RICOH IM 460F/370F with 拡張 HDD タイプ M54
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 460F/370F with 拡張 HDD タイプ M54 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 種別がデジタル複合機(以下、MFP と言う)である、TOE の識別情報を以下に示す。

TOE 名称:

RICOH IM 460F/370F with 拡張 HDD タイプ M54

バージョン: J-1.00

本 TOE はソフトウェアとハードウェアが搭載される対象 MFP と、TOE を構成するために装着するオプション製品の組み合わせからなる。

対象 MFP は表 1 に示す日本国内向けの製品であり、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	RICOH IM 370F	D0DM-03
2	RICOH IM 460F	D0DN-00

オプション製品は表 2 に示すものが対象であり、製品名によって識別する。

表 2：オプション製品の製品名

No.	オプション製品	製品名
1	HDD	拡張 HDD タイプ M54

対象 MFP とオプション製品の TOE となる組み合わせを表 3 に示す。

対象 MFP にはオプション製品の HDD が必ず搭載される。

表 3：対象 MFP とオプション製品の組み合わせ

No.	MFP		オプション製品
	製品名	機種コード	製品名
1	RICOH IM 370F	D0DM-03	拡張 HDD タイプ M54
2	RICOH IM 460F	D0DN-00	拡張 HDD タイプ M54

これらの 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 4 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 4：バージョン J-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	D0DM5551C
3	IRIPS PS3PDF	1.00	D0DM5553B
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

No.	本体のソフトウェアの名称	バージョン	部番
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
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	Bluetooth サービス	1.00	D0DN1433B

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
45	Bluetooth 認証プラグイン	5.0.0	D0DN1446A
46	DeviceManagementService	1.01.00	D0DN1455D
47	GraphicData	0.10	DXXXXXXX
48	ICCardDispatcher	1.01.00	D0DN1443A
49	iWnn IME	2.16.204	D0E01430C
50	iWnn IME Korean Pack	2.16.2	D0E01433
51	iWnn IME Simplified Chinese Pack	2.16.2	D0E01431
52	iWnn IME Traditional Chinese Pack	2.16.2	D0E01432
53	KerberosService	1.0	D0DN1451B
54	LegacyUIData	0.24	DXXXXXXX
55	ProgramInfoService	1.00	D0DN1434C
56	RemoteSupportService	1.00	D0DN1453B
57	RicohScanGUIService	3.00	D0DN1450C
58	USB カードリーダー対応プラグイン	1.00.00	D0DN1445A
59	かんたんカード認証設定	1.00.00	D0DN1426A
60	かんたん文書印刷	1.00	D0DN1440C
61	アプリケーションサイト	3.06.20	D0DN1441D
62	カンタン入出力	5.0.0	D0DN1427A
63	クラウド設定	1.01.14	D0DN1456D
64	コピー	1.01	D0DN1436D
65	サポート設定	1.00	D0DN1449B
66	スキャナー	1.01	D0DN1437D
67	ストップウィジェット	1.00	D0DN1431B
68	ダイレクト接続	1.25	D0DN1447
69	トレイ設定/用紙残量	1.00	D0DN1442B
70	ドキュメントボックス	1.00	D0DN1454C
71	ファクス	1.01	D0DN1438C
72	プリンター情報確認	1.00	D0DN1435C
73	メディアプリント＆スキャン	1.00	D0DN1439C

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
74	リモートコネクトサポート	1.1.9	D0E01462C
75	導入設定	1.00	D0DN1448B
76	操作部画面の遠隔操作	1.00	D0DN1452C
77	標準 IC カードプラグイン	1.00.00	D0DN1444A
78	言語切り替えｳｨｼﾞｪｯﾄ	1.00	D0DN1428B
79	ecoウィジェット	1.00	D0DN1432B
80	ｻﾌﾟﾗｲ残量表示ｳｨｼﾞｪｯﾄ	1.00	D0DN1429B
81	ﾌｧｸｽ受信文書ｳｨｼﾞｪｯﾄ	1.00	D0DN1430B

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 の使用方法、TOE の主要なセキュリティ機能を述べる。

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、及び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、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、利用者制限、蓄積データ保護機能、残存情報消去、及び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。

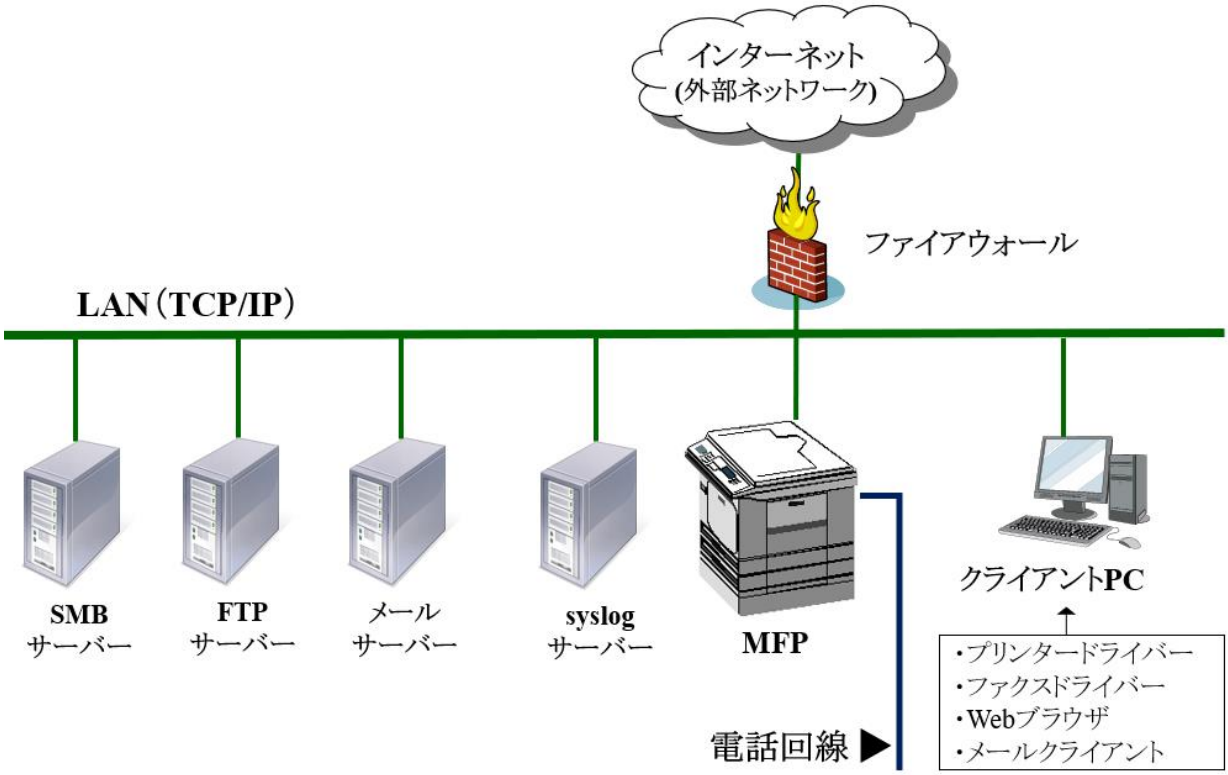

図 1 : TOE の利用環境

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 RPCS ドライバーというプリンタードライバー(1.0.0.0 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 からファクス送信用の文書データ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 PC FAX Generic ドライバーというファクスドライバー(13.1.0.0 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、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 11
- プリンタードライバー: RPCS ドライバー 1.0.0.0
- ファクスドライバー: PC FAX Generic ドライバー 13.1.0.0
- 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、表 2 のオプション製品、表 6 のガイダンスからなる。

MFP 製品は、表 5 に示すバージョン(J-1.00)を構成するソフトウェアを搭載した MFP 本体である。「拡張 HDD タイプ M54」は、HDD のハードウェアであり、全ての MFP 本体に必ず装着する。

MFP 本体及びオプション製品は、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。以下に記載の組み合わせを利用者へ配付する。

表 5：配付する組み合わせ

No.	MFP 本体			オプション製品		ガイダンス	備考
	製品名	機種コード	バージョン	製品名	バージョン		
1	RICOH IM 370F	D0DM-03	J-1.00	拡張 HDD タイプ M54	なし	表 6 を参照	SPDF を標準搭載
2	RICOH IM 460F	D0DN-00	J-1.00	拡張 HDD タイプ M54	なし	表 6 を参照	SPDF を標準搭載

本 TOE のガイダンス文書、配付形式、及び配付方法を表 6 に示す。

表 6：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	D0DM-7002	かんたん操作ガイド	冊子	製品と同梱
2	D0DM-7013	本機を安全にご利用いただくために	冊子	製品と同梱
3	D0DM-7300	安全上のご注意	PDF	Web 配付
4	D0DM7302	使用説明書 RICOH IM 460F/370F	HTML	Web 配付
5	D0E37515	セキュリティーリファレンス	HTML	Web 配付
6	D0DM-7306 2024.02.08	使用説明書〈IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ〉	PDF	Web 配付
7	D0E3-7510 2023.09.28	セキュリティー機能をお使いになるお客様へ	PDF	Web 配付
8	83NHEZ-JAR1.00 v281	ヘルプ	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_460_370-2600-spf/ja/Guidance_ja.zip

ハッシュ値(SHA256): 49c9198b883cf9ffb0b84e35920f3b8cbfc6ed6f784a6fceb5e13b7b0fdeb597

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。

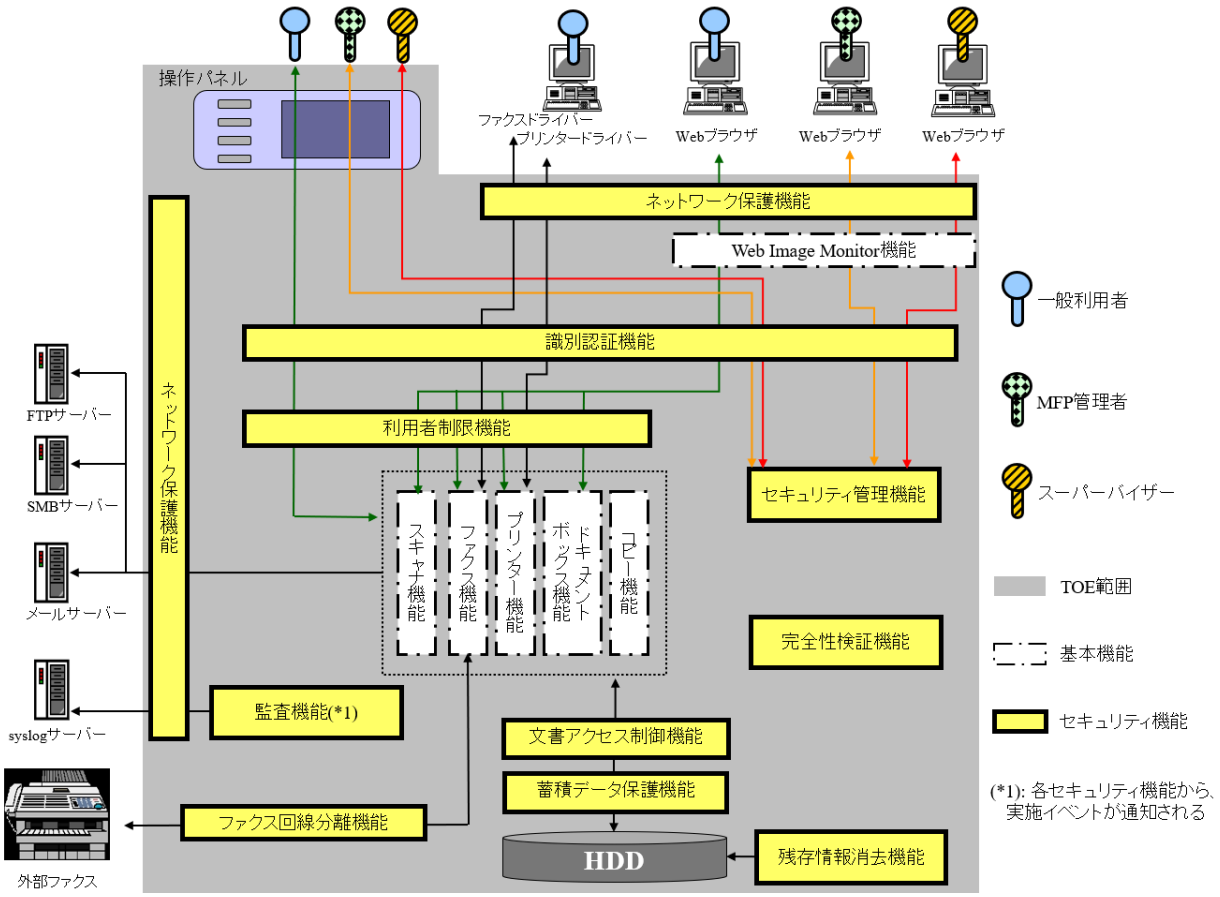

図 2 : TOE の論理的範囲

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、プリンター機能、スキャナー機能、ファクス機能、及びドキュメントボックス機能は TOE の MFP アプリケーションであり、各機能が有する PP の SFR パッケージ機能はカッコ書きで示す。

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(F.CPY)。また、複写印刷する画像を TOE 内へ蓄積することができる(F.SCN 及び F.DSR)。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(F.PRT)。

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(F.DSR。印刷のみ F.DSR 及び F.PRT)。

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(F.DSR)。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。操作パネルで送信前にプレビューもできる(F.SCN)。

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(F.SCN 及び F.DSR)、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(F.DSR)。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。

ファクス機能

ファクス機能は、ファクス送信機能とファクス受信機能からなる。電話回線を利用する G3 規格に準拠したファクスが評価対象である。

ファクス送信機能は、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文書データとして外部ファクス装置に送信する機能を有する。操作パネルで送信前にプレビューもできる(F.FAX)。

また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(F.SCN 及び F.DSR)、またはファクスドライバーから受信した文書データを TOE 内へ蓄積することもでき、蓄積した文書データはファクス送信文書として操作パネルからファクス送信、プレビュー、または削除ができる(F.DSR)。このとき蓄積した文書データはファクス送信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も操作できる。

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文書データを受信し(F.FAX)、TOE 内に蓄積する機能を有する(F.DSR)。蓄積した文書データはファクス受信文書として操作パネルから印刷、プレビュー、または削除ができ、Web ブラウザからダウンロード、プレビュー、または削除ができる(F.DSR。印刷のみ F.DSR 及び F.PRT)。

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(F.SCN 及び F.DSR)、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や削除する機能を有する(F.DSR。印刷のみ F.DSR 及び F.PRT)。

また、他の機能で蓄積した文書データも操作することができる(いずれも F.DSR。印刷のみ F.DSR 及び F.PRT)。以下に示す。

・ドキュメントボックス文書(コピー機能またはプリンター機能で蓄積)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や削除ができる。

・ファクス送信文書に対し、操作パネルから印刷、プレビュー、または削除ができ、Web ブラウザからファクス送信、ダウンロード、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の操作や MFP アプリケーションの利用を許可し、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て、その利用者の役割に対して与えられた権限、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。

利用者制限機能

利用者制限機能は、識別認証機能で認証された TOE の許可利用者の役割、及び利用者毎に設定された操作権限に従って、MFP アプリケーションのジョブ実行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、プリンタードライバー、またはファクス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。

残存情報消去機能

残存情報消去機能は、HDD 上の削除された文書データ、一時的な文書データあるいはその断片に対して、乱数や指定パターンデータを上書きすることにより残存情報の再利用を不可能とする機能である。

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利用者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利用者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 の一部及び TSF 実行コードが完全性を保ったソフトウェア構成であることを MFP 初期立上げ中に検証する自己テスト機能である。

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(本機能名にあるファクス回線と同意)から LAN への侵入を防止するために、電話回線から LAN への入力情報をファクス受信のみに限定したうえで受信ファクスの転送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、HDD に記録されているデータを漏えいから保護するため、HDD に書き込むデータを暗号化する機能である。

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 と TOE が論証適合している PP は、

PP 名称/識別: U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009)

バージョン: 1.0

である。

注釈: 本 PP は Common Criteria Portal に掲載されている「IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B」に適合し、かつ「CCEVS Policy Letter #20」も満たしている。

2.3 パッケージ主張

本 ST のパッケージ適合主張を以下に記す。

本 ST 及び TOE は、パッケージ:EAL2 追加を主張し、ALC_FLR.2 の保証コンポーネントを追加する。以下のパッケージ参照にて示すパッケージ名に適合する。

表 7：パッケージ参照

タイトル	パッケージバージョン
2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B	1.0, dated March 2009
2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B	1.0, dated March 2009
2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B	1.0, dated March 2009
2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B	1.0, dated March 2009
2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B	1.0, dated March 2009
2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B	1.0, dated March 2009

2.4 適合主張根拠

2.4.1 PP の TOE 種別との一貫性主張

PP が対象とする製品の種別は、Hardcopy devices(以下、HCDs と言う)である。HCDs は、スキャナー装置とプリント装置で構成され、電話回線を接続するインタフェースを備えた装置であり、これらの装置を組合せて、印刷(F.PRT)、スキャン(F.SCN)、コピー(F.CPY)、またはファクス(F.FAX)の内、1 機能以上を搭載しているものである。一部の HCDs は、ハードディスクドライブなどの不揮発性記録媒体や、ドキュメントサーバー機能(F.DSR)をもつ。本 TOE の種別は MFP である。TOE は MFP として、不揮発性記録媒体、電話回線を接続するインタフェース、スキャナー装置、及びプリント装置を備え、コピー、スキャナー、プリンター、ファクス、及びドキュメントボックス機能を搭載している。これらによって、印刷(F.PRT)、スキャン(F.SCN)、コピー(F.CPY)、ファクス(F.FAX)、及び文書の保存と取り出し(F.DSR)が可能であることから、本 TOE 種別である MFP は HCDs の特徴を有し、PP の TOE 種別と一貫していると言える。

2.4.2 PP のセキュリティ課題とセキュリティ対策方針との一貫性主張

本 ST の 3 章セキュリティ課題定義は、PP のセキュリティ課題をすべて定義したうえで、P.STORAGE.ENCRYPTION を追加し、4 章セキュリティ対策方針には、PP のセキュリティ対策方針を全て定義したうえで O.STORAGE.ENCRYPTED を追加している。以下に、追加となったセキュリティ課題とセキュリティ対策方針について PP に適合する根拠を示す。

PP は英語で作成されているが、本 ST の 3 章セキュリティ課題定義、及び 4 章セキュリティ対策方針は、PP を日本語訳して記述している。日本語訳するにあたって、PP の直訳に限らず一部理解しやすい表現にしたが、PP の適合要件を逸脱する表現ではない。

以上のことより、本 ST のセキュリティ課題とセキュリティ対策方針は、PP のセキュリティ課題とセキュリティ対策方針と一貫している。

P.STORAGE.ENCRYPTION と O.STORAGE.ENCRYPTED の追加

P.STORAGE.ENCRYPTION と O.STORAGE.ENCRYPTED は HDD に対するデータの暗号化を行うものであり、PP に含まれる他の組織のセキュリティ方針、TOE のセキュリティ対策方針のいずれをも満たしている。よって、P.STORAGE.ENCRYPTION と O.STORAGE.ENCRYPTED の追加はしているが PP には適合していると言える。

2.4.3 PP のセキュリティ要件との一貫性主張

本 TOE の SAR は PP の内容から追加や削減をしておらず、PP と一貫している。

本 TOE の SFR は、Common Security Functional Requirements と 2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-FAX、2600.2-DSR、2600.2-SMI からなる。Common Security Functional Requirements は、PP が指定する必須 SFR であり、2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-FAX、2600.2-DSR、2600.2-SMI は PP が指定する SFR Package から選択したものである。なお、2600.2-NVS は TOE に着脱可能な不揮発性記憶媒体が存在しないため選択しない。

本 ST のセキュリティ要件は、PP のセキュリティ要件に対して追加、具体化している箇所があるが、PP とは一貫している。以下に、追加、具体化している箇所と、それらが PP と一貫している理由を記載する。

FAU_STG.1、FAU_STG.4、FAU_SAR.1、FAU_SAR.2 の追加

本 TOE が監査ログを保持管理するために PP APPLICATION NOTE 7 に従い FAU_STG.1、FAU_STG.4、FAU_SAR.1、FAU_SAR.2 を追加する。

FIA_AFL.1、FIA_UAU.7、FIA_SOS.1 の追加

本 TOE では識別認証機能を実現するために PP APPLICATION NOTE 38 に従い FIA_AFL.1、FIA_UAU.7、FIA_SOS.1 を追加する。

FCS_CKM.1、FCS_CKM.4、FCS_COP.1 の追加

本 TOE においては、管理者に着脱を許可しない不揮発性記憶媒体に対するデータ保護のセキュリティ対策方針として O.STORAGE.ENCRYPTED を主張し、これを実現するために機能要件 FCS_CKM.1、FCS_CKM.4、及び FCS_COP.1 を追加する。

この追加は PP よりも TOE のふるまいを制限するものであり、他の要求を緩和することなく、この ST を満たすすべての TOE は PP も満たすため、PP に対してより制限的である。よって FCS_CKM.1、FCS_CKM.4、及び FCS_COP.1 を追加しているが PP には適合していると言える。

FMT_MOF.1 の追加

本 TOE は O.PROT.NO_ALT に対する PP における共通セキュリティ要件を満たしたうえで、さらに監査ログの設定に関する管理機能の動作及び停止を MFP 管理者に制限する FMT_MOF.1 を追加する。この追加分は他の要求を緩和することなく、この ST を満たすすべての TOE は PP も満たすため、PP に対してより制限的である。よって、FMT_MOF.1 を追加しているが PP には適合していると言える。

FAU_GEN.1 の一貫性主張

FMT_SMR.1 に関連する監査対象事象について、PP で要求する監査情報には Modifications to the group of users that are part of a role とあるが、本 TOE では「利用者グループの改変機能はないため記録なし」としている。これは本 TOE の利用者役割が別の役割に変更できないためであり、監査対象事象にならないので、PP には適合していると言える。他の監査対象事象について、本 TOE では PP が要求または推奨するよりも多くの監査事象を対象としているが、PP が要求または推奨する監査情報及びレベルは満たしたうえで追加したものであり、PP には適合していると言える。

管理者の分類

本 ST では、U.ADMINISTRATOR を MFP 管理者とスーパーバイザーに分類している。TOE 全体またはその一部を管理することを特別に許可され、そのアクションが TOE セキュリティ方針に影響を与える利用者という PP における U.ADMINISTRATOR の定義に対し、いずれの役割も定義から逸脱しない範囲での管理者の分類のため、PP には適合していると言える。

FDP_ACF.1(a)の一貫性根拠

FDP_ACF.1(a)において本 ST では+CPY の文書データにもアクセス制御規則を記載している。PP の CPY SFR パッケージはアクセス制御を求めていないが、PP APPLICATION NOTE 88 に従い、制限をより厳しくしたアクセス制御規則としたものであり、PP には適合していると言える。

よって、本 ST の FDP_ACF.1(a)は PP の FDP_ACF.1(a)を満たしている。

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 8 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をもつ。

表 8 : 利用者定義

利用者定義			説明
利用者 (U.USER)	一般利用者 (U.NORMAL)		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利用ができる。
	管理者 (U.ADMINISTRATOR)	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 ・ファクス受信文書のアクセス管理 ・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、TSF データ、及び機能である。表 9 に定義を示す。

表 9 : 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。

分類	定義
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。
機能	利用者データを操作するために TOE が提供する印刷(F.PRT)、スキャン(F.SCN)、コピー(F.CPY)、ファクス(F.FAX)、及び文書の保存と取り出し(F.DSR)を実現する MFP アプリケーション。

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 10 にて分類を定義する。

表 10 : 利用者データ定義

分類	定義
文書データ (D.DOC)	TOE の管理下にある紙文書、デジタル化された文書、削除された文書、一時的な文書あるいはその断片。
利用者ジョブデータ (D.FUNC)	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 11 にて分類を定義する。

表 11 : TSF データの分類

分類	定義
TSF 保護データ (D.PROT)	編集権限をもった利用者以外の変更から保護しなければならないが、公開されてもセキュリティ上の脅威とならない情報。
TSF 秘密データ (D.CONF)	編集権限をもった利用者以外の変更から保護し、参照権限をもった利用者以外の読み取りから保護し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 12 : TSF データ定義

分類	TSF データ	内容
TSF 保護データ (D.PROT)	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。
	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。
	利用者役割	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。
	文書データの所有者情報	文書データ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。 電話回線から受信した文書データ(+DSR,ファクス受信文書)の場合は、ログインユーザー名のリストが設定される。
	文書データのアクセス許可利用者のリスト	文書データ(+DSR)のセキュリティ属性。ただし、電話回線から受信した文書データ(ファクス受信文書)は除く。 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。
	利用機能リスト	一般利用者に付与される属性。一般利用者に対して利用を許可された機能のリスト(MFP アプリケーション)が付与される。
	機能種別	MFP アプリケーションの属性で、コピー機能、プリンター機能、スキャナー機能、ファクス機能、及びドキュメントボックス機能がある。
TSF 秘密データ (D.CONF)	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。
	HDD 暗号鍵	HDD 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.DOC.DIS **文書データの開示**

TOE が管理している文書データが権限のない者によって閲覧されるかもしれない。

T.DOC.ALT **文書データの改変**

TOE が管理している文書データが権限のない者によって改変されるかもしれない。

T.FUNC.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権限のない者によって改変されるかもしれない。

T.PROT.ALT **TSF 保護データの改変**

TOE が管理している TSF 保護データが権限のない者によって改変されるかもしれない。

T.CONF.DIS **TSF 秘密データの開示**

TOE が管理している TSF 秘密データが権限のない者によって閲覧されるかもしれない。

T.CONF.ALT **TSF 秘密データの改変**

TOE が管理している TSF 秘密データが権限の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

下記の組織のセキュリティ方針をとる。

P.USER.AUTHORIZATION **利用者の識別認証**

運用上の説明責任とセキュリティを維持するために、利用者には、TOE 所有者が許可した場合だけ TOE を使用する権限を付与する。

P.SOFTWARE.VERIFICATION **ソフトウェア検証**

TSF の実行コードの破損を検出するために、それを自己テストする手続きを実装する。

P.AUDIT.LOGGING　　監査ログ記録管理

運用上の説明責任とセキュリティを維持するために、TOE 使用とセキュリティ関連事象の監査証跡を提供する記録を作成して維持し、不正な開示や改変から保護するとともに、権限を付与された者だけが閲覧できるようにする。

P.INTERFACE.MANAGEMENT　外部インタフェース管理

TOE の外部インタフェースが不正使用されないように、その操作を TOE と IT 環境で制御する。

P.STORAGE.ENCRYPTION 記憶装置暗号化

TOE の HDD 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.ACCESS.MANAGEDアクセス管理

TOE の物理的なコンポーネントとデータインタフェースへの許可されないアクセスから保護される、制限された環境または監視された環境に TOE を設置する。

A.USER.TRAINING　利用者教育

TOE 利用者は、組織のセキュリティ方針と手続きを認識し、当該の方針と手続きに従うよう教育を受け、その能力を習得する。

A.ADMIN.TRAINING 管理者教育

管理者は、組織のセキュリティ方針と手続きを認識し、製造業者のガイダンスと文書に従うよう教育を受けて、その能力を習得し、当該の方針と手続きに従って、TOE を適切に構成・操作できる。

A.ADMIN.TRUST　信頼できる管理者

管理者は付与されたアクセス権を悪用しない。

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.DOC.NO_DIS　文書データの開示保護

TOE は文書データが権限のない者によって開示されることから保護しなければならない。

O.DOC.NO_ALT　文書データの改変保護

TOE は文書データが権限のない者によって改変されることから保護しなければならない。

O.FUNC.NO_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権限のない者によって改変されることから保護しなければならない。

O.PROT.NO_ALT　TSF 保護データの改変保護

TOE は TSF 保護データが権限のない者によって改変されることから保護しなければならない。

O.CONF.NO_DIS　TSF 秘密データの開示保護

TOE は TSF 秘密データが権限のない者によって開示されることから保護しなければならない。

O.CONF.NO_ALT　TSF 秘密データの改変保護

TOE は TSF 秘密データが権限のない者によって改変されることから保護しなければならない。

O.USER.AUTHORIZED　利用者の識別認証

TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証しなければならない。

O.INTERFACE.MANAGED　TOE による外部インタフェース管理

TOE はセキュリティ方針に従い、外部インタフェースの操作を管理しなければならない。

O.SOFTWARE.VERIFIED　ソフトウェア検証

TOE は TSF の実行コードを自己検証する手続きを提供しなければならない。

O.AUDIT.LOGGED　監査ログ記録管理

TOE は TOE の使用とセキュリティに関連する事象を記録して管理し、不正な開示や改変を阻止しなければならない。

O.STORAGE.ENCRYPTED　記憶装置暗号化

TOE は、HDD に書き込むデータを、暗号化してから記録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。

4.2.1　IT 環境

OE.AUDIT_STORAGE.PROTECTED　高信頼 IT 製品での監査ログ保護

監査記録を TOE から別の高信頼 IT 製品にエクスポートする場合、TOE 所有者は不正なアクセス、削除、改変から監査記録が保護されることを保証しなければならない。

OE.AUDIT_ACCESS.AUTHORIZED　高信頼 IT 製品の監査ログアクセス制限

TOE が生成した監査記録を TOE から別の高信頼 IT 製品にエクスポートする場合、TOE 所有者は潜在的なセキュリティ違反を検出して、権限のある者だけが監査記録にアクセスすることを保証しなければならない。

OE.INTERFACE.MANAGED　IT 環境による外部インタフェース管理

IT 環境は TOE 外部インタフェースへの不正アクセスに対する保護を提供しなければならない。

4.2.2　非 IT 環境

OE.PHYSICAL.MANAGED　物理的管理

TOE への許可されない物理的アクセスから保護される安全な場所または監視された場所に TOE を設置しなければならない。

OE.USER.AUTHORIZED　利用者への権限付与

TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与しなければならない。

OE.USER.TRAINED　利用者への教育

TOE 所有者は利用者が組織のセキュリティ方針と手続きを認識し、当該の方針と手続きに従うよう教育を与え、利用者がその能力を習得することを保証しなければならない。

OE.ADMIN.TRAINED 管理者への教育

TOE 所有者は、管理者が組織のセキュリティ方針と手続きを認識し、製造業者のガイダンスと文書に従うよう教育して、その能力を習得する時間を確保することで、管理者が当該の方針と手続きに従って、TOE を適切に構成・操作できることを保証しなければならない。

OE.ADMIN.TRUSTED 信頼できる管理者

TOE 所有者は、管理者が付与されたアクセス特権を悪用しないことの信頼を確立しなければならない。

OE.AUDIT.REVIEWED　　ログの監査

TOE 所有者は、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、監査ログが適切な間隔で閲覧されることを保証しなければならない。

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 13 に示す。

表 13 : セキュリティ対策方針根拠

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	OE.AUDIT_STORAGE.PROTCTED	OE.AUDIT_ACCESS_AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	O.STORAGE.ENCRYPTED	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	X						X	X												
T.DOC.ALT		X					X	X												
T.FUNC.ALT			X				X	X												
T.PROT.ALT				X			X	X												
T.CONF.DIS					X		X	X												
T.CONF.ALT						X	X	X												
P.USER.AUTHORIZATION							X	X												
P.SOFTWARE.VERIFICATION									X											
P.AUDIT.LOGGING										X	X	X	X							
P.INTERFACE.MANAGEMENT														X		X				
P.STORAGE.ENCRYPTION															X					
A.ACCESS.MANAGED																	X			
A.ADMIN.TRAINING																		X		
A.ADMIN.TRUST																			X	
A.USER.TRAINING																				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.DOC.DIS

T.DOC.DIS は、O.DOC.NO_DIS、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。
O.DOC.NO_DIS により TOE は文書データが権限の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.DOC.DIS に対抗できる。

T.DOC.ALT

T.DOC.ALT は、O.DOC.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。
O.DOC.NO_ALT により TOE は文書データが権限の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.DOC.ALT に対抗できる。

T.FUNC.ALT

T.FUNC.ALT は、O.FUNC.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。
O.FUNC.NO_ALT により TOE は利用者ジョブデータが権限の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.FUNC.ALT に対抗できる。

T.PROT.ALT

T.PROT.ALT は、O.PROT.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。
O.PROT.NO_ALT により TOE は TSF 保護データが権限の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.PROT.ALT に対抗できる。

T.CONF.DIS

T.CONF.DIS は、O.CONF.NO_DIS、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。O.CONF.NO_DIS により TOE は TSF 秘密データが権限の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.CONF.DIS に対抗できる。

T.CONF.ALT

T.CONF.ALT は、O.CONF.NO_ALT、O.USER.AUTHORIZED、OE.USER.AUTHORIZED によって対抗できる。

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。O.CONF.NO_ALT により TOE は TSF 秘密データが権限の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.CONF.ALT に対抗できる。

P.USER.AUTHORIZATION

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

OE.USER.AUTHORIZED により、TOE 所有者は組織のセキュリティ方針と手続きに従って TOE を使用する権限を利用者に付与し、O.USER.AUTHORIZED により TOE は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する。

これらの対策方針により、P.USER.AUTHORIZATION を順守できる。

P.SOFTWARE.VERIFICATION

P.SOFTWARE.VERIFICATION は、O.SOFTWARE.VERIFIED によって対抗できる。

O.SOFTWARE.VERIFIED により TOE は TSF の実行コードを自己検証する手続きを提供する。

この対策方針により、P.SOFTWARE.VERIFICATION を順守できる。

P.AUDIT.LOGGING

P.AUDIT.LOGGING は、O.AUDIT.LOGGED、OE.AUDIT.REVIEWED、OE.AUDIT_STORAGE.PROTECTED、OE.AUDIT_ACCESS.AUTHORIZED によって対抗できる。

O.AUDIT.LOGGED により、TOE は TOE の使用とセキュリティに関連する事象を記録して管理し、不正な開示や改変を阻止し、OE.AUDIT.REVIEWED により、TOE 所有者は、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、監査ログが適切な間隔で閲覧されることを保証する。

一方、OE.AUDIT_STORAGE.PROTECTED により、監査記録を TOE から別の高信頼 IT 製品にエクスポートする場合、TOE 所有者は不正なアクセス、削除、改変から監査記録が保護されることを保証し、OE.AUDIT_ACCESS.AUTHORIZED により、TOE が生成した監査記録を TOE から別の高信頼 IT 製品

にエクスポートする場合、TOE 所有者は潜在的なセキュリティ違反を検出して、権限のある者だけが監査記録にアクセスすることを保証する。

これらの対策方針により、P.AUDIT.LOGGING を順守できる。

P.INTERFACE.MANAGEMENT

P.INTERFACE.MANAGEMENT は、O.INTERFACE.MANAGED、OE.INTERFACE.MANAGED によって対抗できる。

O.INTERFACE.MANAGED により、TOE はセキュリティ方針に従い、外部インタフェースの操作を管理する。OE.INTERFACE.MANAGED により、IT 環境は TOE 外部インタフェースへの不正アクセスに対する保護を提供する。

これらの対策方針により、P.INTERFACE.MANAGEMENT を順守できる。

P.STORAGE.ENCRYPTION

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

O.STORAGE.ENCRYPTED により、TOE は HDD に書き込むデータを暗号化し、HDD 上には暗号化された情報が記録されることを保証する。

この対策方針により、P.STORAGE.ENCRYPTION を順守できる。

A.ACCESS.MANAGED

A.ACCESS.MANAGED は、OE.PHYSICAL.MANAGED によって運用する。

OE.PHYSICAL.MANAGED により、TOE への許可されない物理的アクセスから保護される安全な場所または監視された場所に TOE を設置する。

この対策方針により、A.ACCESS.MANAGED を実現できる。

A.ADMIN.TRAINING

A.ADMIN.TRAINING は、OE.ADMIN.TRAINED によって運用する。

OE.ADMIN.TRAINED により TOE 所有者は、管理者が組織のセキュリティ方針と手続きを認識し、製造業者のガイダンスと文書に従うよう教育して、その能力を習得する時間を確保することで、管理者が当該の方針と手続きに従って、TOE を適切に構成・操作できることを保証する。

この対策方針により、A.ADMIN.TRAINING を実現できる。

A.ADMIN.TRUST

A.ADMIN.TRUST は、OE.ADMIN.TRUSTED によって運用する。

OE.ADMIN.TRUSTED により、TOE 所有者は、管理者が付与されたアクセス特権を悪用しないことの信頼を確立する。

この対策方針により、A.ADMIN.TRUST を実現できる。

A.USER.TRAINING

A.USER.TRAINING は、OE.USER.TRAINED によって運用する。

OE.USER.TRAINED により、TOE 所有者は利用者が組織のセキュリティ方針と手続きを認識し、当該の方針と手続きに従うよう教育を与え、利用者がその能力を習得することを保証する。

この対策方針により、A.USER.TRAINING 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 外部インタフェースへの制限された情報転送(FPT_FDI_EXP)

ファミリのふるまい

このファミリは、一方の外部インタフェースからもう一方の外部インタフェースへの情報の直接転送を TSF が制限するための要件を定義する。

多くの製品は固有の外部インタフェースで情報を受信し、この情報を他の外部インタフェースから送信する前に変換、処理することを目的としている。一方で、ある製品が攻撃者に、TOE や、TOE の外部インタフェースに接続された機器のセキュリティを侵害するために、外部インタフェースを悪用する能力を提供するかもしれない。そのため、異なる外部インタフェース間の処理されていないデータの直接転送は、許可された管理者役割によって明示的に許可された場合を除いて禁止される。FPT_FDI_EXP ファミリはこの種の機能性を特定するために定義された。

コンポーネントのレベル付け

FPT_FDI_EXP: 外部インタフェースへの制限された情報転送	1

FPT_FDI_EXP.1 外部インタフェースへの制限された情報転送は、定義された外部インタフェースで受信したデータを、もう一方の外部インタフェースから送信される前に、TSF で制御された処理を行うことを要求する機能性を提供する。一方の外部インタフェースから他方へのデータの直接転送は、許可された管理者役割による明示的な許可を要求する。

管理: FPT_FDI_EXP.1

以下のアクションは FMT における管理機能と考えられる:

a) 管理アクティビティを実行することを許可される役割の定義

b) 管理者役割によって直接転送が許可される条件の管理

c) 許可の取消し

監査: FPT_FDI_EXP.1

FAU_GEN セキュリティ監査データ生成を PP/ST に含めた場合、次のアクションは監査対象となる。

予見される監査対象事象はない。

根拠:

しばしば TOE は、ある外部インタフェースで受信したデータを他のインタフェースから送信するのを許可する前に、特定の検査と処理を行うことが想定される。例はファイアウォールシステムだが、入力データを送信する前に特定のワークフローを要求する他のシステムも同様である。そのような(処理されていない)データの、異なる外部インタフェース間での直接転送は、もし許されるなら、許可された役割によってのみ許可される。

直接転送を禁じ、許可された役割だけが許可できることを要求する特性を指定する単独のコンポーネントとして、この機能性を持つことは有用と見なされる。この機能は多くの製品に共通するため、拡張コンポーネントを定義するのは有用と見なされる。

CC は FDP クラスにおいて属性による利用者データフローを定義している。一方でこの ST では、利用者データと TSF データ共に、属性による制御の代わりに運用管理による制御を表現する必要がある。FDP_IFF と FDP_IFC を詳細化してこの目的に使うことは不適切であると考えられる。従って、この機能性を扱うために拡張コンポーネントを定義することとした。

この拡張コンポーネントは利用者データと TSF データ両方を保護し、そのため、FDP あるいは FPT クラスのいずれかに含まれる。この目的が TOE を悪用から保護することであるため、FPT クラスに含めるのが最適であると考えられる。いずれのクラスでも、既存のファミリにはうまく適合しないため、メンバが一つのみの新たなファミリを定義した。

FPT_FDI_EXP.1　外部インタフェースへの制限された情報転送

下位階層:　なし

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

FPT_FDI_EXP.1.1　TSF は、**[割付：外部インタフェースのリスト]**で受け取った情報を、TSF による追加の処理無しに**[割付：外部インタフェースのリスト]**に転送することを制限する能力を提供しなければならない。

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以下に定義する。

表 14 : 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 (D.DOC)	TOE の管理下にある紙文書、デジタル化された文書、削除された文書、一時的な文書あるいはその断片。
	利用者ジョブデータ (D.FUNC)	利用者の文書または文書処理ジョブに関連する情報。
	MFP アプリケーション	PP の SFR パッケージ機能(F.CPY、F.PRT、F.SCN、F.FAX、F.DSR)を実現するコピー機能、プリンター機能、スキャナー機能、ファクス機能、ドキュメントボックス機能の総称。
	F.CPY	コピー: 紙文書(入力)を紙文書(出力)に複製する機能。
	F.PRT	印刷: 電子文書(入力)を紙文書(出力)に変換する機能。
	F.SCN	スキャン: 紙文書(入力)を電子文書(出力)に変換する機能。
	F.FAX	ファクス: 電話回線を介して紙文書(入力)をファクス送信する機能、紙文書(入力)を電話回線経由のファクス送信に変換する機能、及び電話回線を介し受信したファクス文書を紙文書(出力)に変換する機能。
	F.DSR	文書の保存と取り出し: ジョブの実行中に文書を保存し、後続の 1 つ以上のジョブでそれを取り出す機能。

用語の分類	用語の名称	用語の内容
操作	読み取り	印刷、ダウンロード、ファクス送信、文書添付メール送信、フォルダー送信、プレビュー、またはファクス受信のこと。
	削除	TSF データ、またはオブジェクトを削除すること。
	変更	TSF データ、またはオブジェクトを変更すること。
	問い合わせ	TSF データを参照すること。
	新規作成	TSF データを新規に作成すること。
	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。
	実行	MFP アプリケーションのジョブ実行をすること。
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。
	利用者役割	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。
	文書情報属性	PP の SFR パッケージ機能を識別するセキュリティ属性。文書データ(D.DOC)、及び利用者ジョブデータ(D.FUNC)に関連付けられる。 +PRT、+SCN、+CPY、+FAXOUT、+FAXIN、及び+DSR がある。 TOE の実装では使用していないセキュリティ属性である。
	+PRT	文書情報属性のひとつ。印刷ジョブに関連付けられたデータを指す。
	+SCN	文書情報属性のひとつ。スキャンジョブに関連付けられたデータを指す。
	+CPY	文書情報属性のひとつ。コピージョブに関連付けられたデータを指す。
	+FAXOUT	文書情報属性のひとつ。アウトバウンド（送信）ファクスジョブに関連付けられたデータを指す。
	+FAXIN	文書情報属性のひとつ。インバウンド（受信）ファクスジョブに関連付けられたデータを指す。
	+DSR	文書情報属性のひとつ。文書保存・取り出しジョブに関連付けられたデータを指す。

用語の分類	用語の名称	用語の内容
	文書データの所有者情報	文書データ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。 電話回線から受信した文書データ(+DSR,ファクス受信文書)の場合は、ログインユーザー名のリストが設定される。
	文書データのアクセス許可利用者のリスト	文書データ(+DSR)のセキュリティ属性。ただし、電話回線から受信した文書データ(ファクス受信文書)は除く。 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。
	利用機能リスト	一般利用者に付与される属性。一般利用者に対して、利用を許可された機能のリスト(MFP アプリケーション)が付与される。
	機能種別	MFP アプリケーションの属性で、コピー機能、プリンター機能、スキャナー機能、ファクス機能、及びドキュメントボックス機能がある。
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利用ができる。
	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 ・ファクス受信文書のアクセス管理 ・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
その他の用語	MFP 制御ソフトウェア	TOE に組込むソフトウェアの 1 つ。FlashROM に格納されている。

用語の分類	用語の名称	用語の内容
	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。操作パネルの操作パネル制御ボードに格納されている。

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。なお、セキュリティ機能要件は、CC パート 2 に規定のセキュリティ機能要件から、引用する。CC パート 2 に規定されていないセキュリティ機能要件は、PP に規定の拡張セキュリティ機能要件について SMI SFR Package にて定義されている通りに引用する。

また、[CC]で定義された割付と選択操作を行った部分は、**[太文字と括弧]**で識別する。

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: 指定なし]**レベルのすべての監査対象事象;及び
c) **[割付: 表 15 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: FDP_ACF.1(a)におけるジョブタイプ、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、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]**。

表 15：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
・文書データの作成の開始と終了 ・文書データの印刷の開始と終了 ・文書データのダウンロードの開始と終了 ・文書データのファクス送信の開始と終了 ・文書データの文書添付メール送信の開始と終了 ・文書データのフォルダー送信の開始と終了 ・文書データの削除の開始と終了 ・利用者ジョブデータの削除 上記における「文書データの作成・印刷・ダウンロード・ファクス送信・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」が、ジョブタイプに相当する。	FDP_ACF.1(a)
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
ログイン操作の成功と失敗。これには、PP において求められる追加情報である利用者識別をも含む。	FIA_UID.1
表 31 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
利用者グループの改変機能はないため記録なし	FMT_SMR.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]**できねばならない。

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: 最も古くに格納された監査記録への上書き]** 及び**[割付: 監査格納失敗時にとられるその他のアクションはない]**を行わなければならない。

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: MFP 管理者]**が、**[割付: すべてのログ項目]**を監査記録から読み出せるようにしなければならない。

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: なし]**に合致する、指定された暗号鍵生成アルゴリズム**[割付: AES-128 を利用した乱数生成]**と指定された暗号鍵長**[割付: 256 ビット]**に従って、暗号鍵を生成しなければならない。

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:なし]**に合致する、指定された暗号鍵破棄方法**[割付: 0 で上書きする]**に従って、暗号鍵を破棄しなければならない。

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: FIPS197]**に合致する、特定された暗号アルゴリズム**[割付: AES]**と暗号鍵長**[割付: 256 ビット]**に従って、**[割付: HDD に書き込むデータの暗号化、HDD から読み込むデータの復号]**を実行しなければならない。

6.1.3 クラス FDP: 利用者データ保護

6.1.3.1. FDP_ACC.1(a) 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(a) TSF は、**[割付: 表 16 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]**に対して**[割付: 利用者データアクセス制御 SFP]**を実施しなければならない。

表 16: 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(a)

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	文書データ(D.DOC)	読み取り(Read) 削除(Delete)
	利用者ジョブデータ(D.FUNC)	変更(Modify) 削除(Delete)

6.1.3.2. FDP_ACC.1(b) 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(b) TSF は、**[割付: 表 17 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]**に対して**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

表 17: 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(b)

サブジェクト	・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
オブジェクト	・MFP アプリケーション
操作	・実行

6.1.3.3. FDP_ACF.1(a) 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(a) TSF は、以下の**[割付: 表 18 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]**に基づいて、オブジェクトに対して、**[割付: 利用者データアクセス制御 SFP]**を実施しなければならない。

表 18 : サブジェクトとオブジェクトとセキュリティ属性(a)

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 ・利用者役割
サブジェクト	MFP 管理者プロセス	・ログインユーザー名 ・利用者役割
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 ・利用者役割
オブジェクト	文書データ(D.DOC)	・文書情報属性 ・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(D.FUNC)	・文書情報属性 ・利用者ジョブデータの所有者情報

FDP_ACF.1.2(a) 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: 表 19 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 19：文書データと利用者ジョブデータの操作を制御する規則(a)

オブジェクト	文書情報属性	操作	サブジェクト	操作を制御する規則
文書データ (D.DOC)	+PRT +SCN +FAXOUT +CPY	削除(Delete)	一般利用者プロセス	利用者自身の文書データ以外は拒否する。
文書データ (D.DOC)	+PRT	読み取り(Read)	一般利用者プロセス	利用者自身の文書データ以外は拒否する。
文書データ (D.DOC)	+SCN +FAXOUT +CPY	読み取り(Read)	一般利用者プロセス	利用者自身の文書データ以外は拒否する。(*1)
文書データ (D.DOC)	+FAXIN	削除(Delete) 読み取り(Read)	一般利用者プロセス	許可しない。(*1)
文書データ (D.DOC)	+DSR	削除(Delete)	一般利用者プロセス	利用者自身の文書データ以外は拒否する。
文書データ (D.DOC)	+DSR	読み取り(Read)	一般利用者プロセス	利用者自身の文書データ以外は拒否する。 なお、文書データの所有者が他者に読み取り操作を許可した場合は、許可利用者は読み取り操作が可能となる。
利用者ジョブデータ (D.FUNC)	+PRT +SCN +FAXOUT +CPY +DSR	削除(Delete)	一般利用者プロセス	利用者自身の利用者ジョブデータ以外は拒否する。
利用者ジョブデータ (D.FUNC)	+FAXIN	削除(Delete)	一般利用者プロセス	許可しない。(*1)
利用者ジョブデータ (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	変更(Modify)	一般利用者プロセス	許可しない。(*1)

(*1) インタフェースを提供しない。

FDP_ACF.1.3(a) TSF は、次の追加規則、**[割付：表 20 に示すオブジェクトとサブジェクト間の操作を許可する規則]**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。

表 20：文書データと利用者ジョブデータの操作を許可する規則(a)

オブジェクト	文書情報属性	操作	サブジェクト	操作を許可する規則
文書データ (D.DOC)	+PRT +SCN +FAXOUT +CPY	削除(Delete)	MFP 管理者プロセス	許可する。
文書データ (D.DOC)	+DSR	削除(Delete) 読み取り(Read)	MFP 管理者プロセス	許可する。
文書データ (D.DOC)	+FAXIN	読み取り(Read)	MFP 管理者プロセス	許可する。
利用者ジョブデータ (D.FUNC)	+PRT +SCN +FAXOUT +CPY +DSR	削除(Delete)	MFP 管理者プロセス	許可する。

FDP_ACF.1.4(a) TSF は、次の追加規則、**[割付：表 21 に示すオブジェクトとサブジェクト間の操作を拒否する規則]**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。

表 21：文書データと利用者ジョブデータの操作を拒否する規則(a)

オブジェクト	文書情報属性	操作	サブジェクト	操作を拒否する規則
文書データ (D.DOC)	+FAXIN	削除(Delete)	MFP 管理者プロセス	許可しない。(*1)
文書データ (D.DOC)	+PRT +SCN +FAXOUT +CPY	読み取り(Read)	MFP 管理者プロセス	許可しない。(*1)
文書データ (D.DOC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	削除(Delete) 読み取り(Read)	スーパーバイザープロセス	許可しない。(*1)
利用者ジョブデータ (D.FUNC)	+FAXIN	削除(Delete)	MFP 管理者プロセス	許可しない。(*1)

オブジェクト	文書情報属性	操作	サブジェクト	操作を拒否する規則
利用者ジョブデータ (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	変更(Modify)	MFP 管理者プロセス	許可しない。(*1)
利用者ジョブデータ (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	削除(Delete) 変更(Modify)	スーパーバイザープロセス	許可しない。(*1)

(*1) インタフェースを提供しない。

6.1.3.4. FDP_ACF.1(b) 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(b) TSF は、以下の**[割付: 表 22 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]**に基づいて、オブジェクトに対して、**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

表 22 : サブジェクトとオブジェクトとセキュリティ属性(b)

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 利用機能リスト 利用者役割
サブジェクト	MFP 管理者プロセス	ログインユーザー名 利用者役割
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 利用者役割
オブジェクト	MFP アプリケーション	機能種別

FDP_ACF.1.2(b) 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: 表 23 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 23 : MFP アプリケーションの操作を制御する規則(b)

オブジェクト	操作	サブジェクト	操作を制御する規則
MFP アプリケーション (F.CPY 、 F.PRT 、 F.SCN 、 F.FAX 、 F.DSR)	実行	一般利用者プロセス	一般利用者プロセスの利用機能リストで許可した MFP アプリケーションと一致する機能種別の MFP アプリケーションの実行を許可する。

FDP_ACF.1.3(b) TSF は、次の追加規則、**[割付: MFP 管理者プロセスの利用者役割が MFP 管理者の場合、MFP アプリケーションの実行を許可する]**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。

FDP_ACF.1.4(b) TSF は、次の追加規則、**[割付: スーパーバイザープロセスの利用者役割がスーパーバイザーの場合、MFP アプリケーションの実行を拒否する]**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。

6.1.3.5. FDP_RIP.1サブセット情報保護

下位階層: なし

依存性: なし

FDP_RIP.1.1 TSF は、**[割付: 文書データ]**のオブジェクト**[選択: からの資源の割当て解除]**において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

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: 表 24 に示す認証事象]**に関して、**[選択: [割付: 1～5]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。

表 24 : 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
ファクスドライバーから文書データを受信し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: 表 25 に示すアクション]**をしなければならない。

表 25：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：ログインユーザー名、利用機能リスト、利用者役割]**

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：以下の品質尺度]**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。

(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：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]**を許可しなければならない。

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: 認証フィードバックとして表示するダミー文字]**だけを利用者に提供しなければならない。

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: 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]**を許可しなければならない。

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: ログインユーザー名、利用機能リスト、利用者役割]**

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に関する規則はない]**

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: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: syslog 転送機能**][**選択: を停止する、を動作させる**]能力を[**割付: MFP 管理者**]に制限しなければならない。

6.1.5.2. FMT_MSA.1(a) 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(a)TSF は、セキュリティ属性**[割付：表 26 のセキュリティ属性]**に対し**[選択：削除、デフォルト値変更、[割付：新規作成、変更]]**をする能力を**[割付：表 26 の操作を許可する利用者役割]**に制限する**[割付：利用者データアクセス制御 SFP]**を実施しなければならない。

表 26：セキュリティ属性の利用者役割(a)

セキュリティ属性	操作	操作を許可する利用者役割
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
利用者役割	変更	操作を許可する役割なし
文書データの所有者情報 [+PRT 、 +SCN 、 +FAXOUT 、 +FAXIN、+CPY]	変更	操作を許可する役割なし
文書データの所有者情報 [+DSR:電話回線から受信した文書データ以外]	変更	操作を許可する役割なし
文書データの所有者情報 [+DSR:電話回線から受信した文書データ]	変更	MFP 管理者
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)
	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.1(b) 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(b)TSF は、セキュリティ属性**[割付：表 27 のセキュリティ属性]**に対し**[選択：削除、[割付：新規作成、変更]]**をする能力を**[割付：表 27 の操作を許可する利用者役割]**に制限する TOE 機能アクセス制御 SFP**[割付：TOE 機能アクセス制御 SFP]**を実施しなければならない。

表 27：セキュリティ属性の利用者役割(b)

セキュリティ属性	操作	操作を許可する利用者役割
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
利用者役割	変更	操作を許可する役割なし
利用機能リスト	新規作成 変更 削除	MFP 管理者
機能種別	変更	操作を許可する役割なし

6.1.5.4. FMT_MSA.3(a) 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(a) TSF は、その SFP 実施に使用するセキュリティ属性に対して、**[選択：制限的]**のデフォルト値を与える**[割付：利用者データアクセス制御 SFP]**を実施しなければならない。

FMT_MSA.3.2(a) TSF は、オブジェクトまたは情報が生成されるとき、**[割付：表 28 に記す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。

表 28：デフォルト値を上書きできる許可された識別された役割

オブジェクト	セキュリティ属性	許可された識別された役割
文書データ (D.DOC)	文書データの所有者情報	許可された識別された役割はなし
文書データ (D.DOC)	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一般利用者 (操作パネルからの文書データの蓄積時にのみ許可される。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。)
利用者ジョブデータ (D.FUNC)	利用者ジョブデータの所有者情報	許可された識別された役割はなし

6.1.5.5. FMT_MSA.3(b) 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(b)TSF は、その SFP 実施に使用するセキュリティ属性に対して、**[選択: 制限的]**のデフォルト値を与える**[割付: TOE 機能アクセス制御 SFP]**を実施しなければならない。

FMT_MSA.3.2(b)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はなし]**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。

6.1.5.6. 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: 表 29 の TSF データのリスト]**を**[選択: 問い合わせ、削除、[割付: 新規作成、変更]]**する能力を**[割付: 表 29 の利用者役割]**に制限しなければならない。

表 29 : TSF データのリスト

分類	TSF データ	操作	利用者役割
TSF 保護データ (D.PROT)	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 (D.CONF)	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
		変更	当該一般利用者 MFP 管理者
	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
		変更	当該 MFP 管理者 スーパーバイザー
	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

分類	TSF データ	操作	利用者役割
	HDD 暗号鍵	問い合わせ 削除 新規作成	MFP 管理者

6.1.5.7. 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: 表 30 の TSF データのリスト]**を**[選択: 問い合わせ]**する能力を**[割付: 表 30 の利用者役割]**に制限しなければならない。

表 30 : TSF データのリスト

分類	TSF データ	操作	利用者役割
TSF 秘密データ (D.CONF)	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

6.1.5.8. 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: 表 31 に記す管理機能]**

表 31 : 管理機能の特定のリスト

管理機能
syslog 転送機能の停止と動作
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
ログインパスワードの新規作成と変更
ログインユーザー名の新規作成、変更、及び削除
文書データ(+DSR:電話回線から受信した文書データ)の所有者情報の変更

管理機能
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
利用機能リストの新規作成、変更、及び削除
HDD 暗号鍵の問い合わせ、削除、新規作成

6.1.5.9. 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: 一般利用者、MFP 管理者、スーパーバイザー]**を維持しなければならない。

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.1 TSF テスト

下位階層: なし

依存性: なし

FPT_TST.1.1 TSF は、**[選択: [割付: MFP 制御ソフトウェア、操作パネル制御ソフトウェア]]**の正常動作を実証するために、**[選択: 初期立上げ中]**自己テストのスイートを実行しなければならない。

FPT_TST.1.2 TSF は、認可利用者に、**[選択: [割付: HDD 暗号鍵]]**の完全性を検証する能力を提供しなければならない。

FPT_TST.1.3 TSF は、認可利用者に、**[選択: [割付: 保存されている TSF 実行コード]]**の完全性を検証する能力を提供しなければならない。

6.1.6.3. FPT_FDI_EXP.1 外部インタフェースへの制限された情報転送

下位階層: なし

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

FPT_FDI_EXP.1.1 TSF は、**任意の外部インタフェース**で受け取った情報を、TSF による追加の処理無しに**任意の共有メディアインタフェース**に転送することを制限する能力を提供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: MFP 管理者の指定した時間]**後に対話セションを終了しなければならない。

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情報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。

FTP_ITC.1.3 TSF は、**[割付: 文書データ、利用者ジョブデータ、TSF 保護データ、及び TSF 秘密データの LAN 経由通信]**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。

6.2 セキュリティ保証要件

本 TOE の評価保証レベルは EAL2+ALC_FLR.2 である。TOE の保証コンポーネントを表 32 に示す。これは評価保証レベルの EAL2 によって定義されたコンポーネントのセットに ALC_FLR.2 を追加したものである。

表 32 : TOE セキュリティ保証要件(EAL2+ALC_FLR.2)

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
	ALC_FLR.2	欠陥報告手続き
	ASE_CCL.1	適合主張

保証クラス	保証コンポーネント	
ASE: セキュリティターゲット評価	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 33 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 33 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 33 : セキュリティ対策方針と機能要件の対応

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.STORAGE.ENCRYPTED
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_STG.1						**P**				**P**	

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.STORAGE.ENCRYPTED
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(a)	**P**	**P**	**P**								
FDP_ACC.1(b)							**P**				
FDP_ACF.1(a)	**P**	**P**	**P**								
FDP_ACF.1(b)							**P**				
FDP_RIP.1	**P**										
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	
FIA_USB.1							**P**				
FPT_FDI_EXP.1								**P**			
FMT_MOF.1				**P**							
FMT_MSA.1(a)	S	S	S	**P**							
FMT_MSA.1(b)				**P**			S				
FMT_MSA.3(a)	S	S	S								
FMT_MSA.3(b)							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	

	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.STORAGE.ENCRYPTED
FPT_TST.1									**P**		
FTA_SSL.3							**P**	**P**			
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

6.3.2 追跡性の正当化

以下に、TOE セキュリティ対策方針が、対応付けられた TOE セキュリティ機能要件によって実現できることを説明する。**太字**で記載した SFR の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 SFR の項目は、その実現を支援(S)する。

O.DOC.NO_DIS　　文書の開示保護

O.DOC.NO_DIS は、文書データが権限の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(a)

FDP_ACC.1(a)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する。

(2) FDP_ACF.1(a)

FDP_ACF.1(a)によって、文書データに対して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。

(3) FDP_RIP.1

FDP_RIP.1 によって、削除された文書、一時的な文書あるいはその断片の読み取りを防ぐ。

(4) 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。

(5) FMT_MSA.1(a)

FMT_MSA.1(a)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。

(6) FMT_MSA.3(a)

FMT_MSA.3(a)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。

(7) FIA_UID.1

FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

(8) 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。

(9) 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。

これらのセキュリティ機能要件を達成することで O.DOC.NO_DIS を実現できる。

O.DOC.NO_ALT 文書の改変保護

O.DOC.NO_ALT は、文書データが権限の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、以下の SFR を実施する必要がある。

(1) FDP_ACC.1(a)
FDP_ACC.1(a)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する。

(2) FDP_ACF.1(a)
FDP_ACF.1(a)によって、文書データに対して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。

(3) 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。

(4) FMT_MSA.1(a)
FMT_MSA.1(a)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。

(5) FMT_MSA.3(a)
FMT_MSA.3(a)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。

(6) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

(7) 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。

(8) 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。

これらのセキュリティ機能要件を達成することで O.DOC.NO_ALT を実現できる。

O.FUNC.NO_ALT 利用者ジョブデータの改変保護

O.FUNC.NO_ALT は、利用者ジョブデータが権限の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、以下の SFR を実施する必要がある。

(1) FDP_ACC.1(a)
FDP_ACC.1(a)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する。

(2) FDP_ACF.1(a)
FDP_ACF.1(a)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に従ったアクセス制御機能を提供する。

(3) 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。

(4) FMT_MSA.1(a)
FMT_MSA.1(a)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。

(5) FMT_MSA.3(a)

FMT_MSA.3(a)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。

(6) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

(7) 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。

(8) 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。

これらのセキュリティ機能要件を達成することで O.FUNC.NO_ALT を実現できる。

O.PROT.NO_ALT　　TSF 保護データの改変保護

O.PROT.NO_ALT は、TSF 保護データが権限の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、以下の SFR を実施する必要がある。

(1) 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ふるまいの管理を行うことができる。

(2) FMT_MSA.1(a)、FMT_MSA.1(b)
FMT_MSA.1(a)と FMT_MSA.1(b)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。

(3) 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。

(4) 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。

(5) 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。

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

(7) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

これらのセキュリティ機能要件を達成することで O.PROT.NO_ALT を実現できる。

O.CONF.NO_DIS　　TSF 秘密データの開示保護

O.CONF.NO_DIS は、TSF 秘密データが権限の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) 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。

(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。

(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。

(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。

(5) FAU_SAR.1
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する。

(6) FAU_SAR.2
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。

(7) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

これらのセキュリティ機能要件を達成することで O.CONF.NO_DIS を実現できる。

O.CONF.NO_ALT　　TSF 秘密データの改変保護

O.CONF.NO_ALT は、TSF 秘密データが権限の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、以下の 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。

(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。

(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。

(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。

(5) FAU_STG.1
FAU_STG.1 によって監査ログを改変から保護する。

(6) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

これらのセキュリティ機能要件を達成することで O.CONF.NO_ALT を実現できる。

O.USER.AUTHORIZED　　利用者の識別認証

O.USER.AUTHORIZED は、TOE が利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可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、以下の 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、TOE を利用しようとする者に対して、識別認証が行われる。

(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。

(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。

(4) FDP_ACC.1(b)

FDP_ACC.1(b)によって、識別認証に成功した利用者に与えられた MFP アプリケーションの利用権限と利用者役割に従って、利用者に MFP アプリケーションの実行を許可するアクセス制御方針を規定する。

(5) FDP_ACF.1(b)
FDP_ACF.1(b)によって、識別認証に成功した利用者に与えられた MFP アプリケーションの利用権限と利用者役割に従って、利用者に MFP アプリケーションの実行を許可する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。

(6) 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。

(7) 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。

(8) 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。

(9) 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、非アクティブなままのセションを終了して認可を強要する。

(10) FMT_MSA.1(b)
FMT_MSA.1(b)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。

(11) FMT_MSA.3(b)
FMT_MSA.3(b)によって、セキュリティ属性には制限的な値をセットする。

これらのセキュリティ機能要件を達成することで O.USER.AUTHORIZED を実現できる。

O.INTERFACE.MANAGED　　TOE による外部インタフェース管理

O.INTERFACE.MANAGED は、TOE はセキュリティ方針に従い、外部インタフェースの操作を管理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) FIA_UID.1、FIA_UAU.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行い、FIA_UAU.1 によって、識別された利用者の認証を行う。

(2) 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、非アクティブなままのセションを終了し、外部インタフェースの管理を実施する。

(3) FPT_FDI_EXP.1
FPT_FDI_EXP.1 によって、任意の外部インタフェースで受け取ったデータを、TSF による追加の処理無しに任意の共有メディアインタフェースに転送することを防止する。

これらのセキュリティ機能要件を達成することで O.INTERFACE.MANAGED を実現できる。

O.SOFTWARE.VERIFIED　ソフトウェア検証

O.SOFTWARE.VERIFIED は、TOE が TSF の実行コードを自己検証する手続き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、以下の SFR を実施する必要がある。

(1) FPT_TST.1
FPT_TST.1 によって、起動時に HDD 暗号鍵と TSF 実行コードの検証を行い、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自己テストを行う。

このセキュリティ機能要件を達成することで O.SOFTWARE.VERIFIED を実現できる。

O.AUDIT.LOGGED　監査ログ記録管理

O.AUDIT.LOGGED は、TOE は TOE の使用とセキュリティに関連する事象を記録して管理し、不正な開示や改変を阻止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) 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。

(2) FAU_STG.1
FAU_STG.1 によって監査ログを改変から保護する。

(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上書きする。

(4) FAU_SAR.1

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する。

(5) FAU_SAR.2
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。

(6) 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する。

(7) FIA_UID.1
FIA_UID.1 によって、TOE を利用しようとする者の識別を行う。

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

O.STORAGE.ENCRYPTED　記憶装置暗号化

O.STORAGE.ENCRYPTED は HDD 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。

(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。

(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、HDD に書き込むデータを暗号化し、HDD から読み出されるデータを復号する。

これらのセキュリティ機能要件を実施することで O.STORAGE.ENCRYPTED 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 34 に示す。

表 34 : 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(a)	FDP_ACF.1	FDP_ACF.1(a)	OK
FDP_ACC.1(b)	FDP_ACF.1	FDP_ACF.1(b)	OK
FDP_ACF.1(a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(a) FMT_MSA.3(a)	OK ただし、文書情報属性は実装で使用していないため、FMT_MSA.3(a)にはこのセキュリティ属性は不要である。
FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(b) FMT_MSA.3(b)	OK
FDP_RIP.1	なし	なし	OK
FIA_AFL.1	FIA_UAU.1	FIA_UAU.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
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
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	OK
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK
FMT_MSA.1(a)	[FDP_ACC.1 または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1	OK ただし、利用者役割の変更、文書データの所有者情報(+PRT、+SCN 、+FAXOUT 、+FAXIN 、+CPY)の変更、文書データの所有者情報(+DSR:電話回線から受信した文書データ以外)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.1(b)	[FDP_ACC.1 または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1	OK ただし、利用者役割の変更、機能種別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(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1	OK
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b) 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

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
FPT_STM.1	なし	なし	OK
FPT_TST.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。

また、TOE を継続してセキュアに運用するため、運用開始後に発見された欠陥を欠陥報告手続き(ALC_FLR.2)によって適切に修正することは重要である。

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+ALC_FLR.2 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

TOE は、表 35 に示す監査事象発生時に、表 36 に示す監査ログ項目を TOE 内の HDD 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 36 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、ファクスドライバーから受信した文書データの蓄積、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 35：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 31 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や蓄積の失敗
ファクスドライバーから受信した文書データの蓄積の失敗
syslog 転送の失敗
利用者ジョブデータの削除
文書データの作成(蓄積)

監査事象
文書データの読み取り(印刷、ダウンロード、ファクス送信、文書添付メール送信、フォルダー送信)
文書データの削除

表 36 : 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 35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	文書データの作成・印刷・ダウンロード・ファクス送信・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)	・文書データの作成の開始と終了 ・文書データの印刷の開始と終了 ・文書データのダウンロードの開始と終了 ・文書データのファクス送信の開始と終了 ・文書データの文書添付メール送信の開始と終了 ・文書データのフォルダー送信の開始と終了 ・文書データの削除 ・利用者ジョブデータの削除 上記における「文書データの作成・印刷・ダウンロード・ファクス送信・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」が、ジョブタイプに相当する。
	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や蓄積の失敗 ・ファクスドライバーから受信した文書データの蓄積の失敗 ・syslog 転送の失敗

	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
		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
	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や蓄積の失敗
・ファクスドライバーから受信した文書データの蓄積の失敗
・syslog 転送の失敗
・文書添付メール送信の失敗

FAU_GEN.2

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

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、FAU_SAR.2

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 で監査ログのダウンロードが可能である。MFP 管理者以外のすべての利用者には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

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

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

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、及びファクス受信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

TOE は、FIA_UAU.1、及び FIA_UID.1 の照合の結果、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、利用者役割、及び利用機能リストを割り当てる。

FIA_ATD.1

TOE は、ログインユーザー名、利用者役割、及び利用機能リスト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

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、最後の操作から経過した時間が、操作パネルオートログアウト時間(10～999 秒)に達した時、ログアウトする。
・WIM の場合、最後の操作から経過した時間が、WIM オートログアウト時間(3～60 分)に達した時、ログアウトする。
なお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

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

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、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 37 に示すロックアウト対象者は利用者役割毎に定められた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 OFF/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 37：利用者役割毎のロックアウト解除者

利用者役割(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

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、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

FPT_FDI_EXP.1

操作パネルあるいは LAN インタフェースを介したクライアント PC からの入力情報は、必ず TSF による識別認証を行った後、情報入力のアクションを行うため、TSF の関与なしに入力情報が転送されることはない。

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て、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(a)、FDP_ACF.1(a)

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 38 に文書データのアクセス制御規則を示す。TOE は、文書データの削除または読み取りの操作を一般利用者、MFP 管理者、スーパーバイザーに対し制限する。

表 39 に文書データに対する一般利用者の操作を示し、表 40 に文書データに対する MFP 管理者の操作を示す。表 39 及び表 40 以外の操作は、インタフェースを提供しない。

表 38：文書データのアクセス制御規則

利用者役割	文書データ	アクセス制御規則
一般利用者	文書データ (+PRT)	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同一のログインユーザー名を持つ一般利用者に読み取りと削除の操作を許可する。 読み取りに関しては、それ以外の一般利用者には、文書データを表示せず、読み取りの操作は許可しない。 削除に関しては、それ以外の一般利用者には、一時的な文書データに関連するジョブの表示を許可するが、削除の操作は許可しない。
	文書データ (+CPY、+SCN、+FAXOUT)	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同一のログインユーザー名を持つ一般利用者に読み取りと削除の操作を許可する。 読み取りに関しては、それ以外の一般利用者には、読み取りのインタフェースを提供しない。 削除に関しては、それ以外の一般利用者には、一時的な文書データに関連するジョブの表示を許可するが、削除の操作は許可しない。

利用者役割	文書データ	アクセス制御規則
	文書データ (+FAXIN)	ファクス受信データを操作するインタフェースは提供しない。
	文書データ (+DSR) (保存印刷文書、ドキュメントボックス文書、スキャナー文書、ファクス送信文書)	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同一のログインユーザー名を持つ一般利用者に読み取りと削除の操作を許可する。 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の操作を許可する。 それ以外の一般利用者には、文書データを表示せず読み取りと削除の操作を許可しない。
	文書データ (+DSR) (ファクス受信文書)	文書データの所有者情報(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と同一のログインユーザー名を持つ一般利用者に読み取りと削除の操作を許可する。 それ以外の一般利用者には、文書データを表示せず読み取りと削除の操作を許可しない。
MFP 管理者	文書データ (+PRT、+CPY、+SCN、+FAXOUT)	文書データの削除の操作を許可する。
	文書データ (+FAXIN)	ファクス受信(受信ファクスジョブ)は、MFP 管理者による受信とみなし、読み取りの操作を許可する。 ファクス受信データを削除するインタフェースは提供しない。
	文書データ (+DSR) (保存印刷文書)	文書データの削除の操作を許可する。
	文書データ(+DSR) (ドキュメントボックス文書、スキャナー文書、ファクス送信文書)	文書データの読み取りと削除の操作を許可する。
	文書データ(+DSR) (ファクス受信文書)	文書データを操作するインタフェースは提供しない。
スーパーバイザー	文書データ	文書データを操作するインタフェースは提供しない。

表 39：文書データに対する一般利用者の操作

No.	TOE の機能 (TOE の文書名)	操作経路	操作	PP の SFR パッケージ機能
1	コピー機能	操作パネル	削除(*1) 複写印刷	F.CPY (+CPY)
2	スキャナー機能	操作パネル	削除(*1) 文書添付メール送信 フォルダー送信 プレビュー	F.SCN (+SCN)
3	スキャナー機能 (スキャナー文書)	操作パネル	削除 文書添付メール送信 フォルダー送信 プレビュー	F.DSR (+DSR)
4	ファクス機能	操作パネル	削除(*1) ファクス送信 プレビュー	F.FAX (+FAXOUT)
5	ファクス機能 (ファクス送信文書)	操作パネル	削除 ファクス送信 プレビュー	F.DSR (+DSR)
6	ファクス機能 (ファクス受信文書)	操作パネル	削除 印刷 プレビュー	F.DSR (+DSR) F.PRT (+PRT)
7	ファクス機能 (ファクス受信文書)	WIM	削除 ダウンロード プレビュー	F.DSR (+DSR)
8	プリンター機能 (一時保存文書)	操作パネル	削除(*1) 印刷 プレビュー	F.PRT (+PRT)

No.	TOE の機能 (TOE の文書名)	操作経路	操作	PP の SFR パッケージ機能
9	プリンター機能 (一時保存文書)	WIM	削除(*1)	F.PRT (+PRT)
10	プリンター機能 (保存印刷文書)	操作パネル	削除 印刷 プレビュー	F.DSR (+DSR) F.PRT (+PRT)
11	プリンター機能 (保存印刷文書)	WIM	削除	F.DSR (+DSR)
12	ドキュメントボックス機能 (ファクス送信文書、ドキュメントボックス文書)	操作パネル	削除 印刷 プレビュー	F.DSR (+DSR) F.PRT (+PRT)
13	ドキュメントボックス機能 (スキャナー文書)	WIM	削除 文書添付メール送信 フォルダー送信 ダウンロード プレビュー	F.DSR (+DSR)
14	ドキュメントボックス機能 (ファクス送信文書)	WIM	削除 ファクス送信 ダウンロード プレビュー	F.DSR (+DSR)
15	ドキュメントボックス機能 (ドキュメントボックス文書)	WIM	削除 プレビュー	F.DSR (+DSR)

(*1) ジョブをキャンセルすることにより、利用者ジョブデータが扱っていた一時的な文書データが削除される。

表 40： 文書データに対する MFP 管理者の操作

No.	TOE の機能 (TOE の文書)	操作経路	操作	PP の SFR パッケージ機能
1	コピー機能	操作パネル	削除(*1)	F.CPY (+CPY)
2	スキャナー機能	操作パネル	削除(*1)	F.SCN (+SCN)
3	スキャナー機能 (スキャナー文書)	操作パネル	削除	F.DSR (+DSR)
4	ファクス機能	操作パネル	削除(*1)	F.FAX (+FAXOUT)
5	プリンター機能 (一時保存文書)	操作パネル	削除(*1)	F.PRT (+PRT)
6	プリンター機能 (一時保存文書)	WIM	削除(*1)	F.PRT (+PRT)
7	プリンター機能 (保存印刷文書)	操作パネル	削除	F.DSR (+DSR)
8	プリンター機能 (保存印刷文書)	WIM	削除	F.DSR (+DSR)
9	ドキュメントボックス機能 (ファクス送信文書、 ドキュメントボックス文書)	操作パネル	削除	F.DSR (+DSR)
10	ドキュメントボックス機能 (スキャナー文書、 ファクス送信文書、 ドキュメントボックス文書)	WIM	削除 プレビュー	F.DSR (+DSR)

(*1) ジョブをキャンセルすることにより、利用者ジョブデータが扱っていた一時的な文書データが削除される。

(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。ただし、ファクス受信の利用者ジョブデータ(+FAXIN)を削除するインタフェースは提供しない。

利用者ジョブデータを変更(Modify)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 利用者制限機能

利用者制限機能は、識別認証された許可利用者の役割、及び利用者毎に設定された権限に従って、MFP アプリケーションのジョブ実行を許可する機能である。

FDP_ACC.1(b)、FDP_ACF.1(b)

TOE は、一般利用者に対し TOE が提供する MFP アプリケーションのジョブ実行を許可することを決定する TOE 機能アクセス制御 SFP と、MFP 管理者及びスーパーバイザーに対し追加規則を実施することで、利用者制限機能を提供する。

TOE は TOE が提供する MFP アプリケーション(コピー機能、プリンター機能、スキャナー機能、ドキュメントボックス機能、またはファクス機能)のジョブ実行を開始しようとする許可利用者の役割を検証する。利用者役割が一般利用者の場合は、利用機能リストに設定されている MFP アプリケーションと一致する機能種別の MFP アプリケーションのジョブ実行だけを許可する。利用者役割が MFP 管理者の場合には、MFP アプリケーションのジョブ実行を許可する。利用者役割がスーパーバイザーの場合には、MFP アプリケーションのジョブ実行を許可しない。

7.5 蓄積データ保護機能

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

FCS_CKM.1

TOE は、MFP 管理者の操作を受けて HDD 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 HDD 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

HDD 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

TOE は、HDD 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 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、プリンタードライバー、またはファクス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

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、ファクスドライバーから文書データを受信して蓄積、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、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 41 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。ファクス機能利用時は、ファクスドライバーから 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 41 : 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またはファクス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。

7.7 残存情報消去機能

残存情報消去機能は、HDD 上の削除された文書データ、一時的な文書データあるいはその断片に対して、乱数や指定パターンデータを上書きすることにより残存情報の再利用を不可能にする機能である。

FDP_RIP.1

上書きする HDD 領域の消去方法には、逐次消去と一括消去がある。

逐次消去は、HDD 上にある残存情報領域の有無の情報を TOE が常に監視し、残存情報の存在を発見したときに残存情報領域を上書きする方法である。TOE は、利用者の操作によって文書データを削除した時、HDD 上にある文書データのデジタル画像情報が書き込まれている領域に対して、乱数によって上書きする。また、ジョブ終了時に TOE は、ジョブの実行中に HDD 上に生成される一時的な文書データ、あるいはその断片が書き込まれている領域に対して、乱数によって上書きする。

一括消去は、TOE が HDD を一括で上書きする方法である。TOE は、MFP 管理者が指定した上書き方式で HDD を上書きする。一括消去の上書きの方式には、NSA 方式、DoD 方式、乱数書き込み方式、BSI/VSITR 方式、Secure Erase 方式がある。

NSA 方式は、乱数で 2 回上書きし、Null(0)で 1 回上書きする。DoD 方式は、ある値で 1 回上書きし、そのある値の補数で 1 回上書きし、さらに乱数で上書きした後、検証する。乱数書き込み方式は、MFP 管理者が設置時に 3 から 9 回のうち指定した回数を乱数で上書きする。BSI/VSITR 方式は、00, FF, 00, FF, 00, FF, AA の順で上書きする。Secure Erase 方式は、ATA コマンドの secure erase で上書きする。

7.8 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利用者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利用者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。

FMT_SMR.1

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(a)、FMT_MSA.1(b)、FMT_MTD.1(a)、FMT_MTD.1(b)

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 42 に記すように、操作を許可する役割に応じた権限をもつ利用者に、TSF データの操作を許可する。

表 42 : TSF データの管理

分類	TSF データ	操作	操作を許可する利用者役割	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(*3) 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
	利用者役割	変更(*1)	なし	なし
	文書データの所有者情報 [+PRT 、 +SCN 、 +FAXIN 、 +FAXOUT、+CPY]	変更(*1)	なし	なし
	文書データの所有者情報 [+DSR、ファクス受信文書以外]	変更(*1)	なし	なし
	文書データの所有者情報 [+DSR、ファクス受信文書]	変更	MFP 管理者	操作パネル WIM
	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(*4) WIM
		デフォルト値変更	MFP 管理者	操作パネル WIM

分類	TSF データ	操作	操作を許可する利用者役割	操作箇所
	利用者ジョブデータの所有者情報	変更(*1)	なし	なし
	利用機能リスト	新規作成 変更 削除	MFP 管理者	操作パネル WIM
	機能種別	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	
		問い合わせ(*2)	なし	
	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	
		問い合わせ(*2)	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(*2)	なし	
	HDD 暗号鍵	問い合わせ 削除 新規作成	MFP 管理者	操作パネル

(*1) 変更を行うインタフェースは提供しない。

(*2) 問い合わせを行うインタフェースは提供しない。

(*3) 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。

(*4) 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(a)、FMT_MSA.3(b)

表 43 にセキュリティ属性静的初期化のリスト、表 44 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 43 及び表 44 に示した規則に従って、オブジェクト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 43 :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 44 を参照	表 44 を参照

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
	文書データのアクセス許可利用者のリスト	表 44 を参照	表 44 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
MFP アプリケーション	機能種別	MFP アプリケーションのうち各機能(コピー機能、スキャナー機能、プリンター機能、ファクス機能、ドキュメントボックス機能)を識別する値	なし

表 44：文書データの生成ケース毎のセキュリティ属性

文書データの作成	セキュリティ属性	デフォルト値	デフォルト値の上書き
操作パネルから コピー機能で紙文書をスキャンし複写印刷(F.CPY)	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
操作パネルから スキャナー機能で紙文書をスキャンしフォルダー送信または文書添付メール送信(F.SCN)	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
操作パネルから ファクス機能で紙文書をスキャンしファクス送信(F.FAX)	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 プリンター機能で文書データを受信し TOE 内に一時保存(F.PRT)	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
電話回線から ファクス機能で文書データを受信(F.FAX)	なし	なし	なし
電話回線から ファクス機能で文書データを受信し蓄積(F.DSR)	文書データの所有者情報	ファクス受信文書の所有者情報(ログインユーザー名)が設定されたリスト(蓄積受信文書ユーザー)	なし
操作パネルから	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

文書データの作成	セキュリティ属性	デフォルト値	デフォルト値の上書き
スキャナー機能で紙文書をスキャンし蓄積(F.SCN 及び F.DSR)	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(ログインユーザー名のリスト)を上書きできる。
操作パネルから ファクス機能で紙文書をスキャンし蓄積(F.SCN 及び F.DSR)	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(ログインユーザー名のリスト)を上書きできる。
ファクスドライバーから ファクス機能で文書データを受信し蓄積(F.DSR)	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
操作パネルから ドキュメントボックス機能で紙文書をスキャンし蓄積(F.SCN 及び F.DSR)、 またはコピー機能で紙文書をスキャンし蓄積(F.SCN 及び F.DSR)	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(ログインユーザー名のリスト)を上書きできる。
プリンタードライバーから印刷方法をドキュメントボックス蓄積または保存印刷として プリンター機能で文書データを受信し蓄積(F.DSR)	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

7.9 完全性検証機能

完全性検証機能は、TSF の一部及び TSF 実行コードが完全性を保ったソフトウェア構成であることを MFP 初期立上げ中に検証する自己テスト機能である。ここで完全性を検証する対象は、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と HDD 暗号鍵である。

FPT_TST.1

操作パネル制御ソフトウェアの完全性の検証は、操作パネル制御ソフトウェアのハッシュ値の比較または署名の検証により、TOE が初期立上げ中に行う。取得したハッシュ値が正しい値と一致しない、または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。

MFP 制御ソフトウェアの完全性の検証は、ハッシュ値の比較または署名の検証により、TOE が初期立上げ中に行う。取得したハッシュ値が正しい値と一致しない、または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。まず MFP 制御ソフトウェアのハッシュで検証する部分を検証した後、HDD 暗号鍵の完全性を検証する。HDD 暗号鍵から取得したハッシュ値が正しい値と一致しない場合、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。HDD 暗号鍵から取得したハッシュ値が正しい値と一致した場合、TOE は MFP 制御ソフトウェアの署名による検証を行う。取得したハッシュ値が正しい値と一致しない、または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。

操作パネル制御ソフトウェア及び MFP 制御ソフトウェアで取得したハッシュ値が正しい値と一致し、かつ署名が検証された場合、TOE は利用可能になる。

7.10 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、電話回線からの入力情報をファクス受信のみに限定したうえで受信ファクスの転送を禁止する機能である。

FPT_FDI_EXP.1

電話回線からの入力情報に対しては、電話回線からの利用をファクス受信のみに制限し、G3 規格のファクスプロトコルに準拠しない通信が行われた場合は、回線を切断する。TOE 設置時に受信ファクスの転送を禁止する設定を行っているため、受信ファクスが転送される事は無い。

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 45：本 ST に関連する特定の用語

用語	定義
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。
オートログアウト機能	操作パネルあるいは WIM でログイン中に、予め定められた時間アクセスが無かった時に、自動的にログアウトする機能。オートログアウトとも言う。
HDD	ハードディスクドライブの略称。本書で、単に HDD と記載した場合は TOE に取り付けられた HDD を指す。
ジョブ	TOE のコピー、スキャナー、プリンター、ドキュメントボックス機能、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。
MFP アプリケーション	F.CPY、F.PRT、F.SCN、F.FAX、F.DSR を実現するコピー機能、プリンター機能、スキャナー機能、ファクス機能、ドキュメントボックス機能の総称。
コピー機能	MFP アプリケーションのひとつ。F.CPY、F.DSR の SFR パッケージ機能を実現する。
スキャナー機能	MFP アプリケーションのひとつ。F.SCN、F.DSR の SFR パッケージ機能を実現する。
プリンター機能	MFP アプリケーションのひとつ。F.PRT、F.DSR の SFR パッケージ機能を実現する。
ファクス機能	MFP アプリケーションのひとつ。F.FAX、F.DSR の SFR パッケージ機能を実現する。
ドキュメントボックス機能	MFP アプリケーションのひとつ。F.DSR の SFR パッケージ機能を実現する。
一時保存文書	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文書データを受信して TOE 内に一時的に保存された文書データ。文書情報属性は+PRT に相当する。
保存印刷文書	TOE 内に蓄積された文書データのうち、プリンタードライバーから印刷方法で保存印刷を指定して文書データを受信し蓄積されたものを指す。文書情報属性は+DSR に相当する。
ドキュメントボックス文書	TOE 内に蓄積された文書データのうち、コピー機能またはドキュメントボックス機能で操作パネルから紙文書をスキャンして TOE 内に蓄積されたものと、プリンタードライバーから印刷方法でドキュメントボックス蓄積を指定して受信したものを指す。文書情報属性は+DSR に相当する。
スキャナー文書	TOE 内に蓄積された文書データのうち、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蓄積したものを指す。文書情報属性は+DSR に相当する。
ファクス送信文書	TOE 内に蓄積された文書データのうち、ファクス機能で操作パネルから紙文書をスキャンして蓄積したものと、ファクスドライバーから文書データを受信して蓄積したものを指す。文書情報属性は+DSR に相当する。
ファクス受信文書	TOE 内に蓄積された文書データのうち、外部ファクスから電話回線を経由してファクス受信し TOE 内に蓄積されたものを指す。文書情報属性は+DSR に相当する。

用語	定義
蓄積受信文書ユーザー	ファクス受信文書の所有者情報(ログインユーザー名)が設定されたリスト。 すべてのファクス受信文書に対して 1 つのリストが存在する。
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ユニット。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。
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。
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。
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。
TOE 所有者	間接的に TOE に関わり、TOE 資産の保護と、関連するセキュリティ方針の確立に責任を持つ個人または組織を指す。