



Aficio MP C2800/C3300 series with Fax Option Type C5000

セキュリティターゲット

作成者 : 株式会社リコー 船木靖
作成日付 : 2010年7月29日
バージョン : 1.00

更新履歴

バージョン	日付	作成者	詳細
1.00	2010-07-29	船木靖	公開版

目次

1	ST 概説	8
1.1	ST 参照.....	8
1.2	TOE 参照.....	8
1.3	TOE 概要.....	9
1.3.1	TOE の種別.....	9
1.3.2	TOE の使用方法と主要セキュリティ機能.....	9
1.3.3	TOE の利用環境とTOE 以外の構成要素.....	9
1.4	TOE 記述.....	11
1.4.1	TOE の物理的範囲.....	11
1.4.2	ガイダンス文書.....	14
1.4.3	利用者役割.....	16
1.4.3.1	MFP 管理責任者.....	16
1.4.3.2	管理者.....	16
1.4.3.3	スーパーバイザー.....	16
1.4.3.4	一般ユーザー.....	16
1.4.3.5	カスタマー・エンジニア.....	16
1.4.4	TOE の論理的範囲.....	17
1.4.4.1	基本機能.....	17
1.4.4.2	セキュリティ機能.....	19
1.4.5	保護資産.....	22
1.4.5.1	文書データ.....	22
1.4.5.2	印刷データ.....	23
2	適合主張	24
2.1	CC 適合主張.....	24
2.2	PP 主張、パッケージ主張.....	24
2.3	適合根拠.....	24
3	セキュリティ課題定義	25
3.1	脅威.....	25
3.2	組織のセキュリティ方針.....	25

3.3	前提条件	26
4	セキュリティ対策方針	27
4.1	TOEのセキュリティ対策方針	27
4.2	運用環境のセキュリティ対策方針	28
4.3	セキュリティ対策方針根拠	28
4.3.1	追跡性	28
4.3.2	追跡性の正当化	29
5	拡張コンポーネント定義	32
6	セキュリティ要件	33
6.1	セキュリティ機能要件	33
6.1.1	クラスFAU：セキュリティ監査	33
6.1.2	クラスFCS：暗号サポート	37
6.1.3	クラスFDP：利用者データ保護	38
6.1.4	クラスFIA：識別と認証	40
6.1.5	クラスFMT：セキュリティ管理	43
6.1.6	クラスFPT：TSFの保護	49
6.1.7	クラスFTP：高信頼パス/チャネル	49
6.2	セキュリティ保証要件	51
6.3	セキュリティ要件根拠	52
6.3.1	追跡性	52
6.3.2	追跡性の正当化	53
6.3.3	依存性分析	57
6.3.4	セキュリティ保証要件根拠	58
7	TOE要約仕様	59
7.1	TOEセキュリティ機能	59
7.1.1	SF.AUDIT 監査機能	60
7.1.1.1	監査ログの生成	60
7.1.1.2	監査ログの読み出し	62
7.1.1.3	監査ログの保護	62
7.1.1.4	タイムスタンプ	62
7.1.2	SF.I&A 利用者識別認証機能	62
7.1.2.1	利用者の識別認証	62
7.1.2.2	識別認証失敗時のアクション	63

7.1.2.3	パスワードのフィードバックエリア保護.....	64
7.1.2.4	パスワードの登録.....	64
7.1.3	SF.DOC_ACC 文書データアクセス制御機能.....	64
7.1.3.1	一般ユーザーの文書データ操作.....	65
7.1.3.2	文書管理者の文書データ操作.....	65
7.1.4	SF.SEC_MNG セキュリティ管理機能.....	65
7.1.4.1	文書データ利用者リスト管理.....	65
7.1.4.2	管理者情報管理.....	66
7.1.4.3	スーパーバイザー情報管理.....	67
7.1.4.4	一般ユーザー情報管理.....	67
7.1.4.5	機器制御データ管理.....	68
7.1.5	SF.CE_OPE_LOCK 保守機能移行禁止機能.....	69
7.1.6	SF.CIPHER 暗号化機能.....	69
7.1.6.1	文書データの暗号化.....	69
7.1.7	SF.NET_PROT ネットワーク通信データ保護機能.....	69
7.1.7.1	クライアント PC からの Web サービス機能利用.....	70
7.1.7.2	クライアント PC からの印刷とファクス送信.....	70
7.1.7.3	TOE からのメール送信.....	70
7.1.7.4	TOE からのフォルダ配信.....	70
7.1.8	SF.FAX_LINE 電話回線 I/F 侵入防止機能.....	70
7.1.9	SF.GENUINE MFP 制御ソフトウェア検証機能.....	70
8	付録.....	71
8.1	用語の説明.....	71
8.2	参考資料.....	74

図一覧

図 1 :TOE の利用環境.....	10
図 2 :TOE のハードウェア構成.....	12
図 3 :TOE の論理的範囲.....	17

表一覧

表 1 :管理者役割一覧.....	16
表 2 :文書データ操作権限と文書データ操作の対応表.....	20
表 3 :セキュリティ環境とセキュリティ対策方針の関連.....	29
表 4 :監査対象事象リスト.....	33
表 5 :暗号鍵生成のリスト.....	37
表 6 :暗号操作のリスト.....	38
表 7 :サブジェクトと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リスト.....	38
表 8 :サブジェクトとオブジェクトとセキュリティ属性.....	38
表 9 :アクセスを管理する規則.....	39
表 10 :アクセスを明示的に管理する規則.....	39
表 11 :サブジェクト、情報、及び操作のリスト.....	40
表 12 :サブジェクトまたは情報に対応するセキュリティ属性.....	40
表 13 :認証事象のリスト.....	41
表 14 :ロックアウト解除アクション.....	41
表 15 :属性の最初の関連付けに関する規則.....	43
表 16 :セキュリティ属性の管理役割.....	44
表 17 :静的属性初期化の特性.....	44
表 18 :TSF データ管理のリスト.....	45
表 19 :管理機能の特定のリスト.....	46
表 20 :高信頼パスが要求されるサービス.....	50
表 21 :TOE セキュリティ保証要件(EAL3).....	51
表 22 :セキュリティ対策方針と機能要件の関連.....	52
表 23 :TOE セキュリティ機能要件の依存性対応表.....	57
表 24 :TOE セキュリティ機能要件とTOE セキュリティ機能の関連.....	59
表 25 :監査事象と監査情報.....	61
表 26 :利用者役割と認証方法.....	63
表 27 :利用者役割毎のロックアウト解除者.....	63
表 28 :文書データ利用者リストの初期値.....	65
表 29 :文書データ利用者リストへの操作と操作可能者.....	65
表 30 :管理者情報へのアクセス.....	66
表 31 :一般ユーザー情報に対する許可操作.....	67
表 32 :機器制御データの管理者リスト.....	68
表 33 :HDD 蓄積データ暗号操作のリスト.....	69
表 34 :本 ST に関連する特定の用語.....	71

1 ST 概説

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

1.1 ST 参照

本 ST の識別情報を以下に記述する。

ST タイトル : Aficio MP C2800/C3300 series with Fax Option Type C5000 セキュリティーターゲット

ST バージョン : 1.00

作成日付 : 2010 年 7 月 29 日

作成者 : 株式会社リコー 船木靖

1.2 TOE 参照

本 TOE は、デジタル複合機 (以下、MFP という) に、オプション製品であるファクスコントローラユニット (以下、FCU という) を取り付けたもので、MFP 名称とソフトウェア/ハードウェアバージョン、および FCU 名称とバージョンで識別する。TOE は、下記 MFP のいずれかと FCU の組合せで、かつソフトウェア/ハードウェアバージョンが一致するものである。

製造者 : 株式会社リコー

MFP 名称 :

Ricoh Aficio MP C2800、Ricoh Aficio MP C2800G、Ricoh Aficio MP C3300、Ricoh Aficio MP C3300G
Savin C2828、Savin C2828G、Savin C3333、Savin C3333G

Lanier LD528C、Lanier LD528CG、Lanier LD533C、Lanier LD533CG

Lanier MP C2800、Lanier MP C3300

Gestetner MP C2800、Gestetner MP C3300

nashuatec MP C2800、nashuatec MP C3300

Rex-Rotary MP C2800、Rex-Rotary MP C3300

infotec MP C2800、infotec MP C3300

MFP ソフトウェア/ハードウェアバージョン:

ソフトウェア	System/Copy	1.22
	Network Support	8.27
	Scanner	01.23
	Printer	1.22
	Fax	04.00.00
	Web Support	1.10
	Web Uapl	1.08
ハードウェア	Network Doc Box	1.03
	Ic Key	1100
	Ic Ctlr	03

FCU 名称 : Fax Option Type C5000

FCU バージョン: GWFCU3-13 (WW) 04.04.00

キーワード : デジタル複合機、文書、コピー、印刷、スキャナー、ファクス、ネットワーク、オフィス

1.3 TOE 概要

本章では、TOE の種別、TOE の使用方法と主要セキュリティ機能、及び TOE の利用環境と TOE 以外の構成要素について記述する。

1.3.1 TOE の種別

TOE は IT 製品であり、紙文書の電子化、文書管理、印刷をするためのコピー機能、スキャナー機能、プリンター機能、ファクス機能 (オプション) を提供するデジタル複合機以下、MFP というである。

1.3.2 TOE の使用方法と主要セキュリティ機能

TOE は、紙文書あるいは電子文書を TOE 内に入力する入力機能、入力した文書データを蓄積する蓄積機能、入力したまたは蓄積している文書データを出力する出力機能を持つ。紙文書の入力は、MFP が備えるスキャナー装置で読み込み、電子文書の入力は、ネットワーク接続か USB 接続したクライアント PC から受信するか、ファクス受信する。出力機能には、プリント出力、ファクス送信、ネットワーク接続しているサーバーかクライアント PC への転送がある。TOE は、これらの各機能のいずれかを組合せて、コピー機能、スキャナー機能、プリンター機能、ファクス機能として提供する。

利用者は、操作パネルからこれらの機能を利用できる。また、これら機能の一部をリモート操作することもできる。

本 ST における TOE の主要なセキュリティ機能は以下のとおりである。

1. 監査機能
2. 識別認証機能
3. 文書データアクセス制御機能
4. 蓄積データ保護機能
5. ネットワーク通信データ保護機能
6. セキュリティ管理機能
7. 保守機能移行禁止機能
8. 電話回線からの侵入防止機能
9. MFP 制御ソフトウェア検証機能

上記のセキュリティ機能については、「1.4.4.2 セキュリティ機能」にて各機能の内容を記述する。

1.3.3 TOE の利用環境と TOE 以外の構成要素

TOE は、オフィスに設置されることを想定する。オフィスでは、利用者の必要に応じて IT 製品と TOE を、ネットワーク接続、電話回線接続、あるいは USB 接続することができる。利用者は TOE を、TOE の操作パネ

ル、内部ネットワークに接続されたクライアントPC、またはUSB 接続されたクライアントPC から操作することができる。想定するTOEの利用環境について図 1 に示し解説する。

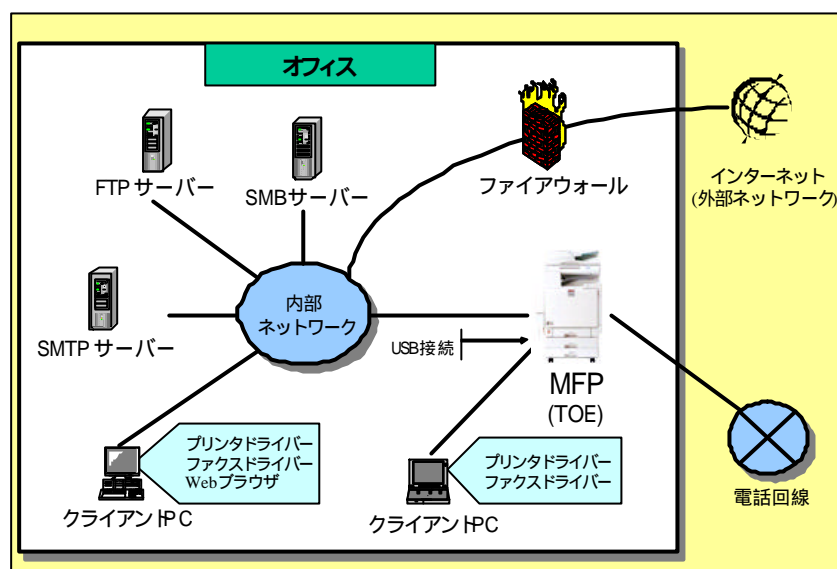


図 1 : TOE の利用環境

TOE 以外の構成要素について以下に記す。

内部ネットワーク

TOE と各種サーバー (FTP サーバー、SMB サーバー、SMTP サーバー) およびクライアントPC を接続する。ファイアウォールを介してインターネットに接続される。内部ネットワークでは IPv4 を使用する。

クライアントPC

内部ネットワークに接続し、クライアントPC の Web ブラウザから TOE にアクセスして TOE の操作とデータ通信ができる。クライアントPC には、Internet Explorer 6.0 以降をインストールしておく必要がある。内部ネットワーク、または USB にクライアントPC を接続して、印刷、ファクス送信する場合は、利用者操作ガイドに記載するホームページから PCL プリンタドライバー、ファクスドライバーをクライアントPC へダウンロードし、インストールする必要がある。

FTP サーバー

TOE の文書データを FTP サーバーにフォルダ配信する場合に利用される。

SMB サーバー

TOE の文書データを SMB サーバーにフォルダ配信する場合に利用される。

SMTP サーバー

TOE の文書データをクライアントPC にメール送信する場合に利用される。

電話回線

ファクスオプションが搭載されている場合に利用される、外部のファクスとの送受信を行うための回線。

ファイアウォール

内部ネットワークと外部ネットワークの間に設置し、内部ネットワークを外部ネットワークから保護する装置。

1.4 TOE 記述

本章では、TOE の物理的範囲、ガイダンス文書、利用者役割、TOE の論理的範囲、及び保護資産について記述する。

1.4.1 TOEの物理的範囲

TOE の物理的範囲は、図 2 に示すように操作パネルユニット、エンジンユニット、ファクスユニット、コントローラボード、Ic Ctr、HDD、ネットワークユニット、USB ポート SD CARD スロットのハードウェアで構成されるMFP である。TOE のハードウェア構成要素を図 2 に図示して概要を記述する。

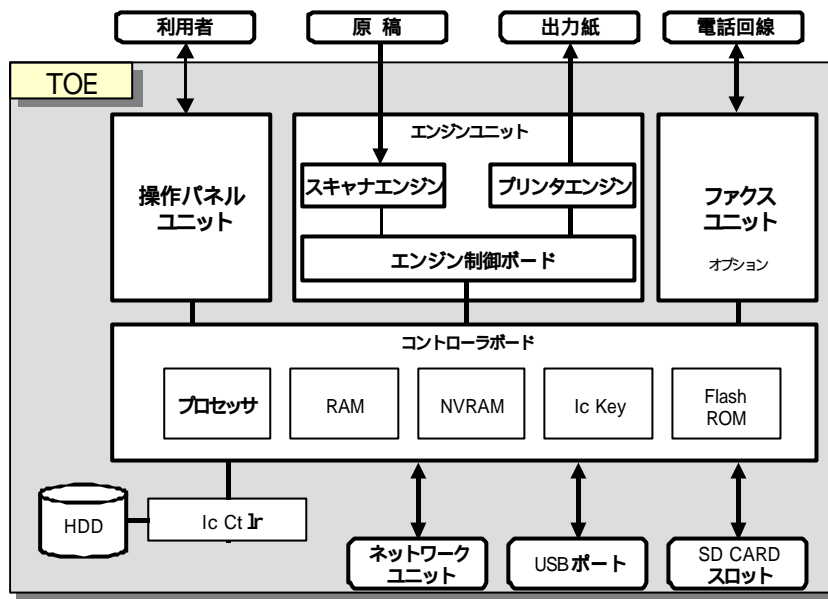


図 2 : TOE のハードウェア構成

操作パネルユニット(以下、操作パネルと言う)

操作パネルはTOE に組み付けられたTOE の利用者がTOE 操作に使用するインターフェース装置で、ハードキー、LED、タッチパネル付き液晶ディスプレイと操作パネル制御ボードで構成される。操作パネル制御ボードには、操作パネル制御ソフトウェアがインストールされている。操作パネル制御ソフトウェアは、ハードキーやタッチパネル付き液晶ディスプレイからの入力をMFP 制御ソフトウェアに送信、あるいはMFP 制御ソフトウェアからの指示を受信して LED の点灯及び消灯、タッチパネル付き液晶ディスプレイの画面表示を実行する。

エンジンユニット

エンジンユニットは、スキャナーエンジン、プリンタエンジン、エンジン制御ボードで構成される。スキャナーエンジンは紙文書を読み込むための入力装置で、プリンタエンジンは紙文書を印刷し排出する出力装置である。エンジン制御ボードには、エンジン制御ソフトウェアがインストールされている。エンジン制御ソフトウェアは、スキャナーエンジンやプリンタエンジンの状態をMFP 制御ソフトウェアに送信したり、MFP 制御ソフトウェアの指示によってスキャナーエンジンやプリンタエンジンを動作させたりする。

ファクスユニット(オプション)

ファクスユニットはモデム機能を持ち電話回線と接続してファクスの送受信を行なう装置である。ファクスユニットにはMFP 制御ソフトウェアとのインターフェースがあり、MFP 制御ソフトウェアにファクス通信状態を通知したり、MFP 制御ソフトウェアの指示によってファクス通信の制御を実行したりする。

コントローラボード

コントローラボードはプロセッサ、FlashROM、RAM、NVRAM、Ic Key が載った基板である。コントローラボードは操作パネルユニット、エンジンユニット、ファクスユニット、ネットワークユニット、USB ポート、SD CARD スロット、Ic Ctlr と接続される。Ic Ctlr にはさらに HDD が接続される。プロセッサ、FlashROM、RAM、NVRAM、Ic Key の概要を以下に記載する。

[プロセッサ]

MFP 動作における基本的な演算処理をおこなう半導体チップ。

[FlashROM]

MFP 制御ソフトウェアがインストールされているメモリ。

[RAM]

画像メモリとして利用される揮発性メモリ。

[NVRAM]

MFP の動作を決定するMFP 制御データが入った不揮発性メモリ

[Ic Key]

乱数発生、暗号鍵生成の機能を持ち、MFP 制御ソフトウェアの改ざん検知に利用されるセキュリティチップ。

Ic Ctlr

Ic Ctlr は HDD に保管する情報を暗号化し、HDD から読み出す情報を復号する機能を持ったセキュリティチップである。

HDD

HDD は画像データ、識別認証に利用するユーザー情報が書込まれるハードディスクドライブである。

ネットワークユニット

ネットワークユニットは Ethernet (100BASE-TX/10BASE-T) をサポートしたネットワークのインターフェース基板である。

USB ポート

USB ポートは、クライアントPC とTOE をUSB 接続し、クライアントPC から印刷、あるいはファクス送信するために使用する。

SD CARD スロット

SD CARD スロットは、カスタマー・エンジニア (以下、CE と言う) が SD カードを使った保守作業をするために使用するスロットであり、TOE 側面にあって、通常はカバーで覆われネジ止めされている。CE は、保守作業する際に、このカバーを外して SD カードを出し入れする。

特に設置時には、CE が蓄積データ保護機能を活性化するための SD カードをこのスロットにセットして、蓄積データ保護機能を活性化にする。

1.4.2 ガイダンス文書

本 TOE のガイダンス文書には、[英語版-1]、[英語版-2]、[英語版-3]のガイダンスセットがあり、販売地域に応じていずれかのガイダンスのセットを付属する。以下に、ガイダンスセット毎のガイダンス文書を示す。

[英語版-1]

- C2828/C3333/C4040/C5050/C2828G/C3333G/C4040G/C5050G
MP C2800/C3300/C4000/C5000
LD528C/LD533C/LD540C/LD550C/LD528CG/LD533CG/LD540CG/LD550CG
Aficio MP C2800/C3300/C4000/C5000/C2800G/C3300G/C4000G/C5000G
Operating Instructions
About This Machine
- C2828/C3333/C4040/C5050/C2828G/C3333G/C4040G/C5050G
MP C2800/C3300/C4000/C5000
LD528C/LD533C/LD540C/LD550C/LD528CG/LD533CG/LD540CG/LD550CG
Aficio MP C2800/C3300/C4000/C5000/C2800G/C3300G/C4000G/C5000G
Operating Instructions
Troubleshooting
- Notes for Users
- Caution on Use of the Optional USB 2.0/SD Slot Type A (Media Slot)
- Quick Reference Copy Guide
- Quick Reference Fax Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide
- Manuals for Users
C2828/C3333/C4040/C5050
MP C2800/MP C3300/MP C4000/MP C5000
LD528C/LD533C/LD540C/LD550C
Aficio MP C2800/MP C3300/MP C4000/MP C5000
- Manuals for Administrators
C2828/C3333/C4040/C5050
MP C2800/MP C3300/MP C4000/MP C5000
LD528C/LD533C/LD540C/LD550C
Aficio MP C2800/MP C3300/MP C4000/MP C5000
- Notes for Security Functions
- Notes for Administrators:Using this Machine in a CC-Certified Environment

[英語版-2]

- Quick Reference Copy Guide
- Quick Reference Fax Guide
- Quick Reference Printer Guide

-
- Quick Reference Scanner Guide
 - Manuals for This Machine
 - Notes for Users
 - Caution on Use of the Optional USB 2.0/SD Slot Type A (Media Slot)
 - Manuals for Users
MP C2800/MP C3300/MP C4000/MP C5000
Aficio MP C2800/MP C3300/MP C4000/MP C5000
A
 - Manuals for Administrators
Security Reference
MP C2800/MP C3300/MP C4000/MP C5000
Aficio MP C2800/MP C3300/MP C4000/MP C5000
 - Notes for Security Functions
 - Notes for Administrators:Using this Machine in a CC-Certified Environment

[英語版-3]

- MP C2800/C3300/C4000/C5000
MP C2800/C3300/C4000/C5000
Aficio MP C2800/C3300/C4000/C5000
Operating Instructions
About This Machine
- MP C2800/C3300/C4000/C5000
MP C2800/C3300/C4000/C5000
Aficio MP C2800/C3300/C4000/C5000
Operating Instructions
Troubleshooting
- Notes for Users
- Caution on Use of the Optional USB 2.0/SD Slot Type A (Media Slot)
- Quick Reference Copy Guide
- Quick Reference Fax Guide
- Quick Reference Printer Guide
- Quick Reference Scanner Guide
- Manuals for Users
MP C2800/MP C3300/MP C4000/MP C5000
Aficio MP C2800/MP C3300/MP C4000/MP C5000
- Manuals for Administrators
MP C2800/MP C3300/MP C4000/MP C5000
Aficio MP C2800/MP C3300/MP C4000/MP C5000
- Notes for Security Functions
- Notes for Administrators:Using this Machine in a CC-Certified Environment

1.4.3 利用者役割

本章では、本 TOE の運用に関連する者の役割について記述する。

1.4.3.1 MFP 管理責任者

MFP 管理責任者とは、TOE を利用する組織の中で TOE の管理者とスーパーバイザーを選任する役割を持った者のことを言う。

MFP 管理責任者は、4名までの管理者と、スーパーバイザーを1名選任する。管理者を選任する際には、ユーザー管理、機器管理、ネットワーク管理、文書管理の管理者役割の内、少なくとも1つ以上の管理者役割を管理者に与える。

1.4.3.2 管理者

管理者とは、TOE に管理者として登録された利用者のことで、TOE には管理者を1から4名まで登録する。管理者の管理者役割は、ユーザー管理、機器管理、ネットワーク管理、文書管理がある。管理者は、管理者役割を兼任することができ、管理者役割は必ず1人以上の管理者に割り当てられる。TOE の工場出荷時には管理者が1人設定され、その管理者が4つの管理者役割を兼任する設定になっており、TOE の設置時に MFP 管理責任者に管理者として選任された者が、選任された管理者のID、パスワード、管理者役割を設定変更する。表 1 に管理者役割毎の管理作業を記述する。

表 1：管理者役割一覧

管理者役割	説明
ユーザー管理	一般ユーザーを管理する。
機器管理	機器の管理と、監査をする。
ネットワーク管理	TOE のネットワーク接続を管理する。
文書管理	TOE 内に蓄積されている文書を管理する。

1.4.3.3 スーパーバイザー

スーパーバイザーとは、管理者パスワードの管理をする役割をもった利用者で、管理者パスワードを変更することができる。TOE には、スーパーバイザーが1名登録されている。工場出荷時のTOE には、デフォルトのスーパーバイザーが登録されており、MFP 管理責任者がスーパーバイザーとして選任した者がデフォルトのスーパーバイザーID とパスワードを設定しなおす。

1.4.3.4 一般ユーザー

一般ユーザーとは、ユーザー管理者によってアドレス帳に登録された TOE の許可利用者のことであり、TOE への文書データ蓄積と、TOE に蓄積されている文書データに対して操作することができる。

1.4.3.5 カスタマー・エンジニア

カスタマー・エンジニア (以下、CE と言う) とはメーカー、サービス会社、販売会社に所属して TOE の保守をする専門知識を有する者を言う

1.4.4 TOEの論理的範囲

TOEの論理的範囲は、TOEが提供する機能である。本章では、TOEが利用者に提供するサービスである「基本機能」とTOEの脅威に対抗するための「セキュリティ機能」について図3に図示し、内容を記述する。

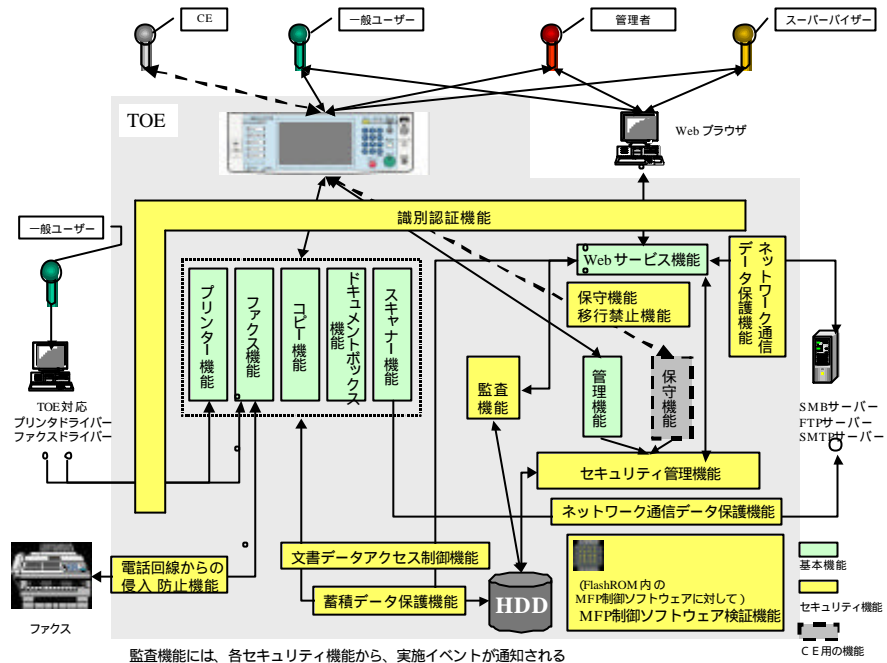


図 3 : TOE の論理的範囲

1.4.4.1 基本機能

基本機能には、操作パネルから操作するコピー機能、プリンター機能、ファクス機能、スキャナー機能、ドキュメントボックス機能、および管理機能と、クライアントPCのWebブラウザから利用するWebサービス機能がある。

コピー機能、ドキュメントボックス機能、プリンター機能、ファクス機能、およびスキャナー機能は一般ユーザーに提供される機能である。管理機能は、管理者またはスーパーバイザーに提供される機能である。これら操作パネルから操作する機能は、操作パネル上の機能選択ボタンを押下してから利用する。

Webサービス機能は、一般ユーザー、管理者、およびスーパーバイザーが、その役割に応じた機能が利用できる。

コピー機能

コピー機能は、原稿をスキャンし、読み取ったイメージデータを利用者が指定する部数、倍率、編集指定(たとえば複数ページの原稿イメージを1枚の用紙に印刷する集約指定)などの印刷条件に従って印刷する機能である。また、読み取った原稿イメージを文書データとしてD-BOXに蓄積することができる。コピー

機能で D-BOX に蓄積された文書データは、同じ基本機能である後述の「ドキュメントボックス機能」を使って印刷、削除することができる。

プリンター機能

プリンター機能は、クライアントPC から送られる印刷データを印刷する機能である。TOE はクライアントPC からネットワークまたは USB ポートで印刷データを受信する。TOE は受信した印刷データを直接印刷あるいは蓄積印刷によって印刷する。蓄積印刷では、印刷データは文書データとして D-BOX に蓄積され、蓄積された文書データは同じ基本機能である後述の「ドキュメントボックス機能」を使って印刷、削除することができる。

ファクス機能

ファクス機能は、電話回線を通してファクス装置と送受信する機能である。ファクス機能には、ファクス受信機能 (以下、ファクス受信と言う)、ファクス送信機能 (以下、ファクス送信と言う)、ファクス送受信データを印刷や削除する機能がある。

ファクス受信は、受信したファクスデータを印刷するか、ファクス受信データに変換し D-BOX に蓄積する。D-BOX に蓄積したファクス受信データは、ファクス機能または同じ基本機能である後述の「ドキュメントボックス機能」を使って印刷、削除することができる。

ファクス送信には、操作パネルから操作する直接送信、メモリ送信、蓄積文書ファクス送信と、クライアントPC から操作する PC ファクス送信がある。ファクスで送信するために、D-BOX に蓄積した文書データは、同じ基本機能である後述の「ドキュメントボックス機能」を使って印刷、削除することができる。

尚、MFP はファクス機能の一部として IP-ファクスとインターネットファクス機能を提供するが、IP-ファクスとインターネットファクス機能は、本評価の対象外である。

スキャナー機能

スキャナー機能は、紙原稿を電子化してクライアントPC で扱えるようにするために、原稿をスキャンし、読み取ったイメージデータを文書データとしてネットワーク経由でフォルダ配信、メール送信する機能である。また、読み取ったイメージデータを D-BOX に文書データとして蓄積することができる。スキャナー機能を使って D-BOX に蓄積した文書データはスキャナー機能で、メール送信、フォルダ配信、削除することができる。

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、原稿をスキャンし、読み取ったイメージデータを D-BOX に文書データとして蓄積する機能である。また、コピー機能、プリンター機能、ファクス機能及びドキュメントボックス機能で D-BOX に蓄積された文書データを印刷、削除することができる。スキャナー機能で蓄積された文書データは扱うことができない。文書データを印刷する際、操作する利用者に応じて、蓄積している文書データの印刷条件が更新される。

管理機能

管理機能は、機器動作を決定する情報、TOE をネットワーク接続するための情報、利用者に関する情報、文書データを利用制限するための情報を設定する機能で、TOE の許可利用者 (一般ユーザー、管理者、スーパーバイザー) それぞれの役割に応じて、設定できる情報が決められている。管理機能は、操作パネルから操作するか、クライアントPC から Web サービス機能にアクセスして操作することができる。設定する情報によっては、操作パネルからだけ設定できる情報、クライアントPC からだけ設定できる情報もある。管

理機能のうち、セキュリティに係わる機能を後述「1.4.4.2 セキュリティ機能」の「セキュリティ管理機能」に記載する。

尚、本機能で利用制限するアドレス帳のバックアップ/リストアは、本評価の対象外である。

Web サービス機能

Web サービス機能は、TOE の許可利用者（一般ユーザー、管理者、スーパーバイザー）がクライアントPC からTOE をリモート操作するための機能である。リモート操作するためには、クライアントPC に Web ブラウザをインストールし、TOE とクライアントPC をネットワークで接続する必要がある。利用者は、Web ブラウザからTOE の Web サーバーに接続することで Web サービス機能が利用できる。リモート操作できるTOE の操作は以下の通りである。

1. D-BOX に蓄積している文書データの印刷
印刷できるのは、コピー機能、ドキュメントボックス機能、ファクス機能、プリンター機能で蓄積した文書データ。文書データを印刷する際、操作する利用者に応じて、蓄積している文書データの印刷条件が更新される。
2. D-BOX に蓄積している文書データの送信
送信できるのは、スキャナー機能で蓄積した文書データ。
3. D-BOX に蓄積している文書データの削除
4. D-BOX に蓄積している文書データのダウンロード
ダウンロードできるのは、スキャナー機能、またはファクス機能で蓄積した文書データ。
5. 管理機能の一部
6. TOE の状態確認

1.4.4.2 セキュリティ機能

セキュリティ機能には、監査機能、識別認証機能、文書データアクセス制御機能、蓄積データ保護機能、ネットワーク通信データ保護機能、セキュリティ管理機能、保守機能移行禁止機能、電話回線からの侵入防止機能、MFP 制御ソフトウェア検証機能がある。本章では、これらセキュリティ機能について記述する。

監査機能

監査機能は、TOE の運用状況を確認、あるいはセキュリティ侵害を検知するために必要な事象発生時に監査ログを記録する機能である。記録した監査ログは、機器管理者だけに読み出し、削除の操作を許可する。監査ログの読み出しは Web サービス機能、監査ログの削除は操作パネルと Web サービス機能を利用して実施できる。

識別認証機能

識別認証機能は、操作パネル、クライアントPC から TOE を利用しようとする者に利用者 ID と認証情報を入力させ利用者の特定と本人確認をする機能である。ただし、クライアントPC からの印刷あるいはファクス送信の場合は、TOE ではないプリンタドライバーまたはファクスドライバーから利用者が、利用者 ID と認証情報を入力後に TOE へ送信する。TOE は、受信した利用者 ID と認証情報で識別認証をする。

また、識別認証機能には、同じ利用者 ID で認証に連続で失敗した回数がログインパスワード入力許容回数に達した場合、その利用者 ID を一時的にログインできなくするアカウントロック、利用者がパスワードを入

力中に盗み見られないよう 認証フィールドバックエリアに表示するパスワードを伏字で表示する認証フィールドバックエリア保護、予めユーザー管理者が設定するパスワード最小桁数とパスワード複雑度の条件を満たすパスワードだけを登録するパスワード品質維持が含まれる。

本 TOE が持つ識別認証機能は他にもあるが、上記以外の識別認証機能は、本評価の対象外である。

文書データアクセス制御機能

文書データアクセス制御機能は、特定の利用者だけに D-BOX に蓄積している文書データの操作を許可する機能である。

文書データの操作には、読み出しと削除がある。それぞれの操作内容を下に記す。

読み出し :D-BOX に蓄積している文書データを読み出すこと

削除 D-BOX に蓄積している文書データを削除すること

TOE が、文書データへの操作を許可する特定の利用者は、文書管理者と一般ユーザーである。

文書管理者には、全ての文書データに対して削除操作を許可する。

一般ユーザーには、文書データ操作権限で許可された操作だけを許可する。文書データ操作権限には、閲覧、編集、編集/削除、フルコントロールがある。このうち編集権限は、文書データに対する許可操作は閲覧権限と同じで、その他に印刷条件の更新も許可される。文書データ操作権限と文書データ操作の関係を表 2 に記述する。

表 2 : 文書データ操作権限と文書データ操作の対応表

文書データ操作 文書データ操作権限	文書データ読み出し	文書データ削除
閲覧	X	
編集	X	
編集/削除	X	X
フルコントロール	X	X

X 操作可能 空欄 操作不可

各文書データは、文書データ操作権限を一般ユーザー毎に設定することができる。

蓄積データ保護機能

蓄積データ保護機能は、HDD に記録されている文書データを漏洩から保護するため、文書データを正規の方法で読み出す以外は文書データの内容を理解することを困難にする機能である。

ネットワーク通信データ保護機能

ネットワーク通信データ保護機能は、ネットワーク上の文書データと印刷データを不正なアクセスから保護する機能である。文書データまたは印刷データの送信方法によって、通信データを保護するための通信プ

ロトコルは異なる。以下に、送信方法と保護手段の対応関係を記述する。

尚、使用する通信プロトコルは、ネットワーク管理者がTOEの設置環境やTOEの用途に応じて決定する。

1. クライアントPCからWebサービス機能を利用した文書データのダウンロード (SSLプロトコル)
2. クライアントPCからの印刷、またはファクス送信 (SSLプロトコル)
3. TOEからFTPサーバー、またはSMBサーバーへの文書データ配信 (PSECプロトコル)
4. TOEからクライアントPCへ文書データを添付したメールの送信 (MIME)

セキュリティ管理機能

セキュリティ管理機能は、同じセキュリティ機能である前述の「識別認証機能」で認証に成功した管理者、スーパーバイザー、一般ユーザーに対して、その利用者役割に応じたセキュリティ管理のための操作を許可する機能である。

1. 文書データ利用者リスト管理

文書データ利用者リスト管理は、文書データ利用者リストの変更を特定の利用者だけに許可する機能である。文書データ利用者リストの変更には、文書オーナーの変更、文書データ利用者リストへ文書利用者を新規登録、文書データ利用者リストに登録済みの文書利用者の削除、文書データ操作権限の変更がある。このうち文書オーナーの変更は、文書管理者のみに許可する。その他の操作は、文書管理者、文書オーナー、文書データに対してフルコントロールの権限を持つ文書利用者に許可される。

文書データ蓄積時の、文書データ利用者リストには、文書データデフォルトアクセス権リストが設定される。

2. 管理者情報管理

管理者情報管理とは、管理者の登録と削除、管理者役割の追加と削除、管理者IDと管理者パスワードの変更を特定の利用者に許可することである。

管理者の登録と管理者役割の追加は、管理者だけに許可される操作である。管理者の削除、管理者役割の削除、管理者IDの変更は当該管理者に許可される操作である。管理者パスワードの変更は、当該管理者とスーパーバイザーに許可される操作である。尚、管理者役割の追加は、自身に割り当てられている管理者役割に限るという条件があり、管理者役割の削除には、他の管理者が削除対象の管理者役割を持っている場合だけに限ると言う条件がある。

管理者は、1つ以上の管理者役割を持つ必要があるため、管理者が他の管理者を登録する際には、自身が持つ管理者役割の中から1つ以上を新規の管理者に付与(追加)する必要がある。また、管理者が自身の管理者役割を全て削除した場合、その管理者の管理者情報は自動で削除される。

3. 一般ユーザー情報管理

一般ユーザー情報管理とは、一般ユーザー情報の新規作成、変更、削除の操作を特定の利用者役割だけに許可することである。利用者役割と許可される操作の関係は、ユーザー管理者には、一般ユーザー情報の新規作成、変更、削除が許可され、一般ユーザーには、アドレス帳に登録されている自身の一般ユーザー情報の変更が許可される。ただし、一般ユーザーは自身の一般ユーザー情報であっても一般ユーザーIDを変更できない。

4. スーパーバイザー情報管理

スーパーバイザーのIDとパスワードの変更をスーパーバイザーに許可する。

5. 機器制御データ管理

機器管理者、ユーザー管理者、及び文書管理者の役割に応じた機器制御データのデータ項目の設定を、それぞれの管理者に許可する。

保守機能移行禁止機能

保守機能は、機器管理者から依頼を受けたCEが操作パネルからTOEの保守サービスを実行する機能で、保守機能移行禁止機能は、保守機能の操作を禁止する機能である。本STでは保守機能移行禁止機能を稼働させた状態を評価範囲とする。

電話回線からの侵入防止機能

電話回線からの侵入防止機能は、ファクスユニットが装着された機器において、TOEに接続した電話回線からは許可された通信だけを受付ける機能である。

MFP制御ソフトウェア検証機能

MFP制御ソフトウェア検証機能は、FlashROMにインストールされているMFP制御ソフトウェアの実行コードの完全性をチェックすることで、MFP制御ソフトウェアが正規のものであることを確認する機能である。

1.4.5 保護資産

本章では、本TOEが保護対象とする資産(文書データ、印刷データ)について記述する。

1.4.5.1 文書データ

文書データは、TOE外から様々な手段でTOE内に取込まれる。TOE内に取込まれた文書データは、TOE内に蓄積するか、TOE外に出力することができる。TOE内に蓄積している文書データは、削除することができる。

文書データの取り込み

文書データの取込みには、以下の2通りがある。

1. スキャナーユニットからの取込み
TOEのスキャナーから紙原稿のイメージを読み込み文書データを生成する。
2. ネットワークUSBからの取込み
TOEがネットワーク回線あるいはUSBから受信した印刷データをTOEが扱える形式に変換し文書データを生成する。

文書データの蓄積

TOE内に蓄積している文書データは、D-BOXに蓄積される。D-BOXに蓄積されている文書データは、不正アクセスと漏洩から保護される。

文書データの出力

文書データの出力には、以下の5通りがある。

1. クライアントPC (メール宛先)に送信
2. SMB サーバー及びFTP サーバーに送信
3. TOE からクライアントPC にダウンロード
4. 印刷
5. ファクス送信

このうち、1.から 3.の出力方式において、通信経路上にある文書データは、漏洩から保護され、改ざんがあった場合は検知される。

1.4.5.2 印刷データ

印刷データとは、印刷あるいはファクスの出力イメージが記述されたデータで、印刷あるいはファクスする際にクライアントPC 内の文書からクライアントPC にインストールされているプリンタドライバーあるいはファクスドライバーによって生成され、内部ネットワーク経由またはUSB ポートからTOE に取り込まれる。印刷データは、クライアントPC からTOE に送信される際の内部ネットワーク経路において、漏洩から保護され、改ざんがあった場合は検知される。

2 適合主張

本章では、適合の主張について記述する。

2.1 CC 適合主張

本 ST 及び TOE の CC 適合主張は以下のとおりである。

- ・ 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 2006 年 9 月 バージョン 3.1 改訂第 1 版(翻訳第 1.2 版) CCMB-2006-09-002

パート2:

セキュリティ機能コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版(翻訳第 2.0 版)
CCMB-2007-09-002

パート3:

セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版(翻訳第 2.0 版)
CCMB-2007-09-003

- ・ 機能要件 :パート2適合
- ・ 保証要件 :パート3適合

2.2 PP 主張、パッケージ主張

本 ST 及び TOE が適合している PP はない。

本 ST は、以下の通りパッケージ適合を主張する。

パッケージ EAL3 適合

2.3 適合根拠

本 ST は PP 適合を主張していないので、PP 適合根拠はない。

3 セキュリティ課題定義

本章では、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 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、記述する。本章に記述する脅威は、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者による攻撃であり、攻撃者は基本レベルの攻撃能力を持つ者とする。

T.ILLEGAL_USE (TOEの不正利用)

攻撃者が、TOE の外部インターフェース (操作パネル、ネットワークインターフェース、USB インターフェース、またはSD CARD インターフェース)からTOE に不正にアクセスし文書データを読み出す、あるいは文書データを削除するかもしれない。

T.UNAUTH_ACCESS (TOE内に蓄積されている保護資産へのアクセス違反)

TOE の許可利用者が、TOE の許可利用者に提供する TOE の外部インターフェース (操作パネル、ネットワークインターフェース、あるいはUSB インターフェース)から文書データに対して利用権限を越えたアクセスをするかもしれない。

T.ABUSE_SEC_MNG (セキュリティ管理機能の不正利用)

セキュリティ管理機能の利用を許可されないものが、セキュリティ管理機能を不正に利用するかもしれない。

T.SALVAGE (メモリの持ち去り)

攻撃者が、TOE からHDD を持ち去り、文書データを暴露するかもしれない。

T.TRANSIT (通信経路上の盗聴、改ざん)

攻撃者が、内部ネットワーク上のTOE が送受信する文書データと印刷データを不正に入手し漏洩、または改ざんするかもしれない。

T.FAX_LINE (電話回線からの侵入)

攻撃者が電話回線からTOE に不正にアクセスするかもしれない。

3.2 組織のセキュリティ方針

IT 製品にインストールされたソフトウェアの完全性を要求する組織のために、以下のセキュリティ方針を想定する。

P.SOFTWARE (ソフトウェアの完全性確認)

TOE 内の FlashROM にインストールされているMFP 制御ソフトウェアが正規のものであることを確認する手段が提供されていること。

3.3 前提条件

本 TOE の利用環境に関わる前提条件を識別し、記述する。

A.ADMIN (管理者の条件)

管理者は、管理者に課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、一般ユーザーに TOE をセキュアに運用させるものとする。さらに、管理者は、管理者の特権を利用して悪意を持った不正をしないものとする。

A.SUPERVISOR (スーパーバイザーの条件)

スーパーバイザーは、スーパーバイザーに課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、スーパーバイザーの特権を利用して悪意を持った不正をしないものとする。

A.NETWORK (ネットワークの接続条件)

TOE が接続されるネットワークをインターネットなどの外部ネットワークと接続する場合は、外部ネットワークから内部ネットワークを保護するものとする。

4 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、運用環境のセキュリティ対策方針、及びセキュリティ対策方針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.AUDIT (監査)

TOE は、セキュリティ機能関連事象を監査ログとして記録し、セキュリティ侵害の事後検出を可能とするための監査ログ読み出し機能を機器管理者だけに供給しなければならない。

O.I&A (利用者の識別認証)

TOE は、利用者が TOE のセキュリティ機能を利用するのに先立って識別認証を実施し、認証に成功した利用者には、その利用者が操作権限を有する機能の利用を許可しなければならない。

O.DOC_ACC (保護資産のアクセス制御)

TOE は、一般ユーザーに対して、文書データ操作権限に従って、文書データへのアクセスを保証しなければならない。また TOE は、文書管理者に対して D-BOX に蓄積している文書データの削除を許可しなければならない。

O.MANAGE (セキュリティ管理)

TOE は、セキュリティ機能のふるまい、TSF データ、セキュリティ属性の管理を、セキュリティが維持できる特定の利用者だけに許可しなければならない。

O.MEM.PROTECT (メモリ蓄積データの暴露防止)

TOE は、HDD に蓄積されている文書データを解読が困難な形式にしなければならない。

O.NET.PROTECT (ネットワーク伝送データの保護)

TOE は、通信経路上の文書データ、印刷データを盗聴から保護し、改ざんを検知しなければならない。

- O.GENUINE (MFP 制御ソフトウェアの完全性保護)**
TOE は、FlashROM にインストールされているMFP 制御ソフトウェアが正規のものであることを確認する機能をTOE の利用者に提供しなければならない。
- O.LINE_PROTECT (電話回線からの侵入防止)**
TOE は、ファクスユニットに接続されている電話回線からTOE への不正なアクセスを防がなければならない。

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.ADMIN (信頼できる管理者)**
MFP 管理責任者は、信頼のおける人を管理者として選任し、その管理者に対して管理者の役割に応じた教育を実施しなければならない。教育を受けた管理者は、TOE の管理者ガイダンスに明示された一般ユーザーに対するセキュアな運用のための遵守事項を、一般ユーザーに周知徹底するよう指導しなければならない。
- OE.SUPERVISOR (信頼できるスーパーバイザー)**
MFP 管理責任者は、信頼のおける人をスーパーバイザーとして選任し、そのスーパーバイザーに対してスーパーバイザーの役割に応じた教育を実施しなければならない。
- OE.NETWORK (TOE を接続するネットワーク環境)**
TOE を接続する内部ネットワークをインターネットなどの外部ネットワークと接続する場合、内部ネットワークを運用管理する組織が、外部ネットワークと内部ネットワーク間の不要なポートを閉じなければならない。(例えば、ファイアウォールの設置)

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記述する。

以下の記述より、すべてのセキュリティ対策方針が達成された場合、「3 セキュリティ課題定義」にて定義されたセキュリティ課題は解決される。すなわち、すべての脅威は対抗され、すべての組織のセキュリティ方針は達成され、全ての前提条件は実現される。

4.3.1 追跡性

本章では、前述の「5.1 脅威」、「5.2 組織のセキュリティ方針」、及び「5.3 前提条件」に対する、「4.1 TOE のセキュリティ対策方針」または「4.2 運用環境のセキュリティ対策方針」の対応関係を表 3 で示す。表中「X」は、対応関係にあることを示している。

表 3 から明らかなように、各セキュリティ対策方針は、少なくとも1つ以上の脅威、組織のセキュリティ方針、及び前提条件に対応している。また、セキュリティ対策方針は、前提条件に対応していない(表 3 中の網掛け部分)。

表 3 : セキュリティ環境とセキュリティ対策方針の関連

TOE セキュリティ環境 セキュリティ対策方針	A.ADMIN	A.SUPERVISOR	A.NETWORK	T.ILLEGAL_USE	T.UNAUTH_ACCESS	T.ABUSE_SEC_MNG	T.SALVAGE	T.TRANSIT	T.FAX_LINE	P.SOFTWARE
O.AUDIT				X		X	X	X	X	
O.I&A				X	X	X				
O.DOC_ACC					X					
O.MANAGE						X				
O.MEM.PROTECT							X			
O.NET.PROTECT								X		
O.GENUINE										X
O.LINE_PROTECT									X	
OE.ADMIN	X									
OE.SUPERVISOR		X								
OE.NETWORK			X							

4.3.2 追跡性の正当化

以下に、各セキュリティ対策方針が「5.1 脅威」、「5.2 組織のセキュリティ方針」、及び「5.3 前提条件」を満たすのに適している根拠を記述する。

A.ADMIN (管理者の条件)

A.ADMIN は、管理者は、管理者に課せられた作業において TOE をセキュアに運用するために必要な知識を持ち、一般ユーザーにTOEをセキュアに運用させるものとする。さらに、管理者は、管理者の特権を利用した悪意を持った不正をしないことを前提としている。

OE.ADMIN によって、MFP 管理責任者が信頼のおける人を管理者に選任し、管理者の役割に応じた教育を実施する。教育を受けた管理者は、TOEの管理者ガイダンスに明示された一般ユーザーに対するセキュアな運用のための遵守事項を一般ユーザーに周知徹底するよう指導する。よって A.ADMIN は実現できる。

A.SUPERVISOR (スーパーバイザーの条件)

A.SUPERVISOR は、スーパーバイザーが、スーパーバイザーに課せられた作業においてTOE をセキュアに運用するための必要な知識を持ち、スーパーバイザーの特権を利用した悪意を持った不正をしないことを前提としている。

OE.SUPERVISOR によって、MFP 管理責任者が信頼をおける人をスーパーバイザーに選任し、スーパーバイザーの役割に応じた教育を実施する。よって A. SUPERVISOR は実現できる。

A.NETWORK (ネットワークの接続条件)

A.NETWORK は、TOE が接続されるネットワークをインターネットなどの外部ネットワークと接続する場合は、外部ネットワークから内部ネットワーク保護することを前提としている。

OE.NETWORK によって、TOE を接続する内部ネットワークをインターネットなどの外部ネットワークと接続する場合、内部ネットワークを運用管理する組織が、外部ネットワークと内部ネットワークの不要なポートを閉じる。よって、A.NETWORK は実現できる。

T.ILLEGAL_USE (TOEの不正利用)

本脅威に対して TOE は、O.I&A によって利用者がTOE のセキュリティ機能を利用するのに先立って識別認証し、認証に成功した許可利用者に対して、その利用者が操作権限を有する機能の利用を許可する。また、O.AUDIT によって、O.I&A 実施を監査ログとして記録し、機器管理者がO.I&A のセキュリティ侵害の事後検出をするため、監査ログ読み出し機能を機器管理者だけに提供する。

従って、TOE は T.ILLEGAL_USE に対抗できる。

T.UNAUTH_ACCESS (TOE 内に蓄積されている保護資産へのアクセス違反)

本脅威に対して TOE は、O.I&A によって識別された許可利用者に対して O.DOC_ACC によって許可利用者の役割と許可利用者に割り当てられた文書データ操作権限に応じて、文書データへのアクセスを許可する。具体的には、許可利用者が一般ユーザーならば、その一般ユーザーに与えられた文書データ操作権限に従って文書データへの操作を許可し、許可利用者が文書管理者ならば D-BOX に蓄積している文書データの削除を許可する。

従って、TOE は T.UNAUTH_ACCESS に対抗できる。

T.ABUSE_SEC_MNG (セキュリティ管理機能の不正利用)

本脅威に対して TOE は、O.I&A にて認証に成功した利用者 TOE のセキュリティ機能の使用を許可する。さらに、O.MANAGE によってセキュリティ機能のふるまい、TSF データ、セキュリティ属性の管理を特定の利用者に制限する。また、O.AUDIT によって、O.I&A 及び O.MANAGE の実施を監査ログとして記録し、機器管理者が O.I&A 及び O.MANAGE のセキュリティ侵害の事後検出をするため、監査ログ読み出し機能を機器管理者だけに提供する。

従って、TOE は T.ABUSE_SEC_MNG に対抗できる。

T.SALVAGE (メモリの持ち去り)

本脅威に対して TOE は、O.MEM.PROTECT によって、HDD をTOE 以外の IT 製品に取り付けて文書データを読み出して解読することが困難な形式に変換する。また、O.AUDIT によって、O.MEM.PROTECT の実施を監査ログとして記録し、O.MEM.PROTECT が必ず実施されていることを、機器管理者が事後検出す

るため、監査ログ読み出し機能を機器管理者だけに提供する。
従って、TOEはT.SALVAGEに対抗できる。

T.TRANSIT (通信経路上の盗聴、改ざん)

本脅威に対して TOE は、O.NET.PROTECT によって、通信経路上の文書データ、印刷データを漏洩から保護し、改ざんを検知する。また O.AUDIT によって、O.NET.PROTECT の実施を監査ログとして記録し、O.NET.PROTECT が実施されたことを、機器管理者が事後確認するため、監査ログ読み出し機能を機器管理者だけに提供する。
従って、TOEはT.TRANSITに対抗できる。

T.FAX_LINE (電話回線からの侵入)

本脅威に対して TOE は、O.LINE_PROTECT によってファクスユニットに接続された電話回線からTOEへの侵入を防ぐ。また、O.AUDIT によって、O.LINE_PROTECT の実施を監査ログとして記録し、O.LINE_PROTECT が必ず実施されていることを、機器管理者が事後検出するため、監査ログ読み出し機能を機器管理者だけに提供する。
従って、TOEはT.FAX_LINEに対抗できる。

P.SOFTWARE (ソフトウェアの完全性確認)

本組織のセキュリティ方針に対して TOE は、O.GENUINE によって TOE の利用者が FlashROM にインストールされているMFP 制御ソフトウェアが正規のものであることを確認できる。
従って、TOEはP.SOFTWAREに対抗できる。

5 拡張コンポーネント定義

本 ST 及び TOE では、拡張したセキュリティ要件、すなわち「2.1 CC 適合主張」にて適合を主張する CC に記載されていない新規のセキュリティ要件とセキュリティ保証要件は定義しない。

6 セキュリティ要件

本章では、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について記述する。

6.1 セキュリティ機能要件

本章では、「4.1 TOE のセキュリティ対策方針」で定義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。尚、セキュリティ機能要件は、CC Part2 に規定のセキュリティ機能要件から引用する。

また、CC Part2 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

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 4 に示す TOE の監査対象事象]**。

機能要件毎に割り付けられた監査対象とすべきアクション (CC における規定) と、それに対応するTOE の監査対象事象を表 4 に記述する。

表 4：監査対象事象リスト

機能要件	監査対象とすべきアクション	TOE の監査対象事象
FAU_GEN.1	なし	-
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	監査事象は記録しない
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	監査事象は記録しない
FAU_STG.1	なし	-
FAU_STG.4	a) 基本: 監査格納失敗によってとられるアクション。	監査事象は記録しない
FCS_CKM.1	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	<個別に定義した監査対象事象> 1.HDD 暗号鍵生成 (結果 成功/失敗)

機能要件	監査対象とすべきアクション	TOEの監査対象事象
FCS_COP.1	a) 最小: 成功と失敗及び暗号操作の種類別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	<個別に定義した監査対象事象> 1.文書データの蓄積の成功 2.文書データの読み出しの成功
FDP_ACC.1	なし	-
FDP_ACF.1	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	<個別に定義した監査対象事象> 1.文書データの蓄積の成功 2.文書データの読み出しの成功 3.文書データの削除の成功
FDP_IFC.1	なし	-
FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた、情報の特定のサブセット例えば、対象物の劣化の監査)。	a) 最小 1. ファクス機能 受信
FIA_AFL.1	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼働)。	a) 最小 1.ロックアウトの開始 2.ロックアウトの解除
FIA_ATD.1	なし	-
FIA_SOS.1	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	b) 基本 1.一般ユーザー認証情報の新規作成 (結果 :成功/失敗) 2.一般ユーザー認証情報の変更 (結果 :成功/失敗) 3.管理者認証情報の変更 (結果 :成功/失敗) 4.スーパーバイザー認証情報の変更 (結果 :成功/失敗)
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。	基本 1.ログイン (結果 :成功/失敗)
FIA_UAU.7	なし	-

機能要件	監査対象とすべきアクション	TOEの監査対象事象
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	b) 基本 1.ログイン (結果 成功/失敗)
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)	b) 基本 1.ログイン (結果 成功/失敗)
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	<個別に定義した監査対象事象> 1.管理者役割の追加、削除 2.文書データ利用者リストの変更
FMT_MSA.3	a) 基本: 許有的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	監査事象は記録しない
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	<個別に定義した監査対象事象> 1.一般ユーザー認証情報の新規作成 2.一般ユーザー認証情報の変更 3.一般ユーザー認証情報の削除 4.管理者認証情報の変更 5.スーパーバイザー認証情報の変更 6.システム時計の日時変更 7.監査ログの全削除
FMT_SMF.1	a) 最小 管理機能の使用	<個別に定義した監査対象事象> 1.管理者役割の追加、削除 2.ロックアウト解除者によるロックアウト解除 3.システム時計の日時変更
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	a) 最小 1.管理者役割の追加、削除
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供。	a) 最小 1.システム時計の日時変更
FPT_TST.1	a) 基本: TSF 自己テストの実行とテストの結果。	-
FTP_ITC.1	a) 最小: 高信頼チャネル機能の失敗。 b) 最小: 失敗した高信頼チャネル機	<個別に定義した監査対象事象> 1.高信頼性IT製品との通信 (結果 成功/失敗、通信先 IP アドレス)

機能要件	監査対象とすべきアクション	TOEの監査対象事象
	能の開始者とターゲットの識別。 c) 基本: 高信頼チャネル機能のすべての使用の試み。 d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。	
FTP_TRP.1	a) 最小: 高信頼パス機能の失敗。 b) 最小: もし得られれば、すべての高信頼パス失敗に関する利用者の識別情報。 c) 基本: 高信頼パス機能のすべての使用の試み。 d) 基本: もし得られれば、すべての高信頼パス呼出に関する利用者の識別情報。	<個別に定義した監査対象事象> 1. リモート利用者との通信 (結果 成功/失敗)

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:通信先 IP アドレス、他者の利用者認証情報を新規作成/変更/削除した場合の対象者 ID、ロックアウト対象者、ロックアウト解除対象者、ロックアウト解除方法操作対象文書データID]。

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:機器管理者]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。

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。

FAU_STG.1 保護された監査証拠格納

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**] できなければならない。

FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 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。

6.1.2 クラス FCS : 暗号サポート

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:表 5 に示す標準]**に合致する、指定された暗号鍵生成アルゴリズム**[割付: 表 5 に示す暗号鍵生成アルゴリズム]**と指定された暗号鍵長**[割付: 表 5 に示す暗号鍵長]**に従って、暗号鍵を生成しなければならない。

表 5 : 暗号鍵生成のリスト

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
HDD 暗号鍵	BSI-AIS31	TRNG	256 ビット

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: 表 6 に示す標準]**に合致する、特定された暗号アルゴリズム**[割付: 表 6 に示す暗号アルゴリズム]**と暗号鍵長**[割付: 表 6 に示す暗号鍵長]**に従って、**[割付: 表 6 に示す暗号操作]**を実行しなければならない。

表 6 : 暗号操作のリスト

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
HDD 暗号鍵	FIPS197	AES	256ビット	- 文書データを HDD に書き込む際の暗号化 - 文書データを HDD から読み込む際の復号

6.1.3 クラス FDP : 利用者データ保護

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: 表 7 のサブジェクトと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リスト]に対して[割付: MFP アクセス制御SFP]を実施しなければならない。

表 7 : サブジェクトと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リスト

サブジェクト	オブジェクト	サブジェクトとオブジェクト間の操作
管理者プロセス	文書データ	文書データ削除
一般ユーザプロセス	文書データ	文書データ蓄積 文書データ読み出し 文書データ削除

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: 表 8 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: MFP アクセス制御SFP]を実施しなければならない。

表 8 : 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	管理者プロセス	- 管理者 ID - 管理者役割
サブジェクト	一般ユーザプロセス	- 一般ユーザ ID - 文書データデフォルトアクセス権リスト
オブジェクト	文書データ	- 文書データ利用者リスト

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: 表 9 に示すサブジェクトのオブジェクトに対する操作と、操作に対するアクセスを管理する規則]。

表 9 : アクセスを管理する規則

サブジェクト	オブジェクトに対する操作	アクセスを管理する規則
一般ユーザープロセス	文書データ蓄積	一般ユーザーは、文書データを蓄積することができる。文書データが蓄積される際、一般ユーザープロセスに関連付けられた文書データデフォルトアクセス権リストが、蓄積する文書データに関連付けられた文書データ利用者リストにコピーされる。
	文書データ読み出し	一般ユーザープロセスに関連付けられた一般ユーザーID と文書データに関連付けられた文書データ利用者リストの文書オーナーID か文書利用者ID のいずれかが一致し、一致したID に付与された文書データ操作権限が、閲覧か編集か編集/削除かフルコントロールの場合、その一般ユーザープロセスに対して文書データの読み出しが許可される。
	文書データ削除	一般ユーザープロセスに関連付けられた一般ユーザーID と文書データに関連付けられた文書データ利用者リストの中文書オーナーID か文書利用者ID のいずれかが一致し、一致したID に付与された文書データ操作権限が編集/削除かフルコントロールの場合、その一般ユーザープロセスに対して文書データの削除が許可される。

FDP_ACF.1.3 TSF は、次の追加規則、[割付: 表 10 に示すサブジェクトのオブジェクトに対する操作を明示的に承認する規則]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 10 : アクセスを明示的に管理する規則

サブジェクト	オブジェクトに対する操作	アクセスを管理する規則
管理者プロセス	文書データの削除	管理者プロセスに関連付けられた管理者役割に文書管理者が含まれる場合、管理者プロセスにD-BOX に蓄積されている全ての文書データの削除操作を許可する。

FDP_ACF.1.4 TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則はなし]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。

FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 TSF は、[割付: 表 11 にリストしたサブジェクト、情報、及び操作]に対して[割付: 電話回線

情報フロー SFP]を実施しなければならない。

表 11 : サブジェクト、情報、及び操作のリスト

サブジェクト	情報	操作
- ファクスユニットのファクスプロセス - コントローラボードのファクス受信プロセス	電話回線から受信したデータ	受渡し

(注 受渡しとは、電話回線から受信したデータをコントローラボードがファクスユニットから受け取ること)

FDP_IFF.1 単純セキュリティ属性

下位階層: なし

依存性: FDP_IFC.1 サブセット情報フロー制御

FMT_MSA.3 静的属性初期化

FDP_IFF.1.1 TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付: 電話回線情報フロー SFP]を実施しなければならない。: [割付: 表 12 に示すサブジェクトまたは情報と、各々に対応するセキュリティ属性]

表 12 : サブジェクトまたは情報に対応するセキュリティ属性

種別	サブジェクトまたは情報	セキュリティ属性
サブジェクト	ファクスユニットのファクスプロセス	セキュリティ属性はなし
サブジェクト	コントローラボードのファクス受信プロセス	セキュリティ属性はなし
情報	電話回線から受信したデータ	データ種別

(注 :データ種別とは、電話回線から受信するデータの種類のことであり、ファクスデータとファクスデータ以外がある)

FDP_IFF.1.2 TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない [割付:電話回線から受信したデータの種別が、ファクスデータの場合、ファクスユニットのファクスプロセスはコントローラボードのファクス受信プロセスに電話回線から受信したデータの通過を許可する。]。

FDP_IFF.1.3 TSFは、[割付: 追加の情報フロー制御SFP規則はなし]を実施しなければならない。

FDP_IFF.1.4 TSF は、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に許可する規則はなし]に基づいて、情報フロー を明示的に許可しなければならない。

FDP_IFF.1.5 TSF は、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に拒否する規則はなし]に基づいて、情報フローを明示的に拒否しなければならない。

6.1.4 クラス FIA : 識別と認証

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 13 に示す認証事象における、利用者毎の認証失敗累積回数]に関して、
[選択: 『割付: 1 から 5』内における管理者 (詳細化 機器管理者) 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 13 : 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
クライアントPC の Web ブラウザからTOE を使用する利用者認証
クライアントPC から印刷する際の利用者認証
クライアントPC からファクス送信する際の利用者認証

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択:に達する]とき、TSF は、[割付: 表 14 に示すロックアウト解除アクションのいずれかが取られるまで、認証試行に失敗した利用者をロックアウトする]をしなければならない。

表 14 : ロックアウト解除アクション

ロックアウト解除アクション	内容
オートロックアウト解除	不成功の認証試行が定義した回数に達してから、予め設定されたロックアウト時間 (機器管理者が設定する 1 分から 9999 分で設定) 経過後、ロックアウトになっている利用者の最初の識別認証実施でロックアウトが解除される。尚、機器管理者はロックアウト時間を無期限と設定することもでき、その場合は、時間経過によるロックアウト解除は行われず、他のロックアウト解除操作によってのみ解除できる。
マニュアルロックアウト解除	機器管理者のロックアウト解除時間の設定値に係わらず、ロックアウトした利用者役割ごとに定められている、ロックアウト解除者の解除操作によって、当該利用者のロックアウトが解除される。ロックアウト対象者とロックアウト解除者の関係については FMT_MTD.1 で規定する。 尚、特別なロックアウト解除操作として、管理者 (全管理者役割) 及びスーパーバイザーがロックアウトした場合は、TOE の再起動がロックアウト解除者による解除操作と同じ効果を持つ。

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:一般ユーザーID、文書データデフォルトアクセス権リスト、管理者 ID、管理者役割、スーパーバイザーID]

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) 使用できる文字とその文字種:

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)

(2) 登録可能な桁数:

一般ユーザーの場合

ユーザー管理者が設定するパスワード最小桁数 (8から32桁) 以上、128桁以下

管理者、スーパーバイザーの場合

ユーザー管理者が設定するパスワード最小桁数 (8から32桁) 以上、32桁以下

(3) 規則:

ユーザー管理者が設定するパスワード複雑度にしたがった文字種の組合せで作成したパスワードの登録を許可する。ユーザー管理者は、パスワード複雑度に複雑度1か複雑度2を設定する。

FIA_UAU.2 **アクション前の利用者認証**

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 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、各利用者に認証が成功することを要求しなければならない。

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:パスワード1文字に対して、ダミー文字 (* :アスタリスク、または 黒丸) を認証フィードバックエリアに表示**だけを利用者に提供しなければならない。

FIA_UID.2 **アクション前の利用者識別**

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1 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。

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:一般ユーザーID、文書データデフォルトアクセス権リスト、管理者 ID、管理者役割、スーパーバイザーID]

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: 表 15 にリストした属性の最初の関連付けに関する規則]

表 15 : 属性の最初の関連付けに関する規則

利用者	サブジェクト	利用者セキュリティ属性
一般ユーザー	一般ユーザープロセス	一般ユーザーID、 文書データデフォルトアクセス権リスト
管理者	管理者プロセス	管理者 ID、 管理者役割
スーパーバイザー	スーパーバイザープロセス	スーパーバイザーID

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:管理者は自身に割り当てられた管理者役割を他の管理者に追加することができる。また、自身の管理者役割を削除することができる。ただし、管理者が管理者役割を削除することによって、その管理者役割を持つ管理者がいなくなる場合は削除できない。]

6.1.5 クラス FMT : セキュリティ管理

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: 表 16 のセキュリティ属性に対し[選択: 問い合わせ、変更、削除、割付: 新規作成、変更、追加]をする能力を割付: 表 16 の利用者役割]に制限する[割付: MFP アクセス制御SFP]を実施しなければならない。

表 16：セキュリティ属性の管理役割

セキュリティ属性	操作	利用者役割
一般ユーザーID (一般ユーザー情報のデータ項目)	問い合わせ、新規作成、削除	- ユーザー管理者
	問い合わせ	- 一般ユーザー
管理者 ID	新規作成	- 管理者
	問い合わせ、変更	- 当該管理者
	問い合わせ	- スーパーバイザー
管理者役割	問い合わせ、追加、削除	- 当該管理者役割を割り当てられている管理者
スーパーバイザーID	問い合わせ、変更	- スーパーバイザー
文書データ利用者リスト	問い合わせ、改変	- 文書管理者 - 文書オーナー - 当該文書データに対してフルコントロールの文書データ操作権限を持つ一般ユーザー
文書データデフォルトアクセス権リスト (一般ユーザー情報のデータ項目)	問い合わせ、改変	- ユーザー管理者 - 当該一般ユーザー

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: [割付 表 17 に示す限定的な]デフォルト値を与える[割付: MFP アクセス制御SFP]を実施しなければならない。

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。

表 17：静的属性初期化の特性

オブジェクト	オブジェクトに関連付けられるセキュリティ属性	オブジェクト生成時のデフォルト値とその特性
一般ユーザーが蓄積する文書データ	文書データ利用者リスト	予め当該一般ユーザー (文書オーナー) の文書データデフォルトアクセス権リストとして設定された値。この値は、ユーザー管理者または当該一般ユーザーにより任意の設定が可能であり、制限的でも許

		可的でもなく、限定的な特性を持つ。
--	--	-------------------

FMT_MTD.1 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 TSF は、[割付: 表 18 の TSF データ管理のリスト]を[選択: 問い合わせ、改変、削除、割付: 登録、変更、全削除、新規作成]する能力を[割付: 表 18 の役割]に制限しなければならない。

表 18 : TSF データ管理のリスト

TSFデータ	操作	利用者役割
一般ユーザー認証情報 (一般ユーザー情報のデータ項目)	新規作成、 変更、 削除	ユーザー管理者
	変更	一般ユーザー情報の当該一般ユーザー
スーパーバイザー認証情報	変更	スーパーバイザー
管理者認証情報	変更	スーパーバイザー、 当該管理者
ログインパスワード入力許容回数	問い合わせ、 改変	機器管理者
ロックアウト解除タイマー設定	問い合わせ、 改変	機器管理者
ロックアウト時間	問い合わせ、 改変	機器管理者
システム時計の日時 年月日設定、時刻 (時分秒) 設定	問い合わせ、 改変	機器管理者
	問い合わせ	一般ユーザー、 ユーザー管理者、 ネットワーク管理者、 文書管理者、 スーパーバイザー
パスワード最小桁数	問い合わせ、 改変	ユーザー管理者
パスワード複雑度	問い合わせ、 改変	ユーザー管理者
HDD 暗号鍵	問い合わせ、 新規作成	機器管理者
監査ログ	問い合わせ、 全削除	機器管理者
保守機能移行禁止設定	問い合わせ、 改変	機器管理者

TSFデータ	操作	利用者役割
	問い合わせ	一般ユーザー、 ユーザー管理者、 ネットワーク管理者、 文書管理者、 スーパーバイザー
一般ユーザーのロックアウトフラグ	問い合わせ、 改変	ユーザー管理者
管理者のロックアウトフラグ	問い合わせ、 改変	スーパーバイザー
スーパーバイザーのロックアウトフラグ	問い合わせ、 改変	機器管理者
S/MIME 利用者情報(一般ユーザー情報のデータ項目)	問い合わせ、 新規作成、 削除、 変更	ユーザー管理者、 S/MIME 利用者情報の当該一般ユーザー
	問い合わせ	一般ユーザー
フォルダ配信先情報	問い合わせ	ユーザー管理者 一般ユーザー

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 19 に記述する管理機能の特定のリスト]。

表 19 : 管理機能の特定のリスト

機能要件	管理要件	管理項目
FAU_GEN.1	なし	-
FAU_SAR.1	a) 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	a)管理者役割の中の機器管理者の管理
FAU_SAR.2	なし	-
FAU_STG.1	なし	-
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	なし: アクションは固定であり、管理対象とならない
FCS_CKM.1	なし	-
FCS_COP.1	なし	-
FDP_ACC.1	なし	-
FDP_ACF.1	a)明示的なアクセスまたは拒否に基づ	a)管理者役割の中の文書管理者の管理

機能要件	管理要件	管理項目
	く決定に使われる属性の管理。	
FDP_IFC.1	なし	-
FDP_IFF.1	a)明示的なアクセスに基づく決定に使われる属性の管理。	なし：明示的なアクセスに基づく決定に使われる属性(データ種別)は固定であり、変更するためのインターフェースもないため。
FIA_AFL.1	a)不成功の認証試行に対する閾値の管理; b)認証失敗の事象においてとられるアクションの管理。	a) セキュリティ管理機能(機器制御データ管理):機器管理者によるログインパスワード入力許容回数の管理 b)ロックアウト対象者に対するロックアウト解除者とロックアウト解除操作の管理
FIA_ATD.1	a)もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし:利用者に対する追加のセキュリティ属性を定義する機能はない
FIA_SOS.1	a)秘密の検証に使用される尺度の管理。	セキュリティ管理機能(機器制御データ管理):ユーザー管理者が機器制御データの次の設定項目を管理 -パスワード最小桁数 -パスワード複雑度
FIA_UAU.2	a)管理者による認証データの管理; b)このデータに関係する利用者による認証データの管理。	-セキュリティ管理機能(一般ユーザー情報管理):ユーザー管理者による一般ユーザー認証情報の管理と、一般ユーザーによる本人の一般ユーザー認証情報の管理 -セキュリティ管理機能(管理者情報管理):管理者本人による管理者認証情報の管理 -セキュリティ管理機能(管理者情報管理):管理者による管理者の新規登録 -セキュリティ管理機能(管理者情報管理):スーパーバイザーによる管理者認証情報の管理 -セキュリティ管理機能(スーパーバイザー情報管理):スーパーバイザーによるスーパーバイザー認証情報の管理
FIA_UAU.7	なし	-
FIA_UID.2	a)利用者識別情報の管理。	-セキュリティ管理機能(一般ユーザー情報管理):ユーザー管理者による一般ユーザーIDの管理 -セキュリティ管理機能(管理者情報管理):管理者による自身の管理者IDの管理 -セキュリティ管理機能(管理者情報管理):管理者による管理者の新規登録 -セキュリティ管理機能(スーパーバイザー情報管理):スーパーバイザーによるスー

機能要件	管理要件	管理項目
		パーバイザーID の管理
FIA_USB.1	a)許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b)許可管理者は、サブジェクトのセキュリティ属性を変更できる。	a) なし：デフォルトのサブジェクトのセキュリティ属性は定義できない。 b)管理者は、自身に割り当てられている管理者役割を他の管理者に追加できるとともに、管理者役割を削除できる。
FMT_MSA.1	a)セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること b)セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a)管理者による管理者役割の管理 b)なし：セキュリティ属性が特定の値を引き継ぐための規則はない
FMT_MSA.3	a) 初期値を特定し得る役割のグループを管理すること b) 所定のアクセス制御 SFP に対するデフォルト値の許有的あるいは制限的設定を管理すること c)セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a)なし：初期設定を特定できる役割のグループはない b) 文書データデフォルトアクセス権リストの管理 -ユーザー管理者にアドレス帳に登録されている全ての一般ユーザー情報の文書データデフォルトアクセス権リストの改変を許可 -一般ユーザーに自身の一般ユーザー情報の文書データデフォルトアクセス権リストの改変を許可 c)なし：セキュリティ属性が特定の値を引き継ぐための規則はない
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし：TSF データと相互に影響を及ぼし得る役割のグループはない
FMT_SMF.1	なし	-
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	管理者による管理者役割の管理
FPT_STM.1	a) 時間の管理。	セキュリティ管理機能 (機器制御データ管理)：機器管理者が、機器制御データの次の設定項目を管理 -システム時計の年月日、時刻 (時、分、秒)
FPT_TST.1	a) 初期立ち上げ中、定期間隔、あるいは特定の条件下など、TSF 自己テストが動作する条件の管理; b) 必要ならば、時間間隔の管理。	a)なし：TSF 自己テストが動作する条件は固定。 b)なし：時間間隔に管理はない
FTP_ITC.1	a) もしサポートされていれば、高信頼チャンネルを要求するアクションの構成。	なし：TSF 間高信頼チャンネルを要求するアクションは固定であるため
FTP_TRP.1	a) もしサポートされていれば、高信頼パスを要求するアクションの構成。	なし：高信頼パスを要求するアクションは固定であるため

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:一般ユーザー、管理者 (機器管理者、文書管理者、ユーザー管理者、ネットワーク管理者)、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**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。

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 dc Ctlr の暗号化機能]]の正常動作を実証するために、[選択: 初期立ち上げ中]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、許可利用者に、[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、許可利用者に、格納されている 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。

6.1.7 クラス FTP : 高信頼バスチャネル**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]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: TOE から SMB サーバーへのフォルダ配信サービス (PSec)、TOE から FTP サーバーへのフォルダ配信サービス (PSec)]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。

- FTP_TRP.1 **高信頼パス**
 下位階層: なし
 依存性: なし
- FTP_TRP.1.1 TSF は、それ自身と**選択: リモート**利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、**[選択: 改変、暴露]**からの通信データの保護を提供する通信パスを提供しなければならない。
- FTP_TRP.1.2 TSF は、**[選択: TSF、リモート利用者]**が、高信頼パスを介して通信を開始することを許可しなければならない。
- FTP_TRP.1.3 TSF は、**[選択: 最初の利用者認証、[割付: TOE の Web サービス、クライアントPC からの印刷サービス、クライアントPC からのファクス送信サービス、TOE からクライアントPC へのメール送信サービス]]**に対して、高信頼パスの使用を要求しなければならない。
- FTP_TRP.1.2 に示す高信頼パスを介して通信をする各利用者が使用する、FTP_TRP.1.3 で示された高信頼パスが要求されるサービスを表 20 に記述する。

表 20 : 高信頼パスが要求されるサービス

通信関係者	高信頼パスが要求されるサービス
TSF	TOE からクライアントPC へのメール送信サービス (S/MIME)
リモート利用者	最初の利用者認証 (SSL) クライアントPC からの TOE の Web サービス (SSL) クライアントPC からの印刷サービス (SSL) クライアントPC からのファクス送信サービス (SSL)

6.2 セキュリティ保証要件

本TOEの評価保証レベルはEAL3である。TOEの保証コンポーネントを表 21 に示す。これは評価保証レベルのEAL3によって定義されたコンポーネントのセットであり、他の要件は追加していない。

表 21 : TOE セキュリティ保証要件(EAL3)

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.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
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.3 許可の管理
	ALC_CMS.3 実現表現の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
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.2 カバレッジの分析
	ATE_DPT.1 テスト 基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト- サンプル
AVA: 脆弱性評価	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記述する。

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、「4.1 TOE のセキュリティ対策方針」で定義したセキュリティ対策方針は達成される。

6.3.1 追跡性

TOE セキュリティ機能要件とTOE セキュリティ対策方針の対応関係を表 22 に示す。表中「X」は、対応関係にあることを示している。

表 22 から、TOE セキュリティ機能要件が1つ以上のTOE セキュリティ対策方針に対応していることが分かる。

表 22 : セキュリティ対策方針と機能要件の関連

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FAU_GEN.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1					X			
FCS_COP.1					X			
FDP_ACC.1			X					
FDP_ACF.1			X					
FDP_IFC.1								X
FDP_IFF.1								X
FIA_AFL.1		X						
FIA_ATD.1		X						
FIA_SOS.1		X						
FIA_UAU.2		X						
FIA_UAU.7		X						
FIA_UID.2		X						
FIA_USB.1		X						

	O.AUDIT	O.I&A	O.DOC_ACC	O.MANAGE	O.MEM.PROTECT	O.NET.PROTECT	O.GENUINE	O.LINE_PROTECT
FMT_MSA.1				X				
FMT_MSA.3				X				
FMT_MTD.1				X				
FMT_SMF.1				X				
FMT_SMR.1				X				
FPT_STM.1	X							
FPT_TST.1					X		X	
FTP_ITC.1						X		
FTP_TRP.1						X		

6.3.2 追跡性の正当化

本章では、TOEセキュリティ対策方針が、表 22にて対応付けたTOEセキュリティ機能要件によって実現できることを記述する。

O.AUDIT 監査

表 22にてO.AUDITに対応している機能要件が、O.AUDITを満たすのに適している根拠を以下に示す。

a) 監査ログを記録する

O.AUDITを実現するためには、セキュリティ機能の実施を監査ログとして記録する必要がある。これに対してFAU_GEN.1は、監査機能の開始と終了、識別認証機能の実施、利用者による保護資産の操作、保護資産の暗号化、及び主要な管理機能の実施時に、監査情報を生成する。事象の発生日付・時刻、事象の種別、サブジェクトの識別情報、事象の結果を記録する。

b) 監査機能を提供する

O.AUDITを実現するためには、監査できる形式の監査ログを機器管理者だけに提供する必要がある。これに対して、FAU_SAR.1は、機器管理者が、検証できる形式で監査ログを読み出せるように、FAU_SAR.2によって、機器管理者以外が監査ログを読み出すことを禁止する。

c) 監査ログを保護する

O.AUDITを実現するためには、監査ログを適切に保護する対策が必要である。これに対して、FAU_STG.1は、監査ログを不正な削除から保護し、不正な改ざんを防止する。また、FAU_STG.4は、監査ログファイルがいっぱいになった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に新しい監査ログを上書きすることで最新の監査ログが損失することを防止する。

d) 信頼できる事象発生時間

O.AUDITを実現するためには、セキュリティ侵害を適切に管理するために正確な事象発生時間を記

録する対策が必要である。

これに対して、FPT_STM.1 は、信頼できるタイムスタンプを提供する。

O.I&A 利用者の識別認証

表 22 にて O.I&A に対応している機能要件が、O.I&A を満たすのに適している根拠を以下に示す。

- a) 利用者が TOE を利用する前に利用者の識別認証をする
O.I&A を実現するためには、利用者が TOE のセキュリティ機能を利用するのに先立って、許可利用者であることを識別認証しなければならない。
これに対して FIA_UID.2 は、利用者が TOE のセキュリティ機能を利用する前に利用者の識別を行ない、FIA_UAU.2 は、識別された利用者の認証を行なう
- b) 識別認証が成功した利用者に TOE の利用を許可する
O.I&A を実現するためには、利用者が TOE のセキュリティ機能利用前に実施する認証に成功した場合、その利用者が操作権限を持つ機能の利用を許可しなければならない。
これに対して FIA_ATD.1 と FIA_USB.1 は、識別認証に成功した利用者に対して、その利用者を代行するサブジェクトを結合する。さらに、サブジェクトにセキュリティ属性を関連付け維持する。
- c) パスワードの解読を困難にする
O.I&A を実現するためには、利用者認証に使うパスワードを、利用者が入力中に盗み見られたり、簡単に推測されたりすることを防止しなければならない。
これに対して、FIA_UAU.7 は、利用者がパスワードを 1 文字入力する毎に、認証フィードバックエリアに伏字 (* :アスタリスクまたは 黒丸) を表示することでパスワードの盗み見を防止し、FIA_SOS.1 は、ユーザー管理者が設定するパスワードの最小桁数、パスワードの文字種組合せを満たすパスワードだけの登録を許可することで推測が困難なパスワードだけを有効にし、FIA_AFL.1 は、操作パネルからの利用者認証、クライアント PC の Web ブラウザからの利用者認証、クライアント PC から印刷する際の利用者認証、及びクライアント PC からファクス送信する際の利用者認証の失敗回数累計が、機器管理者が設定したログインパスワード入力許容回数に達した利用者をロックアウトすることで、パスワード解読の機会を少なくしている。

O.DOC_ACC 保護資産のアクセス制御

表 22 にて O.DOC_ACC に対応している機能要件が、O.DOC_ACC を満たすのに適している根拠を以下に示す。

- a) 文書データへのアクセス制御を規定して実施する
O.DOC_ACC を実現するためには、利用者に結び付けられたサブジェクトの種類と、サブジェクトに関連付けられたセキュリティ属性毎に定められた文書データ操作権限に準じて、各利用者に文書データの操作を許可しなければならない。
これに対して FDP_ACC.1 と FDP_ACF.1 は、管理者プロセスに関連付けられた管理者役割が文書管理者ならば、その管理者プロセスに文書データを削除する操作を許可する。一般ユーザーに対しては、一般ユーザープロセスに対して文書データの蓄積を許可し、さらに一般ユーザープロセスに関連付けられた一般ユーザー ID が、各文書データの文書データ利用者リストに登録されていれば、その文書データを操作することを許可する。許可する操作は、文書データ利用者リストに一般ユーザー ID 毎に設定されている文書データ操作権限に従う

O. MANAGE セキュリティ管理

表 22 にて O.MANAGE に対応している機能要件が、O.MANAGE を満たすのに適している根拠を以下に示す。

a) セキュリティ属性の管理

O.MANAGE を実現するためには、セキュリティ属性の管理を特定の利用者に限定しなければならない。また、セキュリティ属性のひとつである文書データ利用者リストのデフォルト値に限定的な値をセットしなければならない。

これに対して FMT_MSA.1 は、一般ユーザーID の問い合わせ、新規作成、及び変更をユーザー管理者に許可し、一般ユーザーID の問い合わせを一般ユーザーに許可し、管理者ID の問い合わせ、及び新規作成を管理者に許可し、管理者 ID の問い合わせ、及び変更を当該管理者に許可し、管理者 ID の問い合わせをスーパーバイザーに許可し、管理者役割の問い合わせ、追加、及び削除を当該管理者役割を持った管理者に許可し、スーパーバイザーID の問い合わせ、及び変更をスーパーバイザーに許可し、文書データ利用者リストの問い合わせ、及び改変を文書管理者、文書オーナー、及び当該文書データに対してフルコントロールの文書データ操作権限を持つ一般ユーザーに許可し、文書データデフォルトアクセス権リストの問い合わせ、及び改変をユーザー管理者と当該一般ユーザーに許可する。FMT_MSA.3 は、文書データを新規蓄積する際の文書データ利用者リストのデフォルト値を限定的な値に設定する。

b) TSF データの管理と保護

O.MANAGE を実現するためには、TSF データへのアクセスを特定の利用者に限定しなければならない。

これに対して、FMT_MTD.1 は、ログインパスワード入力許容回数、ロックアウト解除タイマー設定、ロックアウト時間、及びスーパーバイザーのロックアウトフラグの問い合わせと設定、システム時計の日時と保守機能移行禁止設定の設定、HDD 暗号鍵の新規作成と問い合わせ、ならびに監査ログの問い合わせと全削除を機器管理者に限定し、システム時計の日時、保守機能移行禁止設定の問い合わせをTOEの許可利用者に許可し、パスワード最小桁数、パスワード複雑度、及び一般ユーザーのロックアウトフラグの問い合わせと設定をユーザー管理者に限定し、一般ユーザー認証情報の設定とS/MIME利用者情報の新規作成、削除、及び変更をユーザー管理者と当該一般ユーザーに限定し、S/MIME 利用者情報の問い合わせ、フォルダ配信先情報の問い合わせをユーザー管理者と一般ユーザーに限定し、管理者のロックアウトフラグの問い合わせと設定、スーパーバイザー認証情報の設定をスーパーバイザーに限定し、管理者認証情報の変更をスーパーバイザーと当該管理者に限定する。

c) 管理機能の特定

O.MANAGE を実現するためには、実装するTSF に対して必要なセキュリティ管理機能を実施しなければならない。

これに対して、FMT_SMF.1 は、セキュリティ機能要件に対する必要なセキュリティ管理機能を特定している。

d) セキュリティ管理機能の利用許可

O.MANAGE を実現するためには、セキュリティ管理機能を許可利用者役割に応じてセキュリティ管理機能の利用を許可するため、許可利用者に対してセキュリティ管理の役割とセキュリティ管理機能の操作権限を関連付け維持しなければならない。

FMT_SMR.1 は、許可利用者に対して一般ユーザー、管理者 (ユーザー管理者、機器管理者、文書管理者、ネットワーク管理者)、スーパーバイザーのうちいずれかの役割を関連付け維持する。

O.MEM.PROTECT メモリ蓄積データの暴露防止

表 22 にて O.MEM.PROTECT に対応している機能要件が、O.MEM.PROTECT を満たすのに適している根拠を以下に示す。

- a) 適切な暗号鍵生成と暗号操作をする
- O.MEM.PROTECT を実現するためには、HDD に蓄積されている文書データが、TOE を利用した正規の手段で読み出す以外は、文書データの解読が困難な形式にしなければならない。
- これに対して、FCS_CKM.1 は、BSI-AIS31 に基づく暗号鍵生成アルゴリズムTRNG で鍵長 256 ビットの暗号鍵を生成し、FCS_COP.1 は、生成された暗号鍵を使って FIPS197 に合致する暗号アルゴリズム AES で、文書データが HDD に蓄積される時に文書データを暗号化し、文書データが HDD から読み出されるときに復号する。さらに、FTP_TST.1 は TOE 起動時に、暗号鍵の正当性のテストと暗号操作をする Ic Ctlr の動作テストをテストし、文書データが暗号化されずに HDD に蓄積されることを防ぐ。

O.NET.PROTECT ネットワーク通信データの保護

表 22 にて O.NET.PROTECT に対応している機能要件が、O.NET.PROTECT を満たすのに適している根拠を以下に示す。

- a) 通信経路の資産を保護
- O.NET.PROTECT を実現するためには、通信経路上の文書データまたは印刷データを漏洩から保護し、改ざんを検知しなければならない。
- これに対して、FTP_ITC.1 は、TOE と FTP サーバー、及び TOE と SMB サーバー間のフォルダ配信において IPsec プロトコルに対応することで、ネットワーク上の文書データに対して漏洩から保護し、改ざんを検知する。また FTP_TRP.1 は、TOE とリモート利用者間に後述する高信頼パスを対応することで、ネットワーク上の文書データに対して漏洩から保護し、改ざんを検知する。TOE からクライアント PC へのメール送信サービスにおいて S/MIME でのメール送信に対応、クライアント PC からの Web サービス利用、クライアント PC からの印刷サービス利用、クライアント PC からのファクス送信サービス利用において SSL プロトコルに対応して、通信経路上の文書データまたは印刷データを漏洩から保護し、改ざんを検知する。

O.GENUINE MFP 制御ソフトウェアの完全性保護

表 22 にて O.GENUINE に対応している機能要件が、O.GENUINE を満たすのに適している根拠を以下に示す。

- a) MFP 制御ソフトウェアの完全性チェック
- O.GENUINE を実現するためには、FlashROM にインストールされている MFP 制御ソフトウェアが正規のものであること検証しなければならない。
- これに対して、FPT_TST.1 は、TOE の起動時に FlashROM にインストールされている MFP 制御ソフトウェアの実行コードの完全性をテストし正規のものであることを確認する。

O.LINE_PROTECT 電話回線からの侵入防止

表 22 にて O.LINE_PROTECT に対応している機能要件が、O.LINE_PROTECT を満たすのに適している根拠を以下に示す。

- a) ファクス回線侵入禁止
- O.LINE_PROTECT を実現するためには、攻撃者が電話回線を介して TOE へ不正アクセスすることを防止しなければならない。

これに対して、FDP_IFC.1及びFDP_IFF.1は、ファクスユニットに接続された電話回線から受信したデータの種類がファクスデータのときのみ、ファクスユニットのファクスプロセスからコントローラボードのファクス受信プロセスに受信データを通過させる。

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 での依存性の対応状況を表 23 に示す。

表 23： TOEセキュリティ機能要件の依存性対応表

TOEセキュリティ機能要件	CCが要求する依存性	STの中で満たしている依存性	STの中で満たしていない依存性
FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_STG.4	FAU_STG.1	FAU_STG.1	なし
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1	FCS_CKM.4
FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	なし
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	なし
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3	なし
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_ATD.1	なし	なし	なし
FIA_SOS.1	なし	なし	なし
FIA_UAU.2	FIA_UID.1	FIA_UID.2	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	FIA_UAU.1
FIA_UID.2	なし	なし	なし
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	なし

TOE セキュリティ機能要件	CC が要求する依存性	ST の中で満たしている依存性	ST の中で満たしていない依存性
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	なし
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	なし
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.2	FIA_UID.1
FPT_STM.1	なし	なし	なし
FPT_TST.1	なし	なし	なし
FTP_ITC.1	なし	なし	なし
FTP_TRP.1	なし	なし	なし

以下に、依存性が満たされていない場合でも問題ない根拠を記述する。

FCS_CKM.4 への依存性除去理由

本 TOE では、HDD 暗号鍵は、Ic Ctlr 内の外部からアクセスできない場所に格納される。また、TOE の運用開始時に管理者が生成した後は、暗号鍵の削除は行われず、新たな暗号鍵への上書きによる変更だけが行われる。従って、標準の方法を用いた暗号鍵廃棄の機能要件は不要である。

FIA_UAU.1 への依存性除去理由

FIA_UAU.1 の上位階層である FIA_UAU.2 を採用しているため、FIA_AFL.1、及び FIA_UAU.7 から FIA_UAU.1 への依存性は満たされる。

FIA_UID.1 への依存性除去理由

FIA_UID.1 の上位階層である FIA_UID.2 を採用しているため、FIA_UAU.2、及び FMR_SMR.1 から FIA_UID.1 への依存性は満たされる。

6.3.4 セキュリティ保証要件根拠

本 TOE は商用製品であり、一般的なオフィスで使用されることを想定し、本 TOE へは、基本レベルの攻撃能力を持つ攻撃者からの攻撃を想定する。

また、アーキテクチャ設計(ADV_TDS.2)は市販製品の正当性を示すのに十分である。さらに、TSF を回避あるいは改ざん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脆弱性分析(AVA_VAN.2)で十分である。

一方で、攻撃をより困難にするために関連情報の秘密を守る必要があり、開発環境についてもセキュアな環境であることを保証すること、すなわち開発セキュリティ(ALC_DVS.1)は重要である。

従って、評価期間及びコストを考慮すると、本 TOE に対する評価保証レベルは EAL3 が妥当である。

7 TOE 要約仕様

本章では、本 TOE のセキュリティ機能の要約仕様を記述する。

7.1 TOE セキュリティ機能

TOE は「6.1」章で記述したセキュリティ機能要件を満たすため、以下の TOE セキュリティ機能を提供する。

SF.AUDIT 監査機能

SF.I&A 利用者識別認証機能

SF.DOC_ACC 文書データアクセス制御機能

SF.SEC_MNG セキュリティ管理機能

SF.CE_OPE_LOCK 保守機能移行禁止機能

SF.CIPHER 暗号化機能

SF.NET_PROT ネットワーク通信データ保護機能

SF.FAX_LINE 電話回線 I/F 侵入防止機能

SF.GENUINE MFP 制御ソフトウェア検証機能

これら TOE セキュリティ機能は「6.1」章で記述したセキュリティ機能要件と表 24 の通り対応している。

表 24 : TOE セキュリティ機能要件と TOE セキュリティ機能の関連

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.2	X								
FAU_STG.1	X								
FAU_STG.4	X								
FCS_CKM.1						X			
FCS_COP.1						X			
FDP_ACC.1			X						
FDP_ACF.1			X						

	SF.AUDIT	SF.I&A	SF.DOC_ACC	SF.SEC_MNG	SF.CE_OPE_LOCK	SF.CIPHER	SF.NET_PROT	SF.FAX_LINE	SF.GENUINE
FDP_IFC.1								X	
FDP_IFF.1								X	
FIA_AFL.1		X		X					
FIA_ATD.1		X							
FIA_SOS.1		X							
FIA_UAU.2		X							
FIA_UAU.7		X							
FIA_UID.2		X							
FIA_USB.1		X		X					
FMT_MSA.1				X					
FMT_MSA.3				X					
FMT_MTD.1	X			X	X	X			
FMT_SMF.1		X		X					
FMT_SMR.1		X		X					
FPT_STM.1	X								
FPT_TST.1						X			X
FTP_ITC.1							X		
FTP_TRP.1							X		

以下に、これらTOE セキュリティ機能と対応するセキュリティ機能要件について記述する。

7.1.1 SF.AUDIT 監査機能

TOE は、電源が供給され TOE が起動する時に監査機能を開始し、TOE への電源が断たれるまで稼働を続ける。監査機能が稼働している間は、監査事象発生時に監査ログを記録する。記録した監査ログは、監査前に損失しないよう保護する。監査ログの読み出し、及び監査ログの全削除は機器管理者だけに許可する。

以下に、「SF.AUDIT 監査機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.1.1 監査ログの生成

TOE は、監査事象発生時に監査ログを生成し監査ログファイルへ追加する。監査ログは、共通監査情報と個別監査情報で構成される。共通監査情報は、全ての監査事象で記録するデータ項目で、個別監査情報は、監査するために付加情報を必要とする監査事象を生成する際に記録するデータ項目である。各監査

対象事象に対する監査情報を表 25 に示す。

監査ログを監査ログファイルに追加する際、監査ログファイルに空き領域が無い場合は、監査ログの事象の日時・時刻が最も古い監査ログに上書きする。

表 25：監査事象と監査情報

監査事象	監査ログ	
	共通監査情報	個別監査情報
監査機能の開始(*1)	- 事象の日付・時刻 - 事象の種別 (本表の監査事象) - サブジェクト識別情報 (※4) - 結果	-
監査機能の終了(*1)		-
ログイン		-
ロックアウトの開始		ロックアウト対象者
ロックアウトの解除(*2)		ロックアウト解除対象者 解除方法 (オートロックアウト解除/マニュアルロックアウト解除)
TOE 起動時のロックアウト解除		-
HDD 暗号鍵生成		-
文書データの蓄積の成功		操作対象文書データID
文書データの読み出しの成功 (*3)		操作対象文書データID
文書データの削除の成功		操作対象文書データID
ファクス受信		-
利用者パスワードの変更 (パスワードの新規作成、削除も含む)		他者の利用者認証情報を新規作成/変更/削除した場合の対象者 ID
管理者役割の削除		-
管理者役割の追加		-
文書データ利用者リストの変更		操作対象文書データID
システム時計の日時変更		-
高信頼 IT 製品との通信		通信先 IP アドレス
リモー 利用者との通信	-	
監査ログの全削除	-	

- : 個別監査情報はなし

*1 監査機能の開始事象は、TOEの起動事象で代用する。本 TOE では、監査機能の終了事象を記録しない。監査機能の開始と終了は、監査機能が稼動していない状態を監査するものであるが、本 TOE は、TOE の機能が動作している間は監査機能が常に稼動しており、監査機能が稼動していない状態を監査する必要はないため監査機能の終了事象を記録しなくとも監査機能として十分である。

*2 :マニュアルロックアウト解除の特別な操作となるTOEの再起動による管理者およびスーパーバイザーのロックアウト解除については、TOE の起動事象で代用する。

*3 :文書データの読み出しの成功で、操作対象文書データID に記録するのは、D-BOX に蓄積している文書データの印刷、メール送信、フォルダ配信、Web サービス機能からのダウンロードが対象となる。

*4 :共通監査情報のサブジェクト識別情報には、記録する事象が利用者の操作によって発生した事象の場合は利用者 ID、TOE が発生させた事象の場合は、利用者 ID と重複しないシステムを識別できる ID が設定される。

尚、TOE は監査ログを改変するためのインターフェースが無いため、不正な監査ログの改変はなく、監査ログを削除できる機器管理者は、管理者の特権を利用した悪意を持った不正をしない。

以上により、FAU_GEN.1(監査データ生成)、FAU_STG.1(保護された監査証跡格納)、及びFAU_STG.4(監査データ喪失の防止)は実現される。

7.1.1.2 監査ログの読み出し

TOE は、機器管理者だけに Web サービス機能から監査ログをテキスト形式で読み出すことを許可する。

以上により、FAU_SAR.1(監査レビュー)、FAU_SAR.2(限定監査レビュー)、及びFMT_MTD.1(TSF データ管理)は実現される。

7.1.1.3 監査ログの保護

TOE は、機器管理者だけに操作パネルとWeb サービス機能から監査ログを全削除することを許可する。

以上により、FAU_SAR.1(監査レビュー)、FAU_SAR.2(限定監査レビュー)、及びFMT_MTD.1(TSF データ管理)は実現される。

7.1.1.4 タイムスタンプ

TOE は、監査ログの事象の日付 時刻に、TOE 内のシステム時間の日時を提供する。

以上により、FPT_STM.1(高信頼性タイムスタンプ)は実現される。

7.1.2 SF.I&A 利用者識別認証機能

TOE は、許可利用者に役割や権限に応じた TOE の操作を許可するため、TOE のセキュリティ機能を利用するのに先立って識別認証をする。

以下に、「SF.I&A 利用者識別認証機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.2.1 利用者の識別認証

TOE は、操作パネルまたは Web サービス機能から TOE のセキュリティ機能を利用しようとする者に対してログイン画面を表示して利用者 ID とパスワードの入力を要求し、利用者によって入力された利用者 ID とパスワードで識別認証要求をする。

また TOE は、クライアント PC から、印刷要求あるいはファクス送信要求を受けたときは、クライアント PC から送信される利用者 ID とパスワードで識別認証をする。

TOE は、いずれの識別認証においても、認証に成功した利用者として、その利用者の利用者役割 (一般ユーザー、管理者、スーパーバイザー) に応じたプロセス (一般ユーザープロセス、管理者プロセス、スーパーバイザープロセス) を結合し、各プロセスにセキュリティ属性を関連付けて維持する。利用者が一般ユーザーの場合は、一般ユーザーに一般ユーザープロセスを結合し、一般ユーザープロセスに一般ユーザー ID と文書データデフォルトアクセス権リストを関連付け維持し、利用者が管理者の場合は、管理者に管理者プロセスを結合し、管理者プロセスに管理者 ID と管理者役割を関連付け維持し、利用者がスーパーバイザーの場合は、スーパーバイザーにスーパーバイザープロセスを結合し、スーパーバイザープロセスにスー

スーパーバイザーID を関連付け維持する。

認証方法は、利用者役割毎に異なる。利用者役割毎の認証方法を表 26 に記述する。

表 26：利用者役割と認証方法

利用者役割	認証方法
一般ユーザー	利用者がTOEに入力した利用者IDとパスワードが、アドレス帳に登録されている一般ユーザーIDとそのパスワードと一致することを確認する。
管理者	利用者がTOEに入力した利用者IDとパスワードが、TOEに登録されている管理者IDとそのパスワードと一致することを確認する。
スーパーバイザー	利用者がTOEに入力した利用者IDとパスワードが、TOEに登録されているスーパーバイザーIDとそのパスワードと一致することを確認する。

以上により、FIA_ATD.1(利用者属性定義)、FIA_UAU.2(アクション前の利用者認証)、FIA_UID.2(アクション前の利用者識別)、FIA_USB.1(利用者・サブジェクト結合)、FMT_SMF.1(管理機能の特定)、及びFMT_SMR.1(セキュリティ役割)は実現できる。

7.1.2.2 識別認証失敗時のアクション

TOEは、「7.1.2.1 利用者の識別認証」に記した識別認証の失敗回数を利用者ID毎にカウントし、失敗回数の累積がログインパスワード入力許容回数に達した利用者をロックアウトし、当該利用者のロックアウトフラグを「有効」にセットする。ログインパスワード入力許容回数は機器管理者が1から5回の間で設定する回数である。

また、TOEは、「7.1.2.1 利用者の識別認証」に記した識別認証で認証に成功した場合、認証に成功した利用者の失敗回数の累積をリセットし、0からカウントする。

TOEは、ロックアウトフラグが「有効」になっている利用者に対し、以下の(1)または(2)のいずれかのロックアウト解除アクションが取られた時、その利用者のロックアウトフラグを「無効」にセットし、ロックアウトを解除する。

(1) オートロックアウト解除

利用者がロックアウトになった時からロックアウト解除時間経過後の最初の識別認証時にロックアウトを解除する。ロックアウト経過時間は、機器管理者が1分から9999分(分単位)の間で設定する時間である。尚、機器管理者は、ロックアウト解除時間を無期限に設定することもできる。無期限とした場合は、利用者のロックアウトは、マニュアルロックアウト解除によってのみ解除される。

(2) マニュアルロックアウト解除

表 27 に示す利用者役割毎に決められたロックアウト解除者がWebサービス機能からロックアウト解除することを許可する。尚、特別なロックアウト解除操作として、管理者(全管理者役割)及びスーパーバイザーがロックアウトした場合は、TOEの再起動によって、そのロックアウトが解除される。

表 27：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
一般ユーザー	ユーザー管理者
管理者(全管理者役割)	スーパーバイザー

利用者役割 (ロックアウト対象者)	ロックアウト解除者
スーパーバイザー	機器管理者

以上により、FIA_AFL.1(認証失敗時の取り扱い)、及びFMT_SMF.1(管理機能の特定)は実現できる。

7.1.2.3 パスワードのフィードバックエリア保護

TOEは、一般ユーザー、管理者、スーパーバイザーが、操作パネル及びクライアントPCのWebブラウザから入力するパスワード1文字毎に、伏字(*:アスタリスク、あるいは:黒丸)を表示する。

以上により、FIA_UAU.7(保護された認証フィードバック)は実現できる。

7.1.2.4 パスワードの登録

TOEは、操作パネルとWebサービス機能から一般ユーザー、管理者、スーパーバイザーのパスワードを以下の(1)に記載する文字を使用して登録、変更する機能を提供する。

登録、変更するパスワードは、以下の(2)、(3)の条件に合致することをチェックし、条件に合致した場合はパスワードを登録し、条件に合致しない場合はパスワード登録をせずエラー表示する。

- (1) 使用できる文字とその文字種：

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)

- (2) 登録可能な桁数：

一般ユーザーの場合

ユーザー管理者が設定するパスワード最小桁数 (8から32桁) 以上、128桁以下

管理者、スーパーバイザーの場合

ユーザー管理者が設定するパスワード最小桁数 (8から32桁) 以上、32桁以下

- (3) 規則：

ユーザー管理者が設定するパスワード複雑度に準じた文字種の組合せで作成したパスワードの登録を許可する。ユーザー管理者は、パスワード複雑度に複雑度1か複雑度2を設定する。

以上により、FIA_SOS.1(秘密の検証)、及びFMT_SMF.1(管理機能の特定)は実現できる。

7.1.3 SF.DOC_ACC 文書データアクセス制御機能

TOEは、利用者による文書データの蓄積、読み出し、削除の操作をアクセス制御する。文書データのアクセス制御は、識別認証機能で認証された許可利用者の利用者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、アクセス可能な文書データだけを許可利用者が認証された操作パネル、あるいはクライアントPCに表示する。本章では、文書データのアクセス制御を利用者役割毎に記述する。

以下に、「SF.DOC_ACC 文書データアクセス制御機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.3.1 一般ユーザーの文書データ操作

TOE は、文書データの蓄積を一般ユーザーに許可し、蓄積されている文書データの読み出し、削除の操作を文書データ利用者リストに従って許可する。文書データ利用者リストには、文書データの操作を許可する一般ユーザーの一般ユーザーID と文書データ操作権限が記録されている。TOE は、一般ユーザープロセスに関連付けられている一般ユーザーID が、文書データ利用者リストに登録されていれば、その一般ユーザーID の文書データ操作権限の範囲で操作を許可する。

文書データ操作権限と文書データ操作対応の関係を表 2 に示す。

尚、文書データを蓄積した際の、文書データ利用者リストの値は表 28 に記述する値とする。

表 28 : 文書データ利用者リストの初期値

文書データのタイプ	文書データ利用者リストの初期値
一般ユーザーが蓄積する文書データ	文書データデフォルトアクセス権リスト

以上により、FDP_ACC.1(サブセットアクセス制御)、及び FDP_ACF.1(セキュリティ属性によるアクセス制御)は実現できる。

7.1.3.2 文書管理者の文書データ操作

TOE は、操作パネルまたは Web サービス機能からログインしている利用者が文書管理者である場合、その利用者に対して文書データを一覧表示し、選択した文書データまたは表示された全ての文書データを全削除することを許可する。

以上により、FDP_ACC.1(サブセットアクセス制御)、及び FDP_ACF.1(セキュリティ属性によるアクセス制御)は実現できる。

7.1.4 SF.SEC_MNG セキュリティ管理機能

TOE は「SF.I&A 利用者識別認証機能」で識別認証された利用者の利用者役割に応じたセキュリティ管理機能を提供する。

以下に、「SF.SEC_MNG セキュリティ管理機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.4.1 文書データ利用者リスト管理

文書データ利用者リスト管理とは、操作パネルまたは Web サービス機能から文書データ利用者リストの操作を特定の利用者だけに許可する機能である。文書データ利用者リストへの操作には、文書オーナーの変更、文書オーナーの文書データ操作権限変更、文書利用者の新規登録、文書利用者の削除、及び文書利用者の文書データ操作権限変更があり、それぞれに操作することを許可される利用者が決められている。文書データ利用者リストへの操作と操作を許可された利用者の関係を表 29 に記述する。

表 29 : 文書データ利用者リストへの操作と操作可能者

文書データ利用者リストへの操作	操作可能者
文書オーナーの変更	- 文書管理者

文書オーナーの文書データ操作権限変更	- 文書管理者 - 文書オーナー - フルコントロール権限を持つ一般ユーザー
文書利用者の新規登録	- 文書管理者 - 文書オーナー - フルコントロール権限を持つ一般ユーザー
文書利用者の削除	- 文書管理者 - 文書オーナー - フルコントロール権限を持つ一般ユーザー
文書利用者の文書データ操作権限変更	- 文書管理者 - 文書オーナー - フルコントロール権限を持つ一般ユーザー

TOE は、ログインしている利用者が文書管理者ならば、全ての文書データ利用者リストに対して文書オーナーの変更、文書オーナーのアクセス権変更、文書利用者の新規登録、文書利用者の削除、および文書利用者のアクセス権変更の操作を許可する。

ログインしている利用者が一般ユーザーならば、その一般ユーザーがフルコントロール権限で設定されている文書データ利用者リストに対してだけ、文書オーナーの文書データ操作権限変更、文書利用者の新規登録、文書利用者の削除、及び文書利用者の文書データ操作権限変更の操作を許可する。ただし、文書オーナーは、フルコントロール権限が設定されていなくとも、オーナーになっている文書データの文書データ利用者リストを文書オーナーの文書データ操作権限変更、文書利用者の新規登録、文書利用者の削除、文書利用者の文書データ操作権限変更を許可する。

以上により、FMT_MSA.1(セキュリティ属性の管理)、FMT_MSA.3(静的属性初期化)、及び FMT_SMF.1(管理機能の特定)は実現される。

7.1.4.2 管理者情報管理

管理者情報管理は、操作パネルまたは Web サービス機能から管理者情報に関する操作を特定の利用者だけに許可する機能である。

管理者情報には、管理者 ID、管理者認証情報、管理者役割がある。管理者情報の操作には、管理者 ID の新規作成、問い合わせ、及び変更、管理者認証情報の変更、及び管理者役割の問い合わせ、追加、及び削除があり、それぞれ操作を許可される利用者が決められている。管理者情報の操作と、管理者情報の操作を許可される利用者の関係を表 30 に記述する。

表 30 : 管理者情報へのアクセス

管理者情報の操作	操作可能者
管理者 ID の新規作成	管理者
管理者 ID の変更	当該管理者
管理者 ID の問い合わせ	当該管理者、スーパーバイザー
管理者認証情報の変更	当該管理者、スーパーバイザー
管理者役割の追加、問い合わせ	当該管理者役割を持つ管理者
管理者役割の削除	当該管理者役割を持つ管理者 ただし、他に当該管理者役割を持つ管理者がない場合は不可

TOE は、ログインしている利用者が管理者あるいはスーパーバイザーならば、それぞれに表 30 に記述した操作を許可する。

以上により、FIA_USB.1(利用者・サブジェクト結合)、FMT_MSA.1(セキュリティ属性の管理)、FMT_MTD.1(TSF データの管理)、FMT_SMF.1(管理機能の特定)、及びFMT_SMR.1(セキュリティ役割)は実現される。

7.1.4.3 スーパーバイザー情報管理

スーパーバイザー情報管理は、スーパーバイザーID の問い合わせと変更、およびスーパーバイザー認証情報の変更を操作パネルまたは Web サービス機能からスーパーバイザーだけに許可する機能である。

TOE は、操作パネルまたはクライアントPC からログインした利用者がスーパーバイザーならば、スーパーバイザーID の問い合わせと変更、およびスーパーバイザー認証情報を変更することを許可する。

以上により、FMT_MSA.1(セキュリティ属性の管理)、FMT_MTD.1(TSF データの管理)、FMT_SMF.1(管理機能の特定)、及びFMT_SMR.1(セキュリティ役割)は実現される。

7.1.4.4 一般ユーザー情報管理

一般ユーザー情報管理は、一般ユーザーID、一般ユーザー認証情報、文書データデフォルトアクセス権リスト、及びS/MIME利用者情報を含む一般ユーザー情報の新規作成、変更、削除の全部または一部操作を操作パネルまたは Web サービス機能から特定の利用者に許可する機能である。

TOE は、操作パネルまたは Web サービス機能からログインしている利用者が、ユーザー管理者、または一般ユーザーならば、その利用者に対して表 31 に記述する操作を許可する。

表 31：一般ユーザー情報に対する許可操作

一般ユーザー情報に対する操作	操作可能者
アドレス帳へ一般ユーザー情報の新規作成 (一般ユーザーID、一般ユーザー認証情報、S/MIME 利用者情報)	ユーザー管理者
アドレス帳に登録されている一般ユーザー情報の編集 (一般ユーザー認証情報、文書データデフォルトアクセス権リスト、S/MIME利用者情報)	ユーザー管理者 一般ユーザー情報の当該一般ユーザー
アドレス帳に登録されている一般ユーザー情報の問い合わせ (一般ユーザーID、文書データデフォルトアクセス権リスト、S/MIME利用者情報)	ユーザー管理者 一般ユーザー情報の当該一般ユーザー
アドレス帳に登録されている一般ユーザー情報の問い合わせ (一般ユーザーID、S/MIME利用者情報)	一般ユーザー
アドレス帳に登録されている一般ユーザー情報の削除 (一般ユーザーID、一般ユーザー認証情報、S/MIME 利用者情報)	ユーザー管理者
アドレス帳に登録されている一般ユーザー情報の削除 (S/MIME利用者情報)	S/MIME利用者情報の当該一般ユーザー

尚、一般ユーザー情報を新規作成した際の、文書データデフォルトアクセス権リストの値は、新規作成する一般ユーザーID が文書オーナーとして設定され、文書データに許可される操作は文書データの読み出しと文書データ利用者リストの改変になる。

以上により、FMT_MSA.1(セキュリティ属性の管理)、FMT_MTD.1(TSF データの管理)、FMT_SMF.1(管理機能の特定)、及びFMT_SMR.1(セキュリティ役割)は実現される。

7.1.4.5 機器制御データ管理

機器制御データ管理は、機器制御データの設定を特定の利用者だけに許可する機能である。

TOE は、機器制御データを設定する機能を、特定の利用者に特定の箇所から許可する。TOE が許可する機器制御データ毎の設定値の範囲、操作、設定許可者、及び設定箇所を表 32 に示す。

尚、TOE は、ユーザー管理者と一般ユーザーにフォルダ配信先情報の問い合わせを許可する。

表 32 : 機器制御データの管理者リスト

機器制御データ項目	設定値の範囲	操作	設定許可者	設定箇所
ログインパスワード入力許容回数	1~ 5(回)の整数値	問い合わせ、 改変	機器管理者	Web サービス機能
ロックアウト解除タイム設定	有効または無効	問い合わせ、 改変	機器管理者	Web サービス機能
ロックアウト時間	1~ 9999(分)の整数値	問い合わせ、 改変	機器管理者	Web サービス機能
パスワード最小桁数	8~ 32(桁)の整数値	問い合わせ、 改変	ユーザー管理者	操作パネル
パスワード複雑度	複雑度 1 または 複雑度 2	問い合わせ、 改変	ユーザー管理者	操作パネル
システム時計の日時	年月日、時刻 (時、分、秒)	問い合わせ、 改変	機器管理者	操作パネル、 Web サービス機能
		問い合わせ	一般ユーザー、 ユーザー管理者、 ネットワーク管理者、 文書管理者、 スーパーバイザー	
一般ユーザーのロックアウトフラグ	無効	問い合わせ、 改変	ユーザー管理者	Web サービス機能
管理者のロックアウトフラグ	無効	問い合わせ、 改変	スーパーバイザー	Web サービス機能
スーパーバイザーのロックアウトフラグ	無効	問い合わせ、 改変	機器管理者	Web サービス機能

以上により、FIA_AFL.1(認証失敗時の取り扱い)、FMT_MTD.1(TSF データの管理)、FMT_SMF.1(管理機能の特定)、及びFMT_SMR.1(セキュリティ役割)は実現できる。

7.1.5 SF.CE_OPE_LOCK 保守機能移行禁止機能

保守機能移行禁止機能は、機器管理者が設定する保守機能移行禁止設定の設定値に従って、CE の保守機能利用を制御する機能である。

TOE は、操作パネルから保守機能移行禁止設定を設定する機能を機器管理者に提供し、全ての許可利用者に設定値を参照する機能を提供する。保守機能移行禁止設定が「しない」の場合は CE が保守機能を実行することを許可し、保守機能移行禁止設定が「する」の場合は、CE が保守機能を利用することを許可しない。

以上により、FMT_MTD.1(TSF データの管理)は実現される。

7.1.6 SF.CIPHER 暗号化機能

TOE は、HDD に蓄積する文書データを暗号化する。

以下に、「SF.CIPHER 暗号化機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.6.1 文書データの暗号化

TOE は、HDD に書き込む直前にデータを Ic Ctr で暗号化し、HDD から読み出した直後にデータを Ic Ctr で復号する。この処理は、HDD に書き込み読み出しする全てのデータに対して行われ、文書データも同様に TOE によって暗号化/復号される。

HDD 暗号鍵は、機器管理者が生成する。TOE は、ログインしている利用者が機器管理者の場合、HDD 暗号鍵を生成するための画面を操作パネルから提供する。

機器管理者が操作パネルから HDD 暗号鍵の生成を指示すると、TOE は、標準 BSI-AIS31 に準拠した暗号鍵生成アルゴリズム TRNG で 256 ビットの HDD 暗号鍵を生成し、HDD のデータ書き込み/読み出しの際には表 33 に示す暗号操作を実施する。

表 33 : HDD 蓄積データ暗号操作のリスト

暗号操作のトリガ	暗号操作	標準	暗号アルゴリズム	鍵長
HDD へのデータ書き込み	暗号化	FIPS197	AES	256 ビット
HDD からのデータ読み出し	復号			

HDD 暗号鍵は印刷することもできる。TOE は、ログインしている利用者が機器管理者の場合、HDD 暗号鍵の印刷をするための画面を操作パネルから機器管理者に提供する。印刷した暗号鍵は、TOE 内の暗号鍵が壊れた場合に、暗号鍵を復旧するために使用する。

また TOE は、起動時に Ic Ctr の暗号化機能が正常に動作することと、HDD 暗号鍵の完全性を検証する。

HDD 暗号鍵の完全性が確認できなかった場合は、HDD 暗号鍵が変更されていることを表示する。

以上により、FCS_CKM.1(暗号鍵生成)、FCS_COP.1(暗号操作)、FMT_MTD.1(TSF データの管理)、及び FPT_TST.1(TSF テスト)は実現される。

7.1.7 SF.NET_PROT ネットワーク通信データ保護機能

ネットワーク通信データ保護機能は、内部ネットワーク上を流れる文書データ、印刷データを漏洩から保護し、文書データ、印刷データの改ざんを検知する機能である。

以下に、「SF.NET_PROT ネットワーク通信データ保護機能」の機能項目の説明と対応するセキュリティ機能要件を記述する。

7.1.7.1 クライアント PC からの Web サービス機能利用

TOE は、クライアント PC から Web サービス機能を利用する要求があると、クライアント PC と TOE 間を高信頼パスとして SSL プロトコルで接続する。

以上により、FTP_TRP.1(高信頼パス)は実現される。

7.1.7.2 クライアント PC からの印刷とファクス送信

TOE は、クライアント PC から印刷要求、あるいはファクス送信要求を受信すると、クライアント PC と TOE 間を高信頼パスとして SSL プロトコルで接続する。

以上により、FTP_TRP.1(高信頼パス)は実現される。

7.1.7.3 TOE からのメール送信

TOE は、TOE からクライアント PC に文書データをメール送信する際に、文書データを電子メールに添付し、その電子メールを S/MIME 送信する。尚、S/MIME 送信先情報は、一般ユーザー情報の S/MIME 利用者情報として管理され、利用者はこの管理された送信先情報のみを使用してメール送信する。

以上により、FTP_TRP.1(高信頼パス)は実現される。

7.1.7.4 TOE からのフォルダ配信

TOE は、TOE から SMB サーバー、または FTP サーバーにフォルダ配信する際、TOE と SMB サーバー間、または TOE と FTP サーバー間を高信頼チャンネルとして IPsec プロトコルで接続する。尚、フォルダ配信先情報は、予め TOE に機器制御データとして登録管理され、利用者はこの管理された配信先情報のみを使用してフォルダ配信する。

以上により、FTP_ITC.1(TSF 間高信頼チャンネル)は実現される。

7.1.8 SF.FAX_LINE 電話回線 I/F 侵入防止機能

TOE は、ファクスユニットが電話回線から受信したデータの種別がファクスデータの場合は、受信データをコントローラボードに引渡し、受信したデータの種別がファクスデータ以外の場合は、受信したデータをコントローラボードに渡さず読み捨てる。

以上により、FDP_IFC.1(サブセット情報制御フロー)、及び FDP_IFF.1(単純セキュリティ属性)は実現される。

7.1.9 SF.GENUINE MFP 制御ソフトウェア検証機能

MFP 制御ソフトウェア検証機能は、TOE 起動時に FlashROM にインストールされている MFP 制御ソフトウェアが正規のものであることを確認する機能である。

TOE は、TOE 起動時に MFP 制御ソフトウェアの実行コードの完全性をチェックする。完全性が確認できた場合は、利用者が TOE を利用できる状態にする。完全性が確認できなかった場合は、MFP 制御ソフトウェアが正規のものでなかったことを表示する。

以上により、FPT_TST.1(TSF テスト)は実現される。

8 付録

8.1 用語の説明

本 ST を明確に理解するために、特定の用語の意味を表 34 に定義する。

表 34 : 本 ST に関連する特定の用語

用語	定義
D-BOX	HDD 上の文書データを格納する領域。
FTP サーバー	File Transfer Protocol (ファイル転送プロトコル) を用いて、クライアントとファイルを送受信するためのサーバー。
HDD	ハードディスクドライブの略称。TOE 内に取り付けられた HDD を指す。
Ic Ctr	HDD に書込むデータを暗号化し、HDD から読み込むデータを復号するハードウェア装置。
Ic Key	暗号処理専用のマイクロプロセッサと、セキュア通信で利用される秘密鍵を含んだ EEPROM が内蔵されたチップ。 正当性確認や暗号処理などに利用する鍵と乱数の種が保管されている。
IP-ファクス	TCP/IP を使用しているネットワークに直接接続されたファクス同士で文書の送受信をする機能のこと。また、電話回線に接続されたファクスに文書を送信することもできる。
MFP	デジタル複合機の略称。本 ST では TOE を指す。
MFP 管理責任者	MFP を設置する組織の中で、MFP の管理者とスーパーバイザーを選任する権限を持った者 (あるいは、組織の責任者)。 例 MFP の購入者、MFP の所有者、MFP を設置する部署の責任者、IT 部門の責任者。
MFP 制御ソフトウェア	TOE に組込むソフトウェアの 1 つで、TOE を識別する要素のうち、System/Copy、Network Support、Scanner、Printer、Fax、Web Support、Web Uapl、Network Doc Box を含んでいる。 MFP を構成するユニットやデバイスのリソース管理を行ない、動作を制御する。
MFP 制御データ	MFP の動作を決定する設定値項目の総称。
PC ファクス送信	クライアント PC をネットワークまたは USB で接続し、クライアント PC 内の文書データを、TOE を介してファクス送信する機能のこと。
S/MIME 利用者情報	S/MIME を利用するにあたって必要となる一般ユーザー毎の情報。 メールアドレス、ユーザー証明書、S/MIME 利用規定値が含まれる。
SMB サーバー	Server Message Block (サーバメッセージブロック) プロトコルを用いて、クライアントとファイルを共有するためのサーバー。
SMTP サーバー	Simple Mail Transfer Protocol (簡易メール転送プロトコル) を用いて、電子メールを送信するためのサーバー。
アドレス帳	一般ユーザー情報をレコードとして登録したデータ。

用語	定義
アドレス帳のバックアップ/リストア	アドレス帳をSDカードにバックアップ、あるいはSDカードにバックアップしているアドレス帳をTOEにリストアすること。
インターネットファクス	ファクスの原稿を読み込んでからE-Mail形式に変換し、インターネットを使ってメールアドレスを持っている機器に送信する機能のこと。
カスタマー・エンジニア (CE)	メーカー、サービス会社、販売会社に所属して TOE の保守をする専門知識を有する者。
コントローラボードのファクス受信プロセス	ファクスユニットからのファクス通信状態の受信、及びファクスユニットへのファクス通信指示を行う、コントローラボード内のMFP制御ソフトウェア。
スーパーバイザー	TOEの許可利用者のひとつで、管理者のパスワードを管理する者。
スーパーバイザーID	スーパーバイザー情報のデータ項目であり、スーパーバイザーを識別認証するための識別符号。本 TOE においては、スーパーバイザーのログインユーザー名を指す。
スーパーバイザー認証情報	スーパーバイザー識別認証用のパスワード。
ネットワーク管理	管理者役割のひとつで、TOE ネットワーク接続の管理を実施する役割。ネットワーク管理の役割を持った管理者をネットワーク管理者と言う。
ネットワーク制御データ	MFP 制御データのうち、MFP をネットワークに接続するためのデータ項目。
パスワード最小桁数	登録可能なパスワードの最小桁数。
パスワード複雑度	登録可能なパスワードの文字種組合せ数の最小数。 文字種は、英大文字、英小文字、数字、記号の4種がある。 パスワード複雑度には、複雑度1と複雑度2がある。複雑度1の場合は2種類以上の文字種、複雑度2の場合は3種類以上の文字種を組合せてパスワードを作らなければならない。
ファクスユニットのファクスプロセス	コントローラボードの MFP 制御ソフトウェアにファクス通信状態通知、及びコントローラボードの MFP 制御ソフトウェアの指示によってファクス通信を行う、ファクスユニット内の制御ソフトウェア。
フォルダ配信	TOE からネットワーク経由でSMB サーバー、FTP サーバーのフォルダに文書データを送信する機能のこと。
メール送信	TOE から文書データを添付した電子メールを送信する機能のこと。
メモリ送信	スキャンした原稿をメモリに蓄積してからダイヤルし、ファクスデータをファクス送信する機能のこと。
ユーザー管理	管理者役割のひとつで、一般ユーザーの管理を実施する役割。ユーザー管理の役割を持った管理者をユーザー管理者と言う。
ログインパスワード入力許容回数	同一利用者 ID で、パスワード認証失敗によりロックアウトとなるまでの回数。
ロックアウト	特定の利用者 ID に対して TOE へのアクセスを禁止すること。
ロックアウトフラグ	許可利用者毎に割り付けられるデータで、ロックアウトされた利用者のロックアウトフラグは「有効」にセットされ、ロックアウト解除された利用者のロックアウトフラグは「無効」にリセットされる。ロックアウトフラグの操作が許可された管理者またはスーパーバイザーは、ロックアウトされた利用者のロックアウトフラグを「無効」に設定することで、ロックアウトされた利用者のロックアウトを解除できる。

用語	定義
ロックアウト解除タイムー設定	管理者が予め設定した時間でロックアウトが解除される動作を有効または無効にする設定。この設定が無効の場合は、管理者が直接操作することでロックアウトが解除される。
一般ユーザー	TOE の許可利用者のひとつで、TOE の基本機能を利用する者。
一般ユーザーID	一般ユーザー情報のデータ項目であり、一般ユーザーを識別認証するための識別符号。本 TOE においては、一般ユーザーのログインユーザー名を指す。
一般ユーザー情報	一般ユーザーに関する情報がデータ項目として構成されているレコード。データ項目には、一般ユーザーID、一般ユーザー認証情報、文書データデフォルトアクセス権リスト、S/MIME 利用者情報が含まれる。
一般ユーザー認証情報	一般ユーザー識別認証用のパスワード。
印刷データ	クライアントPC 内の文書を、印刷またはファクス送信するためにクライアントPC から TOE へ送信するデータ。印刷データを印刷するためにはプリンタドライバ、ファクス送信するためにはファクスドライバをクライアントPC にインストールしておく必要がある。 印刷データはネットワークユニット及びUSB ポートからTOE に取り込まれる。
印刷条件	印刷時の用紙サイズ、変倍率、加工印刷情報(両面、集約など)のこと。蓄積している文書データの印刷条件は、その文書データを印刷する利用者に応じて更新される。
外部ネットワーク	MFP が設置されている組織が管理できないネットワーク。一般的には汎用インターネットのことを指す。
管理者	TOE の許可利用者のひとつで、TOE を管理する者。管理者には、管理者役割が付与され、管理者役割に沿った管理作業を実施する。管理者は4名まで登録でき、1つ以上の管理者役割が付与される。
管理者ID	管理者情報のデータ項目であり、管理者を識別認証するための識別符号。本 TOE においては、管理者のログインユーザー名を指す。
管理者認証情報	管理者識別認証用のパスワード。
管理者役割	管理者に付与する管理機能。管理者役割にはユーザー管理、機器管理、ネットワーク管理、文書管理の4つがあり、それぞれの管理者役割は、登録されている管理者のいずれかに割り当てられる。
機器管理	管理者役割のひとつで、機器の管理、及び監査を実施する役割。機器管理の役割を持った管理者を機器管理者と言う
機器制御データ	MFP 制御データのうち、セキュリティ機能のふるまいに係わるデータ項目。
操作パネル	タッチパネル付き液晶ディスプレイ、ハードキー、LED で構成され、利用者がMFP の操作に利用する表示入力装置。 操作パネルユニットとも言う。
蓄積データ保護機能	HDD に記録されている文書データを漏洩から保護する機能。
蓄積印刷	TOE が受信した印刷データを文書データに変換しD-BOX に蓄積する機能のこと。D-BOX に蓄積した文書データは、後から印刷することができる。
蓄積文書ファクス送信	予めファクス送信のためにD-BOX に蓄積されている文書データをファクス送信する機能のこと。
直接印刷	TOE が受信した印刷データを、用紙に印刷する機能のこと。

用語	定義
直接送信	原稿スキャン前にダイヤルし、原稿をスキャンしながらファクスデータをファクス送信する機能のこと。
内部ネットワーク	MFP が設置されている組織が管理するネットワーク。通常はイントラネットとして構築されているオフィス内 LAN 環境のこと。
文書オーナー	文書データの所有者として文書データ利用者リストに登録された一般ユーザーのこと。
文書データ	MFP の許可利用者が、以下に記す通りの操作のいずれかで MFP に取込んだ電子データ。 1. MFP の許可利用者の操作によって、紙原稿のイメージをスキャンしデジタル化した電子データ。 2. MFP の許可利用者が MFP に送信した印刷データを、MFP が受信し MFP が扱った形式にした電子データ。
文書データデフォルトアクセス権リスト	一般ユーザー情報のデータ項目のひとつ。 新規で蓄積する文書データの文書データ利用者リストに設定するデフォルト値のこと。
文書データ利用者リスト	文書データ毎に設定される一般ユーザーのアクセス制御リスト。
文書管理	管理者役割のひとつで、TOE に蓄積されている文書データが保存されている D-BOX と、文書データのアクセス制御リストである文書データ利用者リストの管理を実施する役割。文書管理の役割を持った管理者を文書管理者と言う。
文書利用者	文書データ利用者リストに登録された、文書オーナーを除く一般ユーザーのこと。

8.2 参考資料

以下に本書を作成する際に参考にした資料を示す。

- CC バージョン 3.1 改訂第 2 版

評価基準：

英語版」

Common Criteria for Information Technology Security Evaluation Version 3.1

Part 1: Introduction and general model Revision 1 (CCMB-2006-09-001)

Part 2: Security functional components Revision 2 (CCMB-2007-09-002)

Part 3: Security assurance components Revision 2 (CCMB-2007-09-003)

翻訳版」

情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1

パート1: 概説と一般モデル 改訂第 1 版 [翻訳第 1.2 版]

パート2: セキュリティ機能コンポーネント 改訂第 2 版 [翻訳第 2.0 版]

パート3: セキュリティ保証コンポーネント 改訂第 2 版 [翻訳第 2.0 版]

評価方法：

英語版」

Common Methodology for Information Technology Security Evaluation Version 3.1
Evaluation methodology Revision 2(CCMB-2007-09-0004)

翻訳版」

情報技術セキュリティ評価のための共通方法 バージョン3.1
評価方法 改訂第2版[翻訳第2.0版]