KONICA MINOLTA

AccurioPress 6136P

Security Target

Version 1.01

2018/11/21

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
2018/08/31	1.00	情報機器事業開発本部 システム制御開発センター 第1システム制御開発部	工藤	工藤	安加賀	初版
2018/11/21	1.01	情報機器事業開発本部 システム制御開発センター 第1システム制御開発部	工藤	工藤	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　　：　AccurioPress 6136P Security Target
・STバージョン　：　1.01
・作成日　　：　2018年11月21日
・作成者　　：　コニカミノルタ株式会社

1.2. TOE reference

・TOE名称　　：　AccurioPress 6136P
・バージョン　　：　G00-20
・製造者　　：　コニカミノルタ株式会社

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プリンタである。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)で使用されるプリンタであり、プリンタ機能、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 にはファクス機能は搭載していない。

1.3.2. TOE の使用方法

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

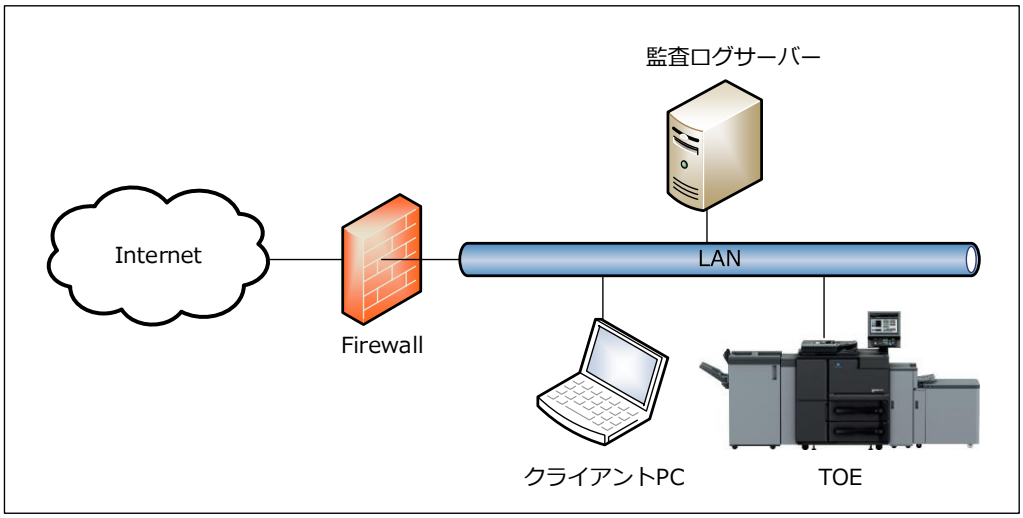


Figure 1-1 TOE の利用環境

TOE は Figure 1-1 TOE の利用環境に示すように 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。以下に TOE と TOE 以外のハードウェア、ソフトウェアについて記述する。

(1) TOE(プリンタ本体)
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
- 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
LAN に接続することによって TOE のクライアントとして動作する。
利用者は、クライアント PC にプリンタドライバをインストールすることで、クライアント PC から TOE にアクセスし以下の操作を行うことができる。
- 電子文書の蓄積・印刷

また、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

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

1.3.3. TOE に必要な TOE 以外のハードウェア／ソフトウェア

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

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)	Windows7 Professional SP1 (64 ビット)
クライアント PC (Web ブラウザ)	Firefox 63.0.1
クライアント PC (プリンタドライバ)	KONICA MINOLTA AccurioPress 6136 / 6120 / 6136P ドライバ PS Plug-in Ver 2.0.358, PCL Ver.2.0.5.0
監査ログサーバー	Apache httpd 2.4.23 (WebDav)

1.3.4. TOE の主要なセキュリティ機能

TOE は、ユーザーが生成したドキュメントデータを印刷、保存し、また LAN を経由してファイルサーバーなどの IT 機器にドキュメントデータを送信する。TOE はこれらドキュメントデータの不正な暴露や改ざんより保護するため以下のようなセキュリティ機能を備える。

- 識別認証機能
- データアクセス制御機能
- 利用者制限制御機能
- セキュリティ管理機能
- アップデートデータ検証機能
- 自己テスト機能
- ネットワーク通信保護機能
- 監査ログ機能
- ストレージ暗号化機能
- 暗号鍵鍵材料保護機能

1.4. TOE description

本章では TOE の物理的範囲、論理的範囲の概要を記述する。

1.4.1. TOE の物理的範囲

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、プリンタユニット、制御基板、HDD・SSD、USB I/F、Network I/F から構成されるプリンタである。

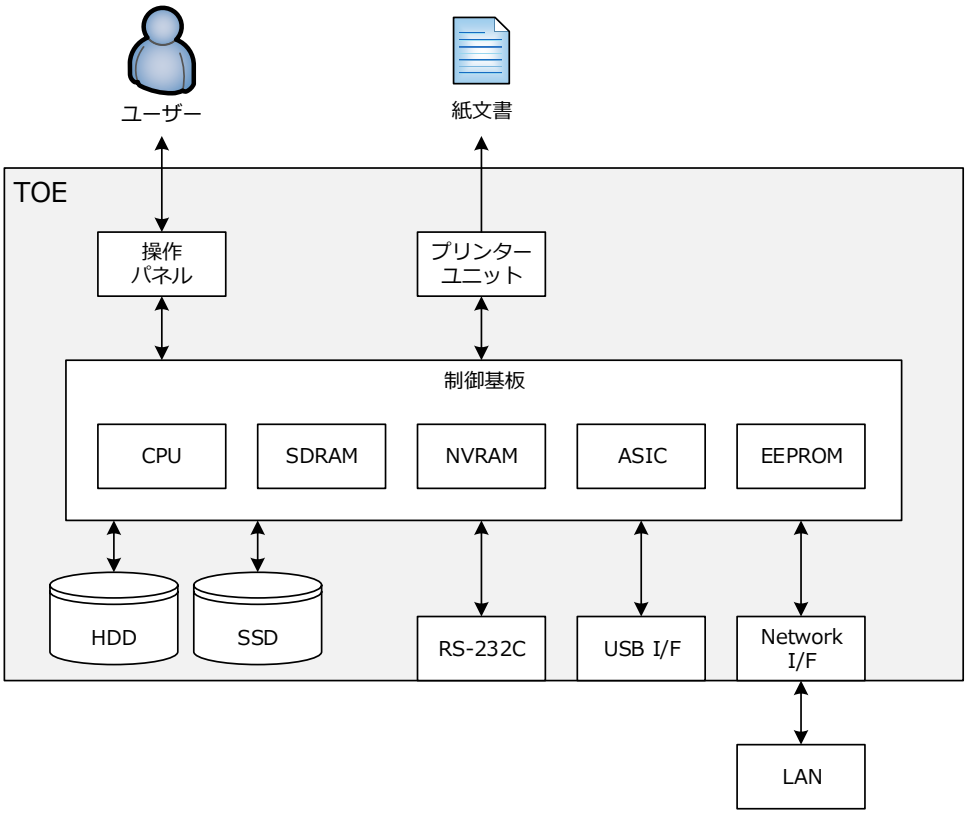


Figure 1-2 TOE の物理的範囲

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	プリンタユニット	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。
3	制御基板	TOE を制御する装置。
4	CPU	中央演算処理装置。
5	SDRAM	作業領域として利用される揮発性メモリ。
6	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。
7	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。
8	EEPROM	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。
9	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。
10	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。
11	Network I/F	10BASE-T、100BASE-TX、Gigabit Ethernet をサポートするインターフェース。
12	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
画像制御系	I1~I5	画像制御処理及び操作部制御
音源系	T	操作部音声データ
ブラウザ	W	ブラウザ処理
プリンタ系	C	プリンタ基板制御
コントローラ	P1~2	プリンタコントローラ制御

1.4.1.3. ガイダンス

以下にガイダンスの一覧を示す。ガイダンスは html あるいは PDF 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.
AccurioPress 6136 / 6136P / 6120 ユーザーズガイド	1.00
AccurioPress 6136 / 6136P / 6120 ユーザーズガイド　セキュリティー機能編(管理者)	1.00

AccurioPress 6136 / 6136P / 6120 ユーザーズガイド　セキュリティー機能編(ユーザー)	1.00

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 を構成するプリンタ本体の識別は以下の通りである。
プリンタ本体は 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。

Table 1-5 TOE の構成要素

構成要素	識別
プリンタ本体	AccurioPress 6136P

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。

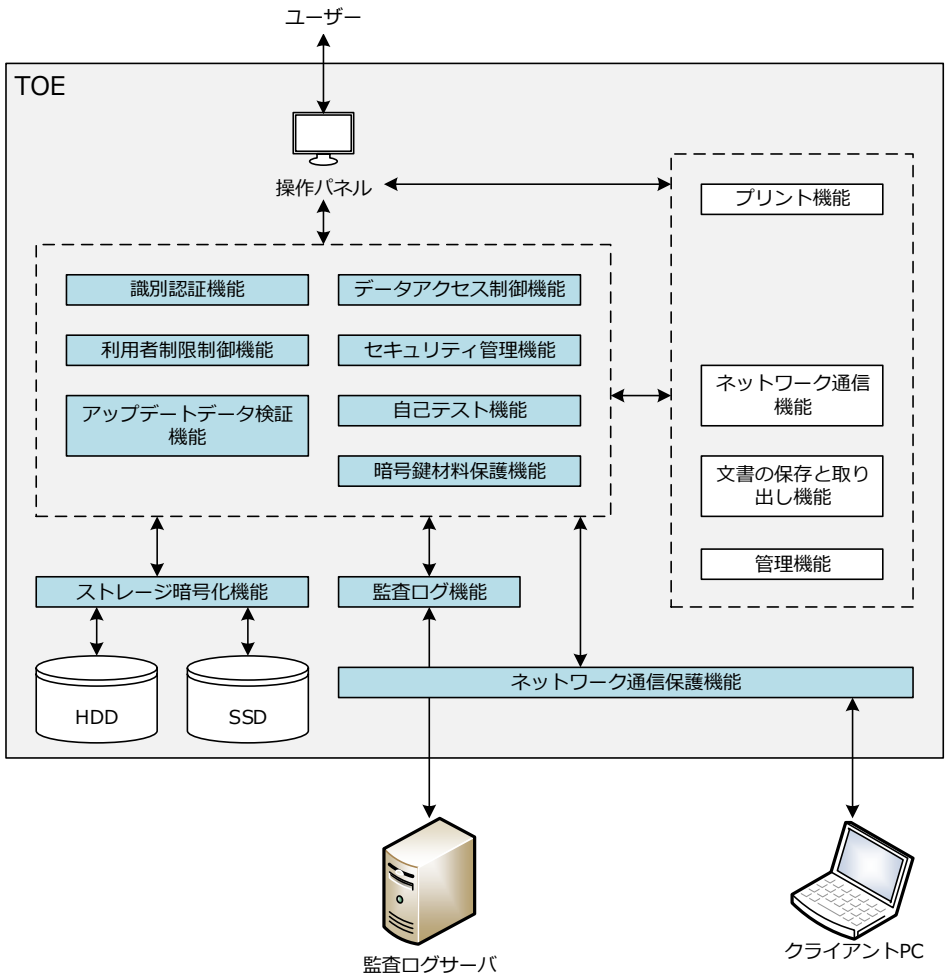


Figure 1-3 TOE の論理的範囲

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	プリント機能	クライアントから LAN を経由して受信したドキュメントデータを印刷、あるいは HDD に保存する機能。
2	管理機能	TOE は、認証された管理者だけがパネルから操作することが可能な管理者設定画面において各種設定の管理などの機能を提供する。管理者は、管理者機能を使用して、TOE が有する機能の動作設定を行う。管理者機能によりプリンタ枚数の管理、トラブルシューティング及びトナーの管理など、TOE の運用に関わる情報を管理する。
3	文書の保存と取り出し機能	HDD にドキュメントデータを保存、あるいは蓄積したドキュメントデータを取り出す機能。

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 TOE の許可利用者であるかどうかをユーザー名とパスワードによって検証し、TOE の許可利用者であることが確認できた場合に TOE の利用を許可する機能。認証方法は本体認証のみが使用可能。
2	データアクセス制御機能	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蓄積文書への操作を許可する機能。
3	利用者制限制御機能	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操作権限に基づいて、印刷機能、スキャン機能、コピー機能、文書の保存と取り出し等の機能、および、実行中のジョブに含まれる蓄積文書以外の文書への操作の制御をする機能。
4	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。セキュリティ強化モード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。
5	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
6	自己テスト機能	TSF 実行ファームウェア及びデバイスが正常であることを TOE の起動時に検証する機能。
7	ネットワーク通信保護機能	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と TOE の間の通信データを暗号化する。
8	監査ログ機能	TOE の使用およびセキュリティに関連する事象（以下、監査事象という）のログを

		日時情報等とともに監査ログとして記録し、記録した監査ログを監査できる形式で提供する機能。監査ログ情報は保存のため外部監査ログサーバーにセキュアに送信される。
9	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。
10	暗号鍵材料保護機能	ストレージ暗号化機能で用いた鍵材料を保護する機能。

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
ドキュメントデータ	ドキュメントデータは、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、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、AccurioPress 6136P 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ボタンの名称である。
内部ネットワーク	内部ネットワークは、AccurioPress 6136P を導入する組織の LAN である。クライアント PC や各種サーバー(例えば webDav サーバーなど)が接続されている。
外部ネットワーク	外部ネットワークは、上記で定義された「内部ネットワーク」以外のネットワーク(例えばインターネットなど)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。セキュリティ強化モード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。
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	管理者が設定する時間。この時間が経過すると自動的にログアウトする。操作パネルからの操作が対象。
ジョブ	ハードコピー装置に送出される文書処理タスク。単一の処理タスクは 1 本以上の文書を処理できる。

Designation	Definition
セキュリティ強化モード	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、セキュリティ強化モードが有効になっている状態のみが TOE としての環境である。
プリントジョブ投入機能	TOE がクライアント PC から送信されたユーザー名、ログインパスワード、印刷データを受け入れる機能。ユーザー名、ログインパスワードによる識別認証が成功した場合のみ印刷データを受け入れる。
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／削除、権限の付与／削除／変更を行う機能。
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、セキュリティ強化モード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 は暗号化ワードを使用して暗号鍵を生成する。
監査ログ管理機能	監査ログ満杯時の動作の設定を行う機能。
監査ログ機能	監査ログを取得する機能。
高信頼チャネル機能	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
高信頼チャネル管理機能	高信頼チャネル機能の実行のほか、SSL/TLS サーバー証明書や暗号方式の管理を行う機能。
時刻情報	時刻の情報。監査対象事象が発生した場合、この時刻情報が監査ログに記録される。
ISW	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。セキュリティ強化モード時は USB メモリを使用した更新のみ実施できる。
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。
認証＆プリント機能 (AUTH PRINT)	ネットワーク上のコンピューターから送信されたユーザー名、パスワードを伴う文書をプリント指示された文書として保存する機能。

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

Required Uses

本 TOE はプリント機能に加え、ネットワーク通信、管理機能を持つハードコピー装置（以下、HCD と言う）である。このことから PP が求める必須用途をサポートしている。またこれらの必須用途と関連する要件全てについて適合を主張するものである。

Conditionally Mandatory Uses

本 ST は HCD-PP の「1.3.1.2 Conditionally Mandatory Uses」記載の要件のうち、「Storage and retrieval」「Field-Replaceable Nonvolatile Storage」をサポートしており、B.1.1 FPT_KYP_EXT.1、B.1.2 FCS_KYC_EXT.1、B.1.3 FDP_DSK_EXT.1 との適合を主張するものである。

Communications protocol

本 ST では、外部 IT エンティティとの間に、セキュアな通信プロトコルとして IPsec を実装しており、D.2.1 FCS_IPSEC_EXT.1、D.2.5 FCS_COP.1(g)、D.2.6 FIA_PSK_EXT.1 との適合を主張するものである。

Optional Uses

本 ST では HCD-PP の「1.3.1.3 Optional Uses」記載のオプション用途を選択しない。

Exact Conformance

本 ST のセキュリティ要件は、PP のセキュリティ要件に対して正確適合しており、具体化している箇所があるが、PP とは一貫している。

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_COMPROMIS E	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_ UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMIS E	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_PROTECT ION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRY PTION	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. FAU_CKM_EXT Extended: Cryptographic Key Management

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

Component leveling:

FCS_CKM_EXT.4: Extended: Cryptographic Key Material Destruction	4

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

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

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

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

5.3. FCS_IPSEC_EXT Extended: IPsec selected

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

Component leveling:

FCS_IPSEC_EXT.1 Extended: IPsec selected	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to : No other components

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

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

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

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

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

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

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

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

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

5.4. FCS_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, 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*].	

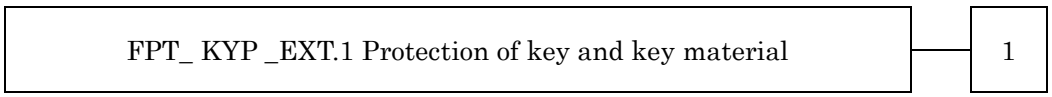
Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

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.

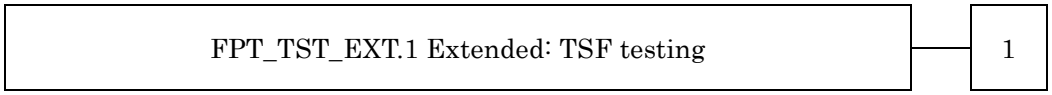
This extended component protects the TOE by means of strong authentication using Preshared Key, and it is therefore placed in the FPT class with a single component.

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 で操作完了または詳細化したことを示す。
- ***イタリック且つボールドで示される表記***は、本 ST で“割付”、または“選択”されていることを示す。
- 青文字は、“割付”、または“選択”を行った結果を示す。
- アンダーラインで示される原文の直後に***括弧書きでイタリック且つボールドで示される表記***は、アンダーラインされた原文箇所が本 ST で“詳細化”されていることを示す。
- ラベルの後に括弧付けで示される番号は、当該機能要件が本 ST で“繰返し”されて使用されていることを示す。

■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 information	Details
Job completion	FDP_ACF.1	Type of job	・プリントジョブの完了 ・プリントジョブの保存

			・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
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	・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), FTP_TRP.1(b)	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) The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in

Refinement: 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

FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to : No other components.

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

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

[selection: 128 bit, 256 bit]

- 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

- ***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*]

- Refer to Table 6-2

[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*]

- Refer to Table 6-2

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)] with a minimum of [selection: *128 bits, 256 bits*]

- Refer to Table 6-2

[assignment: *number of hardware-based sources*]

- Refer to Table 6-2

[selection: 128 bits, 256 bits]

- 256 bits

Table 6-2 Cryptographic Operation (Random Bit Generation)

用途	乱数生成サービス	ソフトウェアベースのノイズ源	ハードウェアベースのノイズ源
ディスク上のデータ保護	HMAC_DRBG (SHA-256) SP800-90A	0	1
ネットワーク通信の暗号化	HMAC_DRBG (SHA-256) SP800-90A	0	1

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 6-3 and Table 6-4**.

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 6-3 and Table 6-4**.

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 6-3 and Table 6-4.***

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*]

- U.ADMIN はすべての D.USER.DOC、D.USER.JOB の削除が可能

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 6-3 D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	**Operation :**	***Submit a document to be printed***	**View image or Release printed output**	***Modify stored document***	***Delete stored document***
	Job owner	(note 1)	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】 Table6-3 は、下記の状況での SFP を記述している。

- **Print :** 利用者が、プリンタドライバの出力を、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印刷データに対する SFP。プリント出力操作は、プリンタドライバから直接プリントする操作の他、印刷データを HDD 保存

し、HDD 保存されたデータをプリント出力する操作が可能である。

- **Storage / retrieval：**
  利用者が、プリンタドライバの出力画像データを 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、画像データに対する SFP。

※「HDD 保存」は、保存場所や保存方法の違いによって、一時保存や機密保存と呼ばれる場合もある。
※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
※本 TOE はスキャン装置を搭載していないため「Scan」「Copy」時の操作及びアクセス制御は存在しない

Table 6-4 D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	**Operation：**	***Create print job***	**View print queue / log**	***Modify print job***	***Cancel print job***
	Job owner	(note 1)		denied	
	U.ADMIN	denied		denied	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】 Table6-4 は、下記の状況での SFP を記述している。

- **Print：** 利用者が、プリンタドライバの出力を、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ジョブデータに対する SFP。プリント出力操作は、プリンタドライバから直接プリントする操作の他、印刷データを HDD 保存し、HDD 保存されたデータをプリント出力する操作が可能である。
- **Storage / retrieval：**
  利用者が、プリンタドライバの出力画像データを 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。

※「HDD 保存」は、保存場所や保存方法の違いによって、一時保存や機密保存と呼ばれる場合もある。
※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
※本 TOE はスキャン装置を搭載していないため「Scan」「Copy」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 6-5

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 6-5

[assignment: *list of actions*]

- Refer to Table 6-5

Table 6-5 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
印刷ポートでの認証	met	なし

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)

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

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

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*]
- modify the behaviour of

[assignment: *list of functions*]
- セキュリティ強化モードの設定
- サービスログイン許可設定機能
- 監査ログ機能
- 高信頼チャネル機能
- ユーザー管理機能

FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to : No other components
Dependencies : [FDP_ACC.1 Subset access control, ~~or FDP_IFC.1 Subset information flow control~~]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised*

identified roles].

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

- Refer to Table 6-6

[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	query, modify, create

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]*] default values for security attributes that are used to enforce the SFP.

- restrictive

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

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

- no role

FMT_MTD.1 Management of TSF data

(for O.ACCESS_CONTROL)

Hierarchical to : No other components

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

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6-7, Table 6-8 and Table 6-9.**

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	U.ADMIN, the owning U.NORMAL.
U.NORMAL のユーザー名	Modify	U.ADMIN

Table 6-8 Operation of TSF Data (2)

TSF Data *not owned by a U.NORMAL*

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

Table 6-9 Operation of TSF Data (3)

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

TSF Data	Operations	Authorized Roles
日時情報	query, modify	U.ADMIN
暗号化ワード	modify	U.ADMIN
パスワード規約	query, modify	U.ADMIN
ネットワーク設定	query, modify	U.ADMIN
監査ログサーバー設定	query, 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の管理機能
U.ADMIN による監査ログ管理機能
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 による監査ログ手動出力
U.ADMIN による暗号化ワードの設定・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 によるファームウェア診断機能の実施
U.ADMIN によるデバイス診断機能の実施
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
  - 管理者は最終操作による処理が完了してから 30 分間
- プリンタドライバの場合、対話セッションはない
- 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]

- 監査ログサーバー(WebDAV)

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***]

- 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**.

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

(for O.COMMS_PROTECTION)

Hierarchical to : No other components

Dependencies : [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) Refinement: The TSF shall **use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

[selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS]

- IPsec

FTP_TRP.1.2(b) Refinement: The TSF shall permit [selection: **the TSF, remote users**] to initiate communication via the trusted path.

[selection: **the TSF, remote users**]

- remote users

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

< 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 The TSF shall not store plaintext keys that are part of the keychain specified by

Refinement 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*]

- 128bits
- 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: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*]

- *with no support for NAT traversal*

[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***]

- Refar to Table 6-11

Table 6-11 cryptographic hashing services

用途	暗号ハッシュサービス
IPsec IKEv1 認証アルゴリズム	SHA-1, SHA-256, SHA-384, SHA-512

鍵導出関数に使用する PRF の生成	SHA-256
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	SHA-256

< 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*]

- 384bit

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.

].

[

・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.

]

- CBC: IVs shall be non-repeating

6.2. Security assurance requirements

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

Table 6-12 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 6-13 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) FCS_COP.1(d)	FCS_COP.1(a) 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(f) FCS_COP.1(g) FCS_COP.1(h) FCS_CKM_EXT.4 FCS_RBG_EXT.1	FCS_COP.1(f) FCS_COP.1(g) FCS_COP.1(h) FCS_CKM_EXT.4 FCS_RBG_EXT.1	
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	N/A
FCS_RBG_EXT.1	No dependencies.	No dependencies.	N/A
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A
FDP_ACF.1	FDP_ACC.1 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,	FCS_IPSEC_EXT.1	N/A

機能要件	依存関係	ST で満たす依存関係	依存関係を満たしていない要件
	or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]		
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1	N/A
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1	N/A
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
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	FCS_RBG_EXT.1	N/A
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	データアクセス制御機能
3	利用者制限制御機能
4	セキュリティ管理機能
5	アップデートデータ検証機能
6	自己テスト機能
7	ネットワーク通信保護機能
8	監査ログ機能
9	ストレージ暗号化機能
10	暗号鍵材料保護機能

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、あるいはプリンタドライバを用いてユーザー名とパスワードを TOE に入力する（webConnection 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）

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（webConnection 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（webConnection 使用時）を用いて管理者パスワードを TOE に入力する。プリンタドライバから管理者認証を行うことはできない。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

識別認証の全ての動作において、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(プリンタドライバなどの印刷ポートでの認証は除く)。

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(32 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 によるリモート管理機能実施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 にて TOE 設定の確認はできるが変更はできない)。

FIA_UAU.7

TOE は、利用者が操作パネル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 あるいはプリンタドライバ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。
- プリンタドライバの場合、対話セッションはない。プリンタドライバから要求された処理が受け付けられた際にログインし、その処理の完了直後にログアウトを行う。
- 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. データアクセス制御機能

FDP_ACC.1, FDP_ACF.1

TOE は Table 6-3、Table 6-4 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及びプリンタドライバ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

- 操作パネルでプリント、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。
- 利用者ジョブデータ及び利用者文書データへのアクセスは各データに保存された所有者情報と一致するタスク属性を持つ利用者(すなわち Job owner)だけに制限される。HDD 保存ジョブの一覧表示は利用者の User ID と所有者情報が一致するジョブのみが表示され、ジョブへの操作（閲覧、改変、削除）もログインした利用者の User ID と所有者情報が一致するジョブに対してのみ実行できる（他の利用者所有ジョブへの操作手段が提供されない）。
- 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。

(2) プリンタドライバ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

- プリントジョブの作成及び保存ジョブの作成操作のみが実行可能。プリンタドライバにてユーザー名とパスワードを入力することにより、データ送信タイミングに TOE にて識別認証が実施される。識別認証成功時にはプリンタドライバで指示された操作が実行されるが、識別認証失敗時には操作がキャンセルされ実行されない。
- 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。
- プリンタドライバでの識別認証において管理者パスワードではログインすることはできない（操作キャンセルとなる）。

7.3. 利用者制限制御機能

FIA_ATD.1

利用者は、識別認証成功時に FIA_USB.1 により利用者を代行するタスクのタスク属性(User ID、Admin ID) が関連付けられる。関連付けられたタスク属性はログアウトまで維持する。識別認証失敗時にはタスク属性の関連付けを行わない。

FDP_ACC.1, FDP_ACF.1

TOE はプリント、保存／取り出し機能の操作を行う利用者に対し識別認証を求める。検証の結果許可利用者・管理者と判断された者だけ、Table 6-3、Table 6-4 に記載された利用者データアクセス制御に基づき機能の操作を許可し、TOE の利用を許可する。なお、出力予約ジョブの状態一覧及びジョブ履歴（出力履歴／送信履歴／未出力履歴）一覧の確認操作については識別認証を求めない。

7.4. 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。及び利用者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。識別認証成功時には FIA_USB.1 により利用者に役割(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。関連付けられた役割は、ログアウトまで維持する。

Table 7-3 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
セキュリティ強化モード設定	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
監査ログ管理機能	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及びログファイルを置くディレクトリ設定)を行う。	変更	操作パネル
ユーザー管理機能	TOE へのタスク属性 UserID を持つユーザーの登録、削除、属性(権限)の登録・変更・削除を行う。ユーザーの登録において Table 6-3、Table 6-4 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.NORMAL のログインパスワードの設定機能	U.NORMAL のログインパスワードの設定を行う。	登録、変更	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も含む)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
監査ログ手動出力機能	任意のタイミングで監査ログを監査ログサーバーへ送信する。	変更	操作パネル
暗号化ワードの設定・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
ファームウェア診断機能	自己テスト機能のファームウェアに対する診断を任意のタイミングで実施する。	実行	操作パネル
デバイス診断機能	自己テスト機能のデバイスに対する診断を任意のタイミングで実施する。	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 7-4 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。	登録、変更	操作パネル

7.5. 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 デジタル証明アルゴリズム(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 SHA-256 でハッシュ値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

7.6. 自己テスト機能

FPT_TST_EXT.1

TOE は電源 ON すると、まず本体制御ファームウェア、コントローラ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コントローラ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機能時に 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。

上記処理終了後、続いてデバイスの自己テストとして本体制御ファームウェアが各デバイスを接続認識したタイミングにおいて、各デバイス上の特定データについて Read/write/verify を実施しデータの完全性を検証する(Table 7-5 参照)。

Table 7-5 各デバイスの自己テスト機能の検証内容

デバイス	検証内容
HDD	ジョブ保存領域(Table 7-15 参照)に 4Kbytes 分のデータを Read/write/verify の実施を行う。
SSD	SSD 上の特定ファイルのハッシュ値を計算し、ファームウェアにて保持している値（該当ファイルのハッシュ値を予め計算したもの）と比較することで検証を行う。
NVRAM	検証用の領域を 8bytes 分確保し、上記領域に Read/write/verify の実施を行う

いずれの機能についても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全ての要素(TSF を実施するファームウェアの完全性、及び TSF データを保存する SSD / HDD / NVRAM デバイスの動作)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。

7.7. ネットワーク通信保護機能

FPT_SKP_EXT.1

TOE のネットワーク通信保護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 SDRAM 及び HDD のコントローラ領域に保存される。HDD 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、SDRAM 及び HDD 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(b), FCS_RBG_EXT, FCS_COP.1(a)

TOE は暗号化アルゴリズムに 128bit 及び 256bit の AES-CBC を使用した通信の暗号化を行う。

TOE は 128bit 及び 256bit の対称暗号鍵の生成時に HMAC_DRBG を用いた乱数生成処理を実行する。

このとき、エントロピー値として intel CPU の RDRAND 命令をアセンブラ関数から呼び出して入手した 768bit 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（RSA BSAFE Crypto-C）の乱数生成関数(HMAC-DRBG)に入力することで乱数生成する。(詳細は 7.9 章 FCS_RBG_EXT.1 参照)

FCS_CKM.4, FCS_CKM_EXT.4

TOE において、ネットワーク通信保護機能に使用される暗号鍵及びその鍵材料は HDD のコントローラ領域もしくは SDRAM 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。鍵交換や認証に使用される鍵情報は HDD に保存され、不要となるタイミングは TOE を廃棄する時、及び暗号鍵の再生成時に限定される。TOE の廃棄時には管理者にデータ抹消機能を実施することをガイダンスで案内されている。データ抹消機能では、HDD の全領域に固定値(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)についてはセッション終了後に不要となるため、SDRAM 上に保存され TOE の電源 OFF と共にデータは削除される。

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

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

Table 7-6 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

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

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	プリンタドライバによって蓄積・印刷指示された電子文書の受信	IPsec

FCS_CKM.1(a)

TOE は非対称暗号鍵の生成において NIST SP800-56A Revision 2 の要件に適合した実装を行っている。Table 7-8 にセクションの対応必要性及び実装の有無を示す。IKE SA のネゴシエーション時に使用される

Table 7-8 SP800-56A Revision 2 セクションの対応必要性

NIST SP800-56A Section Reference	実装の有無	Rationale for deviation
5.4	yes	
5.5	yes	
5.6	yes	
5.6.2	yes	
5.6.2.1.2	yes	
5.6.2.2.1	yes	
5.6.2.2.2	yes	
5.6.2.1.5	yes	
5.6.2.2.3	yes	
5.6.3.1	yes	
5.6.3.2	yes	
5.6.3.3	yes	
5.8	no	Not needed for TOE operation, therefore not implemented.
6	yes	
7	no	Not needed for TOE operation, therefore not implemented.
9	no	Not needed for TOE operation, therefore not implemented.

FCS_IPSEC_EXT.1, FIA_PSK_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。
    ※ESP では拡張シーケンス番号(ESN)を使用している。
- 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
  - 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 デジタル証明アルゴリズム(rDSA) 2048bit、FIPS PUB 186-4, “Digital Signature Standard”に準拠)、事前共有鍵
- 認証方式:事前共有鍵
  - 事前共有鍵文字列:22 文字の文字列(ASCII 文字列、または HEX 値)
  - 認証アルゴリズム:SHA-1、SHA-256、SHA-384、SHA-512 ※FCS_COP.1(c)に従う暗号ハッシングサービスを使用

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。
- IP 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・拒否のうちどの動作を行うか選択できる。IP パケットの条件としては TCP や UDP 等のプロトコル、ポート、送信元 IP アドレス、送信先 IP アドレス等が設定できる。IP ポリシーは グループ 1~10 の 10 グループまで設定することができ、番号が小さいグループの設定が優先的に適応される。
- デフォルトアクション: IPsec ポリシーに合致する設定がなかった場合の動作を下記から選択できる。(この設定について管理者に対し、破棄を選択する様ガイダンスで案内している。)
  - 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

7.8. 監査ログ機能

TOE は監査ログを取得するとともに取得した監査ログサーバーに送信を行う。

FAU_GEN.1, FAU_GEN.2

TOE は以下の事象を監査対象事象とし、発生時にログを記録する。

Table 7-9 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
管理者認証の実施	Admin ID	OK/NG
管理者パスワードの変更/登録	Admin ID	OK
ユーザー認証の実施	User ID / 未登録 ID	OK/NG
管理者によるユーザーの作成	Admin ID	OK
管理者によるユーザーパスワードの変更／登録	Admin ID	OK
管理者によるユーザーの削除	Admin ID	OK
管理者によるユーザーの属性変更	Admin ID	OK
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
セキュリティー強化モードの設定／変更	Admin ID	OK/NG
HDD ロックパスワードの変更	Admin ID	OK
パスワード規約設定の変更	Admin ID	OK
ネットワーク設定の変更	Admin ID	OK
サービスログイン許可設定の変更	Admin ID	OK
監査ログの出力(手動/自動共)	Admin ID	OK/errNo
監査ログ送信先設定の変更	Admin ID	OK

監査対象事象	ID (サブジェクト識別情報 *1)	結果
HDD 暗号化機能の起動	未登録 ID	OK
HDD 暗号化設定の変更	Admin ID	OK
HDD 暗号化パスワードの変更	Admin ID	OK
ISW の実行	Admin ID	OK/NG
ファームウェア診断の実施	Admin ID / 未登録 ID	OK/NG
デバイス診断の実施	Admin ID / 未登録 ID	OK/NG
日時設定	Admin ID	OK
監査機能の起動	Admin ID / 未登録 ID	OK
監査機能の終了	Admin ID / User ID / 未登録 ID	OK
保存ジョブの削除	User ID / Admin ID	OK
プリントジョブの印刷	User ID	OK/NG
プリントジョブの保存	User ID	OK/NG
保存ジョブの印刷	User ID	OK/NG
保存ジョブの変更・再保存(移動・複製)	User ID	OK/NG
保存ジョブの読出し	User ID	OK/NG
保存ジョブのファイル出力	User ID	OK/NG
IPsec セッション確立の失敗	Admin ID / User ID / 未登録 ID	OK/errNo(*2)

(*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)下記の IPsec セッション失敗要因を示す固有値を記録する

- 内部エラー
- 入力チェックなし
- セキュリティプロトコルエラー
- マニュアル設定 SPI(受信)重複エラー
- マニュアル設定 SPI(受信)重複エラー
- IPsec 暗号化アルゴリズムエラー
- IPsec 認証アルゴリズムエラー
- マニュアル設定 IPsec 暗号化鍵エラー(送信)
- マニュアル設定 IPsec 暗号化鍵重複エラー(送信)
- マニュアル設定 IPsec 暗号化鍵エラー(受信)
- マニュアル設定 IPsec 暗号化鍵重複エラー(受信)
- マニュアル設定 IPsec 認証鍵エラー(送信)
- マニュアル設定 IPsec 認証鍵重複エラー(送信)
- マニュアル設定 IPsec 認証鍵エラー(受信)
- マニュアル設定 IPsec 認証鍵重複エラー(受信)
- DH グループエラー
- IPsec SA Lifetime エラー
- 鍵交換方式エラー
- IKE 認証方式エラー
- マニュアル設定 SPI エラー(送信)
- マニュアル設定 SPI エラー(受信)
- ReplayDetection エラー
- AES_CBC 鍵長エラー
- AES_CTR 鍵長エラー
- AES_GCM 鍵長エラー
- AES_GCM_64 鍵長エラー
- AES_GMAC 鍵長エラー
- SHA2 鍵長エラー
- ESN 有効の場合、リプレイ防御が無効はエラー
- 通信先設定 OK
- IKE 設定入力チェックなし
- IKEv1 ネゴシエーションモードエラー
- IKE 暗号化アルゴリズムエラー
- IKE 認証アルゴリズムエラー
- IKE DH グループエラー
- IKE ライフタイムエラー
- IKE AES_CBC 鍵長エラー
- IKE SHA2 鍵長エラー

ログは事象に対応する個別のナンバー(ジョブはその種別ごとに異なるナンバーを割り当て)とともに、事象発生時刻(年月日時分秒)、サブジェクト識別情報、事象の結果を記録する。

FAU_STG_EXT.1

記録された監査ログデータは 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(webDAV)に従いログファイルの送信を行う。ログのローカル保持サイズ、ログ保存領域フル時の対応、ログ送信タイミングなどは Table 7-10 を参照のこと。

Table 7-10 監査ログデータの仕様

監査ログデータの取り扱い	概要
ログ情報の保管領域	ストレージ暗号化機能にて暗号化された HDD 領域(*1)
ログ情報の保持サイズ(件数)	1 ファイルあたり 11KB(約 200 件)、最大 100 ファイル(1MB、約 20000 件)を TOE 内に保持
ログ情報の保持サイズ 最大容量到達時の処理	保持しているログファイルのうち、一番古いもの 1 ファイルを削除
ログ情報送信タイミング	60 分毎、もしくは管理者機能「監査ログのサーバー送信」ボタン押下時(手動送信)
送信対象となるログ情報	TOE 内に保持されている 11KB 記録済のログファイルを送信対象とする。「監査ログのサーバー送信」ボタン押下時は保存されている全てのログ情報を送信対象とする
送信成功時の処理	送信済かつ 11KB 記録済ログファイルの削除 ログ送信(成功)イベントを監査ログに記録
送信失敗時の処理	ログ送信(エラー)イベントを監査ログに記録 (手動送信のみ)操作パネルにエラーメッセージを表示

(*1) Table 7-15 に示された HDD の本体制御領域に保存される。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。

FTP_ITC.1

TOE は監査ログサーバー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 7-11 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
監査ログサーバー(WebDAV)	IPsec	AES(128bits、256bits)

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。

7.9. ストレージ暗号化機能・暗号鍵材料保護機能

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 HMAC_DRBG を用いた乱数生成処理実行の際には、エントロピー値として intel CPU の RDRAND 命令をアセンブラ関数から呼び出して入手した 768bit

のビット列を生成し(詳細は 7.9 章 FCS_RBG_EXT.1 参照)、ファームウェア内のライブラリソフトウェア(RSA BSAFE Crypto-C)の乱数生成関数に入力することで乱数生成する。

Table 7-12 使用暗号化アルゴリズム

Algorithm	Standard	SFR Reference
HMAC_DRBG	SP 800-90A	FCS_RBG_EXT.1
AES-CBC 128bits/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 7-13 に記載された暗号鍵を生成している。

Table 7-13 ストレージ暗号化に使用する暗号鍵

鍵種	概要
DEK①(128bit)	ストレージデバイス上のデータ暗号化
DEK②(256bit)	ストレージデバイス上のデータ暗号化
KEK(256bit)	DEK①及び DEK②保存時の暗号化

管理者は TOE の利用時、「暗号化ワード設定機能」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) EEPROM 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) EEPROM から暗号化された 2 種類の DEK を読込み、上記の鍵にて復号化、SDRAM 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 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ワード (64 文字)
     ※ ユーザー入力値が 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)
     ※ Entropy input 値(768bit)は RDRAND から供給されたものを使用。
   - iterationCount:1000 回
(4) 新たに生成された KEK で、2 つの DEK を暗号化する。
(5) EEPROM に KEK 導出時の鍵材料(パスワード・Salt)と、暗号化した 2 つの DEK を保存する。

なお、暗号化ワードは最大 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 7-14 参照)を組み合わせた文字列を設定できる。

Table 7-14 暗号化ワードに使用できる特殊文字(32 文字)

暗号化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 EEPROM 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) EEPROM から暗号化された 2 種類の DEK を読込み、再導出した KEK にて復号化、SDRAM 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 EEPROM、可搬記憶媒体に該当する媒体には保存されず SDRAM のみに保存される。鍵材料は基板上の EEPROM 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 の 2 種類の鍵は全て TOE の基板上の EEPROM 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。鍵材料は SDRAM に保存されることはあるが、NVRAM や EEPROM、可搬記憶媒体に該当する媒体には一切保存されない。
- 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 7-13 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 TSF 情報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/EEPROM である(SDRAM 上の TSF データは電源 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 7-15、Table 7-16 に示す。

Table 7-15 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	ファームウェアの格納	暗号化しない	－	－	－
	TOE 設定情報格納領域(用紙設定等)	暗号化ファイルシステム	DEK①	AES(CBC)	常時
	オフィス連携関連データ格納先(連携アプリ設定情報の保存等)	暗号化ファイルシステム	DEK①	AES(CBC)	常時
HDD	ジョブ保存領域(ジョブ管理データ・ジョブ及び機械状態ログ)	各データファイルを暗号化	DEK②	AES(CBC)	常時
	ジョブ保存領域(画像データ・サムネイル)	各データファイルを暗号化	DEK②	AES(CBC)	HDD 暗号化設定:ON
	SWAP 領域(未使用)	暗号化しない	－	－	－
	コントローラ領域(ネットワーク送受信データの一時保存等)	暗号化ファイルシステム	DEK①	AES(CBC)	常時
	本体制御領域(監査ログデータ／ユーザー認証データ／web 関連設定／スタンプ等)	暗号化ファイルシステム	DEK①	AES(CBC)	常時

Table 7-16 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

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
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・電	パスワード情報を暗号化して保存	DEK②	AES(CBC)	常時

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
	子文書送信先含む)	(上記に該当しないエリアは平文)			
EEPROM	DEK①・DEK②	暗号化して保存	KEK	AES(CBC)	常時
	KEK 鍵材料	平文のまま	—	—	—

Table 7-15、Table 7-16 に記載された各項目について説明する。

- 暗号化対応方法列に「暗号化ファイルシステム」と記載されている領域はファイルシステムによる暗号化・復号化が実施される。暗号化ファイルシステムは指定した HDD/SSD のパーティション(領域)の全てのファイルの 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(DEK①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・ジョブ及び機械状態ログ)」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(DEK②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、管理者が操作パネルより設定できる「HDD 暗号化設定」が ON に設定されることにより暗号化機能が有効化される。ただし、セキュリティ強化モード ON 時は HDD 暗号化設定 ON に固定され、強制的に暗号化される。
- 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

- 本 TOE で使用する鍵は最大 256bit であるため、256bit 以上のエントロピーを収集するために、RDRAND という乱数生成命令を持つ intel 社の CPU(Intel® Core™ i5-4570S 2.9GHz)を使用する。
- RDRAND 命令では、1 回の乱数ビット列のリクエストに対し、64bit の乱数を出力する。ここで、RDRAND 命令は SP800-90A に従った処理を行っており、その乱数出力について、1bit あたり 0.5bit 以上の最小エントロピーを含むことが、参考文献 (*1)の記述からわかっている。また RDRAND 命令はその 1 つのシードから 511 個を上限として 128bit の乱数を生成される。(つまり、同じシード値から 511*2=1022 個以上の連続する DRNG 乱数が生成されることはない。)
- そこで TOE は、同じシードから生成された値の利用を避ける為、RDRAND に対して乱数ビット列を 1022×12 回リクエストし、シード値が同じ乱数を除外して得られた 12 個の 64bit の乱数ビット列を連結して 768bit のビット列とする。このビット列には少なくとも 384(=768×0.5)bit のエントロピーが含まれると想定する。
- このビット列を HMAC_DRBG にシード値として入力する。HMAC_DRBG としてはファームウェア内のライブラリソフトウェア(RSA BSAFE Crypto-C)の乱数生成関数を使用しており、SP800-90A に従った HMAC_DRBG (SHA-256)である。

(*1) Mike Hamburg, Paul Kocher, Mark E. Marson: ANALYSIS OF INTEL'S IVY BRIDGE DIGITAL RANDOM NUMBER GENERATOR. Technical Report. Cryptography Research, Inc. (March 2012)

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の鍵材料は EEPROM の特定領域に保存され、セキュリティ強化モード状態に関わらず 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。そのため、暗号鍵が不要となるタイミングは TOE を廃棄する時、及び暗号鍵の再生成時に限定される。TOE の廃棄時には管理者にデータ抹消機能を実施することをガイダンスで案内されている。EEPROM は可搬記憶媒体には該当しないが、データ抹消機能を実施すると鍵材料及び鍵保存領域を固定値(0)で 1 回上書き処理を行う。また、鍵材料から生成した KEK や、KEK で復号した DEK は SDRAM 上に保存され、TOE の電源 OFF と共に削除される。

以上