RICOH IM 370,

nashuatec IM 370,

Rex Rotary IM 370,

Gestetner IM 370

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: 2024 年 2 月 26 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 370,
nashuatec IM 370,
Rex Rotary IM 370,
Gestetner IM 370 セキュリティターゲット

バージョン: 1.00

作成日付: 2024 年 2 月 26 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 370,
nashuatec IM 370,
Rex Rotary IM 370,
Gestetner IM 370

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 に示す日本国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 370	D0DM-27

この MFP はファクス機能のない製品である。この MFP に搭載されるソフトウェアのバージョンと部番の識別情報を表 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。

表 2 : バージョン E-1.00 のソフトウェアのバージョンと部番

No.	本体のソフトウェアの名称	バージョン	部番
1	CTL System	1.04	D0DM5550F
2	Printer	1.00	D0DM5552C
3	IRIPS PS3PDF	1.00	D0DM5554B
4	CheetahSystem	1.04	D0DN1420F
5	appsite	3.06.20	D0DN1441D
6	bleservice	1.00	D0DN1433B
7	camelsl	1.00	D0DN1452C
8	cispluginble	5.0.0	D0DN1446A
9	cispluginkeystr	1.00.00	D0DN1445A
10	cispluginnfc	1.00.00	D0DN1444A
11	devicemanagemen	1.01.00	D0DN1455D
12	ecoinfo	1.00	D0DN1432B
13	faxinfo	1.00	D0DN1430B
14	helpservice	1.00	D0DN1449B
15	iccd	1.01.00	D0DN1443A
16	introductionset	1.00	D0DN1448B
17	iwnnimelanguage	2.16.2	D0E01433
18	iwnnimelanguage	2.16.2	D0E01431
19	iwnnimelanguage	2.16.2	D0E01432
20	iwnnimeml	2.16.204	D0E01430C
21	kerberos	1.0	D0DN1451B
22	langswitcher	1.00	D0DN1428B
23	mediaappappui	1.00	D0DN1439C
24	mlpsmartdevicec	5.0.0	D0DN1427A
25	optimorurcmf	1.1.9	D0E01462C
26	programinfoserv	1.00	D0DN1434C
27	remotesupport	1.00	D0DN1453B
28	rsisetup	1.01.14	D0DN1456D

No.	本体のソフトウェアの名称	バージョン	部番
29	simpleauth	1.00.00	D0DN1426A
30	simpledirectcon	1.25	D0DN1447
31	simpleprinter	1.00	D0DN1435C
32	smartcopy	1.01	D0DN1436D
33	smartdocumentbo	1.00	D0DN1454C
34	smartfax	1.01	D0DN1438C
35	smartprtstoredj	1.00	D0DN1440C
36	smartscanner	1.01	D0DN1437D
37	smartscannerex	3.00	D0DN1450C
38	stopwidget	1.00	D0DN1431B
39	tonerstate	1.00	D0DN1429B
40	traywidget	1.00	D0DN1442B
41	Engine	1.04:06	D0DM5500D

No.	操作パネルのソフトウェアのソフトウェア名	バージョン	部番
42	Firmware	1.04	D0DN1420F
43	Keymicon	1.08	表示なし
44	Application Site	3.06.20	D0DN1441D
45	Bluetooth Authentication Plugin	5.0.0	D0DN1446A
46	BluetoothService	1.00	D0DN1433B
47	Change Languages	1.00	D0DN1428B
48	Cloud Settings	1.01.14	D0DN1456D
49	Copy	1.01	D0DN1436D
50	DeviceManagementService	1.01.00	D0DN1455D
51	Direct Connection	1.25	D0DN1447
52	Document Server	1.00	D0DN1454C
53	Eco-friendly	1.00	D0DN1432B
54	Fax	1.01	D0DN1438C
55	Fax RX File	1.00	D0DN1430B
56	GraphicData	0.10	DXXXXXXX

No.	操作パネルのソフトウェアのソフトウェア名	バージョン	部番
57	ICCardDispatcher	1.01.00	D0DN1443A
58	Installation Settings	1.00	D0DN1448B
59	iWnn IME	2.16.204	D0E01430C
60	iWnn IME Korean Pack	2.16.2	D0E01433
61	iWnn IME Simplified Chinese Pack	2.16.2	D0E01431
62	iWnn IME Traditional Chinese Pack	2.16.2	D0E01432
63	KerberosService	1.0	D0DN1451B
64	LegacyUIData	0.24	DXXXXXXX
65	Print/Scan (Memory Storage Device)	1.00	D0DN1439C
66	Printer	1.00	D0DN1435C
67	ProgramInfoService	1.00	D0DN1434C
68	Proximity Card Reader Support Plugin	1.00.00	D0DN1445A
69	Quick Card Authentication Config.	1.00.00	D0DN1426A
70	Quick Print Release	1.00	D0DN1440C
71	Remote Panel Operation	1.00	D0DN1452C
72	RemoteConnect Support	1.1.9	D0E01462C
73	RemoteSupportService	1.00	D0DN1453B
74	RicohScanGUIService	3.00	D0DN1450C
75	Scanner	1.01	D0DN1437D
76	Smart Device Connector	5.0.0	D0DN1427A
77	Standard IC Card Plugin	1.00.00	D0DN1444A
78	Stop	1.00	D0DN1431B
79	Supply Information	1.00	D0DN1429B
80	Support Settings	1.00	D0DN1449B
81	Tray/Remaining Paper	1.00	D0DN1442B

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、ドキュメントボックス、プリンター、スキャナー機能を有した MFP である。本 TOE にはファクス機能は搭載されていない。

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、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、ドキュメントボックス、プリンター、及びスキャナーの各機能を利用する。

TOE が扱う文書データ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、及び暗号化通信のセキュリティ機能を提供する。TOE における発生事象は MFP 管理者が監査ログとして確認でき、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 はソフトウェア構成の完全性の検証を行う。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。また TOE はファクス機能を搭載しないため、ファクス回線分離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。

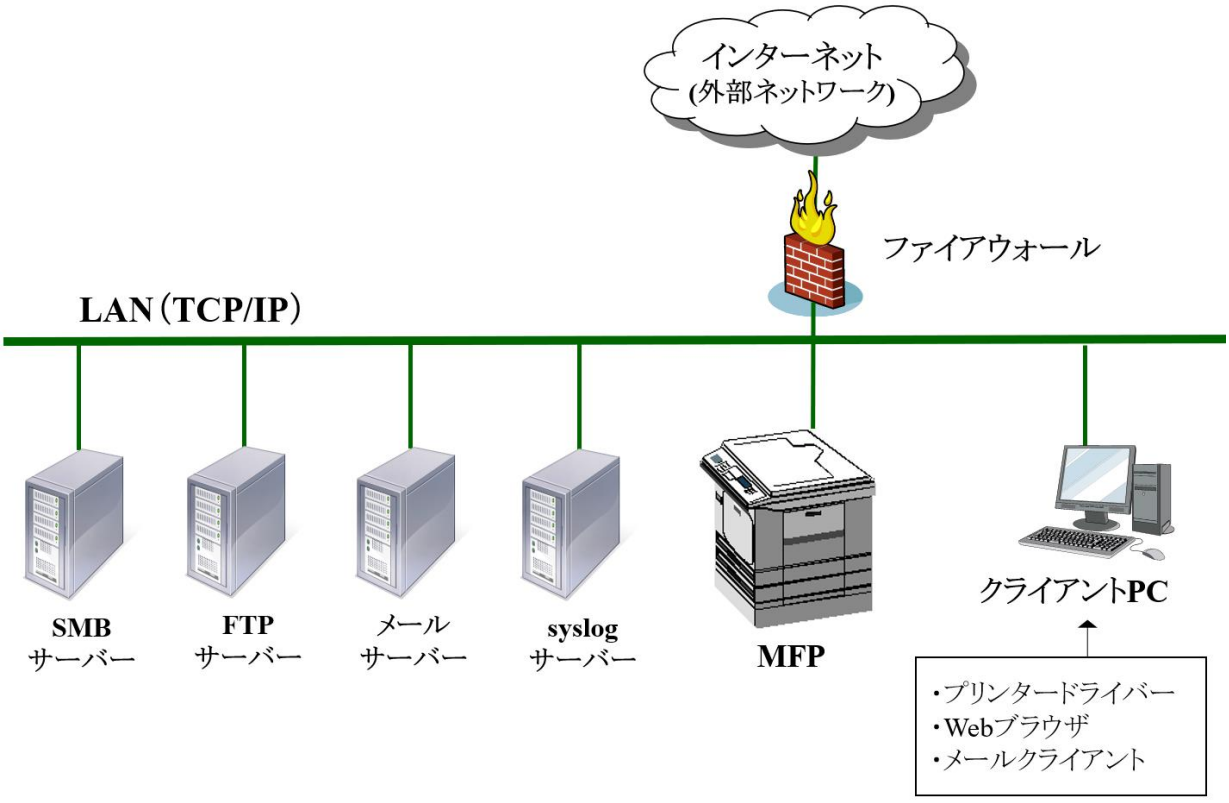

図 1 : TOE の利用環境

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 の各種設定や利用者データ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 から文書データを一時保存または蓄積するためには、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。電子メールを受信するクライアント PC には、S/MIME に対応したメールクライアントをインストールしておく必要がある。
- SMB サーバー
  - TOE のスキャナー機能でスキャンした文書データを SMB プロトコルで送信する場合に使用されるサーバー。なお通信は IPsec で保護する。フォルダー送信を利用するために必要である。
- FTP サーバー
  - TOE のスキャナー機能でスキャンした文書データを FTP プロトコルで送信する場合に使用されるサーバー。なお通信は IPsec で保護する。フォルダー送信を利用するために必要である。
- メールサーバー
  - TOE が電子メールを送信する場合に使用される、SMTP プロトコルに対応したサーバー。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 11
  - プリンタードライバー: PCL6 Driver 1.1.0.0
  - Web ブラウザ: Microsoft Edge 107
  - メールクライアント: Thunderbird 102.6.0
- SMB サーバー: Windows 10
- FTP サーバー: Windows 10(IIS10) バージョン V10.0.19041.804

  Linux (Ubuntu 20.04) vsftpd 3.0.3
- メールサーバー: Windows 10 P-Mail Server Manager version 1.91
- syslog サーバー: Linux (Ubuntu 20.04) rsyslogd 8.2001.0

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 1 の MFP 製品と、表 4 のガイダンスからなる。MFP 製品は、表 3 に示すバージョン(E-1.00)を構成するソフトウェアを搭載した製品が対象である。

MFP 本体は配送業者が利用者へ配送する。

ガイダンスは[英語版-1]のガイダンスのセットを配付する。ガイダンスは MFP 本体に同梱して配付するものと Web にて配付するものがある。

以下に記載の組み合わせを利用者へ配付する。

表 3 : 配付する組み合わせ

No.	MFP 本体			ガイダンス	備考
	製品名	機種コード	バージョン		
1	IM 370	D0DM-27	E-1.00	[英語版-1]	SPDF を標準搭載

[英語版-1]のガイダンスセットのガイダンス文書、配付形式、及び配付方法を表 4 に示す。

表 4 : [英語版-1]のガイダンス文書

No.	部番	ガイダンス名称	配付形式	配付方法
1	D0E3-7546	Safe Use of This Machine	冊子	製品と同梱
2	D0DM-7310	Safety Information	PDF	Web 配付
3	D0DM7314	User Guide IM 370/370F/460F/460FTL	HTML	Web 配付
4	D0E37534	Security Reference	HTML	Web 配付
5	D0DM-7318 2023.12.13	Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	PDF	Web 配付
6	D0DM-7319 2023.09.29	Notes on Security Functions	PDF	Web 配付
7	83NHEZ-ENZ1.00 v281	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_370-eal2-sp/en/Guidance_eu.zip

ハッシュ値(SHA256): 65f71d0a73156d19be73fff793bc2a38d9877ea264cb24ff27f6c1a3cc189611

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。

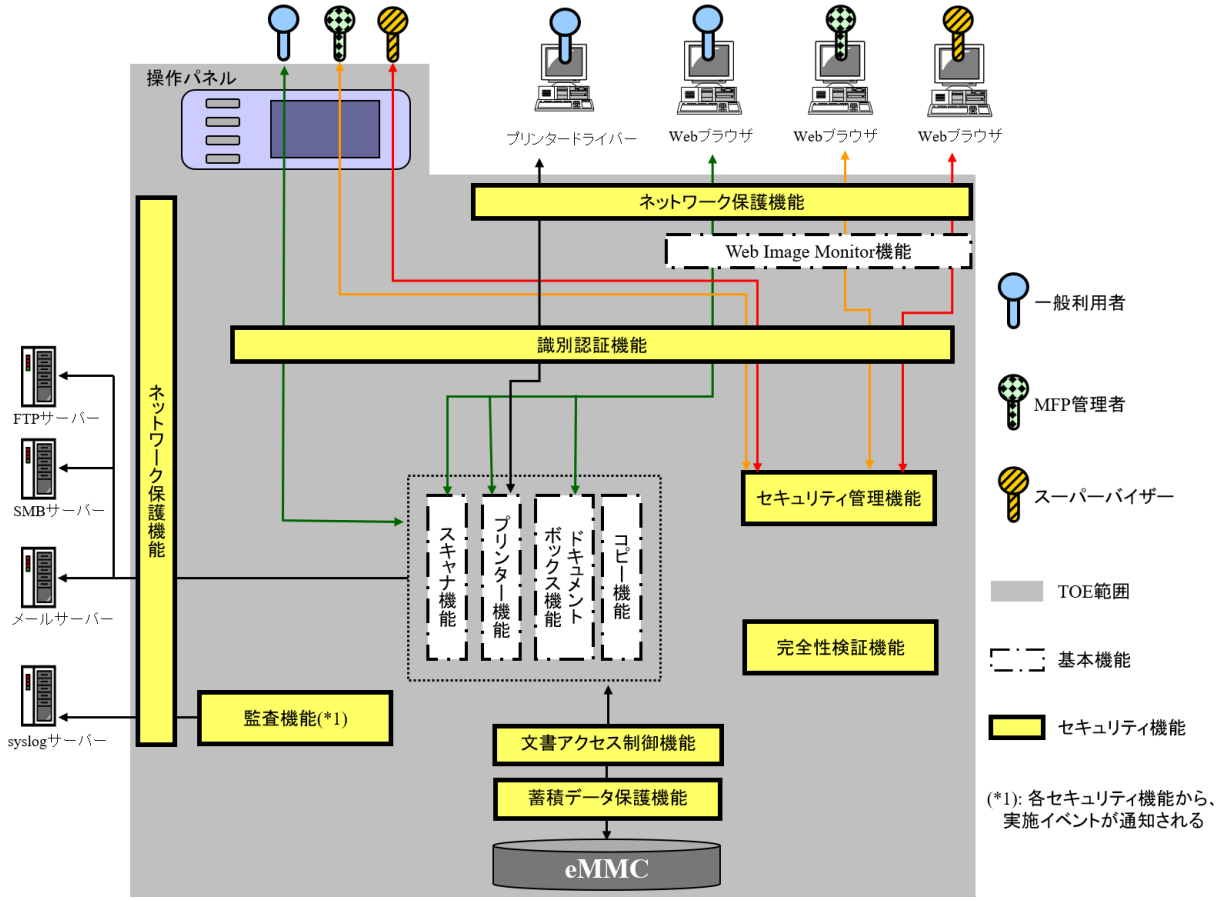

図 2 : TOE の論理的範囲

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。

コピー機能

コピー機能は、操作パネルから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を有する。また、複写印刷する画像を TOE 内へ蓄積することができる。このとき蓄積した文書データはドキュメントボックス文書として操作パネルまたは Web ブラウザからドキュメントボックス機能で操作できる。

プリンター機能

プリンター機能は、プリンタードライバーから一時保存扱いとなる印刷方法の指定で受信した文書データを TOE 内へ一時保存し、文書データを一時保存文書データとして操作パネルから印刷、プレビュー、または削除するか、Web ブラウザで削除する機能を有する。

プリンタードライバーで保存印刷を印刷方法に指定した場合、プリンタードライバーから TOE が受信した文書データを TOE 内へ蓄積でき、蓄積した文書データは保存印刷文書として操作パネルで印刷、プレビュー、または削除するか、Web ブラウザで削除することができる。

プリンタードライバーでドキュメントボックス蓄積を印刷方法に指定した場合、プリンタードライバーから文書データを TOE 内へ蓄積することができる。このとき蓄積した文書データはドキュメントボックス文書として操作パネルまたは Web ブラウザからドキュメントボックス機能で操作できる。

スキャナー機能

スキャナー機能は、操作パネルから紙文書をスキャンして読み取った画像を FTP サーバーや SMB サーバーへフォルダー送信する機能、及びメールサーバーへ文書添付メール送信する機能を有する。

操作パネルから紙文書をスキャンした画像は TOE 内に蓄積することができ、蓄積した文書データはスキャナー文書として操作パネルからフォルダー送信、文書添付メール送信、プレビュー、または削除ができる。このとき蓄積した文書データはスキャナー文書として Web ブラウザからドキュメントボックス機能でも操作できる。

ドキュメントボックス機能

ドキュメントボックス機能は、操作パネルから紙文書をスキャンし読み取った画像を TOE 内へ蓄積し、蓄積した文書データをドキュメントボックス文書として操作パネルから印刷、プレビュー、または削除するか、Web ブラウザからプレビューまたは削除する機能を有する。ドキュメントボックス機能以外で TOE 内へ蓄積した文書データに対しても以下のように操作することができる。

・コピー機能またはプリンター機能で蓄積されたドキュメントボックス文書に対し、操作パネルで印刷、プレビュー、または削除ができ、Web ブラウザでプレビューまたは削除ができる。

・スキャナー文書に対し、Web ブラウザからフォルダー送信、文書添付メール送信、ダウンロード、プレビュー、または削除ができる。

Web Image Monitor 機能

Web Image Monitor 機能は、TOE の利用者が Web ブラウザで TOE をリモート操作するための機能である。WIM と記述されることもある。

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 の使用の事象、及び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として記録し、記録した監査ログを、監査できる形式で提供する機能である。記録した監査ログは MFP 管理者のみダウンロード、削除できる。

監査ログに記録する日付・時刻は TOE のシステム時計から取得する。監査ログファイルに監査ログを追加記録する領域がない場合には、最新の監査ログを最も古い監査ログに上書きする。TOE は、監査ログを 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、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い認証に成功した利用者だけに管理機能や利用者データの操作を許可し、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。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、その利用者の役割に与えられた権限、または利用者毎に与えられた権限に基づいて、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。

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。WIM、またはプリンタードライバーを利用する際のクライアント PC との通信は TLS によって暗号化し、フォルダー送信の際の SMB サーバー及び FTP サーバーとの通信は IPsec で保護する。また文書添付メール送信の際のメールサーバーとの通信は S/MIME によって保護し、監査ログ転送設定が有効な場合の syslog サーバーとの通信は TLS によって暗号化する。

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、一般利用者、MFP 管理者、及びスーパーバイザーの役割に与えられた権限、または利用者毎に与えられた権限に基づいて、TSF データへの操作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 5 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 5 : 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、利用者データの操作ができる。
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利用者。 ・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 ・監査ログの操作 ・ネットワーク設定情報の操作 ・一般利用者及びスーパーバイザーのロックアウト状態の解除
	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利用者。 ・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

TOE が守るべき保護資産は、利用者データ、及び TSF データである。表 6 に定義を示す。

表 6 : 資産分類

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。

3.2.1 利用者データ

利用者データは、文書データと利用者ジョブデータに分類される。表 7 にて分類を定義する。

表 7 : 利用者データ定義

分類	定義
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。 eMMC に蓄積保存される文書データ(蓄積文書データ)と、プリンタードライバーから受信して TOE に一時保存する文書データ(一時保存文書データ)を対象とする。蓄積文書データにはスキャナー文書、保存印刷文書、及びドキュメントボックス文書が含まれる。
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。

3.2.2 TSF データ

TSF データは、TSF 保護データと TSF 秘密データに分類される。表 8 にて分類を定義する。

表 8 : TSF データの分類

分類	定義
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。
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 データの分類毎に、本 TOE で扱う TSF データを以下に示す。

表 9 : TSF データ定義

分類	TSF データ	内容
TSF 保護データ	ロックアウトの設定	ロックアウトポリシーに関する設定。
	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。
	S/MIME 利用者情報	文書添付メール送信において S/MIME を利用する際に必要となる情報。利用者ごとに設定する項目(メールアドレス、ユーザー証明書)、及び S/MIME 設定(暗号化設定)が含まれる。MFP 管理者によって管理登録される。

分類	TSF データ	内容
	送信先フォルダー	フォルダー送信において、送信先のサーバー及びサーバー内のフォルダーへのパス情報、アクセスのための識別認証情報を含んだ情報。MFP 管理者によって登録管理される。
	監査ログの設定	監査ログの転送に関する設定。
	暗号通信設定	クライアント、サーバーとの TLS 通信、IPsec 通信に関する設定。
	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。
	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。
	文書データの所有者情報	文書データ(一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書)のセキュリティ属性。文書データの所有者情報(ログインユーザー名)が設定される。
	文書データのアクセス許可利用者のリスト	文書データ(一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書)のセキュリティ属性。 文書データへのアクセス(閲覧)を許可する利用者情報(ログインユーザー名)が設定される。 文書データの所有者自身が他の一般利用者に読み取りを許可できる。
	利用者ジョブデータの所有者情報	利用者ジョブデータのセキュリティ属性。 利用者ジョブデータの所有者情報(ログインユーザー名)が設定される。
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	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。

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。本章に記す脅威は、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　　文書データの開示

TOE が管理している文書データが、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.DOCUMENT_DATA_ALT　　文書データの改変

TOE が管理している文書データが、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.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、権限をも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.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 文書データの開示保護

TOE は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 文書データの改変保護

TOE は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、保護することを保証する。

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、保護することを保証する。

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、保護することを保証する。

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、保護することを保証する。

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.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 10 に示す。

表 10 : 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	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										
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									

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	OE.PHYSICAL_PROTECTION	OE.NETWORK_PROTECTION	O.EMMC_ENCRYPTION	OE.TRAINED_ADMIN	OE.TRUSTED_ADMIN	OE.TRAINED_USER
P.AUDIT										X	X	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 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_ALT により TOE は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 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.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から、保護する。

これらの対策方針により、T.JOB_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.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から、保護する。

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 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.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から、保護する。

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 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.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から、保護する。

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 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。

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。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.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 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。
本章で使用する用語を表 11 に定義する。

表 11 : 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	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。 eMMC に蓄積保存される文書データ(蓄積文書データ)と、プリンタードライバーから受信して TOE に一時保存する文書データ(一時保存文書データ)を対象とする。蓄積文書データにはスキャナー文書、保存印刷文書、及びドキュメントボックス文書が含まれる。
	一時保存文書データ	プリンタードライバーから受信し TOE に一時保存された文書データ。
	スキャナー文書	蓄積文書データのうちのひとつ。スキャナー機能で TOE に蓄積された文書データ。
	保存印刷文書	蓄積文書データのうちのひとつ。印刷方法に保存印刷を指定してプリンタードライバーから受信し TOE に蓄積された文書データ。
	ドキュメントボックス文書	蓄積文書データのうちのひとつ。コピー機能またはドキュメントボックス機能で TOE に蓄積された文書データ、及び印刷方法にドキュメントボックス蓄積を指定してプリンタードライバーから受信し 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、プリンター及びドキュメントボックスの各機能の開始から終了までの作業に関する情報。

用語の分類	用語の名称	用語の内容
操作	読み取り	印刷、文書添付メール送信、フォルダー送信、ダウンロード、またはプレビューすること。
	削除	TSF データ、またはオブジェクトを削除すること。
	新規作成	TSF データを新規に作成すること。
	問い合わせ	TSF データを参照すること。
	変更	TSF データ、またはオブジェクトを変更すること。
	デフォルト値変更	TSF データのデフォルト値を変更すること。
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。
	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。
	文書データの所有者情報	文書データ(一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書)のセキュリティ属性。文書データの所有者情報(ログインユーザー名)が設定される。
	文書データのアクセス許可利用者のリスト	文書データ(一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書)のセキュリティ属性。 文書データへのアクセス(閲覧)を許可する利用者情報(ログインユーザー名)が設定される。 文書データの所有者自身が他の一般利用者に読み取りを許可できる。
	利用者ジョブデータの所有者情報	利用者ジョブデータのセキュリティ属性。 利用者ジョブデータの所有者情報(ログインユーザー名)が設定される。
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、スキャナー機能、プリンター機能、ドキュメントボックス機能の実行、中止)ができる。

用語の分類	用語の名称	用語の内容
	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利用者。 ・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 ・監査ログの操作 ・ネットワーク設定情報の操作 ・一般利用者及びスーパーバイザーのロックアウト状態の解除
	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利用者。 ・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

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 12 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、ジョブタイプ、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 12 に記す。

表 12 : 監査対象事象リスト

監査対象事象	関連 SFR
監査ログのダウンロードと削除	FAU_STG.1 FAU_SAR.1 FAU_SAR.2
・一時保存文書データ、保存印刷文書、ドキュメントボックス文書の印刷の開始と終了 ・スキャナー文書のダウンロードの開始と終了 ・スキャナー文書の文書添付メール送信の開始と終了 ・スキャナー文書のフォルダー送信の開始と終了 ・一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書の削除 ・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 FPT_STM.1
オートログアウトによるセションの終了	FTA_SSL.3
高信頼チャネル機能の失敗	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***

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。**

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*]

- *なし*

[割付: *暗号鍵生成アルゴリズム*]

- ***AES-128 を利用した乱数生成***

[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 13 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 13 : 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	一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	読み取り 削除 変更
	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 14 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 14 : サブジェクトとオブジェクトとセキュリティ属性

分類	サブジェクトまたはオブジェクト	セキュリティ属性
サブジェクト	一般利用者プロセス	ログインユーザー名 ユーザー権限
サブジェクト	MFP 管理者プロセス	ログインユーザー名 ユーザー権限
サブジェクト	スーパーバイザープロセス	ログインユーザー名 ユーザー権限
オブジェクト	一時保存文書データ	文書データの所有者情報
オブジェクト	スキャナー文書 保存印刷文書 ドキュメントボックス文書	文書データの所有者情報 文書データのアクセス許可利用者のリスト
オブジェクト	利用者ジョブデータ	利用者ジョブデータの所有者情報

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 15 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 15 : オブジェクトとサブジェクト間の操作を制御する規則

オブジェクト	操作	サブジェクト (セキュリティ属性)	利用者データアクセス制御 SFP の規則
一時保存文書データ	読み取り 削除	一般利用者プロセス (ログインユーザー名、ユーザー権限)	許可しない。ただし、オブジェクトの「文書データの所有者情報」に登録されているログインユーザー名と一致する一般利用者プロセスに操作を許可する。
スキャナー文書 保存印刷文書 ドキュメントボックス文書	読み取り	一般利用者プロセス (ログインユーザー名、ユーザー権限)	許可しない。ただし、オブジェクトの「文書データの所有者情報」に登録されているログインユーザー名と一致する一般利用者プロセスに操作を許可する。さらに、オブジェクトの「文書データのアクセス許可利用者のリスト」に登録されているログインユーザー名と一致する一般利用者プロセスに操作を許可する。
スキャナー文書 保存印刷文書 ドキュメントボックス文書	削除	一般利用者プロセス (ログインユーザー名、ユーザー権限)	許可しない。ただし、オブジェクトの「文書データの所有者情報」に登録されているログインユーザー名と一致する一般利用者プロセスに操作を許可する。
利用者ジョブデータ	削除	一般利用者プロセス (ログインユーザー名、ユーザー権限)	許可しない。(*1) ただし、オブジェクトの「利用者ジョブデータの所有者情報」に登録されているログインユーザー名と一致する一般利用者プロセスに操作を許可する。

(*1) インタフェースを提供しない。

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 16 に示すアクセスを明示的に許可する規則***

表 16 : アクセスを明示的に許可する規則

オブジェクト	操作	サブジェクト (セキュリティ属性)	利用者データアクセス制御 SFP の規則
一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	削除	MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	許可する。
スキャナー文書 ドキュメントボックス文書	読み取り	MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	許可する。
利用者ジョブデータ	削除	MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	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 17 に示すアクセスを明示的に拒否する規則***

表 17 : アクセスを明示的に拒否する規則

オブジェクト	操作	サブジェクト (セキュリティ属性)	利用者データアクセス制御 SFP の規則
一時保存文書データ 保存印刷文書	読み取り	MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	拒否する。(*1)
一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	読み取り 削除	スーパーバイザープロセス (ユーザー権限、ログインユーザー名)	拒否する。(*1)
一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	変更	一般利用者プロセス (ユーザー権限、ログインユーザー名)	いずれのサブジェクトにも、文書データの操作を拒否する。(*1)
		MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	

オブジェクト	操作	サブジェクト (セキュリティ属性)	利用者データアクセス制御 SFP の規則
		スーパーバイザープロセス (ユーザー権限、ログインユーザー名)	
利用者ジョブデータ	削除	スーパーバイザープロセス (ユーザー権限、ログインユーザー名)	拒否する。(*1)
利用者ジョブデータ	変更	一般利用者プロセス (ログインユーザー名、ユーザー権限)	いずれのサブジェクトにも、利用者ジョブデータの操作を拒否する。(*1)
		MFP 管理者プロセス (ユーザー権限、ログインユーザー名)	
		スーパーバイザープロセス (ユーザー権限、ログインユーザー名)	

(*1)インタフェースを提供しない。

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 18 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]

- ***1～5***

表 18 : 認証事象のリスト

認証事象
操作パネルを使用する際の利用者認証

認証事象
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文書データを受信し一時保存または蓄積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、を上回った***

[割付: *アクションのリスト*]

- ***表 19 に示すアクション***

表 19 : 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
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
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

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*

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*

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 20 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]*]

- ***デフォルト値変更、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 20 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 20 : 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]	新規作成 変更 削除	MFP 管理者
ログインユーザー名 [MFP 管理者に紐づく場合]	新規作成	MFP 管理者
	変更	当該 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
ユーザー権限	変更	操作を許可する役割なし
文書データの所有者情報	変更	操作を許可する役割なし
文書データのアクセス許可利用者のリスト	変更	MFP 管理者 文書データの所有者(一般利用者)

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)
	デフォルト値変更	MFP 管理者
利用者ジョブデータの所有者情報	変更	操作を許可する役割なし

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*]

- ***表 21 の操作を許可する役割(ユーザー権限)***

表 21 : デフォルト値を上書きする操作を許可する役割

オブジェクト	セキュリティ属性	操作を許可する役割(ユーザー権限)
一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	文書データの所有者情報	操作を許可する役割なし
スキャナー文書	文書データのアクセス許可利用者のリスト	文書データを作成する当該一般利用者
保存印刷文書	文書データのアクセス許可利用者のリスト	操作を許可する役割なし
ドキュメントボックス文書	文書データのアクセス許可利用者のリスト	文書データを作成する当該一般利用者 (操作パネルからの文書データの蓄積時のみデフォルト値の上書きが許可される。プリンタードライバーからの文書データの蓄積時にデフォルト値を上書きするインタフェースはない。)

オブジェクト	セキュリティ属性	操作を許可する役割(ユーザー権限)
利用者ジョブデータ	利用者ジョブデータの所有者情報	操作を許可する役割なし

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***

[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 保護データ	ロックアウトの設定	変更	MFP 管理者
	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
	S/MIME 利用者情報	新規作成 変更 削除	MFP 管理者
	送信先フォルダー	新規作成 変更 削除	MFP 管理者
	監査ログの設定	変更	MFP 管理者
	暗号通信設定	変更	MFP 管理者
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]	変更	当該一般利用者 MFP 管理者
		新規作成	MFP 管理者

分類	TSF データ	操作	操作を許可する役割(ユーザー権限)
	ログインパスワード [MFP 管理者に紐づく場合]	変更	当該 MFP 管理者 スーパーバイザー
		新規作成	MFP 管理者
	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
	eMMC 暗号鍵	新規作成 問い合わせ 削除	MFP 管理者

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
ログインユーザー名の新規作成、変更、削除
文書データのアクセス許可利用者のリストの変更、デフォルト値変更
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、新規作成
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
S/MIME 利用者情報の新規作成、変更、及び削除
送信先フォルダーの新規作成、変更、及び削除
監査ログの設定の変更
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*、*MFP 管理者*、*スーパーバイザー***

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*]

- ***MFP 管理者の指定した時間***

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*]

- ***スキャナー機能***
- ***syslog 転送機能***
- ***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
	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対応

	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.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FAU_GEN.1									**P**	
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**							
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**					
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**		

	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.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
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 文書データの開示保護

O.DOCUMENT_DATA_DIS は、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、TOE が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、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、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、文書データ生成時のデフォルトのセキュリティ属性の管理を行う。

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　　文書データの改変保護

O.DOCUMENT_DATA_ALT は、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、TOE が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) FDP_ACC.1、FDP_ACF.1
FDP_ACC.1 と FDP_ACF.1 によって、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、文書データ生成時のデフォルトのセキュリティ属性の管理を行う。

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から、TOE が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) 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生成時のデフォルトのセキュリティ属性の管理を行う。

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、TOE が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、TOE が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 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、TOE が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 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)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が認証され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) 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_USB.1
FIA_USB.1 によって、セキュリティ属性を、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 である。

(3) FIA_ATD.1
FIA_ATD.1 によって、識別認証前に、TOE に登録された各利用者のセキュリティ属性を維持する。

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

(4) 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。

(5) 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品質尺度を満たす場合のみパスワード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。

(6) 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。

(7) FTA_SSL.3
FTA_SSL.3 によって、利用者の最終操作から MFP 管理者の指定した時間経過後、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。

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) 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を削除し、新しい監査ログを記録する。

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	本 ST の SFR	充足性
FAU_GEN.1	FPT_STM.1	FPT_STM.1	OK
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	OK
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	OK
FAU_STG.4	FAU_STG.1	FAU_STG.1	OK
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	OK
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	OK
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4	OK
FCS_CKM.4	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]	FCS_CKM.1	OK
FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	OK
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	OK
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	OK
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	OK
FIA_ATD.1	なし	なし	OK
FIA_SOS.1	なし	なし	OK
FIA_UAU.1	FIA_UID.1	FIA_UID.1	OK
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	OK
FIA_UID.1	なし	なし	OK
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	OK

TOE セキュリティ機能要件	要求された依存性	本 ST の SFR	充足性
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK
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	OK ただし、ユーザー権限の変更、文書データの所有者情報の変更、利用者ジョブデータの所有者情報の変更を実施するインタフェースが提供されていないため、FMT_SMF.1 には、これらの管理機能は不要である。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	OK
FMT_MTD.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK
FMT_MTD.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1	OK ただし、ログインパスワードの問い合わせを実施するインタフェースが提供されていないため、FMT_SMF.1 にはこの管理機能は不要である。
FMT_SMF.1	なし	なし	OK
FMT_SMR.1	FIA_UID.1	FIA_UID.1	OK
FPT_STM.1	なし	なし	OK
FPT_TST_EXP.1	なし	なし	OK
FTA_SSL.3	なし	なし	OK
FTP_ITC.1	なし	なし	OK

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 の監査事象を利用者の識別情報と紐づけたログを監査ログとして eMMC に記録し、記録した監査ログを監査できる形式で提供する機能である。記録した監査ログは、MFP 管理者のみダウンロード、削除の操作ができる。高信頼タイムスタンプを提供する機能、監査ログ満杯時の制御機能もこの機能に含む。監査ログは転送して 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 に示す監査ログ項目を eMMC に記録する。監査ログ項目には、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 に示す監査ログ項目を記録する監査事象発生時のみ記録する。監査対象事象のうち高信頼チャネル機能の失敗については、高信頼チャネルを介した通信を行う機能の失敗を指し、その機能は WIM、フォルダー送信、文書添付メール送信、プリンタードライバーから受信した文書データの一時保存や蓄積、及び syslog 転送が該当するため、それらの通信の失敗のログを監査事象としている。

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
監査ログのダウンロードと削除
ログイン操作の成功と失敗
ロックアウトの開始と解除
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
WIM の通信の失敗
フォルダー送信の失敗
文書添付メール送信の失敗
プリンタードライバーから受信した文書データの一時保存及び蓄積の失敗
syslog 転送の失敗
利用者ジョブデータの削除
一時保存文書データ、保存印刷文書、ドキュメントボックス文書の印刷の開始と終了

監査事象
スキャナー文書のダウンロードの開始と終了
スキャナー文書の文書添付メール送信の開始と終了
スキャナー文書のフォルダー送信の開始と終了
一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書の削除

表 29 : 監査ログ項目のリスト

	監査ログ項目	監査ログ項目への設定値	監査ログ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	ジョブタイプ	文書データの印刷・ダウンロード・文書添付メール送信・フォルダー送信・削除、利用者ジョブデータの削除(利用者ジョブデータの削除は、キャンセル詳細の欄に値が記録される)	・一時保存文書データ、保存印刷文書、ドキュメントボックス文書の印刷 ・スキャナー文書のダウンロード ・スキャナー文書の文書添付メール送信 ・スキャナー文書のフォルダー送信 ・一時保存文書データ、スキャナー文書、保存印刷文書、ドキュメントボックス文書の削除 ・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	・WIM の通信の失敗 ・フォルダー送信の失敗 ・プリンタードライバーから受信した文書データの一時保存及び蓄積の失敗 ・syslog 転送の失敗
		文書添付メール送信時の宛先メールアドレス	・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

	監査ログ項目	監査ログ項目への設定値	監査ログを記録する監査事象
	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。監査事象が「文書データの削除」の場合は、成功のみ記録する。

以下の監査事象では、失敗と記録する。

・WIM の通信の失敗

・フォルダー送信の失敗

・プリンタードライバーから受信した文書データの一時保存及び蓄積の失敗

・syslog 転送の失敗

・文書添付メール送信の失敗

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、監査ログの削除を MFP 管理者だけに許可する。監査ログの削除操作は 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、監査ログファイルに監査ログを追加記録する領域がない場合には、最新の監査ログを最も古い監査ログに上書きする。

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、及び問い合わせ情報の参照の実行は、識別認証をしなくても TOE の利用を許可する。

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 MFP 管理者の指定した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。

なおプリンタードライバーからの要求に対しても識別認証を行うが、このとき文書データの受信完了とともにログアウトするため、自動でログアウトするべき持続する対話セションはない。

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。

間違ったパスワードの入力によるログイン失敗時、MFP 管理者が設定したパスワードの入力許容回数(1～5 回)に達した場合、または超えた場合にロックアウトする。

認証失敗の回数はログイン元(操作パネル、WIM、及びプリンタードライバー)が異なっても合算してカウントする。

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。

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

・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

・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 : 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
MFP 管理者	スーパーバイザー
スーパーバイザー	MFP 管理者

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、識別認証機能で認証された TOE の許可利用者に対し、その利用者の役割に与えられた権限、または利用者毎に与えられた権限に基づいて、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.1 (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、利用者データアクセス制御 SFP を実施することで、文書アクセス制御機能を提供する。利用者データアクセス制御 SFP の規則は(1)文書データのアクセス制御ルール、(2)利用者ジョブデータへのアクセ

ス制御ルールに分けられ、それらに従って、TOE は利用者による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) **文書データのアクセス制御ルール**

表 31 に文書データのアクセス制御規則を示す。TOE は、文書データの削除及び読み取りの操作を一般利用者、MFP 管理者、及びスーパーバイザーに対し制限する。文書データを変更するインタフェースは提供しない。とくに一般利用者の操作については表 32 に示し、表 32 以外の操作のインタフェースは提供しない。

表 31 : 文書データのアクセス制御規則

ユーザー権限	文書データ	アクセス制御規則
一般利用者	一時保存文書データ	一時保存文書データの「文書データの所有者情報」と同一のログインユーザー名をもつ一般利用者に読み取りと削除を許可する。 それ以外の一般利用者には文書データを一覧に表示せず、削除と読み取りの操作は許可しない。
	スキャナー文書 保存印刷文書 ドキュメントボックス文書	「文書データの所有者情報」と同一のログインユーザー名をもつ一般利用者に読み取りと削除を許可する。 また、「文書データのアクセス許可利用者のリスト」に登録されているログインユーザー名をもつ一般利用者に読み取りを許可する。 それ以外の一般利用者には文書データを一覧に表示せず、読み取りと削除を許可しない。
MFP 管理者	一時保存文書データ 保存印刷文書	操作パネルと WIM での削除を許可する。 読み取りのインタフェースは提供しない。
	スキャナー文書 ドキュメントボックス文書	操作パネルと WIM での削除を許可する。 WIM でのプレビューを許可する(その他の読み取りのインタフェースは提供しない)。
スーパーバイザー	一時保存文書データ スキャナー文書 保存印刷文書 ドキュメントボックス文書	削除及び読み取りのインタフェースは提供しない。

表 32 : 文書データに対する一般利用者の操作

No.	オブジェクト	操作	操作箇所	MFP アプリケーション
1	一時保存文書データ	削除 印刷 プレビュー	操作パネル	プリンター機能
2	一時保存文書データ	削除	WIM	プリンター機能
3	スキャナー文書	削除(*1) 文書添付メール送信 フォルダー送信 プレビュー	操作パネル	スキャナー機能
4	スキャナー文書	削除(*1) 文書添付メール送信 フォルダー送信 プレビュー ダウンロード	WIM	ドキュメントボックス機能
5	保存印刷文書	削除(*1) 印刷 プレビュー	操作パネル	プリンター機能
6	保存印刷文書	削除(*1)	WIM	プリンター機能
7	ドキュメントボックス文書	削除(*1) 印刷 プレビュー	操作パネル	ドキュメントボックス機能
8	ドキュメントボックス文書	削除(*1) プレビュー	WIM	ドキュメントボックス機能

(*1) 削除は文書データの所有者に許可する操作であり、所有者から文書データのアクセス(閲覧)を許可された他の利用者に対し許可する操作には該当しない。

(2) **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(ジョブをキャンセル)する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。

・一般利用者の場合:利用者ジョブデータの所有者情報に登録されているログインユーザー名が一致する場合に、削除の操作を許可する。それ以外の一般利用者には、利用者ジョブデータの表示を許可するが、利用者ジョブデータの削除は許可しない。

・MFP 管理者の場合:利用者ジョブデータの削除を許可する。

・スーパーバイザーの場合:利用者ジョブデータを操作するインタフェースは提供しない。

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、改ざんを検出する機能である。WIM、またはプリンタードライバーを利用する際のクライアント PC との通信は TLS によって暗号化し、フォルダー送信の際の SMB サーバー及び FTP サーバーとの通信は IPsec で保護する。また文書添付メール送信の際のメールサーバーとの通信は S/MIME によって保護し、監査ログ転送設定が有効な場合の syslog サーバーとの通信は TLS によって暗号化する。

FTP_ITC.1 (TSF 間高信頼チャネル)

TOE は、高信頼 IT 製品間との通信(WIM の通信、フォルダー送信、文書添付メール送信、プリンタードライバーから文書データを受信して一時保存または蓄積、syslog サーバーへの転送)を行う際は、通信先によって異なる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、またはプリンタードライバーが暗号化通信を開始するのを許可する。TOE はメールサーバー、SMB サーバー、FTP 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 33 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。文書添付メール送信の利用時は、メールサーバーと暗号化通信(S/MIME)を行う。フォルダー送信の利用時は必ず、FTP サーバーまたは SMB サーバーと暗号化通信(IPsec)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 33 : 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(*1)	TLS1.2	AES(128bits、256bits)
	TLS1.3	AES(128bits、256bits)、ChaCha20(256bit)
FTP サーバー	IPsec	AES(128bits、192bits、256bits)
SMB サーバー	IPsec	AES(128bits、192bits、256bits)
メールサーバー	S/MIME	AES(128bits、256bits)
syslog サーバー	TLS1.2	AES(128bits、256bits)
	TLS1.3	AES(128bits、256bits)、ChaCha20(256bit)

(*1) プリンタードライバーを利用する通信の場合、サポートするプロトコルの TLS バージョンはクライアント PC の OS バージョンに依存する。

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、CTR_DRBG(AES-128)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_SMF.1、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1(a)、FMT_MTD.1(b) (管理機能の特定、セキュリティ機能のふるまいの管理、セキュリティ属性の管理、TSF データの管理)

TOE は以下の管理機能を実行する。

・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 34 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。

表 34 : 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 保護データ	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 WIM
	オートログアウトの設定	変更	MFP 管理者	操作パネル WIM
	S/MIME 利用者情報	新規作成 変更 削除	MFP 管理者	操作パネル(*2) WIM
	送信先フォルダー	新規作成 変更 削除	MFP 管理者	操作パネル WIM
	監査ログの設定	変更	MFP 管理者	操作パネル WIM
	暗号通信設定	変更	MFP 管理者	操作パネル WIM
	ログインユーザー名 [一般利用者に紐づく場合]	新規作成 変更 削除	MFP 管理者	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]	新規作成	MFP 管理者	操作パネル WIM
		変更	当該 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	操作パネル WIM
	ユーザー権限	変更(*1)	なし	なし
	文書データの所有者情報	変更(*1)	なし	なし
	文書データのアクセス許可利用者のリスト	変更	MFP 管理者 文書データの所有者(一般利用者)	操作パネル(*3) WIM
		デフォルト値変更	MFP 管理者	操作パネル WIM
	利用者ジョブデータの所有者情報	変更(*1)	なし	なし
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	MFP 管理者	操作パネル WIM
		変更	当該一般利用者 MFP 管理者	操作パネル WIM
		問い合わせ(*1)	なし	なし

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
	ログインパスワード [MFP 管理者に紐づく場合]	新規作成	MFP 管理者	操作パネル WIM
		変更	当該 MFP 管理者 スーパーバイザー	操作パネル WIM
		問い合わせ(*1)	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(*1)	なし	なし
	eMMC 暗号鍵	問い合わせ 削除 新規作成	MFP 管理者	操作パネル

(*1): インタフェースを提供しない。

(*2): 操作パネルからできる操作は、S/MIME 利用者情報に含まれる、利用者ごとに設定する項目のメールアドレスの操作のみである。

(*3): 保存印刷文書の場合、操作パネルでは文書データのアクセス許可利用者のリストを操作できず、WIM でのみ操作できる。

FMT_MSA.3 (静的属性初期化)

表 35 にセキュリティ属性静的初期化のリスト、表 36 に文書データの生成ケース毎のセキュリティ属性を示す。

TOE は、表 35 及び表 36 に示した規則に従って、オブジェクトの生成時のセキュリティ属性のデフォルト値を設定する。セキュリティ属性のデフォルト値の上書きについては、限られた場合のみに許可し、なしと記すものについては上書きのインタフェースを提供しない。

表 35 : セキュリティ属性静的初期化のリスト

オブジェクト	セキュリティ属性	デフォルト値	デフォルト値の上書き
文書データ	文書データの所有者情報	表 36 を参照	表 36 を参照
	文書データのアクセス許可利用者のリスト	表 36 を参照	表 36 を参照
利用者ジョブデータ	利用者ジョブデータの所有者情報	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	なし

表 36 : 文書データの生成ケース毎のセキュリティ属性

オブジェクトの生成	セキュリティ属性	デフォルト値	デフォルト値の上書き
プリンタードライバーから 一時保存印刷を指定し一時保存した 一時保存文書データ	文書データの所有者情報	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	なし
プリンタードライバーから 保存印刷を指定し蓄積した 保存印刷文書	文書データの所有者情報	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	なし
	文書データのアクセス許可利用者のリスト	文書データ作成者の「文書データのアクセス許可利用者のリスト」のデフォルト値(ログインユーザー名のリスト)	なし
プリンタードライバーから ドキュメントボックス蓄積を指定し蓄積した ドキュメントボックス文書	文書データの所有者情報	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	なし
	文書データのアクセス許可利用者のリスト	文書データ作成者の「文書データのアクセス許可利用者のリスト」のデフォルト値(ログインユーザー名のリスト)	なし
操作パネル(コピー機能またはドキュメントボックス機能)から 紙文書をスキャンして蓄積した ドキュメントボックス文書	文書データの所有者情報	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	なし
	文書データのアクセス許可利用者のリスト	文書データ作成者の「文書データのアクセス許可利用者のリスト」のデフォルト値(ログインユーザー名のリスト)	操作パネルから文書データ作成者がアクセス(閲覧)を許可した値(ユーザー名のリスト)を上書きできる。
操作パネル(スキャナー機能)から 紙文書をスキャンして蓄積した スキャナー文書	文書データの所有者情報	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	なし
	文書データのアクセス許可利用者のリスト	文書データ作成者の「文書データのアクセス許可利用者のリスト」のデフォルト値(ログインユーザー名のリスト)	操作パネルから文書データ作成者がアクセス(閲覧)を許可した値(ユーザー名のリスト)を上書きできる。

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。

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 37 : 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。本体の制御ボードに格納されている。
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、プリンター及びドキュメントボックスの各機能の開始から終了までの作業。
MFP アプリケーション	TOE が提供するコピー、スキャナー、プリンター及びドキュメントボックスの各機能の総称。
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	スキャナー機能で操作パネルから紙文書をスキャンして読み取った画像または蓄積したスキャナー文書を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、S/MIME によって保護される。
フォルダー送信	スキャナー機能で操作パネルから紙文書をスキャンして読み取った画像または蓄積したスキャナー文書を MFP からネットワーク経由で SMB サーバー内の共有フォルダーに対して SMB プロトコルで送信する、もしくは FTP サーバーのフォルダーに対して FTP プロトコルで文書データを送信する機能。この機能を実現するための通信は、IPsec によって保護される。
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。
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。