KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 with UK-112 Security Target

Version 1.17

2021/04/02

コニカミノルタ株式会社

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2020/11/04	1.00	第1PPサービス開発部	羽賀	芳野	安加賀	初版
2020/11/20	1.01	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2020/11/27	1.02	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2020/12/08	1.03	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2020/12/22	1.04	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2020/12/24	1.05	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/01/06	1.06	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/01/18	1.07	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/01/25	1.08	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/02	1.09	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/04	1.10	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/08	1.11	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/10	1.12	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/17	1.13	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/02/26	1.14	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/03/08	1.15	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/03/18	1.16	第1PPサービス開発部	羽賀	芳野	安加賀	誤記の修正
2021/04/02	1.17	PPシステム制御開発部	羽賀	芳野	安加賀	誤記の修正

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

—【 図目次 】

—【 表目次 】

1. ST introduction

1.1. ST reference

・ST名称　：KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 with UK-112 Security Target
・STバージョン　：1.17
・作成日　：2021年04月02日
・作成者　：コニカミノルタ株式会社

1.2. TOE reference

・TOE名称　：KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 with UK-112
・バージョン　：GM2-20

上記 TOE は、本体(KONICA MINOLTA AccurioPress C4080, KONICA MINOLTA AccurioPress C4070, KONICA MINOLTA AccurioPrint C4065 のいずれか、ファームウェアバージョン GM2-20)及び必須オプションである HDD ユニット(商品名 UK-112)から構成される。TOE のバージョン GM2-20 は、ファームウェアを識別するための情報である Table1-3 に記載のファームウェア種類とバージョン名の組合せにより構成される。なお、KONICA MINOLTA AccurioPrint C4065 は日本国内では販売しない(KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 は日本国内及び海外で購入できる)。

1.3. TOE overview

本TOEは、基本的に中程度の文書セキュリティ、ネットワークセキュリティ、情報保証が要求される商用情報処理環境で使用されるデジタル複合機（以下、MFPと称する）である。この環境では通常、日常の企業運営で扱う機密／非機密情報が処理される。

1.3.1. TOE の種別

TOE はネットワーク環境(LAN)で使用される MFP であり、コピー機能、スキャン機能、ドキュメントの保存と取り出しを行う機能を有する。なお、本 TOE にはファクス機能、及び PC からプリントジョブを印刷及び保存する機能は搭載していない。

1.3.2. 使用法と主要なセキュリティ機能

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

利用者を特定し、許可利用者のみ TOE の利用を許可する識別認証機能、利用者に与えられた権限に従って文書へのアクセスや TOE の各種操作を制限するアクセス制御機能、セキュリティ機能の設定を管理者の権限を持つ利用者に制限するセキュリティ管理機能、セキュリティ関連の事象を記録し、ログサーバーへ送信する監査機能、TOE と外部 IT 機器との通信を IPsec によって保護する高信頼通信機能、HDD・SSD に記録されているデータを暗号化するストレージ暗号化機能、不正ファームウェアによるアップデートを防止するアップデートデータ検証機能と TSF の正常動作を実証する自己テスト機能。

1.3.3. 運用環境

TOE の運用環境を Figure1-1 に示す。TOE は LAN 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。

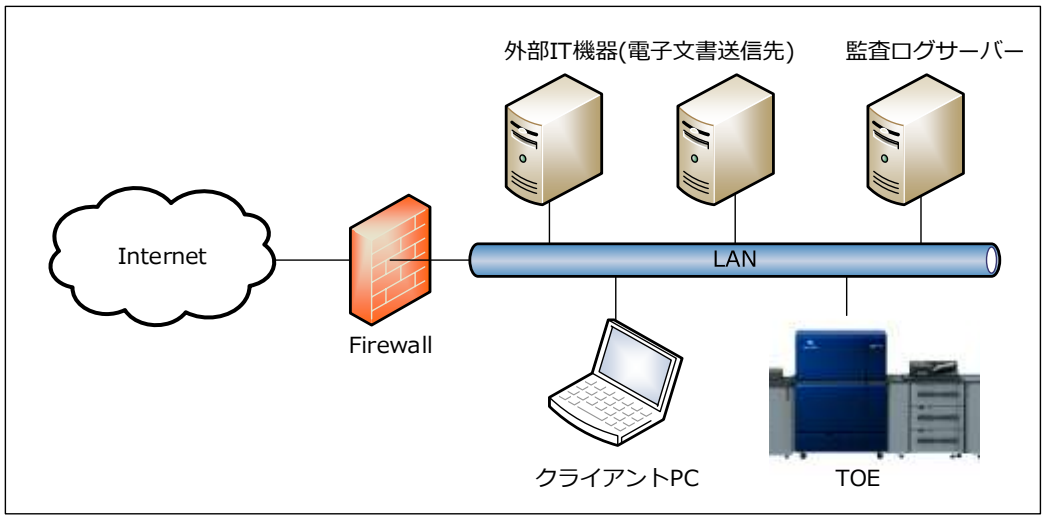


Figure 1-1 TOE の利用環境

(1) TOE(MFP 本体)
TOE はオフィス内 LAN に接続される。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。

- TOE の各種設定
- 紙文書のコピー・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・削除

(2) LAN
TOE の設置環境で利用されるネットワーク。

(3) 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。

(4) クライアント PC
web ブラウザソフトを利用して、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。

- Web Connection（管理者認証後、ブラウザ上で TOE のファームウェアバージョンを確認できる）

(5) 監査ログサーバー
TOE の監査機能の送信先となるサーバー。利用者は監査ログ情報の送信先として syslog サーバーを指定できる。

(6) 外部 IT 機器（電子文書送信先）
電子文書の送信先となる外部 IT 機器。利用者は WebDAV サーバー、SMB サーバー、FTP サーバーを送信先として指定できる。

1.3.4. TOE に必要な TOE 以外のハードウェア／ソフトウェア

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

Table 1-1 評価構成

ハードウェア/ソフトウェア		評価で使用したバージョン等
クライアントPC(OS)		Windows 10 Pro
	Webブラウザ	Microsoft Internet Explorer 11
	IPsec	OS内蔵
監査ログサーバー		rsyslog 8.1901.0
	IPsec	strongswan 5.8.0
FTPサーバー		vsftpd 3.0.3
	IPsec	strongswan 5.8.0
WebDAVサーバー		apache2 2.4.38
	IPsec	strongswan 5.8.0
SMBサーバー		samba 4.9.5
	IPsec	strongswan 5.8.0

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

1.4.1.1. TOE の物理的構成

TOE の物理的範囲は以下の図に示すように、操作パネル、スキャナーユニット、プリンタユニット、制御基板、HDD・SSD、USB I/F、Network I/F から構成される MFP である。

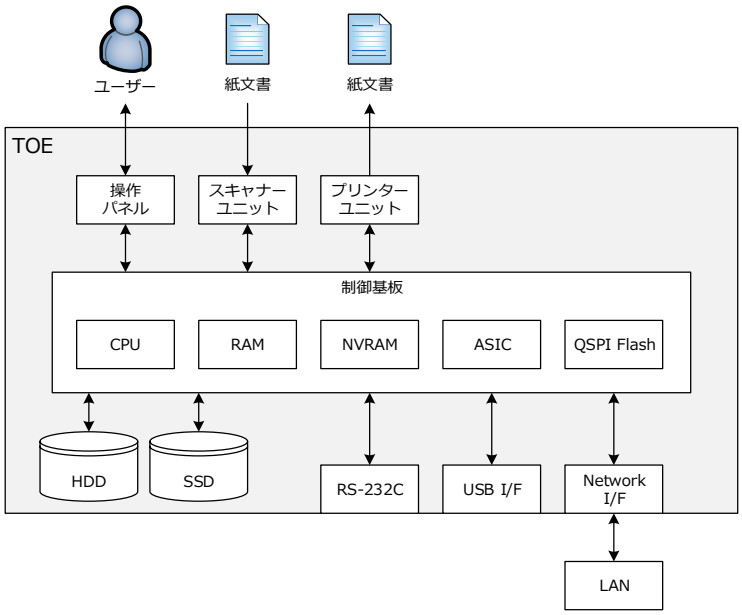


Figure 1-2 TOE の物理的範囲

Table 1-2 構成

No.	Function	Definition
1	操作パネル	タッチパネル液晶ディスプレイとスタートキー、ストップキーなどのハードウェアキーを備えた TOE を操作するためのデバイス。
2	スキャナーユニット	紙から図形、写真を読み取り、電子データに変換するためのデバイス。
3	プリンターユニット	制御基板からの指示により、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。
4	制御基板	TOE 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性メモリ。
7	ASIC	画像データの圧縮展開機能を実装した特定利用目的集積回路。
8	NVRAM	TOE の動作を決定する設定データや TSF データが保存される不揮発性メモリ。
9	QSPI Flash	暗号鍵（KEK）の鍵材料が保存される半導体記憶装置。可搬記憶媒体ではない。本装置は基板上に直付けされており着脱することはできない。
10	HDD・SSD	可搬記憶媒体として、画像データや一時画像データの保存、および作業領域などに利用される。
11	RS-232C I/F	シリアル接続することが可能なインターフェース。公衆回線と接続されるモデムと接続して遠隔診断機能(CS Remote Care)に利用できるが、TOE においては使用が禁止される。
12	Network I/F	10BASE-T、100BASE-TX、Gigabit Ethernet をサポートするインターフェース。
13	USB I/F	キーボードやマウスといった操作デバイス及び USB メモリを接続しファームウェアの書き換えや画像データの保存・取り出しを行う USB インターフェース。ただし、TOE においては USB デバイスの使用は禁止される（ファームウェアアップデート機能における USB メモリの使用を除く）。

1.4.1.2. TOE のファームウェア構成

TOE のファームウェア構成要素を以下に示す。

Table 1-3 TOE のファームウェア構成

ファームウェア種類	ROM 種別	Definition	バージョン名(GM2-20 構成 FW)
画像制御系/1	I1	画像制御処理及び操作部制御	AC570Y0-00I1-GM2-20
画像制御系/2	I2	同上	AC570Y0-00I2-G00-20
画像制御系/3	I3	同上	AC570Y0-00I3-G00-20
画像制御系/4	I4	同上	AC570Y0-00I4-GM2-20
画像制御系/5	I5	同上	AC570Y0-00I5-GM2-20
ADF 系	F	原稿自動送り装置制御	AAMP0Y0-00F1-G00-03
音源系	T	操作部音声データ	AC570Y0-00T1-G00-10
ブラウザー	W	ブラウザ処理	AC570Y0-00W1-G00-20
スキャナー	L	スキャナー基板処理	AC570Y0-00L1-G00-10
プリンター系	C	プリント制御	AC570Y0-00C1-G00-20
ネットワーク制御	P9	ネットワーク制御処理	AC570Y0-00P9-GM2-20
プリンターサブ CPU	D	プリント基板制御	AC570Y0-00D1-G00-1000

1.4.1.3. ガイダンス

以下にガイダンスの一覧を示す。一般ユーザー向けのガイダンス(ユーザーズガイド)は html ファイルの形式で販売会社からユーザーにマニュアルの参照先 URL を連絡し提供を行う。また、セキュリティ機能のガイダンス(ユーザーズガイド セキュリティー機能編)は exe ファイルの形式で、販売会社からユーザーに可搬記憶媒体を用いて提供を行う。

Table 1-4 ガイダンス一覧

名称	Ver.	補足
KONICA MINOLTA AccurioPress C4080/C4070 ユーザーズガイド	02.10.00	日本語版
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 ユーザーズガイド セキュリティー機能編(管理者)	1.0 (2021-04-02)	日本語版
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 ユーザーズガイド セキュリティー機能編(ユーザー)	1.0 (2021-04-02)	日本語版
KONICA MINOLTA AccurioPress C4080/C4070 / AccurioPrint C4065 User's Guide	02.10.00	英語版
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 User's Guide Security Functions (Administrator)	1.0 (2021-04-02)	英語版
KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 User's Guide Security Functions (User)	1.0 (2021-04-02)	英語版

なお、日本語版ガイダンスは日本国内のみ配布、英語版ガイダンスは海外(日本国外)のみの配布となる。また KONICA MINOLTA AccurioPrint C4065 は日本国内では販売しない(KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 は日本国内及び海外で購入できる)。

1.4.1.4. TOE の構成要素の識別

TOE の構成要素を以下に示す。
TOE を構成する MFP 本体及び HDD ユニットの識別は以下の通りである。
MFP 本体は TOE を構成するハードウェア及びファームウェアが組み込まれた形式で、販売会社から初期設定を行う技術者を伴ってユーザーに提供を行う。また、HDD ユニットはオプション機材の形式で搬入される。

Table 1-5 TOE の構成要素

構成要素	識別	FW バージョン
MFP 本体 (右のいずれか)	KONICA MINOLTA AccurioPress C4080, KONICA MINOLTA AccurioPress C4070, KONICA MINOLTA AccurioPrint C4065	FW バージョン　GM2-20
HDD ユニット	UK-112	

1.4.2. TOE の論理的範囲

以下に TOE のセキュリティ機能と基本機能を記述する。

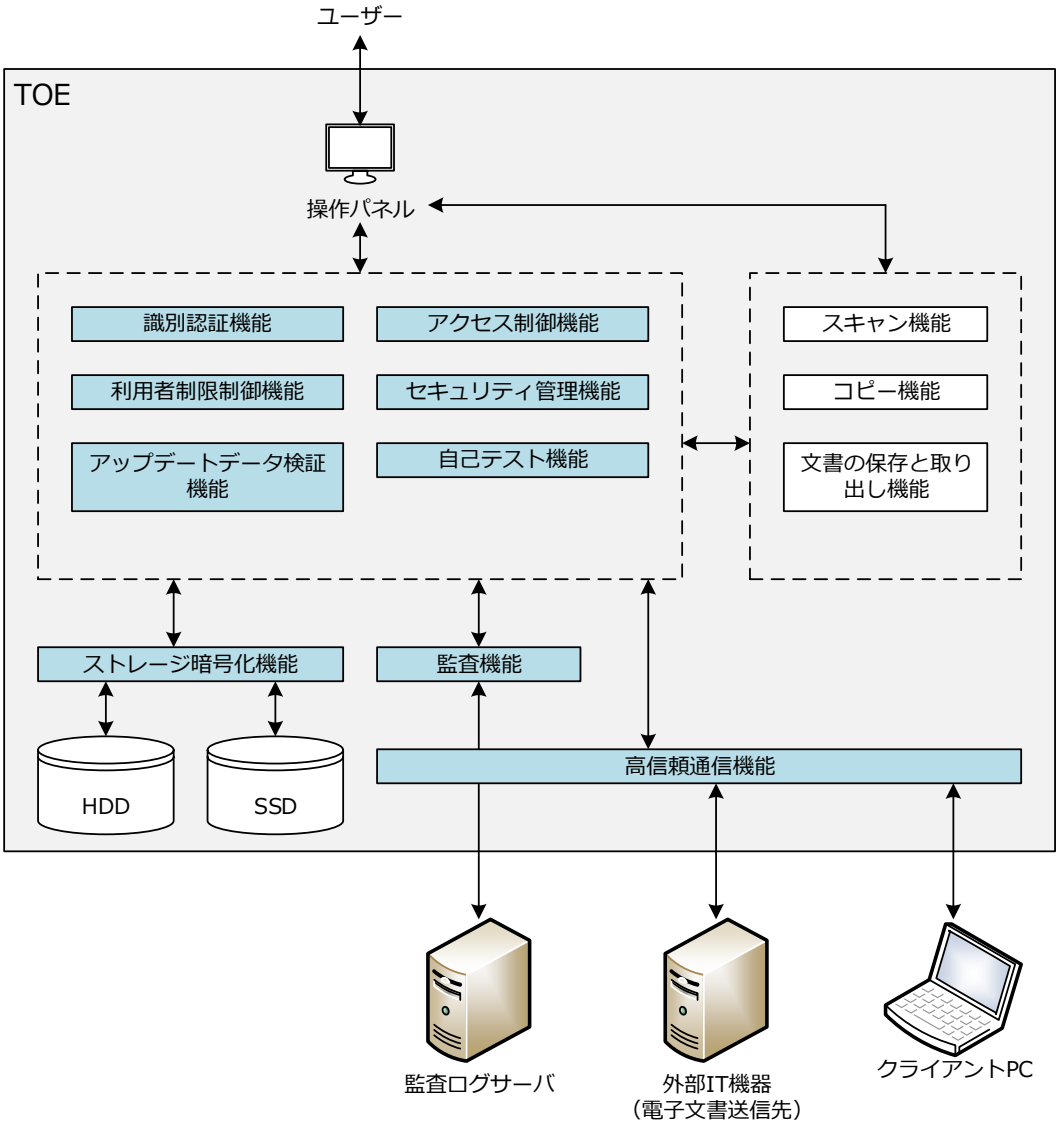


Figure 1-3 TOE の論理的範囲

1.4.2.1. 基本機能

TOE は以下の基本機能を有する。

Table 1-6 TOE の基本機能

No.	Function	Definition
1	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電子文書を生成し外部 IT 機器(WebDAV サーバー、SMB サーバー、FTP サーバー)に送信する機能
2	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電子文書を生成し複写印刷、あるいは HDD に保存する機能。
3	文書の保存と取り出し機能	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電子文書を生成し HDD に保存、あるいは蓄積した電子文書を取り出し印刷する機能。 蓄積した電子文書は改変、削除が可能である。

1.4.2.2. セキュリティ機能

以下に、TOE のセキュリティ機能を記述する。

Table 1-7 TOE のセキュリティ機能

No.	Function	Definition
1	識別認証機能	TOE を利用しようとする者が許可利用者であることを利用者から取得した識別認証情報を使って検証し、許可利用者と判断された者だけに TOE の利用を許可する機能。認証方式には TOE 自身が識別認証を行う本体装置認証方式のみが使用可能。本機能には以下の機能が含まれる。 ・認証失敗した場合に一定時間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 ・操作パネルにおいて、識別認証されたユーザーの操作が一定時間ない場合、そのセッションを終了する機能
2	アクセス制御機能	TOE 内の保護資産に対し、許可された利用者のみがアクセス可能となるように、保護資産へのアクセスを制限する機能。
3	ストレージ暗号化機能	HDD・SSD に記録されているデータを漏洩から保護するために、それらを暗号化する機能。
4	高信頼通信機能	LAN 利用時にネットワーク上の盗聴による情報漏えいを防止する機能。クライアント PC と TOE の間の通信データ、及び監査ログサーバーや外部 IT 機器(電子文書の送信先として利用できるサーバー。WebDAV サーバー、SMB サーバー、FTP サーバーの 3 種)と TOE の間の通信データを IPsec 通信により暗号化する。
5	セキュリティ管理機能	識別認証機能で認証された TOE の許可利用者に対して、その利用者の役割に対して与えられた権限または利用者毎に与えられた権限に基づいて TSF データに対する操作に関する制御、及びセキュリティ機能のふるまいの管理をおこなう機能。セキュリティ強化設定の設定やユーザーの作成/パスワード変更、監査ログサーバーの設定、日時の変更などが該当する。
6	監査機能	TOE の使用およびセキュリティに関連する事象(以下、監査事象という)のログを日時情報等とともに外部監査ログサーバーに送信する機能。
7	アップデートデータ検証機能	TOE のファームウェアのアップデートを実施する前に、ファームウェアの真正性を保証するためデジタル署名検証を実施する機能
8	自己テスト機能	TSF 実行ファームウェアが正常であることを TOE の起動時に検証する機能。

1.5. 用語

本 ST では以下の略語・用語を使用する。

Table 1-8 用語

Designation	Definition
電子文書	電子文書は画像、文字や図形などの情報を電子化したデータである。
紙文書	紙文書は、画像、文字や図形などの情報を持つ紙媒体の文書である。
操作パネル	操作パネルは、KONICA MINOLTA AccurioPress C4080 / AccurioPress C4070 / AccurioPrint C4065 シリーズの筐体に付属するタッチパネル式ディスプレイ及び操作

Designation	Definition
	ボタンの名称である。
SMB	SMB とは、Microsoft 系 OS においてネットワーク上でコンピューター同士が通信を行うためのアプリケーションプロトコルである。
ユーザー	管理者によりユーザー名とログインパスワードが TOE に登録された一般利用者。ログインによる識別認証機能成功により User ID と紐付けられる。
管理者	管理者パスワードを知る利用者。管理者機能利用時に要求される識別認証機能成功により Admin ID と紐付けられる。
サービスモード	TOE の設置・保守点検や修理などを行う技術者であるサービスエンジニア（以下、CE と呼称）用の各種設定画面。記憶媒体やスキャナ・プリントなどのデバイスの微調整等の機能を実施できる。サービスモードは、操作パネルからのみ確認・変更を行うことができる。ただしサービスログイン許可設定機能(管理者が設定可能)の設定により本機能は無効化できる。
SC コード	重大なソフトウェア及びハードウェア異常が発生した時に、操作パネルに表示されるエラーコード。SC コードの表示と共に TOE は動作を停止、操作を受け付けない状態に移行する。このコードが表示された時は、管理者はサービスエンジニアを呼ぶようガイダンスにて案内されている。
ネットワーク管理機能	ネットワーク経由で管理者の識別認証後利用可能となる機能（リモート管理機能）であり、インターネット ISW 機能（インターネットを用いて、外部サーバーから、TOE の書き換えを行う機能）、Web Connection（Web ブラウザを使用して TOE の設定変更や状態確認をするための機能）が存在する。セキュリティ強化設定が有効化されている場合は Web Connection のファームウェアバージョン確認機能のみが利用でき、その他の機能は利用できない。
FTP 送信	電子文書を FTP サーバーにアップロードする機能。
SMB 送信	電子文書をコンピューターやサーバーの共有フォルダーへ送信する機能。
WebDAV 送信	電子文書を WebDAV サーバーにアップロードする機能。
オートリセット	ログイン中に、予め設定された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。
オートリセット時間	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、セキュリティレベルの低いネットワーク設定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。なお、セキュリティ強化設定が有効な状態のみが TOE としての環境である。
User ID	一般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。
Admin ID	管理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。
ユーザー管理機能	ユーザーの登録／変更／削除を行う機能。
ユーザー認証機能	TOE の利用者を認証する機能。本体認証と中間認証、外部認証の 3 種類あるが、セキュリティ強化設定が有効な時は本体認証のみが使用できる。
ログイン	TOE において、ユーザー名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。
暗号化パスワード	HDD・SSD の暗号化において使用する暗号鍵の生成において使用するデータ。TOE は暗号化パスワードで設定された文字列を使用して暗号鍵を生成する。
監査機能	監査対象事象に対して監査ログを生成、記録し、ログサーバーへ送信する機能。

Designation	Definition
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。
ファームウェア	TOE 及びその周辺装置（フィニッシャー）の基本的な制御を司る機能を持ったソフトウェアであり、TOE は複数のファームウェアで構成されている。TSF 機能の実現には本体制御ファームウェア、及びコントローラファームウェアを使用している。
ファームウェアアップデート	ネットワーク経由もしくは USB メモリから入手したアップデートデータを使用してファームウェアの更新を行う機能。セキュリティ強化設定が有効な時は USB メモリを使用した更新のみ実施できる。ISW とも呼ばれる。

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	:	Part2 (CCMB-2017-04-002) Extended, and Part3 (CCMB-2017-04-003) Conformant

2.2. PP claim

本 ST は、以下の PP に適合する。

PP identification	:	
PP Title	:	Protection Profile for Hardcopy Devices
PP registration	:	
PP version	:	1.0 dated September 10, 2015
Date	:	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
  Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
  なし

3. Security Problem Definition

本章では、利用者と保護対象資産の定義、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. Users

TOE の利用者は、以下のように分類される。

Table 3-1 User Categories

Designation	Asset category	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.ADMIN	Administrator	A User who has been identified and authenticated and has an

		administrative role

3.2. Assets

保護資産は、User Data, TSF Data である。各資産は以下のように定義される。

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 は下記 2 つの種別から構成される。

Table 3-3 User Data Type

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 は下記 2 つの種別から構成される。

Table 3-4 TSF Data

Designation	TSF 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. Threats

This section describes threats to assets described in clause in 3.2.

Table 3-5 Threats for the TOE

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 while in a degraded state.
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 Policies

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

Table 3-6 Organizational Security Policies for the TOE

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.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

3.5. Assumptions

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

Table 3-7 Assumptions for the TOE

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. Security Objectives for the Operational environment

This section describes the Security Objectives that must be fulfilled in the operational environment of the TOE.

Table 4-1 Security Objectives for the Operational environment

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

5. Extended components definition

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

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

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

Component leveling:

FAU_STG_EXT.1: Extended: External Audit Trail Storage	1

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

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

Audit:
The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:
- There are no auditable events foreseen.

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

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

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

5.2. 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 Destruction	4

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

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

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

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

5.3. FCS_IPSEC_EXT Extended: IPsec selected

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

Component leveling:

FCS_IPSEC_EXT.1 Extended: IPsec selected	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to : No other components

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

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

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

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

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

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

FCS_IPSEC_EXT.1.6	The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].
FCS_IPSEC_EXT.1.7	The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.
FCS_IPSEC_EXT.1.8	The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; IKEv1 SA lifetimes can be established based on [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].
FCS_IPSEC_EXT.1.9	The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE*], *no other DH groups*].
FCS_IPSEC_EXT.1.10	The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.

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

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

5.4. FCS_KDF_EXT Extended: Cryptographic Key Derivation

Family Behavior:
This family specifies the means by which an intermediate key is derived from a specified set of submasks.

Component leveling:

FCS_KDF_EXT:Cryptographic Key Derivation	1

FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

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_KDF_EXT ***Extended: Cryptographic Key Derivation***

Hierarchical to : No other components

Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),
[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108* [selection: *KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode]*, *NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

Rationale:

The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.

This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.5. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family Behavior:

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

Component leveling:

FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

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_KYC_EXT.1 ***Extended: Key Chaining***

Hierarchical to : No other components.

Dependencies : [FCS_COP.1(e) Cryptographic operation (Key Wrapping),

FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(f) Cryptographic operation (Key Encryption),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or
FCS_COP.1(i) Cryptographic operation (Key Transport)]

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):* [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

Rationale:
Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain.However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.6. FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning

Family Behavior:
This family ensures that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

Component leveling:

FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning	1

FCS_PCC_EXT.1 Cryptographic Password Construction and Conditioning, requires the TSF to accept passwords of a certain composition and condition them appropriately.

Management:
No specific management functions are identified

Audit:
There are no auditable events foreseen.

FCS_PCC_EXT.1 Extended: Cryptographic Password Construct and Conditioning

Hierarchical to : No other components
Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and

shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] that meet the following: [assignment:*PBKDF recommendation or specification*].

Rationale:

The TSF is required to ensure that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

This extended component protects the Data Encryption Keys using cryptographic algorithms and Robust BEV in the maintained key chains, and it is therefore placed in the FCS class with a single component.

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

Family Behavior:

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

Component leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

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

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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

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

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

5.8. FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation

Family Behavior:
This family ensures that salts, nonces, and IVs are well formed.

Component leveling:

FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	1

FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation), requires the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

Management:
No specific management functions are identified

Audit:
There are no auditable events foreseen.

FCS_SNI_EXT.1	***Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)***	
	Hierarchical to :	No other components
	Dependencies :	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_SNI_EXT.1.1	The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.	
FCS_SNI_EXT.1.2	The TSF shall only use unique nonces with a minimum size of [64] bits.	
FCS_SNI_EXT.1.3	The TSF shall create IVs in the following manner: [・CBC: IVs shall be non-repeating, ・CCM: Nonce shall be non-repeating. ・XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer, ・GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.].	

Rationale:

The TSF is required to ensure that the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.
This extended component protects the communication data and storage data using cryptographic algorithms with specified Salt, Nonce and Initialization Vector Generation, and it is therefore placed in the FCS class with a single component.

5.9. FDP_DSK_EXT Extended: Protection of Data on Disk

Family Behavior:
This family is to mandate the encryption of all protected data written to the storage.

Component leveling:

FDP_DSK_EXT.1 Extended: Protection of Data on Disk	1

FDP_DSK_EXT.1 Extended:Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

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_DSK_EXT.1	**Extended: Protection of Data on Disk**		
	Hierarchical to	:	No other components
	Dependencies	:	FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).
FDP_DSK_EXT.1.1	The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d) , use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*], such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.		
FDP_DSK_EXT.1.2	The TSF shall encrypt all protected data without user intervention.		

Rationale:
Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.10. 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.

5.11. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family Behavior:

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

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

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

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

Audit:
The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:
- There are no auditable events foreseen.

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

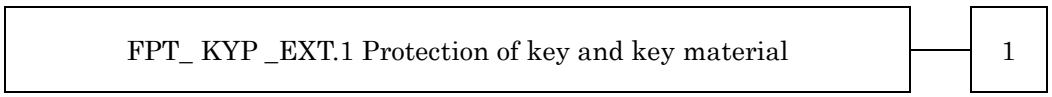
Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

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

5.12. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:
This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

Component leveling:



FPT_ KYP _EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

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_KYP_EXT.1	**Extended: Protection of Key and Key Material**		
	Hierarchical to	:	No other components.
	Dependencies	:	No dependencies.
FPT_KYP_EXT.1.1	The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device.		

Rationale:

Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

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

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to : No other components.

Dependencies : No dependencies.

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

Rationale:

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

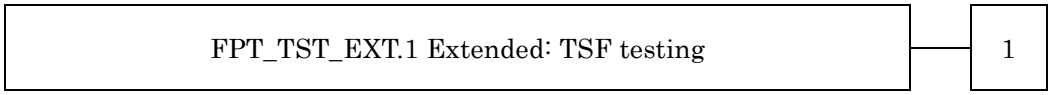
This extended component protects the TOE by means of strong authentication using Preshared Key, and it is therefore placed in the FPT class with a single component.

5.14. FPT_TST_EXT Extended: TSF testing

Family Behavior:

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

Component leveling:



FPT_TST_EXT.1 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.

5.15. FPT_TUD_EXT Extended: Trusted Update

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

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

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

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

Audit:
The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:
- There are no auditable events foreseen.

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

Rationale:

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

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

6. Security Requirements

本章では、セキュリティ要件について記述する。

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、5 章を参照。

＜セキュリティ機能要件“操作”の明示方法＞

以下の機能エレメントの記述の中において、下記のルールに基づいて装飾を行っている。

- **ボールドで示される表記**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、本 ST で選択もしくは割り付けた SFR 内のテキストを示す。選択または割付した値は青文字部分に示す。
- ***ボールドイタリック書体***は、PP で完成または詳細化された SFR の部分に対し、ST において選択され、かつ／または完成された SFR 内のテキストを示す。選択または割付した値は青文字部分に示す。
- アンダーラインは本 ST で詳細化を行った結果を示す（表の場合は表題のみに明示）
- 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。

■必須 SFR

6.1.1. 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*] ▪ none
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*]. [assignment: *other audit relevant information*] ▪ none

Table 6-1 Audit data requirements

Auditable event	Relevant SFR	Additional	Details

		information	
Job completion	FDP_ACF.1	Type of job	・コピーの完了 ・スキャンの完了 ・コピージョブの保存 ・保存ジョブの読出し ・保存ジョブの印刷 ・保存ジョブのファイル出力 ・保存ジョブの削除 ・保存ジョブの複製 ・保存ジョブの変更
Unsuccessful User authentication	FIA_UAU.1	None	・ログインの成功 ・ログインの失敗
Unsuccessful User identification	FIA_UID.1	None	・ログインの成功 ・ログインの失敗
Use of management functions	FMT_SMF.1	None	・セキュリティ管理機能の使用
Modification to the group of Users that are part of a role	FMT_SMR.1	None	ユーザーの役割の変更機能が存在しない為記録は行わない
Changes to the time	FPT_STM.1	None	・日時の変更
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a)	Reason for failure	・通信確立の失敗及び失敗の理由

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.

6.1.2. 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* ...]

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

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) The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as**

Refinement **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*]

- 128bit
- 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,*** ...]

- 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

[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 SP800-38A

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(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 ...***]

- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]

[**assignment:** ***2048 bits or greater***]

- 2048bits

[**selection:** Case: Digital ...]

- 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

[selection: *128 bits, 256 bits*]

- 256 bits

6.1.3. Class FDP: User data protection

FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : No other components

Dependencies : FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : No other components

Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

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

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [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"
Scan	**Operation :**	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	denied	denied	denied
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	**Operation :**	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2)	denied	denied	
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage / retrieval	**Operation :**	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***

	Job owner	(note 1)			
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

【補足】 Table6-2 は、下記の状況での SFP を記述している。

- **Scan：** 利用者がスキャンされた画像データをスキャン画像送信先に送信する操作を行った時に、HCD 内に一時的に保持される画像データに対する SFP。
- **Copy：** 利用者がスキャンされた画像データをプリントする操作を行なった時に、HCD 内に一時的に保持される画像データに対する SFP。
- **Storage / retrieval：**
  利用者がスキャンされた画像データを HDD 保存する操作を行なった時に、HDD に保存された画像データに対する SFP。

※本 TOE は FAX 機能を搭載していないため「Fax send」「Fax receive」時の操作及びアクセス制御は存在しない。またネットワークからの印刷機能を搭載していないため「Print」時の操作及びアクセス制御は存在しない。

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

		"Create"	"Read"	"Modify"	"Delete"
Scan	**Operation：**	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2)		denied	denied
	U.ADMIN	denied		denied	denied
	U.NORMAL			denied	denied
	Unauthenticated	denied		denied	denied
Copy	**Operation：**	***Create copy job***	***View copy status / log***	***Modify copy job***	***Cancel copy job***
	Job owner	(note 2)		denied	
	U.ADMIN	denied		denied	denied
	U.NORMAL			denied	denied
	Unauthenticated	denied		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)			
	U.ADMIN	denied		denied	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

【補足】 Table6-3 は、下記の状況での SFP を記述している。

- **Scan：** 利用者がスキャンされた画像データをスキャン画像送信先に送信する操作を行った時に、HCD 内に一時的に保存されるジョブのジョブデータに対する SFP。
- **Copy：** 利用者がスキャンされた画像データをプリントする操作を行なった時に、HCD 内に一時的に保存されるジョブのジョブデータに対する SFP。
- **Storage / retrieval：**
  利用者がスキャンされた画像データを HDD 保存する操作を行なった時に、HDD に保存された印刷データ、または、ジョブデータに対する SFP。

※本 TOE は FAX 機能を搭載していないため「Fax send」「Fax receive」時の操作及びアクセス制御は存在しない。またネットワークからの印刷機能を搭載していないため「Print」時の操作及びアクセス制御は存在しない。

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 or retrieval Job.*

6.1.4. 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*]]

[assignment: *positive integer number*],

- 1

[assignment: *list of authentication events*]

- Refer to Table 6-4

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*]

- Refer to Table 6-4

[assignment: *list of actions*]

- Refer to Table 6-4

Table 6-4 Authentication failure handling

authentication events	*met, surpassed*	*list of actions*]
操作パネルにおける管理者／ユーザー認証	met	5 秒間の認証停止
Web Connection における管理者認証	met	5 秒間の認証停止

FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)

Hierarchical to : No other components

Dependencies : No dependencies

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

[assignment: *list of security attributes*].

- タスク属性(User ID、Admin ID)
- 役割(U.NORMAL、U.ADMIN)

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*]]

- "!", "@", "#", "$", "%", "^", "&", "*", "(", ")" and [assignment: *other characters*]

[assignment: *other characters*]

- "-", "¥", "[", "]", ":", ";", ",", ".", "/", "'", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?" and "_" (管理者)
- "-", "¥", "[", "]", ":", ";", ",", ".", "/", " ", "'", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?" and "_" (一般利用者)

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***]

- TOE の状態確認および表示等の設定
- スキャン操作によるスキャンデータの送信履歴、コピー操作による出力履歴、出力がキャンセルされたジョブの履歴である未出力履歴、出力が完了していないジョブの出力予約の閲覧

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 文字毎に秘匿文字の表示

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***]

- TOE の状態確認および表示等の設定
- スキャン操作によるスキャンデータの送信履歴、コピー操作による出力履歴、出力がキャンセルされたジョブの履歴である未出力履歴、出力が完了していないジョブの出力予約の閲覧

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*].

- タスク属性(User ID、Admin ID)
- 役割(U.NORMAL、U.ADMIN)

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

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

- Admin ID(1 つのみ固定)で認証された場合、役割 U.ADMIN を関連付ける
- その他の ID で認証された場合役割 U.NORMAL を関連付ける。

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].

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

- なし

6.1.5. 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*]

- Refer to Table 6-5

[assignment: *list of functions*]

- Refer to Table 6-5

Table 6-5 Management of Security Functions behavior

Security Functions	Operations
セキュリティ強化設定機能	disable, enable
サービスログイン許可設定機能	disable, enable
全データ上書き削除機能	determine the behaviour of
監査ログ送信先設定機能	modify the behavior of
高信頼通信機能	modify the behavior of

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 6-6

[assignment: *list of security attributes*]

- Refer to Table 6-6

[assignment: *the authorized identified roles*]

- Refer to Table 6-6

Table 6-6 Management of Object Security Attribute

Security Attribute	Authorized Identified Roles	Operations
User ID	U.ADMIN	登録、modify、delete

FMT_MSA.3 Static attribute initialisation

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : 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]*]

- restrictive

FMT_MSA.3.2 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.

Refinement

[**selection: *U.ADMIN, no role***]

- no role

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 The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6-7, Table 6-8 and Table 6-9.**

Refinement

Table 6-7 Operation of TSF Data (1)

TSF Data *owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL*

TSF Data	Operations	Authorized Roles
U.NORMAL のログインパスワード	Modify	the owning U.NORMAL.
U.NORMAL のログインパスワード	登録、Modify	U.ADMIN,

Table 6-8 Operation of TSF Data (2)

TSF Data *not owned by a U.NORMAL*

TSF Data	Operations	Authorized Roles
日時情報	modify	U.ADMIN
暗号化パスワード	modify	U.ADMIN
パスワード規約	query, modify	U.ADMIN
U. ADMIN のログインパスワード	Modify	U.ADMIN

Table 6-9 Operation of TSF Data (3)

TSF Data: *software, firmware, and related configuration data*

TSF Data	Operations	Authorized Roles
TOE のファームウェア更新に関するデータ(更新対象のファームウェア)	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*].

~~Refinement~~

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

- refer to Table 6-10

Table 6-10 list of management functions

management functions
U.ADMIN によるセキュリティ強化設定機能

U.ADMIN による監査ログ送信先設定機能
U.ADMIN によるユーザー管理機能※
U.NORMAL による自身のログインパスワードの変更機能
U.ADMIN による自身のログインパスワードの変更機能
U.ADMIN による日時情報の変更機能
U.ADMIN によるパスワード規約変更機能
U.ADMIN によるネットワーク設定の登録・変更機能
U.ADMIN による暗号化パスワードの変更機能
U.ADMIN によるファームウェアアップデート機能
U.ADMIN による全データ上書き削除機能
U.ADMIN によるサービスログイン許可設定機能

※ユーザー管理機能には、U.ADMIN による U.NORMAL のログインパスワードの管理、サブジェクトのセキュリティ属性の管理が含まれる。

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 The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

Refinement

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

6.1.6. 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

6.1.7. 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、
  - 一般利用者は最終操作および最終操作による処理が完了してからオートリセット時間によって決定される時間（オートリセット機能が無効の時は 1 分間）
  - 管理者は最終操作による処理が完了してから 30 分間
- Web Connection の場合、対話セッションはない

6.1.8. Class FTP: Trusted path/channels

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]*]

- [assignment: other capabilities]

[assignment: other capabilities]

- ファイルサーバー(WebDAV, FTP, SMB)
- 監査ログサーバー(syslog)

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***]

- 電子文書送信機能
- 監査ログのサーバー送信機能

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**.

< Appendix B: Conditionally Mandatory Requirements (Confidential Data on Field-Replaceable Nonvolatile Storage Devices) >

6.1.9. Class FPT: Protection of the TSF

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

(for O.KEY_MATERIAL)

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

FPT_KYP_EXT.1.1 Refinement	The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

6.1.10. Class FCS: Cryptographic support

FCS_KYC_EXT.1 Extended: Key Chaining

(for O.STORAGE_ENCRYPTION)

Hierarchical to : No other components.

Dependencies : [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(f) Cryptographic operation (Key Encryption),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or
FCS_COP.1(i) Cryptographic operation (Key Transport)]

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):* [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

[selection: *one, using a submask as the BEV or DEK; intermediate ...*]

- intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): [selection: key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)]

[selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]

- key encryption as specified in FCS_COP.1(f)
- key derivation as specified in FCS_KDF_EXT.1

[selection: *128 bits, 256 bits*]

- 256bit

6.1.11. Class FDP: User data protection

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

(for O.STORAGE_ENCRYPTION)

Hierarchical to : No other components

Dependencies : FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

FDP_DSK_EXT.1.1 The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d) , use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*], such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.

[selection: *perform encryption in accordance with FCS_COP.1(d) , use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*]

- perform encryption in accordance with FCS_COP.1(d)

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

< Appendix D: Selection-based Requirements (Confidential Data on Field-Replaceable Nonvolatile Storage Devices) >

6.1.12. Class FCS: Cryptographic support

FCS_COP.1(d) **Cryptographic operation (AES Data Encryption/Decryption)**

(for O.STORAGE_ENCRYPTION)

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(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection: *CBC, GCM, XTS*] mode** and cryptographic key sizes **[selection: *128 bits, 256 bits*]** that meet the following: **AES as specified in ISO/IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*]**.

[selection: *CBC, GCM, XTS*]

- CBC

[selection: *128 bits, 256 bits*]

- 256bits

[selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*]

- CBC as specified in ISO/IEC 10116

FCS_COP.1(f) **Cryptographic operation (Key Encryption)**

(selected from FCS_KYC_EXT.1.1)

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(f) Refinement The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[selection: *CBC, GCM*] mode]** and cryptographic key sizes **[selection: *128 bits, 256 bits*]** that meet the following: **[AES as specified in ISO /IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772*]**.

[selection: *CBC, GCM*]

- CBC

[selection: *128 bits, 256 bits*]

- 256bits

[selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772*]

- CBC as specified in ISO/IEC 10116

< Appendix D: Selection-based Requirements (Protected Communications) >

6.1.13. Class FCS: Cryptographic support

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

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 as defined ...; IKEv2 as defined*]

- IKEv1 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*]

[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 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*]].

[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 ...

[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*

[assignment: *other DH groups that are implemented by the TOE*]

- none

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

6.1.14. Class FCS: Cryptographic support

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

6.1.15. Class FIA: Identification and authentication

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*] ▪ no other lengths
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

< Appendix D: Selection-based Requirements (Trusted Update) >

6.1.16. Class FCS: Cryptographic support

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

< Appendix D: Selection-based Requirements (Passphrase-based Key Entry) >

6.1.17. Class FCS: Cryptographic support

FCS_PCC_EXT.1 **Extended: Cryptographic Password Construct and Conditioning**

(for O. STORAGE_ENCRYPTION)

Hierarchical to : No other components

Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] that meet the following: [**NIST SP 800-132**].

[assignment: *positive integer of 64 or more*]

- 64

[assignment: *other supported special characters*]

- "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "-", "¥", "[", "]", ":", ";", ",", ".", "/", "'", "", "=", "~", "|", "`", "{", "}", "+", "<", ">", "?" and "_"

[selection: *SHA-256, SHA384, SHA-512*]

- SHA-256

[assignment: *positive integer of 1000 or more*]

- 1000

[selection: *128, 256*]

- 256

FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

(for O. STORAGE_ENCRYPTION)

Hierarchical to : No other components

Dependencies : FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication), [if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

[selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*]

- a RNG generated submask as specified in FCS_RBG_EXT.1
- a conditioned password submask

[selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*]

- NIST SP 800-132

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

(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)

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_COP.1(c) Cryptographic operation (Hash Algorithm),

	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(h) Refinement	The TSF shall perform [**keyed-hash message authentication**] in accordance with [**selection:** *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*] and cryptographic key sizes [assignment: *key size (in bits) used in HMAC*] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"; ISO/IEC 10118**]. [**selection**: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*] ▪ HMAC-SHA-256 [assignment: *key size (in bits) used in HMAC*] ▪ 512bit

FCS_SNI_EXT.1	**Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)**	
	(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)	
	Hierarchical to :	No other components
	Dependencies :	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_SNI_EXT.1.1	The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.	
FCS_SNI_EXT.1.2	The TSF shall only use unique nonces with a minimum size of [64] bits.	
FCS_SNI_EXT.1.3	The TSF shall create IVs in the following manner: [・CBC: IVs shall be non-repeating, ・CCM: Nonce shall be non-repeating. ・XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer, ・GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.].	

6.2. Security assurance requirements

This section describes Security Assurance Requirements (SARs) for the TOE.

Table 6-11 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 6-12 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	FPT_STM.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A
FAU_STG_EXT.1	FPT_STM.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1	N/A
FCS_CKM.1(a)	[FCS_COP.1(b), or FCS_COP.1(i)] FCS_CKM_EXT.4	FCS_COP.1(b) FCS_CKM_EXT.4	N/A
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)] FCS_CKM_EXT.4 FCS_RBG_EXT.1	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_CKM_EXT.4 FCS_RBG_EXT.1	N/A
FCS_CKM_EXT.4	[FCS_CKM.1(a), or FCS_CKM.1(b)] FCS_CKM.4	FCS_CKM.1(a) FCS_CKM.1(b) FCS_CKM.4	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_COP.1(a)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A
FCS_COP.1(b)	FCS_CKM.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	IPsec 通信（FCS_IPSEC_EXT.1）の場合。アップデート機能（FPT_TUD_EXT.1）の場合は、FCS_CKM.1(a)、FCS_CKM_EXT.4 は満たさないが、鍵生成はおこなわないため問題ない。
FCS_RBG_EXT.1	No dependencies.	No dependencies.	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A

機能要件	依存関係	ST で満たす依存関係	依存関係を満たしていない要件
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	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_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_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	N/A
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	N/A
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.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(c)	FCS_COP.1(b) 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
FPT_KYP_EXT.1	No dependencies.	No dependencies.	N/A
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_COP.1(f)	N/A
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	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_COP.1(d)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A
FCS_COP.1(f)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1 FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1	FIA_PSK_EXT.1 FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1	N/A
FCS_COP.1(g)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A
FIA_PSK_EXT.1	FCS_RBG_EXT.1	-	乱数ビット生成器を用いたビットベースの事前共有鍵生成を選択していないため。
FCS_COP.1(c)	No dependencies.	No dependencies.	N/A
FCS_PCC_EXT.1	FCS_COP.1(h)	FCS_COP.1(h)	N/A
FCS_KDF_EXT.1	FCS_COP.1(h) FCS_RBG_EXT.1	FCS_COP.1(h) FCS_RBG_EXT.1	N/A
FCS_COP.1(h)	FCS_CKM.1(b) FCS_COP.1(c) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_COP.1(c) FCS_CKM_EXT.4	N/A
FCS_SNI_EXT.1	FCS_RBG_EXT.1	FCS_RBG_EXT.1	N/A

7. TOE Summary specification

TOE のセキュリティ機能要件より導かれる TOE のセキュリティ機能の一覧を Table 7-1 に示す。詳細は後述の項にて説明する。

Table 7-1 セキュリティ機能一覧

No.	セキュリティ機能名称
1	識別認証機能
2	アクセス制御機能
3	ストレージ暗号化機能
4	高信頼通信機能
5	セキュリティ管理機能
6	監査機能
7	アップデートデータ検証機能
8	自己テスト機能

7.1. 識別認証機能

FIA_UAU.1, FIA_UID.1

＜一般利用者の識別認証＞

TOE は、利用者からユーザー名とパスワードを取得して本体認証方式による識別認証を行い、検証の結果許可利用者と判断された者だけ TOE の利用を許可する。利用者は操作パネルを用いてユーザー名とパスワードを TOE に入力する（Web Connection で実施できるのは管理機能のみであるため本項目は該当しない）。TOE は登録されたユーザー名・パスワードと一致することを確認する。識別認証を実行前にできる操作は下記に限られる

- 機械状態の確認（予約されたジョブの状態・用紙トレイ内の紙サイズや残量など）
- セキュリティ機能に関係しない設定の確認・変更（用紙設定・画像調整・フィニッシャー位置調整などの印刷に関わる設定）
- スキャン操作によるスキャンデータの送信履歴、コピー操作による出力履歴、出力がキャンセルされたジョブの履歴である未出力履歴、出力が完了していないジョブの出力予約の閲覧

なお、利用者が一般利用者として TOE の利用を許可されている状態で管理者の識別認証操作を行った場合には、一般利用者としての TOE の利用が不可能（ログアウト）状態となり、別の利用者として管理機能を許可される事となる。管理機能の利用終了時に元の一般利用者として TOE が利用できるようになることはない。

＜管理者の識別認証＞

管理者の識別認証の仕組みは一般利用者の識別認証と異なる。

操作パネルや web ブラウザ（Web Connection 使用時）において、利用者が管理機能の利用できる画面に遷移する際、TOE は利用者に管理者パスワードの入力を求める。管理者パスワードを知る利用者がすなわち管理者という考えであり、管理者設定画面に遷移する操作自体を識別と捉えるため、ここではユーザー名の入力は求めない（一般利用者は管理者役職をあわせ持つことはできない）。TOE は、利用者から管理者パスワードを取得して本体認証方式による識別認証を行い、検証の結果管理者と判断された者だけ TOE の管理機能の利用を許可する。利用者は操作パネル、あるいは web ブラウザ（Web Connection 使用時）を用いて管理者パスワードを TOE に入力する。TOE は登録された管理者パスワードと一致することを確認する。識別認証を実行前に一切管理機能を行うことはできない。なお、利用者が管理機能の利用を許可されている状態では一般利用者として識別認証操作を行う事はできない（手段が存在しない）。

FIA_AFL.1

TOE は、操作パネルにおける管理者及びユーザー認証、及び Web Connection における管理者識別認証において、認証が失敗(1 回)した場合、TOE は利用者に対して次の認証試行を 5 秒間実行しない。

FIA_PMG_EXT.1

TOE は、下記の利用者パスワードにアルファベットの大文字と小文字、数字、及び以下の特殊文字を組み合わせた文字列を設定できる。

Table 7-2 パスワードに使用できる特殊文字

管理者パスワードに使用できる特殊文字(32 文字)											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	“	‘	=	~	|
`	{	}	+	<	>	?	_				

一般利用者パスワードに使用できる特殊文字(32 文字)											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	ｽﾍﾟｰｽ	‘	=	~	|
`	{	}	+	<	>	?	_				

また TOE は利用者が下記の利用者パスワードを設定、あるいは変更を行う場合、新たに設定されるパスワードが「パスワード最小文字数」設定値以上の文字数か確認を行う(パスワード最小文字数は、管理者によって 8 文字～64 文字の範囲で設定される)。条件を満たさない場合は設定を反映せず、再設定を要求するメッセージを表示する。

- 管理者パスワード
- ユーザーパスワード

FIA_USB.1

TOE は利用者の識別認証後、利用者を代行するタスクにユーザー識別子(User ID) 及び役割 U.NORMAL が関連づけられる。また、管理者の識別認証後は、利用者を代行するタスクに Admin ID 及び役割 U.ADMIN が関連づけられる。なお利用者を代行するタスクはインターフェース毎に関連付けられる為、Web Connection での管理者識別認証中にパネルから一般利用者や管理者の識別認証を実施することも可能である(なお、Web Connection においては、ファームウェアバージョンの確認のみが可能である)。

FIA_UAU.7

TOE は、利用者が操作パネル・web ブラウザからの認証のためパスワードを入力する際、入力した文字の代わりに入力文字数分のダミー文字(*)で表示する。

FTA_SSL.3

TOE は操作パネル、Web Connection で識別認証された利用者が以下の条件を満たした場合、そのセッションを終了する。

- 操作パネルの場合、一般利用者は最終操作による処理が完了してから1分後（オートリセット機能が無効時）、あるいは設定されたオートリセット時間(1 分～9 分の間で設定可能)が経過した場合ログアウトされる。また管理者は最終操作による処理が完了してから 30 分後にログアウトされ、再認証が要求される。
- Web Connection の場合、識別認証が成功し、ブラウザにファームウェアバージョンを表示した直後にログアウトを行う

7.2. アクセス制御機能

FDP_ACC.1, FDP_ACF.1

TOE は Table 6-2、Table 6-3 に記載された利用者データアクセス制御に基づき、利用者に対して利用者文書データと利用者ジョブデータへの操作を制限する。 各データへのアクセスは操作パネルを用いてのみ実施できる。

(1) 操作パネル利用時の利用者文書データ、及び利用者ジョブデータへの操作制限

- 操作パネルでスキャン、コピー、保存／取り出し機能を実行する画面に遷移する際には TOE への識別認証が要求され、未認証で各機能を利用することはできない。またこのとき管理者パスワードではログインすることはできない（各機能を利用することは出来ない）。
- 利用者ジョブデータ及び利用者文書データの作成において、各データに所有者情報として User ID が記録される。
- 管理者は識別認証後、管理者設定画面において、一般利用者による HDD 保存ジョブの一覧（ジョブ 1 ページ目のサムネイル画像、ファイル名、最終更新日時などを参照できる）の表示、及び各ジョブの削除を実行できる。また、保存ジョブ自動削除期間を設定することにより、一定期間を過ぎた保存ジョブを削除することができる。なお、HDD に保存された利用者文書データ及び利用者ジョブデータに対し、Modify は I/F が存在せず実行できない。
- HDD に保存された利用者文書データ及び利用者ジョブデータに対し、Job owner は Read, Modify, Delete ができる。HDD 保存ジョブの一覧表示画面において、ジョブの保存／取り出し機能、及び出力が完了していないジョブの出力予約の表示ができるが、この画面ではログイン利用者が操作可能なジョブのみが表示され他の利用者所有ジョブは表示されない。即ち I/F が存在しないため他の利用者所有ジョブの保存／取り出し機能は実行できない。また出力が完了していないジョブの出力予約では、Read, Modify, Delete するための I/F が存在しないため実行できない。
- Job owner は、コピー操作により作成された利用者文書データ及び利用者ジョブデータを、ストップボタンを押下することにより Delete できる。ただし、Job owner であってもコピー操作により作成された利用者文書データの Read, Modify、利用者ジョブデータの Modify は I/F が存在しないため実行できない。
- Job owner であってもスキャン操作により作成された利用者文書データの Read, Modify, Delete、利用者ジョブデータの Modify, Delete は I/F が存在しないため実行できない。
- スキャン操作によるスキャンデータの送信履歴、コピー操作による出力履歴、出力がキャンセルされたジョブの履歴である未出力履歴、出力が完了していないジョブの出力予約は未認証ユーザーを含め誰でも閲覧できる。

FIA_ATD.1

TOE は利用者に対し、利用者を代行するタスクのタスク属性(User ID、Admin ID) 及び役割(U.NORMAL、U.ADMIN) を属性として定義する。タスク属性と役割の割当タイミングは下記。

- 一般利用者: 管理者が操作パネルからユーザーの登録を行った時に、利用者属性としてユニークな UserID と固定の役割として U.NORMAL が割り当てられる
- 管理者: 管理者は AdminID が 1 つだけが存在し、追加や削除はできない。固定の役割として U.ADMIN が割り当てられている

7.3. ストレージ暗号化機能

ストレージデバイス暗号化機能は TOE 起動後、本体制御ファームウェアに組み込まれた暗号化ライブラリによって有効化され、無効化のタイミングでは各デバイスの暗号化対象領域にアクセスすることはできない。デバイスに書き込む前にデータを暗号化し、デバイスから読み出し後にデータを復号する。この処理は、各デバイスに書き込み/読み出しする全ての暗号化対象データに対して行われる。ここでは暗号化機能に使用する暗号鍵の材料保護機能と併せて、下記にて詳細を説明する。

FCS_COP.1(d), FCS_KYC_EXT.1, FCS_COP.1(f), FCS_CKM.1(b), FPT_SKP_EXT.1, FCS_PCC_EXT.1, FCS_KDF_EXT.1, FCS_COP.1(h), FPT_KYP_EXT.1,FCS_SNI_EXT.1,FCS_COP.1(c)

TOE は以下の規格に従った暗号化アルゴリズムを実装している。なお CTR_DRBG を用いた乱数生成処理実行の際には、ソフトウェアエントロピー源から取得した値 1024bit のビット列を生成し、ファームウェア内のライブラリソフトウェア（GUARD FIPS Security Toolkit）の乱数生成関数に入力することで乱数生成する。

Table 7-3 使用暗号化アルゴリズム

Algorithm	Standard	SFR Reference
CTR_DRBG	NIST SP 800-90A	FCS_RBG_EXT.1
PBKDF2	NIST SP 800-132	FCS_KDF_EXT.1 FCS_PCC_EXT.1
HMAC-SHA-256	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2” ISO/IEC 10118	FCS_COP.1(h)
AES-CBC 256bits	ISO/IEC 10116	FCS_COP.1(d) FCS_COP.1(f)

TOE はストレージの暗号化を実現するため Table 7-4 に記載された暗号鍵を生成している。

Table 7-4 ストレージ暗号化に使用する暗号鍵

鍵種	概要
DEK(256bit)	ストレージデバイス上のデータ暗号化に使用。TOE の製造工程のなかで CTR_DRBG(AES-256)に従った乱数生成を実行して生成。
KEK(256bit)	DEK 保存時の暗号化に使用。

管理者は TOE の利用時、「暗号化パスワード設定機能」を実行することにより必ず KEK の登録・生成を行うよう、ガイダンスにて案内される。この機能では KEK の再生成も行うことができる。この機能において管理者が暗号化パスワードを再設定することにより下記の処理が実行される。

(1) QSPI Flash に保存された鍵材料から鍵導出関数により KEK を作成する。
(2) QSPI Flash から暗号化された DEK を読込み、上記の鍵にて復号化、RAM に展開する。
(3) ユーザーが設定したパスワードを元に、本体制御ファームウェアに組み込まれた暗号化ライブラリが持つパスワードベースの鍵導出関数(PBKDF2)によって 256bit の KEK を新たに生成する。なお導出時の各パラメータは下記。
    - PRF：HMAC-SHA-256 ※FCS_COP.1(c)に従う SHA-256(ISO/IEC 10118-3:2004 に準拠)を使用
    - パスワード：パネルからユーザーが設定した暗号化パスワード（64 文字）
        ※ アルファベットの大文字と小文字、数字、及び特殊文字（Table 7-5 参照）を組み合わせた文字列を設定できる。最大 64 文字。64 文字に満たない場合は左詰めし null padding とする
    - Salt：FCS_RBG_EXT.1 の TSS 記載の乱数生成器で生成した乱数(384bit)
        ※ ソフトウェアエントロピー源から取得した値（1024bit)を Entropy Input(1024bit)として利用し、得た乱数を使用している。
    - iterationCount：1000 回
    - IV：PDKDF2 に該当するパラメータはない。
(4) 新たに生成された KEK で、DEK を暗号化する。

(5) QSPI Flash に KEK 導出時の鍵材料(パスワード・Salt)と、暗号化した DEK を保存する。

Table 7-5 パスワードに使用できる特殊文字(32 文字)

暗号化パスワードに使用できる特殊文字(32 文字)											
!	@	#	$	%	^	&	*	(	)	-	¥
[	]	:	;	,	.	/	“	‘	=	~	|
`	{	}	+	<	>	?	_				

上記の手段によって生成された暗号鍵は TOE 起動時にその初期化処理の中で以下のように利用される。

(1) TOE の副電源 ON によりブートローダが起動し、SSD のファームウェア格納領域から各ファームウェアを読込み実行する。
(2) TOE のファームウェアは QSPI Flash から鍵材料(パスワード及び Salt)を読み込み、パスワードベースの鍵導出関数(PBKDF2)による鍵導出を行う。
(3) QSPI Flash から暗号化された DEK を読込み、再導出した KEK にて復号化、RAM に展開する。
(4) TOE のファームウェアは、復号化された DEK を用いて SSD 及び NVRAM に保存された設定情報を復号化し、TOE のセキュリティ機能を含む全ての機能の初期化を実施、完了後操作パネルに基本画面を表示し、利用者が TOE の機能を利用可能な状態とする。

上記に示した様に

- KEK 鍵は NVRAM や QSPI Flash、可搬記憶媒体に該当する媒体には保存されず RAM のみに保存される。鍵材料は基板上の QSPI Flash 上に保存されるが、可搬記憶媒体に該当する媒体には保存されない。
- DEK 鍵は TOE の基板上の QSPI Flash に暗号化された状態で格納されるが、可搬記憶媒体に該当する媒体には保存されない。鍵材料に該当するものは存在しない。
- 復号化された DEK 鍵は RAM のみに保存される。可搬記憶媒体に該当する媒体には保存されない。
- KEK/DEK の鍵、鍵材料共に外部からアクセスするインターフェースは存在しない。

以上のことから暗号鍵は保護されていると考えられる。

FDP_DSK_EXT.1

TOE は、Table 7-4 記載の暗号鍵を使用しデータの暗号化を行う。

TOE において、暗号化対象となる利用者文書データと秘密の TSF データを保持可能なデバイスは可搬記憶媒体となる SSD/HDD 及び可搬記憶媒体に該当しない NVRAM/QSPI Flash である(RAM 上の TSF データは副電源 OFF と共に消去される)。ここに挙げたデバイス以外は TSF 情報を扱わない、もしくは副電源 OFF 時に TSF データを保持する能力を持っていない為暗号化の対象としていない。各デバイスの暗号化の対象となるデータについて Table 7-6、Table 7-7 に示す。

Table 7-6 各デバイス(可搬記憶媒体)の暗号化対象となるデータ

Storage	内容・領域	暗号化対応方法	暗号鍵	アルゴリズム	暗号化条件
SSD	SSD システム領域(パーティションテーブル等)	暗号化対象外	－	－	－
	ファームウェアの格納	暗号化対象外	－	－	－
	TOE 設定情報格納領域(管理者設定の設定値保存)	暗号化ファイルシステム	DEK	AES(CBC)	常時
	SWAP 領域(無効化)	未使用	－	－	－
	コントローラ領域(TOE のネットワーク設定、通信先サーバアドレ	暗号化ファイルシステム	DEK	AES(CBC)	常時

	ス、パスワード)				
	本体制御領域(認証データ)	暗号化ファイルシステム	DEK	AES(CBC)	常時
	監査ログ情報	暗号化ファイルシステム	DEK	AES(CBC)	常時
HDD (RAID 0)	ジョブ保存領域(ジョブ管理データ／ジョブログ)	独自実装	DEK	AES(CBC)	常時
	ジョブ保存領域(画像データ・サムネイル)	独自実装	DEK	AES(CBC)	常時

Table 7-7 各デバイス(可搬記憶媒体以外)の暗号化対象となるデータ

Device	内容・領域	暗号化対応方法	暗号鍵	アルゴリズム	暗号化条件
NVRAM	TOE 設定情報格納領域(ユーザー認証を除くパスワード情報、スキャン機能宛先／監査ログ送信先設定)	パスワード情報を暗号化して保存(上記に該当しないエリアは平文)	DEK	AES(CBC)	常時
QSPI Flash	DEK	暗号化して保存	KEK	AES(CBC)	常時
	KEK 鍵材料	平文のまま	－	－	－

Table 7-6、Table 7-7 に記載された各項目について説明する。

- 暗号化ファイルシステムは、暗号化対応方法列に「暗号化ファイルシステム」と記載されているパーティション(領域)全てのファイルの Read/Write を管理し、その際暗号化・復号化処理を必ず実施するファイルシステムソフトウェアであり、暗号化・復号化処理を回避できるインターフェースは存在しない。暗号化ファイルシステムによる暗号化処理は、コニカミノルタの工場において TOE の製造工程のなかで有効化される(DEK 鍵の作成と暗号化ファイルシステムでの利用設定も行われる)。その為管理者が暗号化機能を有効化する操作は必要ない(無効化する手段も存在しない)。
- HDD の「ジョブ保存領域(ジョブ管理データ・ジョブログ)」はジョブ管理データ入出力を司るインターフェースによる暗号化・復号化が実施される。ジョブ管理データは上記インターフェースで全ての Read/Write を行い、その際暗号化・復号化処理を必ず実施するため、暗号化・復号化処理を回避できるインターフェースは存在しない。ジョブ管理データ入出力インターフェースによる暗号化処理は、コニカミノルタの工場において TOE の製造工程のなかで有効化される(DEK 鍵の作成とジョブ管理データ入出力インターフェースでの利用設定も行われる)。その為管理者が暗号化機能を有効化する操作は必要ない(無効化する手段も存在しない)。
- HDD の「ジョブ保存領域(画像データ・サムネイル)」は画像データ入出力を司るインターフェースによる暗号化・復号化が実施される。画像データは上記インターフェースで全ての Read/Write を行い、その際暗号化・復号化処理を必ず実施するため、暗号化・復号化処理を回避できるインターフェースは存在しない。画像データ入出力インターフェースによる暗号化処理は、コニカミノルタの工場において TOE の製造工程のなかで有効化される(DEK 鍵の作成とジョブ管理データ入出力インターフェースでの利用設定も行われる)。その為管理者が暗号化機能を有効化する操作は必要ない(無効化する手段も存在しない)。
- SSD の「ファームウェアの格納領域」は暗号化を行わない領域である。該当する領域は OS 標準ファイルシステムによって Read/Write を行うが、利用者に対して直接ファイルアクセスを行うインターフェースは提供されない。

FCS_RBG_EXT.1

TOE は、NIST SP 800-90A に準拠する CTR DRBG(AES-256)と、1 つのソフトウェアノイズ源から構成される RBG を実装する。上記 CTR DRBG は、Derivation Function と Reseed を利用するが、Prediction Resistance 機能は動作しない。ソフトウェアノイズ源は、CPU の内部状態に影響を与える条件分岐コード等の実装とクロックカウ

ンター値取得処理をループ処理内に実装しており、ループ処理実行時間のばらつきをクロックカウンター経由で取得し、raw データを得る。シフト演算と XOR を用いて raw データに含まれるエントロピーをビット全体に撹拌、圧縮するコンディショニングを実施し、ビット全体のエントロピー率を上げた後、エントロピー値として出力する。

TOE は、この RBG を利用して乱数を生成し、暗号鍵 KEK の鍵材料及び暗号鍵 DEK(鍵長 256bit)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、ノイズ源として利用するソフトウェアを起動し、必要サイズのエントロピー値を取得して利用する。このエントロピー値は、NIST SP800-90A の 10.2.1 に示される Instantiate と Reseed に必要な最小エントロピー量(TOE の場合、セキュリティ強度と同じ 256bit)を満たしており、十分なエントロピーが含まれている。

FCS_CKM.4, FCS_CKM_EXT.4

TOE において、ストレージ暗号化機能に使用される暗号鍵 KEK の鍵材料は現地交換不可な QSPI Flash に保存され、セキュリティ強化設定状態に関わらず TOE の基本制御に関わる設定情報を含む各データの保護に利用される。KEK 及び DEK 鍵の保存先と破棄タイミングを Table7-8 に示す。

管理者はガイダンスで TOE の廃棄時に全データ上書き削除機能を実施することを案内されている。

Table 7-8 鍵の保存先と破棄

鍵		保存先	破棄タイミング	破棄の方法
KEK	鍵材料	QSPI Flash	TOE 破棄時	0x00 で 1 回上書き削除
	鍵導出関数により鍵材料から生成した鍵	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除
DEK	鍵(暗号化された状態)	QSPI Flash	TOE 破棄時	0x00 で 1 回上書き削除
	鍵(平文)	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除

7.4. 高信頼通信機能

FPT_SKP_EXT.1

TOE の高信頼通信機能で使用されるすべての事前共有鍵、対称鍵、及びプライベート鍵は RAM 及び SSD のコントローラ領域に保存される。SSD のコントローラ領域は暗号化ファイルシステムにより保護されている(詳細はストレージ暗号化機能の TSS を参照)。また、RAM 及び SSD に保存された暗号鍵にアクセスするインターフェースは存在しない。

以上のことから暗号鍵は保護されていると考えられる。

FCS_CKM.1(a)

TOE は、Web Connection の PKI 設定による IPsec 通信の鍵確立で用いる IPsec 証明書の生成において、NIST SP800-56B, Revision 2 の 6.3.1.3 節に記載の rsakpg1-crt 方式に記載の方法で、鍵長 2048bit の RSA 非対称鍵を生成する。また、IPsec 通信(FTP_ITC.1 参照)の鍵確立において、NIST SP800-56A, Revision 3 の 5.6.1.1.1 節に記載の Using the Approved Safe-Prime Groups に記載の方法で、Diffie-Hellman グループ 14 による非対称鍵を生成する。

FCS_CKM.1(b)

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

FCS_RBG_EXT.1

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

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

FCS_COP.1(a)

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

FTP_TRP.1(a)

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 7-9 管理者が利用できる高信頼パス(FTP_TRP.1(a))

通信先	暗号化対象となる通信内容・機能	プロトコル
クライアント PC	ブラウザによる Web Connection の利用	IPsec

FTP_ITC.1

TOE は IT 機器との通信において暗号化通信を行う。TOE が提供する暗号化通信は以下の通りである。(セキュリティ強化設定が有効な場合)

Table 7-10 TOE が提供する暗号化通信

通信先	プロトコル	暗号アルゴリズム	関連するインターフェース
ファイルサーバー(FTP)	IPsec	AES(128bits、256bits)	操作パネルからスキャン機能の実行
ファイルサーバー(WebDAV)	IPsec	AES(128bits、256bits)	操作パネルからスキャン機能の実行
ファイルサーバー(SMB)	IPsec	AES(128bits、256bits)	操作パネルからスキャン機能の実行
監査ログサーバー(syslog)	IPsec	AES(128bits、256bits)	Table 7-14 参照

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

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
    ※上記の選択によって、メッセージダイジェスト長が 160 ビットで鍵長 160 ビットの HMAC-SHA-1、メッセージダイジェスト長が 256 ビットで鍵長 256 ビットの HMAC-SHA-256、メッセージダイジェスト長が 384 ビットで鍵長 384 ビットの HMAC-SHA-384、メッセージダイジェスト長が 512 ビットで鍵長 512 ビットの HMAC-SHA-512 のいずれかに従い、鍵付きハッシングによるメッセージ認証符号(HMAC)を用いた通信を行う。
    ※ハッシュアルゴリズムは FCS_COP.1(c)に従う SHA-1, SHA-256, SHA-384, SHA-512 (ISO/IEC

10118-3:2004 に準拠)を使用
※ESP では拡張シーケンス番号(ESN)をサポートしている。

- 鍵交換方式:IKEv1

<IKEv1 使用時の設定>

- IKEv1 暗号化アルゴリズム:AES_CBC-128、AES_CBC-256
- IKEv1 認証アルゴリズム:ISO/IEC 10118-3:2004 に準拠する SHA-1、SHA-256、SHA-348、SHA-512
- ネゴシエーションモード:Main Mode
- フェーズ 1(メインモード)鍵有効時間:600～86,400 秒
- フェーズ 2(クイックモード)鍵有効時間:600～28,800 秒
- Diffie-Hellman Group:グループ 14

- ピア認証方式:デジタル署名(RSA デジタル署名アルゴリズム(rDSA) 2048bit、FIPS PUB 186-4, "Digital Signature Standard"に準拠)、ハッシュアルゴリズム:SHA-256(ISO/IEC 10118-3:2004 に準拠)、事前共有鍵

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 Any のプロトコル、通信先 IP アドレス(個別、またはサブネット指定)が設定できる。IPsec ポリシーは IP ポリシーグループ 1~10 の 10 グループまで設定でき、送信、受信の両方のパケットに適用される。1 つの通信相手に、複数の IPsec ポリシーが設定された場合、IPsec ポリシーグループ 1～10 の登録順序に関わらず、下記の優先順位で動作が適用される。
  優先度:高　保護 ＞ 破棄 ＞ 通過　優先度:低
- デフォルトアクション: IPsec ポリシーに合致する設定がなかった場合の動作を下記から選択できる。(この設定について管理者に対し、破棄を選択する様ガイダンスで案内している。)
  - 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

FIA_PSK_EXT.1

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

- テキストベースの事前共有鍵
  - 長さ:22 文字
  - 利用可能文字:ASCII 文字列(アルファベットの大文字と小文字、数字、及び特殊文字("!", "@", "#", "$", "%", "^", "&", "*", "(", ")")を組み合わせた文字列)、または HEX 値
  - 条件付けの方法:SHA-1、SHA-256、SHA-384、SHA-512

FCS_CKM.4, FCS_CKM_EXT.4

TOE において、高信頼通信機能に使用される暗号鍵及びその鍵材料は SSD のコントローラ領域もしくは RAM に保存され、保護通信確立時の鍵交換、認証、あるいは通信の暗号化に利用される。IPsec 通信で利用する鍵、鍵材料の保存先と破棄の方法を Table 7-11 に示す。管理者によって設定された事前共有鍵、IPsec 証明書のプライベート鍵は、SSD に保存され、不要となるタイミングは TOE を廃棄する時に限定される。TOE の廃棄時には管理者に全データ上書き削除機能を実施することをガイダンスで案内されている。全データ上書き削除機能では、暗号鍵及び鍵材料保存領域を固定値(0)で 1 回上書き処理を行う。IPSec などで使用されるセッション鍵(一時的な暗号鍵)は RAM 上に保存される。これらは TOE の副電源 OFF により不要になるため削除される。

Table 7-11 鍵の保存先と破棄

鍵	保存先	破棄タイミング	破棄の方法
IPsec 証明書の鍵ペア	SSD	TOE 破棄時	0x00 で上書き削除
IPsec 事前共有鍵	SSD	TOE 破棄時	0x00 で上書き削除
IPsec cookie/nonce	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除
IKE 用共有秘密鍵（IKEv1 フェーズ 1 で生成される）	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除
IPsec 用共有秘密鍵（IKEv1 フェーズ 2 で生成される）	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除
IPsec の Diffie-Hellman 共有鍵	RAM	鍵が不要となる時(TOE の副電源遮断時)	TOE の副電源遮断により RAM から削除

7.5. セキュリティ管理機能

FMT_MOF.1, FMT_SMF.1, FIA_UID.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1

TOE は利用者に対して下記の管理機能を提供する。それぞれの管理機能は記載されたインターフェースからのみ操作可能である。操作パネルで下記の管理機能を実行する画面に遷移する際には TOE への識別認証が要求され、未認証で管理機能を利用することはできない。識別認証成功時には利用者に役割（U.ADMIN、U.NORMAL）を関連付け、それぞれの役割に提供される機能の利用を許可する。また、関連付けられた役割はログアウトまで維持される。利用者の役割に提供されていない管理機能を利用することはできない。TOE は、Table 6-2、Table 6-3 のアクセス制御において、利用者文書データ、利用者ジョブデータを作成した利用者の User ID を Job owner として割り当てる。TOE は割り当てられる User ID を上書きする機能を持たない。

Table 7-12 U.ADMIN に提供される管理機能

管理機能	内容	許可された操作	操作可能なインターフェース
セキュリティ強化設定機能	セキュリティ強化設定の有効化／無効化を行う。	変更	操作パネル
監査ログ送信先設定機能	監査ログ送信設定（送信先サーバーの IP アドレス等のネットワーク設定）を行う。	変更	操作パネル
ユーザー管理機能	U.ADMIN は User ID を持つユーザーの登録、変更、削除ができる（U.ADMIN による U.NORMAL のログインパスワードの設定機能もこれに含まれる）。ユーザーの登録において Table 6-2、Table 6-3 に記載された利用者データアクセス制御に基づいて、属性に適切な初期値が設定される。	変更、削除、作成	操作パネル
U.ADMIN のログインパスワード変更機能	U.ADMIN が U.ADMIN のパスワードを変更する。	変更	操作パネル
日時情報の変更機能	日時情報を設定する。	変更	操作パネル
パスワード規約の変更機能	パスワード規約（パスワード最小文字数設定）の設定・変更を行う。	変更	操作パネル
ネットワーク設定の登録・変更機能	ネットワーク設定（TOE の IP アドレス、DNS サーバーの IP アドレス、ポート番号等、NetBIOS 名、IPsec 設定等）の設定・変更を行う。	変更	操作パネル

管理機能	内容	許可された操作	操作可能なインターフェース
暗号化パスワードの設定・変更機能	ストレージ暗号化機能で使用する暗号鍵(KEK)のもととなるデータである暗号化パスワードを設定・変更する。	変更	操作パネル
ファームウェアアップデート機能	TOE のファームウェアアップデートを実施する。	実行	操作パネル
全データ上書き削除機能	暗号鍵及び鍵材料保存領域を固定値(0)で 1 回上書き処理を行う	実行	操作パネル
サービスログイン許可設定機能	サービスモード利用の許可／禁止の設定を行う	変更	操作パネル

Table 7-13 U.NORMAL に提供される管理機能

管理機能	内容	許可された操作	操作可能なインターフェース
U.NORMAL のログインパスワードの設定機能	U.NORMAL が自身のログインパスワードの設定を行う。	変更	操作パネル

7.6. 監査機能

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

FAU_GEN.1, FAU_GEN.2

TOE は、以下の事象を監査対象事象とし、事象発生時刻(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 7-14 監査対象事象一覧

監査対象事象	ID (サブジェクト識別情報 *1)	結果	関連するインターフェース
管理者認証の実施	Admin ID	OK/NG	FIA_UAU.1, FIA_UID.1 参照
管理者パスワードの変更/登録	Admin ID	OK	Table 7-12 参照
ユーザー認証の実施	User ID / 未登録 ID	OK/NG	FIA_UAU.1, FIA_UID.1 参照
管理者によるユーザーの作成	Admin ID	OK	Table 7-12 参照
管理者によるユーザーパスワードの変更／登録	Admin ID	OK	Table 7-12 参照
管理者によるユーザーの削除	Admin ID	OK	Table 7-12 参照
管理者によるユーザーの属性変更	Admin ID	OK	Table 7-12 参照
ユーザーによるユーザーの属性変更(ユーザーパスワード変更など)	User ID	OK	Table 7-13 参照
セキュリティ強化設定の変更	Admin ID	OK/NG	Table 7-12 参照
パスワード規約設定の変更	Admin ID	OK	Table 7-12 参照
ネットワーク設定の変更	Admin ID	OK	Table 7-12 参照
サービスログイン許可設定の変更	Admin ID	OK	Table 7-12 参照
監査ログ送信先設定の変更	Admin ID	OK	Table 7-12 参照

監査対象事象	ID (サブジェクト識別情報 *1)	結果	関連するインターフェース
HDD 暗号化パスワードの変更	Admin ID	OK	Table 7-12 参照
ファームウェアアップデート機能(ISW)の実行	Admin ID	OK/NG	Table 7-12 参照
ファームウェア診断の実施	Admin ID / 未登録 ID	OK/NG	FPT_TST_EXT.1 参照
日時設定	Admin ID	OK	Table 7-12 参照
監査機能の起動	未登録 ID	OK	副電源
監査機能の終了	未登録 ID	OK	副電源
保存ジョブの削除	User ID / Admin ID	OK	FDP_ACC.1, FDP_ACF.1 参照
コピージョブの印刷	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
コピージョブの保存	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
スキャンジョブの実行	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
保存ジョブの印刷	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
保存ジョブの変更／再保存(移動・複製)	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
保存ジョブの読出し	User ID	OK/NG	FDP_ACC.1, FDP_ACF.1 参照
IPsec セッション確立の失敗	未登録 ID	errNo(*2)	FTP_ITC.1 参照

(*1)識別認証前に発生した監査対象事象にはサブジェクト識別情報として未登録 ID という固定値を記録する

(*2)IPsec セッション失敗要因を示すエラー情報を記録する

FAU_STG_EXT.1

記録された監査ログ情報は TOE 内で保持された後、管理者が設定した外部監査サーバー(syslog)に従いログファイルの送信を行う。ログ送信タイミングなどは Table 7-15 を参照のこと。

Table 7-15 監査ログ情報の仕様

監査ログ情報の取り扱い	概要
ログ情報の保管領域	ストレージ暗号化機能にて暗号化された SSD 領域
ログ情報送信タイミング	監査対象事象発生時(即時)
送信対象となるログ情報	発生したイベントに関するログ情報
送信失敗時の処理	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ない場合、SSD(*1)に一時保存を行う。最大 10000 件。ログ情報が 10000 件到達時には以降の情報は破棄される。なお一時保存された情報はサーバーとの通信回復時に送信され、併せて SSD 上の情報を削除する。

(*1)Table 7-6 に示された SSD 上のログ保存領域に一時保存される。保存された情報はファイルシステムにより暗号化することにより不正アクセスから保護を行う。詳細は FDP_DSK_EXT.1 の TSS を参照のこと。また TOE はログ情報の保管領域へアクセスするユーザーインターフェースは提供していない為、ログ情報を読みだす手段は存在しない。

FPT_STM.1

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

はクロック機能から提供される。

7.7. アップデートデータ検証機能

FPT_TUD_EXT.1

TOE は管理者のみに以下の機能の実施を許諾する。

- ファームウェアバージョン確認機能
- ファームウェアアップデート機能

管理者は識別認証後管理者設定画面において、もしくは Web Connection から識別認証後に web ブラウザにおいてファームウェアバージョンの確認を実行できる。

また、管理者は識別認証後、管理者設定画面においてファームウェアアップデート機能を実行できる。TOE はファームウェアアップデート実施時、データ転送後のプログラムチェックとして、ファームウェアファイルに含まれるコニカミノルタのデジタル署名を用いてファームウェアファイルの検証を行う。検証の結果問題ないと判断された場合のみ FW の書き換え処理を実施する。(この時、ファームウェアのハッシュ値を計算し SSD の暗号化ファイルシステム内にそのハッシュ値の保存を行う処理も行う。このハッシュ値データは後述する自己テスト機能にて使用する。)デジタル署名検証が失敗した場合、TOE は操作パネルに警告を表示しアップデート処理を中止する。

FCS_COP.1(b), FCS_COP.1(c)

TOE は以下のようにしてデジタル署名検証を用いたファームウェアファイルの検証を行う。

1. ファームウェアファイルにはデジタル署名データとファームウェアデータが含まれる。デジタル署名データは RSA デジタル署名アルゴリズム(rDSA) 2048bit、FIPS PUB 186-4, “Digital Signature Standard”に準拠。
2. TOE が持つ公開鍵にてデジタル署名データを復号化する。
3. 先ほど復号化したデータと、ファームウェアデータを ISO/IEC 10118-3:2004 に準拠する SHA-256 によるハッシュ値の算出したものを比較する。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

7.8. 自己テスト機能

FPT_TST_EXT.1

TOE は副電源 ON すると、まず本体制御ファームウェア、ネットワーク制御ファームウェアの順にファームウェア自己テストの実施を行った後 FW を読み込む。セキュリティ機能の制御を行うファームウェアである本体制御ファームウェア及びネットワーク制御ファームウェアのハッシュ値を計算し、ファームウェア検証時に SSD に記録したハッシュ値データとの一致を確認することで改ざんの有無を検知し TSF 実行コードの完全性を検証する。この時 TOE で使用している暗号化ライブラリもハッシュ値検証の対象となっているため、こちらも完全性が検証される。検証が失敗した場合 TOE は操作パネルに警告(SC コード)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。上記以外のファームウェアについては TSF データに対するアクセス手段及びセキュリティ機能実行能力を持っておらず、TSF データに対するアクセス手段を持っていないことから、ファームウェア検証機能から除外している。

検証が失敗した場合 TOE は操作パネルに警告(SC コード)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。

上記の処理により TSF のふるまいを決定するファームウェアの完全性を確認できるため、TSF が正しく動作していることを実証するために十分なものであるといえる。

以上