者データの管理

FDP_MTD.1　管理者データの管理は、許可利用者が管理者データを管理することを許可する。

管理：FDP_MTD.1

以下のアクションは、FMT管理における管理機能と考えられる。

a）管理者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。

監査：FDP_MTD.1

FAU_GEN　セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである。

a）基本：管理者データの値のすべての改変

下位階層：なし

FDP_MTD.1.1

TSFは、[割付：管理者データのリスト]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：管理者データのリスト]

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

依存性：FMT_SMR.1　セキュリティの役割

FMT_SMF.1　　管理者機能の特定

FPT_STM.1　　高信頼タイムスタンプ

下位階層:なし

FPT_STM.1.1

TSFは、それ自身の使用のため、高信頼タイムスタンプを提供できなければならない。

依存性:なし

FDP_SOS.1　　IT 環境の秘密の検証

FDP_SOS.1　IT環境の秘密の検証は、IT環境の秘密が定義された品質尺度に合っていることをTSFが検証することを要求する。

管理:FDP_SOS.1

以下のアクションは、FMTにおける管理機能と考えられる。

a)　IT環境の秘密の検証に使用される尺度の管理。

監査:FDP_SOS.1

FAU_GEN　セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである。

a)　最小:TSFによる、テストされたIT環境の秘密の拒否;

b)　基本:TSFによる、テストされたIT環境の秘密の拒否または受け入れ;

c)　詳細:定義された品質尺度に対する変更の識別。

下位階層:なし

FDP_SOS.1.1

TSF は、IT 環境の秘密が[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]

- パスワードの品質尺度を以下のように定義する。

  パスワード長:　8 から 32 文字

  構成文字種　:半角英大文字、半角英小文字、半角数字

  許容条件　　:無し

詳細化 :「IT 環境の秘密」→「HDD ロックパスワード」

依存性 : なし

5.1.2. TOE セキュリティ保証要件

本 TOE は、商用の製品において、十分なレベルの品質保証レベルである EAL3 を主張する。EAL3 に対応する TOE セキュリティ保証要件を『表 5.3 TOE セキュリティ保証要件一覧』に示す。

表 5.3 TOE セキュリティ保証要件一覧

保証クラス	保証要件
構成管理	ACM_CAP.3 許可の管理
	ACM_SCP.1 TOE の CM 範囲
配付と運用	ADO_DEL.1 配付手続き
	ADO_IGS.1 設置、生成、及び立ち上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_HLD.2 セキュリティ実施上位レベル設計
	ADV_RCR.1 非形式的対応の実証
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1 セキュリティ手段の識別
テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト:上位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	AVA_MSU.1 ガイダンスの検査
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.1 開発者脆弱性分析

5.2.　IT 環境に対するセキュリティ機能要件

FIA_UID.2[E]　　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1[E]

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　:「TSF」 → 「HDD」

依存性：なし

FIA_UAU.2[E]　　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1[E]

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を認証することを要求しまければならない。

詳細化　:「TSF」 → 「HDD」

依存性：FIA_UID.1　識別のタイミング

5.3. セキュリティ機能強度

TOE 機能強度主張が対象とするのは以下の3つのパスワードメカニズムであり、本 ST において対象とする TOE の機能コンポーネントは対応する以下の7つである。

パスワードメカニズムおよび、対応する TOE 機能コンポーネント

① ユーザ BOX パスワード認証機能

FIA_UID.2、FIA_UAU.2、FIA_UAU.7、FIA_AFL.1、FIA_SOS.1[1]

② 管理者パスワード・CE パスワード認証機能

FIA_UID.2、FIA_UAU.2、FIA_UAU.7、FIA_AFL.1、FIA_SOS.1[2]

③ HDD ロックパスワード認証機能

FDP_SOS.1

TOE コンポーネント機能

FIA_UID.2（利用者識別）

FIA_UAU.2（利用者認証）

FIA_UAU.7（保護されたフィードバック）

FIA_SOS.1[1](秘密の検証)

FIA_SOS.1[2]（秘密の検証）

FDP_SOS.1（IT 環境の秘密の検証）

FIA_AFL.1（認証失敗時の取り扱い）

上記7つの TOE 機能要件に対して、SOF－基本を主張する。また、TOE の最小機能強度に対して、SOF－基本を主張する。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

6.1.1. 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	IA.ADM_ADD は、管理者を TOE に登録する。CE のみが IA.ADM_ADD を操作する。CE は、管理者のパスワードを登録する。 IA.ADM_ADD は、管理者登録のインタフェースを提供する。管理者登録のインタフェースは、登録する管理者に対応するパスワードの入力を要求する。 管理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。 • パスワードは 8 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、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[2] FMT_MTD.1[1] FMT_SMF.1 FMT_SMR.1 FPT_RVM.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。	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1

	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。	
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_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1
IA.PASS パスワードの変更	IA.PASS は、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:自分自身のユーザ BOX のユーザ BOX パスワード 製品関係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 • 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、パスワードを	FIA_SOS.1[1] FIA_SOS.1[2] FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_MTD.1[5] FMT_SMF.1 FMT_SMR.1 FPT_RVM.1

	変更する。	

6.1.2. 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 一般利用者へのアクセスルールと制御	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、アクセスルールに従い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 識別子が示すユーザ BOX 内の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と印刷 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。	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FDP_ACC.1[1] FDP_ACF.1[1] FPT_RVM.1

6.1.3. 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時刻とともに記録する。 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 • 管理者、ユーザ BOX を所有している一般利用者のパスワード登録時の成功 • 管理者、CE、ユーザ BOX を所有している一般利用者のパスワードおよび HDD ロックパスワード変更時の成功 • ドキュメントデータ読み出しの成功	FAU_GEN.1 FPT_RVM.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 FPT_RVM.1

6.1.4. 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 TOE のパスワードの長さチェック機能、HDD の識別・認証機能、監査情報の記録機能、識別・認証機能を有効にする機能、およびそれらを停止にする機能を許可し実行する。	FMT_MOF.1 FPT_RVM.1
MNG.ADM 管理支援機能(管理者)	MNG.ADM は、管理者にのみ以下の処理を許可し実行する。 • ユーザ BOX 作成、ユーザ BOX 識別子の登録とユーザ BOX パスワードの設定 • 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。	FDP_ACC.1[2] FDP_ACF.1[2] FIA_SOS.1[1] FMT_MSA.1 FMT_MSA.3 FAU_STG.1 FAU_SAR.2 FAU_SAR.1 FMT_SMF.1 FMT_SMR.1 FPT_RVM.1

	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、管理者が参照できる形式で表示する。	
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 文字から 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設定／変更する。規則に従っていない場合、変更を拒否する。	FDP_SOS.1 FDP_MTD.1 FPT_RVM.1

6.2. セキュリティ機能強度

本 TOE は、パスワードメカニズムに対し SOF-基本のセキュリティ機能強度を主張する。該当するパスワードメカニズムは、識別認証機能(IA.ADM_AUTH, IA.CE_AUTH, ACL.USR, IA.ADM_ADD 及び IA.PASS)及び管理支援機能(MNG.ADM 及び MNG.HDD)である。

6.3. 保証手段

開発者は、セキュリティ保証要件及び開発組織が規定した開発規約に従って開発する。EAL3 を満たすセキュリティ保証要件のコンポーネント及び保証要件に対応する関連文書を『表 6.1 EAL3 の保証要件と関連文書』に示す。

表 6.1 EAL3 の保証要件と関連文書

保証要件項目	コンポーネント	関連文書
構成管理	ACM_CAP.3	bizhub PRO 1050 及び 1050P 構成管理書 bizhub PRO 1050 設計文書一覧 bizhub PRO 1050 及び 1050P ソースｺｰﾄﾞ一覧 1 bizhub PRO 1050 及び 1050P ソースｺｰﾄﾞ一覧 2
	ACM_SCP.1	bizhub PRO 1050 及び 1050P 構成管理書 bizhub PRO 1050 設計文書一覧 bizhub PRO 1050 及び 1050P ソースｺｰﾄﾞ一覧 1 bizhub PRO 1050 及び 1050P ソースｺｰﾄﾞ一覧 2

配付と運用	ADO_DEL.1	bizhub PRO 1050 及び 1050P 配布規定書 bizhub PRO 1050 インストールマニュアル bizhub PRO 1050 ユーザーズガイド コピー編 bizhub PRO 1050 ユーザーズガイド POD管理者編 bizhub PRO 1050 ユーザーズガイド ネットワークスキャナ編 bizhub PRO 1050 ユーザーズガイド セキュリティ編 bizhub PRO 1050/1050P サービスマニュアルフィールドサービス bizhub PRO 1050 User’s Guide Copier bizhub PRO 1050 User’s Guide POD Administrator’s Reference bizhub PRO 1050 User’s Guide Network Scanner bizhub PRO 1050 User’s Guide Security bizhub PRO 1050/1050P SERVICE MANUAL Field Service bizhub PRO 1050 INSTALLATION MANUAL

	ADO_IGS.1	bizhub PRO 1050 及び 1050P 導入・運用規定書 bizhub PRO 1050 インストールマニュアル bizhub PRO 1050 ユーザーズガイド コピー編 bizhub PRO 1050 ユーザーズガイド POD管理者編 bizhub PRO 1050 ユーザーズガイド ネットワークスキャナ編 bizhub PRO 1050 ユーザーズガイド セキュリティ編 bizhub PRO 1050/1050P サービスマニュアルフィールドサービス bizhub PRO 1050/1050P SERVICE MANUAL Field Service bizhub PRO 1050 INSTALLATION MANUAL bizhub PRO 1050 User’s Guide Copier bizhub PRO 1050 User’s Guide POD Administrator’s Reference bizhub PRO 1050 User’s Guide Network Scanner bizhub PRO 1050 User’s Guide Security
開発	ADV_FSP.1	bizhub PRO 1050 及び 1050P 機能仕様書
	ADV_HLD.2	bizhub PRO 1050 及び 1050P 機能仕様書
	ADV_RCR.1	bizhub PRO 1050 及び 1050P 機能対応書

ガイダンス文書	AGD_ADM.1	bizhub PRO 1050 インストールマニュアル bizhub PRO 1050 ユーザーズガイド コピー編 bizhub PRO 1050 ユーザーズガイド POD管理者編 bizhub PRO 1050 ユーザーズガイド ネットワークスキャナ編 bizhub PRO 1050 ユーザーズガイド セキュリティ編 bizhub PRO 1050/1050P サービスマニュアルフィールドサービス bizhub PRO 1050 INSTALLATION MANUAL bizhub PRO 1050 User’s Guide Copier bizhub PRO 1050 User’s Guide POD Administrator’s Reference bizhub PRO 1050 User’s Guide Network Scanner bizhub PRO 1050 User’s Guide Security bizhub PRO 1050/1050P SERVICE MANUAL Field Service
	AGD_USR.1	bizhub PRO 1050 ユーザーズガイド コピー編 bizhub PRO 1050 ユーザーズガイド POD管理者編 bizhub PRO 1050 ユーザーズガイド ネットワークスキャナ編 bizhub PRO 1050 ユーザーズガイド セキュリティ編 bizhub PRO 1050 User’s Guide Copier bizhub PRO 1050 User’s Guide POD Administrator’s Reference bizhub PRO 1050 User’s Guide Network Scanner bizhub PRO 1050 User’s Guide Security
ライフサイクルサポート	ALC_DVS.1	bizhub PRO 1050 及び 1050P 開発セキュリティ規定書
テスト	ATE_COV.2	bizhub PRO 1050 及び 1050P 機能テスト書
	ATE_DPT.1	bizhub PRO 1050 及び 1050P 機能分析書

	ATE_FUN.1	bizhub PRO 1050 及び 1050P 機能テスト書
	ATE_IND.2	無し(bizhub PRO 1050 テストセット)
脆弱性評定	AVA_MSU.1	bizhub PRO 1050 及び 1050P 導入・運用規定書 bizhub PRO 1050 インストールマニュアル bizhub PRO 1050 ユーザーズガイド コピー編 bizhub PRO 1050 ユーザーズガイド POD管理者編 bizhub PRO 1050 ユーザーズガイド ネットワークスキャナ編 bizhub PRO 1050 ユーザーズガイド セキュリティ編 bizhub PRO 1050/1050P サービスマニュアルフィールドサービス bizhub PRO 1050 INSTALLATION MANUAL bizhub PRO 1050 User’s Guide Copier bizhubPRO 1050 User’s Guide POD Administrator’s Reference bizhub PRO 1050 User’s Guide Network Scanner bizhub PRO 1050 User’s Guide Security bizhub PRO 1050/1050P SERVICE MANUAL Field Service
	AVA_SOF.1	bizhub PRO 1050 及び 1050P 脆弱性分析書
	AVA_VLA.1	bizhub PRO 1050 及び 1050P 脆弱性分析書

7. PP 主張

本 ST が準拠する PP はない。

8. 根拠

8.1. セキュリティ対策方針根拠

脅威に対応するセキュリティ対策方針の関係を『表 8.1 脅威及び前提条件とセキュリティ対策方針の対応』に示す。

表 8.1 脅威及び前提条件とセキュリティ対策方針の対応

脅威/前提条件/組織のセキュリティ方針 ＼ セキュリティ対策方針	T.HDDACCESS	T.ACCESS	T.IMPADMIN	ASM.PLACE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.USR
O.IA(利用時の識別と認証)	✔	✔	✔					
O.MANAGE(管理機能の提供)	✔		✔					
O.CE(CE 機能の提供)			✔					
O.DATAACCESS(ドキュメントデータへのアクセス制限)		✔	✔					
O.AUDIT(監査情報の記録)	✔	✔	✔					
OE.PLACE(設置場所の管理)				✔				
OE.NET(ネットワークの管理)					✔			
OE.USR(一般利用者の教育)								✔
OE.ADMIN(管理者の条件)						✔		
OE.CE(CE の保証)							✔	
OE.HDD(HDD 自身のアクセス制限)	✔							

以下に、『表 8.1 脅威及び前提条件とセキュリティ対策方針の対応』の根拠を示す。

T.HDDACCESS:HDD への不正なアクセス

TSF は O.IA で識別された正当な管理者により、O.MANAGE の管理機能で HDD1 と HDD2 の HDD

ロックパスワードを変更し、管理する。また、TSF は、O.AUDIT により、管理者の識別・認証の失敗を監査情報として記録するため、管理者以外が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。OE.HDD によって、HDD1、HDD2 は識別・認証を行い、正当な利用者である TOE のみにアクセスを制限するため、不正な HDD1、HDD2 へのアクセスを防止する。以上に示すように、脅威 **T.HDDACCESS** は対策方針 O.IA、O.MANAGE、O.AUDIT 及び OE.HDD によって対抗できる。

T.ACCESS：BOX への不正なアクセス

TSF は O.IA で識別認証したユーザ BOX を所有する正当な一般利用者にのみそのユーザ BOX 内のドキュメントデータへの読み出しを、O.DATAACCESS 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』であるドキュメントデータへのアクセス機能に関する操作を監査情報として記録するため、一般利用者が所有するユーザ BOX の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。以上に示すように、対策方針 O.IA、O.DATAACCESS、及び O.AUDIT で脅威 T.ACCESS に対抗出来る。

T.IMPADMIN：CE、管理者へのなりすまし

TSF は CE を O.IA で識別認証する。TSF は識別認証した正当な CE に O.CE で管理者を決定する機能を提供する。TSF は、決定された管理者を O.IA で識別認証する。TSF は識別認証した正当な管理者に、O.MANAGE でユーザ BOX を管理する機能を提供する。管理者はこの機能を使ってユーザ BOX の所有者を決定する。TSF は O.IA で識別認証したユーザ BOX を所有する正当な一般利用者にのみそのユーザ BOX 内のドキュメントデータの読み出しを、O.DATAACCESS により許可する。また、TSF は、O.AUDIT により、CE、管理者の識別・認証の失敗を監査情報として記録するため、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。

以上に示すように、脅威 T.IMPADMIN は対策方針 O.IA、O.CE、O.MANAGE、O.DATAACCESS および O.AUDIT で対抗出来る。

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

OE.NET では、管理者はドキュメントデータの漏洩が発生しない内部ネットワークに TOE を設置する。内部ネットワークの通信を暗号化する機器で構成することで、実現は可能である。

以上に示すように、前提条件 ASM.NET は対策方針 OE.NET によって実現できる。

ASM.ADMIN：信頼できる管理者

OE.ADMIN では、管理者の条件を規定している。責任者は、不正を行わない人物を管理者に選任する。

以上に示すように、前提条件 ASM.ADMIN は対策方針 OE.ADMIN によって実現できる。

ASM.CE:保守契約

OE.CE では、TOE を導入する組織は、TOE の保守を担当する組織と CE は不正な行為を行わない旨を明記した保守契約を締結することを規定している。以上に示すように、前提条件 ASM.CE は対策方針 OE.CE によって実現できる。

ASM.USR:一般利用者の管理

管理者は OE.USR で一般利用者がユーザ BOX パスワードを他者に漏らさないように教育する。これにより一般利用者は利用者自身のユーザ BOX パスワードを漏らさない。以上に示すように、前提条件 ASM.USR は対策方針 OE.USR によって実現できる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

8.2.1.1. セキュリティ機能要件 FDP_MTD.1 および FDP_SOS.1 の導入理由

要件: IT 環境のセキュリティ機能の制御および IT 環境の秘密の検証を、TOE セキュリティ機能要件で行う。

TSF は、OE.HDD が正しく識別・認証を行えるようにするため、識別・認証に使う HDD ロックパスワードを改変より保護する必要がある。このため、TOE セキュリティ機能要件が必要である。

HDD ロックパスワードは、IT 環境としての HDD の TSF データであると同時に IT 環境の秘密である。これらは、TOE から見ると、利用者データとなる。しかし、IT 環境のセキュリティ機能を制御するデータであるため、実質的には管理者のみが扱う TSF データの特性を持つ。この様なデータを TOE の FMT/FIA クラスでは扱えず、一般利用者に対するアクセス制御の対象でもない。

このデータの管理を FDP_ACC/FDP_ACF で扱うと、これに対応するサブジェクトは管理者だけとなるため、許可条件を書くことができない(常に許可となってしまうため)。

また、HDD ロックパスワードは「IT 環境の秘密」であるため、FIA クラスでは扱えない。

このため、FDP クラスに新たに管理的な特性を持つ機能要件を定義する必要があった。

これらの TOE セキュリティ機能要件は、管理要件 FMT_MTD.1、FIA_SOS.1 に倣って作成した。

8.2.1.2. 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

セキュリティ対策方針に対する TOE セキュリティ機能要件の対応を『表 8.2 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』に示す。

表 8.2 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

セキュリティ対策方針 / IT セキュリティ機能要件		O.IA	O.MANAGE	O.CE	O.DATAACCESS	O.AUDIT	OE.HDD
TOE セキュリティ機能要件	FIA_UID.2	✔					
	FIA_UAU.2	✔					
	FIA_UAU.7	✔					
	FIA_AFL.1	✔					
	FIA_SOS.1[1]	✔	✔				
	FIA_SOS.1[2]		✔	✔			
	FDP_SOS.1		✔				
	FDP_ACC.1[1]				✔		
	FDP_ACC.1[2]		✔				
	FDP_ACF.1[1]				✔		
	FDP_ACF.1[2]		✔				
	FAU_GEN.1					✔	
	FAU_STG.1					✔	
	FAU_STG.4					✔	
	FAU_SAR.1					✔	
	FAU_SAR.2					✔	
	FMT_MTD.1[1]			✔			
	FMT_MTD.1[2]			✔			
	FMT_MTD.1[3]		✔				
	FMT_MTD.1[4]	✔					
	FMT_MTD.1[5]		✔				
	FMT_MSA.1		✔				
	FMT_MSA.3		✔				

	FMT_SMR.1	✔	✔	✔	✔		
	FMT_MOF.1	✔	✔	✔	✔	✔	
	FPT_RVM.1	✔	✔	✔	✔	✔	
	FMT_SMF.1	✔	✔	✔	✔		
	FPT_STM.1					✔	
	FDP_MTD.1		✔				
IT 環境のセキュリティ機能要件	FIA_UID.2[E]						✔
	FIA.UAU.2[E]						✔

以下に、『表 8.2 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』の根拠を示す。

O.IA：利用時の識別と認証

CE であることを FIA_UID.2 で識別し、CE 本人であることを FIA_UAU.2 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 で識別し、管理者本人であることを FIA_UAU.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。

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 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 で認証することで、正当なそのユーザ 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 で管理者、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。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。

認証したユーザ BOX を所有する正当な一般利用者に対し、その一般利用者が所有するユーザ BOX のユーザ BOX パスワードの変更を FMT_MTD.1[4]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[1]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 BOX を所有している一般利用者を FMT_SMR.1 で維持する。以上の機能は FPT_RVM.1 によりバイパスされることなく、FMT_MOF.1 によって有効に動作する状態になる。

従って、対応するセキュリティ機能要件により対策方針 O.IA は実現可能である。

O.MANAGE：管理機能の提供

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。当初、だれも利用出来ないユーザ BOX パスワードが設定された状態でユーザ BOX はその利用を制限されているが、FMT_MTD.1[3]が管理者にユーザ BOX パスワードの変更を許可することで、利用可能となる。以降、一般利用者はこのユーザ BOX のユーザ BOX 識別子を知ることでそのユーザ BOX の所有者となる。また、ユーザ BOX パスワードを登録する場合は、FIA_SOS.1[1]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。

FDP_MTD.1 は管理者に、HDD1、HDD2 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。これにより、HDD1、HDD2 の不正アクセスを防ぐことができる。このパスワードは、FDP_SOS.1 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[5]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。パスワードが変更されることで、一般利用者から入力した管理者パスワードが一致する可能性を低くする。

ユーザ BOX 識別子、ユーザ BOX パスワード、HDD1、HDD2 のロックパスワードの管理を FMT_SMF.1 で特定する。管理者、CE、及び対象のユーザ BOX を所有している一般利用者を FMT_SMR.1 で維持する。以上の機能は FPT_RVM.1 によりバイパスされることはない。また、FMT_MOF.1 で管理者に、セキュリティ機能の起動／停止を許可する。

従って、対応するセキュリティ機能要件により O.MANAGE は実現可能である。

O.CE：CE 機能の提供

CE は管理者のパスワードを FMT_MTD.1[1]で登録出来る。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[2]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。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[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一般利用者が入力した 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 で維持する。以上の機能は FPT_RVM.1 によりバイパスされることはなく、FMT_MOF.1 で有効に動作する状態になる。

従って、対応するセキュリティ機能要件により O.CE は実現可能である。

O.DATAACCESS：ドキュメントデータへのアクセス制限

FDP_ACC.1[1]と FDP_ACF.1[1]を使ってユーザ BOX へのアクセス制御を実現する。O.DATAACCESS は利用者受付機能(サブジェクト)に、ユーザ BOX を所有する正当な一般利用者が所有するユーザ BOX 内の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。以上により、そのユーザ BOX を所有している一般利用者のみがユーザ BOX 内のドキュメントデータを操作可能となる。

対象のユーザ BOX を所有している一般利用者を FMT_SMR.1 で維持する。ユーザ BOX 識別子の管

理を FMT_SMF.1 で特定する。以上の機能は FPT_RVM.1 によりバイパスされることはなく、FMT_MOF.1 で有効に動作する状態になる。

従って、対応するセキュリティ機能要件により O.DATAACCESS は実現可能である。

O.AUDIT：監査情報の記録

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 FPT_RVM.1 によりバイパスされることなく、FMT_MOF.1 で有効に動作する状態になる。以上により必要な監査情報は格納される。

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。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により O.AUDIT は実現可能である。

OE.HDD：HDD の保護

FIA_UID.2[E]、FIA_UAU.2[E]は、HDD1、HDD2 に識別・認証に成功した TOE にのみアクセスを許可する。これにより、HDD1、HDD2 は不正なアクセスを防止できる。

従って対応するセキュリティ機能要件により、OE.HDD は実現可能である。

8.2.1.3. 保証要件がセキュリティ機能要件　FDP_MTD.1、FDP_SOS.1 をサポートすることの適切性

FDP_MTD.1 は、FMT_MTD.1 の『TSF データ』を『管理者データ』に変更するだけで、意味的には、『セキュリティ機能を制御する』 FMT_MTD.1 と同じである。また、FDP_SOS.1 は、FIA_SOS.1 の『秘密』を『IT 環境の秘密』に変更するだけで、意味的には、『秘密の検証』 FIA_SOS.1 と同じである。
よって、FMT_MTD.1、FIA_SOS.1 と同じ保証要件、すなわち、今の保証要件で対応できる。

8.2.2. TOE セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間の依存関係は『表 8.3 TOE セキュリティ機能要件間の依存関係』に示すように、すべての必要な依存関係を満たしている。

表 8.3 TOE セキュリティ機能要件間の依存関係

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
1	FIA_UID.2	FIA_UID.1	なし		
2	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	なし	FIA_UID.1 の調停アクションが不要のため、FIA_UID.2 を利用している。
3	FIA_UAU.7	なし	FIA_UAU.1	なし	FIA_UAU.1 の調停アクションが不要のため、FIA_UAU.2 を利用している。
4	FIA_AFL.1	なし	FIA_UAU.1	なし	FIA_UAU.1 の調停アクションが不要のため、FIA_UAU.2 を利用している。
5	FIA_SOS.1[1]	なし	なし		
6	FIA_SOS.1[2]	なし	なし		
7	FDP_SOS.1	なし	なし		
8	FDP_ACC.1[1]	なし	FDP_ACF.1	10	
9	FDP_ACC.1[2]	なし	FDP_ACF.1	11	
10	FDP_ACF.1[1]	なし	FDP_ACC.1 FMT_MSA.3	8 なし	FMT_MSA.3 については、同一のオブジェクトに対するアクセス制御である FDP_ACF.1[2]の依存関係で満たされている。
11	FDP_ACF.1[2]	なし	FDP_ACC.1 FMT_MSA.3	9 23	
12	FAU_GEN.1	なし	FPT_STM.1	28	
13	FAU_STG.1	なし	FAU_GEN.1	12	
14	FAU_STG.4	FAU_STG.3	FAU_STG.1	13	
15	FAU_SAR.1	なし	FAU_GEN.1	12	

16	FAU_SAR.2	なし	FAU_SAR.1	15	
17	FMT_MTD.1[1]	なし	FMT_SMR.1 FMT_SMF.1	26 25	
18	FMT_MTD.1[2]	なし	FMT_SMR.1 FMT_SMF.1	26 25	
19	FMT_MTD.1[3]	なし	FMT_SMR.1 FMT_SMF.1	26 25	
20	FMT_MTD.1[4]	なし	FMT_SMR.1 FMT_SMF.1	26 25	
21	FMT_MTD.1[5]	なし	FMT_SMR.1 FMT_SMF.1	26 25	
22	FMT_MSA.1	なし	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	9 26 25	
23	FMT_MSA.3	なし	FMT_MSA.1 FMT_SMR.1	22 26	
24	FMT_MOF.1	なし	FMT_SMR.1 FMT_SMF.1	26 25	
25	FMT_SMF.1	なし	なし		
26	FMT_SMR.1	なし	FIA_UID.1	なし	FIA_UAU.1 の調停アクションが不要のため、FIA_UAU.2 を利用している。
27	FPT_RVM.1	なし	なし		
28	FPT_STM.1	なし	なし		
29	FDP_MTD.1	なし	FMT_SMR.1 FMT_SMF.1	26 25	
30	FIA_UID.2[E]	FIA_UID.1	なし		
31	FIA_UAU.2[E]	FIA_UAU.1	FIA_UID.2[E]	30	FIA_UID.1 の調停アクションが不要のため、FIA_UID.2 を利用している。

8.2.3. TOE セキュリティ機能要件の相互作用

No	TOE セキュリティ 機能要件	防御を提供している機能	
		迂回	非活性化
1	FIA_UID.2	FPT_RVM.1	FMT_MOF.1
2	FIA_UAU.2	FPT_RVM.1	FMT_MOF.1
3	FIA_UAU.7	FPT_RVM.1	FMT_MOF.1
4	FIA_AFL.1	FPT_RVM.1	FMT_MOF.1
5	FIA_SOS.1[1]	なし	FMT_MOF.1
6	FIA_SOS.1[2]	なし	FMT_MOF.1
7	FDP_SOS.1	なし	FMT_MOF.1
8	FDP_ACC.1[1]	FPT_RVM.1	FMT_MOF.1
9	FDP_ACC.1[2]	FPT_RVM.1	FMT_MOF.1
10	FDP_ACF.1[1]	FPT_RVM.1	FMT_MOF.1
11	FDP_ACF.1[2]	FPT_RVM.1	FMT_MOF.1
12	FAU_GEN.1	FPT_RVM.1	FMT_MOF.1
13	FAU_STG.1	FPT_RVM.1	FMT_MOF.1
14	FAU_STG.4	FPT_RVM.1	FMT_MOF.1
15	FAU_SAR.1	FPT_RVM.1	FMT_MOF.1
16	FAU_SAR.2	FPT_RVM.1	FMT_MOF.1
17	FMT_MTD.1[1]	FPT_RVM.1	FMT_MOF.1
18	FMT_MTD.1[2]	FPT_RVM.1	FMT_MOF.1
19	FMT_MTD.1[3]	FPT_RVM.1	FMT_MOF.1
20	FMT_MTD.1[4]	FPT_RVM.1	FMT_MOF.1
21	FMT_MTD.1[5]	FPT_RVM.1	FMT_MOF.1
22	FMT_MSA.1	FPT_RVM.1	FMT_MOF.1
23	FMT_MSA.3	FPT_RVM.1	FMT_MOF.1
24	FMT_MOF.1	FPT_RVM.1	
25	FMT_SMF.1	なし	FMT_MOF.1
26	FMT_SMR.1	なし	FMT_MOF.1
27	FPT_RVM.1		FMT_MOF.1
28	FPT_STM.1	なし	なし
29	FDP_MTD.1	FPT_RVM.1	FMT_MOF.1

【迂回】　FPT_RVM.1

TOE の管理機能及び CE 機能を使用するにあたり、管理者及び CE は識別認証(FIA_UID.2、

FIA_UAU.2、FIA_UAU.7、FIA_AFL.1)を実施する。

ユーザ BOX のドキュメントデータは、アクセス制御(FDP_ACC.1[1][2]と FDP_ACF.1[1][2])を元にアクセスされる。

監査データは必ず採取される。(FAU_GEN.1、FAU_STG.4)

監査データの参照は管理者のみ可能である。(FAU_SAR.1、FAU_SAR.2、FAU_STG.1)

各種 TSF データおよび管理者データの操作は各データに対応する利用者にのみ可能である。(FAU_SAR.2、FMT_MTD.1[1]～[5]、FMT_MSA.1、FMT_MSA.3、FMT_MOF.1、FDP_MTD.1)

FPT_RVM.1 により、以上が確実に実行されるため、迂回を防止する。

【非活性化】 FMT_MOF.1

FMT_MOF.1 によりセキュリティ強化モードを有効にすることで、TSF の非活性化防止が実現されている。

【改ざん】

本 TOE では、アクセス制御は、HDD1 のユーザ BOX に対するもののみである。
ユーザ BOX に対するアクセス制御は、操作パネル経由のプロセスに限定されるため、不正なサブジェクトは存在しない。よって、不正なサブジェクトの入り込む余地はないため、FPT_SEP.1 は不要である。

8.2.4. セキュリティ対策方針に対するセキュリティ機能強度の一貫性

本 TOE は、「2.TOE 記述」で一般利用者の攻撃能力について、低レベルであることを想定しており、「3.TOE セキュリティ環境」で、「操作パネルから操作する。」か「不正な読み出し装置を HDD に接続する。」と記述しており、特にスキルの高い攻撃者を想定していない。また、物理的な面と人的な面で十分なセキュリティを確保した条件下で運用されることを想定している。このため、セキュリティ強度は、低レベルの攻撃能力を要する脅威エージェントからの攻撃に対して、十分に対抗できる SOF-基本を 『5.3. セキュリティ強度』で主張している。

以下に、本 TOE を安全に動作させるための運用対策を示す。

- TOE を、製品関係者のみが操作可能な区画に設置する。
- 管理者は内部ネットワークからデータが漏洩しない環境を設定する。
- 管理者は一般利用者に対して TOE がセキュアな状態を維持するための教育及び啓蒙を実施する。
- 責任者は、不正を行わない人物を管理者として選任し管理する。
- 責任者又は管理者は、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。

よって、脅威エージェントを以下の人物に特定できる。

攻撃能力 : 低レベル

以上により、上記の攻撃能力を有した脅威エージェントに対して十分な対抗性があることからセキュリティ対策方針に対する最小機能強度として SOF-基本が適切であり、一貫している。

8.2.5. 保証要件根拠

本 TOE は、商用利用される製品であり、低レベルの攻撃能力を有する脅威に対抗するために、TOE の機能と外部インタフェースの仕様、開発者テストの結果、明らかな脆弱性に対する開発者の分析及び機能強度分析などが必要となる。したがって、評価保証レベルは EAL3 が妥当である。

8.3. TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応』に示す。

表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応

IT セキュリティ機能 / TOE セキュリティ機能要件	IA・ADM_ADD	IA・ADM_AUTH	IA・CE_AUTH	IA・PASS	ACL・USR	AUD・LOG	AUD・MNG	MNG・MODE	MNG・ADM	MNG・HDD
FIA_UID.2		✔	✔		✔					
FIA_UAU.2		✔	✔		✔					
FIA_UAU.7		✔	✔		✔					
FIA_AFL.1		✔	✔		✔					
FIA_SOS.1[1]				✔					✔	
FIA_SOS.1[2]	✔			✔						
FDP_SOS.1										✔
FDP_ACC.1[1]					✔					
FDP_ACC.1[2]									✔	
FDP_ACF.1[1]					✔					
FDP_ACF.1[2]									✔	
FAU_GEN.1						✔				
FAU_STG.1									✔	
FAU_STG.4							✔			
FAU_SAR.1									✔	
FAU_SAR.2									✔	
FMT_MTD.1[1]	✔			✔						

FMT_MTD.1[2]				✔						
FMT_MTD.1[3]				✔						
FMT_MTD.1[4]				✔						
FMT_MTD.1[5]				✔						
FMT_MSA.1									✔	
FMT_MSA.3									✔	
FMT_MOF.1								✔		
FMT_SMF.1	✔			✔					✔	
FMT_SMR.1	✔			✔					✔	
FPT_RVM.1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
FPT_STM.1						✔				
FDP_MTD.1										✔

以下に、『表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応』の根拠を示す。

FIA_UID.2

管理者に対しては IA.ADM_AUTH で管理者の識別を実施する。CE に対しては IA.CE_AUTH で CE の識別を実施する。ユーザ BOX を所有している一般利用者に対しては ACL.USR でユーザ 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、IA.ADM_AUTH、IA.CE_AUTH 及び ACL.USR を実装することで FIA_UID.2 を実現できる。

FIA_UAU.2

管理者に対しては IA.ADM_AUTH で、管理者の認証を実施する。CE に対しては IA.CE_AUTH で、CE の認証を実施する。ユーザ BOX を所有している一般利用者に対しては ACL.USR でユーザ BOX を所有している一般利用者の認証を実施できる。

以上により、IA.ADM_AUTH、IA.CE_AUTH 及び ACL.USR を実装することで FIA_UAU.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、及びユーザ BOX を所有している一般利用者の認証のためのパスワード入力時は ACL.USR で、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 及び ACL.USR を実装することで FIA_UAU.7 を実現できる。

FIA_SOS.1[1]

ユーザ BOX パスワードの登録に対しては MNG.ADM で、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、MNG.ADM 及び 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 で、管理者パスワード及び 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.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。

FDP_SOS.1

FDP_SOS.1 は、ハードディスクのパスワード登録に対して MNG_HDD で、パスワード規則に従った許容値の範囲であるか判定している。

以上により、MNG_HDD を実装することで、FDP_SOS.1 を実現できる。

FIA_AFL.1

管理者に対しては IA.ADM_AUTH で、CE に対しては IA.CE_AUTH で、ユーザ BOX を所有している一般利用者に対しては、ACL.USR で認証の不成功時に、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、次の認証試行を 5 秒間実行しない。

以上により、IA.ADM_AUTH、IA.CE_AUTH 及び ACL.USR を実装することで、FIA_AFL.1 を実現できる。

FDP_ACC.1[1]

ACL.USR では、アクセス制御方針 1 に基づき、ドキュメントデータの読み出しを実行する。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_ACC.1[2]

MNG.ADM はアクセス制御方針 2 に基づき、ユーザ BOX の作成を行う。

以上により、MNG.ADM を実装することで FDP_ACC.1[2]を実現できる。

FDP_ACF.1[1]

ACL.USR では、アクセス制御方針 1 に基づき、ドキュメントデータの読み出しを実行する。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_ACF.1[2]

MNG.ADM はアクセス制御方針 2 に基づき、ユーザ BOX の作成を行う。

以上により、MNG.ADM を実装することで FDP_ACF.1[2]を実現できる。

FAU_GEN.1

セキュリティ機能の動作に関する監査情報を AUD.LOG で記録する。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.1

監査格納領域内データを管理者のみアクセスができる機能を MNG.ADM で実装する。

以上により、MNG.ADM を実装することで FAU_STG.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。

FAU_SAR.1

監査記録を MNG_ADM で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

管理者のみが監査記録を参照できるように MNG.ADM で制限する。

以上により、MNG.ADM を実装することで FAU_SAR.2 を実現できる。

FMT_MTD.1[1]

管理者のパスワードの登録を IA.ADM_ADD で、また変更を IA.PASS で CE にのみ許可し実行する。

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

FMT_MTD.1[2]

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[2]を実現できる。

FMT_MTD.1[3]

ユーザ BOX パスワードの変更を MNG.ADM で管理者に許可し実行する。

以上により、MNG.ADM を実装することで FMT_MTD.1[3]を実現できる。

FMT_MTD.1[4]

ユーザ BOX パスワードの変更を IA.PASS でユーザ 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[4]を実現できる。

FMT_MTD.1[5]

管理者パスワードの変更を IA.PASS で管理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[5]を実現できる。

FMT_MSA.1

ユーザ BOX 生成のためにユーザ BOX 識別子の登録を MNG.ADM で管理者のみに許可し実行する。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_MSA.3

ユーザ BOX の初期化に必要なユーザ BOX へのユーザ BOX 識別子の登録とユーザ BOX パスワードの設定を MNG.ADM で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、ユーザ BOX パスワードを設定することで一般利用者が利用可能な状態となる。

以上により、MNG.ADM を実装することで FMT_MSA.3 を実現できる。

FMT_MOF.1

本 ST で規定したセキュリティ機能の有効の設定を MNG.MODE で管理者に許可し実行する。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_SMF.1

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

FMT_SMR.1

ユーザ BOX 識別子とユーザ BOX パスワードの 登録と、CE と管理者のパスワードとユーザ BOX パスワードの変更を実現することで役割の維持を実現する。管理者の登録を IA.ADM_ADD、ユーザ BOX を所有する一般利用者の登録を MNG.ADM、管理者と CE とユーザ BOX パスワードの変更を IA.PASS で実装する。以上により、IA.ADM_ADD、IA.PASS 及び MNG.ADM を実装することで FMT_SMR.1 を実現できる。

FPT_STM.1

監査記録を生成する機能を AUD.LOG で実現する。これにより AUD.LOG の実装で FPT_STM.1 を実装できる。

FDP_MTD.1

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 FDP_MTD.1 を実装できる。

8.3.2. セキュリティ機能強度根拠

『6.2 セキュリティ機能強度』で述べたように、識別認証機能(IA.ADM_AUTH、IA_CE_AUTH、ACL_USR、IA_ADM_ADD及びIA.PASS) 及び管理支援機能(MNG.ADM及びMNG_HDD)のパスワードメカニズムにおいて、SOF-基本を主張する。『5.3. セキュリティ強度』で述べたようにセキュリティ機能要件に対して最小機能強度は SOF-基本を主張しており、『6.2 セキュリティ機能強度』で主張する SOF-基本と一貫している。

8.3.3. 保証手段根拠

『6.3 保証手段』において、EAL3 で必要とするすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段に示す関連規約によって、本 ST が規定した TOE セキュリティ保証要件が要求する証拠を網羅している。

したがって、EAL3 における TOE セキュリティ保証要件を実現できる。

8.4. PP 主張根拠

本 ST が準拠する PP はない。