KONICA MINOLTA bizhub 4750i/bizhub 4050i with FK-517, DEVELOP ineo 4750i/ineo 4050i with FK-517 セキュリティターゲット

バージョン：2.00

発行日：2021年3月3日

作成者：コニカミノルタ株式会社

―【 目次 】――――――――――――――――――――――――――――――

―【 図目次 】――――――――――――――――――――――――――――――――

―【 表目次 】――――――――――――――――――――――――――――――――

1. ST Introduction

1.1. ST Reference

・ST名称　：KONICA MINOLTA bizhub 4750i/bizhub 4050i with FK-517, DEVELOP ineo 4750i/ineo 4050i with FK-517セキュリティターゲット
・STバージョン　：2.00
・作成日　：2021年3月3日
・作成者　：コニカミノルタ株式会社

1.2. TOE Reference

・TOE名称　：KONICA MINOLTA bizhub 4750i/bizhub 4050i with FK-517, DEVELOP ineo 4750i/ineo 4050i with FK-517
・バージョン　：G00-19

TOE の物理的コンポーネントは、MFP 本体と FAX キットの 2 つである。
本 TOE は、以下のいずれかの組み合わせから成る。

仕向	MFP 本体		FAX キット
日本以外	KONICA MINOLTA bizhub 4750i	ファームウェア (バージョン: ACT90Y0-F000-G00-19)	FK-517 (AA1K)
日本／日本以外	KONICA MINOLTA bizhub 4050i		
日本以外	DEVELOP ineo 4750i		
	DEVELOP ineo 4050i		

1.3. TOE Overview

1.3.1. TOE の種別

TOE はネットワーク環境(LAN)で使用されるデジタル複合機（MFP）であり、コピー、スキャン、プリント、ファクス、文書の保存と取り出しを行う機能を有する。

1.3.2. 使用法と主要なセキュリティ機能

TOE は、LAN と公衆回線に接続され、利用者がプリント、スキャン、コピー、ファクス、文書の保存と取り出しを行う機能を備えている。また、利用者の文書やセキュリティ関連データを保護するため、下記セキュリティ機能を備える。

利用者を特定する識別認証機能、利用者に与えられた権限に従って文書へのアクセスや TOE の各種操作を制限するアクセス制御機能、セキュリティ機能の設定を管理者の権限を持つ利用者に制限するセキュリティ管理機能、セキュリティ関連の事象を記録し、ログサーバーへ送信する監査機能、TOE と外部 IT 機器との通信を IPsec によって保護する高信頼通信機能、高信頼通信機能において通信データの暗号化に利用する暗号化機能、PSTN と LAN 間の分離を保証する FAX 分離機能、不正ファームウェアによるアップデートを防止するアップデート機能と

TSF の正常動作を実証する自己テスト機能による高信頼な運用機能。

1.3.3. 運用環境

TOE の運用環境を図 1-1 に示す。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って TOE を操作することが出来る。

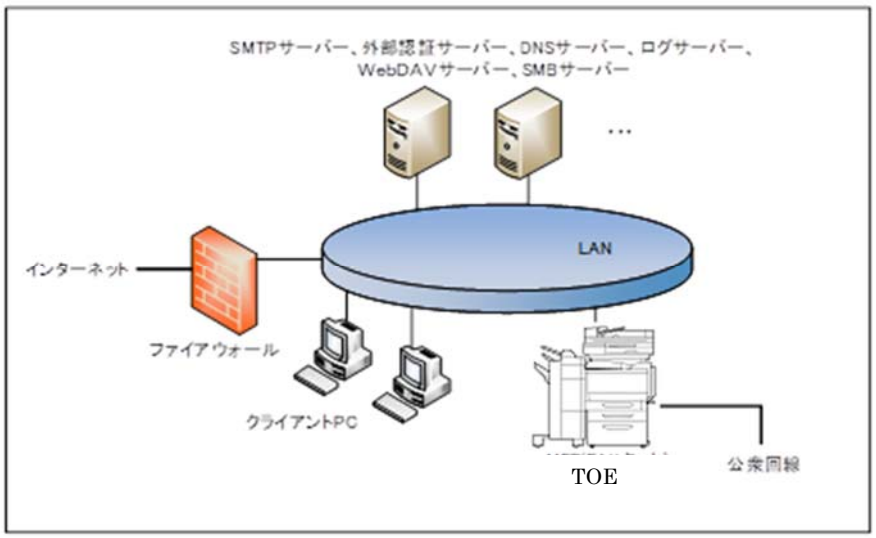

図 1-1 TOE の運用環境

(1) TOE(MFP 本体)
TOE はオフィス内 LAN と公衆回線に接続され、下記機能を処理する。
・電子文書の受信
・ファクス受信
利用者は操作パネルから以下の処理を行うことができる。
・MFP の各種設定
・紙文書のコピー・ファクス送信・電子文書としての蓄積・ネットワーク送信
・蓄積文書の印刷・ファクス送信・ネットワーク送信・削除

(2) TOE(FAX キット)
TOE でファクス機能を使用するため必要な装置。MFP 本体に装着する。

(3) LAN
TOE の設置環境で利用されるネットワーク。

(4) 公衆回線
外部ファクスと送受信するための電話回線。

(5) ファイアウォール
インターネットからオフィス内 LAN へのネットワーク攻撃を防止するための装置。

(6) クライアント PC

LAN に接続することによって TOE のクライアントとして動作する。利用者は、クライアント PC にプリンタドライバーをインストールすることで、クライアント PC から TOE にアクセスし以下の操作を行うことができる。

・電子文書の蓄積・印刷

また、利用者は、クライアント PC に Web ブラウザをインストールすることで、クライアント PC から TOE にアクセスし、以下の操作を行うことができる。

・WC

(7) SMTP サーバー

スキャンしたデータや TOE 内に保存されている電子文書を E メール送信する場合に使用されるサーバー。

(8) 外部認証サーバー

TOE の利用者を識別認証するサーバー。外部サーバー認証方式で運用する場合だけ必要となる。外部サーバー認証方式においては Kerberos 認証を用いる。

(9) DNS サーバー

ドメイン名を IP アドレスに変換するサーバー。

(10) ログサーバー

TOE の監査ログ送信機能の送信先となるサーバー。利用者は監査ログが記録されたファイルの送信先として WebDAV サーバーを指定できる。

(11) WebDAV サーバー

スキャンしたデータや TOE 内に保存されている電子文書を TOE から送信し、格納するサーバー。

(12) SMB サーバー

スキャンしたデータや TOE 内に保存されている電子文書を TOE から送信し、格納するサーバー。

1.3.4. TOE に必要な TOE 以外のハードウェア／ソフトウェア

TOE を利用するにあたって必要となるハードウェア/ソフトウェアとして、TOE 評価に用いた構成を以下に示す。

Table 1-1 評価構成

ハードウェア/ソフトウェア		評価で使用したバージョン等
クライアントPC(OS)		Windows 10 Pro
	Webブラウザ	Microsoft Internet Explorer 11
	プリンタドライバー	KONICA MINOLTA 4750iSeries PCL / PS Version 2.1.13.0
	IPsec	OS内蔵
外部認証サーバー		Microsoft Windows Server 2012 R2に搭載されるActiveDirectory
	DNSサーバー（注）	OS内蔵
	IPsec	OS内蔵
SMTPサーバー		Postfix 3.4.5
	IPsec	strongswan 5.8.0

ハードウェア/ソフトウェア		評価で使用したバージョン等
DNSサーバー		bind9 9.11.5
	IPsec	strongswan 5.8.0
ログサーバー		apache2 2.4.38
	IPsec	strongswan 5.8.0
WebDAVサーバー		apache2 2.4.38
	IPsec	strongswan 5.8.0
SMBサーバー		samba 4.9.5
	IPsec	strongswan 5.8.0

(注)外部認証を使用する場合は、Microsoft Windows Server 2012 R2 の DNS サーバーを使用する必要があります。

1.4. TOE Description

本章では TOE の物理的範囲、論理的範囲の概要を記述する。

1.4.1. TOE の物理的範囲

TOE の物理的範囲は、必須オプションである FAX キットを装着した MFP 本体である。TOE は、MFP 本体(ファームウェア内蔵)、FAX キット、ガイダンスの単位で配付される。TOE を構成するハードウェア／ソフトウェア、ガイダンスを下記に示す。

MFP 本体には USB IF が実装されているが、運用中はアップデート機能でのみ有効化されるため、利用者が個人的なストレージデバイス(ポータブルフラッシュメモリデバイス等)を接続して利用することはできない。また、MFP 本体には RS-232C IF が実装されているが、運用中は無効化されているため、利用者が本インタフェースを利用することはできない。

Table 1-2 TOE を構成するハードウェア／ソフトウェア

配付単位	商品名	バージョン/部品番号	形式	配付方法
MFP 本体(右のいずれか)	bizhub 4750i	ファームウェアバージョン ACT90Y0-F000-G00-19	バイナリ形式のファームウェアを内蔵したハードウェア	専用箱に梱包して業者により配送する。
	bizhub 4050i			
	ineo 4750i			
	ineo 4050i			
FAX キット	FK-517	部品番号 AA1K	ハードウェア	専用箱に梱包して業者により配送する。

Table 1-3 TOE を構成するガイダンス

配付単位	ガイダンス名称	バージョン	言語	形式	配付方法
FULL 版	bizhub 4050i ユーザーズガイド	1.00	日本語	exe ファイル(*2)（電子署名付与）	サービスマンが持参する(*1)。
	bizhub 4750i/4050i User's Guide	1.00	英語		
	ineo 4750i/4050i User's Guide	1.00	英語		
セキュリティ機能編	bizhub 4050i ユーザーズガイド セキュリティ機能編	1.02	日本語	exe ファイル(*3)	サービスマンが持参する(*1)。

	bizhub 4750i/4050i User's Guide [Security Operations]	1.02	英語	（電子署名付与）	
	ineo 4750i/4050i User's Guide [Security Operations]	1.02	英語		

(*1)MFP 本体に対応するガイダンス（FULL 版とセキュリティ機能編）をサービスマンが配付する。言語は日本語版と英語版があり、日本仕向けは購入者が希望する版を配付し、日本以外仕向けは、英語版を配付する。
(*2)exe ファイルを実行することで html ファイルを入手する。
(*3)exe ファイルを実行することで pdf ファイルを入手する。

1.4.2. TOE の論理的範囲

以下に TOE のセキュリティ機能と基本機能を記述する。

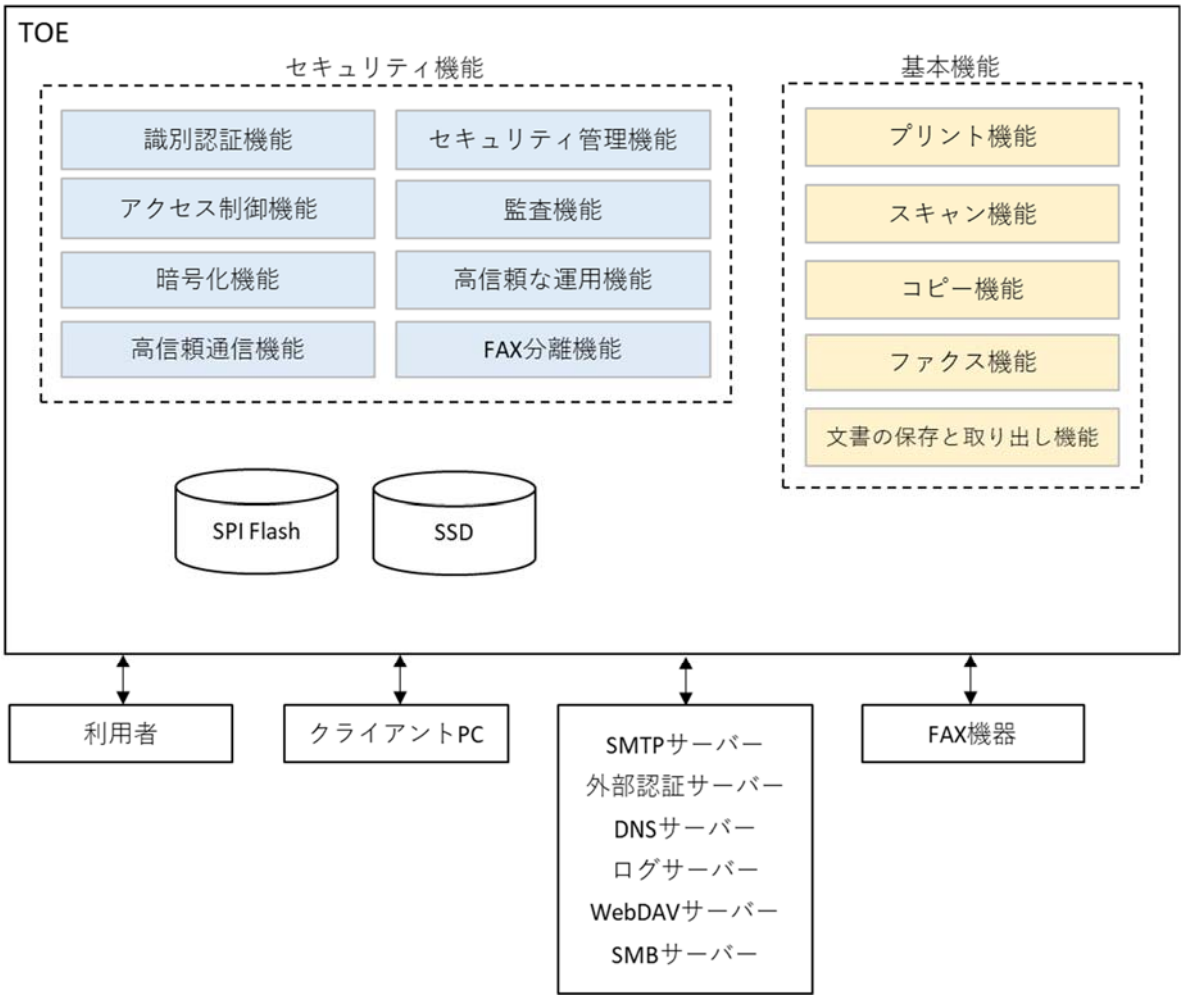

図 1-2 TOE の論理的範囲

1.4.2.1. 基本機能

以下に、TOE の基本機能を記述する。

Table 1-4 TOE の基本機能

No.	Function	Definition
1	プリント機能	利用者が LAN 経由で電子文書を TOE に一時保存し、印刷する機能。 クライアント PC のプリンタドライバーもしくは WC から、認証&プリントボックスに電子文書を一時保存できる。また、WC からパスワード暗号化 PDF ボックスへ電子文書を一時保存できる。利用者が操作パネルから一時保存した電子文書の印刷を実行した場合、該当電子文書は TOE から削除される。
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って、紙文書をスキャナで読み取り、電子文書に変換して、送信（E-mail、WebDAV、SMB）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って、紙文書をスキャナで読み取って、読み取った画像を複写印刷する機能。
4	ファクス機能	標準ファクシミリプロトコルを用いて、公衆電話回線交換網(PSTN)を介して文書を送受信する機能。 ・ファクス送信機能 操作パネルから送信先を指定し、紙文書をスキャナで読み取り、電子文書に変換して、指定した外部ファクスへ送信する機能。操作パネルから、個人ボックスに保存されている電子文書をファクス送信することもできる。 ・ファクス受信機能 外部ファクスから電話回線を介して電子文書を受信する機能。
5	文書の保存と取り出し機能	個人ボックス、強制メモリ受信ボックス、パスワード暗号化PDFボックスに電子文書を保存、もしくは保存した電子文書を取り出す機能。 個人ボックスに対して、紙文書をスキャナで読み取り、電子文書に変換して保存、クライアント PC のプリンタドライバーもしくは WC から電子文書を保存、ファクス機能によって受信した F コード付きファクス文書を保存できる。強制メモリ受信ボックスに対して、ファクス機能によって受信したファクス文書を保存できる。パスワード暗号化 PDF ボックスに対して、クライアント PC の WC から電子文書を保存できる。 個人ボックスに保存された電子文書は、操作パネルから印刷、SMTP サーバー/WebDAV サーバー/SMB サーバーへのファイル送信、ファクス送信、WC から SMTP サーバー/WebDAV サーバー/SMB サーバーへのファイル送信、ダウンロードができる。強制メモリ受信ボックスに保存された電子文書は、操作パネルから印刷、WC からダウンロードができる。パスワード暗号化 PDF ボックスに保存された電子文書は、操作パネルから個人ボックスへの保存ができる。

1.4.2.2. セキュリティ機能

以下に、TOE のセキュリティ機能を記述する。

ストレージデバイス上の暗号化に関する機能は、TOE が提供するセキュリティ機能に含まれない。

Table 1-5 TOE のセキュリティ機能

No.	Function	Definition
1	識別認証機能	TOE を利用しようとする者が許可利用者であることを利用者から取得した識別認証情報を使って検証し、許可利用者と判断された者だけに TOE の利用を許可する機能。強制メモリ受信ボックスへアクセスする場合（ファクス受信を除く）、利用者の識別認証に加え、強制メモリ受信ボックスパスワードによる認証も実施する。認証方式には TOE 自身が識別認証を行う本体装置認証方式と外部の認証サーバーを使用する外部サーバー認証方式がある。本機能には以下の機能が含まれる。 ・連続した認証失敗回数が設定値に達した場合に認証を停止する機能 ・ログイン時に、入力したパスワードをダミー文字で表示する機能 ・パスワードの品質を保護するために管理者が予め設定した最小パスワード長の条件を満たしたパスワードだけを登録する機能 ・識別認証されたユーザーの操作が一定時間ない（管理者が設定した時間ない）場合、そのセッションを終了する機能
2	アクセス制御機能	TOE 内の保護資産に対し、許可された利用者のみがアクセス可能となるように、保護資産へのアクセスを制限する機能。
3	暗号化機能	LAN 上での通信中に、データ資産へアクセスできないように暗号化する機能。データ暗号化の有効性は、国際的に承認された暗号アルゴリズムの使用により保証される。
4	高信頼通信機能	LAN 利用時にネットワーク上の盗聴による情報漏えいを防止する機能。IPsec によって通信路を保護する。クライアント PC、SMTP サーバー、外部認証サーバー、DNS サーバー、ログサーバー、WebDAV サーバー、SMB サーバーと TOE の間の通信データを暗号化する。3.暗号化機能によってネットワーク上を流れる保護資産を暗号化することで保護する。 通信が既知の終端との間で行われることを保証する機能。
5	セキュリティ管理機能	識別認証機能で認証された管理者(U.ADMIN)、一般利用者（U.NORMAL）が、それぞれの役割に提供された TOE のセキュリティ機能に関する設定、参照が可能であることを保証する機能。
6	監査機能	TOE の使用およびセキュリティに関連する事象（以下、監査事象という）のログを日時情報等とともに監査ログデータとして記録する機能。プロトコルは WebDAV を使用する。ログファイルは、高信頼通信機能を用いてログサーバーに送信され、ログサーバーから閲覧することができる。内部監査ログ格納機能はサポートしない。
7	高信頼な運用機能	TOE のファームウェアアップデートを開始する前に、アップデート対象のファームウェアの真正性を検証し、それが正規のものであることを確認する機能(アップデート機能)。TOE の起動時に異常を検出し操作を受け付けない状態に移行することでファームウェアの完全性を保証する機能(自己テスト機能)。
8	FAX 分離機能	TOE のファクス I/F が、PSTN と LAN 間のデータ・ブリッジを生成するために使えないことを保証する機能。

1.4.3. 用語

本 ST で使用する用語の意味を定義する。

Table 1-6 用語

Designation	Definition
電子文書	電子文書は、文字や図形などの情報を電子化した文書データである。
紙文書	紙文書は、文字や図形などの情報を持つ紙媒体の文書である。
蓄積文書	保存と取り出しの対象となる(Storage and retrieval による操作の対象となる)電子文書。
ファクス文書	ファクス機能により公衆回線を介して外部ファクスと送受信する文書。
ジョブ	ハードコピー装置に送出される文書処理タスク。単一の処理タスクは 1 本以上の文書を処理できる。
WC	Web Connection。クライアント PC の Web ブラウザを通して TOE を操作する機能、インタフェース。
操作パネル	TOE を操作するための専用コントロールデバイス。タッチパネル液晶ディスプレイで構成される。
スキャナユニット	TOE で紙文書から図形、写真を読み取り、電子データに変換するためのデバイス。
プリンタユニット	TOE で印刷用に変換された画像データを印刷出力するデバイス。
制御コントローラユニット	TOE を制御する装置。
ファームウェア	TOE を制御するソフトウェア。
CPU	中央演算処理装置。
RAM	作業領域として利用される揮発メモリ。
SPI Flash	TOE の動作を決定する TSF データが保存される現地交換不可な不揮発メモリ。
SSD	256GB の現地交換不可な記憶媒体。ファームウェア、操作パネルやネットワークからのアクセスに対するレスポンス等で表示するための各国言語データ、TOE の設定値データ、電子文書がファイルとして保存される。
Ethernet I/F	TOE と LAN を接続するためのインタフェース。10BASE-T、100BASE-TX、Gigabit Ethernet をサポートする。
USB I/F	TOE と USB デバイスを接続するためのインタフェース。
RS-232C I/F	D-sub9 ピンを介して、TOE へシリアル接続することができるインタフェース。TOE 故障時にサービスマンがメンテナンス機能で使用する。
SMB 送信	スキャンしたデータや TOE 内に保存されている電子文書などを、コンピューターで扱えるファイルに変換して、コンピューターやサーバーの共有フォルダーへ送信する機能。
WebDAV 送信	スキャンしたデータや TOE 内に保存されている電子文書などを、コンピューターで扱えるファイルに変換して、WebDAV サーバーにアップロードする機能。ログサーバーへログ送信する場合にも使用する。
ボックス	プリント機能、ファクス機能、文書の保存と取り出し機能において、利用者文書データや利用者ジョブデータを TOE に蓄積する機能。運用中は、認証&プリントボックス、パスワード暗号化 PDF ボックス、強制メモリ受信ボックス、個人ボックスが利用できる。
認証&プリントボックス	一般利用者が、クライアント PC のプリンタドライバー、もしくは WC からプリント機能を実行した時、電子文書が一時保存される。一般利用者は、操作パネルから一時保存された電子文書の印刷を実行することができる。

Designation	Definition
パスワード暗号化 PDF ボックス	一般利用者が、クライアント PC の WC からパスワードで暗号化された PDF の印刷もしくは保存を実行した時、電子文書が一時保存される。一般利用者は、操作パネルから一時保存された電子文書の印刷もしくは保存を実行することができる。
強制メモリ受信ボックス	ファクス機能により受信した F コードが指定されていないファクス文書を保存する。管理者が強制メモリ受信設定で強制メモリ受信を有効に設定した場合に利用できる(運用中は有効に設定されている)。また、管理者が強制メモリ受信設定で設定した強制メモリ受信ボックスパスワードで保護される。強制メモリ受信ボックスパスワードを知っている一般利用者は､操作パネルとクライアント PC の WC から、ファクス文書を取り出すことができる。
個人ボックス	一般利用者が、自身が所有する個人ボックスに対し、操作パネル、クライアント PC のプリンタドライバー、もしくは WC から電子文書を保存できる。ファクス機能により受信したジョブに F コードが指定されている場合、指定された個人ボックスへファクス文書を保存する。一般利用者が、自身が所有する個人ボックスに対し、操作パネル、クライアント PC の WC から電子文書を取り出せる。
親展受信	ファクス機能により受信した F コードが指定されたファクス文書を個人ボックスへ保存する機能。個人ボックスの所有者である一般利用者と管理者が、個人ボックス毎に有効/無効と親展受信用パスワードを設定できる。
F コード	SUB アドレスと送信 ID で構成される。親展受信が有効に設定されている個人ボックスへファクス送信する際には、該当個人ボックスの登録番号と親展受信用パスワードを F コードの SUB アドレスと送信 ID として入力する。
役割	ログイン実行時、利用者に関連付けられるセキュリティ関連の役割。TOE には、一般利用者(U.NORMAL)、管理者(U.ADMIN)の役割がある。
一般利用者 (U.NORMAL)	一般利用者(U.NORMAL)としてTOEの利用を許可された利用者。利用者がユーザー名、ユーザーパスワード、管理者権限なしでログインに成功した時、一般利用者(U.NORMAL)として識別される。ユーザー画面で提供される機能を利用できる。
管理者 (U.ADMIN)	管理者(U.ADMIN)として TOE の利用を許可された利用者。TOE の管理者には、ログイン方法の違いにより、ユーザー管理者(U.USER_ADMIN)とビルトイン管理者(U.BUILTIN_ADMIN)がある。管理者画面で提供されるセキュリティ管理機能を利用できる。
ユーザー管理者 (U.USER_ADMIN)	利用者がユーザー名、ユーザーパスワード、管理者権限ありでログインに成功した時、ユーザー管理者(U.USER_ADMIN)として識別される。
ビルトイン管理者 (U.BUILTIN_ADMIN)	管理者パスワードを知る利用者。利用者が管理者パスワードでログインに成功した時、ビルトイン管理者(U.BUILTIN_ADMIN)として識別される。
サービスマン	サービスパスワードを知る利用者。利用者がサービスパスワードでログインに成功した時、サービス画面で提供される機能を利用できる。TOE の設置やトラブル対応をサポートする。
User ID	TOEが利用者を識別する識別子。利用者がログインに成功した場合、利用者属性として関連付けられる。一般利用者、ユーザー管理者の場合、ユーザー管理機能の登録番号が割り当てられる。ビルトイン管理者は、専用の固定番号が割り当てられる。
ログイン	利用者からクレデンシャルを取得して識別認証を実行し、識別認証に成功した場合、TOEを利用可能な状態にすること。操作パネル、WC、プリンタドライバーから実行できる。

Designation	Definition
ユーザー名	一般利用者、ユーザー管理者が、ログイン時にクレデンシャルとして入力する識別子。本体装置認証の場合、TOEはユーザー名によって利用者が登録ユーザーかどうかを識別する。ユーザー管理機能で一般利用者を登録する際に設定し、以降は変更できない。
ログインパスワード	利用者が、ログイン時にクレデンシャルとして入力するパスワード。本体装置認証の場合、TOEはログインパスワードによって利用者を認証する。ユーザーパスワード、管理者パスワード、サービスパスワードがある。
ユーザーパスワード	一般利用者のログインパスワード。本体装置認証の場合、管理者はユーザー管理機能で一般利用者毎にユーザーパスワードを設定できる。一般利用者は、自身のユーザーパスワードを変更できる。
管理者パスワード	ビルトイン管理者のログインパスワード。TOE出荷時は、所定の管理者パスワードが設定されており、TOE設置時にビルトイン管理者が初期値から変更する。以降、管理者が変更できる。
サービスパスワード	サービスマンのログインパスワード。
一時利用停止	管理者が一般利用者のTOEの利用を停止する機能。管理者は、ユーザー管理機能において登録されたUser ID毎に一時利用停止の設定と解除ができる。一時利用停止が設定されたUser IDを持つ一般利用者がログインを実行した場合、TOEは関連付けた利用者属性を破棄するため、該当利用者はログインに失敗し、TOEを利用できない。
管理者権限	管理者が一般利用者に管理者役割でのTOEの利用を許可する機能。管理者は、ユーザー管理機能において登録されたUser ID毎に管理者権限の設定と解除ができる。管理者権限が設定されたUser IDを持つ一般利用者が管理者権限ありでログインに成功した場合、管理者役割でTOEを利用できる。管理者権限が設定されていないUser IDを持つ一般利用者が管理者権限ありでログインを実行した場合、TOEは関連付けた利用者属性を破棄するため、該当利用者はログインに失敗し、TOEを利用できない。
機能制限	管理者が一般利用者の利用可能な機能を制限する機能。管理者は、ユーザー管理機能において登録されたUser ID毎に機能制限の設定と解除ができる。機能制限が設定されたUser IDを持つ一般利用者がログインを実行した場合、TOEは利用を制限された機能のUIを非表示もしくは操作不可状態で表示するため、制限対象の機能を利用できない。

2. Conformance Claims

2.1. CC Conformance Claims

本 ST は、以下の Common Criteria（以降、CC と記す）に適合する。

CC version	:	Version 3.1 Release 5
CC conformance	:	CC Part 2 (CCMB-2017-04-002) extended, CC Part 3 (CCMB-2017-04-003) conformant

2.2. PP Claim

本 ST は、以下の PP、Errata に適合する。

PP Name	:	Protection Profile for Hardcopy Devices
PP Version	:	1.0 dated September 10, 2015
Errata	:	Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. PP Conformance Rationale

PP が要求する以下の条件を満足し、PP の要求通り「Exact Conformance」である。そのため、TOE 種別は PP と一貫している。

・Required Uses
Printing, Scanning, Copying, Network communications, Administration
・Conditionally Mandatory Uses
PSTN faxing, Storage and retrieval
・Optional Uses
なし

3. Security Problem Definition

3.1. Users

TOE の利用者は、以下のように分類される。

Table 3-1 User Categories

名称	分類名	定義
一般利用者 (U.NORMAL)	一般利用者 (U.NORMAL)	ユーザー名、ユーザーパスワードで識別認証された利用者。一般利用者(U.NORAML)の役割を持つ。
ユーザー管理者 (U.USER_ADMIN)	管理者 (U.ADMIN)	管理者によって管理者権限を付与され、ユーザー名、ユーザーパスワード、管理者権限ありで識別認証された利用者。管理者(U.ADMIN)の役割を持つ。
ビルトイン管理者 (U.BUILTIN_ADMIN)	管理者 (U.ADMIN)	管理者パスワードによって識別認証された利用者。管理者(U.ADMIN)の役割を持つ。

3.2. Assets

TOE における保護資産は以下の通りである。

Table 3-2 Asset categories

Designation	Asset category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

3.2.1. User Data

User Data は、以下の 2 つの種別から構成される。

Table 3-3 User Data types

Designation	User Data type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

3.2.2. TSF Data

TSF Data は、以下の 2 つの種別から構成される。

Table 3-4 TSF Data types

Designation	User Data type	Definition
D.TSF.PROT	Protected TSF	TSF Data for which alteration by a User who is neither the data

Designation	User Data type	Definition
	Data	owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3. Threat Definitions

Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 3-5 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4. Organizational Security Policy Definitions

TOE が実現すべき OSP を以下に示す。

Table 3-6 Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

3.5. Assumption Definitions

Assumptions are conditions that must be satisfied in order for the Security Objectives and functional requirements to be effective.

Table 3-7 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4. Security Objectives

4.1. Definitions of Security Objectives for the Operational Environment

Table 4-1 Security Objectives for the Operational Environment

Designation	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

5. Extended components definition

本章では、拡張したセキュリティ機能要件を定義する。なお、拡張要件は全て HCD-PP で定義されているものをそのまま使用している。

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:
This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component leveling:

FAU_STG_EXT.1: Extended: External Audit Trail Storage	1

FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:
The following actions could be considered for the management functions in FMT:
- The TSF shall have the ability to configure the cryptographic functionality.

Audit:
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.

FAU_STG_EXT.1	**Extended: Protected Audit Trail Storage**		
	Hierarchical to	:	No other components
	Dependencies	:	FAU_GEN.1 Audit data generation, FTP_ITC.1 Inter-TSF trusted channel
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.		

Rationale:
The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2. FAU_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:
This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

Component leveling:

FCS_CKM_EXT.4: Extended: Cryptographic Key Material Destruction	4

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

Management:
The following actions could be considered for the management functions in FMT:
- There are no management actions foreseen.

Audit:
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.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

	Hierarchical to	: No other components
	Dependencies	: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction
FCS_CKM_EXT.4.1	The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.	

Rationale:
Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior:
This family addresses requirements for protecting communications using IPsec.

Component leveling:

FCS_IPSEC_EXT.1 Extended: IPsec selected	1

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:

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

- There are no management actions foreseen.

Audit:

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

- Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to : No other components

Dependencies : FIA_PSK_EXT.1 Extended:Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: *tunnel mode, transport mode*].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109,* [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; IKEv2 as defined in RFCs 5996, [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash*

functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; IKEv1 SA lifetimes can be established based on [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE*], *no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.

Rationale:

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4. FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family Behavior:

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management:

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

- There are no management actions foreseen.

Audit:

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.

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Hierarchical to : No other components.

Dependencies : No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

Rationale:

Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.5. FDP_FXS_EXT Extended: Fax Separation

Family Behavior:

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

Component leveling:

FDP_FXS_EXT.1 Extended: Fax Separation	1

FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

Management:

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

- There are no management actions foreseen.

Audit:

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.

FDP_FXS_EXT.1 Extended: Fax separation

Hierarchical to : No other components

Dependencies : No dependencies

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

Rationale:

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.

This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.6. FIA_PMG_EXT Extended: Password Management

Family Behavior:

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component leveling:

FIA_PMG_EXT.1 Extended: Password Management	1

FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management:

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

- There are no management actions foreseen.

Audit:

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.

FIA_PMG_EXT.1 Extended: Password Management

Hierarchical to : No other components

Dependencies : No dependencies

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

・Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: *other characters*]];

・Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

Rationale:
Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.7. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family Behavior:
This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

Management:
The following actions could be considered for the management functions in FMT:
- There are no management actions foreseen.

Audit:
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.

FIA_PSK_EXT.1	***Extended: Pre-Shared Key Composition***	
	Hierarchical to :	No other components
	Dependencies :	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FIA_PSK_EXT.1.1	The TSF shall be able to use pre-shared keys for IPsec.	
FIA_PSK_EXT.1.2	The TSF shall be able to accept text-based pre-shared keys that are: ・22 characters in length and [selection: [assignment: *other supported lengths*], *no other lengths*]; ・composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).	
FIA_PSK_EXT.1.3	The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].	

Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.8. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:
This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys.This is a new family modelled as the FPT Class.

Component leveling:

FPT_SKP_EXT.1 Extended: Protection of TSF Data	1

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject.It is the only component of this family.

Management:
The following actions could be considered for the management functions in FMT:
- There are no management actions foreseen.

Audit:
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.

FPT_SKP_EXT.1	**Extended: Protection of TSF Data**		
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.		

Rationale:
Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

This extended component protects the TOE by means of strong authentication using Preshared Key, and it is therefore placed in the FPT class with a single component.

5.9. FPT_TST_EXT Extended: TSF testing

Family Behavior:
This family addresses the requirements for self-testing the TSF for selected correct operation.

Component leveling:

FPT_TST_EXT.1 Extended: TSF testing	1

FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management:
The following actions could be considered for the management functions in FMT:
- There are no management actions foreseen.

Audit:
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.

FPT_TST_EXT.1	**Extended: TSF testing**	
	Hierarchical to :	No other components
	Dependencies :	No dependencies
FPT_TST_EXT.1.1	The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.	

Rationale:
TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing.In particular, there is no SFR defined for TSF testing.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.10. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:
This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

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

- There are no management actions foreseen.

Audit:
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.

FPT_TUD_EXT.1	**Extended: Trusted Update**		
	Hierarchical to	:	No other components
	Dependencies	:	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), FCS_COP.1(c) Cryptographic operation (Hash Algorithm).
FPT_TUD_EXT.1.1	The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.		
FPT_TUD_EXT.1.2	The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.		
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.		

Rationale:
Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software.In particular, there is no SFR defined for importing TSF Data.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6. Security Requirements

6.1. Security Functional Requirements

この章では、4.1 章で規定されたセキュリティ対策方針を実現するための、TOE のセキュリティ機能要件を記述する。なお、セキュリティ機能要件は、CC Part2 に規定のセキュリティ機能要件から、引用する。CC Part2 に規定されていないセキュリティ機能要件は、PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015、Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017)に規定の拡張セキュリティ機能要件から、引用する。

＜表記法＞
ボールド書体は、PP で完了または詳細化したことを示す。
*イタリック*書体は、ST で選択もしくは割り付けた部分を示す。
ボールドイタリック書体は、PP で完成または詳細化された SFR の部分に対し、ST において選択され、かつ／または完成されたことを示す。
[]内は、ST で選択もしくは割り付けた値を示す。
括弧内に文字、例えば、(a)、(b)、・・・、が続くような SFR コンポーネントは、繰返しを示す。
拡張コンポーネントは、SFR 識別に「_EXT」を追加して識別される。

6.1.1. Mandatory Requirements

6.1.1.1. Class FAU: Security Audit

FAU_GEN.1	**Audit data generation** (for O.AUDIT) 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: a) Start-up and shutdown of the audit functions; b) All auditable events for the **not specified** level of audit; and c) **All auditable events specified in Table 6-1,**[*なし*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 6-1,** [*なし*].

Table 6-1 Auditable Events

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None

Auditable event	Relevant SFR	Additional information
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

FAU_GEN.2 User identity association

(for O.AUDIT)

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_STG_EXT.1 Extended: External Audit Trail Storage

(for O.AUDIT)

Hierarchical to : No other components.
Dependencies : FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

6.1.1.2. Class FCS: Cryptographic Support

FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

(for O.COMMS_PROTECTION)

Hierarchical to : No other components.

Dependencies : [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) ~~]~~
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) **Refinement**: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [**

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;***

・ ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

FCS_CKM.1(b) **Cryptographic Key Generation (Symmetric Keys)**

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to : No other components.

Dependencies : [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption) ~~]~~
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b) **Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: No Standard.**

FCS_CKM_EXT.4 **Extended: Cryptographic Key Material Destruction**

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to : No other components.

Dependencies : [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

FCS_CKM.4 **Cryptographic key destruction**

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to : No other components.

Dependencies : [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],

FCS_CKM.4.1 **Refinement:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***For volatile memory, the destruction shall be executed by*** [***powering off a device***]. ***For nonvolatile storage, the destruction shall be executed by a*** [***single***] ***overwrite of key data storage location consisting of*** [***a static pattern***], ***followed by a*** [***none***]. ***If read-verification of the overwritten data fails, the process shall be repeated again;***] that meets the following: [***no standard***].

FCS_COP.1(a) **Cryptographic Operation (Symmetric encryption/decryption)**

(for O.COMMS_PROTECTION)

Hierarchical to : No other components.

Dependencies : [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(a) **Refinement**: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [*CBC mode*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:
・FIPS PUB 197, "Advanced Encryption Standard (AES)"
・[*NIST SP 800-38A*]

FCS_COP.1(b) **Cryptographic Operation (for signature generation/verification)**

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to : No other components.

Dependencies : [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a [***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits, 3072 bits]*** that meets the following **[*FIPS PUB 186-4, "Digital Signature Standard"*]**.

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)

Hierarchical to : No other components.
Dependencies : No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [*NIST SP 800-90A*] using [*CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] *software-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.1.1.3. Class FDP: User Data Protection

FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : No other components.
Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 6-2 and Table 6-3**.

FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : No other components.
Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 6-2 and Table 6-3**.

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 6-2 and Table 6-3***.

FDP_ACF.1.3 **Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*なし*].

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*機能制限に基いて、対象機能への利用者のアクセスを拒否*].

Table 6-2 D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation :*	*Submit a document to be printed*	*View image or Release printed output*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	*Operation :*	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)	denied		
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	*Operation :*	*Submit a document for copying*	*View scanned image or Release printed copy output*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	*Operation :*	*Submit a document to send as a fax*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)	denied		
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	*Operation:*	*Receive a fax and store it*	*View fax image or Release printed fax output*	*Modify image of received fax*	*Delete image of received fax*
	Fax owner	(note 3)			
	U.ADMIN	(note 4)	denied	denied	
	U.NORMAL	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied
Storage/ retrieval	*Operation :*	*Store document*	*Retrieve stored document*	*Modify stored document*	*Delete stored document*
	Job owner	(note 5)			
	U.ADMIN	denied	denied	denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Table 6-3 D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation :*	*Create print job*	*View print queue / log*	*Modify print job*	*Cancel print job*
	Job owner	(note 1)		denied	
	U.ADMIN	denied		denied	

	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Scan	***Operation :***	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Copy	***Operation :***	***Create copy job***	***View copy status / log***	***Modify copy job***	***Cancel copy job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Fax send	***Operation:***	***Create fax send job***	***View fax job queue / log***	***Modify fax send job***	***Cancel fax send job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Fax receive	***Operation:***	***Create fax receive job***	***View fax receive status / log***	***Modify fax receive job***	***Cancel fax receive job***
	Fax owner	(note 3)		denied	
	U.ADMIN	(note 4)		denied	
	U.NORMAL	(note 4)		denied	denied
	Unauthenticated	(note 4)		denied	denied
Storage / retrieval	***Operation :***	***Create storage / retrieval job***	***View storage / retrieval log***	***Modify storage / retrieval job***	***Cancel storage / retrieval job***
	Job owner	(note 6)		denied	
	U.ADMIN	denied		denied	
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied

・Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.
・Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.
・Note 3: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.
・Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.
・Note 5: Fax receive により create された文書の Job owner は Note 3、クライアント PC から送信された文書の Job owner は Note 1、スキャナを用いて生成された文書の Job owner は Note 2、パスワード

暗号化 PDF ボックスからの保存により create された文書の Job owner は Note1 とする。

・Note 6: Create storage job において、Fax receive により create されたジョブの Job owner は Note 3、クライアント PC から送信されたジョブの Job owner は Note 1、スキャナを用いて生成されたジョブの Job owner は Note 2、パスワード暗号化 PDF ボックスからの保存により create されたジョブの Job owner は Note1 とする。Create retrieval job の Job owner は Note 2 とする。

6.1.1.4. Class FIA: Identification and Authentication

FIA_AFL.1 **Authentication failure handling**

(for O.USER_I&A)

Hierarchical to : No other components.

Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* [*1～3*]] unsuccessful authentication attempts occur related to [*ログインパスワードによる認証, 強制メモリ受信ボックスパスワードによる認証*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met, surpassed*], the TSF shall [*解除操作が実施されるまで該当利用者のログインパスワードによる認証を停止, 解除操作が実施されるまで強制メモリ受信ボックスパスワードによる認証を停止*].

FIA_ATD.1 **User attribute definition**

(for O.USER_AUTHORIZATION)

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: [*User ID, 管理者権限, 機能制限, 強制メモリ受信ボックスへのアクセス権*].

FIA_PMG_EXT.1 **Extended: Password Management**

(for O.USER_I&A)

Hierarchical to : No other components.

Dependencies : No dependencies

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!", "@", "#", "$", "%", "^", "&", "*", "(", ")",* ["-", "¥", "[", "]", ":", ";", ",", ".", "/", "'", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?", "_", " ", *(強制メモリ受信ボックスパスワードの場合)""""*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_UAU.1 **Timing of authentication**

(for O.USER_I&A)

Hierarchical to : No other components.
Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 **Refinement:** The TSF shall allow [*ファクス受信、TOEの状態確認および表示等の設定*] on behalf of the user to be performed before the user is authenticated.

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**

(for O.USER_I&A)

Hierarchical to : No other components.
Dependencies : FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*入力された文字データ 1 文字毎に"＊"または"●"の表示*] to the user while the authentication is in progress.

FIA_UID.1 **Timing of identification**

(for O.USER_I&A and O.ADMIN_ROLES)

Hierarchical to : No other components.
Dependencies : No dependencies

FIA_UID.1.1 **Refinement:** The TSF shall allow [*ファクス受信、TOEの状態確認および表示等の設定*] on behalf of the user to be performed before the user is identified.

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**

(for O.USER_I&A)

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: [*User ID, 管理者権限, 機能制限, 強制メモリ受信ボックスへのアクセス権*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*User IDに一時利用停止が設定されている場合、該当利用者に関連付けたセキュリティ属性を破棄する,管理者権限が付与されていない利用者が管理者権限ありでログインを実行した場合、該当利用者に関連付けたセキュリティ属性を破棄する*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*強制メモリ受信ボッ*

クスパスワードの認証に成功した場合、該当利用者の強制メモリ受信ボックスへのアクセス権を有効にする，強制メモリ受信ボックスパスワードの認証に失敗した場合、該当利用者の強制メモリ受信ボックスへのアクセス権を無効にする].

6.1.1.5. Class FMT: Security Management

FMT_MOF.1 **Management of security functions behavior**

(for O.ADMIN_ROLES)

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 **Refinement:** The TSF shall restrict the ability to [*disable, enable, modify the behavior of*] the functions [*refer to Table 6-4*] to **U.ADMIN**.

Table 6-4 Management of Security Functions behavior

Security Functions	Operations
セキュリティ強化設定	disable, enable
ユーザー認証方式	modify the behavior
監査機能	modify the behavior
高信頼通信機能	modify the behavior
強制メモリ受信	modify the behavior

FMT_MSA.1 **Management of security attributes**

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

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 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [*modify, delete,* [*create, 一時利用停止／一時利用停止の解除, 付与, 設定*]] the security attributes [*Table 6-5のSecurity Attributes*] to [*Table 6-5のAuthorised Identified Roles*].

Table 6-5 Management of Subject Security Attribute

Security Attributes	Authorized Identified Roles	Operations
User ID	U.ADMIN	Create Delete 一時利用停止／一時利用停止の解除
	U.ADMIN U.NORMAL	個人ボックスの所有者の設定

Security Attributes	Authorized Identified Roles	Operations
	U.ADMIN 当該ボックスの owner である U.NORMAL	個人ボックスの所有者の変更
管理者権限	U.ADMIN	Delete 付与
機能制限	U.ADMIN	Delete 設定

FMT_MSA.3 **Static attribute initialization**

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical t : No other components.
Dependencies : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 **Refinement:** The TSF shall allow the **[*no role*]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 **Management of TSF data**

(for O.ACCESS CONTROL)

Hierarchical to : No other components.
Dependencies : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 **Refinement:** The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6-6.**

Table 6-6 Management of TSF Data

Data	Operation	Authorised role(s)
[assignment: *list of TSF Data* ***owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear,* [assignment: *other operations*]]	**U.ADMIN, the owning U.NORMAL.**
ユーザーパスワード	[assignment: *other operations*] *登録*	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
強制メモリ受信ボックスパスワード	[assignment: *other operations*] *登録*	**U.ADMIN**
	modify	

Data	Operation	Authorised role(s)
[assignment: *list of TSF Data* ***not owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	**U.ADMIN**
管理者パスワード	*modify*	**U.ADMIN**
日時情報	*modify*	
システムオートリセット時間	*modify*	
自動ログアウト時間	*modify*	
認証失敗回数閾値	*modify*	
認証失敗回数（U.BUILTIN_ADMIN 以外）	*clear*	
パスワード規約	*modify*	
外部認証サーバー設定	*modify* [assignment: *other operations*] *登録*	
管理者認証の操作禁止解除時間	*modify*	
ネットワーク設定	*modify* [assignment: *other operations*] *登録*	
[assignment: ***list of software, firmware, and related configuration data***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	**U.ADMIN**
TOE のソフトウェア/ファームウェア更新に関するデータ（更新対象のソフトウェア/ファームウェア、更新に関係するコンフィグデータ	*modify*	**U.ADMIN**

FMT_SMF.1 **Specification of Management Functions**

(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

Hierarchical to : No other components.

Dependencies: : No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*refer to Table 6-7*].

Table 6-7 list of management functions

management functions
U.ADMIN によるセキュリティ強化設定機能
U.ADMIN によるユーザー管理機能
U.ADMIN によるユーザー認証設定機能
U.ADMIN による外部認証サーバー設定機能
U.ADMIN による高信頼通信管理機能
U.ADMIN によるネットワーク設定の登録・変更機能

management functions
U.ADMIN による日時情報の変更機能
U.ADMIN による監査ログ管理機能
U.ADMIN によるシステムオートリセット時間の変更機能
U.ADMIN による自動ログアウト時間の変更機能
U.ADMIN による管理者認証の操作禁止解除時間の変更機能
U.ADMIN によるパスワード規約変更機能
U.ADMIN による認証失敗回数閾値の変更機能
U.ADMIN による認証失敗回数（U.BUILTIN_ADMIN 以外）のクリア機能
U.ADMIN によるボックス管理機能
U.ADMIN による強制メモリ受信設定機能
U.BUILTIN_ADMIN による管理者パスワード設定機能
U.NORMAL によるボックス管理機能
U.NORMAL による自身のユーザーパスワード設定機能

FMT_SMR.1 **Security roles**

(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)

Hierarchical to : No other components.

Dependencies : FIA_UID.1 Timing of identification

FMT_SMR.1.1 **Refinement:** The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.1.6. Class FPT: Protection of the TSF

FPT_SKP_EXT.1 **Extended: Protection of TSF Data**

(for O.COMMS_PROTECTION)

Hierarchical to : No other components.

Dependencies : No dependencies

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_STM.1 **Reliable time stamps**

(for O.AUDIT)

Hierarchical to : No other components.

Dependencies : No dependencies

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

FPT_TST_EXT.1 **Extended: TSF testing**

(for O.TSF_SELF_TEST)

Hierarchical to : No other components.
Dependencies : No dependencies

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

FPT_TUD_EXT.1 Extended: Trusted Update

(for O.UPDATE_VERIFICATION)

Hierarchical to : No other components.
Dependencies : FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [*no other functions*] prior to installing those updates.

6.1.1.7. Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)

Hierarchical to : No other components.
Dependencies : No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*操作パネルの場合、システムオートリセット時間によって決定される時間, WC の場合、自動ログアウト時間によって決定される時間, プリンタドライバーの場合、対話セッションはない*].

6.1.1.8. Class FTP: Trusted Path/Cannels

FTP_ITC.1 **Inter-TSF trusted channel**

(for O.COMMS_PROTECTION, O.AUDIT)

Hierarchical to : No other components.
Dependencies : [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1 **Refinement:** The TSF shall **use [*IPsec*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [*authentication server, [SMTPサーバー, DNSサーバー, ログサーバー, WebDAVサーバー, SMBサーバー]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 **Refinement:** The TSF shall permit **the TSF**, **or the authorized IT entities**, to initiate communication via the trusted channel

FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [***authentication service, mail service, DNS service, log transmission service, WebDAV service, SMB service***].

FTP_TRP.1(a) **Trusted path (for Administrators)**

(for O.COMMS_PROTECTION)

Hierarchical to : No other components.
Dependencies : [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) **Refinement**: The TSF shall **use** [***IPsec***] **to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(a) **Refinement**: The TSF shall permit **remote administrators** to initiate communication via the trusted path

FTP_TRP.1.3(a) **Refinement:** The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

FTP_TRP.1(b) **Trusted path (for Non-administrators)**

(for O.COMMS_PROTECTION)

Hierarchical to : No other components.
Dependencies : [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b)	**Refinement** : The TSF shall **use** [***IPsec***] **to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
FTP_TRP.1.2(b)	**Refinement**: The TSF shall permit [***remote users***] to initiate communication via the trusted path
FTP_TRP.1.3(b)	**Refinement**: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

6.1.2. Conditionally Mandatory Requirements

6.1.2.1. PSTN Fax-Network Separation

FDP_FXS_EXT.1 **Extended: Fax separation**

(for O.FAX_NET_SEPARATION)

Hierarchical to : No other components.
Dependencies : No dependencies

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

6.1.3. Selection-based Requirements

6.1.3.1. Protected Communications

FCS_IPSEC_EXT.1 **Extended: IPsec selected**

(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to : No other components.
Dependencies : FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_IPSEC_EXT.1. The TSF shall implement the IPsec architecture as specified in RFC 4301.

1 FCS_IPSEC_EXT.1.2	The TSF shall implement [*transport mode*].
FCS_IPSEC_EXT.1.3	The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.
FCS_IPSEC_EXT.1.4	The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [*the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC*].
FCS_IPSEC_EXT.1.5	The TSF shall implement the protocol: [*IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [*RFC 4304 for extended sequence numbers*], *and* [*RFC 4868 for hash functions*]].
FCS_IPSEC_EXT.1.6	The TSF shall ensure the encrypted payload in the [*IKEv1*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [*no other algorithm*].
FCS_IPSEC_EXT.1.7	The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.
FCS_IPSEC_EXT.1.8	The TSF shall ensure that [*IKEv1 SA lifetimes can be established based on* [*length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].
FCS_IPSEC_EXT.1.9	The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [*no other DH groups*].
FCS_IPSEC_EXT.1.10	The TSF shall ensure that all IKE protocols perform Peer Authentication using the [*RSA*] algorithm and Pre-shared Keys.

FCS_COP.1(g) **Cryptographic Operation (for keyed-hash message authentication)**

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to : No other components.

Dependencies : [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or~~ FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) **Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-**[***SHA-1, SHA-256, SHA-384, SHA-512***]**, key size** [***160, 256, 384, 512 bits***], **and message digest sizes** [***160, 256, 384, 512***] **bits** that meet the following:
"**FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

FIA_PSK_EXT.1 **Extended: Pre-Shared Key Composition**

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to : No other components.

	Dependencies :	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FIA_PSK_EXT.1.1	The TSF shall be able to use pre-shared keys for IPsec.	
FIA_PSK_EXT.1.2	The TSF shall be able to accept text-based pre-shared keys that are: 22 characters in length and [*no other lengths*]; composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").	
FIA_PSK_EXT.1.3	The TSF shall condition the text-based pre-shared keys by using [*SHA-1, SHA-256, SHA-512*, [*SHA-384*]] and be able to [*use no other pre-shared keys*].	

6.1.3.2. Trusted Update

FCS_COP.1(c)	**Cryptographic operation (Hash Algorithm)** (selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)	
	Hierarchical to :	No other components.
	Dependencies :	No dependencies.
FCS_COP.1.1(c)	**Refinement**: The TSF shall perform **cryptographic hashing services** in accordance with [***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].	

6.2. Security Assurance Requirements

The TOE security assurance requirements specified in Table 6-8 provides evaluative activities required to address the threats identified in 3.3 of this ST.

Table 6-8 TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.3. Security Requirements Rationale

6.3.1. The dependencies of security requirements

TOE セキュリティ機能要件間の依存関係を下表に示す。

Table 6-9 The dependencies of security requirements

機能要件	依存関係	STで満たす依存関係	依存関係を満たしていない要件
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	N/A
	FIA_UID.1	FIA_UID.1	N/A
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1	N/A
	FTP_ITC.1	FTP_ITC.1	N/A
FCS_CKM.1(a)	FCS_COP.1(b) FCS_COP.1(i)	FCS_COP.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_CKM.1(b)	FCS_COP.1(a) FCS_COP.1(d) FCS_COP.1(e) FCS_COP.1(f) FCS_COP.1(g) FCS_COP.1(h)	FCS_COP.1(a) FCS_COP.1(g)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A
FCS_CKM.4	FCS_CKM.1(a) or FCS_CKM.1(b)	FCS_CKM.1(a) FCS_CKM.1(b)	N/A
FCS_CKM_EXT.4	FCS_CKM.1(a) or FCS_CKM.1(b)	FCS_CKM.1(a) FCS_CKM.1(b)	N/A
	FCS_CKM.4	FCS_CKM.4	N/A
FCS_COP.1(a)	FCS_CKM.1(b)	FCS_CKM.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_COP.1(b)	FCS_CKM.1(a)	FCS_CKM.1(a)	IPsec通信（FCS_IPSEC_EXT.1）の場合。アップデート機能（FPT_TUD_EXT.1）の場合は、FCS_CKM.1(a)、FCS_CKM_EXT.4は満たさないが、鍵生成はおこなわないため問題ない。
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	
FCS_COP.1(c)	No dependencies	No dependencies	N/A
FCS_COP.1(g)	FCS_CKM.1(b)	FCS_CKM.1(b)	N/A
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	N/A
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1	FIA_PSK_EXT.1	N/A

機能要件	依存関係	STで満たす依存関係	依存関係を満たしていない要件
	FCS_CKM.1(a)	FCS_CKM.1(a)	N/A
	FCS_COP.1(a)	FCS_COP.1(a)	N/A
	FCS_COP.1(b)	FCS_COP.1(b)	N/A
	FCS_COP.1(c)	FCS_COP.1(c)	N/A
	FCS_COP.1(g)	FCS_COP.1(g)	N/A
	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A
FCS_RBG_EXT.1	No dependencies	No dependencies	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	N/A
	FMT_MSA.3	FMT_MSA.3	N/A
FDP_FXS_EXT.1	No dependencies	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A
FIA_ATD.1	No dependencies	No dependencies	N/A
FIA_PMG_EXT.1	No dependencies	No dependencies	N/A
FIA_PSK_EXT.1	FCS_RBG_EXT.1	—	乱数ビット生成器を用いたビットベースの事前共有鍵生成を選択していないため。
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A
FIA_UID.1	No dependencies	No dependencies	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_MSA.1	FDP_ACC.1	FDP_ACC.1	N/A
	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	N/A
	FMT_SMR.1	FMT_SMR.1	N/A
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	N/A
	FMT_SMF.1	FMT_SMF.1	N/A
FMT_SMF.1	No dependencies	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A
FPT_SKP_EXT.1	No dependencies	No dependencies	N/A
FPT_STM.1	No dependencies	No dependencies	N/A
FPT_TST_EXT.1	No dependencies	No dependencies	N/A
FPT_TUD_EXT.1	FCS_COP.1(b)	FCS_COP.1(b)	N/A
	FCS_COP.1(c)	FCS_COP.1(c)	N/A
FTA_SSL.3	No dependencies	No dependencies	N/A
FTP_ITC.1	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or	FCS_IPSEC_EXT.1	N/A

機能要件	依存関係	STで満たす依存関係	依存関係を満たしていない要件
	FCS_HTTPS_EXT.1		
FTP_TRP.1(a)	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(b)	FCS_IPSEC_EXT.1 or FCS_TLS_EXT.1 or FCS_SSH_EXT.1 or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A

7. TOE Summary specification

TOE が提供するセキュリティ機能の要約仕様を示す。

Table 7-1 セキュリティ機能一覧

No.	セキュリティ機能名称
1	識別認証機能
2	アクセス制御機能
4	暗号化機能
5	高信頼通信機能
6	セキュリティ管理機能
7	監査機能
8	高信頼な運用機能
9	FAX 分離機能

7.1. 識別認証機能

TOE は、利用者からクレデンシャルを取得して識別認証を行い、検証の結果、許可利用者と判断された者だけに TOE の利用を許可する識別認証機能を提供する。

FIA_UAU.1、FIA_UID.1

TOE は、Table7-2 に示す3つの認証方式をサポートし、管理者がユーザー認証設定機能で設定できる。

操作パネルもしくは WC から TOE を利用する場合、ユーザー名、ユーザーパスワード、管理者権限を入力する。ビルトイン管理者として操作パネルもしくは WC から TOE を利用する場合、ビルトイン管理者用のログイン画面から管理者パスワードを入力する。プリンタドライバーから TOE を利用する場合、ユーザー名、ユーザーパスワードを入力する。

TOE は、入力されたクレデンシャルを元に識別認証を実施し、成功した場合のみ TOE の利用を許可する。外部サーバー認証方式が設定されている場合、利用者はユーザー名とユーザーパスワードに加えて、外部認証サーバ ID を入力する。TOE は、ユーザー名を指定された外部認証サーバーに送り、返答された信任状に対して、ユーザーパスワードから生成したユーザー鍵による復号をおこなって復号が成功した場合に認証成功、復号が失敗した場合に認証失敗と判断する。ビルトイン管理者の識別認証は、認証方式の設定に関わらず、常に本体装置認証方式で実施される。

TOE は、強制メモリ受信設定機能において、管理者が強制メモリ受信ボックスにパスワードを設定する機能を提供し、運用中は強制メモリ受信ボックスパスワードが設定されている。操作パネルもしくは WC から識別認証に成功した一般利用者が、強制メモリ受信ボックスへアクセスすると、強制メモリ受信ボックスパスワードによる認証が要求され、認証に成功した場合のみアクセスが許可される。よって、強制メモリ受信ボックスパスワードを知らない一般利用者は、強制メモリ受信ボックスに保存されたファクス文書を操作することができない。強制メモリ受信ボックスパスワードの認証は、認証方式の設定に関わらず、常に本体装置認証方式で実施される。

識別認証は上記インタフェース毎に実施するため、管理者が WC からリモート管理機能実施中に、一般利用者がパネルから識別認証を実施し、成功した場合、TOE を操作することができる。ただし、管理者がログイン中は、他の管理者の識別認証が禁止されるため、2 人以上の管理者が同時に TOE を利用するとはできない。

プリンタドライバーから TOE を利用する場合、対話セッションはなく、TOE が電子文書を受信した時、電子文書に含まれるクレデンシャル（ユーザー名、ユーザーパスワード）により識別認証を実施する。成功した場合、利用者の役割として一般利用者(U.NORMAL)を割り当て、該当一般利用者が所有者する電子文書として TOE に保存する。失

敗した場合、受信した電子文書をTOEに保存せずに破棄する。プリンタドライバーは、管理者がTOEを利用する手段を提供しない。

識別認証を実行する前に可能な操作は、下記の通り。

・ファクス受信。

・TOEの状態確認および表示等の設定として下記操作が可能。

- 操作パネルからの装置情報表示(ファームウェアのバージョン表示など)
- 操作パネルからのジョブ表示
- 操作パネルからの拡大表示設定
- WCの表示言語の切り替え

Table 7-2 ユーザー認証設定機能

認証方式	識別認証
本体装置認証	TOEが識別認証を行う。ユーザー名とユーザーパスワード、管理者パスワード、強制メモリ受信ボックスパスワードが、TOEに登録されている情報と一致することを確認する。
外部サーバー認証	TOEが外部認証サーバー(Active Directory)を利用して識別認証を行う。TOEは、ユーザー名をKerberos version 5プロトコルを利用して利用者が指定した外部認証サーバーへ送信し、返答された信任状に対してユーザーパスワードから生成したユーザー鍵による復号を行い、識別認証を実施する。
本体装置＋外部サーバー認証	本体装置認証、外部サーバー認証のいずれかで識別認証を行う。利用者がログイン実行時に認証方式を選択する。

FIA_ATD.1

TOEは、ユーザー管理機能で登録された一般利用者毎に、利用者属性としてUser ID、管理者権限、機能制限のアクセス権を定義する。また、利用者属性として、強制メモリ受信ボックスへのアクセス権も定義する。強制メモリ受信ボックスへのアクセス権は、強制メモリ受信設定機能による強制メモリ受信ボックスパスワードの設定によって実現される。また、ビルトイン管理者の利用者属性として、User IDを定義する。

FIA_USB.1

一般利用者、ユーザー管理者が識別認証に成功した場合、TOEは利用者属性(User ID、管理者権限、機能制限、強制メモリ受信ボックスへのアクセス権)を関連付ける。ビルトイン管理者が識別認証に成功した場合、TOEは利用者属性(User ID)を関連付ける。

この時、User IDに一時利用停止が設定されている場合、TOEは該当利用者に関連付けた利用者属性を破棄する。また、ユーザー管理者としてログインを実行した利用者に管理者権限が付与されていない場合、該当利用者に関連付けた利用者属性を破棄する。

一般利用者が識別認証に成功した後、強制メモリ受信ボックスへアクセスする際、強制メモリ受信ボックスパスワードによる認証が要求され、認証に成功した場合、TOEは該当利用者の利用者属性である強制メモリ受信ボックスへのアクセス権を有効にする。認証に失敗した場合、TOEは該当利用者の利用者属性である強制メモリ受信ボックスへのアクセス権を無効にする。

FIA_AFL.1

TOEは、利用者の識別認証において、管理者があらかじめ設定したチェック回数(1～3 回)以上の連続失敗を検知した時、該当利用者の認証を停止する認証操作禁止機能を提供する。利用者に管理者権限が付与されている場合、一般利用者としての認証失敗回数とユーザー管理者としての認証失敗回数は積算される。

ビルトイン管理者の認証が停止された場合、TOEの電源をOFF/ONし、起動から操作禁止解除時間設定に設定されている時間を経過後に認証停止を解除する。一般利用者もしくはユーザー管理者の認証が停止された場合、認

証停止状態でない管理者が認証失敗回数の消去機能を実行することで認証停止を解除する。

TOE は、外部サーバー認証方式による識別認証でも同様に、上記の認証失敗時の動作を実施する。

強制メモリ受信ボックスパスワードの識別認証において、管理者があらかじめ設定したチェック回数(1～3 回)以上の連続失敗を検知した時、強制メモリ受信ボックスパスワードの認証を停止する。強制メモリ受信ボックスパスワードの認証が停止された場合、認証停止状態でない管理者が認証失敗回数の消去機能を実行することで認証停止を解除する。

FIA_UAU.7

TOE は、対話セッションの認証処理（操作パネルもしくは WC からのログイン）においてログインパスワード、強制メモリ受信ボックスパスワードを入力する際、入力された文字データ 1 文字毎に“＊”または”●”を表示する。

FIA_PMG_EXT.1

TOE で利用者パスワードとして使用可能な文字は、アルファベットの大文字と小文字、数字、記号（“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “-”, “¥”, “[”, “]”, “:”, “;”, “,”, “.”, “/“, “\”, “=”, “~”, “|”, “`”, “{”, “}”, “+”, “<”, “>“, “?” ,“_”およびスペース）、特殊文字(97 文字)である。強制メモリ受信ボックスパスワードの場合、上記に加え“””(ダブルクォーテーション)も利用できる。管理者は、最小パスワード長を 8～64 文字の範囲で設定することができる。よって、最小パスワード長として 15 文字以上の長さを設定できる。

FTA_SSL.3

TOE は、操作パネル、WC で識別認証された利用者が以下の条件を満たした場合、そのセッションを終了する。プリンタドライバーの場合、対話セッションはなく、プリンタドライバーから要求された処理が受け付けられた際にログインし、その処理の完了直後にログアウトを行う。

- 操作パネルの場合、利用者は最終操作による処理が完了してから、システムオートリセット時間(1～9 分の間で設定可能)が経過した場合、ログアウトされる。
- WC の場合、利用者は最終操作による処理が完了してから、自動ログアウト時間(1～60 分の間で設定可能)が経過した場合、ログアウトされる。

7.2. アクセス制御機能

FDP_ACC.1、FDP_ACF.1

TOE は、Table 6-2、Table 6-3 の利用者データアクセス制御に基づき、Table 7-3～Table 7-14 に記載の通り、利用者文書データと利用者ジョブデータへの操作を制限する。許可されない操作については、インタフェースを非表示もしくは操作不可状態で表示、または、操作要求に対して権限がないため操作できない旨のメッセージを表示し操作を拒否する。

識別認証により許可された一般利用者(U.NORAML)が、Table 7-3～Table 7-14 の Create 操作を実行した時、ジョブ所有者(Job owner)となり、TOE は文書もしくはジョブの所有者情報として User ID を記録する。TOE は、管理者(U.ADMIN)が Create 操作を実行するインタフェースを提供しない。ファクス受信機能(Fax receive)は、TOE の操作なしに、外部ファクスからのファクス受信により Create 操作が実行されるため、ファクス受信完了までの文書もしくはジョブのジョブ所有者は、管理者に割り当てられる(*1)。F コードが指定されていないファクス受信の場合、ファクス文書は強制メモリ受信ボックスへ保存されるため、ファクス受信完了後のジョブ所有者は、強制メモリ受信ボックスパスワードを知る一般利用者となる(*2)。F コードが指定されているファクス受信の場合、ファクス文書は指定された個人ボックスへ保存されるため、ファクス受信後のジョブ所有者は、個人ボックスの所有者である一般利用者がジョブ所有者となる(*3)。パスワード暗号化 PDF ボックスからの保存（Storage/retrival）は、ダイレクトプリント実行時に、保存が設定さ

れた文書をパスワード暗号化 PDF ボックスから取り出し、操作者の個人ボックスへ保存することにより Create 操作が実行される。保存実行後の文書もしくはジョブのジョブ所有者は、個人ボックスの所有者である一般利用者となる。

TOE は、ユーザー管理機能において、管理者が一般利用者毎に利用可能な機能を制限する機能制限設定を備えている。TOE は、利用者属性の機能制限に基いて、制限対象機能のインタフェースを非表示もしくは操作不可状態で表示する。よって、機能制限が設定された一般利用者は、Table 7-3～Table 7-14 のうち制限対象機能を用いた操作を利用することはできない。

TOE は、強制メモリ受信設定機能において、管理者が一般利用者の強制メモリ受信ボックスへのアクセスを制限する強制メモリ受信設定を備えており、運用中は強制メモリ受信ボックスパスワードによってアクセスが制限されている。TOE は、利用者属性の強制メモリ受信ボックスへのアクセス権に基いて、有効な場合、該当利用者の強制メモリ受信ボックスへのアクセスを許可し、無効な場合、該当利用者の強制メモリ受信ボックスへのアクセスを拒否する。よって、強制メモリ受信ボックスパスワードを知らない一般利用者は、Table 7-3～Table 7-14 のうち強制メモリ受信ボックスへのアクセスが必要な操作を利用することはできない。

TOE は、ボックス管理機能において、管理者もしくは一般利用者が、個人ボックスの所有者(User ID)を設定する機能、管理者もしくは個人ボックスの所有者である一般利用者が、個人ボックスの所有者(User ID)を変更する機能を備えており、個人ボックスと個人ボックス内に保存された文書へのアクセスを制限する。TOE は、個人ボックスの所有者(User ID)に基いて、一般利用者が同じ User ID を持つ場合には、該当個人ボックスのインタフェースを提供して、該当個人ボックスへのアクセスを許可する。一方、一般利用者が異なる User ID を持つ場合には、TOE は該当個人ボックスのインタフェースを非表示にするため、Table 7-3～Table 7-14 で該当個人ボックスへのアクセスが必要な操作を利用することはできない。

<Table 7-3～Table 7-14 の補足>
TOE が提供するインタフェースは下記の通り。
PN：操作パネル、WC：Web Connection、PD：プリンタドライバー

表中の記載は下記の通り。
○：TOE がサポートするもの、-：TOE がサポートしないもの

注記は下記の通り。
*1：U.ADMIN
*2：強制メモリ受信ボックスパスワードを知る U.NORMAL
*3：F コードで指定された個人ボックスの所有者である U.NORMAL

Table 7-3 D.USER.DOC(Print)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	印刷を実行。
		-	○	-	ダイレクトプリントを実行。
		-	○	-	パスワード暗号化 PDF に対して、印刷を指定してダイレクトプリントを実行。
Read	Job owner	○	-	-	認証&プリントボックスから文書を選択して、文書プレビューを表示。

		○	-	-	認証&プリントボックスから文書を選択し、印刷を実行。（印刷完了により文書は削除される。）
		○	-	-	パスワード暗号化 PDF ボックスから文書を選択し、印刷を実行。（印刷にはパスワード入力が必要。印刷完了により文書は削除される。）
Modify	Job owner	○	-	-	認証&プリントボックスからの印刷において、印刷設定を実行。
Delete	Job owner	○	-	-	認証&プリントボックスから文書を削除。
		○	-	-	パスワード暗号化 PDF ボックスから文書を削除。
	Job owner U.ADMIN	○	○	-	ジョブ削除に伴う文書削除。

Table 7-4 D.USER.DOC(Scan)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	スキャナユニットに原稿をセットして、スキャン/ファクスメニュー画面から宛先（ファックス宛先を除く）を指定して、送信を実行。
Read	-	-	-	-	なし。
Modify	Job owner	○	-	-	Create 操作で応用設定を実行。
Delete	Job owner U.ADMIN	○	○	-	ジョブ削除に伴う文書削除。

Table 7-5 D.USER.DOC(Copy)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	スキャナユニットに原稿をセットして、コピーメニュー画面からコピーを実行。
Read	Job owner	○	-	-	Create 操作を実行。
Modify	Job owner	○	-	-	Create 操作で応用設定を実行。
Delete	Job owner U.ADMIN	○	○	-	ジョブ削除に伴う文書削除。

Table 7-6 D.USER.DOC(Fax send)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	スキャナユニットに原稿をセットして、スキャン/ファクスメニュー画面からファクス宛先を選択して送信を実行。
Read	-	-	-	-	なし。
Modify	Job owner	○	-	-	Create 操作で応用設定を実行。
Delete	Job owner U.ADMIN	○	○	-	ジョブ削除に伴う文書削除。

Table 7-7 D.USER.DOC(Fax receive)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner(*1)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定していないファクスを受信。
		-	-	-	TOE の操作なし。外部ファクスから F コードを指定したファクスを受信。
Read	Job owner	○	○	-	強制メモリ受信ボックスからファクス文書を選択し、文書プレビューを表示。
		○	○	-	個人ボックスからファクス文書を選択し、文書プレビューを表示。
		○	-	-	強制メモリ受信ボックスからファクス文書を選択し、印刷実行を実行。 （印刷完了によりファクス文書は削除される。）
		○	-	-	個人ボックスからファクス文書を選択し、印刷実行を実行。 （印刷完了によりファクス文書は削除される。）
Modify	Job owner	○	-	-	個人ボックスからファクス文書を印刷する際に、応用設定を実行。
		○	○	-	個人ボックスからファクス文書を選択し、編集。
Delete	Job owner U.ADMIN	○	○	-	強制メモリ受信ボックスからファクス文書を削除。
	Job owner	○	○	-	個人ボックスからファクス文書を削除。
	Job owner U.ADMIN	○	○	-	ファクス文書の印刷ジョブ削除に伴うファクス文書の削除。
		○	○	-	個人ボックスの削除に伴うファクス文書の削除。

Table 7-8 D.USER.DOC(Storage/retrieval)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	ボックス保存を実行。
		-	○	-	ボックス保存を指定してダイレクトプリントを実行。
		○	-	-	スキャナユニットに原稿をセットして、ボックスメニュー画面から個人ボックスを指定して、ボックス保存を実行。
		-	○	-	パスワード暗号化 PDF に対して、ボックス保存を指定してダイレクトプリントを実行。
		○			パスワード暗号化 PDF ボックスから文書を選択し、保存を実行。(選択された文書が操作者の個人ボックスに移動)
	Job owner(*2)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定していないファクス受信後、強制メモリ受信ボックスへファクス文書を保存。
	Job owner(*3)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定したファクス受信後、指定された個人ボックスへファクス文書を保存。
Read	Job owner	○	○	-	個人ボックスから文書を選択し、文書プレビューを表示。

					(ファクス文書を除く。ファクス文書の文書プレビューは、Table 7-7 の Read 操作により制御される。)
		○	-	-	個人ボックスから文書を選択し、印刷、送信、ファクスによる送信、移動、コピーのいずれかを実行。 （ファクス文書の印刷を除く。ファクス文書の印刷は、Table 7-7 の Read 操作により制御される。）
		-	○	-	個人ボックスから文書を選択し、送信、ダウンロード、移動、コピーのいずれかを実行。
		-	○	-	強制メモリ受信ボックスから文書を選択し、ダウンロードを実行。
		○	-	-	パスワード暗号化 PDF ボックスから文書を選択し、保存を実行。 （保存にはパスワード入力が必要。保存完了により文書は削除される。）
Modify	Job owner	○	○	-	個人ボックスから文書を選択し、編集。 (ファクス文書を除く。ファクス文書の編集は、Table 7-7 の Modify 操作により制御される。)
		○	○	-	Read 操作(送信、印刷)において、応用設定を実行。 (ファクス文書の印刷を除く。ファクス文書の印刷における応用設定は、Table 7-7 の Modify 操作により制御される。)
		○	-	-	強制メモリ受信ボックスからファクス文書を選択し、編集(名称変更)。
Delete	Job owner	○	○	-	個人ボックスから文書を削除。 （ファクス文書の削除を除く。ファクス文書の削除は、Table 7-7 の Delete 操作により制御される。）
		○	-	-	パスワード暗号化 PDF ボックスから文書を削除。
	Job owner U.ADMIN	○	○	-	個人ボックスの削除に伴う文書の削除。 （ファクス文書の削除を除く。ファクス文書の削除は、Table 7-7 の Delete 操作により制御される。）

Table 7-9 D.USER.JOB(Print)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	-	-	○	クライアント PC から文書を選択し、プリンタドライバーで印刷を実行後、操作パネルで認証&プリントボックスに一時保存された文書を選択し、印刷を実行。 （印刷完了により文書は削除される。）
		-	○	-	クライアント PC の WC から文書を選択し、ダイレクトプリントを実行後、操作パネルで認証&プリントボックスに一時保存された文書を選択し、印刷を実行。 （印刷完了により文書は削除される。）
		-	○	-	クライアント PC の WC からパスワード暗号化 PDF 文書を選択し、印刷を指定してダイレクトプリントを実行後、操作パネルでパスワード暗号化 PDF ボックスから一時保存された文書を選択し、印刷を実行。

					（印刷にはパスワード入力が必要。印刷完了により文書は削除される。）
Read	Job Owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。 （パスワード暗号化 PDF の受信中ジョブを除く。）
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
Delete	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。 （認証&プリントボックスからの印刷ジョブの場合、ジョブ削除により文書も削除される。）

Table 7-10 D.USER.JOB(Scan)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORAML	○	-	-	スキャナユニットに原稿をセットして、スキャン/ファクスメニュー画面から宛先（ファックス宛先を除く）を指定して、送信を実行。
Read	Job owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
Delete	Job owner	○	-	-	スキャナユニットにより原稿読み取り中に、原稿読み取り中画面で停止を実行もしくはストップキーを押下し、停止中ジョブの削除を実行。 （ジョブ削除により文書も削除される。）
	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。 （ジョブ削除により文書も削除される。）

Table 7-11 D.USER.JOB(Copy)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORAML	○	-	-	スキャナユニットに原稿をセットして、コピーメニュー画面からコピーを実行。
Read	Job owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
Delete	Job owner	○	-	-	スキャナユニットにより原稿読み取り中に、原稿読み取り中画面で停止を実行もしくはストップキーを押下し、停止中ジョブの削除を実行。 （ジョブ削除により文書も削除される。）
	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。 （ジョブ削除により文書も削除される。）

Table 7-12 D.USER.JOB(Fax send)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner U.NORMAL	○	-	-	スキャナユニットに原稿をセットして、スキャン/ファクスメニュー画面からファクス宛先を選択して送信を実行。
Read	Job owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
Delete	Job owner	○	-	-	スキャナユニットにより原稿読み取り中に、原稿読み取り中画面で停止を実行もしくはストップキーを押下し、停止中ジョブの削除を実行。 （ジョブ削除により文書も削除される。）
	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。 （ジョブ削除により文書も削除される。）

Table 7-13 D.USER.JOB(Fax receive)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner(*1)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定していないファクスを受信。
		-	-	-	TOE の操作なし。外部ファクスから F コードを指定したファクスを受信。
	Job owner(*2)	○	-	-	強制メモリ受信ボックスからファクス文書を選択し、印刷実行を実行。 （印刷完了によりファクス文書は削除される。）
	Job owner(*3)	○	-	-	個人ボックスからファクス文書を選択し、印刷実行を実行。 （印刷完了によりファクス文書は削除される。）
Read	Job owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。 （印刷ジョブの場合、ジョブ削除によりファクス文書も削除される。）

Table 7-14 D.USER.JOB(Storage/retrieval)のアクセス制御

操作	操作可能な利用者	インタフェース			操作方法
		PN	WC	PD	
Create	Job owner	-	-	○	ボックス保存を実行。
	U.NORAML	-	○	-	ボックス保存を指定してダイレクトプリントを実行。

		○	-	-	スキャナユニットに原稿をセットして、ボックスメニュー画面から個人ボックスを指定して、ボックス保存を実行。
		-	○	-	ボックス保存を指定してパスワード暗号化 PDF のダイレクトプリントを実行。
	Job owner(*2)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定していないファクス受信後、ファクス文書を強制メモリ受信ボックスへ保存。
	Job owner(*3)	-	-	-	TOE の操作なし。外部ファクスから F コードを指定したファクス受信後、ファクス文書を指定された個人ボックスへ保存。
	Job owner U.NORMAL	○	-	-	個人ボックスから文書を選択し、印刷、送信、ファクスによる送信、移動、コピーのいずれかを実行。 （ファクス文書の印刷を除く。ファクス文書の印刷は Table 7-13 の Create 操作により制御される。）
		-	○	-	個人ボックスから文書を選択し、送信、ダウンロード、移動、コピーのいずれかを実行。
	Job owner U.NORMAL	-	○	-	強制メモリ受信ボックスからファクス文書を選択し、ダウンロードを実行。
	Job owner U.NORMAL	○	-	-	パスワード暗号化 PDF ボックスから文書を選択し、保存を実行。 （保存にはパスワード入力が必要。保存完了により文書は削除される。）
Read	Job owner U.ADMIN U.NORMAL	○	○	-	ジョブ表示を表示。 （パスワード暗号化 PDF の受信中ジョブを除く）。
	Unauthenticated	○	-	-	
Modify	-	-	-	-	なし。
Delete	Job owner	○	-	-	スキャナユニットにより原稿読み取り中に、原稿読み取り中画面で停止を実行もしくはストップキーを押下し、停止中ジョブの削除を実行。 （ジョブ削除により文書も削除される。）
		○	-	-	個人ボックスからの印刷を実行した後、ストップキーを押下し、停止中ジョブの削除を実行。 （ジョブ削除後も文書は削除されない。）
	Job owner U.ADMIN	○	○	-	ジョブ表示からジョブを削除。

7.3. 暗号化機能

FCS_CKM.1(a)

TOE は、IPsec 通信の鍵確立で用いる IPsec 証明書の生成において、NIST SP800-56B, Revision 1 の 6.3.1.3 節に記載の rsakpg1-crt 方式に記載の方法で、鍵長 2048bit の RSA 非対称鍵を生成する。また、IPsec 通信の鍵確立において、NIST SP800-56A, Revision 3 の 5.6.1.1.1 節に記載の Using the Approved Safe-Prime Groups に記載の方法で、Diffie-Hellman グループ 14 による非対称鍵を生成する。

FCS_CKM.1(b)

TOE は、IPsec 通信の通信開始時、もしくは SA ライフタイム経過後の鍵確立において、FCS_RBG_EXT.1 に記載の RBG で乱数を生成し、128bit もしくは 256bit の対称暗号鍵を生成する。TOE は、DRBG 関数(CTR DRBG(AES-256))を呼び出すことで上記 RBG を起動し、乱数を生成する。

FCS_RBG_EXT.1

TOE は、NIST SP 800-90A に準拠する CTR DRBG(AES-256)と、1 つのソフトウェアエントロピー源から構成される RBG を実装する。上記 CTR DRBG は、Derivation Function と Reseed を利用するが、Prediction Resistance 機能は動作しない。ソフトウェアエントロピー源は、CPU の内部状態に影響を与える条件分岐コード等の実装とクロックカウンター値取得処理をループ処理内に実装しており、ループ処理実行時間のばらつきをクロックカウンター経由で取得し、raw データを得る。シフト演算と XOR を用いて raw データに含まれるエントロピーをビット全体に撹拌、圧縮するコンディショニングを実施し、ビット全体のエントロピー率を上げた後、エントロピー値として出力する。

TOE は、この RBG を利用して乱数を生成し、高信頼通信機能の暗号鍵(鍵長 256bit と 128bit)生成に利用する。TOE が乱数生成する際、CTR DRBG でシードマテリアル(Entropy Input と Nonce)が必要になった場合、エントロピー源として利用するソフトウェアを起動し、必要サイズのエントロピー値を取得して利用する。このエントロピー値は、NIST SP800-90A の 10.2.1 に示される Instantiate と Reseed に必要な最小エントロピー量(TOE の場合、セキュリティ強度と同じ 256bit)を満たしており、十分なエントロピーが含まれている。

FIA_PSK_EXT.1

TOE は、IPsec 用の事前共有鍵として、下記テキストベースの事前共有鍵が利用できる。テキストベースの事前共有鍵は、下記ハッシュアルゴリズムを用いてビット列へ変換される。

・テキストベースの事前共有鍵
- 長さ：22 文字
- 利用可能文字：ASCII 文字列、または HEX 値
- 条件付けの方法：SHA-1、SHA-256、SHA-384、SHA-512

FCS_COP.1(a)

TOE は、IPsec 通信の ESP 暗号化アルゴリズムとして、FIPS PUB 197 と NIST SP 800-38A に適合した鍵長 128bit と 256bit の AES-CBC を利用する。また、TOE は、IPsec 通信の IKEv1 暗号化アルゴリズムとして、FIPS PUB 197 と NIST SP 800-38A に適合した鍵長 128bit と 256bit の AES-CBC を利用する。

FCS_COP.1(b)

TOE は、アップデート機能のファームウェア検証において、FIPS PUB 186-4 に適合した鍵長 2048bit の RSA デジタル署名アルゴリズムを利用する。また、IPsec 通信のピア認証において、FIPS PUB 186-4 に適合した鍵長 2048bit の RSA デジタル署名アルゴリズム（署名生成）を、デジタル署名検証において、FIPS PUB 186-4 に適合した鍵長 2048bit と 3048bit の RSA デジタル署名アルゴリズム（署名検証）を利用する。

FCS_COP.1(c)

TOE は、7.7.1 章に記載のアップデート機能において、以下のようにしてデジタル署名検証を用いたファームウェアデータの検証を行う。その中で、ISO/IEC 10118-3:2004 に準拠する SHA-256 によるハッシュ値の算出を実行する。

(1) TOE が持つ RSA 公開鍵(鍵長 2048bit)でデジタル署名データを復号化する。
(2) SHA-256 でファームウェアデータのハッシュ値を算出する。
(3) (1)と(2)の値を比較する。一致すればファームウェアデータが正常であると判断する。

また、TOE は、IPsec 通信の IKEv1 認証アルゴリズムとして、ISO/IEC 10118-3:2004 に準拠する SHA-1、SHA-256、SHA-348、SHA-512 によるハッシュ値の算出を実行する。

FCS_COP.1(g)

TOE は、IPsec 通信において、FIPS PUB 198-1 で定義される The Keyed-Hash Message Authentication Code、FIPS PUB 180-3 で定義される Secure Hash Standard に準拠する下記鍵付ハッシュメッセージ認証による ESP を実装する。

・メッセージダイジェスト長：160、256、384、512
・鍵長：160、256、384、512
・暗号アルゴリズム：HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512

FCS_CKM.4、FCS_CKM_EXT.4

TOE は、IPsec 通信で利用する鍵、鍵材料の保存先と破棄の方法を Table 7-15 に示す。管理者によって設定された事前共有鍵、IPsec 証明書のプライベート鍵は、現地交換不可な SSD に保存される。管理者がこれらの鍵の削除を実行した時、0x00 で上書き削除する。IPsec で使用されるセッション鍵(一時的な暗号鍵)は、RAM 上に保存される。これらは TOE の電源 OFF により不要になるため削除される。

Table 7-15 鍵の保存先と破棄

鍵		保存先	破棄タイミング	破棄の方法
事前共有鍵	管理者によって設定された事前共有鍵	SSD	管理者による事前共有鍵削除・変更（高信頼通信管理機能）時	0x00 で上書き削除
	管理者によって設定された事前共有鍵を変換して生成した鍵	RAM	電源 OFF	—
対称鍵	IKE 用共有秘密鍵（IKEv1 フェーズ 1 で生成される）	RAM	電源 OFF	—
	IPsec 用共有秘密鍵（IKEv1 フェーズ 2 で生成される）	RAM	電源 OFF	—
プライベート鍵	IPsec 証明書のプライベート鍵	SSD	管理者による証明書削除（高信頼通信管理機能）時	0x00 で上書き削除
	IPsec の Diffie-Hellman プライベート鍵（IKEv1 フェーズ 1 で生成される）	RAM	電源 OFF	—

7.4. 高信頼通信機能

FTP_ITC.1

TOE は、Table 7-16 に示す IT 機器との通信において、IPsec プロトコルを利用するため、チャネルデータが平文で送信されることはない。

Table 7-16 IT 機器との通信

TSF が許可する IT 機器	プロトコル

TSF が許可する IT 機器	プロトコル
SMTP サーバー	IPsec
外部認証サーバー	IPsec
DNS サーバー	IPsec
ログサーバー	IPsec
WebDAV サーバー	IPsec
SMB サーバー	IPsec

FTP_TRP.1(a)

TOE は、管理者が TOE をリモート管理する方法として、クライアント PC のブラウザで動作する WC を提供する。TOE とクライアント PC 間の通信は、高信頼通信パスである IPsec プロトコルを利用する。リモート管理のためにクライアント PC から TOE へアクセスした時、TOE は IPsec プロトコルでのみ通信を開始し、端点の識別と、通信データ漏洩からの保護と、通信データ改変の検知を保証する。

FTP_TRP.1(b)

TOE は、管理者でない利用者が TOE へリモートアクセスする方法として、クライアント PC のブラウザで動作する WC とプリンタドライバーを提供する。TOE とクライアント PC 間の通信は、高信頼通信パスである IPsec プロトコルを利用する。リモートアクセスのためにクライアント PC から TOE へアクセスした時、TOE は IPsec プロトコルでのみ通信を開始し、端点の識別と、通信データ漏洩からの保護と、通信データ改変の検知を保証する。

FCS_IPSEC_EXT.1

TOE は、RFC4301 に準拠する IPsec アーキテクチャを実装する。管理者のみが、IPsec プロトコルとして下記設定値を設定、変更できるが、下記以外の設定値を利用することはできない。

- IPsec カプセル化設定：トランスポートモード
- セキュリティプロトコル：ESP(RFC 4303 に準拠)
  - ESP 暗号化アルゴリズム：AES-CBC-128、AES-CBC-256(RFC 3602 に準拠)
  - ESP 認証アルゴリズム：HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512
- 鍵交換方式：IKEv1(RFC 2407,2408,2409,4109 に準拠)
  - IKEv1 暗号化アルゴリズム：AES-CBC-128、AES-CBC-256(RFC 3602 に準拠)
  - ネゴシエーションモード：Main Mode
  - SA ライフタイム
    - フェーズ 1 の SA：600～86400 秒
    - フェーズ 2 の SA：600～28800 秒
  - Diffie-Hellman Group：グループ 14
  - ESN：無効、有効(RFC 4304 に準拠)
- IKE 認証方式：デジタル署名(RSA)、テキストベースの事前共有鍵
  - デジタル署名
    - RSA-2048 （署名生成、署名検証）
    - RSA-3072 （署名検証）
    - 認証アルゴリズム： SHA-256、SHA-384、SHA-512(RFC 4868 に準拠)
  - テキストベースの事前共有鍵
    - 管理者が設定する事前共有鍵：22 文字の文字列(ASCII 文字列、または HEX 値)
    - 認証アルゴリズム：SHA-1、SHA-256、SHA-384、SHA-512(RFC 4868 に準拠)
  - プロトコル指定
    - プロトコル識別：指定なし（Any）

- IPsec 使用設定
  - DefalutAction：破棄
  - 証明書検証強度設定：有効期限：確認する
    鍵使用法：確認しない
    チェーン：証明書のパスを確認する
    失効確認：確認しない

また、TOE は IPsec セキュリティポリシーデータベース(SPD)を実装しており、管理者により以下の設定ができる。

・IPsec ポリシー: IP パケットの条件を指定して、それぞれの条件に合致した IP パケットに対し保護・通過・破棄のうちどの動作を行うか選択できる。IPsec ポリシーの観点からインバウンドパケットとアウトバウンドパケットは、同じルールで処理される。IP パケットの条件としては Any のプロトコル、通信先 IP アドレス（個別、またはサブネット指定）が設定できる。

・IPsec ポリシーは IP ポリシーグループ 1~10 の 10 グループまで設定できる。1 つの通信相手に、複数の IPsec ポリシーが設定された場合、IPsec ポリシーグループ 1～10 の登録順序に関わらず、下記の優先順位で動作が適用される。

優先度:高　　保護　＞　破棄　＞　通過　　優先度:低

・デフォルトアクション： IPsec ポリシーに合致する設定がなかった場合の動作を下記から選択できる。（この設定について管理者に対し、破棄を選択するようガイダンスで指示している。）

- 破棄：IPsec ポリシーの設定に合致しない IP パケットは破棄する
- 通過：IPsec ポリシーの設定に合致しない IP パケットは通過させる

7.5. セキュリティ管理機能

FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1

TOE は、利用者に対して下記管理機能を提供する。各管理機能は、記載されたインタフェースからのみ操作可能である。プリンタドライバーは、管理機能を提供しない。操作パネルもしくは WC で下記の管理機能を実行する画面に遷移する際には、TOE への識別認証が要求され、未認証で管理機能を利用することはできない。ログイン時、利用者に役割(U.ADMIN、U.NORMAL)を関連付け、関連付けられた役割はログアウトまで維持する。利用者の役割に提供されていない管理機能を利用することはできない。TOE は、Table 6-2、Table 6-3 のアクセス制御において、セキュリティー属性の初期値として利用者文書データ、利用者ジョブデータを作成した一般利用者の User ID を割り当てる。ファクス受信機能により生成される利用者文書データ、利用者ジョブデータは、TOE 外の利用者によって作成されるため、セキュリティー属性の初期値として管理者の User ID を割り当て、ファクス受信中のアクセス制御を実施する。ファクス受信完了後は、F コードが指定されていないファクス受信の場合、ファクス文書は強制メモリ受信ボックスに保存されるため、強制メモリ受信ボックスのアクセス権での制御となり、セキュリティー属性は関係ない。初期値は管理者の UserID が割り当てられる。F コードが指定されているファクス受信の場合、セキュリティー属性の初期値として指定された個人ボックスの User ID が割り当てられる。詳細は、「7.2 アクセス制御」を参照のこと。TOE は、初期値として割り当てられた User ID を上書きする機能を持たない。

Table 7-17 管理者に提供される管理機能

管理機能	内容	許可された操作	操作可能なインタフェース
ユーザー管理機能	TOE の利用者属性 User ID を持つユーザーの登録/	登録、変更、削	操作パネル、WC

管理機能	内容	許可された操作	操作可能なインタフェース
	削除、ユーザーパスワードの登録/変更、一時利用停止の設定/解除、機能制限の設定/解除、管理者権限の付与/削除を行う。ユーザー登録された利用者が文書、もしくはジョブを作成した時、セキュリティー属性の初期値として User ID が設定され、Table 6-2、Table 6-3 の利用者データアクセス制御が実施される。なお、ユーザーを削除すると、当該ユーザーが所有者である文書も削除される。	除	
管理者パスワード設定機能	管理者パスワードを設定する。工場出荷時、管理者パスワードにはデフォルト値が設定されている。運用開始時の設置手続きにおいて、ビルトイン管理者が設定変更する。	変更	操作パネル
ユーザー認証設定機能	ユーザー認証方式の設定を行う。本体装置認証、外部サーバー認証、本体装置＋外部サーバー認証のいずれかを選択する。ビルトイン管理者は、常に本体装置認証で識別認証される。	変更	操作パネル、WC
外部認証サーバー設定機能	外部サーバー認証方式で利用する外部認証サーバーの設定を行う。	登録、変更、削除	操作パネル、WC
認証失敗回数閾値の変更機能	認証失敗回数の閾値を設定する。利用者の連続した認証失敗回数が、この設定値に達した時、TOE は該当利用者に対する認証を停止する。	変更	操作パネル、WC
管理者認証の操作禁止解除時間の変更機能	連続した認証失敗回数が閾値に達することによりビルトイン管理者の認証が停止された場合、認証停止が解除されるまでの時間を設定する。	変更	操作パネル、WC
認証失敗回数(ビルトイン管理者以外)のクリア機能	認証失敗回数をクリアする機能。この操作により、ビルトイン管理者以外の利用者の認証停止を解除することができる。	実行	操作パネル、WC
パスワード規約の変更機能	パスワード規約（パスワード最小文字数設定も含む）の設定・変更を行う。	変更	操作パネル、WC
セキュリティ強化設定機能	セキュリティ強化設定の有効／無効を設定する。 有効に設定した時、セキュリティ機能のふるまいに関係する設定をセキュアな値に一括設定し、その設定を維持する。ネットワークを介した TOE の更新機能、メンテナンス機能（RS-232C I/F を使用）、ネットワーク設定管理初期化機能などの利用が禁止される。利用者が禁止された機能実行や設定変更を実行した場合、警告画面を表示し、利用者が操作の継続を指示した場合、セキュリティ強化設定は無効に変更される。	変更	操作パネル、WC
日時情報の変更機能	日時情報を設定する。監査対象事象が発生した場合、この日時情報が監査ログに記録される。	変更	操作パネル、WC
システムオートリセット時間の変更機能	操作パネル操作中のシステムオートリセット時間の設定を行う。	変更	操作パネル、WC
自動ログアウト時間の変	WC 操作中の自動ログアウト時間の設定を行う。	変更	WC

管理機能	内容	許可された操作	操作可能なインタフェース
更機能			
高信頼通信管理機能	高信頼通信機能である IPsec 通信の設定を行う。IPsec 通信設定、事前共有鍵設定、IPsec 証明書設定の登録、変更、削除。	登録、変更、削除	操作パネル、WC
ネットワーク設定機能	ネットワーク設定(TOE の IP アドレス、DNS サーバーの IP アドレス、ポート番号等、NetBIOS 名等)の登録、変更を行う。	登録、変更	操作パネル、WC
監査ログ管理機能	監査機能の有効/無効、監査ログの取得方法、ログサーバー、自動送信条件の設定と、監査ログの送信と削除を行う。	登録、変更	操作パネル、WC
ボックス管理機能	個人ボックスの登録、変更(ボックス名の変更、ボックスパスワードの登録/変更、所有者ユーザーの変更など)、削除を行う。	登録、変更、削除	操作パネル、WC
強制メモリ受信設定機能	強制メモリ受信の有効/無効、強制メモリ受信ボックスパスワードの登録/変更を行う。	登録、変更	操作パネル、WC

Table 7-18 一般利用者に提供される管理機能

管理機能	内容	許可された操作	操作可能なインタフェース
ユーザーパスワード設定機能	ユーザーパスワードの設定を行う。利用者は、識別認証後、自身のユーザーパスワードを変更することができる。	変更	操作パネル、WC
ボックス管理機能	個人ボックスの登録を行う。また、利用者が所有する個人ボックスに対して変更(ボックス名の変更、ボックスパスワードの登録/変更、所有者ユーザーの変更など)と削除を行う。	登録、変更、削除	操作パネル、WC

FPT_SKP_EXT.1

TOE は、IPsec 通信で利用する暗号鍵のうち、管理者によって設定された事前共有鍵と IPsec 証明書のプライベート鍵を現地交換不可能な不揮発ストレージである SSD に保存する。それ以外の暗号鍵は、RAM に保存する(Table 7-15 参照)。TOE は保存された事前共有鍵、プライベート鍵、暗号鍵を閲覧する機能を提供しないため、利用者が TOE の操作によりそれらを読み出すことはできない。TOE は、MFP 本体に RS-232C IF を実装しているが、運用中は無効化されているため、利用者がこのインタフェースを利用して、SSD の内部データを取り出すことはできない。また、RS-232C IF 以外に、TOE の外部から SSD の内部データを取り出すインタフェースを実装していない。SSD は現地交換不可なストレージであるため、利用者が SSD を取り外して内部データを取り出すことはできない。以上のことから、利用者は保存された事前共有鍵、プライベート鍵、暗号鍵を読み出すことはできない。

7.6. 監査機能

TOE は、監査対象事象に対して監査ログを生成、記録し、ログサーバーへ送信する。

FAU_GEN.1、FAU_GEN.2

TOE は、以下の事象を監査対象事象とし、事象発生時刻(年月日時分秒)、事象の種別、サブジェクト識別情報、

事象の結果を記録する。

Table 7-19 監査対象事象一覧

監査対象事象	ID (サブジェクト識別情報 *1)	結果
ユーザー認証の実施	Admin ID/User ID/未登録 ID	OK/NG
強制メモリ受信ボックスパスワード認証の実施	User ID	OK/NG
ユーザー管理機能による登録、変更、削除	Admin ID	OK/NG
ユーザーパスワードの変更	User ID	OK/NG
管理者パスワードの変更	Admin ID	OK
ユーザー認証設定の変更	Admin ID	OK
外部認証サーバー設定の登録、変更	Admin ID	OK
認証失敗回数閾値の変更	Admin ID	OK
管理者認証の操作禁止解除時間の変更	Admin ID	OK
認証失敗回数(U.BUILTIN_ADMIN 以外)のクリア	Admin ID	OK
パスワード規約変更機能	Admin ID	OK/NG
セキュリティ強化モード設定の変更	Admin ID	OK
日時情報の変更	Admin ID	OK
システムオートリセット時間の変更	Admin ID	OK
自動ログアウト時間の変更	Admin ID	OK
高信頼通信管理設定の登録、変更、削除	Admin ID	OK/NG
ネットワーク設定の登録、変更	Admin ID	OK/NG
監査ログ取得機能の開始	Admin ID	OK
監査ログ取得機能の終了	Admin ID	OK
監査ログ管理機能の登録、変更	Admin ID	OK
ボックス管理機能による個人ボックスの登録、変更、削除	Admin ID/User ID	OK/NG
強制メモリ受信設定機能の登録、変更	Admin ID	OK/NG
プリントジョブの保存	User ID	OK/NG
プリントジョブの印刷	User ID	OK/NG
スキャンジョブの送信	User ID	OK/NG
コピージョブの印刷	User ID	OK/NG
ファクス送信ジョブの送信	User ID	OK/NG
ファクス受信ジョブの受信	システム ID	OK/NG
ファクス受信ジョブの印刷	User ID	OK/NG
保存ジョブの保存	User ID	OK/NG
ファクス受信ジョブの保存	システム ID	OK/NG
保存ジョブの印刷	User ID	OK/NG
保存ジョブの送信	User ID	OK/NG
保存ジョブのファクス送信	User ID	OK/NG
保存ジョブのダウンロード	User ID	OK/NG
保存ジョブの移動	User ID	OK/NG
保存ジョブの複製	User ID	OK/NG
保存ジョブの削除	User ID	OK/NG
IPsec セッション確立の失敗	システム ID	errNo(*2)

(*1)識別認証前に発生した監査対象事象の ID(サブジェクト識別情報)は、未登録 ID という固定値を記録する。
ファクス受信は識別認証を行わないためシステムID(固定値:システム(MFP))を記録する。

IPsec セッション確立の失敗においてもシステムID(固定値:システム(MFP))を記録する。
(*2)"1414"(セキュア通信(IPSec)の失敗)などの所定のエラーが記録される。

FAU_STG_EXT.1

TOEは、監査機能の有効/無効、監査ログの取得方法、ログサーバー、自動送信条件の設定と、監査ログの送信と削除を管理者が実施する監査ログ管理機能を提供する。ログサーバーは、WebDAV サーバーを利用する。監査ログの取得方法は自動送信を設定し、IPsec 通信を利用してログサーバーへ監査ログを送信する。TOE とログサーバー間の IPsec 通信は、高信頼通信管理機能により設定する。

TOEは、ログ情報をログファイルとしてTOE内のローカル保存領域に一時保存し、自動送信条件で設定した日時もしくは設定したログ蓄積量に達した場合、もしくは管理者が監査ログ送信を実行した場合に、XML データに変換してログサーバーへ送信する。

TOE 内に一時保存されたログファイルは、XML データに変換後もしくは管理者が監査ログ削除を実行した時、削除する。XML データは、ログサーバーへの送信完了後、次のログファイルの XML データ変換の際に削除する。TOE 内に一時保存されたログファイル、XML データへアクセスするインタフェースは、管理者による監査ログの送信と削除のみであり、一般利用者や攻撃者が不正にアクセスすることはできない。

ネットワーク障害などでログサーバーにログ情報を送信できず、TOE 内のローカル保存領域が満杯になった場合、実行できる機能は以下の機能に制限される。

・電源 OFF による監査ログ取得機能の終了
・電源 ON による監査ログ取得機能の開始
・ユーザー認証（操作パネルからの管理者ログインのみ許可）
・管理者による監査ログ送信、もしくは削除

管理者が監査ログ送信もしくは監査ログ削除を実行し、ローカル保存領域の満杯状態が解消されることで、制限が解除される。

Table 7-20 監査ログデータの仕様

監査ログデータの取り扱い	概要
ログ情報の保管領域	SSD に保存する
ログ情報の保持サイズ	ログ情報はログファイルとして一時保存し、XML データに変換してログサーバーに送信する。 ログファイルは最大 40MB 保存可能で、下記いずれかのタイミングで、ログサーバーへの送信のため XML データに変換する。変換後、当該ログファイルは削除する。 ・管理者が設定した日時もしくは蓄積量に達した場合 ・36MB に達した場合 ・管理者が監査ログ送信を実行した場合 XML データはログサーバーに送信後、次の XML データが生成される際に削除する。送信失敗の場合、最大 76MB（ログファイル 40MB、XML データ 36MB）が TOE 内に一時保存される。

FPT_STM.1

TOE はクロック機能を有し、管理者のみに TOE の時刻を変更する機能を提供する。監査ログに記録する時刻情報はクロック機能から提供される。

7.7. 高信頼な運用機能

7.7.1. アップデート機能

FPT_TUD_EXT.1

管理者は、操作パネルもしくは WC で識別認証後、管理者画面でファームウェアバージョンの確認を実行できる。

また、管理者は、ファームウェアデータとデジタル署名データを格納した USB メモリを TOE に装着し、操作パネルで識別認証後、管理者画面でファームウェアのアップデート機能を実行できる。ファームウェアデータには、システムコントローラやプリントコントローラといった各種ファームウェアと、SHA-256 によって算出した各ファームウェアのハッシュ値情報（7.7.2.に記載の自己テスト機能で利用する）が含まれている。デジタル署名データは、SHA-256 で算出したファームウェアデータのハッシュ値に対して、FIPS PUB 186-4, “Digital Signature Standard”に記載の RSA デジタル署名アルゴリズム(鍵長 2048bit、署名スキーム PKCS #1 Ver 1.5)で署名したデータである。

管理者がアップデート機能を実行した時、TOE はインストールを開始する前に RSA 公開鍵（鍵長 2048bit、出荷時に TOE にインストールされている）を使用して、ファームウェアデータのデジタル署名検証を実施する。署名検証が失敗した場合は、操作パネルに警告を表示し、ファームウェアの書き換え処理は行わない。署名検証が成功した場合は、ファームウェアと各ファームウェアのハッシュ値情報をインストールする。デジタル署名検証の手順は、下記の通り。

(1) TOE が持つ RSA 公開鍵(鍵長 2048bit)でデジタル署名データを復号化する。
(2) SHA-256 でファームウェアデータのハッシュ値を算出する。
(3) (1)と(2)の値を比較する。一致すればファームウェアデータが正常であると判断する。

7.7.2. 自己テスト機能

FPT_TST_EXT.1

TOE は、電源 ON 時に、以下の表に示したテストを順番に実施し、異常が検出された場合、操作パネルに警告を表示し、動作を停止、操作を受け付けない状態に移行する。これにより、TSF を実施するファームウェアの完全性を確認できる。

Table 7-21 自己テスト

No.	対象	テスト
1	システムコントローラ等の各種ファームウェア	SHA-256 で算出した各ファームウェアのハッシュ値と、アップデート機能で TOE へインストールされたハッシュ値情報に記録されている値が一致することを確認。TOE で利用する暗号化ライブラリもハッシュ値検証の対象となる。
2	暗号化ライブラリ アルゴリズム：SHA,HMAC 等	各暗号アルゴリズムに対する既知解テスト KAT test for SHA-1、KAT test for SHA-512、KAT test for HMAC SHA-256、KAT test for AES encryption (CBC, 128-bit key)、KAT test for AES decryption (CBC, 128-bit key)、KAT for RSA 2048-bit (PKCS #1 v1.5)、KAT for DSA (signing P=2048/N=256; verification P=1024/N=160)、KAT for Diffie-Hellman を実施。
3	暗号化ライブラリ アルゴリズム：DRBG	エントロピー源として利用するソフトウェアを設定し、DRBG 関数のヘルステスト（NIST SP800-90A の「11.3 Health Testing」に基づき、Instantiate、Generate、Reseed の機能について既知解テスト）を実施。

7.8. FAX 分離機能

FDP_FXS_EXT.1

TOE が実装するファクスインタフェースの利用方法として、公衆回線を介した外部 FAX 機器からのファクス受信と、利用者が操作パネルから実行するファクス送信がある。ファクスインタフェース経由で送受信が許可されているデータは、上記利用方法に示したファクス文書だけである。

TOE は、ファクスモデム機能を実装しており、Super G3 プロトコルおよび G3 プロトコルをサポートする。ファクスモデムは、ファクス送受信のみを実行し、公衆回線を介した他のコマンドは一切受け付けない。また、TOE は、PSTN と LAN 間のネットワークブリッジを形成する機能を持たない。

以上のことから、利用者が TOE のファクスインタフェースを用いて利用できるのは、ファクス送受信のみである。

以上