Multi functional printer (digital copier) 7222/7322/7228/7235 シリーズ セキュリティターゲット 第10版

2004年3月24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 -

改訂番号	改訂内容	承認者	審査者	作成者
1	・ 新規作成	2003/11/28 北本浩一	2003/11/28 伊藤　丘	2003/11/28 小田昭彦
2	・ Scan to PC(SMB)機能の追加に伴う追記と誤記修正 ・ 2 章：図 2.2 を修正(ユーザ BOX を TOE に含める) ・ 2 章:書き込み機能の説明を修正 ・ 3 章：T.ACCESS を修正 ・ 4 章：O.RESIDUAL を削除、 ・ 4 章:O.DATAACCESS を修正 ・ 5 章:FDP_ACC.1、FAU_GEN.1、FMT_MOF.1[2]、FMT_MOF.1[3]を修正 ・ 5 章：FMT_MTD.1[1]を削除、FMT_MTD.1[2]と FMT_MTD.1[3] を FMT_MTD.1[1] と FMT_MTD.1[2]に修正 ・ 5 章：FMT_SMR.1 を削除 ・ 6 章:上記の修正の反映 ・ ・ 8 章:上記の修正の反映	2004/1/5 北本浩一	2004/1/5 伊藤　丘	2003/12/26 小田昭彦
3	・ 2 章：図 2.2 と図 2.3 を修正(ユーザ BOX のハッチをはずす、ユーザ BOX とドキュメントデータファイルを複数図示する) ・ 2 章：ユーザ BOX とドキュメントデータファイルが複数存在可能であることを追加 ・ 2 章:TOE の機能を修正 ・ 2 章:CE 機能に ISW 機能を追加 ・ 3 章：ASM.NET、ASM.SECMODE、OSP.MANAGE を追加 ・ 3 章：T.ACCESS を修正 ・ 4 章：OE.NET、OE.SECMODE を追加 ・ 4 章：O.DATAACCESS、O.CE と O.AUDIT を修	2004/2/6 北本浩一	2004/2/6 伊藤　丘	2004/2/6 小田昭彦

	正 ・ 5 章 : FIA_SOS.1 の秘密を詳細化 ・ 5 章:FIA_UID.2 と FIA_UAU.2 の利用者を詳細化 ・ 5 章:FMT_MSA.3 のセキュリティ属性を詳細化 ・ 5 章 :FMT_SMR.1 、 FMT_MTD.1[3][4] と FPT_SEP.1 を追加 ・ 5 章:FMT_MSA.1[2]を削除 ・ 5 章 : FDP_ACF.1.2 と FAU_GEN.1.1 修正 ・ 5 章:FMT_MOF.1[1][2]を削除 FMT_MOF.1[3] を FMT_MOF.1 に変更と FMT_MOF.1 を修正 ・ 5 章 : FMT_SMF.1 の管理項目を修正 ・ 6 章 : IA.ADM_ADD, IA_ADM_AUTH, IA.CE_AUTH, IA.PASS, ACL.USR, RD.TEMP, AUD.LOG, MNG_MODE, MNG.ADM 修正 ・ 8 章:上記の修正の反映 （以上、所見報告書 ASE-001-01～ASE-005-01 の指摘に対しての修正対応） ・ 表 6.1 の関連文書名を実際の文書名称へ修正 ・ 所見報告書 ASE-006-01 の指摘に対して、表 2.1 欄から SMB の説明を削除し、2.2 の用語説明に改めて記載 ・ 所見報告書 ASE-007-01 の指摘に対して、6.1.2 アクセス制御のセキュリティ機能群に PC(SMB)機能を記載			
4	・ TOE の正式名称を確認し、関連箇所の修正 ・ TOE へ海外名称を追記	2004/2/6 北本浩一	2004/2/6 伊藤　丘	2004/2/6 小田昭彦
5	・ 2 章 TOE の範囲に関する記述を修正 ・ 2 章 管理機能より 一般利用者の登録/削除を削除 ・ 3 章 OSP.RIP を追加 ・ 4 章 O.RIP を追加 ・ 5 章 FDP_ACC.1[2]、FDP_ACF.1[2]を追加 ・ 5 章 ドキュメントデータファイル識別子を	2004/2/18 北本浩一	2004/2/18 伊藤　丘	2004/2/18 小田昭彦

	削除 ・ 8.3.1　FMT_MSA.1[3]、FMT_MSA.1[4]の項目を削除			
6	・ 所見報告書 ASE-010-01 に対して、「1.2 項 ST 概説」の中で、TOE 名称と搭載シリーズ機器の説明を追加 ・ 図 2.2 の修正（ハッチ箇所の説明追加）	2004/2/24 北本浩一	2004/2/24 伊藤　丘	2004/2/24 小田昭彦
7	・ 6.3 保証手段にガイダンス資料(英語版)を追加 ・ 6.1.5　MNG.MODE を修正 ・ 誤記修正	2004/3/11 北本浩一	2004/3/11 伊藤　丘	2004/3/11 小田昭彦
8	・ 所見報告書 ASE-011-01 に対して、TOE セキュリティ環境記述の追加を実施 ・ 所見報告書 ASE-012-01 に対して、TOE セキュリティ環境記述の追加を実施	2004/3/16 北本浩一	2004/3/16 伊藤　丘	2004/3/16 小田昭彦
9	・ FMT_MSA.3.1 の詳細化についての記述追加と、8.3.3 文章の文末を修正を実施	2004/3/23 北本浩一	2004/3/23 伊藤　丘	2004/3/23 小田昭彦
10	・ 誤記修正	2004/3/24 北本浩一	2004/3/24 伊藤　丘	2004/3/24 小田昭彦

- 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) 7222/7322/7228/7235 シリーズ セキュリティターゲット
バージョン：	第 10 版
作成日：	2004 年 3 月 24 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：	国内：7222/7322/7228/7235 全体制御ソフトウェア 海外：7222/7228/7235 control software
バージョン：	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

7222/7322/7228/7235 全体制御ソフトウェアと 7222/7228/7235 control software は名称が異なるだけで同一物である（後者に 7322 が除かれているのは、7322 は海外仕向けが無いためである)。以降 TOE の名称を 7222/7322/7228/7235 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 7222 シリーズ、7222 series、7322 シリーズ、7228 シリーズ、7228 series、7235 シリーズ、7235 series（以下、以上の 7 種類の搭載製品シリーズを総称して「7222/7322/7228/7235 シリーズ」と呼ぶ) に搭載する「 7222/7322/7228/7235 全体制御ソフトウェア」について記述している。

7222/7322/7228/7235 全体制御ソフトウェアは、コピー/プリント/スキャナ/FAX を活用し

た機能(コピー機能、プリンタ機能、FAX 機能、Scan to FTP 機能、Scan to Email 機能、Scan to PC(SMB)機能、PC-FAX 保存機能、i-FAX 機能)を有する。TOE は、7222/7322/7228/7235 全体制御ソフトウェアである。TOE の機能が取り扱う資産は、ドキュメントデータである。

1.3. CC 適合

パート 2 適合

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、7222/7322/7228/7235 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、7222/7322/7228/7235 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、7222/7322/7228/7235 全体制御ソフトウェア全体である。TOE を搭載する 7222/7322/7228/7235 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/プリント/スキャナ/FAX を活用した機能、7222/7322/7228/7235 シリーズを運用管理するための機能及び 7222/7322/7228/7235 シリーズを保守管理するための機能を提供する。

7222/7322/7228/7235 シリーズの利用環境として『
図 **2.1** 7222/7322/7228/7235 シリーズの利用環境』に示すオフィスを想定する。

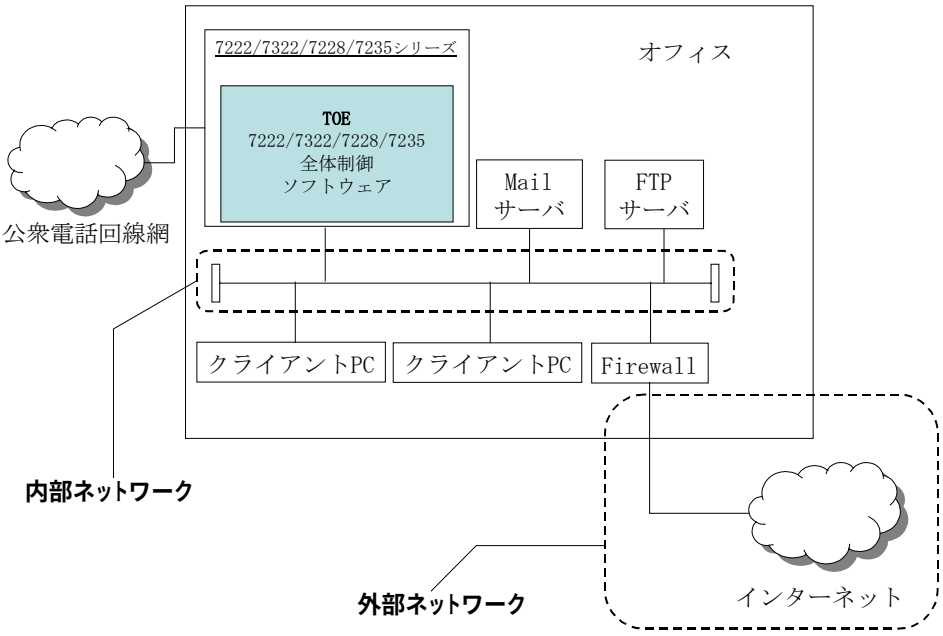

図 2.1 **7222/7322/7228/7235 シリーズの利用環境**

TOE は、内部ネットワークや公衆電話回線網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 7222/7322/7228/7235 シリーズは、『
図 **2.1** 7222/7322/7228/7235 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 7222/7322/7228/7235 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. 7222/7322/7228/7235 シリーズの関連者と役割

7222/7322/7228/7235 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、7222/7322/7228/7235 シリーズを導入する組織に在籍し、7222/7322/7228/7235 シリーズのコピー/プリント/スキャナ/FAX に関する機能を利用する。特に TOE に登録することで、7145 シリーズの HDD オプション上に存在するユーザ BOX を所有することが出来る。

- 管理者

  管理者は、7222/7322/7228/7235 シリーズを導入する組織に在籍し、7222/7322/7228/7235 シリーズの運用管理を行う。7222/7322/7228/7235 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、7222/7322/7228/7235 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、7222/7322/7228/7235 シリーズの保守を委託されている企業に在籍する。CE は 7222/7322/7228/7235 シリーズが提供する保守管理の機能を利用し、7222/7322/7228/7235 シリーズの保守作業を行う。責任者又は管理者と 7222/7322/7228/7235 シリーズの保守契約を締結している。
- FAX 利用者

  FAX 利用者は、公衆電話回線網に接続している FAX 機器を利用し、7222/7322/7228/7235 シリーズにドキュメントデータを送信する。

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。

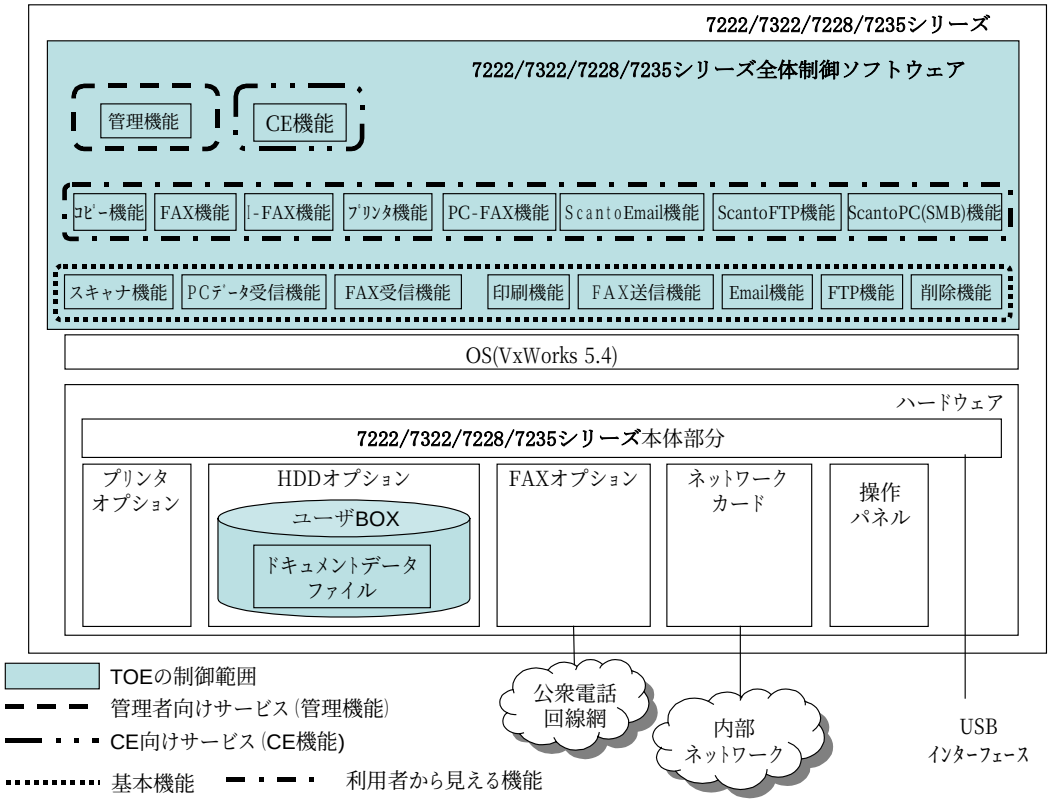

図 2.2 TOE の構成

7222/7322/7228/7235 シリーズは、ハードウェア、OS 及び 7222/7322/7228/7235 全体制御ソフトウェアから構成される。ハードウェアは、7222/7322/7228/7235 シリーズ本体部分、プリンタオプション、HDD オプション、FAX オプション、操作パネル及びネットワークカードである。7222/7322/7228/7235 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を搭載している。USB インタフェースは、TOE の設置生成を行う際にコンピュータと接続するためのインタフェースである。プリンタオプションは、印刷用の紙に文字や図形を印刷する。HDD オプションには記憶装置が存在する。FAX オプションは、公衆電話回線網に接続可能な公衆電話回線ポート及びアナログ信号とデジタル信号を変換するモデムを装備する。OS には、VxWorks 5.4 を使用する。7222/7322/7228/7235 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 7222/7322/7228/7235 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。

HDD オプションの記憶装置上には、7222/7322/7228/7235 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 7222/7322/7228/7235 シリーズ上に複数作成することが出来る。ドキュメントデータファイルはユーザ 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。

7222/7322/7228/7235 シリーズは、FAX 利用者や CE による公衆電話回線網経由の処理要求、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る。TOE の機能は処理要求を処理する。

2.6.　7222/7322/7228/7235 全体制御ソフトウェアの機能構成

7222/7322/7228/7235 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

基本機能は、一般利用者及び FAX 利用者がユーザ BOX 内に存在するドキュメントデータファイルに格納された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。基本機能の概念を『図 2.3 基本機能の処理概念』に示す。

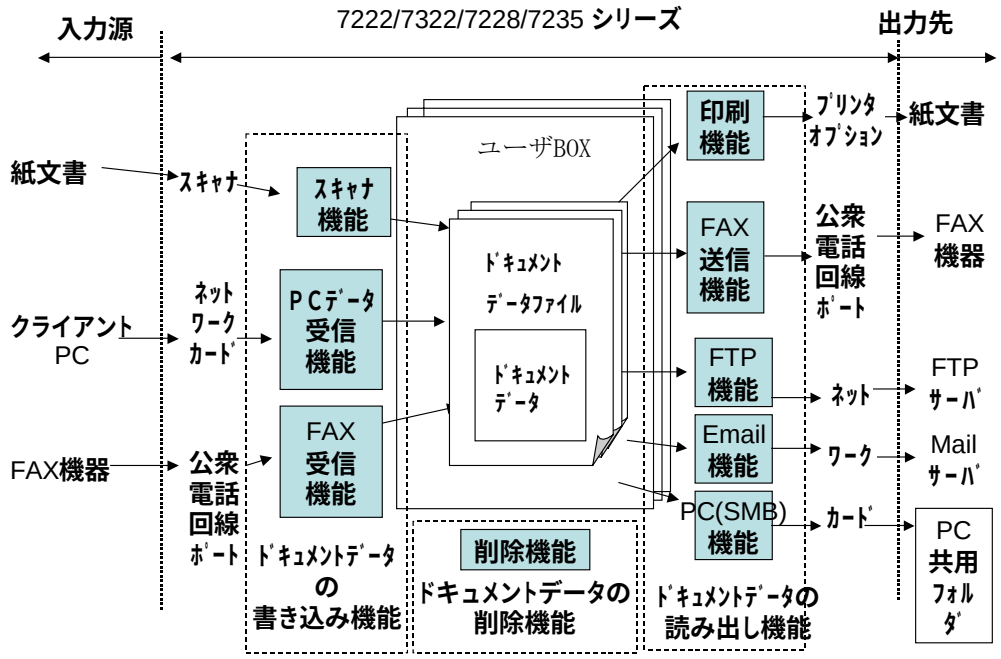

図 2.3 基本機能の処理概念

基本機能は、ドキュメントデータの書き込み、ドキュメントデータの読み出し及びドキュメントデータの削除である。

『表 2.1 利用者から見える機能と基本機能の対応』に示すとおり、利用者から見える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 利用者から見える機能と基本機能の対応

No	利用者から見える機能	基本機能
1	コピー機能	スキャナ機能と印刷機能
2	FAX 機能	スキャナ機能と FAX 送信機能、FAX 受信機能と印刷機能
3	i-FAX 機能	PC データ受信機能と Email 機能
4	プリンタ機能	PC データ受信機能と印刷機能
5	PC-FAX 機能	PC データ受信機能と FAX 送信機能
6	Scan to Email 機能	スキャナ機能と Email 機能
7	Scan to FTP 機能	スキャナ機能と FTP 機能
8	Scan to PC(SMB)機能	スキャナ機能と PC(SMB)機能
9	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』に示したユーザ BOX を利用する機能を以下に述べる。

2.6.1.1. ドキュメントデータの書き込み機能

本機能はユーザ BOX に以下の 3 つの方法でドキュメントデータを追加書き込み(上書きはできない)する。

(1) スキャナ機能

一般利用者は操作パネルから指示を入力し、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、ユーザ BOX に追加保存する。

(2) PC データ受信機能

一般利用者は、クライアント PC から指示を入力し内部ネットワーク経由でドキュメントデータをユーザ BOX に追加保存する。

(3) FAX 受信機能

FAX 利用者は、公衆電話回線網に繋がる FAX 機器からドキュメントデータを、ユーザ BOX に追加保存する。

2.6.1.2. ドキュメントデータの読み出し機能

本機能はユーザ BOX から自分で登録したドキュメントデータを他人からの出力処理から保護しながら以下の 5 つの方法で読み出す処理をする。本機能は操作パネルからのみ可能である。

(1) 印刷機能

一般利用者は操作パネルからユーザ BOX 識別子とユーザ BOX パスワードを入力し、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みを印刷する。

(2) FAX 送信機能

一般利用者は操作パネルからユーザ BOX 識別子とユーザ BOX パスワードを入力し、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みを公衆電話回線網に繋がる FAX 機器に送信する。

(3) Email 機能

一般利用者は操作パネルよりユーザ BOX 識別子とユーザ BOX パスワードを入力し、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みをメールに添付し Mail サーバに送信する。

(4) FTP 機能

一般利用者は操作パネルよりユーザ BOX 識別子とユーザ BOX パスワードを入力し、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みを FTP サーバに送信する。

(5) PC(SMB)機能

一般利用者は操作パネルよりユーザ BOX 識別子とユーザ BOX パスワードを入力し、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みを内部ネットワークに接続されている PC の共用フォルダに送信する。

2.6.1.3. ドキュメントデータの削除機能

一般利用者は、ユーザ BOX 識別子とユーザ BOX パスワードを入力し、一般利用者自身のユーザ BOX に格納されたドキュメントデータのみを削除することができる。本機能は操作パネルからのみ可能である。

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可能である。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、HDD の初期化処理、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。

- KRDS

  CE は公衆回線網に接続したコンピュータから操作し、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。なお、KRDS は、CCITT T.30 で規定された FAX 転送の国際標準規約 G3 に準拠した手順により通信を行う。

- ISW

  CE は 7222/7322/7228/7235 シリーズに USB インタフェースで接続したコンピュータから操作し、TOE を更新するための初期設定を行う。

2.7. 保護対象となる資産

TOE の保護対象となる資産を以下に示す。

- ユーザ BOX 内に格納されているドキュメントデータ

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、内部ネットワークに接続されていて、製品関係者のみが利用可能な物理的に保護された区画に設置される。

ASM.PHYSICAL　　筐体の保護

ドキュメントデータが格納される HDD は、CE しか取り外せない。

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、TOE を管理するための十分な管理スキルと信頼性を備えた人物であり、不正な行為を行わない。

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

管理者は、一般利用者にセキュリティ上、正しい操作を促すよう管理を行う。

ASM.SECMODE　セキュリティ機能の実行

管理者はセキュリティ機能を常に動作させる。

3.2. 脅威

T.ACCESS　　不正なアクセス

一般利用者が、操作パネルから操作を行うことにより、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削除する又は漏洩する恐れがある。

3.3. 組織のセキュリティ方針

OSP.MANAGE　　TOE の提供

TOE 開発者は、TOE を販売会社の CE を経由して利用者に提供する。

OSP.RIP　　利用済ドキュメントデータの処置

TOE は削除によって不要となったドキュメントデータを再使用出来ない状態にする。

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 を管理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及び削除を許可する。

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。

O.RIP　　削除データの処置

TOE はドキュメントデータを削除する際、自動的に再使用できない状態にする機能を提供する。

4.2. 環境のセキュリティ対策方針

OE.TIME　　時刻の提供

OS は管理された時刻情報を TOE に提供する。

OE.PLACE　　設置場所の管理

管理者は TOE を内部ネットワークに接続し、製品関係者のみが操作可能な区画に設置する。

OE.NET　ネットワークの管理

管理者は、内部ネットワーク内の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ネットワーク環境を構築する。

OE.SECMODE　　セキュリティ機能の管理

管理者は TOE のすべてのセキュリティ機能を有効にする。

OE.USR　　一般利用者の教育

管理者は、TOE がセキュアな状態を維持するための教育及び啓蒙を一般利用者に対して実施する。

- 一般利用者はユーザ BOX 識別子及びユーザ BOX パスワードは他者に知れないように管理する。

OE.ADMIN　　管理者の条件

責任者は、十分なスキルと信頼性を備えた人物を管理者として選任し管理する。

OE.PHYSICAL　　物理的な管理

ドキュメントデータを格納する HDD は、CE 以外に取り出すことができない構造で物理的に保護されている。

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　　識別のタイミング

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　　認証のタイミング

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_UID.1 識別のタイミング

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試行回数

[回数]

- 1回

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　　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 文字固定

  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;及び
  同一文字のみのパスワードを禁止

詳細化 ： 「秘密」→
「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」

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
  2)ユーザ BOX 内のドキュメントデータの削除

[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
  2)ユーザ BOX の削除

[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内のあらゆるドキュメントデータの読み出し及び削除を許可する。
・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]
下記のいずれかを実行する。

・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。
・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る場合、ユーザBOX識別子に関連づけられたユーザBOXの削除を許可する。

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

FDP_RIP.1　　サブセット残存情報保護

下位階層：なし

FDP_RIP.1.1

TSF は、以下のオブジェクト[選択：への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない:[割付：オブジェクトのリスト]。

[選択：への資源の割当て、からの資源の割当て解除]

- からの資源の割当て解除

[割付：オブジェクトのリスト]

- ユーザ BOX

依存性：なし

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**エラー！参照元が見つかりません。**』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	認証情報の許容値を登録又は変更する際における、認証情報の拒否または受入れ
FDP_ACF.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
FMT_SMF.1	管理機能の使用(FIA_UID.2、FIA_UAU.2、FMT_MTD.1、MFT_MSA.1、FMT_MSA.3、FMT_SMR.1)

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_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]]

- 削除
- 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]
セキュリティ強化機能 ： すべてのセキュリティ機能を有効化する機能

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

[割付：許可された識別された役割]
管理者

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	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
	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	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_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使わ	

機能要件	管理要件	管理項目
	れる属性の管理	ユーザ BOX 識別子
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
FDP_RIP.1	いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOE において設定可能にされる	残存情報保護は常に実施するため、管理項目はない
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 のパスワード
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 のパスワード
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	管理者のパスワード
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 パスワード
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	管理者のパスワード
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	管理者のパスワード
	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 のパスワード 管理者のパスワード ユーザ BOX 識別子
FPT_SEP.1	なし	

機能要件	管理要件	管理項目
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	管理者のパスワード
FMT_SMF.1	なし	
FMT_RVM.1	なし	

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

FPT_SEP.1　　TSF ドメイン分離

下位階層：なし

FPT_SEP.1.1

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

FPT_SEP.1.2

TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

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要件

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に、高信頼タイムスタンプを提供できなければならない。

詳細化：「TSF」→「OS」

依存性：なし

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以下の 2 つである。

FAI_SOS.1(秘密の検証)、FIA_AFL.1(認証失敗時の取り扱い)

両機能要件に対して、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 • パスワードは同一文字のみの値を禁止する 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 FMT_MTD.1[1] FMT_SMF.1 FMT_SMR.1 FPT_SEP.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	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_SEP.1 FPT_RVM.1

	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。	
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_SEP.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 :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。 • 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	FIA_SOS.1 FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_SMF.1 FMT_SMR.1 FPT_SEP.1 FPT_RVM.1

	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 • パスワードは同一文字のみの値を禁止する 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。	

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 • ドキュメントデータの読み出しと FAX 機器へ送信 • ドキュメントデータの読み出しと FTP サーバへの送信 • ドキュメントデータの読み出しと Mail サーバへの送信 • ドキュメントデータの読み出しと PC 共用フォルダへの送信。 • ドキュメントデータの削除 ユーザ BOX 内のドキュメントデータの削除では、RD.TEMP を呼び出しドキュメントデータを消去する。識別と認証が不成功であった場合、5 秒後に、識別と	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FDP_ACC.1[1] FDP_ACC.1[2] FDP_ACF.1 FDP_RIP.1 FPT_SEP.1 FPT_RVM.1

	認証のインタフェースを有効にする。	

6.1.3. 残存データ保護

残存データ保護機能は、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
RD.TEMP 残存データ保護	RD.TEMP は、TOE のドキュメントデータの削除が実施された後に必ず実行し、ドキュメントデータが格納されていた HDD 上の領域を無意味な文字列で書き換える。	FDP_RIP.1 FPT_SEP.1 FPT_RVM.1

6.1.4. 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不成功 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変更時の成功不成功 • ドキュメントデータ読み出しの成功 • ドキュメントデータ削除の成功	FAU_GEN.1 FAU_SAR.1 FPT_RVM.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_SEP.1 FPT_RVM.1

6.1.5. 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 すべてのセキュリティ機能を有効にする機能(セキュリティ強化機能)を許可し実行する。	FMT_MOF.1 FPT_SEP.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 • ユーザ BOX 識別子の削除、RD.TEMP によるユーザ BOX 内の全ドキュメントデータの消去とユーザ BOX 削除(全ユーザ BOX 識別子の削除、RD.TEMP による全ユーザ BOX 内の全ドキュメントデータの消去と全ユーザ BOX の削除をする場合は HDD の初期化となる) • 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 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 • パスワードは同一文字のみの値を禁止する 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	FDP_ACC.1[2] FDP_ACF.1[2] FIA_SOS.1 FMT_MSA.1 FMT_MSA.3 FAU_STG.1 FAU_SAR.2 FAU_SAR.1 FMT_SMF.1 FMT_SMR.1 FPT_SEP.1 FPT_RVM.1

	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。	

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_ADD 及び IA.PASS)及び管理支援機能(MNG.ADM)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	7222/7322/7228/7235 構成管理書 7222/7322/7228/7235 設計文書一覧 7222/7322/7228/7235 ソースコード一覧
	ACM_SCP.1	7222/7322/7228/7235 構成管理書 7222/7322/7228/7235 設計文書一覧 7222/7322/7228/7235 ソースコード一覧

配付と運用	ADO_DEL.1	7222/7322/7228/7235 配布規定書 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｺﾋﾟｰ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾈｯﾄﾜｰｸ/ｽｷｬﾅ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾄﾞｷｭﾒﾝﾄﾌｫﾙﾀﾞ編 7145/7222/7322/7228/7235 ｻｰﾋﾞｽﾏﾆｭｱﾙﾌｨｰﾙﾄﾞｻｰﾋﾞｽ編 7222/7228/7235 User's Guide Copier 7222/7228/7235 User's Guide Network Setup and Scanner Operations 7222/7228/7235 User's Guide Security 7222/7228/7235 User's Guide Document Folder Operations 7145/7222/7228/7235 SERVICE MANUAL Field Service

	ADO_IGS.1	7222/7322/7228/7235 導入・運用規定書 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｺﾋﾟｰ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾈｯﾄﾜｰｸ/ｽｷｬﾅ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾄﾞｷｭﾒﾝﾄﾌｫﾙﾀﾞ編 7145/7222/7322/7228/7235 ｻｰﾋﾞｽﾏﾆｭｱﾙﾌｨｰﾙﾄﾞｻｰﾋﾞｽ編 7222/7322/7228/7235 ｲﾝｽﾄｰﾙﾏﾆｭｱﾙ 7222/7228/7235 User's Guide Copier 7222/7228/7235 User's Guide Network Setup and Scanner Operations 7222/7228/7235 User's Guide Security 7222/7228/7235 User's Guide Document Folder Operations 7145/7222/7228/7235 SERVICE MANUAL Field Service 7222/7228/7235 INSTALLATION MANUAL
開発	ADV_FSP.1	7222/7322/7228/7235 機能仕様書
	ADV_HLD.2	7222/7322/7228/7235 機能仕様書
	ADV_RCR.1	7222/7322/7228/7235 機能対応書

ガイダンス文書	AGD_ADM.1	7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｺﾋﾟｰ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾈｯﾄﾜｰｸ/ｽｷｬﾅ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾄﾞｷｭﾒﾝﾄﾌｫﾙﾀﾞ編 7145/7222/7322/7228/7235 ｻｰﾋﾞｽﾏﾆｭｱﾙﾌｨｰﾙﾄﾞｻｰﾋﾞｽ編 7222/7228/7235 User's Guide Copier 7222/7228/7235 User's Guide Network Setup and Scanner Operations 7222/7228/7235 User's Guide Security 7222/7228/7235 User's Guide Document Folder Operations 7145/7222/7228/7235 SERVICE MANUAL Field Service
	AGD_USR.1	7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｺﾋﾟｰ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾈｯﾄﾜｰｸ/ｽｷｬﾅ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾄﾞｷｭﾒﾝﾄﾌｫﾙﾀﾞ編 7222/7228/7235 User's Guide Copier 7222/7228/7235 User's Guide Network Setup and Scanner Operations 7222/7228/7235 User's Guide Security 7222/7228/7235 User's Guide Document Folder Operations
ライフサイクルサポート	ALC_DVS.1	7222/7322/7228/7235 開発ｾｷｭﾘﾃｨ規定書
テスト	ATE_COV.2	7222/7322/7228/7235 機能テスト書
	ATE_DPT.1	7222/7322/7228/7235 機能分析書
	ATE_FUN.1	7222/7322/7228/7235 機能テスト書

	ATE_IND.2	無し（7222/7322/7228/7235 テストセット）
脆弱性評定	AVA_MSU.1	7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｺﾋﾟｰ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾈｯﾄﾜｰｸ/ｽｷｬﾅ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 7222/7322/7228/7235 ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ ﾄﾞｷｭﾒﾝﾄﾌｫﾙﾀﾞ編 7145/7222/7322/7228/7235 ｻｰﾋﾞｽﾏﾆｭｱﾙﾌｨｰﾙﾄﾞｻｰﾋﾞｽ編 7222/7228/7235 User's Guide Copier 7222/7228/7235 User's Guide Network Setup and Scanner Operations 7222/7228/7235 User's Guide Security 7222/7228/7235 User's Guide Document Folder Operations 7145/7222/7228/7235 SERVICE MANUAL Field Service
	AVA_SOF.1	7222/7322/7228/7235 脆弱性分析書
	AVA_VLA.1	7222/7322/7228/7235 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 / セキュリティ対策方針	T・ACCESS	ASM・PLACE	ASM・PHYSICAL	ASM・SECMDE	ASM・NET	ASM・ADMIN	ASM・CE	ASM・USR	OSP・MANAGE	OSP・RIP
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)	✔									
O.RIP(削除データの処置)										✔
OE.TIME(時刻の利用)	✔									
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.PHYSICAL(物理的な管理)			✔							

OE.SECMODE(セキュリティ機能の管理)				✔							

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.ACCESS：不正なアクセス

TSF は管理者を 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。管理者はこの管理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への読み出し及び削除を、O.DATAACCESS により許可する。

また、O.AUDIT 及び OE.TIME 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は正確な時刻と共に監査情報として記録するため、他の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に効果がある。

以上に示すように、対策方針 O.IA、O.MANAGE、O.DATAACCESS、O.AUDIT 及び OE.TIME で脅威 T.ACCESS に対抗出来る。

ASM.PLACE：TOE の設置条件

TOE は OE.PLACE によって、内部ネットワークに接続し製品関係者のみが操作可能な区画に設置される。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.PHYSICAL：筐体の保護

OE.PHYSICAL では、HDD は CE 以外に取り出すことができない構造で物理的に保護されている。

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

ASM.SECMODE：セキュリティ機能の実行

管理者は OE.SECMODE で　管理者は TOE のすべてのセキュリティ機能を有効にする。これによりセキュリティ機能は常に動作する。

以上に示すように、前提条件 ASM.SECMODE は対策方針 OE.SECMODE 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。TOE と内部ネットワークの間に TOE の通信を暗号化する機器を設置することで、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、十分なスキルと信頼性を備えた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 で一般利用者にセキュアな状態を維持するための教育及び啓蒙を一般利用者に行う。これにより一般利用者は必要な知識(HDD 上のデータの漏洩の危険性と対策、ユーザ BOX 識別子とユーザ BOX パスワードの機密保持)を身につけ、セキュリティを護る行動がとれる。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。

OSP.MANAGE：CE と管理者の役割分担

TSF は O.IA で CE を識別認証する。TSF は識別認証した正当な CE に O.CE で管理者に管理機能を使用可能にする機能を提供する。これにより、利用者は使用可能となる。

以上に示すように、組織のセキュリティ方針 OSP.MANAGE は対策方針 O.IA、及び O.CE によって実現できる。

OSP.RIP：利用済ドキュメントデータの処置

TSF は O.RIP でドキュメントデータを削除する際、自動的に再使用できない状態にする機能を提供する。これにより、削除されて不要となったドキュメントデータは再使用出来ない状態となる。

以上に示すように、組織のセキュリティ方針 OSP.RIP は対策方針 O.RIP 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

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 TOE 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 TOE セキュリティ機能要件の対応

セキュリティ対策方針 / TOE セキュリティ機能要件		O・IA	O.MANAGE	O.CE	O・DATAACCESS	O・AUDIT	O・RIP	OE・TIME
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	✔	✔	✔				
	FDP_ACC.1[1]				✔			
	FDP_ACC.1[2]		✔					
	FDP_ACF.1[1]				✔			
	FDP_ACF.1[2]		✔					
	FDP_RIP.1						✔	
	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_MSA.1		✔					
	FMT_MSA.3		✔					
	FMT_SMR.1	✔	✔	✔	✔			
	FPT_SEP.1	✔	✔	✔	✔	✔	✔	
	FMT_MOF.1	✔	✔	✔	✔	✔	✔	
	FPT_RVM.1	✔	✔	✔	✔	✔	✔	
	FMT_SMF.1	✔	✔	✔	✔			
IT 環境に対するセキュリティ機能要件	FPT_STM.1							✔

以下に、『表 8.2 セキュリティ対策方針と TOE 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、不正な利用者の CE、管理者、及びユーザ BOX を所有している一般利用者の識別認証成功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(*)を表示し、パスワードを秘匿する。

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 で指定されたパスワード規則に従っているか検証され、暴露されやすいユーザ BOX パスワードへの変更

を抑止している。

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も、FMT_SEP.1 により改ざんされることはなく、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対策方針 O.IA は可能である。

O.MANAGE：管理機能の提供

O.IA で管理者は認証される。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。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]でユーザ BOX パスワードを変更することで、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 で指定されたパスワード規則に従っているか検証され、暴露されやすいユーザ BOX パスワードの登録を抑止している。さらに、FDP_ACC.1[2]、FDP_ACF.1[2] 、FMT_MSA.1 で管理者によりユーザ BOX 識別子を削除することで格納されたドキュメントデータとともにユーザ BOX を削除できる。

ユーザ BOX 識別子とユーザ BOX パスワードの管理を FMT_SMF.1 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も、FMT_SEP.1 により改ざんされることはなく、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.MANAGE は可能である。

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。また、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、一般利用者から入力した CE や管理者のパスワードが一致する可能性を低くする。

ユーザ BOX 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も、FMT_SEP.1 により改ざんされることもなく、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 は可能である。

O.DATAACCESS：ドキュメントデータへのアクセス制限

O.IA で対象のユーザ BOX を所有している一般利用者は認証される。さらに 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と削除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。以上の機能は FPT_RVM.1 によりバイパスされることも、FMT_SEP.1 により改ざんされることもなく、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 は可能である。

O.AUDIT：監査情報の記録

必要な監査情報を 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も、FMT_SEP.1 によって改ざんされることもなく、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採取され安全に保護される。

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 は可能である。

O.RIP：削除データの処置

ドキュメントデータを削除する際に、自動的に削除されたドキュメントデータが格納された HDD 上の領域を FDP.RIP.1 で消去することで再使用できない状態に確実にすることが出来る。以上の機能は FPT_RVM.1 によりバイパスされることも、FMT_SEP.1 により改ざんされることもなく、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、OE.RIP は可能である。

OE.TIME：時刻の利用

本対策方針は、TOE が利用する時刻情報が OS によって管理されることから、適合性に対し以下の根拠が成り立つ。

FPT_STM.1 では、OS がタイムスタンプ機能を実装し、TOE に提供する。

従って、対応するセキュリティ機能要件により、OE.TIME は可能である。

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	なし	なし		
6	FDP_ACC.1[1]	なし	FDP_ACF.1	8	
7	FDP_ACC.1[2]	なし	FDP_ACF.1	9	
8	FDP_ACF.1[1]	なし	FDP_ACC.1 FMT_MSA.3	6 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。
9	FDP_ACF.1[2]	なし	FDP_ACC.1 FMT_MSA.3	7 21	

10	FDP_RIP.1	なし	なし		
11	FAU_GEN.1	なし	FPT_STM.1	27	
12	FAU_STG.1	なし	FAU_GEN.1	11	
13	FAU_STG.4	FAU_STG.3	FAU_STG.1	12	
14	FAU_SAR.1	なし	FAU_GEN.1	11	
15	FAU_SAR.2	なし	FAU_SAR.1	14	
16	FMT_MTD.1[1]	なし	FMT_SMR.1 FMT_SMF.1	24 23	
17	FMT_MTD.1[2]	なし	FMT_SMR.1 FMT_SMF.1	24 23	
18	FMT_MTD.1[3]	なし	FMT_SMR.1 FMT_SMF.1	24 23	
19	FMT_MTD.1[4]	なし	FMT_SMR.1 FMT_SMF.1	24 23	
20	FMT_MSA.1	なし	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	6 24 23	
21	FMT_MSA.3	なし	FMT_MSA.1 FMT_SMR.1	20 24	
22	FMT_MOF.1	なし	FMT_SMR.1 FMT_SMF.1	24 23	
23	FMT_SMF.1	なし	なし		
24	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。
25	FPT_SEP.1	なし	なし		
26	FPT_RVM.1	なし	なし		
27	FPT_STM.1	なし	なし		

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		
		改ざん	迂回	非活性化
1	FIA_UID.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
2	FIA_UAU.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
3	FIA_UAU.7	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
4	FIA_AFL.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
5	FIA_SOS.1	FPT_SEP.1	なし	FMT_MOF.1
6	FDP_ACC.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
7	FDP_ACC.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
8	FDP_ACF.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
9	FDP_ACF.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
10	FDP_RIP.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
11	FAU_GEN.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
12	FAU_STG.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
13	FAU_STG.4	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
14	FAU_SAR.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
15	FAU_SAR.2	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
16	FMT_MTD.1[1]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
17	FMT_MTD.1[2]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
18	FMT_MTD.1[3]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
19	FMT_MTD.1[4]	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
20	FMT_MSA.1	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
21	FMT_MSA.3	FPT_SEP.1	FPT_RVM.1	FMT_MOF.1
22	FMT_MOF.1	FPT_SEP.1	FPT_RVM.1	
23	FMT_SMF.1	FPT_SEP.1	なし	FMT_MOF.1
24	FMT_SMR.1	FPT_SEP.1	なし	FMT_MOF.1
25	FPT_SEP.1		なし	FMT_MOF.1
26	FPT_RVM.1	FPT_SEP.1		FMT_MOF.1
27	FPT_STM.1	なし	なし	なし

【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。

利用後のドキュメントデータが必ず読み出し不可の状態となる(FDP_RIP.1)。

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、セキュリティ属性の操作は対応する利用者にのみ可能である。(FAU_SAR.2、FMT_MTD.1[1]～[4]、FMT_MSA.1、FMT_MSA.3、FMT_MOF.1)

以上を確実に実行するため、FPT_RVM.1 により迂回を防止する。

【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】

FPT_SEP.1 により他の不正なサブジェクトからの TSF の改ざんを抑止するよう TOE が作成されている。従って TSF の改ざん防止が実現されている。

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、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 セキュリティ機能強度』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 は、OS によって管理された時刻情報を利用する。
- 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。
- 管理者は TOE に物理的な攻撃が行われないように管理する。
- 責任者は、十分なスキルと信頼性を備えた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。

上記の運用対策によって、脅威エージェントを以下の人物に特定する。

攻撃能力 ： 低レベル

上記の攻撃能力を有した脅威エージェントにより、本 TOE に対する不正な操作を避けるために、TOE は識別認証機能及びアクセス制御機能を実装する。また、TOE に対する操作を監視するために、TOE は監査機能を実装する。

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エージェントに対抗するために、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 TOE 要約仕様とセキュリティ機能要件の対応』に示す。

表 8.4 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / TOE セキュリティ機能要件	IA・ADM_ADD	IA・ADM_AUTH	IA・CE_AUTH	IA・PASS	ACL・USR	RD・TEMP	AUD・LOG	AUD・MNG	MNG・MODE	MNG・ADM
FIA_UID.2		✔	✔		✔					
FIA_UAU.2		✔	✔		✔					
FIA_UAU.7		✔	✔		✔					
FIA_AFL.1		✔	✔		✔					
FIA_SOS.1	✔			✔						✔
FDP_ACC.1[1]					✔					
FDP_ACC.1[2]										✔
FDP_ACF.1[1]					✔					
FDP_ACF.1[2]										✔
FDP_RIP.1					✔	✔				
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_MSA.1										✔
FMT_MSA.3										✔
FMT_MOF.1									✔	
FMT_SMF.1	✔			✔						✔
FMT_SMR.1	✔			✔						✔
FPT_SEP.1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
FPT_RVM.1	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

以下に、『表 8.4 TOE 要約仕様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

管理者のパスワード登録に対しては IA.ADM_ADD で、ユーザ BOX パスワードの登録に対しては MNG.ADM で、管理者及び CE のパスワード、及びユーザ 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.ADM_ADD、MNG.ADM及びIA.PASSを実装することでFIA_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、認証の不成功時に、管理者及びCE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及びIA.CE_AUTH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と削除を実行する。以上により、ACL.USRを実装することでFDP_ACC.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の作成及び削除を行う。

以上により、MNG.ADMを実装することでFDP_ACC.1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と削除を実行する。以上により、ACL.USRを実装することでFDP_ACF.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の作成及び削除を行う。

以上により、MNG.ADMを実装することでFDP_ACF.1を実現できる。

FDP_RIP.1

ACL.USRがRD.TEMPを呼び出し、RD.TEMPでドキュメントデータの消去を実行したうえ、ACL.USRがドキュメントデータを削除することで、再度利用を不可能にする。

MNG.ADMがRD.TEMPを呼び出し、RD.TEMPでドキュメントデータの消去を実行したうえ、MNG.ADMがドキュメントデータを削除することで、再度利用を不可能にする。

以上により、RD.TEMPとACL.USRを実装することでFDP_RIP.1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
監査記録の生成時に、AUD.LOG で管理者が監査記録を参照できる形式で生成する。
以上により、AUD.LOG 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_MSA.1
ユーザ BOX 生成と削除のためにユーザ BOX 識別子の登録と削除を 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 で規定した全セキュリティ機能の有効/無効の設定を 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 の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_SEP.1

IA.ADM_ADD、IA.ADM_AUTH、IA.CE_AUTH、IA.PASS、ACL.USR、RD.TEMP、AUD.LOG、AUD.MNG、MNG.MODE 及び MNG.ADM を実現することにより不正なサブジェクトは TSF を破壊しない。

以上により、FPT_SEP.1 を実現できる。

FPT_RVM.1

IA.ADM_ADD、IA.ADM_AUTH、IA.CE_AUTH、IA.PASS、ACL.USR、RD.TEMP、AUD.LO、AUD.MNG、MNG.MODE G 及び MNG.ADM は、必ず実行される。

以上により、FPT_RVM.1 を実現できる。

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_ADD 及び IA.PASS)及び管理支援機能(MNG.ADM)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 セキュリティ機能強度』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。