RICOH IM C530F/C530FB,

SAVIN IM C530FB,

LANIER IM C530FB,

nashuatec IM C530F/C530FB,

Rex Rotary IM C530F/C530FB,

Gestetner IM C530F/C530FB

セキュリティターゲット

作成者:　株式会社リコー
作成日付:2022 年 7 月 15 日
バージョン:　1.00

目次

図一覧

表一覧

1 ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、及び TOE 記述について記述する。

1.1 ST 参照

ST の識別情報を以下に示す。

タイトル: RICOH IM C530F/C530FB,
SAVIN IM C530FB,
LANIER IM C530FB,
nashuatec IM C530F/C530FB,
Rex Rotary IM C530F/C530FB,
Gestetner IM C530F/C530FB セキュリティターゲット

バージョン: 1.00

作成日付: 2022 年 7 月 15 日

作成者: 株式会社リコー

1.2 TOE 参照

TOE の識別情報を以下に示す。

TOE 名称: RICOH IM C530F/C530FB,
SAVIN IM C530FB,
LANIER IM C530FB,
nashuatec IM C530F/C530FB,
Rex Rotary IM C530F/C530FB,
Gestetner IM C530F/C530FB

バージョン: E-1.00

TOE 種別: デジタル複合機(以下、MFP と言う)

対象 MFP は表 1 に示す海外向けの製品であり、製品名と機種コードによって識別する。

表 1：対象 MFP の製品名と機種コード

No.	製品名	機種コード
1	IM C530F	D0CT-27
2	IM C530FB	D0CS-17
3	IM C530FB	D0CS-27

これらの MFP に搭載されるソフトウェアとハードウェアの識別情報を表 2 に示す。ソフトウェアは名称、バージョン、及び部番で識別する。ただし、Keymicon、GraphicData、及び LegacyUIData は名称とバージョンで識別する。ハードウェアは名称とバージョンで識別する。

表 2：バージョン E-1.00 のソフトウェアとハードウェアのバージョンと部番

本体のソフトウェアとハードウェアの名称		バージョン	部番
ソフトウェア	CTL System	1.05	D0CS5260F
	CheetahSystem	1.05	D0CS5100F
	appsite	3.03.37	D0CS5176
	bleservice	1.00.02	D0CS5127A
	camelsl	1.11	D0CS5132A
	cispluginble	4.0.4	D0CS5109A
	cispluginkeystr	3.03.02	D0CS5117A
	cispluginnfc	3.03.02	D0CS5116A
	faxinfo	1.00	D0CS5125A
	helpservice	1.00	D0CS5111A
	iccd	3.08.02	D0CS5130A
	introductionset	1.01	D0CS5112A
	iwnnimelanguage	2.8.2	D0BQ1456A
	iwnnimelanguage	2.8.2	D0BQ1454A
	iwnnimelanguage	2.8.2	D0BQ1455A
	iwnnimeml	2.8.201	D0BQ1453C
	kerberos	1.07.04	D0CS5131B
	langswitcher	1.00	D0CS5102A
	mediaappappui	1.00	D0CS5107A
	mlpsmartdevicec	4.1.2	D0CS5101A
	multidevicehub	1.00	D0CS5133A
	optimorurcmf	1.1	D0BQ1499B
	programinfoserv	1.00	D0CS5128A
	remotesupport	1.00	D0CS5110

本体のソフトウェアとハードウェアの名称		バージョン	部番
	simpleauth	3.05.03	D0CS5123A
	simpledirectcon	1.18	D0CS5118
	simpleprinter	1.00	D0CS5103A
	smartcopy	1.00	D0CS5104A
	smartfax	1.01	D0CS5106B
	smartprtstoredj	1.01	D0CS5108B
	smartscanner	1.00	D0CS5105A
	smartscannerex	2.05	D0CS5113B
	stopwidget	1.00	D0CS5126A
	tonerstate	1.00	D0CS5124A
	traywidget	1.00	D0CS5135A
	Engine	011000:01	D0CS5160A
	ADF	2D1000:01	D0CS5161
	Engine(IPU)	1.03:04	D0CS5150D
ハードウェア	Ic Key	12714	表示なし

操作パネルユニットのソフトウェア		バージョン	部番
ソフトウェア	Firmware	1.05	D0CS5100F
	Keymicon	9.10	表示なし
	Application Site	3.03.37	D0CS5176
	Bluetooth Authentication Plugin	4.0.4	D0CS5109A
	BluetoothService	1.00.02	D0CS5127A
	Change Languages	1.00	D0CS5102A
	Copy	1.00	D0CS5104A
	Direct Connection	1.18	D0CS5118
	Fax	1.01	D0CS5106B
	Fax RX File	1.00	D0CS5125A
	GraphicData	0.28	DXXXXXXX
	ICCardDispatcher	3.08.02	D0CS5130A
	Installation Settings	1.01	D0CS5112A
	iWnn IME	2.8.201	D0BQ1453C

操作パネルユニットのソフトウェア		バージョン	部番
	iWnn IME Korean Pack	2.8.2	D0BQ1456A
	iWnn IME Simplified Chinese Pack	2.8.2	D0BQ1454A
	iWnn IME Traditional Chinese Pack	2.8.2	D0BQ1455A
	KerberosService	1.07.04	D0CS5131B
	LegacyUIData	0.22	DXXXXXXX
	Multi Device Hub	1.00	D0CS5133A
	Print/Scan (Memory Storage Device)	1.00	D0CS5107A
	Printer	1.00	D0CS5103A
	ProgramInfoService	1.00	D0CS5128A
	Proximity Card Reader Support Plugin	3.03.02	D0CS5117A
	Quick Card Authentication Config.	3.05.03	D0CS5123A
	Quick Print Release	1.01	D0CS5108B
	Remote Panel Operation	1.11	D0CS5132A
	RemoteConnect Support	1.1	D0BQ1499B
	RemoteSupportService	1.00	D0CS5110
	RicohScanGUIService	2.05	D0CS5113B
	Scanner	1.00	D0CS5105A
	Smart Device Connector	4.1.2	D0CS5101A
	Standard IC Card Plugin	3.03.02	D0CS5116A
	Stop	1.00	D0CS5126A
	Supply Information	1.00	D0CS5124A
	Support Settings	1.00	D0CS5111A
	Tray/Remaining Paper	1.00	D0CS5135A

CC 認証品として購入したい場合は、その旨を営業担当者に依頼すること。

1.3 TOE 概要

本章では、本 TOE の種別、TOE の使用法及び主要なセキュリティ機能の特徴を述べる。

1.3.1 TOE 種別

本 TOE の種別は IT 製品であり、コピー、プリンター、スキャナー、ファクス機能を有した MFP である。

1.3.2 TOE の使用法及び主要なセキュリティ機能の特徴

TOE はオフィスに設置され、電話回線と LAN に接続された図 1 のような環境での使用を想定される MFP である。利用者は、MFP の操作パネルユニット(以下、操作パネルと言う)からの操作や、LAN で接続されたクライアント PC からの操作により、コピー、プリンター、スキャナー、及びファクスの各機能を利用する。

TOE が扱う文書やセキュリティ機能に関する設定情報等の保護資産に対して、TOE への不正アクセスやネットワーク上の通信データへの不正アクセスによる暴露や改ざんを防止するために、識別認証、アクセス制御、eMMC 暗号化、及び TLS 暗号化通信のセキュリティ機能を提供する。TOE は電話回線から LAN への侵入を防ぐ機能も提供する。TOE における発生事象は MFP 管理者が監査ログデータとして確認でき、MFP 管理者は操作パネルまたはクライアント PC から管理機能を利用できる。また TOE は正規のソフトウェア構成の検証を行う。なお TOE は HDD を搭載せず eMMC で利用者データを取り扱うため、残存情報消去機能は評価対象のセキュリティ機能には含まれていない。

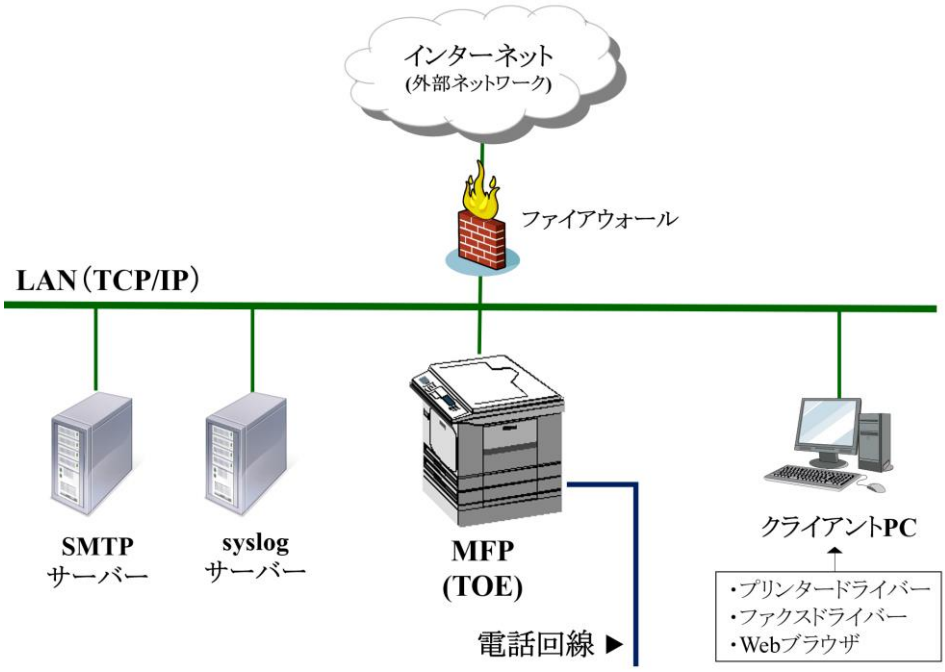

図 1 : TOE の利用環境

1.3.3 TOE に必要な TOE 以外のハードウェア/ソフトウェア

図 1 の利用環境における TOE 以外への説明を以下に示す。

- クライアント PC
  - LAN に接続することによって PC は TOE のクライアントとして動作し、利用者は、クライアント PC から MFP をリモート操作することができる。クライアント PC から MFP の各種設定や蓄積文書の操作をするために、Web ブラウザを利用する必要がある。クライアント PC から文書を蓄積するためには、TLS に対応した機能(IPP over SSL）を持った、リコーによって提供される PCL6 Driver というプリンタードライバー(1.1.0.0 以降のバージョン)をインストールしておく必要がある。またクライアント PC からファクス送信するためには、TLS に対応した機能(IPP over SSL）を持った、リコーによって提供さ

れる LAN Fax Driver というファクスドライバー(9.5.0.0 以降のバージョン)をインストールしておく必要がある。

- SMTP サーバー
  - TOE が電子メールを送信する場合に使用される、SMTP プロトコルを利用し、TLS に対応したサービスをインストールしたサーバー。スキャナー機能(文書添付メール送信)を利用するために必要である。
- syslog サーバー
  - TOE が記録した監査ログデータを受信できる、syslog プロトコルを利用し、TLS に対応したサービスをインストールしたサーバー。監査ログデータは、syslog サーバーにも転送ができる。転送設定を有効にした場合は、監査ログデータの転送先として使用される。

TOE はネットワーク利用のため LAN に接続され、外部ファクスと送受信するために電話回線に接続される。TOE を外部ネットワークに接続するためには、ファイアウォールを設置して外部ネットワークの不正アクセスから TOE を保護する必要がある。

TOE 評価で使用した TOE 以外のハードウェア/ソフトウェアを以下に示す。

- クライアント PC
  - OS:Windows 10、及び Windows 8.1
  - プリンタードライバー: PCL6 Driver 1.1.0.0
  - ファクスドライバー: LAN Fax Driver 9.5.0.0
  - Web ブラウザ: Internet Explorer 11、及び Microsoft Edge 44
- SMTP サーバー: Linux(Ubuntu 18.04.3 LTS) postfix 3.3.0
- syslog サーバー: Linux(Ubuntu18.04.2 LTS) rsyslogd 8.32.0

1.4 TOE 記述

本章では、TOE の物理的範囲、及び TOE の論理的範囲を述べる。

1.4.1 TOE の物理的範囲

TOE は、表 3 の MFP 製品と、表 4 と表 5 のガイダンスからなる。MFP 製品は、表 2 に示した TOE バージョンのハードウェアとソフトウェアを搭載した製品が対象である。MFP 製品は配送業者が利用者へ配送する。ガイダンスは MFP 製品に同梱して配付するものと Web にて配付するものがある。ガイダンスは英語表示であり、北米向けの[英語版-1]または欧州向けの[英語版-2]のいずれかのガイダンスセットを配付する。

以下に記載の組み合わせで利用者へ配付する。

表 3: 配付する組み合わせ

No.	MFP		ガイダンス
	製品名	機種コード	
1	IM C530F	D0CT-27	[英語版-2]

No.	MFP		ガイダンス
2	IM C530FB	D0CS-17	[英語版-1]
3	IM C530FB	D0CS-27	[英語版-2]

表 4 と表 5 に[英語版-1]、[英語版-2]のガイダンスセット毎のガイダンス文書、配付形式、及び配付方法を示す。

表 4 : [英語版-1]のガイダンス

No.	製品のガイダンス文書			
	部番	ガイダンス名称	配付形式	配付方法
1	D0BW-7035	Product Warranty Registration	冊子	製品と同梱
2	D0BW-7050A	For Users of This Product	冊子	製品と同梱
3	D0CS-7015	IM C530FB / IM C530F MULTIFUNCTION PRINTER LIMITED WARRANTY – FOR U.S. ONLY	冊子	製品と同梱
4	D0CS-7017	Notes for Users	冊子	製品と同梱
5	D0CS-7118	Notes for Users	冊子	製品と同梱
6	D256-7819A	Notes for Using This Machine Safely	冊子	製品と同梱
7	D256-7840A	SOFTWARE LICENSE AGREEMENT	冊子	製品と同梱
8	D0CS-7307	Safety Information	PDF	Web 配付
9	D0CS-7303	User Guide Selected Version	PDF	Web 配付
10	D0CS7305	Security Reference	HTML	Web 配付
11	D0CS7291	Setup	HTML	Web 配付
12	D0CS7292	Introduction and Basic Operations	HTML	Web 配付
13	D0CS7293	Copy	HTML	Web 配付
14	D0CS7294	Fax	HTML	Web 配付
15	D0CS7295	Scan	HTML	Web 配付
16	D0CS7296	Printer	HTML	Web 配付
17	D0CS7297	Maintenance	HTML	Web 配付
18	D0CS7298	Troubleshooting	HTML	Web 配付
19	D0CS7299	Settings	HTML	Web 配付

No.	製品のガイダンス文書			
	部番	ガイダンス名称	配付形式	配付方法
20	D0CS7300	Specifications	HTML	Web 配付
21	D0CS7301	Security	HTML	Web 配付
22	D0CS7302	Driver Installation Guide	HTML	Web 配付
23	D0CS-7027 2022.03.02	Notes on Security Functions	PDF	Web 配付
24	D0CS-7025 2022.07.14	Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	PDF	Web 配付
25	83NHENENZ1.10 v228	Help	HTML	Web 配付

Web 配付するガイダンスは、以下の URL からダウンロードできる。

https://support.ricoh.com/services/device/ccmanual/IM_C530/en/Guidance_na.zip

ハッシュ値(SHA256): 7d81777137c3e1a870b981a3bfd1d7fb420c50792510057fcc9ac500ab5bed9b

表 5 : [英語版-2]のガイダンス

No.	製品のガイダンス文書			
	部番	ガイダンス名称	配付形式	配付方法
1	D0BW-7050A	For Users of This Product	冊子	製品と同梱
2	D0CS-7017	Notes for Users	冊子	製品と同梱
3	D0CS-7116	Notes for Users	冊子	製品と同梱
4	D0CS-7117	Notes for Users	冊子	製品と同梱
5	D0CS-7290	Notes for Users	冊子	製品と同梱
6	D256-7819A	Notes for Using This Machine Safely	冊子	製品と同梱
7	D256-7840A	SOFTWARE LICENSE AGREEMENT	冊子	製品と同梱
8	D0CS-7306	Safety Information	PDF	Web 配付
9	D0CS-7303	User Guide Selected Version	PDF	Web 配付
10	D0CS7305	Security Reference	HTML	Web 配付
11	D0CS7291	Setup	HTML	Web 配付
12	D0CS7292	Introduction and Basic Operations	HTML	Web 配付

No.	製品のガイダンス文書			
	部番	ガイダンス名称	配付形式	配付方法
13	D0CS7293	Copy	HTML	Web 配付
14	D0CS7294	Fax	HTML	Web 配付
15	D0CS7295	Scan	HTML	Web 配付
16	D0CS7296	Printer	HTML	Web 配付
17	D0CS7297	Maintenance	HTML	Web 配付
18	D0CS7298	Troubleshooting	HTML	Web 配付
19	D0CS7299	Settings	HTML	Web 配付
20	D0CS7300	Specifications	HTML	Web 配付
21	D0CS7301	Security	HTML	Web 配付
22	D0CS7302	Driver Installation Guide	HTML	Web 配付
23	D0CS-7027 2022.03.02	Notes on Security Functions	PDF	Web 配付
24	D0CS-7025 2022.07.14	Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	PDF	Web 配付
25	83NHENENZ1.10 v228	Help	HTML	Web 配付

Web 配付するガイダンスは、以下の URL からダウンロードできる。

https://support.ricoh.com/services/device/ccmanual/IM_C530/en/Guidance_eu.zip

ハッシュ値(SHA256): 105f0cd68c7499c4676191e7e92408b0b47dae246126dca2bc15b75cce91fe5e

1.4.2 TOE の論理的範囲

TOE の論理的範囲を以下に記述する。

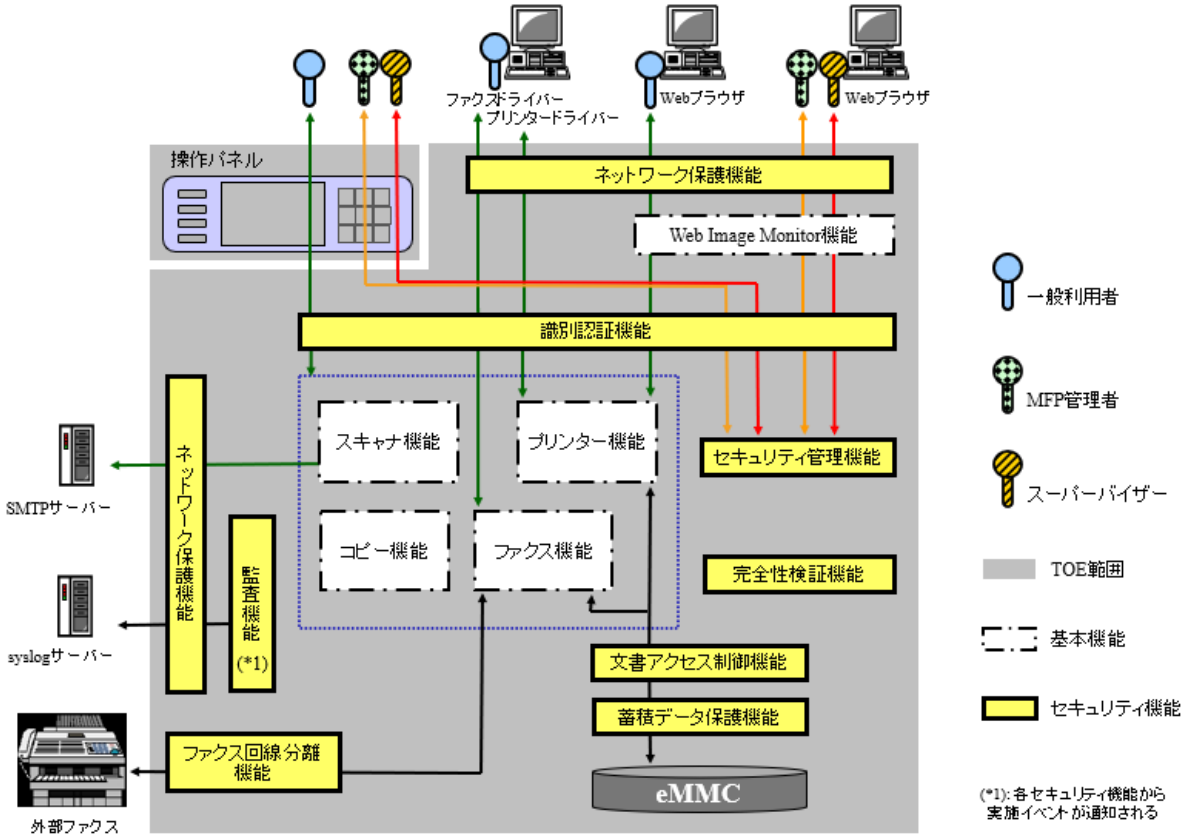

図 2 : TOE の論理的範囲

図 2 のように基本機能とセキュリティ機能があり、それぞれの機能を以下で説明する。

1.4.2.1. 基本機能

以下に、基本機能の概要を記述する。

Web Image Monitor 機能

Web Image Monitor 機能(以下、WIM と言う)は、TOE の利用者が TOE をリモート操作するための機能である。本機能は、TOE と LAN 経由で接続したクライアント PC の Web ブラウザから利用する。

コピー機能

コピー機能は、利用者による操作パネルからの操作によって、紙文書をスキャンして読み取った画像を複写印刷する機能である。複写する画像は、利用者が変倍などの編集をすることができる。

プリンター機能

プリンター機能は、クライアント PC のプリンタードライバーから TOE が受信した文書データを機密印刷文書データとして eMMC に蓄積する機能と、その文書データを利用者が WIM から削除、または操作パネルから印刷、削除する機能である。

スキャナー機能

スキャナー機能は、利用者が操作パネルから操作することによって、紙文書をスキャンしてSMTPサーバーに送信できる機能である。

文書データの送信方法は、文書添付メール送信である。文書添付メール送信は、MFP管理者が予めTOEに登録するセキュアな通信が可能なメールサーバーとメールアドレスに対してのみ行える。

ファクス機能

ファクス機能は、電話回線を利用するG3のファクスプロトコルを使う、ファクス送信機能とファクス受信機能からなる。

ファクス送信機能は、紙文書をスキャンして読み取った画像、または電子文書の画像を、文書データとして外部ファクスに送信する機能である。電子文書の画像をファクス送信する場合は、ファクスドライバーを用いる。ファクスの送信先には予めTOEに登録された電話番号だけを許可する。

ファクス受信機能は、外部ファクスから電話回線を介して受信した文書データをeMMCに蓄積する機能である。蓄積した文書データは、操作パネルから印刷することができる。

1.4.2.2. セキュリティ機能

以下に、セキュリティ機能を記述する。

監査機能

監査機能は、TOEのセキュリティに関連する事象(以下、監査事象と言う)を利用者の識別情報と紐づけたログを監査ログデータとしてeMMCに記録し、記録した監査ログデータを監査できる形式で提供する機能である。記録した監査ログデータのダウンロード・削除は、MFP管理者だけが実施できる。

監査ログデータに記録する日付・時刻はTOEのシステム時計から取得する。監査ログデータファイルに監査ログデータを追加記録する領域がない場合には、最新の監査ログデータを最も古い監査ログデータに上書きする。TOEは、監査ログデータをsyslogサーバーへ転送することもできる。

識別認証機能

識別認証機能は、TOEが認証に成功した利用者だけに管理機能の操作やMFPアプリケーションの操作を許可し、失敗した場合は許可しないために、TOEを利用しようとする者が許可利用者であるかを検証する機能である。利用者のログインユーザー名とログインパスワードの入力を受け付けて検証する。本機能には、以下の機能が含まれる。

・ログインパスワード入力をする際にパスワードをダミー文字で表示する認証フィードバック領域の保護機能

・連続で認証に失敗した回数が閾値に達した場合に利用者に対してログインを許可しない状態にするロックアウト機能

・ログインパスワードの品質を保護するため、MFP管理者が予め制限したパスワードの最小桁数と必須使用の文字種の条件を満たしたパスワードだけを登録する機能

・ログイン状態から一定時間操作が行われない場合に自動的にログアウトする機能

文書アクセス制御機能

文書アクセス制御機能は、識別認証機能で認証された TOE の許可利用者に対し、ユーザー権限、またはログインユーザー名に基づいて、利用者文書データや利用者ジョブデータへの操作を許可する機能である。

ネットワーク保護機能

ネットワーク保護機能は、高信頼 IT 製品(クライアント PC、syslog サーバー、SMTP サーバー)との通信を行う際、暗号化通信を提供することによってネットワーク上のモニタリングによる情報漏えいを防止し、通信内容の改ざんを検出する機能である。TOE はこの機能を TLS によって実装する。

ファクス回線分離機能

ファクス回線分離機能は、電話回線から LAN へ侵入されることを防止するために、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止する機能である。

蓄積データ保護機能

蓄積データ保護機能は、eMMC に記録されているデータを漏えいから保護するため、eMMC に書き込むデータを暗号化する機能である。

セキュリティ管理機能

セキュリティ管理機能は、ユーザー権限、またはログインユーザー名に基づいて、TSF データへの操作に関する制御やセキュリティ機能のふるまいに関する制御を行う機能である。制御を可能にするために、セキュリティ管理機能の操作をする役割を維持し識別認証機能で認証された TOE の許可利用者に紐づける機能、セキュリティ属性に適切なデフォルト値を設定する機能がある。

完全性検証機能

完全性検証機能は、TSF の実行コードの完全性を検証する自己テスト機能である。

2 適合主張

本章では適合の主張について述べる。

2.1 CC 適合主張

本 ST と TOE の CC 適合主張は以下の通りである。

- 適合を主張する CC のバージョン

  パート 1:

  概説と一般モデル 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版] CCMB-2017-04-001

  パート 2:

  セキュリティ機能コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版] CCMB-2017-04-002

  パート 3:

  セキュリティ保証コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版] CCMB-2017-04-003
- 機能要件: パート 2 拡張
- 保証要件: パート 3 適合

2.2 PP 主張

本 ST 及び TOE が適合する PP はない。

2.3 パッケージ主張

本 ST 及び TOE は、パッケージ:EAL2 適合を主張する。

追加する保証コンポーネントはない。

2.4 適合主張根拠

本 ST 及び TOE は、PP 適合を主張しない。

3 セキュリティ課題定義

本章は、利用者、資産、脅威、組織のセキュリティ方針、及び前提条件について記述する。

3.1 利用者定義

本項で TOE に関連する利用者定義を行う。

利用者は、一般利用者と管理者からなり、管理者は MFP 管理者とスーパーバイザーに分かれる。

利用者は表 6 の説明のように、それぞれの役割に応じて分類され、一般利用者、MFP 管理者、スーパーバイザーそれぞれの役割に応じた権限としてユーザー権限をもつ。

表 6：利用者定義

利用者定義		説明
一般利用者		TOE の使用を許可された利用者。ログインユーザー名を付与され、コピー機能、ファクス機能、スキャナー機能、プリンター機能の利用ができる。
管理者	MFP 管理者	TOE の管理を行う、以下のようなことができる権限をもつ。 ・一般利用者に関する設定の操作 ・MFP の機器動作に関する設定情報の操作 ・監査ログデータの操作 ・ネットワーク設定情報の操作 ・ファクス受信文書データのアクセス管理
	スーパーバイザー	TOE の管理を行う、以下のようなことができる権限をもつ。 ・MFP 管理者のログインパスワードの変更 ・MFP 管理者のロックアウト状態の解除

3.2 保護資産

本項では、資産を以下の 2 つに分類する。

表 7：資産分類

資産分類	定義
利用者データ	TSFの操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ。
TSF データ	TSFの操作に影響を与えるかもしれない、TOEのためのTOEによって作成されたデータ。

利用者データは、以下の 2 つに分けられる。

表 8：利用者データ

利用者データ	定義
利用者文書データ	電子的またはハードコピーの形式で、利用者の文書に含まれる情報。 とくに eMMC に蓄積保存される利用者文書データを蓄積文書データと呼ぶ。 さらにプリンタードライバーから機密印刷で蓄積されたものを機密印刷文書データと呼び、外部ファクスから電話回線を介して蓄積されたものをファクス受信文書データと呼ぶ。
利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報。

3.2.1 TSF データ

TSF データは、以下の 2 種類に分類する。

表 9：TSF データ分類

TSF データ分類	定義
TSF 秘密データ	秘密とする TSF データで、権限のある利用者以外からの閲覧や改変ができないように保護されなければならない情報。
TSF 保護データ	保護された TSF データで、公開されてもセキュリティ上の脅威とならないが、不正な改変から保護されなければならない情報。

分類ごとの、本 TOE で扱う TSF データを以下に示す。

表 10 TSF データ

分類	TSF データ	内容
TSF 秘密データ	ログインパスワード	各ログインユーザー名に対応したパスワード。
	監査ログデータ	発生事象が記録される監査ログのデータ。
	eMMC 暗号鍵	eMMC 内のデータの暗号化に利用される暗号鍵。
TSF 保護データ	ログインユーザー名	一般利用者、MFP 管理者、及びスーパーバイザーのいずれかに紐づく、利用者の識別子。TOE はその識別子により利用者を特定する。
	蓄積受信文書ユーザー	ファクス受信文書データへのアクセスを許可されている一般利用者のログインユーザー名のリストである。すべてのファクス受信文書データに対して 1 つのリストが存在する。
	ロックアウトの設定	ロックアウトポリシーやロックアウト状態に関する設定。
	日付・時刻の設定	日付、時刻に関する設定。
	パスワード品質の設定	パスワードポリシーに関する、利用者の認証のために登録する文字の最小桁数や文字種の組み合わせの設定。
	オートログアウトの設定	操作パネルのオートログアウトの設定、及び WIM のオートログアウトの設定。
	監査ログデータの設定	監査ログデータの転送に関する設定。

分類	TSF データ	内容
	暗号通信設定	クライアント、サーバーとの TLS 通信に関する設定。

3.3 脅威

本 TOE の利用、及び利用環境において想定される脅威を識別し、説明する。本項に記す脅威は、TOE の動作について公開されている情報を知識として持っている利用者であると想定する。攻撃者は基本レベルの攻撃能力を持つ者とする。

T.DOCUMENT_DATA_DIS　　利用者文書データの開示

TOE が管理している利用者文書データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって閲覧されるかもしれない。

T.DOCUMENT_DATA_ALT　　利用者文書データの改変

TOE が管理している利用者文書データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその文書へのアクセス権限をもたない者によって改変されるかもしれない。

T. JOB_ALT　　利用者ジョブデータの改変

TOE が管理している利用者ジョブデータが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブデータへのアクセス権限をもたない者によって改変されるかもしれない。

T.PROTECT_DATA_ALT　　TSF 保護データの改変

TOE が管理している TSF 保護データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護データへのアクセス権限をもたない者によって改変されるかもしれない。

T.CONFIDENTIAL_DATA_DIS　　TSF 秘密データの開示

TOE が管理している TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって閲覧されるかもしれない。

T.CONFIDENTIAL_DATA_ALT　　TSF 秘密データの改変

TOE が管理している TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって改変されるかもしれない。

3.4 組織のセキュリティ方針

TOE が従うべき事項として、下記の組織のセキュリティ方針をとる。National Institute of Standards and Technology が作成した Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 を考慮する。

P.AUTHORIZATION 利用者の識別認証

TOE 利用の許可を受けた利用者だけが TOE を利用することができるようにしなければならない。

P.VALIDATION ソフトウェア検証

TSF の実行コードを自己検証できる手段を持たなければならない。

P.AUDIT 監査ログデータの記録管理

運用の説明責任とセキュリティを維持するために、TOE のセキュリティ関連イベントの監査証跡を提供する記録は、作成され、維持され、権限を持たない者からの開示や改ざんから保護され、権限をもつ者によって確認されなければならない。

P.FAX 外部インタフェース管理

TOE が電話回線でのファクス機能を提供するにあたり、電話回線と LAN の間に分離を保証しなければならない。

P.ENCRYPTION eMMC 暗号化

TOE の eMMC に記録しているデータは、暗号化されていなければならない。

3.5 前提条件

本 TOE の利用環境に関わる前提条件を識別し、説明する。

A.PHYSICAL_PROTECTION アクセス管理

MFP 管理者は、ガイダンスに従って TOE を安全で監視下における場所に設置し、不特定多数の者から物理的にアクセスされる機会を制限しているものとする。

A.NETWORK_PROTECTION ネットワーク管理

MFP 管理者は、TOE の LAN インタフェースが外部から直接アクセスされることから保護される運用環境に TOE を設置するものとする。

A.USER 利用者教育

MFP 管理者は、一般利用者が組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っているものとする。

A.ADMIN **管理者教育**

MFP 管理者は組織のセキュリティポリシーやその手順を認識しており、ガイダンスに従ってそれらのポリシーや手順に沿った TOE の設定や処理ができるものとする。

A.TRUSTED_ADMIN **信頼できる管理者**

管理者には、ガイダンスに従ってその特権を悪用しない者が選任されているものとする。

4 セキュリティ対策方針

本章では、TOE に対するセキュリティ対策方針、運用環境に対するセキュリティ対策方針と根拠について記述する。

4.1 TOE のセキュリティ対策方針

本章では、TOE のセキュリティ対策方針を記述する。

O.DOCUMENT_DATA_DIS 利用者文書データの開示保護

TOE は、利用者文書データがログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって開示されることから、保護することを保証する。

O.DOCUMENT_DATA_ALT 利用者文書データの改変保護

TOE は、利用者文書データがログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって改変されることから、保護することを保証する。

O.JOB_ALT 利用者ジョブデータの改変保護

TOE は利用者ジョブデータが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブデータへのアクセス権限をもたない者によって改変されることからの保護を保証する。

O.PROTECT_DATA_ALT TSF 保護データの改変保護

TOE は TSF 保護データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護データへのアクセス権限をもたない者によって改変されることからの保護を保証する。

O.CONFIDENTIAL_DATA_DIS TSF 秘密データの開示保護

TOE は TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって開示されることからの保護を保証する。

O.CONFIDENTIAL_DATA_ALT TSF 秘密データの改変保護

TOE は TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって改変されることからの保護を保証する。

O.AUTHORIZATION 利用者の識別認証

TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証されることを保証する。

O.FAX TOE による外部インタフェース管理

TOE が電話回線でのファクス機能を提供するにあたり、TOE は、電話回線と LAN の間の分離を保証しなければならない。

O.VALIDATION ソフトウェア検証

TOE は TSF の実行コードを自己検証できるための手段の提供を保証する。

O.AUDIT 監査ログデータの記録管理

TOE は、TOE のセキュリティに関連する事象のログを監査ログデータとして作成して維持し、権限をもたない者による開示あるいは改変から保護することを保証する。また権限をもつ者が検証できる形式で監査ログデータを提供する。

O.EMMC_ENCRYPTION eMMC 暗号化

TOE は、eMMC に書き込むデータを、暗号化してから記録する機能を提供することを保証する。

4.2 運用環境のセキュリティ対策方針

本章では、運用環境のセキュリティ対策方針について記述する。

OE.AUDIT 高信頼 IT 製品での監査ログデータ保護

MFP 管理者は、高信頼 IT 製品にエクスポートされた監査ログデータが権限外の者からのアクセス、改変から防御できていることを保証する。

OE.PHYSICAL_PROTECTION 物理的管理

MFP 管理者は、ガイダンスに従って TOE を安全で監視下における場所に設置し、不特定多数の者から物理的にアクセスされる機会を制限することを保証する。

OE.NETWORK_PROTECTION ネットワーク管理

MFP 管理者は、TOE の LAN インタフェースが外部から直接アクセスされることから保護される運用環境に TOE を設置することを保証する。

OE.AUTHORIZED_USER 利用者への権限付与

MFP 管理者は、組織のセキュリティポリシーや手順に従って、利用者に TOE の利用権限を付与することを保証する。

OE.TRAINED_USER　利用者への教育

MFP 管理者は、利用者に組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者がそれらのポリシーや手順に沿っていることを保証する。

OE.TRAINED_ADMIN　管理者への教育

MFP 管理者はガイダンスに従って組織のセキュリティポリシーやその手順に沿った設定や処理ができるよう教育を受け、それらのポリシーや手順に従う能力をもつことを MFP 管理責任者が保証する。

OE.TRUSTED_ADMIN信頼できる管理者

管理者には、ガイダンスに従ってその特権を悪用しない者を MFP 管理責任者が選任することを保証する。

OE.AUDIT_MANAGE　ログの監査

MFP 管理者は、セキュリティ違反や異常な活動パターンを検出するために、監査ログデータの監査を適切な間隔で実施していることを保証する。

4.3　セキュリティ対策方針根拠

本章では、セキュリティ対策方針の根拠を示す。セキュリティ対策は、規定した前提条件に対応するためのもの、脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。

4.3.1　セキュリティ対策方針対応関係表

セキュリティ対策方針と対応する前提条件、対抗する脅威、実現する組織のセキュリティ方針の対応関係を表 11 に示す。

表 11：セキュリティ対策方針根拠

セキュリティ対策方針 / セキュリティ課題定義	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	OE.AUTHORIZED_USER	O.VALIDATION	O.AUDIT	OE.AUDIT	OE.AUDIT_MANAGE	O.FAX	OE.PHYSICAL_PROTECTION	OE.NETWORK_PROTECTION	O.EMMC_ENCRYPTION	OE.TRAINED_ADMIN	OE.TRUSTED_ADMIN	OE.TRAINED_USER
T.DOCUMENT_DATA_DIS	x						x	x											
T.DOCUMENT_DATA_ALT		x					x	x											
T.JOB_ALT			x				x	x											

セキュリティ対策方針 / セキュリティ課題定義	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	OE.AUTHORIZED_USER	O.VALIDATION	O.AUDIT	OE.AUDIT	OE.AUDIT_MANAGE	O.FAX	OE.PHYSICAL_PROTECTION	OE.NETWORK_PROTECTION	O.EMMC_ENCRYPTION	OE.TRAINED_ADMIN	OE.TRUSTED_ADMIN	OE.TRAINED_USER
T.PROTECT_DATA_ALT				X			X	X											
T.CONFIDENTIAL_DATA_DIS					X		X	X											
T.CONFIDENTIAL_DATA_ALT						X	X	X											
P.AUTHORIZATION							X	X											
P.VALIDATION									X										
P.AUDIT										X	X	X							
P.FAX													X						
P.ENCRYPTION																X			
A.PHYSICAL_PROTECTION														X					
A.NETWORK_PROTECTION															X				
A.ADMIN																	X		
A.TRUSTED_ADMIN																		X	
A.USER																			X

4.3.2 セキュリティ対策方針記述

以下に、各セキュリティ対策方針が脅威、前提条件、及び組織のセキュリティ方針を満たすのに適している根拠を示す。

T.DOCUMENT_DATA_DIS

T.DOCUMENT_DATA_DIS は、O.DOCUMENT_DATA_DIS、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE の利用権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.DOCUMENT_DATA_DIS により TOE は利用者文書データを、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって開示されることから保護する。

これらの対策方針により、T.DOCUMENT_DATA_DIS に対抗できる。

T.DOCUMENT_DATA_ALT

T.DOCUMENT_DATA_ALT は、O.DOCUMENT_DATA_ALT、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.DOCUMENT_DATA_ALT により TOE は、利用者文書データがログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって改変されることから保護する。

これらの対策方針により、T.DOCUMENT_DATA_ALT に対抗できる。

T.JOB_ALT

T.JOB_ALT は、O.JOB_ALT、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.JOB_ALT により TOE は利用者ジョブデータが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブデータへのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.APPLICATIONS_ALT に対抗できる。

T.PROTECT_DATA_ALT

T.PROTECT_DATA_ALT は、O.PROTECT_DATA_ALT、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従う利用者に対して、TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.PROTECT_DATA_ALT により TOE は TSF 保護データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護データへのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.PROTECT_DATA_ALT に対抗できる。

T.CONFIDENTIAL_DATA_DIS

T.CONFIDENTIAL_DATA_DIS は、O.CONFIDENTIAL_DATA_DIS、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.CONFIDENTIAL_DATA_DIS により TOE は TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって開示されることはない。

これらの対策方針により、T.CONFIDENTIAL_DATA_DIS に対抗できる。

T.CONFIDENTIAL_DATA_ALT

T.CONFIDENTIAL_DATA_ALT は、O.CONFIDENTIAL_DATA_ALT、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。O.CONFIDENTIAL_DATA_ALT により TOE は TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって改変されることはない。

これらの対策方針により、T.CONFIDENTIAL_DATA_ALT に対抗できる。

P.AUTHORIZATION

P.AUTHORIZATION は、O.AUTHORIZATION、OE.AUTHORIZED_USER によって対抗できる。

OE.AUTHORIZED_USER により、MFP 管理者は組織のセキュリティポリシーや手順に従って、利用者に TOE を利用する権限を与え、O.AUTHORIZATION により TOE は利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者が認証される。

これらの対策方針により、P.AUTHORIZATION を順守できる。

P.VALIDATION

P.VALIDATION は、O.VALIDATION によって対抗できる。

O.VALIDATION により TOE は TSF の実行コードを自己検証できる手段を提供する。

この対策方針により、P.VALIDATION を順守できる。

P.AUDIT

P.AUDIT は、O.AUDIT、OE.AUDIT、OE.AUDIT_MANAGE によって対抗できる。

O.AUDIT により、TOE は TOE のセキュリティに関連する事象のログを監査ログデータとして作成して維持し、権限をもたない者による開示あるいは改変から保護する。また、権限をもつ者が検証できる形式で監査ログデータを提供する。

一方、OE.AUDIT により、MFP 管理者は、高信頼 IT 製品にエクスポートされた監査ログデータが権限外の者からアクセス、改変されることから防御できていることを保証する。さらに OE.AUDIT_MANAGE により、MFP 管理者は、セキュリティ違反や異常な活動パターンを検出するために、監査ログデータの監査を適切な間隔で実施する。

これらの対策方針により、P.AUDIT を順守できる。

P.FAX

P.FAX は、O.FAX によって対抗できる。

O.FAX により、TOE が電話回線でのファクス機能を提供するにあたり、TOE は、電話回線と LAN の間の分離を保証する。

この対策方針により、P.FAX を順守できる。

P.ENCRYPTION

P.ENCRYPTION は、O.EMMC_ENCRYPTION によって対抗できる。

O.EMMC_ENCRYPTION により、TOE は eMMC に書き込むデータを、暗号化してから記録する機能を提供する。

この対策方針により、P.ENCRYPTION を順守できる。

A.PHYSICAL_PROTECTION

A.PHYSICAL_PROTECTION は、OE.PHYSICAL_PROTECTION によって運用する。

OE.PHYSICAL_PROTECTION により、ガイダンスに従って TOE を安全で監視下における場所に設置し、不特定多数の者から物理的にアクセスされる機会を制限する。

この対策方針により、A.PHYSICAL_PROTECTION を実現できる。

A.NETWORK_PROTECTION

A.NETWORK_PROTECTION は、OE.NETWORK_PROTECTION によって運用する。

OE.NETWORK_PROTECTION により、MFP 管理者は、TOE の LAN インタフェースが外部から直接アクセスされることから保護される運用環境に TOE を設置することを保証する。

この対策方針により、A.NETWORK_PROTECTION を実現できる。

A.ADMIN

A.ADMIN は、OE.TRAINED_ADMIN によって運用する。

OE.TRAINED_ADMIN により MFP 管理者は、ガイダンスに従って組織のセキュリティポリシーやその手順に沿った設定や処理ができるよう教育を受け、それらのポリシーや手順に従う能力をもつことを MFP 管理責任者が保証する。

この対策方針により、A.ADMIN を実現できる。

A.TRUSTED_ADMIN

A.TRUSTED_ADMIN は、OE.TRUSTED_ADMIN によって運用する。

OE.TRUSTED_ADMIN により、管理者には、ガイダンスに従ってその特権を悪用しない者を MFP 管理責任者が選任する。

この対策方針により、A.TRUSTED_ADMIN を実現できる。

A.USER

A.USER は、OE.TRAINED_USER によって運用する。

OE.TRAINED_USER により、MFP 管理者は、利用者に組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に従う。

この対策方針により、A.USER を実現できる。

5 拡張コンポーネント定義

本章では、拡張したセキュリティ機能要件を定義する。

5.1 ファクス分離 (FDP_FXS_EXP)

ファミリのふるまい

本ファミリは、TOE が接続される、ファクス電話回線と LAN の間の分離に関する要件に対処する。

コンポーネントのレベル付け

FDP_FXS_EXP.1 ファクス分離は、TOE が接続される電話回線と LAN の間で、ネットワークブリッジを作るためにファクスインタフェースが利用できないことを要求する。

管理: FDP_FXS_EXP.1

・ 予見される管理アクションはない。

監査: FDP_FXS_EXP.1

予見される監査対象事象はない。

FDP_FXS_EXP.1 ファクス分離

下位階層: なし

依存性: なし

FDP_FXS_EXP.1.1 **TSF は、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止しなければならない。**

根拠:

ファクス分離は、電話回線からの攻撃に対して LAN を保護するものである。コモンクライテリアは、TSF または利用者データの保護に適した SFR を提供していない。本拡張コンポーネントは、TSF データまたは利用者データを保護するので、FDP クラスの一つのコンポーネントとする。

5.2 TSF テスト (FPT_TST_EXP)

ファミリのふるまい

本ファミリは、TSF の実行コードの完全性を検証するための TSF の自己テスト要件に対処する。

コンポーネントのレベル付け

FPT_TST_EXP.1 TSF テストは、TSF の実行コードの完全性を検証するために、初期起動時に動作する自己テストのスイートを要求する。

管理: FPT_TST_EXP.1

・ 予見される管理アクションはない。

監査: FPT_TST_EXP.1

予見される監査対象事象はない。

FPT_TST_EXP.1 TSF テスト

下位階層: なし

依存性: なし

FPT_TST_EXP.1.1 **TSF は、TSF の実行コードの完全性を検証するために、初期起動時（及び電源投入時）に、自己テストのスイートを実行しなければならない。**

根拠:

TSF テストは、TSF の実行コードの完全性を検証することを保証するものである。コモンクライテリアが提供する SFR とは、完全性を検証する対象が異なる。本拡張コンポーネントは、TOE を保護するので、FPT クラスの一つのコンポーネントとする。

6 セキュリティ要件

本章は、セキュリティ機能要件、セキュリティ保証要件、及びセキュリティ要件根拠を述べる。
なお、本章で使用する用語を表 12 に定義する。

表 12 : 6 章で使用する用語

用語の分類	用語の名称	用語の内容
サブジェクト	一般利用者プロセス	一般利用者の認証成功時に一般利用者を代行する処理。
	MFP 管理者プロセス	MFP 管理者の認証成功時に MFP 管理者を代行する処理。
	スーパーバイザープロセス	スーパーバイザーの認証成功時にスーパーバイザーを代行する処理。
オブジェクト	機密印刷文書データ	一般利用者によるクライアント PC のプリンタードライバーからの機密印刷によって TOE に蓄積された文書データ。
	ファクス受信文書データ	TOE による外部ファクスからの電話回線を介したファクス受信によって TOE に蓄積された文書データ。
	利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報。TOE のコピー、スキャナー、プリンター、ファクス送信及びファクス受信の各機能の開始から終了までの作業に関する情報。
操作	印刷	蓄積文書データを印刷すること。
	削除	セキュリティ属性、TSF データ、またはオブジェクトを削除すること。
	変更	セキュリティ属性、TSF データを変更すること。
	問い合わせ	セキュリティ属性、TSF データを参照すること。
	新規作成	セキュリティ属性、TSF データを新規に作成すること。
	生成	TSF データを生成すること。
セキュリティ属性	ログインユーザー名	一般利用者、MFP 管理者、及びスーパーバイザーのいずれかに紐づく、利用者の識別子。TOE はその識別子により利用者を特定する。

用語の分類	用語の名称	用語の内容
	蓄積受信文書ユーザー	ファクス受信文書データへのアクセスを許可されている一般利用者のログインユーザー名のリストである。すべてのファクス受信文書データに対して 1 つのリストが存在する。
	ユーザー権限	TOE を利用する一般利用者、MFP 管理者、スーパーバイザーのいずれかの役割、及びその役割に応じた権限。
外部のエンティティ	一般利用者	TOE の使用を許可された利用者。ログインユーザー名を付与され、MFP アプリケーションの操作(コピー機能、ファクス機能、スキャナー機能、プリンター機能の実行、中止)ができる。
	MFP 管理者	TOE の管理を許可された利用者。以下のようなことができる権限をもつ。 ・一般利用者に関する設定の操作 ・MFP の機器動作に関する設定情報の操作 ・監査ログデータの操作 ・ネットワーク設定情報の操作 ・ファクス受信文書データのアクセス管理
	スーパーバイザー	TOE の管理を許可された利用者。MFP 管理者のログインパスワードを変更する権限をもつ。

6.1 セキュリティ機能要件

この章では、4.1 章で規定されたセキュリティ対策方針を実現するための、TOE のセキュリティ機能要件を記述する。

6.1.1 クラス FAU: セキュリティ監査

6.1.1.1. FAU_GEN.1 監査データ生成

下位階層: なし

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1 **TSF は、以下の監査対象事象の監査記録を生成できなければならない:**

a) 監査機能の起動と終了;

b) 監査の[選択: *最小*、*基本*、*詳細*、*指定なし*: から 1 つのみ選択]レベルのすべての監査対象事象;及び

c) [割付: *上記以外の個別に定義した監査対象事象*]。

[選択: *最小*、*基本*、*詳細*、*指定なし*: から 1 つのみ選択]

- ***指定なし***

[割付: ***上記以外の個別に定義した監査対象事象*****]**

- ***表 13 に示すTOE の監査対象事象***

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

[割付: ***その他の監査関連情報*****]**

- ***FIA_UID.1 における利用者識別を試みた全てのログインユーザー名、ログタイプ、高信頼チャネルとの通信先、ロックアウト操作種別、ロックアウト対象者、ロックアウト解除対象者***

関連 SFR と TOE が監査対象とする事象を表 13 に記す。

表 13 : 監査対象事象リスト

監査対象事象	関連 SFR
監査ログデータのダウンロードと削除	FAU_STG.1 FAU_SAR.1 FAU_SAR.2
機密印刷文書データの印刷の開始と終了 機密印刷文書データの削除 ファクス受信文書データの印刷の開始と終了 利用者ジョブデータの削除	FDP_ACF.1
ロックアウトの開始と解除	FIA_AFL.1
ログイン操作の成功と失敗	FIA_UAU.1 FIA_UID.1
表 24 管理機能の使用	FMT_SMF.1
オートログアウトによるセションの終了	FTA_SSL.3
高信頼チャネルとの通信の失敗 (スキャナーからの文書添付メール送信の失敗、 syslog転送の失敗、 ネットワークを介したPCファクスの失敗、 ネットワークを介した機密印刷の失敗、 WIMの通信の失敗)	FTP_ITC.1

6.1.1.2. FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

依存性: FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_GEN.2.1 **識別された利用者のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。**

6.1.1.3. FAU_STG.1 保護された監査証跡格納

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1.1 **TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。**

FAU_STG.1.2 **TSF は、監査証跡に格納された監査記録への不正な改変を[選択: *防止*、*検出*: から 1 つのみ選択]できなければならない。**

[選択: *防止*、*検出*: から 1 つのみ選択]

- ***防止***

6.1.1.4. FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が**満杯**になった場合、**[選択: *監査事象の無視*、*特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止*、*最も古くに格納された監査記録への上書き*: から 1 つのみ選択]及び**[割付: *監査格納失敗時にとられる**その他の**アクション*]を行わなければならない。

[選択: *監査事象の無視*、*特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止*、*最も古くに格納された監査記録への上書き*: から 1 つのみ選択]

- ***最も古くに格納された監査記録への上書き***

[割付: *監査格納失敗時にとられる**その他の**アクション*]

- *なし*

6.1.1.5. FAU_SAR.1 監査レビュー

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

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*]

- ***MFP 管理者***

[割付: *監査情報のリスト*]

- *すべての監査ログデータ*

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。**

6.1.1.6. FAU_SAR.2 限定監査レビュー

下位階層: なし

依存性: FAU_SAR.1 監査レビュー

FAU_SAR.2.1 **TSF は、明示的な読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出しアクセスを禁止しなければならない。**

6.1.2 クラス FCS: 暗号サポート

6.1.2.1. FCS_CKM.1 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2 暗号鍵配付、または FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 **TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。**

[割付: *標準のリスト*]

- ***NIST SP 800-90A***

[割付: *暗号鍵生成アルゴリズム*]

- ***Hash_DRBG(SHA256)***

[割付: *暗号鍵長*]

- ***256 ビット***

6.1.2.2. FCS_CKM.4 暗号鍵破棄

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]

FCS_CKM.4.1 **TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵破棄方法 [割付: *暗号鍵破棄方法*]に従って、暗号鍵を破棄しなければならない。**

[割付: *標準のリスト*]

- *なし*

[割付：*暗号鍵破棄方法*]

- ***0 で上書きする***

6.1.2.3. FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSF は、[割付：*標準のリスト*]に合致する、特定された暗号アルゴリズム[割付：*暗号アルゴリズム*]と暗号鍵長[割付：*暗号鍵長*]に従って、[割付：*暗号操作のリスト*]を実行しなければならない。**

[割付：*標準のリスト*]

- ***FIPS197***

[割付：*暗号アルゴリズム*]

- ***AES***

[割付：*暗号鍵長*]

- ***256 ビット***

[割付：*暗号操作のリスト*]

- ***eMMC に書き込むデータの暗号化、***
  eMMC から読み込むデータの復号

6.1.3 クラス FDP: 利用者データ保護

6.1.3.1. FDP_ACC.1 サブセットアクセス制御

下位階層: なし

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

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

- ***表 14 に示すサブジェクト、オブジェクト、及びサブジェクトとオブジェクト間の操作のリスト***

[割付：*アクセス制御 SFP*]

- ***利用者データアクセス制御 SFP***

表 14：サブジェクト、オブジェクト、及び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	オブジェクト	操作
一般利用者プロセス MFP 管理者プロセス スーパーバイザープロセス	機密印刷文書データ	印刷 削除 変更
	ファクス受信文書データ	印刷 削除 変更
一般利用者プロセス MFP 管理者プロセス スーパーバイザープロセス	利用者ジョブデータ	削除 変更

6.1.3.2. FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

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

FDP_ACF.1.1 **TSF は、以下の[割付：*示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付：*アクセス制御 SFP*]を実施しなければならない。**

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

- ***表 15 に示すサブジェクトまたはオブジェクトと、各々に対応するセキュリティ属性***

[割付：*アクセス制御 SFP*]

- ***利用者データアクセス制御 SFP***

表 15：サブジェクトとオブジェクトとセキュリティ属性

サブジェクトまたはオブジェクト	セキュリティ属性
一般利用者プロセス	ログインユーザー名
MFP 管理者プロセス	ユーザー権限
スーパーバイザープロセス	ユーザー権限
機密印刷文書データ	ログインユーザー名
ファクス受信文書データ	蓄積受信文書ユーザー
利用者ジョブデータ	ログインユーザー名

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

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

- ***表 16 に示すオブジェクトとサブジェクト間の操作を制御する規則***

表 16: オブジェクトとサブジェクト間の操作を制御する規則

サブジェクト (セキュリティ属性)	オブジェクト (セキュリティ属性)	操作	利用者データアクセス制御 SFP の規則
一般利用者プロセス (ログインユーザー名)	機密印刷文書データ (ログインユーザー名)	印刷 削除	一般利用者プロセスのログインユーザー名と、機密印刷文書データを作成した利用者のログインユーザー名が一致した場合のみ印刷及び削除の操作を許可する。
一般利用者プロセス (ログインユーザー名)	ファクス受信文書データ (蓄積受信文書ユーザー)	印刷	一般利用者プロセスのログインユーザー名と蓄積受信文書ユーザーに登録されているログインユーザー名が一致した場合のみ印刷の操作を許可する。
一般利用者プロセス (ログインユーザー名)	利用者ジョブデータ (ログインユーザー名)	削除	一般利用者プロセスのログインユーザー名と利用者ジョブデータのログインユーザー名が一致した場合のみ削除の操作を許可する。

FDP_ACF.1.3 **TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。**

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

- ***表 17 に示すアクセスを明示的に許可する規則***

表 17: アクセスを明示的に許可する規則

サブジェクト (セキュリティ属性)	オブジェクト (セキュリティ属性)	操作	利用者データアクセス制御 SFP の規則
MFP 管理者プロセス (ユーザー権限)	機密印刷文書データ (ログインユーザー名)	削除	MFP 管理者のユーザー権限をもつ MFP 管理者プロセスには、機密印刷文書データの削除の操作を許可する。

サブジェクト (セキュリティ属性)	オブジェクト (セキュリティ属性)	操作	利用者データアクセス制御 SFP の規則
MFP 管理者プロセス (ユーザー権限)	利用者ジョブデータ (ログインユーザー名)	削除	MFP 管理者のユーザー権限をもつ MFP 管理者プロセスには、利用者ジョブデータの削除の操作を許可する。

FDP_ACF.1.4 **TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。**

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

- ***表 18 に示すアクセスを明示的に拒否する規則***

表 18 : アクセスを明示的に拒否する規則

サブジェクト (セキュリティ属性)	オブジェクト (セキュリティ属性)	操作	利用者データアクセス制御 SFP の規則
MFP 管理者プロセス (ユーザー権限)	機密印刷文書データ (ログインユーザー名)	印刷	MFP 管理者のユーザー権限をもつ MFP 管理者プロセスには、機密印刷文書データの印刷の操作を拒否する。
MFP 管理者プロセス (ユーザー権限)	ファクス受信文書データ (ファクス受信文書ユーザー)	印刷	MFP 管理者のユーザー権限をもつ MFP 管理者プロセスには、ファクス受信文書データの印刷の操作を拒否する。
スーパーバイザープロセス (ユーザー権限)	機密印刷文書データ (ログインユーザー名)	印刷 削除	スーパーバイザーのユーザー権限をもつスーパーバイザープロセスには機密印刷文書データの印刷及び削除の操作を拒否する。
スーパーバイザープロセス (ユーザー権限)	ファクス受信文書データ (ファクス受信文書ユーザー)	印刷	スーパーバイザーのユーザー権限をもつスーパーバイザープロセスにはファクス受信文書データの印刷の操作を拒否する。
スーパーバイザープロセス (ユーザー権限)	利用者ジョブデータ (ログインユーザー名)	削除	スーパーバイザーのユーザー権限をもつスーパーバイザープロセスには利用者ジョブデータの削除の操作を拒否する。
一般利用者プロセス (ログインユーザー名)	機密印刷文書データ (ログインユーザー名)	変更	いずれのサブジェクトにも、機密印刷文書データの変更の操作を拒否する。 (*1)
MFP 管理者プロセス (ユーザー権限)			

スーパーバイザープロセス (ユーザー権限)			
一般利用者プロセス (ログインユーザー名)	ファクス受信文書データ (ファクス受信文書ユーザー)	削除 変更	いずれのサブジェクトにも、ファクス受信文書データの削除及び変更の操作を拒否する。 (*2)
MFP 管理者プロセス (ユーザー権限)			
スーパーバイザープロセス (ユーザー権限)			
一般利用者プロセス (ログインユーザー名)	利用者ジョブデータ (ログインユーザー名)	変更	いずれのサブジェクトにも、利用者ジョブデータの変更の操作を拒否する。 (*3)
MFP 管理者プロセス (ユーザー権限)			
スーパーバイザープロセス (ユーザー権限)			

(*1) 本 TOE には機密印刷文書データに対して変更を行うインタフェースはない。

(*2) 本 TOE にはファクス受信文書データに対して変更及び削除を行うインタフェースはない。

(*3) 本 TOE には利用者ジョブデータに対して変更を行うインタフェースはない。

6.1.3.3. FDP_FXS_EXP.1 ファクス分離

下位階層: なし

依存性: なし

FDP_FXS_EXP.1.1 **TSF は、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止しなければならない。**

6.1.4 クラス FIA: 識別と認証

6.1.4.1. FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 **TSF は、[割付: 認証事象のリスト]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。**

[割付: *認証事象のリスト*]

- ***表 19 に示す認証事象***

[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]

- ***[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値***

[割付: 許容可能な値の範囲]

- ***1～10***

表 19 : 認証事象のリスト

認証事象
操作パネルを使用する利用者認証
WIM を使用する際の利用者認証
プリンタードライバーから機密印刷する際の利用者認証
ファクスドライバーからファクス送信する際の利用者認証

FIA_AFL.1.2 **不成功の認証試行が定義した回数[選択: *に達する、を上回った*]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。**

[選択: *に達する、を上回った*]

- ***に達する***

[割付: *アクションのリスト*]

- ***表 20 に示すアクション***

表 20 : 認証失敗時のアクションのリスト

認証不成功者	認証失敗時アクション
一般利用者	MFP 管理者が設定したロックアウト時間、もしくは MFP 管理者が解除するまでロックアウト
スーパーバイザー	MFP 管理者が設定したロックアウト時間、もしくは MFP 管理者が解除、もしくは電源のオフ/オン後一定時間経過するまでロックアウト
MFP 管理者	MFP 管理者が設定したロックアウト時間、もしくはスーパーバイザーが解除、もしくは電源のオフ/オン後一定時間経過するまでロックアウト

6.1.4.2. FIA_ATD.1 利用者属性定義

下位階層: なし

依存性: なし

FIA_ATD.1.1 **TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]**

[割付: *セキュリティ属性のリスト*]

- ***ログインユーザー名、ユーザー権限***

6.1.4.3. FIA_SOS.1 秘密の検証

下位階層: なし

依存性: 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*]

- ***以下の品質尺度***

(1) ***英大文字、英小文字、数字、記号のうち複数の文字種を使うこと(必要な種類数は MFP 管理者がパスワード複雑度として設定する)***

(2) パスワード最小桁数(8～32 桁で MFP 管理者が設定する)以上の半角英数記号であること、かつ

・一般利用者の場合、128 桁以下であること

・MFP 管理者またはスーパーバイザーの場合、32 桁以下であること

6.1.4.4. FIA_UAU.1 認証のタイミング

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 **TSF は、利用者が認証される前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。**

[割付: *TSF 仲介アクションのリスト*]

- ***利用者ジョブデータ一覧の参照、WIM のヘルプの参照、システム状態の参照、カウンタの参照、問い合わせ情報の参照、ファクス受信の実行***

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

6.1.4.5. FIA_UAU.7 保護された認証フィードバック

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

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*]

- ***ダミー文字***

6.1.4.6. FIA_UID.1 識別のタイミング

下位階層: なし

依存性: なし

FIA_UID.1.1 **TSF** は、利用者が識別される前に利用者を代行して実行される**[**割付: ***TSF* 仲介アクションのリスト***]**を許可しなければならない。

[割付: ***TSF* 仲介アクションのリスト***]***

- *利用者ジョブデーター覧の参照*、*WIM* のヘルプの参照、*システム状態の参照*、*カウンタの参照*、*問い合わせ情報の参照*、*ファクス受信の実行*

FIA_UID.1.2 **TSF** は、その利用者を代行する他の **TSF** 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.4.7. FIA_USB.1 利用者-サブジェクト結合

下位階層: なし

依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 **TSF** は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。**: [**割付: *利用者セキュリティ属性のリスト***]**

[割付: *利用者セキュリティ属性のリスト***]***

- *ログインユーザー名*、*ユーザー権限*

FIA_USB.1.2 **TSF** は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。**: [**割付: *属性の最初の関連付けの規則***]**

[割付: *属性の最初の関連付けの規則***]***

- *なし*

FIA_USB.1.3 **TSF** は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。**: [**割付: *属性の変更の規則***]**

[割付: *属性の変更の規則***]***

- *なし*

6.1.5 クラス FMT: セキュリティ管理

6.1.5.1. 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

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

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*]

- ***syslog 転送機能***

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

- ***を停止する、を動作させる***

[割付: *許可された識別された役割*]

- ***MFP 管理者***

6.1.5.2. FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

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 セキュリティの役割
FMT_SMF.1 管理機能の特定

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[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*]

- *表 21 のセキュリティ属性*

[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、[割付: その他の操作]***

[割付: その他の操作]

- ***新規作成、変更***

[割付: *許可された識別された役割*]

- *表 21 の操作を許可する役割(ユーザー権限)*

[割付: *アクセス制御 SFP、情報フロー制御 SFP*]

- ***利用者データアクセス制御 SFP***

表 21：セキュリティ属性のユーザー権限

セキュリティ属性	操作	操作を許可する役割(ユーザー権限)
ログインユーザー名 [一般利用者に紐づく場合]	変更 削除 新規作成	MFP 管理者
ログインユーザー名 [スーパーバイザーに紐づく場合]	変更	スーパーバイザー
ログインユーザー名 [MFP 管理者に紐づく場合]	変更	MFP 管理者
蓄積受信文書ユーザー	変更	MFP 管理者

6.1.5.3. FMT_MSA.3 静的属性初期化

下位階層: なし

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

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に対して[選択: *制限的*、*許可的*、*[割付: その他の特性]*: から 1 つのみ選択]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。**

[選択: *制限的*、*許可的*、*[割付: その他の特性]*: から 1 つのみ選択]

- ***制限的***

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]

- ***利用者データアクセス制御 SFP***

FMT_MSA.3.2 **TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。**

[割付: *許可された識別された役割*]

- ***許可された識別された役割なし***

6.1.5.4. FMT_MTD.1(a) TSF データの管理

下位階層: なし

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

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

[割付: *TSF データのリスト*]

- ***表 22 の TSF データ***

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

- ***問い合わせ*、*削除*、*[割付: その他の操作]***

[割付: その他の操作]

- ***新規作成*、*変更*、*生成***

[割付: *許可された識別された役割*]

- ***表 22 の操作を許可する役割(ユーザー権限)***

表 22 : TSF データのリスト

分類	TSF データ	操作	操作を許可する役割(ユーザー権限)
TSF 秘密データ	ログインパスワード [一般利用者に紐づく場合]	新規作成 変更	MFP 管理者
	ログインパスワード [当該一般利用者本人に紐づく場合]	変更	当該一般利用者
	ログインパスワード [スーパーバイザーに紐づく場合]	変更	スーパーバイザー
	ログインパスワード [MFP 管理者に紐づく場合]	変更	スーパーバイザー MFP 管理者
	eMMC 暗号鍵	問い合わせ 削除 生成	MFP 管理者
TSF 保護データ	ロックアウトの設定	変更	MFP 管理者 スーパーバイザー(*1)
	日付・時刻の設定	変更	MFP 管理者
	パスワード品質の設定	変更	MFP 管理者
	オートログアウトの設定	変更	MFP 管理者
	監査ログデータの設定	変更	MFP 管理者
	暗号通信設定	変更	MFP 管理者

(*1): スーパーバイザーはロックアウトの設定のうち、MFP 管理者に対するロックアウト解除操作のみができる。それ以外のロックアウトの設定は MFP 管理者が行う。

6.1.5.5. FMT_MTD.1(b) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

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

[割付: *TSF データのリスト*]

- 表 23 *の TSF データ*

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

- *問い合わせ*

[割付: *許可された識別された役割*]

- 表 23 *の操作を許可する役割(ユーザー権限)*

表 23 : TSF データのリスト

分類	TSF データ	操作	操作を許可する役割(ユーザー権限)
TSF 秘密データ	ログインパスワード	問い合わせ	操作を許可する役割なし

6.1.5.6. FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 **TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]**

[割付: *TSF によって提供される管理機能のリスト*]

- *表 24 に記す管理機能*

表 24 : 管理機能の特定のリスト

管理機能
syslog 転送機能の停止、動作
ログインパスワードの新規作成、変更
eMMC 暗号鍵の問い合わせ、削除、生成
ログインユーザー名の新規作成、変更、削除
蓄積受信文書ユーザーの変更
ロックアウトの設定の変更
日付・時刻の設定の変更
パスワード品質の設定の変更
オートログアウトの設定の変更

監査ログデータの設定の変更
暗号通信設定の変更

6.1.5.7. FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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*]

- ***一般利用者、スーパーバイザー、MFP 管理者***

FMT_SMR.1.2 **TSF は、利用者を役割に関連付けなければならない。**

6.1.6 クラス FPT: TSF の保護

6.1.6.1. FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

依存性: なし

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

6.1.6.2. FPT_TST_EXP.1 TSF テスト

下位階層: なし

依存性: なし

FPT_TST_EXP.1.1 **TSF は、TSF の実行コードの完全性を検証するために、初期起動時（及び電源投入時）に、自己テストのスイートを実行しなければならない。**

6.1.7 クラス FTA: TOE アクセス

6.1.7.1. FTA_SSL.3 TSF 起動による終了

下位階層: なし

依存性: なし

FTA_SSL.3.1 **TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。**

[割付: *利用者が非アクティブである時間間隔*]

- ***操作パネルオートログアウト時間経過、WIM オートログアウト時間経過***

6.1.8 クラス FTP: 高信頼パス/チャネル

6.1.8.1. FTP_ITC.1 TSF 間高信頼チャネル

下位階層: なし

依存性: なし

FTP_ITC.1.1 **TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。**

FTP_ITC.1.2 **TSF は、[選択: *TSF、他の高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。**

[選択: *TSF、他の高信頼 IT 製品*]

- ***TSF、他の高信頼 IT 製品***

FTP_ITC.1.3 **TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。**

[割付: *高信頼チャネルが要求される機能のリスト*]

- ***スキャナーからの文書添付メール送信機能***
- ***syslog 転送機能***
- ***ファクス機能***
- ***プリンター機能***
- ***WIM 機能***

6.2 セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 である。TOE の保証コンポーネントを表 25 に示す。

表 25 : TOE セキュリティ保証要件(EAL2)

保証クラス	保証コンポーネント	
ADV: 開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.2	セキュリティ実施機能仕様
	ADV_TDS.1	基本設計
AGD: ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ALC: ライフサイクルサポート	ALC_CMC.2	CM システムの使用
	ALC_CMS.2	TOE の一部の CM 範囲

保証クラス	保証コンポーネント	
	ALC_DEL.1	配付手続き
ASE: セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
ATE: テスト	ATE_COV.1	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.2	脆弱性分析

6.3 セキュリティ要件根拠

本章では、セキュリティ要件の根拠を述べる。

以下に示すように、すべてのセキュリティ機能要件が満たされた場合、「4 セキュリティ対策方針」で定義した TOE のセキュリティ対策方針は達成される。

6.3.1 追跡性

TOE のセキュリティ対策方針に対するセキュリティ機能要件の対応関係を下記の表 26 に示す。**太字**で記載した項目は対策方針の主要(**P**)な実現を提供し、標準書体で記載した項目は、その実現を支援(S)する。表 26から明らかなように、セキュリティ機能要件が少なくとも1つ以上のセキュリティ対策方針に対応している。

表 26 : セキュリティ対策方針と機能要件の関連

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FAU_GEN.1										**P**	

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FAU_GEN.2										**P**	
FAU_STG.1						**P**				**P**	
FAU_STG.4										S	
FAU_SAR.1					**P**					**P**	
FAU_SAR.2					**P**					**P**	
FCS_CKM.1											S
FCS_CKM.4											S
FCS_COP.1											**P**
FDP_ACC.1	**P**	**P**	**P**								
FDP_ACF.1	**P**	**P**	**P**								
FDP_FXS_EXP.1								**P**			
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1							S				
FIA_UAU.1							**P**				
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**			S	
FIA_USB.1							**P**				
FMT_MOF.1				**P**							
FMT_MSA.1	S	S	S	**P**							
FMT_MSA.3	S	S	S								
FMT_MTD.1(a)				**P**	**P**	**P**					
FMT_MTD.1(b)					**P**	**P**					
FMT_SMF.1	S	S	S	S	S	S					
FMT_SMR.1	S	S	S	S	S	S					
FPT_STM.1										S	
FPT_TST_EXP.1									**P**		
FTA_SSL.3							S				
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

6.3.2 追跡性の正当化

対応付けられたTOEセキュリティ機能要件によってTOEセキュリティ対策方針が実現できることを以下に説明する。

O.DOCUMENT_DATA_DIS 利用者文書データの開示保護

O.DOCUMENT_DATA_DIS は、利用者文書データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって開示されることを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、以下の SFR を実施する必要がある。

(1) FDP_ACC.1、FDP_ACF.1
FDP_ACC.1 と FDP_ACF.1 によって、利用者文書データに対してのアクセス制御方針を規定し、そのアクセス制御方針に従ったアクセス制御機能を提供する。

FDP_ACC.1 及び FDP_ACF.1 は O.DOCUMENT_DATA_DIS を達成する主要な SFR である。

(2) FTP_ITC.1
FTP_ITC.1 によって、TOE が LAN 経由で送受信する利用者文書データを保護する。

FTP_ITC.1 は O.DOCUMENT_DATA_DIS を達成する主要な SFR である。

(3) FMT_MSA.1

FMT_MSA.1 によって、セキュリティ属性の管理を特定の利用者だけに制限する。

FMT_MSA.1 は O.DOCUMENT_DATA_DIS の達成を支援する SFR である。

(4) FMT_MSA.3
FMT_MSA.3 によって、利用者文書データを生成するとき、そのセキュリティ属性には、必ず制限的な値をセットする。

FMT_MSA.3 は O.DOCUMENT_DATA_DIS の達成を支援する SFR である。

(5) FMT_SMF.1
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.DOCUMENT_DATA_DIS の達成を支援する SFR である。

(6) FMT_SMR.1
FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.DOCUMENT_DATA_DIS の達成を支援する SFR である。

(7) FIA_UID.1
FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.DOCUMENT_DATA_DIS の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.DOCUMENT_DATA_DIS を実現できる。

O.DOCUMENT_DATA_ALT 利用者文書データの改変保護

O.DOCUMENT_DATA_ALT は、利用者文書データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者文書データへのアクセス権限をもたない者によって改変される

ことを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FDP_ACC.1、FDP_ACF.1
FDP_ACC.1 と FDP_ACF.1 によって、利用者文書データに対してのアクセス制御方針を規定し、そのアクセス制御方針に従ったアクセス制御機能を提供する。

FDP_ACC.1 及び FDP_ACF.1 は O.DOCUMENT_DATA_ALT を達成する主要な SFR である。

(2) FTP_ITC.1
FTP_ITC.1 によって、TOE が LAN 経由で送受信する利用者文書データを保護する。

FTP_ITC.1 は O.DOCUMENT_DATA_ALT を達成する主要な SFR である。

(3) FMT_MSA.1

FMT_MSA.1 によって、セキュリティ属性の管理を特定の利用者だけに制限する。

FMT_MSA.1 は O.DOCUMENT_DATA_ALT の達成を支援する SFR である。

(4) FMT_MSA.3
FMT_MSA.3 によって、利用者文書データを生成するとき、そのセキュリティ属性には、必ず制限的な値をセットする。

FMT_MSA.3 は O.DOCUMENT_DATA_ALT の達成を支援する SFR である。

(5) FMT_SMF.1
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.DOCUMENT_DATA_ALT の達成を支援する SFR である。

(6) FMT_SMR.1
FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.DOCUMENT_DATA_ALT の達成を支援する SFR である。

(7) FIA_UID.1
FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.DOCUMENT_DATA_ALT の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.DOCUMENT_DATA_ALT を実現できる。

O.JOB_ALT 利用者ジョブデータの改変保護

O.JOB_ALT は、利用者ジョブデータが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその利用者ジョブデータへのアクセス権限をもたない者によって改変されることを防ぐセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FDP_ACC.1、FDP_ACF.1
FDP_ACC.1 と FDP_ACF.1 によって、利用者ジョブデータに対してのアクセス制御方針を規定し、そのアクセス制御方針に従ったアクセス制御機能を提供する。

FDP_ACC.1 及び FDP_ACF.1 は O.JOB_ALT を達成する主要な SFR である。

(2) FTP_ITC.1
FTP_ITC.1 によって、TOE が LAN 経由で送受信する利用者ジョブデータを保護する。

FTP_ITC.1 は O.JOB_ALT を達成する主要な SFR である。

(3) FMT_MSA.1

FMT_MSA.1 によって、セキュリティ属性の管理を特定の利用者だけに制限する。

FMT_MSA.1 は O.JOB_ALT の達成を支援する SFR である。

(4) FMT_MSA.3

FMT_MSA.3 によって、利用者ジョブデータを生成した時、利用者ジョブデータ(オブジェクト)のセキュリティ属性には、制限的な値をセットする。

FMT_MSA.3 は O.JOB_ALT の達成を支援する SFR である。

(5) FMT_SMF.1

FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.JOB_ALT の達成を支援する SFR である。

(6) FMT_SMR.1

FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.JOB_ALT の達成を支援する SFR である。

(7) FIA_UID.1

FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.JOB_ALT の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.JOB_ALT を実現できる。

O.PROTECT_DATA_ALT　TSF 保護データの改変保護

O.PROTECT_DATA_ALT は、TSF 保護データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護データへのアクセス権限をもたない者によって改変されることから保護するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FMT_MTD.1(a)

FMT_MTD.1(a)によって、TSF 保護データの操作を、許可された利用者のみに制限する。

FMT_MTD.1(a)は O.PROTECT_DATA_ALT を達成する主要な SFR である。

(2) FMT_SMF.1

FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.PROTECT_DATA_ALT の達成を支援する SFR である。

(3) FMT_SMR.1

FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.PROTECT_DATA_ALT の達成を支援する SFR である。

(4) FTP_ITC.1

FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 保護データは保護される。

FTP_ITC.1 は O.PROTECT_DATA_ALT を達成する主要な SFR である。

(5) FMT_MOF.1

FMT_MOF.1 によって、MFP 管理者のみがセキュリティ機能の管理を行うことができる。

FMT_MOF.1 は O.PROTECT_DATA_ALT を達成する主要な SFR である。

(6) FMT_MSA.1

FMT_MSA.1 によって、セキュリティ属性の管理を特定の利用者だけに制限する。

FMT_MSA.1 は O.PROTECT_DATA_ALT を達成する主要な SFR である。

(7) FIA_UID.1

FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.PROTECT_DATA_ALT の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.PROTECT_DATA_ALT を実現できる。

O.CONFIDENTIAL_DATA_DIS　TSF 秘密データの開示保護

O.CONFIDENTIAL_DATA_DIS は、TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 秘密データへのアクセス権限をもたない者によって開示されることから保護するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FMT_MTD.1(a)、FMT_MTD.1(b)

FMT_MTD.1(a)と FMT_MTD.1(b)によって、TSF 秘密データの操作を、許可された利用者のみに制限する。

FMT_MTD.1(a)及び FMT_MTD.1(b)は O.CONFIDENTIAL_DATA_DIS を達成する主要な SFR である。

(2) FMT_SMF.1

FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.CONFIDENTIAL_DATA_DIS の達成を支援する SFR である。

(3) FMT_SMR.1

FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.CONFIDENTIAL_DATA_DIS の達成を支援する SFR である。

(4) FTP_ITC.1

FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 秘密データを保護する。

FTP_ITC.1 は O.CONFIDENTIAL_DATA_DIS を達成する主要な SFR である。

(5) FIA_UID.1

FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.CONFIDENTIAL_DATA_DIS の達成を支援する SFR である。

(6) FAU_SAR.1、FAU_SAR.2

FAU_SAR.1 によって、MFP 管理者が検証できる形式で監査ログデータを読み出せるようにし、FAU_SAR.2 によって、MFP 管理者以外が監査ログデータを読み出すことを禁止する。

FAU_SAR.1 及び FAU_SAR.2 は O.CONFIDENTIAL_DATA_DIS を達成する主要な SFR である。

これらのセキュリティ機能要件を実施することで O.CONFIDENTIAL_DATA_DIS を実現できる。

O.CONFIDENTIAL_DATA_ALT　TSF 秘密データの改変保護

O.CONFIDENTIAL_DATA_ALT は、TSF 秘密データが、ログインユーザー名をもたない者、あるいは、ログインユーザー名はもっているがその TSF 保護データへのアクセス権限をもたない者によって改変されることから保護するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FMT_MTD.1(a)、FMT_MTD.1(b)
FMT_MTD.1(a)と FMT_MTD.1(b)によって、TSF 秘密データの操作を、許可された利用者のみに制限する。

FMT_MTD.1(a)及び FMT_MTD.1(b)は O.CONFIDENTIAL_DATA_ALT を達成する主要な SFR である。

(2) FMT_SMF.1
FMT_SMF.1 によって、セキュリティ機能に対して必要な管理機能を実施する。

FMT_SMF.1 は O.CONFIDENTIAL_DATA_ALT の達成を支援する SFR である。

(3) FMT_SMR.1
FMT_SMR.1 によって、許可された利用者の役割を維持する。

FMT_SMR.1 は O.CONFIDENTIAL_DATA_ALT の達成を支援する SFR である。

(4) FTP_ITC.1
FTP_ITC.1 によって、TOE が LAN 経由で送受信する TSF 秘密データを保護する。

FTP_ITC.1 は O.CONFIDENTIAL_DATA_ALT を達成する主要な SFR である。

(5) FIA_UID.1
FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.CONFIDENTIAL_DATA_ALT の達成を支援する SFR である。

(6) FAU_STG.1
FAU_STG.1 によって監査ログデータを改変から保護する。

FAU_STG.1 は O.CONFIDENTIAL_DATA_ALT を達成する主要な SFR である。

これらのセキュリティ機能要件を実施することで O.CONFIDENTIAL_DATA_ALT を実現できる。

O.AUTHORIZATION 利用者の識別認証

O.AUTHORIZATION は、TOE が利用者の識別認証を要求し、セキュリティポリシーに従って TOE 利用許可に先だって利用者を認証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FIA_UID.1、FIA_UAU.1
FIA_UID.1 と FIA_UAU.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者に対して、識別認証が行われる。

FIA_UID.1 及び FIA_UAU.1 は O.AUTHORIZATION を達成する主要な SFR である。

(2) FIA_ATD.1、FIA_USB.1
FIA_ATD.1 と FIA_USB.1 によって、予め定義された利用者の保護資産へのアクセス手段を管理し、識別認証に成功した利用者に対して関連付ける。

FIA_USB.1 は O.AUTHORIZATION を達成する主要な SFR であり、FIA_ATD.1 は O.AUTHORIZATION の達成を支援する SFR である。

(3) FIA_UAU.7

FIA_UAU.7 によって、ダミー文字を認証フィードバックとして表示することで、ログインパスワードの開示を防止する。

FIA_UAU.7 は O.AUTHORIZATION の達成を支援する SFR である。

(4) FIA_SOS.1

FIA_SOS.1 によって、MFP 管理者が設定するパスワードの最小桁数、パスワードの文字種組合せを満たすパスワードだけの登録を許可することでログインパスワードの推測を困難にする。

FIA_SOS.1 は O.AUTHORIZATION の達成を支援する SFR である。

(5) FIA_AFL.1

FIA_AFL.1 によって、認証失敗を一定回数繰り返した利用者に対して、一定時間 TOE へのアクセスを許可しない。

FIA_AFL.1 は O.AUTHORIZATION の達成を支援する SFR である。

(6) FTA_SSL.3

FTA_SSL.3 によって、ログイン状態の利用者による操作パネル、あるいは WIM の操作が一定時間行われないと、TOE からオートログアウトし、ログイン状態を解除する。よって利用者のセションが管理され、非アクティブなままのセションは終了される。

FTA_SSL.3 は O.AUTHORIZATION の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.AUTHORIZATION を実現できる。

なお TOE が識別認証を行うケースのうち、プリンタードライバー及びファクスドライバーからの要求に対し識別認証を行うときは、文書データの受信完了とともにログイン状態が終了する。よってこのとき持続する対話セションはないため、FTA_SSL.3 で示す必要はない。

O.FAX　TOE による外部インタフェース管理

O.FAX は、TOE が電話回線でのファクス機能を提供するにあたり、TOE は、電話回線と LAN の間の分離を保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FDP_FXS_EXP.1

FDP_FXS_EXP.1 によって、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止する。

FDP_FXS_EXP.1 は O.FAX を達成する主要な SFR である。

このセキュリティ機能要件を実施することで O.FAX を実現できる。

O.VALIDATION ソフトウェア検証

O.VALIDATION は、TOE が TSF の実行コードを自己検証できるための手段の提供を保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FPT_TST_EXP.1

FPT_TST_EXP.1 によって、TSF の実行コードの完全性を検証するために、初期起動時（及び電源投入時）に、自己テストのスイートを実行する。

FPT_TST_EXP.1 は O.VALIDATION を達成する主要な SFR である。

このセキュリティ機能要件を実施することで O.VALIDATION を実現できる。

O.AUDIT 監査ログデータの記録管理

O.AUDIT は、TOE が TOE のセキュリティに関連する事象のログを監査ログデータとして作成して維持し、権限をもたない者による開示あるいは改変から保護することを保証し、権限をもつ者が検証できる形式で監査ログデータを提供するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FAU_GEN.1、FAU_GEN.2
FAU_GEN.1とFAU_GEN.2 によって、監査対象とすべき事象を監査対象とすべき事象の発生要因の識別情報とともに記録する。

FAU_GEN.1 及び FAU_GEN.2 は O.AUDIT を達成する主要な SFR である。

(2) FAU_STG.1

FAU_STG.1 によって監査ログデータを改変から保護する。

FAU_STG.1 は O.AUDIT を達成する主要な SFR である。

(3) FAU_STG.4

FAU_STG.4 によって監査ログデータのファイルが満杯の状態で監査対象の事象が発生した場合は、タイムスタンプの最も古い監査ログデータを削除し、新しい監査ログデータを記録する。

FAU_STG.4 は O.AUDIT の達成を支援する SFR である。

(4) FAU_SAR.1、FAU_SAR.2
FAU_SAR.1 によって、MFP 管理者が検証できる形式で監査ログデータを読み出せるようにし、FAU_SAR.2 によって、MFP 管理者以外が監査ログデータを読み出すことを禁止する。

FAU_SAR.1 及び FAU_SAR.2 は O.AUDIT を達成する主要な SFR である。

(5) FPT_STM.1
FPT_STM.1 によって信頼できるタイムスタンプを提供し、監査ログデータには監査事象が発生した正確な時間を記録する。

FPT_STM.1 は O.AUDIT の達成を支援する SFR である。

(6) FIA_UID.1
FIA_UID.1 によって、操作パネルまたはネットワーク上のクライアント PC から TOE を利用しようとする者を識別する。

FIA_UID.1 は O.AUDIT の達成を支援する SFR である。

これらのセキュリティ機能要件を実施することで O.AUDIT を実現できる。

O.EMMC_ENCRYPTION eMMC 暗号化

O.EMMC_ENCRYPTION は、eMMC に書き込むデータを暗号化することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の SFR を実施する必要がある。

(1) FCS_CKM.1
FCS_CKM.1 によって、指定されたアルゴリズムに従って暗号鍵を生成する。

FCS_CKM.1 は O.EMMC_ENCRYPTION の達成を支援する SFR である。

(2) FCS_CKM.4

FCS_CKM.4 によって、指定された方法に従って暗号鍵を削除する。

FCS_CKM.4 は O.EMMC_ENCRYPTION の達成を支援する SFR である。

(3) FCS_COP.1

FCS_COP.1 によって、指定されたアルゴリズムと鍵長に従って、eMMC に書き込むデータを暗号化し、eMMC から読み出されるデータを復号する。

FCS_COP.1 は O.EMMC_ENCRYPTION を達成する主要な SFR である。

これらのセキュリティ機能要件を実施することで O.EMMC_ENCRYPTION を実現できる。

6.3.3 依存性分析

TOE セキュリティ機能要件について、本 ST での依存性の分析結果を表 27 に示す。

表 27 : TOE セキュリティ機能要件の依存性分析結果

TOE セキュリティ機能要件	要求された依存性	ST の中で満たしている依存性	ST の中で満たしていない依存性
FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	なし
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_STG.4	FAU_STG.1	FAU_STG.1	なし
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4	なし
FCS_CKM.4	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]	FCS_CKM.1	なし
FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	なし
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	なし
FDP_FXS_EXP.1	なし	なし	なし
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	なし
FIA_ATD.1	なし	なし	なし

TOE セキュリティ機能要件	要求された依存性	ST の中で満たしている依存性	ST の中で満たしていない依存性
FIA_SOS.1	なし	なし	なし
FIA_UAU.1	FIA_UID.1	FIA_UID.1	なし
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	なし
FIA_UID.1	なし	なし	なし
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	なし
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	なし
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	なし
FMT_MTD.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	なし
FMT_MTD.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1	FMT_SMF.1
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.1	なし
FPT_STM.1	なし	なし	なし
FPT_TST_EXP.1	なし	なし	なし
FTA_SSL.3	なし	なし	なし
FTP_ITC.1	なし	なし	なし

以下に、依存性が満たされていなくても問題ない根拠を記述する。

FMT_SMF.1 への依存性除去理由

本 TOE の TSF 秘密データであるログインパスワードは、問い合わせを行うインタフェースがない。インタフェースが提供されていないので、管理機能は不要である。

6.3.4 セキュリティ保証要件根拠

本 TOE は市販製品の MFP である。MFP は一般的なオフィスで使用されることを想定しており、本 TOE は強化基本レベル以上の攻撃能力を持つ攻撃者は想定していない。

また、TOE 設計の評価(ADV_TDS.1)は市販製品の正当性を示すのに十分である。さらに、TSF を回避あるいは改変するような攻撃には高い攻撃能力が要求され、これは今回の評価の対象外である。すなわち、一般的なニーズには基本的な攻撃能力を持つ攻撃者からの攻撃への対処(AVA_VAN.2)で十分である。

従って、評価期間とコストを考慮すると、本 TOE に対する評価保証レベルは EAL2 が妥当である。

7 TOE 要約仕様

本章は、TOE 要約仕様をセキュリティ機能毎に示す。さらに、セキュリティ機能は対応するセキュリティ機能要件ごとに示す。

7.1 監査機能

監査機能は、TOE の監査事象のログを監査ログデータとして eMMC に記録し、記録した監査ログデータを監査できる形式で提供する機能である。MFP 管理者のみが監査ログデータの読出しや削除ができる。高信頼タイムスタンプを提供する機能、監査ログデータ満杯時の制御機能もこの機能に含む。監査ログデータは転送して syslog サーバーに保存することもできる。

FAU_GEN.1 (監査データ生成)

TOE は、表 28 に示す監査事象発生時に、表 29 に示す監査ログデータ項目を eMMC に記録する。監査ログデータ項目には、共通ログ項目と個別ログ項目がある。共通ログ項目は、監査ログデータを記録するとき必ず記録する監査データ項目であり、個別ログ項目は、表 29 に示す監査ログデータ項目を記録する監査事象発生時のみ記録する。

表 28：監査事象リスト

監査事象
監査機能の開始
監査機能の終了
監査ログデータのダウンロードと削除
機密印刷文書データの印刷の開始と終了
機密印刷文書データの削除
ファクス受信文書データの印刷の開始と終了
利用者ジョブデータの削除
ロックアウトの開始と解除
ログイン操作の成功と失敗
表 24 管理機能の使用
オートログアウトによるセションの終了
スキャナーからの文書添付メール送信の失敗
syslog 転送の失敗
ネットワークを介した PC ファクスの失敗
ネットワークを介した機密印刷の失敗
WIM の通信の失敗

表 29：監査ログデータ項目のリスト

	監査ログデータ項目	監査ログデータ項目への設定値	監査ログデータを記録する監査事象
共通ログ項目	事象の開始日付・時刻	事象発生時の TOE のシステム時計の値	・表 28 に示す全ての監査対象事象
	事象の終了日付・時刻	事象終了時の TOE のシステム時計の値	
	事象の種別	監査事象の識別情報	
	サブジェクト識別情報	監査事象の発生原因となった利用者のログインユーザー名	
	結果	監査事象の結果(*1)	
個別ログ項目	ログタイプ	文書データの操作(印刷・削除)やジョブのタイプを識別するための情報	・機密印刷文書データの印刷の開始と終了 ・ファクス受信文書データの印刷の開始と終了 ・機密印刷文書データの削除 ・利用者ジョブデータの削除
	ログインユーザー名	利用者識別を試みた全てのログインユーザー名	・ログインの成功と失敗
	通信先	通信先 IP アドレス	・syslog 転送の失敗 ・ネットワークを介した PC ファクスの失敗 ・ネットワークを介した機密印刷の失敗 ・WIM の通信の失敗
		文書添付メール送信時の宛先メールアドレス	・スキャナーからの文書添付メール送信の失敗
	ロックアウト操作種別	ロックアウト開始とロックアウト解除を識別するための情報	・ロックアウトの開始と解除
	ロックアウト対象者	ロックアウトした利用者のログインユーザー名	・ロックアウトの開始と解除
	ロックアウト解除対象者	ロックアウト解除した利用者のログインユーザー名	・ロックアウトの開始と解除

(*1): 成功または失敗と記録する。「機密印刷文書データの削除」の結果は、成功のみ記録する。

以下の監査事象では、失敗と記録する。

・スキャナーからの文書添付メール送信の失敗

・syslog 転送の失敗

・ネットワークを介した PC ファクスの失敗

・ネットワークを介した機密印刷の失敗

・WIM の通信の失敗

FAU_GEN.2 (利用者識別情報の関連付け)

TOE は、誰が監査事象を引き起こしたか識別できるように、監査ログデータにはログインユーザー名を記録する。

FPT_STM.1 (高信頼タイムスタンプ)

TOE は、監査ログデータに記録する日付(年月日)・時刻(時分秒)を TOE のシステム時計から取得する。

FAU_SAR.1 (監査レビュー)

TOE は、MFP 管理者にすべての監査ログデータをテキスト形式で提供する。TOE は、MFP 管理者がアクセスした時のみ WIM で監査ログデータをダウンロードできる。

FAU_SAR.2 (限定監査レビュー)

TOE は、MFP 管理者を除くすべての利用者に監査ログデータをダウンロードするインタフェースを提供しない。

FAU_STG.1 (保護された監査証跡格納)

TOE は、監査ログデータの削除を MFP 管理者だけに許可する。監査ログデータの削除操作は WIM または操作パネルを利用して実施する。監査ログデータの部分的な変更を行うインタフェースは提供しない。

FAU_STG.4 (監査データ損失の防止)

TOE は、監査ログデータファイルに監査ログデータを追加記録する領域がない場合には、最新の監査ログデータを最も古い監査ログデータに上書きする。

7.2 識別認証機能

識別認証機能は、TOE が認証に成功した利用者だけに TOE の利用を許可し、失敗した場合は許可しないために、TOE を利用しようとする者が許可利用者であるかを、利用者から入力されるログインユーザー名とログインパスワードを使って検証する機能である。ロックアウト機能、パスワード保護機能、及びオートログアウト機能もこの機能に含む。

FIA_UAU.1、FIA_UID.1 (利用者認証、利用者識別)

TOE は、ログインユーザー名とログインパスワードで識別認証を行う。

操作パネルまたは WIM が利用される前に、TOE はログイン画面を表示し、利用者のログインユーザー名とログインパスワードの入力を促す。また TOE はプリンタードライバーまたはファクスドライバーから要求を受けたとき、利用者が要求と同時に入力したログインユーザー名とログインパスワードを受信する。利用者が入力したログインユーザー名とログインパスワードが、TOE に予め登録されているログインユーザー名とログインパスワードに一致するか確認することによって識別認証を行う。

識別認証に成功すると、利用者へ TOE の利用を許可し、失敗した場合は許可しない。ただし、利用者ジョブデータ一覧の参照、WIM のヘルプの参照、システム状態の参照、カウンタの参照、問い合わせ情報の参照、及びファクス受信の実行は、識別認証を行う前から利用者に許可する。

FIA_USB.1 (利用者-サブジェクト結合)

TOE は、FIA_UAU.1、及び FIA_UID.1 の結果、認証に成功した利用者が操作を行う処理にログインユーザー名とユーザー権限を割り当てる。

FIA_ATD.1 (利用者属性定義)

TOE は、ログインユーザー名、及びユーザー権限を利用者毎に設定で保持する。個々の利用者には登録時に分類された役割に応じてユーザー権限が設定される。利用者に割り当てられるログインユーザー名は利用者毎に変更が可能である。

FTA_SSL.3 (TSF 起動による終了)

TOE は、利用者がログインした状態で一定時間操作をしないときに自動でログアウトする。

ログインしたインタフェースによって以下のように動作する。

・操作パネルの場合は、最後の操作からの経過時間が操作パネルオートログアウト時間(10～999 秒)に達したとき、自動でログアウトする。

・WIM の場合は、最後の操作からの経過時間が WIM オートログアウト時間(3～60 分)に達したとき、自動でログアウトする。

FIA_UAU.7 (保護された認証フィードバック)

TOE は、操作パネルまたは WIM を利用しようとする者が入力するログインパスワードについて、入力した文字を表示せず、入力した文字数分のダミー文字をログイン画面に表示する。

FIA_AFL.1 (認証失敗時の取り扱い)

ログイン時にパスワードを連続して間違えると、ロックアウト機能が働き、TOE はそのログインユーザー名でのログインを禁止する。ロックアウトされたログインユーザー名では、正しいパスワードを入力したときも認証失敗となり、一定時間が経過してロックアウトが解除されるか、MFP 管理者またはスーパーバイザーがロックアウトを解除するまで、TOE を使用できない。

認証失敗の回数はログイン先(操作パネル、WIM、プリンタードライバー、及びファクスドライバー)が異なっても合算してカウントし、管理者が設定するパスワードの入力許容回数(1～10 回)に達した場合にロックアウトする。

ロックアウトとなったログインユーザー名は、以下の条件の内いずれかが成立するまでログインできない。

・一般利用者は、MFP 管理者が設定したロックアウト時間が経過するまで

・MFP 管理者とスーパーバイザーは、MFP の電源 ON 後に MFP が実行可能状態になってから 60 秒経過するまで

・表 30 に示すロックアウト対象者はロックアウト解除者によってロックアウト解除されるまで

表 30：ロックアウト解除の関係

ロックアウト対象者	ロックアウト解除者
一般利用者	MFP 管理者
スーパーバイザー	MFP 管理者

MFP 管理者	スーパーバイザー

FIA_SOS.1 (秘密の検証)

利用者のログインパスワードは、一定の条件を満たす場合だけ登録できる。満たさなければ登録できない。

使用できる文字とその文字種は以下である。文字種の組み合わせ数(2 種類以上、または 3 種類以上)の条件を決めるパスワード複雑度は、MFP 管理者が設定する。

・英大文字: [A-Z] (26 文字)
・英小文字: [a-z] (26 文字)
・数字: [0-9] (10 文字)
・記号: SP(スペース)! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 文字)

登録可能な桁数の条件は、一般利用者と MFP 管理者、スーパーバイザーの場合で以下のように異なる。

ログインパスワード最小桁数は、8 から 32 桁の範囲で MFP 管理者が設定する。

・一般利用者の場合: ログインパスワード最小桁数以上、128 桁以下
・MFP 管理者またはスーパーバイザーの場合: ログインパスワード最小桁数以上、32 桁以下

7.3 文書アクセス制御機能

文書アクセス制御機能は、TOE の許可利用者に対し、ユーザー権限またはログインユーザー名に基づいて、利用者文書データと利用者ジョブデータへの操作を許可する機能である。

FDP_ACC.1、FDP.ACF (サブセットアクセス制御、セキュリティ属性によるアクセス制御)

TOE は、(1)機密印刷文書データのアクセス制御ルール、(2)ファクス受信文書データのアクセス制御ルール、(3)利用者ジョブデータへのアクセス制御ルールに従って、利用者による蓄積文書データと利用者ジョブデータへの操作を制限する。

(1) **機密印刷文書データのアクセス制御ルール**

TOE は、機密印刷文書データを印刷、及び削除するためのインタフェースを利用者に提供する。機密印刷文書データを変更するインタフェースは提供しない。

機密印刷文書データを作成した一般利用者と同一のログインユーザー名をもつ一般利用者に、機密印刷文書データの操作を許可する。すなわち利用者は自分が作成した機密印刷文書データを操作できる。

一般利用者が操作パネルでログインした後、TOE は操作を許可する機密印刷文書データの一覧と、許可する操作(印刷・削除)のメニューを表示する。なお機密印刷文書データの印刷が終了すると、TOE はその機密印刷文書データを削除する。また一般利用者が WIM でログインした後には、TOE は操作を許可する機密印刷文書データの一覧を表示し、表示された機密印刷文書データに対して、操作(削除)を許可する。操作を許可しない機密印刷文書データは一覧には表示しない。

MFP 管理者のユーザー権限をもつ者が操作パネルまたは WIM でログインした後には、TOE は全ての機密印刷文書データの一覧と、削除の操作メニューを表示する。MFP 管理者は、機密印刷文書データの一覧から削除したい文書を選択して削除を実行することができる。

スーパーバイザープロセスのユーザー権限をもつ者には機密印刷文書データへの操作を許可しない。

(2) **ファクス受信文書データのアクセス制御ルール**

TOE は、ファクス受信文書データを印刷するためのインタフェースを利用者に提供する。

蓄積受信文書ユーザーとして登録されたログインユーザー名をもつ一般利用者に、ファクス受信文書データの操作を許可する。蓄積受信文書ユーザーは、すべてのファクス受信文書データに対して 1 つのリストとして登録される。

一般利用者が操作パネルでログインした後、TOE は許可する操作(印刷)のメニューを表示する。印刷することでのみ、利用者はファクス受信文書データの内容を確認することができる。変更と削除のインタフェースはなく、ファクス受信文書データの印刷が終了すると、TOE はそのファクス受信文書データを削除する。

MFP 管理者とスーパーバイザーのユーザー権限をもつ者にはファクス受信文書データの操作を許可しない。

蓄積受信文書ユーザーを編集するユーザー権限については、「7.6 セキュリティ管理機能」に示す。

(3) **利用者ジョブデータのアクセス制御ルール**

TOE は、利用者ジョブデータを削除するためにキャンセルのインタフェースを利用者に提供する。利用者ジョブデータを変更するインタフェースは提供しない。

利用者ジョブデータのキャンセル(削除)を試みた利用者が、利用者ジョブデータのオーナー(ログインユーザー名が一致する一般利用者)、あるいは MFP 管理者の場合のみ、操作パネルまたは WIM でログイン後に、TOE は利用者ジョブデータをキャンセルするメニューを表示する。他の利用者には利用者ジョブデータへの操作を許可しない。

利用者ジョブデータをキャンセルすると、キャンセルされた利用者ジョブデータが扱っていた文書データは削除される。ただし、キャンセルされた利用者ジョブデータが扱っていた文書データが蓄積文書データの場合は、TOE 内に蓄積したまま削除されない。

7.4 ネットワーク保護機能

ネットワーク保護機能は、高信頼 IT 製品(クライアント PC、syslog サーバー、SMTP サーバー)との通信を行う際、暗号化通信を提供することによってネットワーク上のモニタリングによる情報漏えいを防止し、通信内容の改ざんを検出する機能である。TOE はこの機能を TLS によって実装する。

FTP_ITC.1 (TSF 間高信頼チャネル)

TOE は、高信頼 IT 製品との通信を行う際、内部ネットワークの通信経路上の利用者文書データ、及び TSF データを保護するために、暗号化通信を提供する。

TOE は、クライアント PC の Web ブラウザ、プリンタードライバー、またはファクスドライバーが暗号化通信を開始するのを許可する。TOE は SMTP サーバー、または syslog サーバーとの暗号化通信を開始することができる。

TOE が提供する暗号化通信を表 31 に示す。

WIM 利用時は、Web ブラウザにて暗号化通信が有効な URL を指定することでクライアント PC と暗号化通信を行う。プリンター機能利用時は、プリンタードライバーから TOE へ機密印刷文書データを送信した場合に、クライアント PC と暗号化通信(IPP over SSL)を行う。ファクス機能利用時は、ファクスドライバーから TOE へファクス送信データを送信した場合に、クライアント PC と暗号化通信(IPP over SSL)を行う。スキャナーからの文書添付メール送信機能の利用時は、SMTP サーバーと暗号化通信(SMTP over SSL)を行う。syslog 転送機能の利用時は、syslog プロトコルを利用し、TLS で保護された暗号化通信を syslog サーバーと行う。

表 31 : TOE が提供する暗号化通信

通信先	TOE が提供する暗号化通信	
	プロトコル	暗号アルゴリズム
クライアント PC	TLS1.2	AES(128bits、256bits)
SMTP サーバー	TLS1.2	AES(128bits、256bits)
syslog サーバー	TLS1.2	AES(128bits、256bits)

7.5 蓄積データ保護機能

蓄積データ保護機能は、eMMC に記録されているデータを漏えいから保護するため、eMMC に書き込むデータを暗号化する機能である。

FCS_CKM.1 (暗号鍵生成)

TOE は、MFP 管理者の操作を受けて eMMC の暗号化をするとき、Hash_DRBG(SHA256)のアルゴリズムで 256 ビットの eMMC 暗号鍵の生成を行う。

このとき TOE は、標準 NIST SP 800-90A に準拠したアルゴリズムで乱数を生成する。

FCS_CKM.4 (暗号鍵破棄)

eMMC の暗号化を解除するとき、暗号鍵は 0 で上書き削除される。

FCS_COP.1 (暗号操作)

TOE は、eMMC に書き込み/読み出しするデータに対して、書き込む前に暗号化し、読み出し後に復号する。標準 FIPS197 に準拠し、256 ビットの暗号鍵長の鍵による AES のアルゴリズムを用いて暗号化と復号を行う。

7.6 セキュリティ管理機能

セキュリティ管理機能は、ユーザー権限、またはログインユーザー名に基づいて、TSF データへの操作やセキュリティ機能のふるまいに関する制御を行う機能である。セキュリティ管理機能の操作をする役割を維持し利用者に紐づける機能、セキュリティ属性に適切なデフォルト値を設定する機能がある。

FMT_SMR.1 (セキュリティの役割)

TOE の利用者は、一般利用者、MFP 管理者、またはスーパーバイザーの役割をもつ。役割は TOE に登録されたログインユーザー名と紐づいており、TOE はログインした利用者に、ログインユーザー名に対応する役割を紐づける。

FMT_MSA.1、FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_SMF.1、FMT_MOF.1 (セキュリティ属性の管理、TSF データの管理、管理機能の特定、セキュリティ機能のふるまいの管理)

TOE は次の管理機能を実行する。

・TOE は、セキュリティ属性に対する操作を利用者の役割により制限する。操作を許可する役割に応じたユーザー権限をもつ利用者に、それぞれのセキュリティ属性への操作を許可する。表 32 に記す TSF データのうち、セキュリティ属性はログインユーザー名と蓄積受信文書ユーザーである。

・TOE は、MFP 管理者のみに syslog 転送機能を停止する、または動作させる設定を行うインタフェースを提供する。

・TOE は、TSF データに対する操作を利用者の役割により制限する。表 32 に記すように、操作を許可する役割に応じたユーザー権限をもつ利用者に、TSF データの操作を許可する。機密印刷文書データと利用者ジョブデータのセキュリティ属性を変更するインタフェースはない。またログインパスワードの問い合わせを行うインタフェースはない。

表 32 : TSF データの管理

分類	**TSF データ**	**操作**	**操作を許可する役割 (ユーザー権限)**	操作箇所
TSF 秘密データ	ログインパスワード [一般利用者に紐づく場合]	新規作成 変更	MFP 管理者	操作パネル WIM
		問い合わせ	操作を許可する役割なし	なし
	ログインパスワード [当該一般利用者本人に紐づく場合]	変更	当該一般利用者	操作パネル WIM
		問い合わせ	操作を許可する役割なし	なし
	ログインパスワード [スーパーバイザーに紐づく場合]	変更	スーパーバイザー	操作パネル WIM
		問い合わせ	操作を許可する役割なし	なし
	ログインパスワード [MFP 管理者に紐づく場合]	変更	スーパーバイザー MFP 管理者	操作パネル WIM
		問い合わせ	操作を許可する役割なし	なし
	eMMC 暗号鍵	問い合わせ 削除 生成	MFP 管理者	操作パネル
TSF 保護データ	ログインユーザー名 [一般利用者に紐づく場合]	変更 削除 新規作成	MFP 管理者	操作パネル WIM
	ログインユーザー名 [スーパーバイザーに紐づく場合]	変更	スーパーバイザー	操作パネル WIM
	ログインユーザー名 [MFP 管理者に紐づく場合]	変更	MFP 管理者	操作パネル WIM
	蓄積受信文書ユーザー	変更	MFP 管理者	操作パネル WIM

分類	**TSF データ**	**操作**	**操作を許可する役割 (ユーザー権限)**	操作箇所
	ロックアウトの設定	変更	MFP 管理者	WIM
	日付・時刻の設定	変更	MFP 管理者	操作パネル WIM
	パスワード品質の設定	変更	MFP 管理者	操作パネル
	オートログアウトの設定	変更	MFP 管理者	WIM 操作パネル(*1)
	監査ログデータの設定	変更	MFP 管理者	WIM 操作パネル
	暗号通信設定	変更	MFP 管理者	操作パネル WIM

(*1): 操作パネルのオートログアウトの設定の操作箇所は操作パネルと WIM であり、WIM のオートログアウトの設定の操作箇所は WIM のみである。

FMT_MSA.3 (静的属性初期化)

利用者データアクセス制御 SFP におけるセキュリティ属性には、蓄積受信文書ユーザーとログインユーザー名がある。

・蓄積受信文書ユーザーは、ファクス受信文書データのセキュリティ属性である。初期値には蓄積受信文書ユーザーとして登録された一般利用者のログインユーザー名が設定されるため、制限的なデフォルト値が設定される。

・ログインユーザー名は、機密印刷文書データと利用者ジョブデータのセキュリティ属性である。機密印刷文書データにおける初期値には、機密印刷文書データを作成した一般利用者のログインユーザー名が設定され、利用者ジョブデータにおける初期値には、利用者ジョブデータを作成した一般利用者のログインユーザー名が設定されるため、制限的なデフォルト値が設定される。

これらの制限的なデフォルト値を変更するインタフェースはない。

7.7 完全性検証機能

完全性検証機能は、MFP 制御ソフトウェア、及び操作パネル制御ソフトウェアの実行コードの完全性を検証する自己テスト機能である。

FPT_TST_EXP.1 (TSF テスト)

TOE は、初期立上げ中に制御ソフトウェアの完全性検証を実行する。

MFP 制御ソフトウェア及び操作パネル制御ソフトウェアに対して、ハッシュ値の比較またはデジタル署名の検証を行うことで、TOE は制御ソフトウェアの完全性を検証する。

起動時に取得した完全性検証のためのハッシュ値が正しい値と一致しない、またはデジタル署名が検証されない場合、TOE は、エラーを操作パネルに表示して操作を受け付けない。取得したハッシュ値が正しい値と一致し、かつデジタル署名が検証された場合、TOE は利用可能になる。

7.8 ファクス回線分離機能

ファクス回線分離機能は、電話回線から LAN への侵入を防止するために、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止する機能である。

FDP_FXS_EXP.1 (ファクス分離)

TOE は、電話回線において G3 規格での通信のみを行い他の通信は行わないことで、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止する。

8 用語

本章では、本 ST で使用する特定の用語の意味を以下に定義する。

表 33：本 ST に関連する特定の用語

用語	定義
MFP 制御ソフトウェア	TOE に組込むソフトウェアの 1 つ。本体 eMMC に格納されている。
操作パネル制御ソフトウェア	TOE に組込むソフトウェアの 1 つ。操作パネル制御ボードに格納されている。
ロックアウト	利用者に対してログインを許可しない状態にすること。
オートログアウト	操作パネルあるいは WIM からログイン中に、予め定められた時間アクセスが無かった時、自動的にログアウトする機能。
eMMC	Embedded Multi Media Card の略称。不揮発性メモリであるストレージデバイス。本書で、単に eMMC と記載した場合は TOE 内に取り付けられた eMMC を指す。
ジョブ	TOE のコピー、スキャナー、プリンター、ファクス送信及びファクス受信の各機能の開始から終了までの作業。
文書データ	TOE が扱う紙文書、電子文書の総称。
蓄積文書データ	プリンター機能、及びファクス機能で TOE 内に蓄積される文書データ。機密印刷文書データ、及びファクス受信文書データに分類できる。
MFP アプリケーション	TOE が提供するコピー、スキャナー、プリンター、ファクス受信及びファクス送信の各機能の総称。
操作パネル	液晶タッチパネルディスプレイとハードキーで構成される。利用者が TOE を操作する時に利用する。
WIM	Web Image Monitor 機能のこと。クライアント PC の Web ブラウザから TOE の利用者が TOE をリモート操作するための機能である。
文書添付メール送信	スキャナー機能で読み取った利用者文書データを、MFP から SMTP サーバーを経由してクライアント PC に電子メール形式で送信する機能。この機能を実現するための通信は、TLS によって保護される。
PC ファクス	ファクス機能の 1 つ。クライアント PC のファクスドライバーを利用して、ファクス送信を行う機能。PC FAX と記述されることもある。
SPDF	本装置にセットされた原稿を 1 枚ずつ読み取りガラスに送る装置である、自動原稿送り装置(ADF)の一種。原稿の両面を読み取る場合に、原稿の両面を同時に読み取る。
LAN	ローカルエリアネットワークの略称。TOE の設置環境で利用されるネットワーク。
電話回線	外部ファクスと送受信するための、公衆電話交換網の回線を指す。
ファイアウォール	インターネットからオフィス内へのネットワーク攻撃を防止するための装置。
SMTP サーバー	TOE が電子メールを送信する場合に、使用されるサーバー。

用語	定義
syslog サーバー	syslog プロトコルを利用し、TOE が記録した監査ログデータを受信できるサーバー。
MFP 管理責任者	TOE を利用する組織の中で TOE の管理者を選任する役割を持った、間接的に TOE に関わる者。