EPSON
EXCEED YOUR VISION

EPSON LX-10020M/WF-M21000 with FAX
セキュリティターゲット

ST バージョン：Rev.05

作成日：2021 年 07 月 30 日

作成者：セイコーエプソン株式会社

改訂履歴

Rev.	改訂部	改訂内容	設計部門			制定・改訂 年月日
			作成	確認	承認	
01	・ 全章	・ 新規作成	吉岡	河原 仁木	成澤	2021/03/12
02	・ 1.1, 1.4 ・ 6.1, 7.4 ・ 6.1, 7.2	・ 指摘事項修正 ・ 指摘事項修正 ・ 誤記訂正	吉岡	河原 仁木	成澤	2021/04/05
03	・ 1.1, 1.2, 1.4	・ 誤記訂正	吉岡	河原 仁木	成澤	2021/05/12
04	・ 1.1, 1.4	・ 誤記訂正	吉岡	河原 仁木	成澤	2021/05/28
05	・ 1.1, 1.4, 1.5 ・ 3.1, 3.3, 3.4 ・ 3.5, 6.3	・ 指摘事項修正 ・ 指摘事項修正 ・ 指摘事項修正	吉岡	河原 仁木	成澤	2021/07/30

目次

1. ST Introduction

本章は、ST 参照、TOE 参照、TOE 概要、及び TOE 記述を記す。

1.1. ST Reference

ST 名称: EPSON LX-10020M/WF-M21000 with FAX セキュリティターゲット
ST バージョン: Rev.05
作成日: 2021/07/30
作成者: セイコーエプソン株式会社

1.2. TOE Reference

TOE の識別情報を以下に示す。
TOE 名称: EPSON LX-10020M/WF-M21000 with FAX
TOE バージョン: 1.00
製造者: セイコーエプソン株式会社

TOE は、MFP 本体(日本:LX-10020M、海外:WF-M21000 のいずれか)と FAX(日本:Super G3/G3 Multi Fax Board / PR3FB0、海外:Super G3/G3 Multi Fax Board / PR3FB1)とファームウェア(GR12L4)で構成される。TOE であることは、MFP 本体の型番、FAX の識別情報、ファームウェアの識別情報で確認することができる。

1.3. TOE Overview

本章は、TOE の種別、TOE の使用方法、及び TOE の主要なセキュリティ機能を記す。

1.3.1.TOE の種別

本 ST にて定義する TOE は、LAN 環境で使用され、プリント機能、スキャン機能、コピー機能、FAX 機能及びドキュメントを蓄積する機能を有するデジタル複合機（以下、MFP と略す）のことである。

1.3.2.TOE の使用方法

本 TOE の利用環境を図 1-1 に示す。

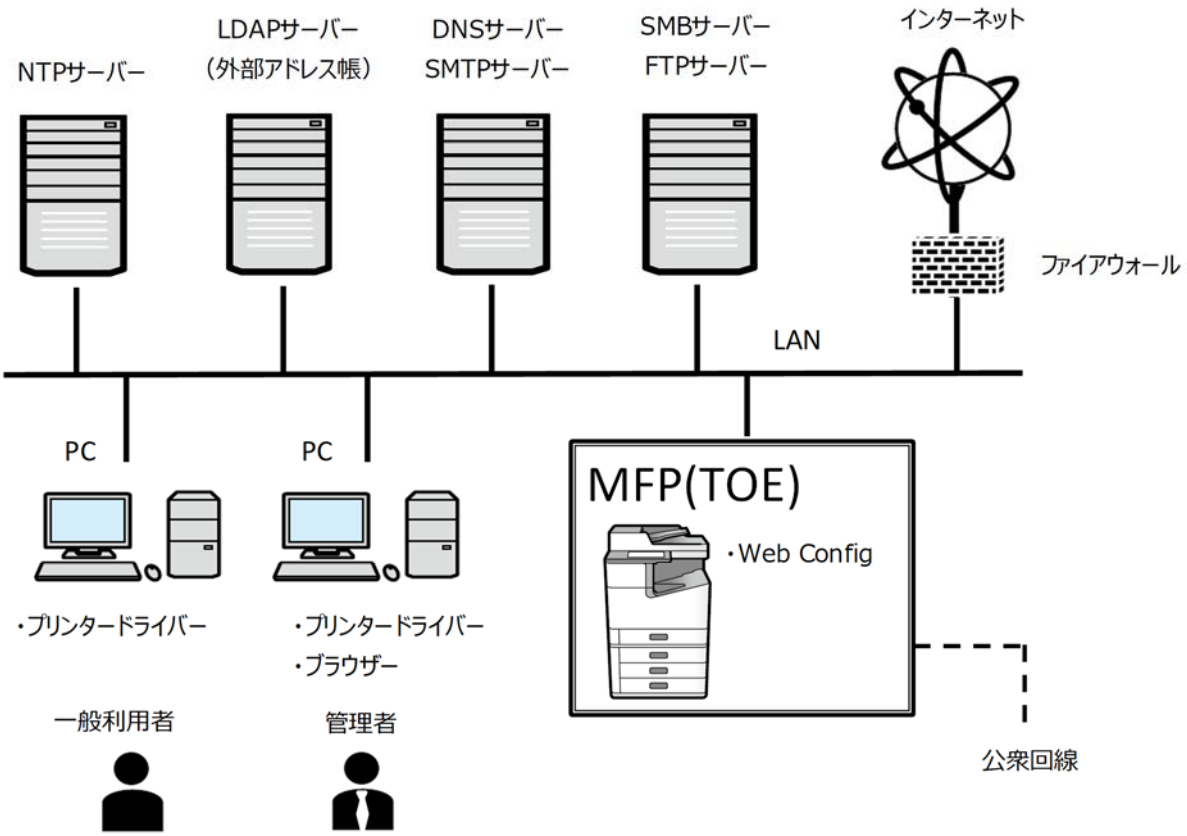

図 1-1. TOE の利用環境

TOE は LAN と公衆回線に接続して使用する。利用者は TOE が備える操作パネルまたは LAN を介して通信することにより、TOE を操作することができる。図 1-1 の各要素に関して、以下に説明する。

(1) MFP

MFP（Multi Function Peripheral）とは、複数の異なる機能（プリンター、スキャナー、コピー、FAX 等）を併せ持つコンピュータ周辺機器のこと。

(2) LAN

LAN（Local Area Network）とは、ケーブルや無線などを使用して、同じ建物の中にあるコンピュータや通信機器、プリンターなどを接続し、データをやり取りするネットワークのこと。

(3) 公衆回線

公衆回線とは、一般の加入電話回線のこと。FAX の送受信に使用する。

(4) ファイアウォール

ファイアウォールとは、あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。

(5) PC

PC（Personal Computer）とは、個人向けの小型、低価格の汎用コンピュータ製品のこと。

(6) NTP サーバー

NTP（Network Time Protocol）にて現在時刻のデータを配信するサーバーソフトウェアのこと。

(7) LDAP サーバー（外部アドレス帳）

LDAP サーバーとは、LDAP（Light Directory Access Protocol）を利用して、インターネットなどの TCP/IP ネットワークにおいて標準的に使用されるディレクトリサービスにアクセスするためのサーバーソフトウェアのこと。また、そのような LDAP サーバーソフトウェアが動作しているサーバー機体を指す。LDAP サーバーにてアドレス帳を管理し、FAX データの宛先指定に使用する。

(8) DNS サーバー / SMTP サーバー

DNS サーバーとは、DNS（Domain Name System）を利用して、内部ネットワーク内の各サーバー名を IP アドレスに変換するためのサーバーソフトウェアのこと。また、そのような DNS サーバーソフトウェアが動作しているサーバー機体を指す。SMTP サーバーとは、SMTP（Simple Mail Transfer Protocol）を利用して、インターネットなどの TCP/IP ネットワークにおいて標準的に使用されるメールを伝送するためのサーバーソフトウェアのこと。また、そのような SMTP サーバーソフトウェアが動作しているサーバー機体を指す。スキャンデータのメール送信用に使用する。DNS サーバーと SMTP サーバーは、独立して設置しても良い。

(9) SMB サーバー / FTP サーバー

SMB サーバーとは、SMB（Server Message Block）を利用して、ネットワーク（LAN）上の複数の Windows コンピュータ間にてファイル共有やプリンター共有などを行うためのサーバーソフトウェアのこと。また、そのような SMB サーバーソフトウェアが動作しているサーバー機体を指す。

FTP サーバーとは、FTP（File Transfer Protocol）を利用して、ファイルの送受信を行うためのサーバーソフトウェアのこと。また、そのような FTP サーバーソフトウェアが動作しているサーバー機体を指す。

これらサーバーは、スキャンデータ及び FAX 受信データの転送用に使用する。

(10) プリンタードライバー

プリンタードライバーとは、コンピュータからプリンターに接続して操作するために必要なソフトウェアのこと。OS にハードウェア制御の機能を追加するデバイスドライバーの一種であり、通常はプリンターの機種ごと、及び OS の種類ごとに固有のものが必要となる。

(11) ブラウザー

ブラウザーとは、データや情報をまとまった形で閲覧するためのソフトウェアのこと。

(12) Web Config

セイコーエプソン製 MFP に内蔵された機能のこと。プリンターまたは複合機の IP アドレスに対して、ブラウザー経由にてアクセスすることにより、各種設定（プリント設定、ネットワーク設定、利用者制限設定、管理者パスワード設定等）を行うことが可能となる。

1.3.3.TOE の主要なセキュリティ機能

本 TOE の主要なセキュリティ機能を以下に記す。

(1) ユーザ識別・認証機能

TOE に対する利用者を識別認証する機能

(2) 利用者データアクセス制御機能

利用者データに対する操作を制御する機能

(3) TOE 機能アクセス制御機能

TOE 機能を制御する機能

(4) セキュリティ管理機能

セキュリティ機能を管理する機能

(5) 残存データ消去機能

削除された文書及び一時的に保存された文書を HDD 及び Flash ROM から完全に消去し、再利用不可とする機能

(6) 自己テスト機能

TSF の一部及び TSF 実行コードが正常であることを MFP 本体起動時に検証する機能

(7) 監査ログ機能

TOE の使用及びセキュリティ関連事象を監査ログとして記録し、参照する機能

(8) ネットワーク保護機能

LAN 利用時、ネットワークの盗聴による情報漏えい及び改変を防止する機能

1.4. TOE Description

本章は、利用者定義、TOE の物理的範囲、ガイダンス、TOE の論理的範囲、及び TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを記す。

1.4.1.利用者定義

本 TOE の利用者を表 1-1 に示す

表 1-1. 利用者定義

名称		定義
U.USER 利用者		Any authorized User.
	U.NORMAL 一般利用者	A User who is authorized to perform User Document Data processing functions of the TOE.
	U.ADMINISTRATOR 管理者	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

1.4.2.TOE の物理的範囲

本 TOE の物理的範囲を図 1-2 に示す。

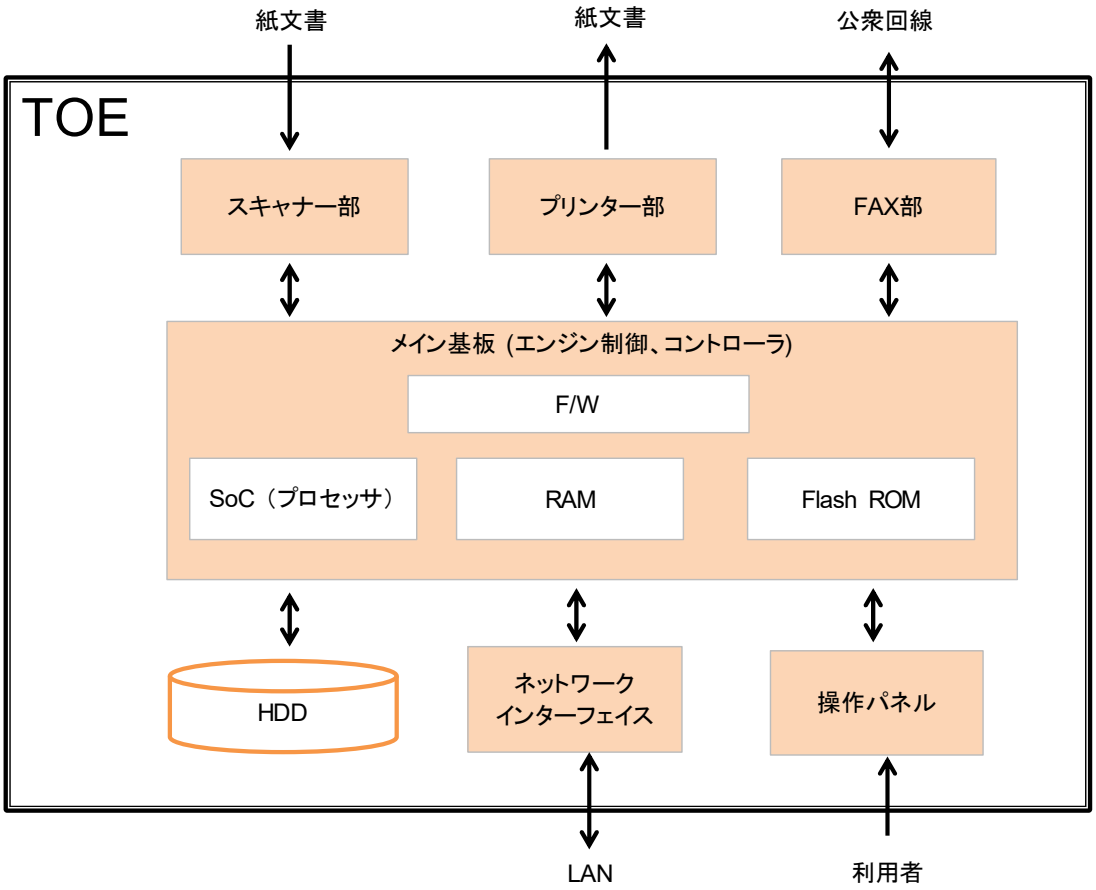

図 1-2. TOE の物理的範囲

TOE はメイン基板、プリンター部、スキャナー部、FAX 部、ネットワークインターフェイス、操作パネル、及び HDD から構成される MFP である。図 1-2 の各要素に関して、以下に説明する。

(1) メイン基板

メイン基板とは、電子部品や集積回路（IC）、それらを接続する金属配線などを高密度に実装した部品のこと。

(2) F/W

F/W（Firmware）とは、コンピュータなどに内蔵されるソフトウェアの一種であり、本体内部の回路や装置などの基本的な制御を司る機能を持つもののこと。

(3) SoC（プロセッサ）

SoC（プロセッサ）とは、各装置の制御やデータの計算・加工を行う装置のこと。メモリに記憶されたプログラムを実行し、入力装置や記憶装置からデータを受け取り、演算・加工した上で、出力装置や記憶装置に出力する。

(4) RAM

RAM（Random Access Memory）とは、データの消去・書き換えが可能なメモリ装置のこと。装置内のどこに記録されたデータであっても等しい時間で読み書き（ランダムアクセス）することができるが、電源が切れるとメモリ上のデータが消える。

(5) Flash ROM

Flash ROM（Read Only Memory）とは、データの消去・書き換えが可能なメモリ装置のこと。電源が切れてもメ

モリ上のデータが消えない。

(6) プリンター部

プリンター部とは、プリント機能の制御を実装した部品のこと。

(7) スキャナー部

スキャナー部とは、スキャン機能の制御を実装した部品のこと。

(8) FAX 部

FAX 部とは、FAX 機能の制御を実装した部品のこと。表 1-2 に記載の FAX ボードを装着することで機能する。

(9) ネットワークインターフェイス

ネットワークインターフェイスとは、MFP を LAN に接続するための装置のこと。

(10) 操作パネル

操作パネルとは、MFP を操作するためのユーザインターフェイス装置のこと。

(11) HDD

HDD（Hard Disk Drive）とは、データを記憶する装置のこと。

TOE の構成品の配付方法を表 1-2 に示す。

表 1-2. TOE の構成品の配付方法

TOE 構成品	形態	配付方法	識別情報
MFP 本体	MFP 装置	クーリエ配送	・日本…LX-10020M ・海外…WF-M21000
FAX	FAX ボード	クーリエ配送	・日本…Super G3/G3 Multi Fax Board / PR3FB0 ・海外…Super G3/G3 Multi Fax Board / PR3FB1
ガイダンス	表 1-3 に示す形態	表 1-3 に示す配付方法	表 1-3 に示す名称及びバージョン
ファームウェア	電子ファイル	サービスマンから受け渡し	バージョン GR12L4

本 TOE を構成するガイダンスを表 1-3 に示す。

表 1-3. TOE を構成するガイダンス一覧

名称	Ver.	形態	配付方法	仕向け
ユーザーズガイド	NPD6659-02 JA	PDF 形式ファイル	Web 配付	日本
セキュリティー機能補足ガイド	NPD6692-01 JA	PDF 形式ファイル	Web 配付	日本
ご使用の前に / Before Use	4140894-00	紙媒体	MFP 本体に同梱	日本/海外
User's Guide	NPD6658-02 EN	PDF 形式ファイル	Web 配付	海外
Supplemental Security Guide	NPD6692-01 EN	PDF 形式ファイル	Web 配付	海外

1.4.3.TOE の論理的範囲

本 TOE の論理的範囲を図 1-3 に示す。

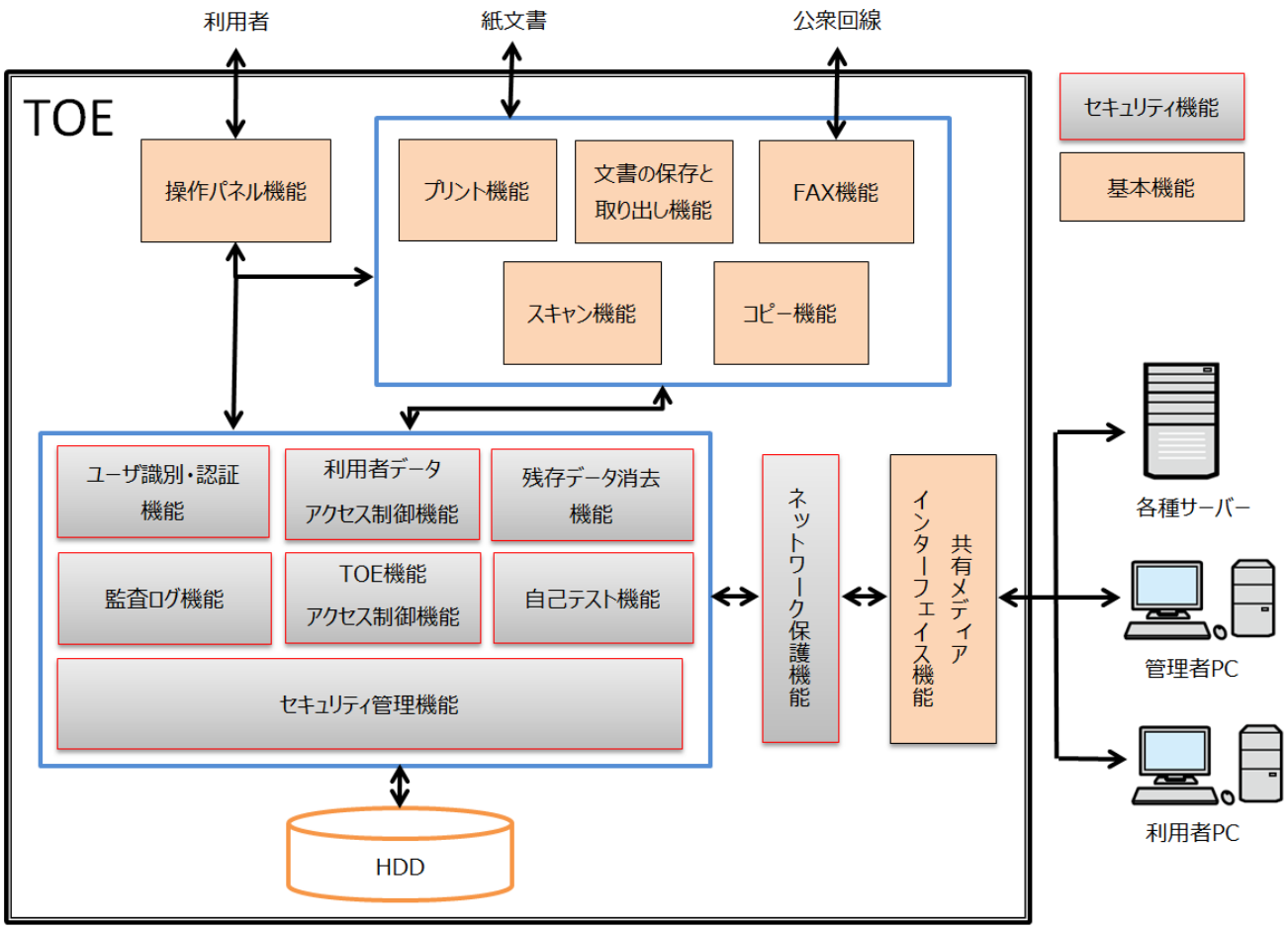

図 1-3. TOE の論理的範囲

図 1-3 の各要素に関して、以下に説明する。

◆ TOE が提供する基本機能

(1) プリント機能

クライアントから LAN を経由して受信したデジタル文書を印刷する機能

(2) スキャン機能

利用者による操作パネルからの操作により、紙文書を読み取り、デジタル文書を生成する機能

(3) コピー機能

利用者による操作パネルからの操作により、紙文書を読み取り、その画像を複写印刷する機能

(4) FAX 機能

外部 FAX にデジタル文書を送信する機能（FAX 送信機能）及び外部 FAX からデジタル文書を受信する機能（FAX 受信機能）

- FAX 送信機能

  公衆回線を介してデジタル文書を外部の FAX 装置に送信する機能

- FAX 受信機能

  公衆回線を介してデジタル文書を外部の FAX 装置から受信する機能

(5) 文書の保存と取り出し機能

TOE 内部にデジタル文書を保存し、その保存したデジタル文書を取り出す機能であり、ボックス機能という

- 個人ボックスにデジタル文書を保存する機能
  スキャナーから読み込んだデジタル文書や PC でボックス保存を指定したデジタル文書を個人ボックスへ保存する機能
- 個人ボックスに保存されたデジタル文書を取り出し利用する機能
  個人ボックスに保存されたデジタル文書を取り出し、印刷、プレビュー、他のシステムへ文書の送信、削除する機能

(6) 共有メディアインターフェイス機能

TOE の利用者がクライアント PC から TOE をリモート操作するための機能

(7) 操作パネル機能

操作パネルを制御する機能

◆ TOE が提供するセキュリティ機能

(1) ユーザ識別・認証機能

利用者に操作パネルまたはネットワークを介してユーザ名とログオンパスワードを入力させることで識別・認証を行う機能。 本機能の中には、管理者がログオンパスワードに対し最小桁数と必須の文字種を設定する機能、ログオンパスワードを入力する際にダミー文字で表示する認証フィードバックの保護機能が含まれる。 また、認証失敗時に一定時間当該アカウントをロックアウトする機能、及びログオン後一定時間無操作状態が継続した場合、自動的にログオフする機能が含まれる。

(2) 利用者データアクセス制御機能

ユーザ識別・認証機能で認証された利用者に対し、そ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応じて、TOE 内の利用者データ、及びジョブデータへの操作を可能となるように制御する機能。

(3) TOE 機能アクセス制御機能

ユーザ識別・認証機能で認証された利用者に対し、アクセス制御規則に基づき、許可された利用者のみに TOE の基本機能を利用可能とするように制御する機能。 TOE の基本機能には以下がある。

・プリント機能
・スキャン機能
・コピー機能
・FAX 受信、送信機能
・文書の保存と取り出し機能

(4) セキュリティ管理機能

セキュリティ管理機能とは、操作パネルまたはネットワークを介し、役割に与えられた権限に基づき、以下の項目を管理する機能のことである。

・セキュリティ属性
・TSF データ
・管理機能
・役割

(5) 残存データ消去機能

プリント、スキャン、コピー、FAX 等の TOE の基本機能を使用時、HDD 及び Flash ROM 上に保存された後に使用不要となったデータ、及び利用者により削除されたデータに対し、特定の値を上書きすることで残存情報を再使用不能とする機能。

(6) 自己テスト機能

TOE のファームウェアの不正改ざんを検出するために、TOE 起動時に TSF の一部が正常動作すること、TSF データの一部及び TSF 実行コードが完全であることを検証する機能。

(7) 監査ログ機能

TOE に対し、いつ、誰が、どのような操作を行ったかの使用履歴、及びセキュリティ関連事象をログとして記録する機能。 ログは管理者だけが監査できるように判読可能なファイル形式での読み出しと削除ができるが、管理者であっても TOE に保存された監査ログ自体を編集することはできない。

(8) ネットワーク保護機能

TOE が各種サーバーやクライアント PC と有線 LAN を用い通信する際、IPsec 暗号化通信を用いてネットワークの盗聴による情報漏えい、及び改変を防止する機能。 また、有線 LAN と電話回線との間の情報転送を、TSF による追加の処理なしに直接転送しない機能も提供する。

1.4.4.TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE を利用するためには、以下のソフトウェア及びそれらが動作するハードウェアが必要である。

表 1-4. TOE に必要な TOE 以外のソフトウェア

ソフトウェア	評価にて使用したバージョン
NTP サーバー	Microsoft Windows Server 2016 Standard
LDAP サーバー	Microsoft Windows Server 2016 Standard
DNS サーバー	Microsoft Windows Server 2016 Standard
SMTP サーバー	hMailServer 5.6.7-B2425
SMB サーバー	Microsoft Windows Server 2016 Standard
FTP サーバー	Microsoft Windows Server 2016 Standard
プリンタードライバー	Microsoft Windows 用 日本語版:Epson Printing System(J) Version 3.01.00 英語版:Epson Printing System(A) Version 3.01.00
ブラウザー	Microsoft Edge

※英語版プリンタードライバーの、( )内の文字はドライバーをインストールした PC のタイムゾーンを示す。
使用する PC のタイムゾーンが北米時間以外の場合、( )内には”W”が表示されるが、同一のプリンタードライバーである。

1.5. 用語・略語

表 1-5 において、本 ST における特定の用語及び略語の意味を定義する。

表 1-5. 用語・略語

用語	定義

一般利用者 User ID	U.NORMAL、D.DOC 及び D.FUNC に付与される属性 U.NORMAL に一意の識別子が付与される
利用者役割	U.USER に付与される属性 一般利用者及び管理者がある U.NORMAL に一般利用者、U.ADMINISTRATOR に管理者が付与される
利用機能リスト	U.NORMAL に付与される属性 U.NORMAL に対して、利用を許可された機能のリストが付与される プリント機能（PRT）、スキャン機能（SCAN）、コピー機能（CPY）、FAX 受信機能（FAXIN）、FAX 送信機能（FAXOUT）、及び文書の保存と取り出し機能（DSR）がある
MFP 機能	TOE が提供するプリント機能、スキャン機能、コピー機能、FAX 機能、及び文書の保存と取り出し機能の総称
機能種別	MFP 機能に付与される属性 プリント属性、スキャン属性、コピー属性、FAX 属性、及び文書の保存と取り出し属性がある
文書情報属性	D.DOC 及び D.FUNC に付与される属性 プリント、スキャン、コピー、FAX 受信、FAX 送信、及び文書の保存と取り出しがある
ジョブ	D.DOC に対する MFP 機能による処理の開始から完了までの処理単位のこと
パスワード付き印刷ジョブ	一般利用者 User ID 及び一般利用者パスワードが付加された印刷ジョブのこと

2. Conformance Claims

本章は、適合主張を記す。

2.1. CC Conformance Claim

本 ST の CC 適合主張を以下に記す。

Common Criteria version:	Version 3.1 Release 5
Common Criteria conformance:	Part 2 extended and Part 3 conformant

2.2. PP Conformance Claim

本 ST の PP 適合主張を以下に記す。

PP identification:	U.S. Government Approved Protection Profile – U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2 TM-2009)
PP version:	1.0

※ 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. Package Conformance Claim

本 ST の Package 適合主張を以下に記す。

This ST conforms to Common Criteria Evaluation Assurance Level (EAL) 2 augmented by ALC_FLR.2. SFR Packages conform to PP are as follows.

- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-FAX, SFR Package for Hardcopy Device FAX Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B (Package Version 1.0, dated March 2009)

2.4. SFR Package functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protec

tion Profile, are listed in 表 2-1.

表 2-1. SFR Package functions

名称	定義
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.5. SFR Package attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that depend on the function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in 表 2-2.

表 2-2. SFR Package attributes

名称	定義
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.6. PP Conformance Rationale

本章は、PP の TOE 種別との一貫性主張、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、及び PP のセキュリティ要件との一貫性主張を記す。

2.6.1.PP の TOE 種別との一貫性主張

本 TOE は、プリント機能、スキャン機能、コピー機能、FAX 機能、文書の保存と取り出し機能、及び共有メディアインターフェイス機能を有する MFP であることから、「2600.2, Protection Profile for Hardcopy Devices, Operational Environment B」記載のハードコピー装置（以下、HCD と略す）と種別は一貫している。また、本 TOE は、取り外し可能な HDD や他の不揮発性記憶システムを持たないため、「2600.2, Protection Profile for Hardcopy Devices, Operational Environment B」に定義された 7 つの SFR パッケージのうち、「2600.2-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B」を除く 6 つの SFR パッケージに適合している。

2.6.2.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

セキュリティ課題に関して、本 ST では、PP にて要求される全てのセキュリティ課題と全く同一であり、一貫している。また、セキュリティ対策方針に関して、IT 環境のセキュリティ対策方針から OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED を削除し、TOE のセキュリティ対策方針として O.AUDIT_STORAGE.PROTECTED と O.AUDIT_ACCESS.AUTHORIZED を追加している。O.AUDIT_STORAGE.PROTECTED と O.AUDIT_ACCESS.AUTHORIZED を実行する内部機能は、OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED にて要求されていることと同等である。

2.6.3.PP のセキュリティ要件との一貫性主張

PP にて要求される SFR と本 ST にて規定する SFR を表 2-3 に示す。

表 2-3. SFR の関係

PP にて要求される SFR	本 ST にて規定する SFR
FAU_GEN.1	FAU_GEN.1
FAU_GEN.2	FAU_GEN.2
	FAU_SAR.1
	FAU_SAR.2
	FAU_STG.1
	FAU_STG.4
FDP_ACC.1(a)	FDP_ACC.1(a)
FDP_ACC.1(b)	FDP_ACC.1(b)
FDP_ACF.1(a)	FDP_ACF.1(a)
FDP_ACF.1(b)	FDP_ACF.1(b)
FDP_RIP.1	FDP_RIP.1
	FIA_AFL.1
FIA_ATD.1	FIA_ATD.1
	FIA_SOS.1
FIA_UAU.1	FIA_UAU.1
	FIA_UAU.7

FIA_UID.1	FIA_UID.1
FIA_USB.1	FIA_USB.1
FMT_MSA.1(a)	FMT_MSA.1(a)
FMT_MSA.1(b)	FMT_MSA.1(b)
FMT_MSA.3(a)	FMT_MSA.3(a)
FMT_MSA.3(b)	FMT_MSA.3(b)
FMT_MTD.1	FMT_MTD.1
FMT_SMF.1	FMT_SMF.1
FMT_SMR.1	FMT_SMR.1
FPT_FDI_EXP.1	FPT_FDI_EXP.1
FPT_STM.1	FPT_STM.1
FPT_TST.1	FPT_TST.1
FTA_SSL.3	FTA_SSL.3
FTP_ITC.1	FTP_ITC.1

本 ST では、PP にて要求される全ての SFR を適用した上で、いくつかの SFR を追加している。また、PP における SFR のうち、FDP_ACF.1.3(b)を除く、全ての SFR と本 ST にて規定する SFR は全く同一である。PP における FDP_ACF.1.3(b)は、管理者権限にて操作するユーザに TOE 機能の操作を全て許可することとなっているのに対して、本 ST ではプリント機能の一部（印刷）を制限している。従って、本 ST での FDP_ACF.1.3(b)は、PP における FDP_ACF.1.3(b)よりも制限的である。

また、PP では、Common Access Control SFP において、D.FUNC に対して操作「Modify」と操作「Delete」を定義している。しかし、本 TOE では、D.FUNC に対する操作「Modify」を許可しない。これは PP よりも制限的なアクセス制御である。

従って、本 ST は PP に対して同等、または、より制限的であることから、PP に対して論証適合している。

3. Security Problem Definition

本章は、保護資産、脅威、組織のセキュリティ方針、及び前提条件を記す。

3.1. 保護資産

保護資産とは、User Data、TSF Data、及び Functions のことである。

(1) User Data

User Data とは、ユーザによって作成される TOE のセキュリティ機能には影響を与えないデータのことであり、以下 2 種類に分類される。

表 3-1. User Data

名称	PP での定義
D.DOC	User Document Data consist of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

(2) TSF Data

TSF Data とは、TOE のセキュリティ機能に影響を与えるデータのことであり、以下 2 種類に分類される。

表 3-2. TSF Data

名称	PP での定義
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

本 TOE が対象とする TSF データを表 3-3 に示す。

表 3-3. 本 TOE が対象とする TSF データ

名称	本 ST での TSF データ	内容
D.PROT	一般利用者 User ID	U.NORMAL の識別情報
	管理者 User ID	U.ADMINISTRATOR の識別情報 識別子“Administrator”が付与される
	スキャン/FAX/電子メールの送信先リストまたはアドレスブック	アドレス帳
	ジョブステータスログ	ジョブ履歴

	パスワードポリシー	パスワードの文字種、及び桁数に関する設定情報
	無操作タイマー設定	操作パネルからのログオンセッションを自動的に終了する時間情報
	管理者認証設定（操作パネル）	操作パネルからの管理者認証を有効化/無効化する設定情報
	利用者制限設定	Web Config から設定可能な各種設定情報（利用機能リストを含む）
	IPsec の設定	IPsec に関する設定情報
	時刻設定	時刻の設定情報
	ネットワーク設定	ネットワークの設定情報
	ファームウェアの完全性検証のためのハッシュ値	ファームウェアのファイルから計算されたハッシュ値 TOE 内に格納される
D.CONF	一般利用者パスワード	U.NORMAL の認証情報
	管理者パスワード	U.ADMINISTRATOR の認証情報
	メールサーバーやファイルサーバーなどの外部装置にアクセスするためのパスワード	メールサーバーへアクセスするためのパスワード ファイルサーバーへアクセスするためのパスワード
	監査ログ	監査ログ機能により生成されるログ情報
	IPsec の事前共有鍵	IPsec において鍵交換に必要な暗号鍵

(3) Functions

Functions とは、表 2-1 に示す機能のことである。

3.2. Threats agents

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE.

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which th ey are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which t hey are not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipat ed threats.

The threats and policies defined in this Security Target address the threats posed by these threat age nts.

3.3. Threats to TOE Assets

This section describes threats to assets described in 3.1.

表 3-4. Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons

T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

表 3-5. Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.4. Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

表 3-6. Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

3.5. Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Security Target are based on the condition that all of the assumptions described in this section are satisfied.

表 3-7. Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedure

	s.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their org anization, are trained and competent to follow the manufacturer’s guidance a nd documentation, and correctly configure and operate the TOE in accordan ce with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purpos es.

4. Security Objectives

本章は、TOE 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を記す。

4.1. Security Objectives for the TOE

This section describes the Security Objectives that the TOE shall fulfill.

表 4-1. Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.

4.2. Security Objectives for the IT environment

This section describes the Security Objectives that must be fulfilled by IT methods in the IT environment of the TOE.

表 4-2. Security Objectives for the IT environment

Objective	Definition
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3. Security Objectives for the non-IT environment

This section describes the Security Objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

表 4-3. Security Objectives for the non-IT environment

Objective	Definition
OE.PHISICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer’s guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4. Security Objectives rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

表 4-4. Completeness of Security Objectives

	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._AUDIT_STORAGE.PROTECTED	O._AUDIT_ACCESS.AUTHORIZED	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.USER.AUTHORIZED	OE.USER.TRAINED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.AUDIT.REVIEWED
T.DOC.DIS	✓						✓								✓				
T.DOC.ALT		✓					✓								✓				
T.FUNC.ALT			✓				✓								✓				
T.PROT.ALT				✓			✓								✓				
T.CONF.DIS					✓		✓								✓				
T.CONF.ALT						✓	✓								✓				
P.USER.AUTHORIZATION							✓								✓				
P.SOFTWARE.VERIFICATION									✓										
P.AUDIT.LOGGING										✓	✓	✓							✓
P.INTERFACE.MANAGEMENT								✓					✓						
A.ACCESS.MANAGED														✓					
A.USER.TRAINING																✓			
A.ADMIN.TRAINING																	✓		
A.ADMIN.TRUST																		✓	

表 4-5. Sufficiency of Security Objectives

Threats. policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

T.DOC.ALT	User Document Data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes res

		ponsibility of the TOE Owner to approp riately grant authorization.
P.USER.AUTHORIZATION	Users will be authorized to u se the TOE.	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.
		OE.USER.AUTHORIZED establishes res ponsibility of the TOE Owner to approp riately grant authorization.
P.SOFTWARE.VERIFICATION	Procedures will exist to selfv erify executable code in the TSF.	O.SOFTWARE.VERIFIED provides proc edures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use an d security-relevant events will be created, maintained, prot ected, and reviewed.	O.AUDIT.LOGGED creates and maintain s a log of TOE use and security-releva nt events and prevents unauthorized di sclosure or alteration.
		O.AUDIT_STORAGE.PROTECTED prote cts audit records from unauthorized acc ess, deletion and modifications.
		O.AUDIT_ACCESS.AUTHORIZED provid es appropriate access to audit records only by authorized persons.
		OE.AUDIT.REVIEWED establishes respo nsibility of the TOE Owner to ensure th at audit logs are appropriately reviewe d.
P.INTERFACE.MANAGEMEN T	Operation of external interfac es will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in acc ordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE extern al interfaces.
A.ACCESS.MANAGED	The TOE environment provid es protection from unmanage d access to the physical co mponents and data interface s of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.USER.TRAINING	Administrators are aware of and trained to follow security	OE.USER.TRAINED establishes respons ibility of the TOE Owner to provide app

	policies and procedures.	ropriate User training.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.

5. Extended components definition

This Security Target defines components that are extensions to Common Criteria 3.1 Revision 2, Part 2. These extended components are defined in the Security Target but are used in SFR Packages and, therefore, are employed only in TOEs whose STs conform to those SFR Packages.

5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behavior:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces	1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities
b) Management of the conditions under which direct forwarding can be allowed by an administrative role
c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Security Target, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Security Target or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: **No other components**

Dependencies: **FMT_SMF.1 Specification of Management Functions**

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

6. Security Requirements

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記す。

6.1. Security Functional Requirements

本章は、各セキュリティ機能要件の操作結果を記す。

6.1.1.Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in 表 6-1;** [assignment: *other specifically defined auditable events*]

[selection, choose one of: *minimum, basic, detailed, not specified*]

- not specified

[assignment: *other specifically defined auditable events*]

- なし

表 6-1. 監査対象事象

監査対象事象	関連 SFR	監査レベル	追加情報	詳細
認証メカニズムの使用に失敗 認証メカニズムの使用に成功	FIA_UAU.1	基本	なし	ログオン操作の失敗 ログオン操作の成功
識別メカニズムの使用に失敗 識別メカニズムの使用に成功	FIA_UID.1	基本	利用者識別の試行（該当する場合）	ログオン操作の失敗（利用者識別情報を含む） ログオン操作の成功
管理機能の使用	FMT_SMF.1	最小	なし	管理機能（表 6-11 参照）の記録
役割の一部をなす利用者グループの改変	FMT_SMR.1	最小	なし	改変はないため記録なし
時間の変更	FPT_STM.1	最小	なし	時刻の変更
高信頼チャネル機能の失敗	FTP_ITC.1	最小	通信先 IP アドレス	IPsec 通信の失敗

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome

(success or failure) of the event; and

- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in 表 6-1: (1) the information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*]

[assignment: *other audit relevant information*]

- なし

FAU_GEN.2 User identity association

Hierarchical to: **No other components**

Dependencies: **FAU_GEN.1 Audit data generation**

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to: **No other components**

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

[assignment: *authorised users*]

- 管理者

[assignment: *list of audit information*]

- 表 6-1 に示す監査対象事象

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: **No other components**

Dependencies: **FAU_SAR.1 Audit review**

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected audit trail storage

Hierarchical to: **No other components**

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorized modifications to the stored audit records in the audit trail.

[selection, choose one of: *prevent, detect*]

- prevent

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

- overwrite the oldest stored audit records

[assignment: *other actions to be taken in case of audit storage failure*]

- なし

6.1.2.Class FDP: User data protection

FDP_ACC.1(a) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the **Common Access Control SFP in 表 6-2 on the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in 表 6-2.**

FDP_ACC.1(b) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP in 表 6-3 on users as subjects, TOE functions as objects, and the right to use the functions as operations.**

FDP_ACF.1(a) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(a) The TSF shall enforce the **Common Access Control SFP in 表 6-2** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in 表 6-2, and for each, the indicated security attributes in 表 6-2.**

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in 表 6-2 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects.**

表 6-2. 制御されたサブジェクトとオブジェクト間の操作を制御する規則

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
D.DOC	+PRT +SCN +CPY +FAXOUT +DSR	Delete Read	U.NORMAL	Denied, except for his/her own documents 文書は、文書を作成した U.NORMAL が所有する
	+FAXIN	Delete Read	U.NORMAL	Denied, except for his/her own documents 受信したファクス文書は、利用機能リストに「FAX 受信機能（FAXIN）」が付与される U.NORMAL が所有する
D.FUNC	+PRT +SCN +CPY +FAXOUT +DSR	Delete	U.NORMAL	Denied, except for his/her own documents 文書は、文書を作成した U.NORMAL が所有する
		Modify	U.NORMAL	Denied
	+FAXIN	Delete	U.NORMAL	Denied, except for his/her own documents 受信したファクス文書は、利用機能リストに「FAX 受信機能（FAXIN）」が付与される U.NORMAL が所有する
		Modify	U.NORMAL	Denied

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

- U.ADMINISTRATOR に対して、文書情報属性が「+PRT」の D.DOC に対する操作「Delete」を許可する。
- U.ADMINISTRATOR に対して、文書情報属性が「+SCN」、「+CPY」、「+FAXIN」、「+FAXOUT」、「+DSR」の D.DOC に対する操作「Read」及び「Delete」を許可する
- U.ADMINISTRATOR に対して、文書情報属性が「+PRT」、「+SCN」、「+CPY」、「+FAXIN」、「+FAXOUT」、「+DSR」の D.FUNC に対する操作「Delete」を許可する

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- U.ADMINISTRATOR に対して、文書情報属性が「+PRT」、「+SCN」、「+CPY」、「+FAXIN」、「+FAXOUT」、「+DSR」の D.FUNC に対する操作「Modify」を許可しない

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** to objects based on the following: **users and [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*].**

[assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]

- 表 6-3 参照

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]].**

[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]

- [assignment: *other conditions*]

[assignment: *other conditions*]

- 表 6-3 参照

表 6-3. 制御されたサブジェクトとオブジェクト間の操作を制御する規則

オブジェクト	操作	サブジェクト	セキュリティ属性	操作を制御する規則
F.PRT	ジョブの実行 ジョブの削除	U.NORMAL	利用機能リスト（PRT）	利用機能リストに「プリント機能（PRT）」が付与されるサブジェクトに対して、操作を許可する
F.SCN	ジョブの実行 ジョブの削除	U.NORMAL	利用機能リスト（SCN）	利用機能リストに「スキャン機能（SCN）」が付与されるサブジェクトに対して、操作を許可する
F.CPY	ジョブの実行 ジョブの削除	U.NORMAL	利用機能リスト（CPY）	利用機能リストに「コピー機能（CPY）」が付与されるサブジェクトに対して、操作を許可する
F.FAX	ジョブの実行 ジョブの削除	U.NORMAL	利用機能リスト（FAXIN） 利用機能リスト（FAXOUT）	利用機能リストに「FAX 受信機能（FAXIN）」及び「FAX 送信機能（FAXOUT）」が付与されるサブジェクトに対して、操作を許可する
F.DSR	ジョブの実行 ジョブの削除	U.NORMAL	利用機能リスト（DSR）	利用機能リストに「文書の保存と取り出し機能（DSR）」が付与されるサブジェクトに対して、操作を許可する

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- U.ADMINISTRATOR に対して、「F.PRT」に対する操作「ジョブの削除」を許可する
- U.ADMINISTRATOR に対して、「F.SCN」、「F.CPY」、「F.FAX」、または「F.DSR」に対する操作「ジョブの実行」及び「ジョブの削除」を許可する

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- なし

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects:

D.DOC, [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]

- deallocation of the resource from

[assignment: *list of objects*]

- なし

6.1.3.Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

- [assignment: positive integer number]

[assignment: *positive integer number*]

- 1

[assignment: *list of authentication events*]

- 管理者による操作パネルからのログオン
- 一般利用者による操作パネルからのログオン
- 管理者による Web Config からのログオン
- パスワード付き印刷ジョブ受付時の認証

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

- 表 6-4 参照

表 6-4. アクションのリスト

ログオンパターン	認証不成功時のアクション
管理者による操作パネルからのログオン	0.6 秒間、当該管理者をロックアウトする
一般利用者による操作パネルからのログオン	0.6 秒間、当該一般利用者をロックアウトする

管理者による Web Config からのログオン	1 秒間、当該管理者をロックアウトする
パスワード付き印刷ジョブ受付時の認証	1 秒間、当該一般利用者をロックアウトする

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- 表 6-5 参照

表 6-5. セキュリティ属性のリスト

利用者	セキュリティ属性
U.NORMAL	一般利用者 User ID 利用者役割 利用機能リスト
U.ADMINISTRATOR	利用者役割

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets（一般利用者パスワード、管理者パスワード） meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

- 桁数:8 桁以上（最大 20 桁まで）とすること
- 文字種:必ず、以下の文字を 1 文字以上含むこと
  - 英大文字
  - 英小文字
  - 数字
  - 記号（!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ ）

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is

authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- 操作パネルでのプリンター情報の表示
- 操作パネルからのプリンター情報の印刷
- 操作パネルでのネットワーク情報の表示
- 操作パネルからのネットワーク情報の印刷
- 操作パネルでのジョブ一覧の表示
- 操作パネルでのヘルプの表示
- Web Config でのプリンター情報の表示
- Web Config でのネットワーク情報の表示
- 操作パネルでの FAX 情報の表示
- 操作パネルからの FAX 情報の印刷
- 操作パネルからのプリンターメンテナンス機能の実行
- プリンタードライバーでのプリンターステータスの表示

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]

- 表 6-6 参照

表 6-6. フィードバックのリスト

アクション	フィードバック
管理者による操作パネルからのログオン	入力回数分の＊文字
一般利用者による操作パネルからのログオン	入力回数分の＊文字
管理者による Web Config からのログオン	入力回数分のマスク文字 ※マスクする文字種はブラウザーに依存する

FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: **No dependencies**

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- 操作パネルでのプリンター情報の表示
- 操作パネルからのプリンター情報の印刷
- 操作パネルでのネットワーク情報の表示
- 操作パネルからのネットワーク情報の印刷
- 操作パネルでのジョブ一覧の表示
- 操作パネルでのヘルプの表示
- Web Config でのプリンター情報の表示
- Web Config でのネットワーク情報の表示
- 操作パネルでの FAX 情報の表示
- 操作パネルからの FAX 情報の印刷
- 操作パネルからのプリンターメンテナンス機能の実行
- プリンタードライバーでのプリンターステータスの表示

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to: **No other components**

Dependencies: **FIA_ATD.1 User attribute definition**

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]

- 表 6-5 参照

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [assignment: *rules for the initial association of attributes*].

[assignment: *rules for the initial association of attributes*]

- なし

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with the

subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*]

- なし

6.1.4.Class FMT: Security management

FMT_MSA.1(a) Management of security attributes

Hierarchical to: **No other components**

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(a) The TSF shall enforce the **Common Access Control SFP in 表 6-2,** [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

- なし

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

- 表 6-7 参照
- [assignment: other operations]

[assignment: *other operations*]

- 表 6-7 参照

[assignment: *list of security attributes*]

- 表 6-7 参照

[assignment: *the authorized identified roles*]

- 表 6-7 参照

表 6-7. セキュリティ属性、操作、及び操作を許可する利用者役割

セキュリティ属性	操作	操作を許可する利用者役割
一般利用者 User ID	【選択した操作】delete	U.ADMINISTRATOR
	【追加した操作】新規作成	
利用者役割	【選択した操作】modify	Nobody
利用機能リスト	【選択した操作】modify	U.ADMINISTRATOR
文書情報属性	【選択した操作】modify	Nobody

FMT_MSA.1(b) Management of security attributes

Hierarchical to: **No other components**

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP in 表 6-3,** [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

- なし

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

- 表 6-8 参照

[assignment: *list of security attributes*]

- 表 6-8 参照

[assignment: *the authorised identified roles*]

- 表 6-8 参照

表 6-8. セキュリティ属性、操作、及び操作を許可する利用者役割

セキュリティ属性	操作	操作を許可する利用者役割
利用者役割	【選択した操作】modify	Nobody
利用機能リスト	【選択した操作】modify	U.ADMINISTRATOR
機能種別	【選択した操作】modify	Nobody

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: **No other components**

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3.1(a) The TSF shall enforce the **Common Access Control SFP in 表 6-2,** [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- なし

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- restrictive

FMT_MSA.3.2(a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- nobody

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: **No other components**

Dependencies: **FMT_MSA.1 Management of security attributes**

FMT_SMR.1 Security roles

FMT_MSA.3.1(b) The TSF shall enforce the **TOE Function Access Control Policy in 表 6-3,** [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

- なし

[selection, *choose one of: restrictive, permissive, [assignment: other property]*]

- restrictive

FMT_MSA.3.2(b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- nobody

FMT_MTD.1 Management of TSF Data

Hierarchical to: **No other components**

Dependencies: **FMT_SMR.1 Security roles**

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1(a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF Data*] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*,** [assignment: *the authorized identified roles* ***except U.NORMAL***]**]].**

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- 表 6-9 参照
- [assignment: other operations]

[assignment: *other operations*]

- 表 6-9 参照

[assignment: *list of TSF Data*]

- 表 6-9 参照

[selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR,* [assignment: *the authorized identified roles* ***except U.NORMAL***]**]]**

- 表 6-9 参照

表 6-9. 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
D.PROT	管理者 User ID	【選択した操作】modify	Nobody
	パスワードポリシー	【選択した操作】modify	U.ADMINISTRATOR
	無操作タイマー設定	【選択した操作】modify	U.ADMINISTRATOR
	管理者認証設定（操作パネル）	【選択した操作】modify	U.ADMINISTRATOR
	利用者制限設定	【選択した操作】modify	U.ADMINISTRATOR
	IPsec の設定	【選択した操作】modify	U.ADMINISTRATOR
	時刻設定	【選択した操作】modify	U.ADMINISTRATOR
	ネットワーク設定	【選択した操作】modify	U.ADMINISTRATOR
	ファームウェアの完全性検証のためのハッシュ値	【選択した操作】modify	Nobody
D.CONF	管理者パスワード	【選択した操作】modify	U.ADMINISTRATOR
		【選択した操作】query	Nobody
	メールサーバーやファイルサーバーなどの外部装置にアクセスするためのパスワード	【選択した操作】modify	U.ADMINISTRATOR
		【追加した操作】新規作成	
		【選択した操作】query	Nobody
	IPsec の事前共有鍵	【選択した操作】modify	U.ADMINISTRATOR
		【選択した操作】query	Nobody

FMT_MTD.1.1(b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF Data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF Data are associated*]].**

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

- 表 6-10 参照

- [assignment: other operations]

[assignment: *other operations*]

- 表 6-10 参照

[assignment: *list of TSF Data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***]

- 表 6-10 参照

[selection, choose one of: ***Nobody,*** **[selection:** ***U.ADMINISTRATOR, the U.NORMAL to whom such TSF Data are associated*****]]**

- 表 6-10 参照

表 6-10. 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
D.PROT	一般利用者 User ID	【選択した操作】delete	U.ADMINISTRATOR
		【追加した操作】新規作成	
	スキャン/FAX/電子メールの送信先リストまたはアドレスブック	【選択した操作】delete	U.ADMINISTRATOR
		【追加した操作】新規作成	
	ジョブステータスログ	【選択した操作】modify	Nobody
D.CONF	一般利用者パスワード	【選択した操作】delete	U.ADMINISTRATOR
		【追加した操作】新規作成	
		【選択した操作】query	Nobody

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

[assignment: *list of management functions to be provided by the TSF*]

- 表 6-11 参照

表 6-11. 管理機能のリスト

管理機能
U.ADMINISTRATOR による「一般利用者 User ID」の登録・削除
U.ADMINISTRATOR による「スキャン/FAX/電子メールの送信先リストまたはアドレスブック」の登録・削除
U.ADMINISTRATOR による「パスワードポリシー」の変更
U.ADMINISTRATOR による「無操作タイマー設定」の変更
U.ADMINISTRATOR による「管理者認証設定（操作パネル）」の変更

U.ADMINISTRATOR による「利用者制限設定」の変更
U.ADMINISTRATOR による「IPsec の設定」の変更
U.ADMINISTRATOR による「時刻設定」の変更
U.ADMINISTRATOR による「ネットワーク設定」の変更
U.ADMINISTRATOR による「一般利用者パスワード」の登録・削除
U.ADMINISTRATOR による「管理者パスワード」の変更
U.ADMINISTRATOR による「メールサーバーやファイルサーバーなどの外部装置にアクセスするためのパスワード」の登録・変更
U.ADMINISTRATOR による「IPsec の事前共有鍵」の変更

FMT_SMR.1 Security roles

Hierarchical to: **No other components**

Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].

[selection: *Nobody,* [assignment: *the authorised identified roles*]]

- Nobody

FMT_SMR.1.2 The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated**.

6.1.5.Class FPT: Protection of the TSF

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: **No other components**

Dependencies: **FMT_SMF.1 Specification of Management Functions**

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to the TSF to **any Shared-medium Interface**.

FPT_STM.1 Reliable time stamps

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]

- during initial start-up

[selection: [assignment: *parts of TSF*], *the TSF*]

- [assignment: parts of TSF]

[assignment: *parts of TSF*]

- 自己テスト機能

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF Data*].

[selection: [assignment: *parts of TSF*], *TSF Data*]

- [assignment: parts of TSF]

[assignment: *parts of TSF*]

- ファームウェアの完全性検証のためのハッシュ値

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.6.Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]

- 表 6-12 参照

表 6-12. 利用者が非アクティブである時間間隔

アクション	利用者が非アクティブである時間間隔
管理者による操作パネルからのログオン	「無操作タイマー設定」指定時間 （管理者により、10 秒から 240 分の範囲で指定可能）
一般利用者による操作パネルからのログオン	「無操作タイマー設定」指定時間

	（管理者により、10 秒から 240 分の範囲で指定可能）
管理者による Web Config からのログオン	20 分

6.1.7.Class FTP: Trusted paths/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface.**

6.2. Security Assurance Requirements

表 6-13 lists the security assurance requirements for 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B, and related SFR packages, EAL 2 augmented by ALC_FLR.2.

表 6-13. IEEE 2600.2 Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL 2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3. Security Requirements Rationale

本章は、セキュリティ機能要件根拠、セキュリティ保証要件根拠、及び依存性分析を記す。

6.3.1.Security Functional Requirements rationale

表 6-14 demonstrate the completeness of SFRs that fulfill the objectives of the TOE. Bold typeface ite ms provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

表 6-14. Completeness of security requirements

	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. AUDIT_STORAGE.PROTECTED	O. AUDIT_ACCESS.AUTHORIZED
FAU_GEN.1										**P**		
FAU_GEN.2										**P**		
FAU_SAR.1					**P**							**P**
FAU_SAR.2					**P**							**P**
FAU_STG.1						**P**					**P**	
FAU_STG.4						**P**					**P**	
FDP_ACC.1(a)	**P**	**P**	**P**									
FDP_ACC.1(b)							**P**					
FDP_ACF.1(a)	S	S	S									
FDP_ACF.1(b)							S					
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**					
FMT_MSA.1(a)	S	S	S									
FMT_MSA.1(b)							S					
FMT_MSA.3(a)	S	S	S									
FMT_MSA.3(b)							S					
FMT_MTD.1				**P**	**P**	**P**						
FMT_SMF.1	S	S	S	S	S	S						
FMT_SMR.1	S	S	S	S	S	S	S					
FPT_FDI_EXP.1								**P**				
FPT_STM.1										S		
FPT_TST.1									**P**			
FTA_SSL.3							**P**	**P**				
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**						

TOE の対策方針を実現する SFR の十分性を表 6-15 に示す。

表 6-15. Sufficiency of security requirements

対策方針	SFR	目的
O.DOC.NO_DIS （不正な開示からの D.DOC の保護）	**FDP_ACC.1(a)**	**アクセス制御方針を確立して保護を実施する**
	FDP_ACF.1(a)	アクセス制御機能を提供してアクセス制御方針を支援する
	FDP_RIP.1	**残存データを利用不能にして保護を実施する**
	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MSA.1(a)	セキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_MSA.3(a)	デフォルトのセキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.DOC.NO_ALT （不正な改変からの D.DOC の保護）	**FDP_ACC.1(a)**	**アクセス制御方針を確立して保護を実施する**
	FDP_ACF.1(a)	アクセス制御機能を提供してアクセス制御方針を

		支援する
	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MSA.1(a)	セキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_MSA.3(a)	デフォルトのセキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.FUNC.NO_ALT （不正な改変からの D.FUNC の保護）	**FDP_ACC.1(a)**	**アクセス制御方針を確立して保護を実施する**
	FDP_ACF.1(b)	アクセス制御機能を提供してアクセス制御方針を支援する
	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MSA.1(a)	セキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_MSA.3(a)	デフォルトのセキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.PROT.NO_ALT （不正な改変からの D.PROT の保護）	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MTD.1	**アクセスを制限して保護を実施する**
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.CONF.NO_DIS	**FAU_SAR.1**	**セキュリティ監査記録を提供して監査方針を実施**

（不正な開示からの D.CONF の保護）		**する**
	FAU_SAR.2	**セキュリティ監査記録の読み出しを制限して監査方針を実施する**
	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MTD.1	**アクセスを制限して保護を実施する**
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.CONF.NO_ALT （不正な改変からの D.CONF の保護）	**FAU_STG.1**	**権限付与されていない削除や改変から保護して監査方針を実施する**
	FAU_STG.4	**監査データの損失を防止して監査方針を実施する**
	FIA_UID.1	利用者識別を要求してアクセス制御とセキュリティの役割を支援する
	FMT_MTD.1	**アクセスを制限して保護を実施する**
	FMT_SMF.1	属性を管理する機能を要求してセキュリティ属性管理を支援する
	FMT_SMR.1	セキュリティの役割を要求してセキュリティ属性管理を支援する
	FTP_ITC.1	**共有メディアインターフェイス上で通信する際、高信頼チャネルの使用を要求して保護を実施する**
O.USER.AUTHORIZED （一般利用者と管理者に対する TOE を使用する権限の付与）	**FDP_ACC.1(b)**	**アクセス制御方針を確立して権限付与を実施する**
	FDP_ACF.1(b)	アクセス制御機能を提供してアクセス制御方針を支援する
	FIA_AFL.1	アクセス制御を要求して権限付与を実施する
	FIA_ATD.1	セキュリティ属性を利用者に関連付けて権限付与を支援する
	FIA_SOS.1	秘密の仕様を要求して権限付与を支援する
	FIA_UAU.1	**利用者認証を要求して権限付与を実施する**
	FIA_UAU.7	利用者認証を要求して権限付与を実施する
	FIA_UID.1	**利用者識別を要求して権限付与を実施する**
	FIA_USB.1	**利用者の役割に関連付けられたサブジェクトのセキュリティ属性を区別して権限付与を実施する**

	FMT_MSA.1(b)	セキュリティ属性管理を実施してアクセス制御機能を支援する
	FMT_MSA.3(b)	デフォルトのセキュリティ属性管理を実施してアクセス制御機能を支援する。
	FMT_SMR.1	セキュリティの役割を要求して権限付与を支援する
	FTA_SSL.3	**休止中のセッションを終了して権限付与を実施する**
O.INTERFACE.MANAGED （外部インターフェイスの管理）	**FIA_UAU.1**	**利用者認証を要求して外部インターフェイス管理を実施する**
	FIA_UID.1	**利用者識別を要求して外部インターフェイス管理を実施する**
	FPT_FDI_EXP.1	**（必要に応じて、）外部インターフェイスから共有メディアインターフェイスへのデータ転送を管理者が管理することを要求して、外部インターフェイスの管理を実施する**
	FTA_SSL.3	**休止中のセッションを終了して外部インターフェイスの管理を実施する**
O.SOFTWARE.VERIFIED （ソフトウェア完全性の検証）	**FPT_TST.1**	**自己テストを要求してソフトウェア検証を実施する**
O.AUDIT.LOGGED （監査対象事象の記録）	**FAU_GEN.1**	**関連事象のロギングを要求して監査方針を実施する**
	FAU_GEN.2	**監査対象事象に関連付けられた情報のロギングを要求して監査方針を実施する**
	FIA_UID.1	利用者識別を事象に関連付けて監査方針を支援する
	FPT_STM.1	事象に関連付けられたタイムスタンプを要求して監査方針を支援する
O. AUDIT_STORAGE.PROTECTED （不正なアクセス、削除、及び改変からの監査データの保護）	**FAU_STG.1**	**権限付与されていない削除や改変から保護して監査方針を実施する**
	FAU_STG.4	**監査データの損失を防止して監査方針を実施する**
O. AUDIT_ACCESS.AUTHORIZED （セキュリティ監査記録の監査）	**FAU_SAR.1**	**セキュリティ監査記録を提供して監査方針を実施する**
	FAU_SAR.2	**セキュリティ監査記録の読み出しを制限して監査方針を実施する**

6.3.2.Security Assurance Requirements rationale

This Security Target has been developed for Hardcopy Devices used in restrictive commercial informati on processing environments that require a relatively high level of document security, operational accoun tability, and information assurance. The TOE environment will be exposed to only a low level of risk b ecause it is assumed that the TOE will be located in a restricted or monitored environment that provid es almost constant protection from unauthorized and unmanaged access to the TOE and its data interf aces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except f or removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating t he TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintenti onal malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their incl usion is expected by the consumers of this TOE.

6.3.3.依存性分析

TOE セキュリティ機能要件に関して、本 ST における依存性の分析結果を表 6-16 に示す。

表 6-16. TOE セキュリティ機能要件の依存性分析結果

機能要件	CC にて要求される依存性	本 ST における依存関係
FAU_GEN.1	・FPT_STM.1	・FPT_STM.1
FAU_GEN.2	・FAU_GEN.1 ・FIA_UID.1	・FAU_GEN.1 ・FIA_UID.1
FAU_SAR.1	・FAU_GEN.1	・FAU_GEN.1
FAU_SAR.2	・FAU_SAR.1	・FAU_SAR.1
FAU_STG.1	・FAU_GEN.1	・FAU_GEN.1
FAU_STG.4	・FAU_STG.1	・FAU_STG.1
FDP_ACC.1(a)	・FDP_ACF.1	・FDP_ACF.1(a)
FDP_ACC.1(b)	・FDP_ACF.1	・FDP_ACF.1(b)
FDP_ACF.1(a)	・FDP_ACC.1 ・FMT_MSA.3	・FDP_ACC.1(a) ・FMT_MSA.3(a)
FDP_ACF.1(b)	・FDP_ACC.1 ・FMT_MSA.3	・FDP_ACC.1(b) ・FMT_MSA.3(b)
FDP_RIP.1	・なし	・なし
FIA_AFL.1	・FIA_UAU.1	・FIA_UAU.1
FIA_ATD.1	・なし	・なし
FIA_SOS.1	・なし	・なし
FIA_UAU.1	・FIA_UID.1	・FIA_UID.1
FIA_UAU.7	・FIA_UAU.1	・FIA_UAU.1

FIA_UID.1	・なし	・なし
FIA_USB.1	・FIA_ATD.1	・FIA_ATD.1
FMT_MSA.1(a)	・[FDP_ACC.1 or FDP_IFC.1] ・FMT_SMR.1 ・FMT_SMF.1	・FDP_ACC.1(a) ・FMT_SMR.1 ・FMT_SMF.1
FMT_MSA.1(b)	・[FDP_ACC.1 or FDP_IFC.1] ・FMT_SMR.1 ・FMT_SMF.1	・FDP_ACC.1(b) ・FMT_SMR.1 ・FMT_SMF.1
FMT_MSA.3(a)	・FMT_MSA.1 ・FMT_SMR.1	・FMT_MSA.1(a) ・FMT_SMR.1
FMT_MSA.3(b)	・FMT_MSA.1 ・FMT_SMR.1	・FMT_MSA.1(b) ・FMT_SMR.1
FMT_MTD.1	・FMT_SMR.1 ・FMT_SMF.1	・FMT_SMR.1 ・FMT_SMF.1
FMT_SMF.1	・なし	・なし
FMT_SMR.1	・FIA_UID.1	・FIA_UID.1
FPT_FDI_EXP.1	・FMT_SMF.1 ・FMT_SMR.1	・FMT_SMF.1 ・FMT_SMR.1
FPT_STM.1	・なし	・なし
FPT_TST.1	・なし	・なし
FTA_SSL.3	・なし	・なし
FTP_ITC.1	・なし	・なし

以上より、全ての依存性を満たしている。

7. TOE Summary Specification

本章は、TOE 要約仕様を記す。

7.1. ユーザ識別・認証機能

ユーザ識別・認証機能とは、TOE に対する利用者を識別認証する機能のことである。ユーザ識別・認証機能に対応するセキュリティ機能要件は以下の通り。

- FIA_AFL.1、FIA_ATD.1、FIA_SOS.1、FIA_UAU.1、FIA_UAU.7、FIA_UID.1、FIA_USB.1、FTA_SSL.3

(1) FIA_AFL.1 認証失敗時の取扱い

TOE は、ログオンまたは認証に失敗した場合、表 7-1 に示す通り、当該アカウントをロック状態にする。また、各ロックアウトは、ユーザ単位ではなくインターフェイス単位に実行される。

表 7-1. 認証失敗時アクションのリスト

ログオンまたは認証のパターン	認証不成功時のアクション
管理者による操作パネルからのログオン	0.6 秒間、当該管理者をロックアウトする
一般利用者による操作パネルからのログオン	0.6 秒間、当該一般利用者をロックアウトする
管理者による Web Config からのログオン	1 秒間、当該管理者をロックアウトする
パスワード付き印刷ジョブ受付時の認証	1 秒間、当該一般利用者をロックアウトする

(2) FIA_ATD.1 利用者属性定義

TOE は、表 7-2 に示す通り、利用者属性を定義し、維持する。

表 7-2. セキュリティ属性のリスト

利用者	セキュリティ属性
U.NORMAL	一般利用者 User ID 利用者役割 利用機能リスト
U.ADMINISTRATOR	利用者役割

(3) FIA_SOS.1 秘密の検証

TOE は、パスワード（一般利用者パスワードまたは管理者パスワード）が定義された品質尺度に合致するか否かを検証する。品質尺度とは、以下の通り。

- 桁数：8 桁以上（最大 20 桁まで）とすること
- 文字種：必ず、以下の文字を 1 文字以上含むこと
  - 英大文字
  - 英小文字
  - 数字
  - 記号（!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ ）

(4) FIA_UAU.1 認証のタイミング

FIA_UID.1　　識別のタイミング

TOE は、一般利用者がログオン時に入力する一般利用者 User ID 及び一般利用者パスワードに関して、TOE 内部に登録された一般利用者 User ID 及び一般利用者パスワードに一致することを検証する。TOE は、一般利用者が発行したパスワード付き印刷ジョブ受付時、TOE 内部に登録された一般利用者 User ID 及び一般利用者パスワードに一致することを検証する。TOE は、管理者がログオン時に入力する管理者 User ID 及び管理者パスワードに関して、TOE 内部に登録された管理者 User ID 及び管理者パスワードに一致することを検証する。TOE は、一般利用者及び管理者による識別認証が実施される前に、以下のアクションを許可する。

- 操作パネルでのプリンター情報の表示
- 操作パネルからのプリンター情報の印刷
- 操作パネルでのネットワーク情報の表示
- 操作パネルからのネットワーク情報の印刷
- 操作パネルでのジョブ一覧の表示
- 操作パネルでのヘルプの表示
- Web Config でのプリンター情報の表示
- Web Config でのネットワーク情報の表示
- 操作パネルでの FAX 情報の表示
- 操作パネルからの FAX 情報の印刷
- 操作パネルからのプリンターメンテナンス機能の実行
- プリンタードライバーでのプリンターステータスの表示

(5) FIA_UAU.7　　保護された認証フィードバック

TOE は、操作パネルまたは Web Config からのログオンに際し、パスワード入力時、表 7-3 に示すダミー文字をログオン画面に表示する。

表 7-3. パスワード入力時のダミー文字

アクション主体	ダミー文字
管理者による操作パネルからのログオン	入力回数分の＊文字
一般利用者による操作パネルからのログオン	入力回数分の＊文字
管理者による Web Config からのログオン	入力回数分のマスク文字 ※マスクする文字種はブラウザーに依存する

(6) FIA_USB.1　　利用者-サブジェクト結合

TOE は、利用者が識別認証に成功した場合、表 7-4 に示す通り、一般利用者 User ID、利用者役割、及び利用機能リストの利用者属性をサブジェクトに関連付ける。

表 7-4. 属性の最初の関連付け規則

利用者	サブジェクト	利用者セキュリティ属性
一般利用者	U.NORMAL	一般利用者 User ID 利用者役割 利用機能リスト

管理者	U.ADMINISTRATOR	利用者役割

(7) FTA_SSL.3 TSF 起動による終了

TOE は、表 7-5 に示す通り、操作パネルまたは Web Config からの操作に際し、一定時間無操作状態が継続した場合、自動的にログオフする。

表 7-5. 利用者が非アクティブである時間間隔

アクション	利用者が非アクティブである時間間隔
管理者による操作パネルからのログオン	「無操作タイマー設定」指定時間 （管理者により、10 秒から 240 分の範囲で指定可能）
一般利用者による操作パネルからのログオン	「無操作タイマー設定」指定時間 （管理者により、10 秒から 240 分の範囲で指定可能）
管理者による Web Config からのログオン	20 分

7.2. 利用者データアクセス制御機能

利用者データアクセス制御機能とは、利用者データに対する操作を制御する機能のことである。利用者データアクセス制御機能に対応するセキュリティ機能要件は以下の通り。

- FDP_ACC.1(a)、FDP_ACF.1(a)、FMT_MSA.3(a)

(1) FDP_ACC.1(a) サブセットアクセス制御

FDP_ACF.1(a) セキュリティ属性によるアクセス制御

TOE は、表 7-6 に示す基本機能により生成される D.DOC 及び D.FUNC に対し、各利用者に対するアクセス制御規則に則り、許可された利用者のみにデータへのアクセスを許可する。

表 7-6. 利用者データアクセス制御機能のアクセス制御規則

データ	セキュリティ属性	操作	利用者	アクセス制御規則
D.DOC （+PRT）	一般利用者 User ID 文書情報属性 「+PRT」	印刷 削除	一般利用者	一般利用者に対して、文書情報属性が「+PRT」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する ・印刷とは、プリンタードライバーから投入され一時保存された印刷データをハードコピー出力する操作である
		削除	管理者	管理者に対して、文書情報属性が「+PRT」のデータに対してのみ操作を許可する
D.DOC （+SCN）	一般利用者 User ID 文書情報属性	メール添付送信 指定フォルダ送信	一般利用者	一般利用者に対して、文書情報属性が「+SCN」かつ一般利用者の一般利用者 User ID と一致するデータに対し

	「+SCN」	削除		てのみ操作を許可する ・メール添付送信とは、D.DOC をメールに添付して送信する操作であり、スキャンとの一連の操作にて完了する ・指定フォルダ送信とは、D.DOC をネットワーク上の共有フォルダに送信する操作であり、スキャンとの一連の操作にて完了する
		メール添付送信 指定フォルダ送信 削除	管理者	管理者に対して、文書情報属性が「+SCN」のデータに対してのみ操作を許可する
D.DOC （+CPY）	一般利用者 User ID 文書情報属性 「+CPY」	コピー印刷 削除	一般利用者	一般利用者に対して、文書情報属性が「+CPY」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する ・コピー印刷とは、スキャンとハードコピー出力との一連の操作にて完了する
		コピー印刷 削除	管理者	管理者に対して、文書情報属性が「+CPY」のデータに対してのみ操作を許可する
D.DOC （+FAXIN）	文書情報属性 「+FAXIN」	FAX 受信印刷 メール添付送信 指定フォルダ送信 FAX 転送 操作パネルでのプレビュー表示 削除	一般利用者	利用機能リストに「FAX 受信機能（FAXIN）」が付与される一般利用者に対して、文書情報属性が「+FAXIN」のデータに対してのみ操作を許可する ・メール添付送信とは、D.DOC をメールに添付して送信する操作であり、FAX 受信との一連の操作にて完了する ・指定フォルダ送信とは、D.DOC をネットワーク上の共有フォルダに送信する操作であり、FAX 受信との一連の操作にて完了する ・FAX 転送とは、D.DOC を別の FAX アドレスに転送する操作であり、FAX 受信との一連の操作にて完了す

				る ・ 操作パネルでのプレビュー表示とは、D.DOC を操作パネルに表示する操作であり、FAX 受信との一連の操作にて完了する
		FAX 受信印刷 メール添付送信 指定フォルダ送信 FAX 転送 操作パネルでのプレビュー表示 削除	管理者	管理者に対して、文書情報属性が「+FAXIN」のデータに対してのみ操作を許可する
D.DOC （+FAXOUT）	一般利用者 User ID 文書情報属性 「+FAXOUT」	FAX 送信 操作パネルでのプレビュー表示 削除	一般利用者	一般利用者に対して、文書情報属性が「+FAXOUT」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する ・ 操作パネルでのプレビュー表示とは、D.DOC を操作パネルに表示する操作であり、FAX 送信との一連の操作にて完了する
		FAX 送信 操作パネルでのプレビュー表示 削除	管理者	管理者に対して、文書情報属性が「+FAXOUT」のデータに対してのみ操作を許可する
D.DOC （+DSR）	一般利用者 User ID 文書情報属性 「+DSR」	ボックス保存文書の印刷 操作パネルでのプレビュー表示 メール添付送信 指定フォルダ送信 削除	一般利用者	一般利用者に対して、文書情報属性が「+DSR」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する ・ ボックス保存文書の印刷とは、個人ボックスに保存された D.DOC をハードコピー出力する操作である ・ 操作パネルでのプレビュー表示とは、D.DOC を操作パネルに表示する操作である ・ メール添付送信とは、D.DOC をメールに添付して送信する操作であり、文書の保存と取り出しとの一連の操

				作にて完了する ・指定フォルダ送信とは、D.DOC をネットワーク上の共有フォルダに送信する操作であり、文書の保存と取り出しとの一連の操作にて完了する
		削除	管理者	管理者に対して、文書情報属性が「+DSR」のデータに対してのみ操作を許可する
D.FUNC （+PRT）	一般利用者 User ID 文書情報属性 「+PRT」	削除	一般利用者	一般利用者に対して、文書情報属性が「+PRT」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+PRT」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない
D.FUNC （+SCN）	一般利用者 User ID 文書情報属性 「+SCN」	削除	一般利用者	一般利用者に対して、文書情報属性が「+SCN」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+SCN」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない
D.FUNC （+CPY）	一般利用者 User ID 文書情報属性 「+CPY」	削除	一般利用者	一般利用者に対して、文書情報属性が「+CPY」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+CPY」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない
D.FUNC （+FAXIN）	文書情報属性 「+FAXIN」	削除	一般利用者	利用機能リストに「FAX 受信機能（FAXIN）」が付与される一般利用者に対して、文書情報属性が「+FAXIN」のデ

				ータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+FAXIN」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない
D.FUNC （+FAXOUT）	一般利用者 User ID 文書情報属性 「+FAXOUT」	削除	一般利用者	一般利用者に対して、文書情報属性が「+FAXOUT」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+FAXOUT」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない
D.FUNC （+DSR）	一般利用者 User ID 文書情報属性 「+DSR」	削除	一般利用者	一般利用者に対して、文書情報属性が「+DSR」かつ一般利用者の一般利用者 User ID と一致するデータに対してのみ操作を許可する
		削除	管理者	管理者に対して、文書情報属性が「+DSR」のデータに対してのみ操作を許可する
		修正	一般利用者 管理者	操作を許可しない

(2) FMT_MSA.3(a) 静的属性初期化

TOE は、実行される MFP 機能に応じて新規に生成される D.DOC 及び D.FUNC に対し、表 7-7 に示す属性を初期値として設定する。

表 7-7. セキュリティ属性の初期値

機能	データ	セキュリティ属性の初期値
MFP 機能 （プリント）	D.DOC（+PRT）	データを作成した一般利用者の「一般利用者 User ID」 文書情報属性（+PRT）
	D.FUNC（+PRT）	
MFP 機能 （スキャン）	D.DOC（+SCN）	データを作成した一般利用者の一般利用者 User ID ※但し、管理者の場合は識別子「Administrator」 文書情報属性（+SCN）
	D.FUNC（+SCN）	
MFP 機能 （コピー）	D.DOC（+CPY）	データを作成した一般利用者の一般利用者 User ID ※但し、管理者の場合は識別子「Administrator」 文書情報属性（+CPY）
	D.FUNC（+CPY）	

MFP 機能 （FAX 受信）	D.DOC（+FAXIN） D.FUNC（+FAXIN）	文書情報属性（+FAXIN）
MFP 機能 （FAX 送信）	D.DOC（+FAXOUT） D.FUNC（+FAXOUT）	データを作成した一般利用者の一般利用者 User ID ※但し、管理者の場合は識別子「Administrator」 文書情報属性（+FAXOUT）
MFP 機能 （文書の保存と取り出し機能）	D.DOC（+DSR） D.FUNC（+DSR）	データを作成した一般利用者の一般利用者 User ID ※但し、管理者の場合は識別子「Administrator」 文書情報属性（+DSR）

尚、FAX 受信に関する文書の owner は、管理者により利用機能リスト「FAX 受信機能（FAXIN）」を付与された一般利用者であり、FAX 送信に関する文書の owner は、管理者により利用機能リスト「FAX 送信機能（FAXOUT）」を付与された一般利用者である。また、表 7-7 に示すセキュリティ属性の初期値はデフォルト値でもあり、このセキュリティ属性によりアクセスが制限されることから制限的であり、デフォルト値と異なる初期値を定義する機能は存在しない。

7.3. TOE 機能アクセス制御機能

TOE 機能アクセス制御機能とは、TOE 機能を制御する機能のことである。TOE 機能アクセス制御機能に対応するセキュリティ機能要件は以下の通り。

- FDP_ACC.1(b)、FDP_ACF.1(b)、FMT_MSA.3(b)

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

TOE は、表 7-8 に示す基本機能に対し、各利用者に対するアクセス制御規則に則り、許可された利用者のみにジョブ実行を許可する。

表 7-8. TOE 機能アクセス制御機能のアクセス制御規則

機能	操作	利用者	アクセス制御規則
MFP 機能 （プリント）	ジョブの実行 ジョブの削除	一般利用者	利用機能リストに「プリント機能（PRT）」が付与される一般利用者に対して、操作を許可する
	ジョブの削除	管理者	管理者に対して、機能種別が「プリント属性」の機能に対してのみ操作を許可する
MFP 機能 （スキャン）	ジョブの実行 ジョブの削除	一般利用者	利用機能リストに「スキャン機能（SCN）」が付与される一般利用者に対して、操作を許可する
	ジョブの実行 ジョブの削除	管理者	管理者に対して、機能種別が「スキャン属性」の機能に対してのみ操作を許可する
MFP 機能 （コピー）	ジョブの実行 ジョブの削除	一般利用者	利用機能リストに「コピー機能（CPY）」が付与される一般利用者に対して、操作を

			許可する
	ジョブの実行 ジョブの削除	管理者	管理者に対して、機能種別が「コピー属性」の機能に対してのみ操作を許可する
MFP 機能 （FAX）	ジョブの実行 ジョブの削除	一般利用者	利用機能リストに「FAX 受信機能（FAXIN）」及び「FAX 送信機能（FAXOUT）」が付与される一般利用者に対して、操作を許可する
	ジョブの実行 ジョブの削除	管理者	管理者に対して、機能種別が「FAX 属性」の機能に対してのみ操作を許可する
MFP 機能 （文書の保存と取り出し）	ジョブの実行 ジョブの削除	一般利用者	利用機能リストに「文書の保存と取り出し機能（DSR）」が付与される一般利用者に対して、操作を許可する
	ジョブの実行 ジョブの削除	管理者	管理者に対して、機能種別が「文書の保存と取り出し属性」の機能に対してのみ操作を許可する

(2) FMT_MSA.3(b) 静的属性初期化

TOE は、新規に登録される U.NORMAL に対し、「利用機能リスト」をセキュリティ属性として設定するが、初期値は全機能を使用不可とする。セキュリティ属性の初期値はデフォルト値でもあり、このセキュリティ属性によりアクセスが制限されることから制限的であり、デフォルト値と異なる初期値を定義する機能は存在しない。

7.4. セキュリティ管理機能

セキュリティ管理機能とは、セキュリティ機能を管理する機能のことである。セキュリティ管理機能に対応するセキュリティ機能要件は以下の通り。

- FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1

(1) FMT_MSA.1(a) セキュリティ属性の管理

TOE は、管理者に対して、以下に記す操作を許可する。

- 一般利用者 User ID の削除、新規作成
- 利用機能リストの改変

利用者役割及び文書情報属性を改変できる役割はない。

(2) FMT_MSA.1(b) セキュリティ属性の管理

TOE は、管理者に対して、以下に記す操作を許可する。

- 利用機能リストの改変

利用者役割及び機能種別を改変できる役割はない。

(3) FMT_MTD.1 TSF データの管理

TOE は、TSF データに対し、表 7-9 に示す操作を許可された役割のみに各操作を許可する。

表 7-9. TSF データの管理

TSF データ	操作	操作を許可する利用者役割
一般利用者 User ID	削除、新規作成	管理者
管理者 User ID	改変	なし
スキャン/FAX/電子メールの送信先リストまたはアドレスブック	削除、新規作成	管理者
ジョブステータスログ	改変	なし
パスワードポリシー	改変	管理者
無操作タイマー設定	改変	管理者
管理者認証設定（操作パネル）	改変	管理者
利用者制限設定	改変	管理者
IPsec の設定	改変	管理者
時刻設定	改変	管理者
ネットワーク設定	改変	管理者
ファームウェアの完全性検証のためのハッシュ値	改変	なし
一般利用者パスワード	削除、新規作成	管理者
	問い合わせ	なし
管理者パスワード	改変	管理者
	問い合わせ	なし
メールサーバーやファイルサーバーなどの外部装置にアクセスするためのパスワード	新規作成、改変	管理者
	問い合わせ	なし
IPsec の事前共有鍵	改変	管理者
	問い合わせ	なし

(4) FMT_SMF.1 管理機能の特定

TOE は、以下に記すセキュリティ管理機能を提供する。

表 7-10. 管理機能のリスト

管理機能
U.ADMINISTRATOR による「一般利用者 User ID」の登録・削除
U.ADMINISTRATOR による「スキャン/FAX/電子メールの送信先リストまたはアドレスブック」の登録・削除
U.ADMINISTRATOR による「パスワードポリシー」の変更
U.ADMINISTRATOR による「無操作タイマー設定」の変更
U.ADMINISTRATOR による「管理者認証設定（操作パネル）」の変更
U.ADMINISTRATOR による「利用者制限設定」の変更

U.ADMINISTRATOR による「IPsec の設定」の変更
U.ADMINISTRATOR による「時刻設定」の変更
U.ADMINISTRATOR による「ネットワーク設定」の変更
U.ADMINISTRATOR による「U.NORMAL の一般利用者パスワード」の登録・削除
U.ADMINISTRATOR による「U.ADMINISTRATOR の管理者パスワード」の変更
U.ADMINISTRATOR による「メールサーバーやファイルサーバーなどの外部装置にアクセスするためのパスワード」の登録・変更
U.ADMINISTRATOR による「IPsec の事前共有鍵」の変更

(5) FMT_SMR.1 セキュリティの役割

TOE は、以下に記す役割を維持し、利用者を役割に関連付ける。

- 一般利用者
- 管理者

7.5. 残存データ消去機能

残存データ消去機能とは、削除された文書及び一時的に保存された文書を HDD 及び Flash ROM から完全に消去し、再利用不可とする機能のことである。残存データ消去機能に対応するセキュリティ機能要件は以下の通り。

- FDP_RIP.1

(1) FDP_RIP.1 サブセット情報保護

TOE は、基本機能による各ジョブ完了後、HDD や Flash ROM に保存された D.DOC を消去する。D.DOC に使用されていた領域は、特定の値（0x00）により順次上書き消去する。HDD の上書き消去に関して、TOE 起動時、及び監視プロセスにより、残存データを発見した場合、上書き消去する。また、TOE は、操作パネルからの手動操作により、上書き消去も可能とする。

7.6. 自己テスト機能

自己テスト機能とは、TSF の一部が正常動作すること、TSF データの一部及び TSF 実行コードが完全であることを、MFP 本体起動時に検証する機能のことである。自己テスト機能に対応するセキュリティ機能要件は以下の通り。

- FPT_TST.1

(1) FPT_TST.1 TSF テスト

TOE は、MFP 本体起動時に、以下に記す自己テストを実行する。

- ファームウェアのファイルからハッシュ値を計算し、TOE 内に格納された値（ファームウェアの完全性検証のためのハッシュ値）と一致することを確認することにより、TSF データの一部（ファームウェアのハッシュ値）及び TSF 実行コードの完全性を検証すると共に、TSF の一部の正常動作を検証する機能を提供する

本自己テストにて異常が認められた場合、TOE は、MFP の操作パネルにエラーメッセージを表示し、その後のいかなる操作も許可しない。

7.7. 監査ログ機能

監査ログ機能とは、TOE の使用及びセキュリティ関連事象を監査ログとして記録し、参照する機能のことである。監査ログ機能に対応するセキュリティ機能要件は以下の通り。

- FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4、FPT_STM.1

(1) FAU_GEN.1 監査データ生成

TOE は、表 7-11 に示す監査対象事象が発生した際、監査データを生成し、監査ログとして記録する。

表 7-11. 監査対象事象

監査対象事象	監査データ	追加情報
監査ログ機能の開始（成功）	・ 監査対象事象の発生日時 ・ 監査対象事象の種別 ・ 監査対象事象のサブジェクト識別情報 ・ 監査対象事象の結果	・ なし
監査ログ機能の終了（成功）		・ なし
認証メカニズムの使用（成功/失敗）		・ なし
識別メカニズムの使用（成功/失敗）		・ なし
管理機能の使用（成功/失敗）		・ なし
時刻の変更（成功/失敗）		・ なし
IPsec 通信の失敗		・ 通信先 IP アドレス

識別メカニズムと認証メカニズムは一体であることから、識別認証に失敗した場合、「識別のみの失敗」を把握する必要はない。従って、監査対象事象「識別メカニズムの使用（成功/失敗）」の追加情報として、「利用者識別の試行」は該当しない。

(2) FAU_GEN.2 利用者識別情報の関連付け

監査対象事象が利用者のアクションによってもたらされたものであるとき、TOE は、その原因となった利用者の識別情報を監査対象事象に関連付ける。

(3) FAU_SAR.1 監査レビュー

TOE は、監査ログの読み出しを管理者に許可する。また、TOE は、管理者が監査ログを解釈できる形式に変換して提供する。管理者は Web Config にログオンし、監査ログ（CSV 形式ファイル）を入手する。

(4) FAU_SAR.2 限定監査レビュー

TOE は、監査ログの読み出しを管理者のみに許可する。

(5) FAU_STG.1 保護された監査証跡格納

TOE は、全ての利用者に対して監査ログの編集を許可しない。また、TOE は監査ログの削除を管理者のみに許可する。

(6) FAU_STG.4 監査データ損失の防止

TOE は、監査ログが満杯になった場合、最も古い日時に格納された監査ログに対して上書きする。

(7) FPT_STM.1　　高信頼タイムスタンプ

TOE は、TOE 内部にシステム時計を有する。監査対象事象が発生した場合、このシステム時計から発生日時を監査ログに記録する。システム時計は、NTP サーバーから正確な日時を取得し、同期させることも可能。

7.8. ネットワーク保護機能

ネットワーク保護機能とは、LAN 利用時、ネットワークの盗聴による情報漏えい及び改変を防止する機能のことである。ネットワーク保護機能に対応するセキュリティ機能要件は以下の通り。

- FPT_FDI_EXP.1、FTP_ITC.1

(1) FPT_FDI_EXP.1　　外部インターフェイスへの制限された情報転送

TOE は、以下の通り、有線 LAN と電話回線の情報転送を固定的に制限する。

- TOE は、有線 LAN から入力された情報を電話回線へ TSF による追加の処理なしに直接転送しない
- TOE は、電話回線から入力された情報を有線 LAN へ TSF による追加の処理なしに直接転送しない

(2) FTP_ITC.1　　TSF 間高信頼チャネル

TOE は、MFP 本体と各種サーバーやクライアント PC と通信する際、高信頼チャネルを介して通信する。TOE は、高信頼チャネルとして、IPsec 暗号化通信を提供する。IPsec 暗号化通信に関する仕様を表 7-12 に示す。

表 7-12. IPsec 仕様

項目	詳細
暗号アルゴリズム	AES(128bits,192bits,256bits)