KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514

セキュリティターゲット

バージョン：2.00

発行日：2020年2月27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 C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514 セキュリティターゲット
・STバージョン　：2.00
・作成日　：2020年2月27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 C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514, DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514
・バージョン　：G00-45

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。KONICA MINOLTA bizhub C360i/bizhub C300i/bizhub C250i/bizhub C036DNi/bizhub C030DNi/bizhub C025DNi with FK-514はMFP本体（KONICA MINOLTA bizhub C360i、KONICA MINOLTA bizhub C300i、KONICA MINOLTA bizhub C250i、KONICA MINOLTA bizhub C036DNi、KONICA MINOLTA bizhub C030DNi、KONICA MINOLTA bizhub C025DNiのいずれかとそのバージョン(G00-45)）にFAXキット（商品名FK-514、それに対応する識別情報A883）を搭載したものであり、DEVELOP ineo+ 360i/ineo+ 300i/ineo+ 250i with FK-514はMFP本体（DEVELOP ineo+ 360i、DEVELOP ineo+ 300i、DEVELOP ineo+ 250iのいずれかとそのバージョン(G00-45)）にFAXキット（商品名FK-514、それに対応する識別情報はA883）を搭載したものである。

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. TOE の使用方法

TOEの利用環境を図示して、使用方法を記述する。なお、TOEに必要なTOE以外のハードウェア／ソフトウェアについては1.3.3に記述する。

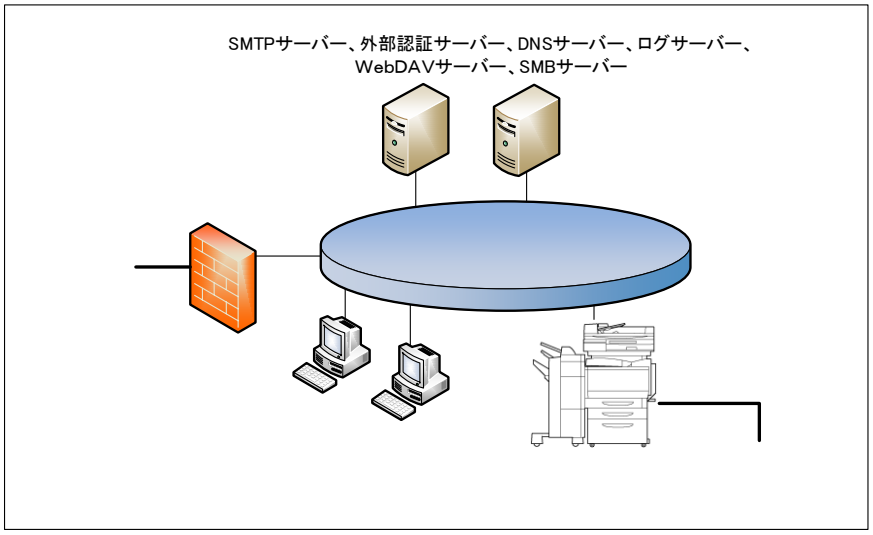

図 1-1 TOE の利用環境

TOEは図 1-1に示すように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。

(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) FAXキット

ファクス機能を使用するため必要な装置。TOE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。

・MFP の各種設定
・電子文書の蓄積・印刷
・蓄積文書のネットワーク送信・ダウンロード・削除

(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。

1.3.3. 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。

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(Webブラウザ)	Microsoft Internet Explorer 11
プリンタドライバー	KONICA MINOLTA C360iSeries PCL / PS
外部認証サーバー	Microsoft Windows Server 2012 R2 Standardに搭載されるActiveDirectory
DNSサーバー	Microsoft Windows Server 2012 R2 Standardに搭載されるActiveDirectory
SMTPサーバー	Black Jumbo Dog Ver. 5.9.5
ログサーバー	Microsoft Windows Server 2012 R2 Standard付属のIIS 8.0
WebDAVサーバー	Microsoft Windows Server 2012 R2 Standard付属のIIS 8.0
SMBサーバー	Microsoft Windows Server 2012 R2 Standardでのファイル共有

1.3.4. TOE の主要なセキュリティ機能

TOE は、LAN と公衆回線に接続され、利用者が文書のプリント、スキャン、コピー、ファクス、文書の保存と取り出し、ネットワーク通信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 FW によるアップデートを防止し、運用中の FW の不正改ざんを検知する高信頼な運用機能。

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は「図 1-2」に示すように、主電源・副電源、操作パネル、スキャナユニット、制御コントローラユニット、プリンタユニット、FAXキットで構成されるMFPである。

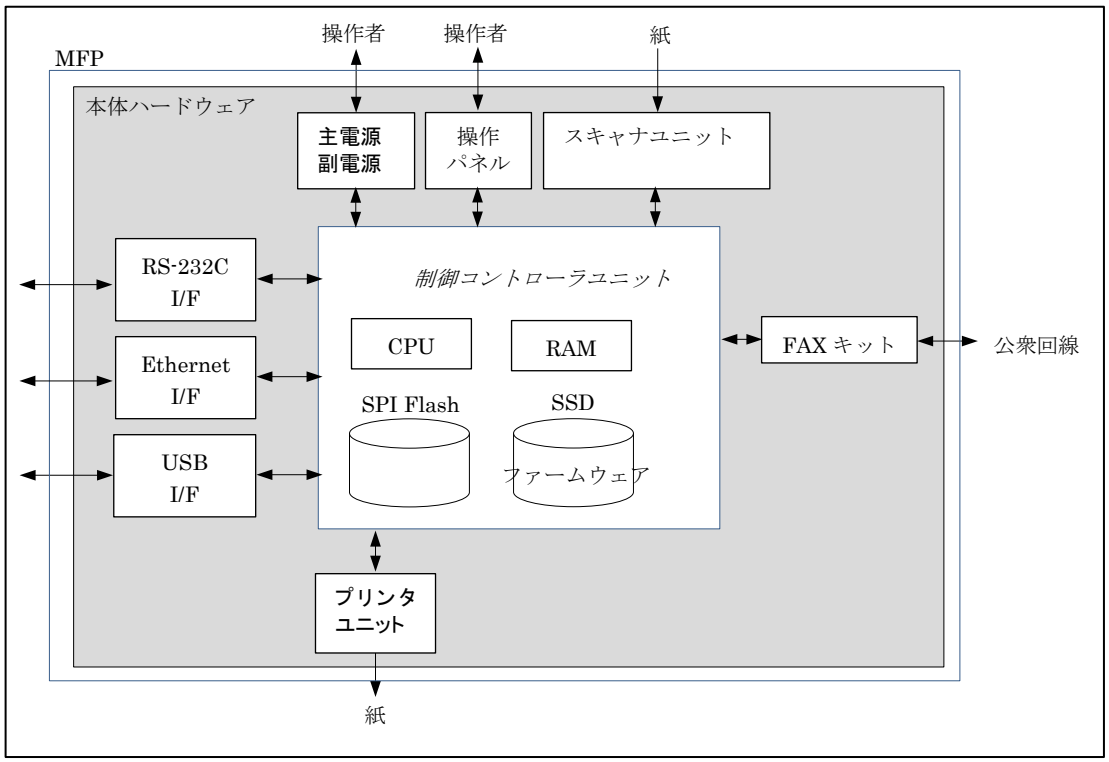

図 1-2 TOE の物理的範囲

(1) 主電源・副電源

MFP を動作させるための電源スイッチ。

(2) 操作パネル

タッチパネル液晶ディスプレイで構成する MFP を操作するための専用コントロールデバイス。

(3) スキャナユニット

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。

(4) 制御コントローラユニット

MFP を制御する装置。

(5) CPU

中央演算処理装置。

(6) RAM

作業領域として利用される揮発メモリ。

(7) SPI Flash

MFP の動作を決定する TSF データが保存される不揮発メモリ（現地交換不可）。

(8) SSD

256GB の現地交換可能ではない記憶媒体。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メッセージデータ、MFP の動作において必要な設定値等の他、電子文書がファイルとして保存される。

(9) ファームウェア

MFP の動作を制御するソフトウェア。

(10)プリンタユニット

制御コントローラからの指示により、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。

(11)RS-232C I/F

D-sub9 ピンを介して、シリアル接続することが可能なインタフェース。故障時などに本インタフェースを介してメンテナンス機能を使用することができる。

(12)Ethernet I/F

10BASE-T、100BASE-TX、Gigabit Ethernet をサポートするインタフェース。

(13)USB I/F

ガイダンスに従って、ファームウェアの書き換えを行う際に使用する。

(14)FAXキット

公衆回線を介して FAX の送受信に利用されるデバイス。

1.4.2. ガイダンス

本 TOE を構成するガイダンスの一覧を以下に示す。

Table 1-1 TOE を構成するガイダンス

種類	ガイダンス名称	バージョン	言語
FULL 版	bizhub C360i/C300i/C250i ユーザーズガイド	1.00	日本語
	bizhub C360i/C300i/C250i User's Guide（※）	1.00	英語
	ineo+ 360i/300i/250i User's Guide	1.00	英語
セキュリティ機能編	bizhub C360i/C300i/C250i ユーザーズガイド　セキュリティ機能編	1.02	日本語
	bizhub　C360i/C300i/C250i/C036DNi/C030DNi/C025DNi　User's Guide [Security Operations]	1.02	英語
	ineo+ 360i/300i/250i User's Guide [Security Operations]	1.02	英語

※bizhub C036DNi, bizhub C030DNi, bizhub C025DNi にも対応する。

1.4.3. TOE の各部分と識別

TOE は、本体ハードウェア、FAX キット、ファームウェア、ガイダンスの単位で配付される。

Table 1-2 本体ハードウェア、FAX キット、ファームウェアの配付形式・配付方法

配付単位	識別	形式	配付方法
本体ハードウェア（右のいずれか）	bizhub C360i	ハードウェア	専用箱に梱包して配付する。
	bizhub C300i		
	bizhub C250i		
	bizhub C036DNi		
	bizhub C030DNi		
	bizhub C025DNi		
	ineo+ 360i		
	ineo+ 300i		
	ineo+ 250i		
FAX キット	FK-514	ハードウェア	専用箱に梱包して配付する。
ファームウェア	AA2J0Y0-F000-G00-45	ファイル（exe）（電子署名付与）	サービスマンが持参する。

Table 1-3 ガイダンスの配付形式・配付方法

ガイダンス	形式	配付方法	備考
FULL 版	ファイル（exe）（電子署名付与）	サービスマンが exe ファイルを持参。exe ファイルを実行することで html を入手する。	本体ハードウェアに対応するガイダンス（FULL 版とセキュリティ機能編）を配付する。日本語／英語は購入者の希望による。
セキュリティ機能編		サービスマンが exe ファイルを持参。exe ファイルを実行することで pdf を入手する。	

1.4.4. 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。

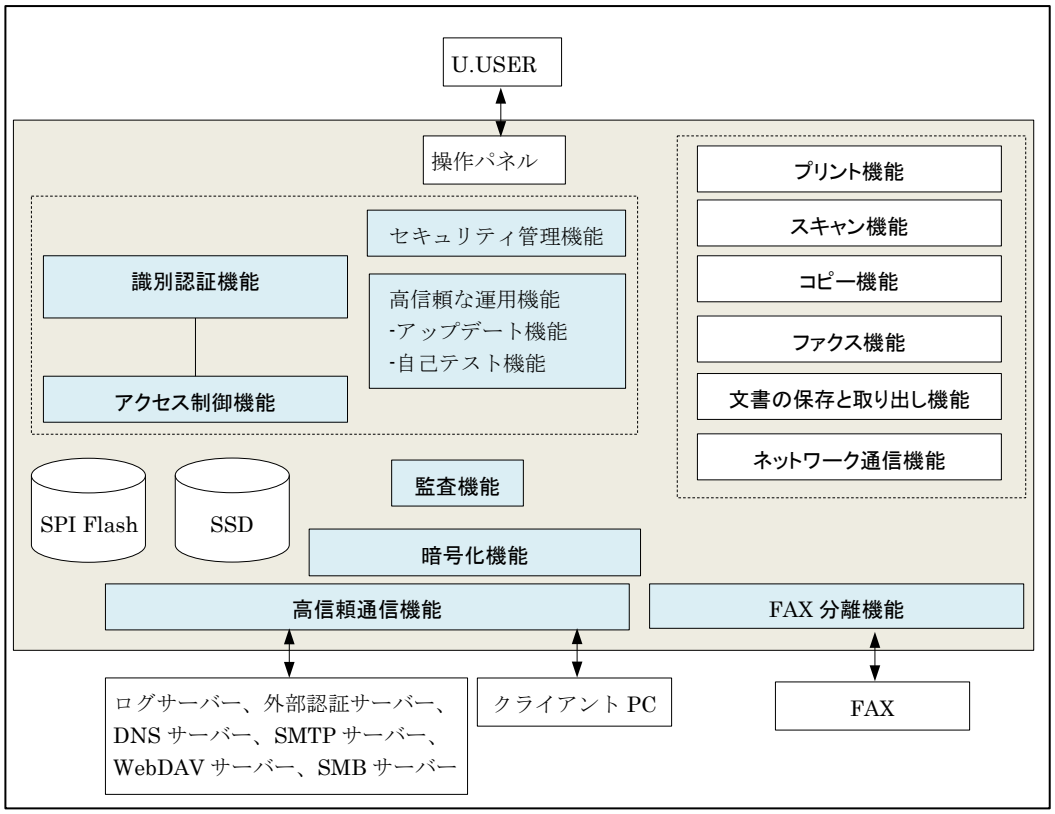

図 1-3 TOE の論理的範囲

1.4.4.1. 基本機能

以下に、TOEの基本機能を記述する。

(1) プリント機能

クライアント PC のプリンタドライバーもしくは WC を利用して、LAN 経由で受信した印刷データを認証&プリントボックスもしくはパスワード暗号化 PDF ボックスに一時蓄積し、印刷する機能。

(2) スキャン機能

利用者による操作パネルからの操作によって、紙文書を読み取って文書ファイルを生成し、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。

TOE は文書を蓄積しておくことが出来、TOE に蓄積されている文書をファクス送信することも出来る。TOEに蓄積されている文書でファクス送信可能なものをファクス送信文書という。また、ファクス受信した文書は TOE 内に蓄積し、印刷、削除、送信（FAX、E-mail、WebDAV、SMB)、ダウンロードをすることができる。

・ファクス送信機能
紙文書およびファクス送信文書を電話回線から外部のファクス装置に送信する機能。
紙文書は操作パネルからの操作によってスキャンしファクス送信する。ファクス送信文書は操作パネルからの操作によってファクス送信する。

・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。

操作パネルからスキャン機能により紙文書を読み取り電子文書を生成して保存、クライアント PC のプリンタドライバーもしくは WC から文書を保存、ファクス受信機能によって受信したファクス文書を保存することができる。保存された電子文書は、操作パネル、WC から取り出しできる。

(6) ネットワーク通信機能

ローカルエリアネットワーク(LAN) 上で文書を送受信する機能。

1.4.4.2. 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。

(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。認証方式には TOE 自身が識別認証を行う本体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動作が一定時間ない（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

強制メモリ受信ボックスにアクセスする場合（ファクス受信を除く)、パスワードの入力を要求し、入力されたパスワードを検証して、正しいパスワードが入力された場合のみアクセスを許可する機能。

(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

データ資産が LAN 上での通信中にアクセスできないようにする（暗号化する）機能。暗号鍵は RAM(揮発メモリ)及び SSD に保存される。

(4) 高信頼通信機能

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。クライアント PC、SMTP サーバー、外部認証サーバー、DMS サーバー、ログサーバー、WebDAV サーバー、SMB サーバーと通信する際、接続先の正当性を検証し、(3)Encryption（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。

(5) セキュリティ管理機能

TOE のセキュリティ設定を構成する能力が、管理者役割の権限が付与された利用者のみに利用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のログを事象発生時刻等とともにログファイルとして記録し、監査できる形式で提供する機能。

ログファイルは、高信頼通信機能を使用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。

(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、および、自己テスト。

(8) FAX分離機能

TOE のファクス I/F が、TOE が接続している PSTN とネットワークとの間のネットワークブリッジを作成するために使用されるのを防止する機能。

1.4.5. 用語

本 ST で使用する用語の意味を定義する。

Table 1-4 用語

Designation	Definition
電子文書	文字や図形などの情報を電子化した文書データ。
紙文書	文字や図形などの情報を持つ紙媒体の文書。
WC	Web Connection. Web ブラウザを通して TOE を操作する機能・インタフェース。
Role	U.USER の役割。 U.NORMAL 、 U.ADMIN が あ り 、 U.ADMIN は さ ら に U.BUILTIN_ADMIN と U.USER_ADMIN に分かれる。
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。
U.BUILTIN_ADMIN （ビルトイン管理者）	U.USER の役割。 あらかじめ TOE に実装されている管理者（ビルトイン管理者）にのみ付与される役割。

Designation	Definition
U.USER_ADMIN （ユーザー管理者）	U.USER の役割。 U.ADMIN によって付与される役割。 U.USER_ADMIN 用のインタフェースからログインに成功することで、この役割での操作ができるようになる。 役割の付与・削除が可能であることと認証失敗時の扱いを除き U.BUILTIN_ADMIN と同じ。
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。
サービスマン	ファームウェアを持参し、TOE の設置をサポートする役割。
システムオートリセット	ログイン中に、予め設定されたシステムオートリセット時間でアクセスがなかった場合に自動的にログアウトする機能。
システムオートリセット時間	管理者が設定する時間。この時間が経過すると自動的にログアウトする。操作パネルからの操作が対象。
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。
セキュリティ強化設定	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機能。この機能が有効になっていることにより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、または利用の際に警告画面が表示されるほか、設定値の変更の際にも警告画面が表示され、設定値の変更（管理者だけが実行可能）を行うとセキュリティ強化設定は無効になる。
セッションの自動終了機能	セッションを自動的に終了する機能。 操作パネル、WC についてそれぞれ一定時間操作がおこなわれないとセッションを自動的に終了する。
プリントジョブ投入機能	TOEがクライアントPCから送信されたユーザーID、ログインパスワード、印刷データを受け入れる機能。ユーザーID、ログインパスワードによる識別認証が成功した場合のみ印刷データを受け入れる。
ボックス	文書を保存するためのディレクトリ。 保存される文書には蓄積文書と実行中のジョブに含まれる文書がある。 ボックスにより、文書を保存、操作することが出来る利用者が異なる。
ボックスパスワード	強制メモリ受信ボックスに設定されるパスワード。
ユーザーID (User ID)	利用者にあたえられている識別子。TOEはその識別子により利用者を特定する。 外部サーバー認証時は、ユーザーID＋外部サーバーIDで構成される。 操作パネル等のインタフェース上では「ユーザー名」と表示される。
ユーザーID一時利用停止・解除	一時利用停止：当該ユーザーIDによるログインを停止すること 解除：一時利用停止を解除すること。
ユーザー管理機能	ユーザーの登録／削除、アクセス権限の付与／削除／変更、役割（U.USER_ADMIN）の付与／Deleteを行う機能。 ※アクセス権限：文書や文書処理に関連する情報にアクセスするための権限

Designation	Definition
ユーザー認証の管理機能	認証方式（本体認証／外部サーバー認証）の設定を行う機能。
ユーザー認証機能	TOEの利用者を認証する機能。 本体認証（内部認証）と外部サーバー認証（外部サーバーによる認証）の２種類がある。 U.BUILTIN_ADMINは本体認証のみで認証される。
ログイン	TOEにおいて、ユーザーIDとログインパスワードによって識別認証を実行すること。
ログインパスワード (LOGIN PASSWORD)	TOEにログインするためのパスワード。
外部サーバー認証設定データ	外部認証サーバーに関する設定データ（外部サーバーが所属するドメイン名などを含む)。
監査ログ管理機能	以下を行う機能。 ・監査ログの蓄積量の設定 ・監査ログの送信日時の設定 ・監査ログの送信 ・監査ログの削除
監査ログ機能	監査ログを取得する機能。
管理者認証の操作禁止解除時間	連続した認証失敗回数が設定値に達することにより U.BUILTIN_ADMINの認証がロックされた場合にロックが解除されるまでの時間。
高信頼チャネル管理機能	高信頼チャネル機能の実行のほか、暗号方式等の管理を行う機能。
高信頼通信機能	LANを経由してやり取りするデータを暗号化して保護する機能(Trusted communications)
時刻情報	時刻の情報。監査対象事象が発生した場合、この時刻情報が監査ログに記録される。
自動ログアウト時間	管理者が設定する時間。この時間が経過すると自動的にログアウトする。WCが対象。
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）文書。
認証&プリント機能 (AUTH PRINT)	ネットワーク上のコンピューターから送信されたユーザーID、パスワードを伴う文書をプリント指示された文書として保存する機能。
認証失敗回数閾値	管理者が設定する閾値。連続した認証失敗回数がこの閾値に達すると認証機能がロックされる。

1.4.6. ボックス

TOE が提供するボックスについて記述する。TOE は以下の種類のボックスを提供する。

（なおこれはボックスの特徴に基づく分類であるが、操作パネル等における表示と必ずしも一致するものではない。また、これ以外に掲示版ボックスなども存在するがここに記述した種類のボックス以外は使用できない。）

Table 1-5 システムボックス

ボックスの種類	説明
強制メモリ受信ボックス	PSTN faxing、Storage and retrieval で使用するボックス。 強制メモリ受信設定は U.ADMIN が行う。 U.ADMIN によってパスワードが設定される。このボックスに保存されている文書に対しては以下の操作が可能。 U.ADMIN ・削除 パスワードを知っている U.NORMAL ・印刷 ・文書名変更 ・ダウンロード ・プレビュー ・削除
パスワード暗号化 PDF ボックス	暗号化 PDF（開くときにパスワードを入力するように設定されている PDF ファイル）を保存するボックス。文書を指定してパスワード入力することで当該文書の印刷等が出来る。 プリント機能、文書の保存と取り出し機能で使用する。
認証&プリントボックス	認証&プリント機能で文書が保存されるボックス。 認証&プリント機能は、利用者がクライアント PC のプリンタドライバー、WC からクレデンシャルを含む印刷データを送信し、TOE が認証&プリントボックスに一時蓄積した後、利用者が操作パネルからログイン後、印刷するプリント機能。

Table 1-6 機能ボックス

ボックスの種類	
個人ボックス	PSTN faxing、Storage and retrieval で使用するボックス。 U.ADMIN と当該ボックスの所有者（当該ボックスの Box User ID と一致する User ID でログイン中のユーザー）のみ操作可能。 このボックスに保存されている文書に対しては以下の操作が可能。 U.ADMIN ・削除 ・ボックスの所有者の変更による当該ボックス内文書の所有者の変更 ボックスの所有者 ・編集 ・印刷 ・PSTN fax で送信 ・削除

ボックスの種類	
	・owner が同じボックスへのコピー／移動 ・E-mail 送信 ・WebDAV 送信 ・SMB 送信 ・ダウンロード ・プレビュー ・ボックスの所有者の変更による当該ボックス内文書の所有者の変更

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における利用者役割は以下の通りである。

Table 3-1 User Categories

Designation			Definition
U.USER （許可利用者）			Any identified and authenticated User.
	U.NORMAL （Normal User）		A User who has been identified and authenticated and does not have an administrative role
	U.ADMIN （Administrator ）	U.BUILTIN_ADMIN （ビルトイン管理者）	A User who has been identified and authenticated and has an administrative role
		U.USER_ADMIN （ユーザー管理者）	

※U.BUILTIN_ADMIN、U.USER_ADMINについては1.4.5用語を参照

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 Data	TSF Data for which alteration by a User who is neither the 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 ST は以下の拡張コンポーネントを定義する。これらは PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015、Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017)において定義された extended components の一部である。

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. FCS_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	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_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: 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 an 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.

5.4. 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.

5.5. 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 Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.6. FPT_TST_EXT.1 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.

5.7. 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 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.

5.8. 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.

5.9. 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 Generation)

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.

5.10. 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 length*s];
- 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.

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。

＜セキュリティ機能要件"操作"の明示方法＞

ボールド書体は、[PP]で完成または詳細化された SFR の部分を示し、コモンクライテリアパート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している。

*イタリック*書体は、ST で選択、かつ／または完成する必要がある部分を示し、[ST]において選択、かつ／または完成されている。

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 の部分を示し、コモンクライテリアパート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している SFR の部分を示している。これらは、また、ST において選択され、かつ／または完成されている。

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,**[assignment: *other specifically defined auditable events*].		
	[assignment: *other specifically defined auditable events*] *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,** [assignment: *other audit relevant information*].		

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
	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
	[assignment: *other audit relevant information*] *なし*		

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 [selection:** ・ ***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 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ・ ***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.**
	[selection: ・ ***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 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ・ ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***] ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

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 [selection: *128 bit, 256 bit*] that meet the following: No Standard.**		
	[selection: *128 bit, 256 bit*] ***128 bit, 256 bit***		

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 [**selection**: ***For volatile memory, the destruction shall be executed by [selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]].*** ***For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static***		

	pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;] that meets the following: [**selection:** *NIST SP800-88, no standard*].
	[**selection**: *For volatile memory, the destruction shall be executed by [selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]].* *For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;*] *For volatile memory, the destruction shall be executed by [selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]].* *For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;*
	[selection: powering off a device,[assignment: other mechanism that ensures keys are destroyed]] *powering off a device*
	[assignment: other mechanism that ensures keys are destroyed] *メモリの解放*
	[selection: single, three or more times] *single*
	[selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern] *a static pattern*
	[selection: read-verify, none] *none*
	[**selection:** *NIST SP800-88, no standard*] *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 [assignment: *one or more modes*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following: **・ FIPS PUB 197, "Advanced Encryption Standard (AES)"** **・ [Selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*]**
	[assignment: *one or more modes*] ***CBC***
	[Selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*] ***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 [selection: ***・ Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment:2048 bits or greater],*** ***・ RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*** ***・ Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*** that meets the following **[selection:** ***Case: Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: RSA Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: Elliptic Curve Digital Signature Algorithm*** ***・ FIPS PUB 186-4, "Digital Signature Standard"*** ***・ The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*** **]**		
	[selection: ***・ Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment:2048 bits or greater],*** ***・ RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*** ***・ Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of***		

	[assignment: 256 bits or greater]] *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]*
	[assignment: 2048 bits or greater] *2048 bits, 3072bits*
	[selection: *Case: Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *Case: RSA Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *Case: Elliptic Curve Digital Signature Algorithm* *・FIPS PUB 186-4, "Digital Signature Standard"* *・The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*] *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 [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].		
	[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] *NIST SP 800-90A*		
	[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*] *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.		
	[selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)] [assignment: *number of software-based sources*] software-based noise source(s)		
	[assignment: *number of software-based sources*] *one software-based source*		
	[selection: *128 bits, 256 bits*]		

	256 bits

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 D.USER.DOC** Access Control SFP **and Table 6-3 D.USER.JOB** Access Control SFP**.**		

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 D.USER.DOC** Access Control SFP **and Table 6-3 D.USER.JOB** Access Control SFP**.**		
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 D.USER.DOC*** Access Control SFP ***and Table 6-3 D.USER.JOB*** Access Control SFP.		
FDP_ACF.1.3	**Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*].		
	[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*] *なし*		
FDP_ACF.1.4	**Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*].		
	[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*] *なし*		

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

		"Create"	**"Read"**	**"Modify"**	**"Delete"**
Print	***Operation :***	***Submit a document to***	***View image or Release***	***Modify stored document***	***Delete stored document***

		be printed	*printed output*		
	Job owner	(note 1)	permitted	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	*Operation :*	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)	denied	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	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)	permitted	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	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	permitted	permitted
	U.ADMIN	denied	denied	denied	permitted
	U.NORMAL	denied	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)	permitted	permitted	(注 1)
	U.ADMIN	(note 4)	denied	denied	(注 1)
	U.NORMAL	(note 4)	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Storage/ retrieval	*Operation :*	*Store document*	*Retrieve stored document*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)	permitted	permitted	permitted
	U.ADMIN	permitted	denied	denied	permitted
	U.NORMAL	permitted	denied	denied	denied
	Unauthenticated	(condition 1)	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)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied

Scan	*Operation :*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	denied	denied
Copy	*Operation :*	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	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)	permitted	denied	permitted
	U.ADMIN	denied	permitted	denied	permitted
	U.NORMAL	denied	permitted	denied	denied
	Unauthenticated	denied	permitted	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)	permitted	denied	permitted
	U.ADMIN	(note 4)	permitted	denied	permitted
	U.NORMAL	(note 4)	permitted	denied	denied
	Unauthenticated	(condition 1)	permitted	denied	denied
Storage / retrieval	*Operation :*	*Create storage / retrieval job*	*View storage / retrieval log*	*Modify storage / retrieval job*	*Cancel storage / retrieval job*
	Job owner	(note 1)	permitted	denied	permitted
	U.ADMIN	permitted	permitted	denied	permitted
	U.NORMAL	permitted	permitted	denied	denied
	Unauthenticated	(condition 1)	permitted	denied	denied

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

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.

Table 6-4 Table 6-2、Table 6-3 の補足

項目	説明
注 1	ファクス受信文書は強制メモリ受信ボックスまたは指定ボックス（個人ボックス）に保存文書として保存される。 受信中のジョブのキャンセルは U.ADMIN が可能で、キャンセルすることにより、保存前の文書（受信中の文書）も削除される。 ファクス受信文書の印刷ジョブのキャンセルは U.ADMIN および当該印刷ジョブを実行した Fax owner が可能。 ファクス受信文書の削除は、Fax owner と U.ADMIN が実行可能。

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 [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].		
	[selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] *an administrator configurable positive integer within*[assignment: *range of acceptable values*]		
	[assignment: *range of acceptable values*] *1～3*		
	[assignment: *list of authentication events*] *本体認証におけるログインパスワードによる認証* *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 [selection: met, surpassed], the TSF shall [assignment: *list of actions*].		
	[selection: *met, surpassed*] *met, surpassed*		
	[assignment: *list of actions*] *ログインパスワードによる認証の停止* *ボックスパスワードによる認証の停止* *＜通常復帰のための操作＞* *U.BUILTIN_ADMIN の認証の場合：TOE の起動処理を行う。（起動処理から管理者認証の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解除処理が行なわれる。）* *それ以外（U.USER_ADMIN を含む）の場合：認証停止状態でない U.ADMIN による認証失敗回数の消去機能の実行*		

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: [assignment: *list of security attributes*].		
	[assignment: *list of security attributes*]. *User ID* *役割* *アクセス権限*		

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: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: *other characters*]]; ・Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;		
	[selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: *other characters*]] "!", "@", "#", "$", "%", "^", "&", "*", "(", ")" [assignment: *other characters*] *"-", "¥", "[", "]", ":", ";", ",", ".", "/", "", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?", "_" and スペース*		

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 [assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is authenticated.		
	[assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] ***本体認証におけるユーザー利用停止状態の確認*** ***ファクス受信*** ***TOE の状態確認および表示等の設定***		

	操作パネルからのファームウェアのバージョンの問い合わせ
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 [assignment: *list of feedback*] to the user while the authentication is in progress.		
	[assignment: *list of feedback*] *入力された文字データ 1 文字毎に“＊”または”●”の表示*		

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 [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is identified.		
	[assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] ***本体認証におけるユーザー利用停止状態の確認*** ***ファクス受信*** ***TOE の状態確認および表示等の設定*** ***操作パネルからのファームウェアのバージョンの問い合わせ***		
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: [assignment: *list of user security attributes*].		
	[assignment: *list of user security attributes*]. *User ID* *役割* *アクセス権限*		
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: [assignment: *rules for the initial association of attributes*].
	[assignment: *rules for the initial association of attributes*] *なし*
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].
	[assignment: *rules for the changing of attributes*] *なし*

6.1.1.5. Class FMT: Security Management

FMT_MOF.1	**Management of security functions behaviour**		
(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 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN**.		
	[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] *modify the behaviour of*		
	[assignment: *list of functions*] *・セキュリティ強化設定* *・ユーザー認証機能* *・監査ログ機能* *・高信頼チャネル機能*		

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 [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].		
	[selection: *change_default, query, modify, delete, [assignment: other operations]*] *Refer to Table 6-5,Table 6-6*		
	[assignment: *list of security attributes*] *Refer to Table 6-5,Table 6-6*		

	[assignment: *the authorized identified roles*] *Refer to Table 6-5,Table 6-6*

Table 6-5 Management of Object Security Attribute

Object Security Attribute	Authorized Identified Roles	Operations
個人ボックスの User ID	当該ボックスの owner U.ADMIN	Modify Create

Table 6-6 Management of Subject Security Attribute

Subject Security Attribute	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
役割 （U.USER_ADMIN）	U.ADMIN	Delete 付与
アクセス権限	U.ADMIN	Delete 付与

FMT_MSA.3	**Static attribute initialisation**		
(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 [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.		
	[selection, choose one of: *restrictive, permissive, [assignment: other property]*] *[assignment: other property]* *refer to Table 6-7*		
FMT_MSA.3.2	**Refinement:** The TSF shall allow the **[selection: *U.ADMIN, no role*]** to specify alternative initial values to override the default values when an object or information is created.		
	[selection: *U.ADMIN, no role*] ***no role***		

Table 6-7 Characteristics Static Attribute Initialization

Object		Attribute	Default values for Object Security Attribute
Print	D.USER.DOC	Job owner	identified by a credential or assigned to an authorized User as part of the process of submitting a print Job
Scan	D.USER.DOC	Job owner	authorized User as part of the process of

Object		Attribute	Default values for Object Security Attribute
			initiating a scan job
Copy	D.USER.DOC	Job owner	authorized User as part of the process of initiating a copy job
Fax send	D.USER.DOC	Job owner	authorized User as part of the process of initiating a fax send job
Fax receive	D.USER.DOC	Fax owner	オブジェクトの保存先が強制メモリ受信ボックスの場合、当該ボックスのパスワードを知っている U.NORMAL、個人ボックスの場合、当該ボックスの owner
Storage / retrieval	D.USER.DOC	Job owner	オブジェクトの保存先が強制メモリ受信ボックスの場合、当該ボックスのパスワードを知っている U.NORMAL、個人ボックスの場合、当該ボックスの owner
Print	D.USER.Job	Job owner	identified by a credential or assigned to an authorized User as part of the process of submitting a print Job
Scan	D.USER.Job	Job owner	authorized User as part of the process of initiating a scan job
Copy	D.USER.Job	Job owner	authorized User as part of the process of initiating a copy job
Fax send	D.USER.Job	Job owner	authorized User as part of the process of initiating a fax send job
Fax receive	D.USER.Job	Fax owner	オブジェクトの保存先が強制メモリ受信ボックスの場合、当該ボックスのパスワードを知っている U.NORMAL、個人ボックスの場合、当該ボックスの owner
Storage / retrieval	D.USER.Job	Job owner	authorized User as part of the process of initiating a storage job

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 6-8.**		

Table 6-8 Management of TSF Data

Data	Operation	Authorised role(s)
[assignment: *list of TSF Data* ***owned by a U.NORMAL or***	[selection: *change default, query, modify, delete, clear,* [assignment:	**U.ADMIN, the owning U.NORMAL.**

Data	Operation	Authorised role(s)
associated with Documents or jobs owned by a U.NORMAL]	*other operations*]]	
U.NORMAL のログインパスワード	[assignment: *other operations*] *登録*	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
ボックスパスワード	[assignment: *other operations*] *登録*	**U.ADMIN**
	modify	
[assignment: *list of TSF Data* ***not owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	**U.ADMIN**
U.BUILTIN_ADMIN のログインパスワード	*modify*	**U.BUILTIN_ADMIN**
時刻情報	*modify*	**U.ADMIN**
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*	
外部サーバー認証設定データ	*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: [assignment: *list of management functions provided by the TSF*].		
	[assignment: *list of management functions provided by the TSF*]		

	refer to Table 6-9

Table 6-9 list of management functions

management functions
U.ADMIN によるセキュリティ強化設定の管理機能
U.ADMIN によるユーザー管理機能
U.ADMIN によるユーザー認証機能の管理機能
U.ADMIN による外部サーバー認証設定データの登録・変更機能
U.ADMIN による高信頼チャネル管理機能
U.ADMIN によるネットワーク設定の登録・変更機能
U.ADMIN による時刻情報の変更機能
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.NORMAL によるボックス管理機能
U.ADMIN によるボックス管理機能
U.NORMAL による自身のログインパスワードの変更機能
U.BUILTIN_ADMIN による自身のログインパスワードの変更機能

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 [selection: *published hash, no other functions*] prior to installing those updates.		
	[selection: *published hash, no other functions*] *no other functions*		

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 [assignment: *time interval of user inactivity*].		
	[assignment: *time interval of user inactivity*] *・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、ファクスの場合、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 [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** 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**.		
	[selection: *IPsec, SSH, TLS, TLS/HTTPS*] ***IPsec***		
	[selection: *authentication server, [assignment: other capabilities]*] ***authentication server, [assignment: other capabilities]***		
	[assignment: other capabilities] ***SMTPサーバー*** ***DNSサーバー*** ***SMBサーバー*** ***ログサーバー*** ***WebDAVサーバー***		
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 [assignment: ***list of services for which the TSF is able to initiate communications***].		
	[assignment: ***list of services for which the TSF is able to initiate communications***]. ***外部サーバー認証*** ***SMTPサーバーとの通信*** ***DNSサーバーとの通信*** ***SMBサーバーとの通信*** ***ログサーバーとの通信*** ***WebDAVサーバーとの通信***		

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** [**selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS***] **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**.
	[**selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS***] ***IPsec***
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** [**selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS***] **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**.		
	[**selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS***] ***IPsec***		
FTP_TRP.1.2(b)	**Refinement**: The TSF shall permit [selection: ***the TSF, remote users***] to initiate communication via the trusted path		
	[selection: ***the TSF, remote users***] ***remote users***		
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. Selectrion-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.1.1	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*].		
	[selection: *tunnel mode, transport 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*].		
	[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*] *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: [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 (with mandatory support for NAT traversal as specified in section 2.23), 4307 [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*]].
	[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 (with mandatory support for NAT traversal as specified in section 2.23), 4307 [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*]] *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*], [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]
	[selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*] *RFC 4304 for extended sequence numbers*
	[selection: *no other RFCs for hash functions, RFC 4868 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*].
	[selection: *IKEv1, IKEv2*] ***IKEv1***
	[selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*] *no other algorithm*
FCS_IPSEC_EXT.1.7 FCS_IPSEC_EXT.1.8	The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode. 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*]].
	[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*]] *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]
	[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*] *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*].
	[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*] *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.
	[selection: *RSA, ECDSA*] *RSA*

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-**[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], **key size** [assignment: **key size (in bits) used in HMAC**], **and message digest sizes [selection: *160, 224, 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."**		
	[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***] ***SHA-1*** ***SHA-256*** ***SHA-384*** ***SHA-512***		
	[assignment: **key size (in bits) used in HMAC**] *160~512bits*		
	[selection: *160, 224, 256, 384, 512*] ***160*** ***256*** ***384*** ***512***		

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 [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 ")").		
	[selection: [assignment: *other supported lengths*], *no other lengths*] [assignment: *other supported lengths*]		
	[assignment: *other supported lengths*] *2~128 characters*		
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*].		
	[selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] *SHA-1* *SHA-256* *SHA-512* [assignment: *method of conditioning text string*]		
	[assignment: *method of conditioning text string*] *SHA-384*		
	[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*] *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 [selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].		

	[selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] ***SHA-1, SHA-256, SHA-384, SHA-512***

6.2. Security Assurance Requirements

The TOE security assurance requirements specified in Table 6-10　provides evaluative activities required to address the threats identified in 3.3 of this ST.

Table 6-10 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 6-11 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

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(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)	高信頼通信機能（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
	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

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
			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_HTTPS_EXT.1	FCS_IPSEC_EXT.1	N/A
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

7.1. 乱数ビット生成

－ 対応する機能要件：FCS_RBG_EXT.1

TOE は、NIST SP 800-90A に準拠する CTR DRBG(AES-256)と、CPU のキャッシュミスや分岐予測ミスの効果によりばらつくタイマー値を取得することでノイズ源とする 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。

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、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 Instatiate 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。

7.2. 識別認証機能

－ 対応する機能要件：FTA_SSL.3、FIA_AFL.1、FIA_PMG_EXT.1、FIA_UAU.1、FIA_UAU.7、FIA_UID.1、FIA_USB.1、FIA_ATD.1

TOE は 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。

TOE を操作する場合は U.BUILTIN_ADMIN、U.USER_ADMIN、U.NORMAL のいずれかの役割を指定し、指定した役割ごとに識別認証をおこなって、識別認証に成功すると対話セッションとして User ID、役割、アクセス権限が結合される。

なお、プリンタドライバーからのプリントジョブ投入時は、役割の指定は行わず、プリントデータとともに投入されるクレデンシャルによって識別認証を行い、識別認証が成功し、クレデンシャルから得られた User ID から特定されるアクセス権が条件を満たす場合にのみ、プリントデータを受け入れる。その場合、U.NORMAL の役割が結合される。プリントジョブの投入は対話セッションの生成は行わず、属性として User ID が付与されたプリントデータを生成する。

強制メモリ受信ボックスにアクセスする場合（ファクス受信を除く）は、パスワードの入力を要求し、入力されたパスワードを検証して、正しいパスワードが入力された場合のみアクセスを許可する。なお、このパスワードは 7.4 セキュリティ管理機能（Administrative roles）に記載した通り、U.ADMIN が登録と変更を行うことができる。

(1) 認証方式

TOE 自身が識別認証を行う本体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存在する。外部サーバー認証方式の場合は入力されたユーザーID を外部認証サーバーに送り、返答された信任状に対して、入力された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。

Table 7-1 認証方式

認証方式	識別認証成功前に可能な操作	SFR
本体認証 外部サーバー認証	本体認証におけるユーザー利用停止状態の確認。 ファクス受信。	FIA_UID.1 FIA_UAU.1

認証方式	識別認証成功前に可能な操作	SFR
	TOE の状態確認および表示等の設定。 操作パネルからのファームウェアのバージョンの問い合わせ。	

※ 認証方式の設定は U.ADMIN が行う。本体認証方式と外部サーバー認証方式は両方を同時に有効にすることができる。両方が有効になっている場合、どちらの方式を使用するのかを U.ADMIN が設定する。U.ADMIN が両方の認証方式の使用を可能と設定した利用者は利用者自身が認証時に方式を選択する。

(2) インタフェース

識別認証機能とインタフェースの関係は以下の通りである。

Table 7-2 識別認証機能とインタフェースの関係

インタフェース	操作	
操作パネル	識別認証を必要とする操作	下記の操作以外。 【I/F】認証画面でログイン操作
	識別認証を必要としない操作	本体認証におけるユーザー利用停止状態の確認。 ファクス受信。 ・Table 7-12 Read（ジョブ表示を表示） ・Table 7-13 Read（ジョブ表示を表示） ・Table 7-14 Read（ジョブ表示を表示） ・Table 7-15 Read（ジョブ表示を表示） ・Table 7-16 Read（ジョブ表示を表示） ・Table 7-17 Read（ジョブ表示を表示） TOE の状態確認および表示等の設定。 操作パネルからのファームウェアのバージョンの問い合わせ。
	識別認証（ログイン）後に認証を必要とする操作	強制メモリ受信ボックスへのアクセス。 【I/F】機能選択画面で強制メモリ受信を選択
WC	識別認証を必要とする操作	下記の操作以外。 【I/F】認証画面でログイン操作
	識別認証を必要としない操作	なし。
プリンタドライバー	識別認証を必要とする操作	プリントジョブの投入。 ・Table 7-6 Create ボックスへの文書の保存。 ・Table 7-11 Create 【I/F】プリンタドライバーがインストールされている PC から印刷またはボックス保存を実行
	識別認証を必要としない操作	なし。
ファクス受信	識別認証を必要とする操作	なし。

インタフェース	操作	
	識別認証を必要としない操作	Access Control SFP で許可されているもの。 ・Table 7-10 Create（外部ファクス機からのファクス受信。）

(3) 外部サーバー認証におけるプロトコル

外部サーバー認証において使用するプロトコルは以下の通りである。

TCP/IP (Kerberos V5)

(4) 本体認証における認証失敗時の処理

本体認証において認証が失敗した場合、TOE は以下の処理を行う。

Table 7-3 認証失敗時の処理

対象	処理	SFR
ログインパスワードによる認証の失敗	連続した認証失敗回数が、U.ADMIN が設定した値（1～3）に達した場合認証を停止する。 U.NORMALとしての認証失敗回数とU.USER_ADMINとしての認証失敗回数は積算される。すなわち、ユーザーAがU.NORMALとしてログインしようとして認証に失敗（1回）し、続けて、U.USER_ADMINとしてログインしようとして認証に失敗（1回）した場合、ユーザーAの認証失敗回数は2回となる。 U.ADMIN による設定値の変更によって連続した認証失敗回数が設定値を超えた状態になった場合も認証を停止する。 U.BUILTIN_ADMINの認証が停止した場合はTOEの起動処理を行うことで、起動処理から管理者認証の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。それ以外の場合は、認証停止状態でないU.ADMIN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_AFL.1
ボックスパスワードによる認証の失敗	連続した認証失敗回数が、U.ADMIN が設定した値（1～3）に達した場合認証を停止する。 認証停止状態でない U.ADMIN 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。	

(5) 識別・認証前に許可されるアクション

識別・認証前に許可されるアクションは以下の通りである。

・本体認証におけるユーザー利用停止状態の確認
・ファクス受信
・TOE の状態確認および表示等の設定
・操作パネルからのファームウェアのバージョンの問い合わせ

(6) フィードバック

対話セッションの認証処理（操作パネルからのログイン、WC からのログイン、ファクス受信以外での強制メモリ受信ボックスへのアクセス）においては入力された文字データ 1 文字毎に“＊”または”●”を表示する。

(7) 利用者パスワードおよびボックスパスワードとして使用可能な文字と最小パスワード長

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)であり、最小パスワード長を U.ADMIN が設定することができる。また、最小パスワード長として 15 文字以上の長さを設定することが出来る。

(8) セッションの終了

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。

Table 7-4 対話セッションの終了

対象	セッション終了	備考
操作パネル	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によって決定される時間経過した場合	システムオートリセット時間は工場出荷時に設定されており、管理者が変更可能。 工場出荷時：1 分 設定可能な時間：1～9 分
WC	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によって決定された時間経過した場合	自動ログアウト時間は工場出荷時に設定されており、管理者が変更可能。 ・管理者モード 工場出荷時：10 分 設定可能な時間： 1,2,3,4,5,6,7,8,9,10,20,30,40,50,60 分から選択 ・ユーザーモード 工場出荷時：60 分 設定可能な時間： 1,2,3,4,5,6,7,8,9,10,20,30,40,50,60 分から選択

7.3. アクセス制御機能

－ 対応する機能要件：FDP_ACC.1、FDP_ACF.1

TSF は利用者データおよび利用者データの操作へのアクセス制御を行う。Table 7-5 に示した規則で owner を特定し、利用者データへのアクセスを、識別認証された管理者（U.ADMIN)、および当該利用者データの owner のみに許可することで、利用者データの操作について Table 6-2、Table 6-3 にもとづいたジョブオーナーに基づくアクセス制御を実施する。

D.USER.DOC Access Control SFP に関する TSF インタフェースは Table 7-6～Table 7-11 に示す通りであり、D.USER.JOB Access Control SFP に関する TSF インタフェースは Table 7-12～Table 7-17 に示す通りである。

なお、ジョブの submit は FIA_USB.1 で結合されたアクセス権限に基づいて許可する。

また、許可されない操作についてはインタフェースを非表示、非アクティブにする、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。

Table 7-5 Job function と owner の関係

Job function	Job owner/Fax owner	
Print	プリントジョブの submit はクライアント PC からプリンタドライバーまたは WC のインタフェースを使用しておこなうが、その際、TOE に対して、プリントデータとクレデンシャル(UserID/パスワード)を送る必要がある。 TOE はプリントジョブの submit において送られたクレデンシャルを持つ authorized User を Job owner として扱う。	
Scan	スキャンジョブの submit は操作パネルから実行する。 操作者は操作パネルで識別認証を行い、それに成功したのちスキャンジョブの submit を行う。そこでこのスキャンジョブを submit した authorized User が Job owner となる。	
Copy	コピージョブの submit は操作パネルから実行する。 操作者は操作パネルで識別認証を行い、それに成功したのちコピージョブの submit を行う。そこでこのコピージョブを submit した authorized User が Job owner となる。	
Fax send	ファクス送信ジョブの submit は操作パネルから実行する。 操作者は操作パネルで識別認証を行い、それに成功したのちファクス送信ジョブの submit を行う。そこでこのファクス送信ジョブを submit した authorized User が Job owner となる。	
Fax receive	ファクス受信文書は強制メモリ受信ボックスまたは個人ボックスに保存される。 ボックスと Fax owner の関係は Storage / retrieval の項に記載する。	
	ファクス受信文書の印刷ジョブの owner（= Fax owner）は当該印刷の実行者となる。	
Storage / retrieval	文書は強制メモリ受信ボックス、パスワード暗号化 PDF ボックス、個人ボックスに保存される。	
	強制メモリ受信ボックス	文書の保存はファクス受信から発生する Storage ジョブによって行われる。保存はボックスの情報をクレデンシャルとして実施され、保存された文書の owner はボックスのパスワードを知っている U.NORMAL となる。 なお、ファクス受信、および、ファクス受信により保存された文書の印刷出力は、owner＝Fax owner として D.USER.JOB Access Control SFP (Fax receive)にしたがってアクセス制御する。
	個人ボックス	文書の保存は、F コード指定されたファクス受信から発生する Storage ジョブ、クライアント PC からの文書の送信、操作パネルでのスキャンによる保存、操作パネルおよびクライアント PC からの操作（個人ボックス間での文書の移動、コピー）によって行われる。いずれの場合も保存先のボックスを指定することで、指定されたボックスの owner の情報をクレデンシャルとして保存が実施され、保存された文書の owner は当該文書が保存されているボックスの owner となる。 なお、ファクス受信、および、ファクス受信により保存された文書の印刷出力は、owner＝Fax owner として D.USER.JOB Access Control SFP (Fax receive)にしたがってアクセス制御する。
	パスワード暗号化 PDF ボックス	文書の保存はパスワード暗号化 PDF の保存を実行（クライアント PC の WC からダイレクトプリントを実行）することで行われる。保存された文書の owner は当該文書の印刷もしくは保存を指示した U.NORMAL となる。

Table 7-6 D.USER.DOC Access Control SFP (Print)に関する TSF インタフェース

操作		インタフェース
Create	Submit a document to be printed	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。
		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。

		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。
Read	View image	操作パネルで、認証&プリントボックスから Create 操作により保存された文書を選択して、文書プレビューを表示。
	Release printed output	操作パネルで、認証&プリントボックスから Create 操作により一時保存された文書を選択し、印刷を実行。 印刷完了で当該一時保存された文書は削除される。
		操作パネルで、パスワード暗号化 PDF ボックスから Create 操作により一時保存された文書を選択し、印刷を実行。(パスワード入力が必要)。 印刷完了で当該一時保存された文書は削除される。
Modify	Modify stored document	操作パネルで、認証&プリントボックスから Create 操作により保存された文書を選択し、印刷設定を実行。
Delete	Delete stored document	操作パネルで、認証&プリントボックスから Create 操作により保存された文書を選択し、削除を実行。
		操作パネルで、パスワード暗号化 PDF ボックスから Create 操作により保存された文書を選択し、削除を実行。
		ジョブの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-7 D.USER.DOC Access Control SFP (Scan) に関する TSF インタフェース

操作		インタフェース
Create	Submit a document for scanning	スキャナユニットに原稿をセットして、操作パネルのスキャン/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	View scanned image	なし。
Modify	Modify stored image	Create 操作において、応用設定を実行。
Delete	Delete stored image	ジョブの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-8 D.USER.DOC Access Control SFP (Copy) に関する TSF インタフェース

操作		インタフェース
Create	Submit a document for copying	スキャナユニットに原稿をセットして、操作パネルのコピーメニュー画面からコピーを実行。
Read	View scanned image	なし。
	Release printed copy output	Create 操作を実行。
Modify	Modify stored image	Create 操作で応用設定を実行。
Delete	Delete stored image	ジョブの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-9 D.USER.DOC Access Control SFP (Fax send) に関する TSF インタフェース

操作		インタフェース
Create	Submit a document to send as a fax	スキャナユニットに原稿をセットして、操作パネルのスキャン/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	View scanned image	なし。
Modify	Modify stored image	Create 操作において応用設定を実行。

操作		インタフェース
Delete	Delete stored image	ジョブの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-10 D.USER.DOC Access Control SFP (Fax receive) に関する TSF インタフェース

操作		インタフェース
Create	Receive a fax and store it	外部ファクス機からのファクス送信を実行。（強制メモリ受信ボックスに保存される）
		外部ファクス機からの F コードを指定してファクス送信を実行。（指定された個人ボックスに保存される）
Read	View fax image	操作パネルで、強制メモリ受信ボックスから Create 操作により保存された文書を選択し、文書プレビューを表示。
		クライアント PC の WC で、強制メモリ受信ボックスから Create 操作により保存された文書を選択し、文書プレビューを表示。
		操作パネルで、個人ボックスから Create 操作により保存された文書を選択し、文書プレビューを表示。
		クライアント PC の WC で、個人ボックスから Create 操作により保存された文書を選択し、文書プレビューを表示。
	Release printed fax output	操作パネルで、強制メモリ受信ボックスから Create 操作により保存された文書を選択し、印刷実行を実行。 印刷完了で当該文書は削除される。
		操作パネルで、個人ボックスから Create 操作により保存された文書を選択し、印刷実行を実行。 印刷完了で当該文書は削除される。
Modify	Modify image of received fax	個人ボックスにおける Read 操作(印刷)において、応用設定を実行。
		操作パネルで、個人ボックスから Create 操作により保存された文書を選択し、編集。
		クライアント PC の WC で、個人ボックスから Create 操作により保存された文書を選択し、編集。
Delete	Delete image of received fax	操作パネルで強制メモリ受信ボックスから Create 操作により保存された文書を選択し、削除。
		クライアント PC の WC で強制メモリ受信ボックスから Create 操作により保存された文書を選択し、削除。
		操作パネルで個人ボックスから Create 操作により保存された文書を選択し、削除。
		クライアント PC の WC で個人ボックスから Create 操作により保存された文書を選択し、削除。
		ジョブの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。
		個人ボックスの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-11 D.USER.DOC Access Control SFP (Storage/retrieval) に関する TSF インタフェース

操作		インタフェース
Create	Store	クライアント PC のプリンタドライバーからボックス保存を実行。

操作		インタフェース
	document	クライアント PC の WC からボックス保存を指定してダイレクトプリントを実行。
		クライアント PC の WC から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。
		スキャナユニットに原稿をセットして、操作パネルの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。
		外部ファクス機からのファクス送信を実行。
		外部ファクス機からの F コードを指定してファクス送信を実行。
Read	Retrieve stored document	操作パネルで、個人ボックスから文書を選択し、文書プレビューを表示。
		操作パネルで、個人ボックスから文書を選択し、印刷を実行。
		操作パネルで、個人ボックスから文書を選択し、宛先（ファクス宛先を除く）を指定して、送信を実行。
		操作パネルで、個人ボックスから文書を選択し、ファクス宛先を指定して、送信を実行。
		操作パネルで、個人ボックスから文書を選択し、移動先ボックスを指定して、文書移動を実行。 操作パネルで、個人ボックスから文書を選択し、コピー先ボックスを指定して、文書コピーを実行。
		クライアント PC の WC で、個人ボックスから文書を選択し、文書プレビューを表示。
		クライアント PC の WC で、個人ボックスから文書を選択し、宛先（ファクス宛先を除く）を指定して、送信を実行。
		クライアント PC の WC で、個人ボックスから文書を選択し、ダウンロードを実行。
		クライアント PC の WC で、個人ボックスから文書を選択し、移動先ボックスを指定して、文書移動を実行。 クライアント PC の WC で個人ボックスから文書を選択し、コピー先ボックスを指定して、文書コピーを実行。 クライアント PC の WC で強制メモリ受信ボックスから Create 操作により保存された文書を選択し、ダウンロードを実行。
		操作パネルで、パスワード暗号化 PDF ボックスから Create 操作により一時保存された文書を選択し、保存を実行。(パスワード入力が必要)。 保存完了で当該一時保存された文書は削除される。
Modify	Modify stored document	操作パネルで個人ボックスから文書を選択し、編集。
		Read 操作(送信、印刷)において、応用設定を実行。
		クライアント PC の WC で、個人ボックスから文書を選択し、編集。 操作パネルで強制メモリ受信ボックスから文書を選択し、編集。
Delete	Delete stored document	操作パネルで強制メモリ受信ボックスから Create 操作により保存された文書を選択し、削除を実行。
		クライアント PC の WC で強制メモリ受信ボックスから Create 操作により保存された文書を選択し、削除を実行。
		操作パネルで個人ボックスから Create 操作により保存された文書を選択し、削除を実行。
		クライアント PC の WC で個人ボックスから Create 操作により保存された文書を選択し、削除を実行。
		操作パネルでパスワード暗号化 PDF ボックスから Create 操作により保存された文書を選択し、削除を実行。

操作		インタフェース
		個人ボックスの削除（操作パネル、クライアント PC の WC から実行）に連動した削除。

Table 7-12 D.USER.JOB Access Control SFP (Print) に関する TSF インタフェース

操作		インタフェース
Create	Create print job	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。 印刷完了により当該一時保存された文書も削除される。
		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。 印刷完了により当該一時保存された文書も削除される。
		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。(パスワード入力が必要)。 印刷完了により当該一時保存された文書も削除される。
Read	View print queue / log	操作パネルでジョブ表示を表示。(パスワード暗号化 PDF の受信中ジョブを除く)。
		WC でユーザーログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
		操作パネルで管理者ログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
		WC で管理者ログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
Modify	Modify print job	なし。
Delete	Cancel print job	操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 認証&プリントボックスの場合、当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 認証&プリントボックスの場合、当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		操作パネルで管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 認証&プリントボックスの場合、当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 認証&プリントボックスの場合、当該ジョブに含まれる文書（D.USER.DOC）も削除される。

Table 7-13 D.USER.JOB Access Control SFP (Scan) に関する TSF インタフェース

操作		インタフェース
Create	Create	スキャナユニットに原稿をセットして、操作パネルのスキャン/ファクスメニュー画面

操作		インタフェース
	scan job	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	View scan status / log	操作パネルでジョブ表示を表示。
		WC でユーザーログイン後にジョブ表示を表示。
		操作パネルで管理者ログイン後にジョブ表示を表示。
		WC で管理者ログイン後にジョブ表示を表示。
Modify	Modify scan job	なし。
Delete	Cancel scan job	Create 操作を実行した後、スキャナユニットにより原稿読み取り中に、操作パネルの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。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、操作パネルで管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。

Table 7-14 D.USER.JOB Access Control SFP (Copy) に関する TSF インタフェース

操作		インタフェース
Create	Create copy job	スキャナユニットに原稿をセットして、操作パネルのコピーメニュー画面からコピーを実行。
Read	View copy status / log	操作パネルでジョブ表示を表示。
		WC でユーザーログイン後にジョブ表示を表示。
		操作パネルで管理者ログイン後にジョブ表示を表示。
		WC で管理者ログイン後にジョブ表示を表示。
Modify	Modify copy job	なし。
Delete	Cancel copy job	Create 操作後、スキャナユニットにより原稿読み取り中に、操作パネルの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。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。 WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、操作パネルで管理者ログイン後、ジョブ表示から Create 操作で

操作		インタフェース
		作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。

Table 7-15 D.USER.JOB Access Control SFP (Fax send) に関する TSF インタフェース

操作		インタフェース
Create	Create fax send job	スキャナユニットに原稿をセットして、操作パネルのスキャン/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	View fax job queue / log	操作パネルでジョブ表示を表示。
		WC でユーザーログイン後にジョブ表示を表示。
		操作パネルで管理者ログイン後にジョブ表示を表示。
		WC で管理者ログイン後にジョブ表示を表示。
Modify	Modify fax send job	不可
Delete	Cancel fax send job	Create 操作を実行した後、スキャナユニットにより原稿読み取り中に、操作パネルの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。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、操作パネルで管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。
		Create 操作を実行後、クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。 当該ジョブに含まれる文書（D.USER.DOC）も削除される。

Table 7-16 D.USER.JOB Access Control SFP (Fax receive) に関する TSF インタフェース

操作		インタフェース
Create	Create fax receive job	外部ファクス機からのファクス送信を実行後、TOE の操作パネルで強制メモリ受信ボックスからファクス受信文書を選択し、印刷実行を実行。
		外部ファクス機からの F コードを指定してファクス送信を実行後、TOE の操作パネルで個人ボックスからファクス受信文書を選択し、印刷を実行。
Read	View fax receive status / log	操作パネルでジョブ表示を表示。
		WC でユーザーログイン後にジョブ表示を表示。
		操作パネルで管理者ログイン後にジョブ表示を表示。
		WC で管理者ログイン後にジョブ表示を表示。
Modify	Modify fax	なし。

操作		インタフェース
	receive job	
Delete	Cancel fax receive job	操作パネルで管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。
		クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。
		操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。
		WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。

Table 7-17 D.USER.JOB Access Control SFP (Storage/retrieval) に関する TSF インタフェース

操作		インタフェース
Create	Create storage job	クライアント PC のプリンタドライバーからボックス保存を実行。
		クライアント PC の WC から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、操作パネルの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、クライアント PC の WC からパスワード暗号化 PDF のダイレクトプリントを実行。
		外部ファクス機からのファクス送信を実行。
		外部ファクス機からの F コードを指定してファクスによる送信を実行。
	Create retrieval job	操作パネルで、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、コピーを実行。(ファクス受信文書の印刷を除く。これは Table 7-16 の Create fax receive job であり、D.USER.JOB Access Control SFP (Fax receive)によるアクセス制御の対象となる。)
		クライアント PC の WC で、個人ボックスから文書を選択し、送信、ダウンロード、移動、コピーを実行。
		クライアント PC の WC で、強制メモリ受信ボックスからファクス受信文書を選択し、ダウンロードを実行。
		操作パネルで、パスワード暗号化 PDF ボックスから Create 操作で一時保存した文書を選択し、保存を実行。(パスワード入力が必要)。 保存完了により当該一時保存された文書も削除される。
Read	View storage/retrieval log	操作パネルでジョブ表示を表示。(パスワード暗号化 PDF の受信中ジョブを除く)。
		WC でユーザーログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
		操作パネルで管理者ログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
		WC で管理者ログイン後にジョブ表示を表示。 (パスワード暗号化 PDF の受信中ジョブを除く)。
Modify	Modify storage/retrieval job	なし。
Delete	Cancel storage job	スキャナユニットにより原稿読み取り中に、操作パネルの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。

操作		インタフェース
		文書（D.USER.DOC）は保存されない。
	Cancel retrieval job	Create retrieval job（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。 印刷対象として選択された文書（D.USER.DOC）は削除されない。
	Cancel storage/retrieval job	操作パネルでユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。
		WC でユーザーログイン後、ジョブ表示から、自身が Create 操作で作成したジョブを削除。
		操作パネルで管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。
		クライアント PC の WC から管理者ログイン後、ジョブ表示から Create 操作で作成されたジョブの削除を実行。

7.4. セキュリティ管理機能

－ 対応する機能要件：FDP_ACF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMR.1、FMT_MOF.1、FMT_SMF.1

管理機能は以下の通りである。

本件に関する TSF インタフェースは FAU_GEN.1、FAU_GEN.2（管理機能の実行のインタフェース）に準ずる。

(1) ユーザー管理機能

U.ADMIN は操作パネルおよびクライアント PC の WC から TOE へのユーザーの登録､削除、変更、一時利用停止、一時利用停止の解除、アクセス権限の付与／Delete、役割（U.USER_ADMIN）の付与／Delete を行うことができる。

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。

(2) TSF データの管理機能

Table 6-8 の通り TSF データを管理する機能を提供する。

(3) 役割の維持

TOE はログイン時に結合された U.ADMIN, U.NORMAL の役割を維持する。

(4) セキュリティ機能のふるまいの管理機能

TOE は以下の機能を U.ADMIN のみに提供する。

Table 7-18 セキュリティ機能のふるまいの管理機能

機能	インタフェース		
		クライアント PC	
	操作パネル	プリンタドライバー	WC
セキュリティ強化設定の管理機能	○	×	○
ユーザー認証機能の管理機能	○	×	○

機能	インタフェース		
		クライアント PC	
	操作パネル	プリンタドライバー	WC
監査ログ管理機能	○	×	○
高信頼チャネル管理機能	○	×	○

(5) ボックス管理機能

U.ADMIN は個人ボックスの User ID を変更することができる。また、個人ボックスの owner は当該個人ボックスの User ID を変更することができる。TOE は User ID によってそのボックスの owner を特定することから、この変更はボックス（および当該ボックス内の文書）の owner の変更を意味する。

U.ADMIN および U.ADMIN によって許可された U.NORMAL は個人ボックスを生成することができる。

U.ADMIN は個人ボックスを削除することができる。また、個人ボックスの owner は当該個人ボックスを削除することができる。ボックスの削除により、当該ボックス内の文書も削除される。

U.ADMIN は強制メモリ受信ボックスのパスワードの登録と変更を行うことができる。

(6) D.USER.DOC、D.USER.Job の属性

D.USER.DOC、D.USER.Job に対して、その生成時に Table 6-7 にしたがって属性（Job owner、Fax owner）を付与する。属性（Job owner、Fax owner）とインタフェースの関係は Table 7-5 で記述した。

7.5. 高信頼な運用機能：アップデート機能

－ 対応する機能要件：FPT_TUD_EXT.1、FCS_COP.1(b)、FCS_COP.1(c)

(1) ファームウェアバージョン確認機能

許可された管理者は、以下の方法でファームウェアバージョンの確認を行うことが出来る。

・クライアント PC の WC でログインし、メンテナンス＞ROM バージョンを選択する。

・操作パネルでログインし、メンテナンス＞ROM バージョンを選択する。

(2) ファームウェアアップデート機能

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。
(1)(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。

7.6. 高信頼な運用機能：自己テスト機能

－ 対応する機能要件：FPT_TST_EXT.1

TOE は、電源 ON 時に、以下の表に示したテストをこの順番に実施し、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 7-19 自己テスト

No.	対象	テスト
1	コントローラファームウェア、その他のファームウェア	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。
2	ファームウェア内のライブラリソフトウェア（SHA,HMAC 等）	Power-up Self-test
3	ファームウェア内のライブラリソフトウェア(DRBG)	エントロピー源として haveged 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。

7.7. 高信頼通信機能

－ 対応する機能要件：FPT_SKP_EXT.1、FTP_ITC.1、FTP_TRP.1(a)、FTP_TRP.1(b)、FCS_CKM.1(a)、FCS_CKM.1(b) 、 FCS_CKM_EXT.4 、 FCS_CKM.4 、 FCS_COP.1(a) 、 FCS_COP.1(b) 、 FCS_COP.1(c) 、 FCS_COP.1(g) 、 FCS_RBG_EXT.1 、 FCS_IPSEC_EXT.1、FIA_PSK_EXT.1

TOE は管理者のみに以下の機能を提供する。

(1) FPT_SKP_EXT.1
TOE の通信保護機能で使用するすべての事前共有鍵、対称鍵、及びプライベート鍵は RAM(揮発メモリ)及び SSD に保存される。これらをアクセスするインタフェースは存在しない。また、RAM(揮発メモリ)に保存される鍵についてもアクセスするインタフェースは存在しない。

Table 7-20 鍵と保存先の関係

No.	対象		保存先
1	事前共有鍵	U.ADMIN によって設定された事前共有鍵	SSD
		U.ADMIN 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
2	対称鍵	IKE 用共有秘密鍵 （IKEv1 フェーズ 1 で生成される）	RAM
		IPsec 用共有秘密鍵 （IKEv1 フェーズ 2 で生成される）	RAM
3	プライベート鍵	IPsec 証明書のプライベート鍵	SSD
		IPsec 通信における鍵確立で用いるプライベート鍵 （IKEv1 フェーズ 1 で生成される）	RAM

(2) FCS_CKM.1(b), FCS_RBG_EXT.1, FCS_COP.1(a)

TOE は暗号化アルゴリズムに 128bit 及び 256bit の AES-CBC を使用した通信の暗号化を行う。使用する暗号鍵（128bit 及び 256bit）は、ファームウェア内のライブラリソフトウェア(DRBG)の乱数生成関数（FCS_RBG_EXT.1）で生成した 128bit の乱数を利用して生成する。

この時乱数生成器が利用するエントロピーの詳細については 7.1 章を参照。

(3) FCS_CKM.4, FCS_CKM_EXT.4

鍵が不要となったタイミングと破棄のタイミングは同じである。

Table 7-21 鍵の破棄

鍵		破棄タイミング	破棄の方法
事前共有鍵	U.ADMIN によって設定された事前共有鍵	管理者による事前共有鍵削除・変更（高信頼チャネル管理機能）時	0x00 で上書き削除
	U.ADMIN によって設定された事前共有鍵を変換して生成した鍵	電源 OFF	—
対称鍵	IKE 用共有秘密鍵	電源 OFF	—
		IKE SA ライフタイム経過後	メモリの解放
		管理者による IP アドレス変更時	メモリの解放
	IPsec 用共有秘密鍵	電源 OFF	—
		IPsec SA ライフタイム経過後	メモリの解放
		管理者による IP アドレス変更時	メモリの解放
プライベート鍵	IPsec 証明書のプライベート鍵	管理者による証明書削除（高信頼チャネル管理機能）時	0x00 で上書き削除
	IPsec 通信における鍵確立で用いるプライベート鍵	電源 OFF	—

(4) FTP_TRP.1(a), FTP_TRP.1(b)

TOE は他の高信頼 IT 機器との通信において暗号化通信を行う。暗号化通信の対象となる機能は以下のとおりである。

Table 7-22 管理者が利用できる高信頼パス(FTP_TRP.1(a))

通信先	内容	プロトコル
クライアント PC	remote administrators はクライアント PC から TOE との対話セッションを確立して管理作業を行うが、その場合の通信は本表に示したプロトコルを使用して行われる。	IPsec

Table 7-23 一般利用者が利用できる高信頼パス(FTP_TRP.1(b))

通信先	内容	プロトコル
クライアント PC	authorized remote users はクライアント PC から TOE にプリントジョブの投入を行う他、クライアント PC から TOE との対話セッションを確立して操作を行うが、それらの通信は本表に示したプロトコルを使用して行われる。	IPsec

(5) FTP_ITC.1

TOE は他の高信頼 IT 機器との通信において暗号化通信を行う。暗号化通信の対象となる機能は以下のとおりである。

Table 7-24 通信で使用するプロトコル

通信先	プロトコル
外部認証サーバー	IPsec
SMTP サーバー	IPsec
DNS サーバー	IPsec
WebDAV サーバー	IPsec
SMB サーバー	IPsec
ログサーバー	IPsec

(6) FCS_CKM.1(a)

TSF は、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 RSA 鍵を生成し、IPsec 証明書(RSA)の生成を行うことができる。生成した IPsec 証明書のプライベート鍵は、SSD に保存される。

また、暗号通信における鍵確立で用いる非対称鍵の生成は、NIST SP800-56A, Revision 3 の 5.6.1.1.1 節に記載の Using the Approved Safe-Prime Groups に適合した方法で行う。

(7) FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g)

TOE が使用する IPsec プロトコルでは下記の設定が利用可能であり他の設定は利用できない。複数記載があるものは管理者が選択できる項目であり、この選択は管理者のみが設定・変更できる。

- 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
  - ESP 暗号化アルゴリズム：AES-CBC-128、AES-CBC-256

- 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
  - IKEv1 暗号化アルゴリズム：AES-CBC-128、AES-CBC-256
  - 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

- 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
  - テキストベースの事前共有鍵
    - U.ADMIN が設定する事前共有鍵：2～128 文字の文字列(ASCII)または HEX 値
    - 認証アルゴリズム：SHA-1、SHA-256、SHA-384、SHA-512

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。IP パケットの条件としては TCP や UDP 等のプロトコル、ポート、送信元 IP アドレス、送信先 IP アドレス等が設定できる。IPsec ポリシーは IP ポリシーグループ 1~10 の 10 グループまで設定することができ、番号が小さいグループの設定が優先的に適応される。
- 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、破棄を選択する様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

7.8. 監査機能

－ 対応する機能要件：FPT_STM.1、FAU_GEN.1、FAU_GEN.2、FAU_STG_EXT.1

TOE は以下の機能を提供する。

(1) 監査ログ取得機能

TOE は、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 7-25 事象と監査ログ

インタフェース	監査対象事象	ID(*1)	結果

インタフェース		監査対象事象		ID(*1)	結果
操作パネル	セキュリティー＞ジョブログ設定＞ジョブログ使用設定＞使用設定(ジョブログの取得を ON に設定する。以後は、電源 ON でも開始される。)	監査ログ取得機能の開始	a	Admin ID	OK
WC	セキュリティー＞ジョブログ設定＞ジョブログ使用設定＞使用設定(ジョブログの取得を ON に設定する。以後は、電源 ON でも開始される。)				
操作パネル	セキュリティー＞ジョブログ設定＞ジョブログ使用設定＞使用設定（ジョブログの取得を ON に設定されている時、電源 OFF する。もしくは、ジョブログの取得を OFF に設定する。）	監査ログ取得機能の終了		Admin ID	OK
WC	セキュリティー＞ジョブログ設定＞ジョブログ使用設定＞使用設定（ジョブログの取得を ON に設定されている時、電源 OFF する。もしくは、ジョブログの取得を OFF に設定する。）				
操作パネル	管理者モードの場合 ホームキー＞設定メニュー＞管理者設定　からログイン	ユーザー認証の実施	b c	Admin ID /User ID/ 未登録 ID	OK/NG
	ユーザーログインの場合 初期画面から下記設定でログイン 操作権限=ユーザー				
WC	管理者モードの場合 初期画面から下記設定でログイン ユーザー種別=管理者				
	ユーザーログインの場合 初期画面から下記設定でログイン ユーザー種別=登録ユーザー 管理者権限でログイン=OFF				
プリンタドライバー	印刷の実行 ボックス保存の実行				
操作パネル	ボックスパスワードによる認証の場合 ボックス＞システム＞強制メモリ			User ID	

インタフェース		監査対象事象		ID(*1)	結果
	受信				
WC	ボックスパスワードによる認証の場合 ボックス＞システムボックスを開く＞強制メモリ受信ボックス				
操作パネル	セキュリティー＞セキュリティー強化設定	U.ADMIN によるセキュリティ強化設定の管理機能	d	Admin ID	OK
WC	セキュリティー＞セキュリティー強化設定				
操作パネル	ユーザー認証設定＞ユーザー登録	U.ADMIN によるユーザー管理機能		Admin ID	OK/NG
WC	ユーザー認証設定＞ユーザー登録				
操作パネル	ユーザー認証/部門管理＞認証方式	U.ADMIN によるユーザー認証機能の管理機能		Admin ID	OK
WC	ユーザー認証/部門管理＞認証方式				
操作パネル	ユーザー認証/部門管理＞外部サーバー設定	U.ADMIN による外部サーバー認証設定データの登録・変更機能		Admin ID	OK
WC	ユーザー認証/部門管理＞外部サーバー設定				
操作パネル	ネットワーク＞TCP/IP 設定＞IPsec （事前共有鍵の登録、変更、削除はこのインタフェースから実行する）	U.ADMIN による高信頼チャネル管理機能		Admin ID	OK/NG
WC	ネットワーク>TCP/IP 設定>IPsec （事前共有鍵の登録、変更、削除はこのインタフェースから実行する）				
WC	セキュリティー＞PKI 設定＞デバイス証明書設定＞デバイス証明書一覧 （証明書の登録、削除はこのインタフェースから実行する）			Admin ID	OK
操作パネル	ネットワーク	U.ADMIN によるネットワーク設定の登録・変更機能		Admin ID	OK/NG
WC	ネットワーク				
操作パネル	セキュリティー＞ジョブログ設定	U.ADMIN による監査ログ管理機能		Admin ID	OK
WC	セキュリティー＞ジョブログ設定				
操作パネル	環境設定＞リセット設定＞システムオートリセット	U.ADMIN によるシステムオートリセット時間の変更		Admin ID	OK

インタフェース		監査対象事象	ID(*1)	結果
WC	環境設定＞リセット設定＞システムオートリセット	機能		
WC	セキュリティー＞自動ログアウト	U.ADMIN による自動ログアウト時間の変更機能	Admin ID	OK
操作パネル	セキュリティー＞セキュリティー詳細＞認証操作禁止機能	U.ADMIN による管理者認証の操作禁止解除時間の変更機能	Admin ID	OK
WC	セキュリティー＞セキュリティー詳細＞認証操作禁止機能			
操作パネル	セキュリティー＞セキュリティー詳細＞パスワード規約	U.ADMIN によるパスワード規約変更機能	Admin ID	OK/NG
WC	セキュリティー＞セキュリティー詳細＞パスワード規約			
操作パネル	セキュリティー＞セキュリティー詳細＞認証操作禁止機能	U.ADMIN による認証失敗回数閾値の変更機能	Admin ID	OK
WC	セキュリティー＞セキュリティー詳細＞認証操作禁止機能			
操作パネル	セキュリティー＞セキュリティー詳細＞認証操作禁止機能	U.ADMIN による認証失敗回数（U.BUILTIN_ADMIN 以外）のクリア機能	Admin ID	OK
WC	セキュリティー＞セキュリティー詳細＞認証操作禁止機能			
操作パネル	・ユーザーログイン＞ホームキー＞設定メニュー＞ユーティリティ＞ボックス＞ボックス一覧 ・ユーザーログイン＞ボックス＞個人	U.NORMAL によるボックス管理機能	User ID	OK/NG
WC	ユーザーログイン＞ボックス＞ボックス一覧			
操作パネル	セキュリティー＞ボックス機能制限	U.ADMIN によるボックス管理機能	Admin ID	OK/NG
	管理者モード＞ホームキー＞設定メニュー＞ボックス＞ボックス一覧			
WC	セキュリティー＞ボックス機能制限			
	管理者モード＞ボックス＞ボックス一覧			
操作パネル	情報表示＞ユーザーパスワード変更	U.NORMAL による自身のログインパスワードの変更機能	User ID	OK
WC	情報表示＞ユーザーパスワード変更			OK/NG

インタフェース		監査対象事象		ID(*1)	結果
操作パネル	セキュリティー＞管理者パスワード設定	U.BUILTIN_ADMIN による自身のログインパスワードの変更機能		Admin ID	OK
Table 7-6～Table 7-17 参照		プリントジョブの保存	e	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
操作パネル	メンテナンス＞日時設定	U.ADMIN による時刻情報の変更機能	d f	Admin ID	OK
WC	メンテナンス＞日時設定				
		IPsec セッション確立の失敗	g h	システム ID	errNo (*2)

(a) Start-up and shutdown of the audit functions
(b) Unsuccessful User authentication
(c) Unsuccessful User identification
(d) Use of management functions
(e) Job completion
(f) Changes to the time
(g) Failure to establish session
(h) Failure to establish an IPsec SA
(*1) サブジェクト識別情報。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。

Table 7-26 インタフェースの補足

インタフェース	詳細	
管理者モード	操作パネル	ホームキー＞設定メニュー＞管理者設定　で管理者パスワードを入力して

インタフェース	詳細	
		ログイン（U.BUILTIN_ADMIN）
		初期画面の操作権限で管理者を選択し、User ID とパスワードを入力してログイン（U.USER_ADMIN）
	WC	初期画面のユーザー種類で管理者を選択し、管理者パスワードを入力してログイン（U.BUILTIN_ADMIN）
		初期画面のユーザー種類で登録ユーザーを選択し、管理者権限でログインをチェックし、管理者を選択し、User ID とパスワードを入力してログイン（U.USER_ADMIN）
ユーザーログイン	操作パネル	初期画面の操作権限でユーザーを選択し、User ID とパスワードを入力してログイン(U.NORMAL)
	WC	初期画面のユーザー種類で登録ユーザーを選択し、User ID とパスワードを入力してログイン(U.NORMAL)
	プリンタドライバー	User ID とパスワードを入力して印刷を実行。 User ID とパスワードを入力してボックス保存を実行。 User ID とパスワードは以下の画面で入力。 基本設定＞ユーザー認証/部門管理設定＞ユーザー認証＞登録ユーザー
ボックスパスワードによる認証	操作パネル	以下の画面でパスワードを入力。 ボックス＞システム＞強制メモリ受信
	WC	以下の画面でパスワードを入力。 ボックス＞システムボックスを開く＞強制メモリ受信ボックス
セキュリティー	操作パネル	管理者モード＞セキュリティー
	WC	管理者モード＞セキュリティー
ユーザー認証/ 部門管理	操作パネル	管理者モード＞ユーザー認証/ 部門管理
	WC	管理者モード＞ユーザー認証/ 部門管理
ユーザー認証設定	操作パネル	管理者モード＞ユーザー認証/ 部門管理＞ユーザー認証設定
	WC	管理者モード＞ユーザー認証/ 部門管理＞ユーザー認証設定
ネットワーク	操作パネル	管理者モード＞ネットワーク
	WC	管理者モード＞ネットワーク
環境設定	操作パネル	管理者モード＞環境設定
	WC	管理者モード＞環境設定
情報表示	操作パネル	ユーザーログイン＞ホームキー＞設定メニュー＞ユーティリティ＞情報表示
	WC	ユーザーログイン＞情報表示
メンテナンス	操作パネル	管理者モード＞メンテナンス
	WC	管理者モード＞メンテナンス

(2) 監査ログ格納機能

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、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。日時および蓄積量の設定は管理者が行う。

ログサーバーへのログ情報の送信は通信保護機能を利用して行う。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 データを参照したり変更したりする機能は存在しない。

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（操作パネルのみ、管理者認証のみ）
・U.ADMIN による監査ログ管理機能（監査ログ送信および削除）

U.ADMIN 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 7-27 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。

(3) 高信頼タイムスタンプ機能

TOE はクロック機能を有し、U.ADMIN に対して TOE の時刻を変更する機能を提供する。時刻情報の変更は FMT_SMF.1 により U.ADMIN のみが可能である。TOE はクロック機能によるタイムスタンプを監査ログ生成時に発行し、監査ログとして記録する。

7.9. FAX 分離機能

－ 対応する機能要件：FDP_FXS_EXT.1

TSF は、ファクスプロトコルを用いて利用者データを送信または受信する以外で、ファクス I/F を経由した通信を禁止する。これにより、TOE のファクス I/F が、TOE が接続している PSTN とネットワークとの間のネットワークブリッジを作成するために使用されるのを防止する。

また、TOE のファクス I/F は、ファクスの送信および受信のみに使用され、他の目的では使用できない。

TOE が提供するファクスモデムの機能は、ファクス送信およびファクス受信のみであり、Super G3 プロトコルおよび G3 プロトコルをサポートする。

以上