

**Canon imageFORCE
8105/8195/8186
with PDL**

Security Target

Version 0.08
2026/04/24

キヤノン株式会社

目次

1	ST 概説	5
1.1	ST 参照	5
1.2	TOE 参照	5
1.3	TOE 概要	5
1.3.1	TOE 種別	5
1.3.2	TOE の使用方法と主要なセキュリティ機能	5
1.3.3	TOE 以外のハードウェア構成とソフトウェア構成	6
1.4	TOE 記述	7
1.4.1	TOE の物理的範囲	7
1.4.2	TOE の論理的範囲	9
1.5	略語・用語	11
2	適合主張	14
2.1	CC 適合主張	14
2.2	PP 主張	14
2.3	パッケージ主張	14
2.4	適合根拠	14
3	セキュリティ課題定義	15
3.1	TOE のユーザー	15
3.2	資産	15
3.2.1	利用者データ	15
3.2.2	TSF データ	15
3.3	脅威	17
3.4	TOE に関する組織のセキュリティ方針	17
3.5	前提条件	17
4	セキュリティ対策方針	19
4.1	運用環境のセキュリティ対策方針	19
5	Extended components definition	20
5.1	FAU_STG_EXT Extended: External Audit Trail Storage	20
5.2	FCS_CKM_EXT Extended: Cryptographic Key Management	20
5.3	FCS_HTTPS_EXT Extended: HTTPS selected	21
5.4	FCS_IPSEC_EXT Extended: IPsec selected	22
5.5	FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)	24
5.6	FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)	24
5.7	FCS_SMC_EXT Extended: Submask Combining	25
5.8	FCS_TLS_EXT Extended: TLS selected	26
5.9	FDP_DSK_EXT Extended: Protection of Data on Disk	28
5.10	FIA_PMG_EXT Extended: Password Management	28
5.11	FIA_PSK_EXT Extended: Pre-Shared Key Composition	29
5.12	FPT_KYP_EXT Extended: Protection of Key and Key Material	30

5.13	FPT_SKP_EXT Extended: Protection of TSF Data	31
5.14	FPT_TST_EXT Extended: TSF testing	31
5.15	FPT_TUD_EXT Extended: Trusted Update.....	32
6	セキュリティ要件	34
6.1	表記法	34
6.2	セキュリティ機能要件	34
6.2.1	Class FAU: Security Audit.....	34
6.2.2	Class FCO: Communication	36
6.2.3	Class FCS: Cryptographic Support.....	36
6.2.4	Class FDP: User Data Protection.....	51
6.2.5	Class FIA: Identification and Authentication	54
6.2.6	Class FMT: Security Management	57
6.2.7	Class FPR: Privacy.....	60
6.2.8	Class FPT: Protection of the TSF	60
6.2.9	Class FRU: Resource Utilization.....	61
6.2.10	Class FTA: TOE Access	61
6.2.11	Class FTP: Trusted Paths/Channels.....	62
6.3	セキュリティ保証要件	63
6.4	セキュリティ機能要件根拠.....	64
6.4.1	The dependencies of security requirements.....	64
7	TOE 要約仕様	67
7.1	ユーザー認証機能	67
7.2	アクセス制御機能.....	68
7.2.1	プリント処理制御機能	68
7.2.2	スキャン処理制御機能	70
7.2.3	コピー処理制御機能	73
7.2.4	文書の保存と取り出し処理制御機能	75
7.3	SSD 暗号化機能	77
7.3.1	暗号化/復号機能	77
7.3.2	暗号鍵管理機能.....	78
7.4	LAN データ保護機能.....	79
7.4.1	IPSec 暗号化機能	79
7.4.2	IPSec 暗号鍵管理機能.....	81
7.4.3	TLS 暗号化機能	83
7.4.4	TLS 暗号鍵管理機能	84
7.4.5	乱数生成機能	85
7.5	署名検証/生成機能	86
7.5.1	TLS 署名生成機能.....	86
7.5.2	IPSec 署名検証/生成機能.....	86
7.6	自己テスト機能	87
7.7	監査ログ機能	87

7.8	高信頼アップデート機能.....	89
7.9	管理機能.....	89
7.9.1	ユーザー管理機能.....	89
7.9.2	デバイス管理機能.....	91
8	参考文献.....	94

商標などについて

- Canon、Canon ロゴ、imageRUNNER、imageRUNNER ADVANCE、imageRUNNER ADVANCE DX、imageFORCE、imagePRESS、imagePRESS Lite はキヤノン株式会社の商標です。
- Microsoft、Windows、Windows Server 2022、Windows 11、Microsoft Edge は、米国 Microsoft Corporation の商標または登録商標です。
- その他、本文中の社名や商品名は、各社の商標または登録商標です。

1 ST 概説

1.1 ST 参照

本節では Security Target(以下、ST と略す)の識別情報を記述する。

ST 名称: Canon imageFORCE 8105/8195/8186 with PDL Security Target
 バージョン: 0.08
 発行者: キヤノン株式会社
 発行日: 2026/04/24

1.2 TOE 参照

本節では TOE の識別情報を記述する。

TOE 参照: Canon imageFORCE 8105/8195/8186 with PDL 404

本 TOE は、MFP 本体、ファームウェア、ページ記述言語処理により構成される (Table 3 参照)。TOE であることは、以下 (Table 1) に示すメーカー名の識別情報、MFP 本体の識別情報、ファームウェアの識別情報、ページ記述言語処理の識別情報により確認することができる。

Table 1—TOE の識別情報

識別情報の種類	識別情報
メーカー名	[Canon]
MFP 本体	下記のいずれか [imageFORCE 8105] [imageFORCE 8195] [imageFORCE 8186]
ファームウェア	[404]
ページ記述言語処理	[PCL] 及び [PS]

1.3 TOE 概要

1.3.1 TOE 種別

TOE は、プリント機能・スキャン機能・コピー機能・文書の保存と取り出し機能を併せ持つデジタル複合機である。また本 TOE はファクス機能を有していない。

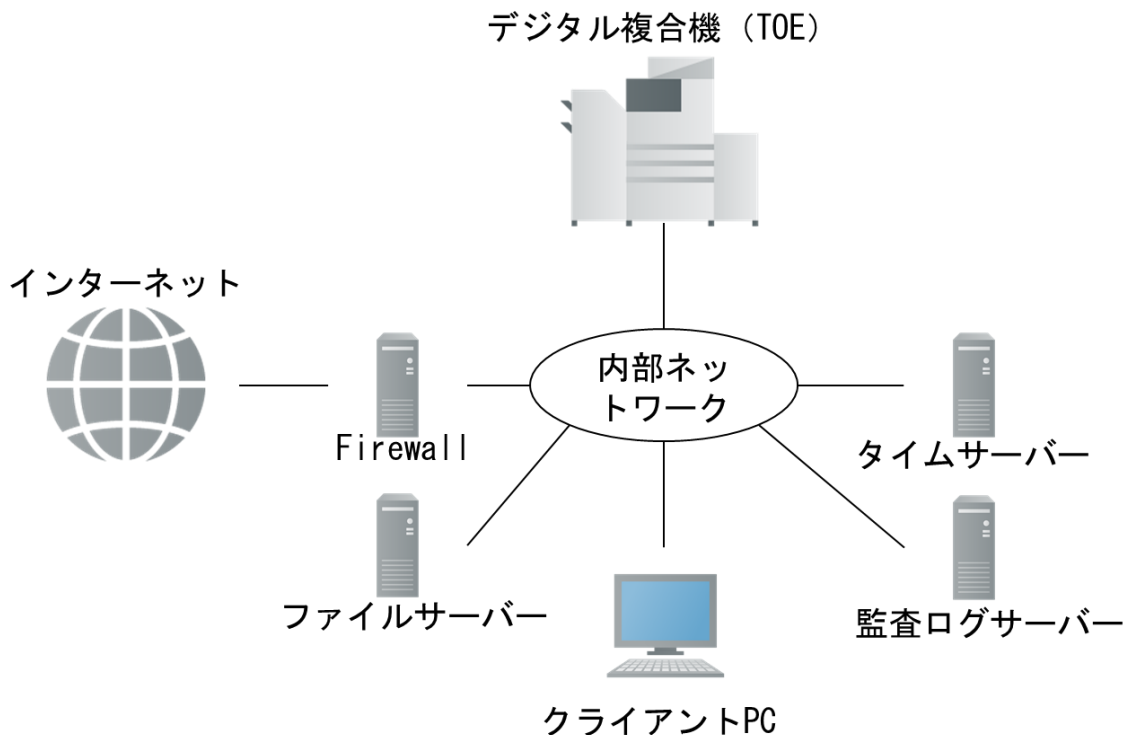
1.3.2 TOE の使用方法と主要なセキュリティ機能

本 TOE は、利用者の文書を扱う、コピー機能、プリント機能、スキャン機能、文書の保存と取り出し機能を有する。これらの文書の改ざん、漏えいを防止するため、TOE には、利用者を識別認証するユーザー認証

機能、権限に基づく文書データや機能に対するアクセス制御機能、TOE 内蔵 SSD の SSD 暗号化機能、ネットワーク通信を保護する LAN データ保護機能及び署名検証/生成機能、起動時に TSF 実行コードの完全性を確認する自己テスト機能、TOE のセキュリティ機能の利用をモニタリングし、モニタリング結果（監査ログ）を監査ログサーバーに送付する機能及び TOE 内部に監査ログを保存する機能を持つ監査ログ機能、TSF 実行コードアップグレード時の実行コードの真正性を確認しつつ更新する高信頼アップデート機能、セキュリティ設定を管理者に限定した管理機能を有する。

Figure 1 は、本 TOE の機能を使用する場合の想定運用環境である。

Figure 1 本 TOE の想定する運用環境



1.3.3 TOE 以外のハードウェア構成とソフトウェア構成

想定運用環境 Figure 1 に存在する、TOE 以外のハードウェア・ソフトウェア構成を以下に示す。

1) タイムサーバー

TOE は正確な時間を取得するため、SNTP に対応したサーバー（本運用では、Windows Server 2022 Standard を想定する）と通信する。

2) 監査ログサーバー

TOE にて生成された監査ログを保存するための外部監査ログサーバー（本運用では、Windows Server 2022 Standard を用いた SMB サーバー）。監査ログサーバーは SMB にて監査ログを取得する。

3) クライアント PC

Windows11 で動作する汎用 PC。TOE にアカウントを持つユーザーは、本 TOE に対応したプリンタードライバー（本運用では、Table 2 に記載のプリンタードライバーを想定）をインストールし設定することで、プリン

トジョブを TOE へ送信することができる。また、管理者はプリントに加え、ウェブブラウザ(本運用では Microsoft Edge を想定)を利用して TOE へアクセスすることで、TOE の管理機能を利用できる。

Table 2—プリンタードライバー

プリンタードライバー名	
Generic Plus UFR II Printer Driver	V3.31 (日本以外仕向け名称。日本仕向け名称は、Generic Plus LIPSLX Printer Driver V3.31)
Generic Plus PS3 Printer Driver	V3.31
Generic Plus PCL6 Printer Driver	V3.31

4) ファイルサーバー

TOE でスキャン文書を送信した際の保存スペース。本運用では Windows Server 2022 Standard を用いた SMB サーバーを想定している。

5) Firewall

TOE が接続する内部ネットワークを、インターネット環境からの不正アクセスから保護する装置。本 TOE の前提条件 A.NETWORK 満たす環境であることを示しており、特定の製品は想定していない。

1.4 TOE 記述

1.4.1 TOE の物理的範囲

TOE はデジタル複合機とガイダンスである。

TOE を構成するデジタル複合機は、指定 Controller Version のファームウェアが動作する MFP 本体であり、ページ記述言語処理(オプションの場合は、PCL option, PS option を購入することで PCL/PS 機能が有効化される)を有するものである。Table 3—製品ラインアップ一覧に示す通り、PCL option、PS option は取扱地域での販売名称に合致した適切なオプションを調達する必要がある。

Table 3—製品ラインアップ一覧

MFP 本体 (Controller Version 404)	取扱地域 ※1	PCL option ¹	PS option ¹
imageFORCE 8105 imageFORCE 8195 imageFORCE 8186	日本	PCLエミュレーション拡張 キット・AS1	PS拡張キット・BF1
imageFORCE 8105 imageFORCE 8195 imageFORCE 8186	米州/欧州/ アジア/豪 州/韓国	PCL Printer Kit-BD1	PS Printer Kit-BD1

※1: MFP の言語表示は、取扱地域が日本の場合は日本語、日本以外の場合は英語表示となる。

販売会社より派遣されるサービスエンジニアは、MFP 本体にサービスエンジニアが持参する指定 Controller Version のファームウェア(直接消費者に配付されない)をインストールし、購入されたライセンス

¹ PCL option/PS option 購入により、ファームウェアの PCL/PS 処理機能が有効化された MFP 本体が提供される。本オプション購入による配送物はない。

情報(直接消費者に配付されない)に従ってページ記述言語処理(PCL, PS)を有効な状態に設定したのち、MFP 本体を消費者へ提供する。

よって配送物は上記作業後に引き渡される MFP 本体であり、Table 4 記載の各識別情報(MFP の前面パネルに記載される [メーカー名]と、MFP の操作パネルに表示される[MFP 本体]、[ファームウェア]、[ページ記述言語処理])によって識別される。

Table 4—TOE を構成するハードウェア/ソフトウェア

TOE の識別	取扱地域	[メーカー名]	[MFP 本体]	[ファームウェア]	[ページ記述言語処理]
Canon imageFORCE 8105 with PDL 404	日本/米州/ 欧州/アジア /豪州/韓国	Canon	imageFORCE 8105 imageFORCE 8195 imageFORCE 8186	404	PCL PS
Canon imageFORCE 8195 with PDL 404					
Canon imageFORCE 8186 with PDL 404					

TOE に含まれる以下のガイダンスは、サービスエンジニアの指示により入手することができる。ガイダンスはウェブサイト(<https://oip.manual.canon/>)より PDF ファイルにて TOE 消費者へ配付される。ウェブサイトアクセス時に取扱地域を選択し、CC 認証製品の該当機種を選択すると、下記ガイダンスを入手できる。

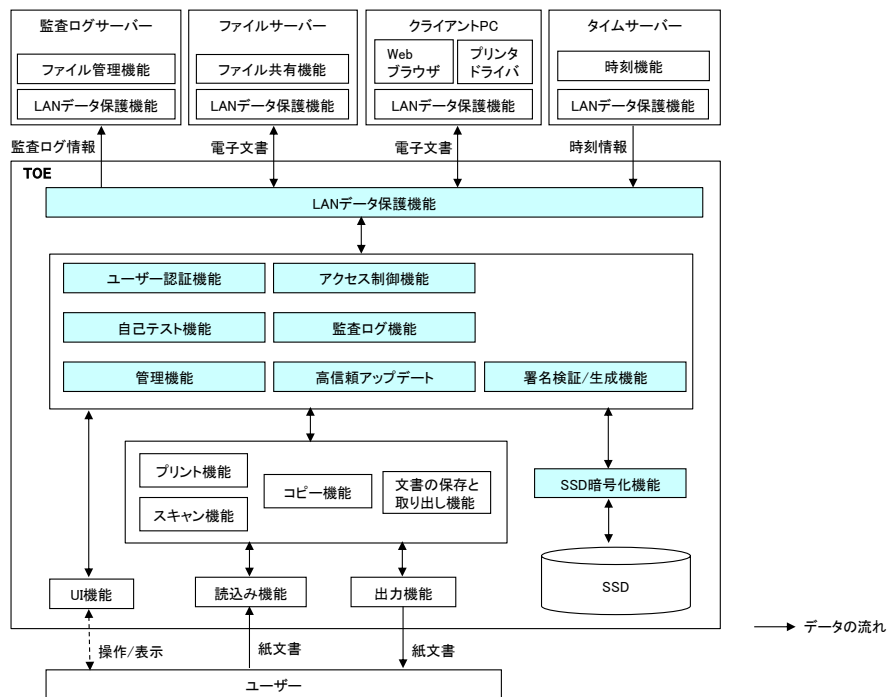
- TOE の識別: Canon imageFORCE 8105 with PDL 404 / Canon imageFORCE 8195 with PDL 404 / Canon imageFORCE 8186 with PDL 404
 - 取扱地域: 日本
 - ガイダンス:
 - ✧ imageFORCE 8100 シリーズ用 Protection Profile for Hardcopy Devices 対応 セキュリティ設定 アドミニストレーターガイド [USRMB-0708-00 20251205]
 - ✧ imageFORCE 8105 / 8195 / 8186 ユーザーズガイド(CC 認証参照用) [USRMB-0709-00]
 - ✧ imageFORCE 8100 シリーズ用 ACCESS MANAGEMENT SYSTEM アドミニストレーターガイド(CC 認証参照用) [USRMB-0710-00]
 - 取扱地域: 米州
 - ガイダンス:
 - ✧ imageFORCE 8100 series Protection Profile for Hardcopy Devices adaptive Security Settings Administrator Guide [USRMB-0711-00 20251212]
 - ✧ imageFORCE 8105 / 8195 / 8186 User's Guide (for CC certification reference) [USRMB-0713-00]
 - ✧ imageFORCE 8100 series ACCESS MANAGEMENT SYSTEM Administrator Guide (for CC certification reference) [USRMB-0715-00]
 - 取扱地域: 欧州/アジア/豪州/韓国
 - ガイダンス:
 - ✧ imageFORCE 8100 series Protection Profile for Hardcopy Devices adaptive Security Settings Administrator Guide [USRMB-0711-00 20251212]
 - ✧ imageFORCE 8105 / 8195 / 8186 User's Guide (for CC certification reference) [USRMB-0717-00]

◇ imageFORCE 8100 series ACCESS MANAGEMENT SYSTEM Administrator Guide (for CC certification reference) [USRMB-0718-00]

1.4.2 TOE の論理的範囲

TOE の論理的範囲を以下の Figure 2 TOE の機能構成で図示する(ユーザー、ファイルサーバー、監査ログサーバー、クライアント PC、タイムサーバーを除く)。TOE のセキュリティ機能は色つきで示す部分である。

Figure 2 TOE の機能構成



TOE は以下のデジタル複合機機能を有する。

- プリント機能
デジタル複合機内の電子文書やクライアント PC から送信される電子文書を紙にプリントする機能である。
- スキャン機能
紙文書をスキャンして生成された電子文書を TIFF や PDF ファイル形式でファイルサーバーに送信する機能である。
- コピー機能
紙文書をスキャナで読み込み、プリントすることにより、紙文書を複写する機能である。
- 文書の保存と取り出し機能

アドバンスドボックスの文書管理機能。スキャナで読み込まれた文書を画像としてアドバンスドボックスの個人スペースに保存できる。個人スペースに保存された電子文書に対して、ファイル名変更、取り出し(プリント、)、削除ができる。

また、TOE は以下の一般機能を有する。

- UI 機能

ユーザーが操作パネルを用いて TOE を操作したり、TOE が操作パネルに表示したりする機能。

また、クライアント PC のブラウザ操作により、ネットワークを通して TOE の操作や管理を行うリモート UI 機能を有する。

- 出力機能

TOE が紙文書を出力する機能。

- 読み込み機能

TOE が紙文書を入力する機能。

TOE は、以下のセキュリティ機能を有する。

- ユーザー認証機能

登録外の人によって勝手に TOE が利用されないように、正当なユーザーを認証する。ユーザー認証は、操作パネルやリモート UI から操作する際、ユーザー名とパスワードの入力を求め、正当なユーザーであることを確認する。またプリンタードライバーよりジョブを受け付ける前にプリンタードライバーを通じてユーザー名の認証を行う。ユーザー情報の確認は、TOE 内で認証する内部認証をサポートする。認証されたユーザーに対して、予めユーザーに割り当てられた権限を与える。認証時は入力されたパスワード文字を特定文字で表示する。認証失敗時には定義したルールによってアクセス制限する機能を有し、認証後無操作状態が続く場合には自動ログアウトする機能を有する。

- アクセス制御機能

ロールに応じてジョブや電子文書、機能に対するアクセスを制限する。

- SSD 暗号化機能

TOE 内蔵 SSD を持ち去って別本体や PC に接続し、SSD 内に記録されたデータを読み取られる脅威に対抗するため、デジタル複合機本体に内蔵された暗号化チップにより TOE 内蔵 SSD に格納されるすべてのデータを暗号化する。暗号化に用いる鍵は TOE の電源 ON 時に暗号化チップ内の RAM 領域に生成され、暗号化チップ内でのみ使われ、外部へ取り出せないように管理される。暗号鍵は、TOE の電源 OFF とともに不要となり消去される。

- LAN データ保護機能

LAN データのスニッファリング対策として、IPsec や TLS にて暗号化する。IPsec は外部機器及びリモート UI との接続時に使用され、さらに管理者によるリモート UI 接続時は TLS も利用可能である。事前共有鍵及びサーバー秘密鍵は TOE 内蔵 SSD 上に暗号化して保存され、保護されている。通信中の生成される鍵は TOE 内の RAM 領域に生成され、TOE の電源 OFF とともに消去される。

- 署名検証/生成機能

LAN データの暗号通信の完全性検証のため、デジタル署名の検証/生成機能を持つ。

- 自己テスト機能

起動時に、ファームウェアの完全性を署名検証により確認する。

- 監査ログ機能

本体動作やユーザーの操作を監査できるように、操作したユーザーのユーザー名や設定された時刻とともに監査ログを生成し、TOE 内蔵 SSD 内に保存する。時刻は管理機能の利用、もしくはタイムサーバーと同期した正確な日時が記録される。保存された全ての監査ログは、リモート UI より管理者のみが閲覧できる。ただし管理者であっても監査ログの変更はできない。また、監査ログは保護された通信を用い監査ログサーバーへ保存される。TOE 内蔵 SSD 内の監査ログ数には上限があり、監査ログ数が保存上限数を超える場合は最も古い監査ログが削除され、新しい監査ログを保存する。

- 高信頼アップデート機能

TOEファームウェアを更新する際、正当なファームウェアを使用することを確認するため、バージョン表示やデジタル署名によるファーム検証をする機能を有する。

- 管理機能

ユーザーやロールを登録・削除するためのユーザー管理機能と各種セキュリティ機能が適切に動作するためのデバイス管理機能であり、ともに管理者のみに操作が限定されている

1.5 略語・用語

本 ST で使用される用語の内、2 章で適合主張している CC および PP で定義された用語については、その定義に従う。それ以外の用語の定義を Table 5 に示す。

Table 5—略語・用語

略語・用語	説明
デジタル複合機	コピー機能、プリント機能、送信 (Universal Send) 機能などを併せ持つ複合機のこと。これらの機能を使用するため、大容量の SSD を内蔵する。
ファームウェア	デジタル複合機上で動作し、セキュリティ機能の制御を司るソフトウェアである。
PDL	印刷内容を表現するページ記述言語であり、各種存在する。プリント機能では、対応するページ記述言語で表現された印刷データを変換し、生成した画像を紙に印刷する。
操作パネル	デジタル複合機を構成するハードウェアのひとつであり、操作キーとタッチパネルから構成され、デジタル複合機を操作するとき 사용되는インターフェースである。
リモート UI	Web ブラウザから LAN を経由してデジタル複合機にアクセスし、デジタル複合機の動作状況の確認やジョブの操作、各種設定などができるインターフェースである。管理者のみが使用できる。
SSD	デジタル複合機に内蔵される不揮発性記憶装置のこと。ファームウェアおよび、保護資産が保存される。

略語・用語	説明
ロール	<p>アクセス制御機能で利用するユーザーの権限であり、各ユーザーにはひとつのロールが関連付けられる。</p> <p>あらかじめ定義されているデフォルトロールに加え、カスタムロールとしてデフォルトロールで決められたアクセス制限値を変更した新規のロールを作成することが可能である。デフォルトロールには以下のロールがある</p> <p>Administrator/Power User/General User/Limited User/Guest User</p> <p>Administrator ロールとは管理機能を利用する権限(管理権限)を示す。</p> <p>本 ST では、管理権限を持つ U.ADMIN が所属する Administrator ロールと、管理権限を持たない U.NORMAL が所属する General User をベースとしたカスタムロールが定義される。</p>
管理者	PP で定義されている U.ADMIN。Administrator ロールが割り当てられた管理権限を有するユーザー。
一般利用者	PP で定義されている U.NORMAL。管理権限を持たない General User ロールから作成するカスタムロールに所属する。
認証ユーザー	管理者を含む TOE で認証された全てのユーザー
ジョブ	<p>ユーザーが TOE の機能を利用して文書进行操作する際のユーザーの作業指示と対象となる文書のデータ(電子文書)を組み合わせたもの。</p> <p>文書の操作には、読み込み、プリント、コピー、保存、削除があり、ユーザーの操作によりジョブの生成、実行、完了までの一連の処理が行われる。</p>
イメージファイル	読み込み、プリント、受信などによってデジタル複合機内に生成された画像データ。
テンポラリイメージファイル	コピー・プリント等のジョブの途中で生成され、ジョブが完了すると不要になるイメージファイル。
電子文書	デジタル複合機内で取り扱われるユーザーデータであり、イメージファイルとプリント設定から構成される。
アドバンスドボックス	<p>デジタル複合機においてスキャナから読み込んだ電子文書を保存する領域であり、保存した電子文書のプリントが可能である。</p> <p>各ユーザー専用の個人スペースと、全ユーザーがアクセスできる共有スペースが存在する。</p> <p>※本 TOE では、共有スペースは利用しない。</p>
Firewall	Internet から内部 LAN への攻撃を防ぐための装置やシステム。
タイムサーバー	Network Time Protocol を使った時刻の問い合わせに答えることができるサーバー。
ファイルサーバー	SMB プロトコルで LAN を介してフォルダーを共有させ、ファイルの保管・アクセス制御を行うファイルサーバー
監査ログサーバー	TOE から SMB プロトコルで LAN を介して出力される監査ログファイルを保存するサーバー。
「プリント」	留め置きプリントを操作する機能を起動する操作パネル上のボタン。

略語・用語	説明
「コピー」	コピー機能を起動する操作パネル上のボタン。
「スキャンして送信」	紙文書を読み込んで、読み込んだ電子文書をファイルサーバーへ送信する機能を起動する操作パネル上のボタン。
「スキャンして保存」	紙文書を読み込んでアドバンスドボックスへ保存する機能を起動する操作パネル上のボタン。
「保存ファイルの利用」	アドバンスドボックスへ保存された電子文書进行操作する機能を起動する操作パネル上のボタン。

2 適合主張

2.1 CC 適合主張

本 ST と TOE は、以下の CC 適合を主張する。

この ST は、以下の Common Criteria (以下、CC と略す) に適合する。

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

2.2 PP 主張

この ST および TOE は、以下の PP に完全適合する。

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

2.3 パッケージ主張

この ST において、適合を主張するパッケージはない。

2.4 適合根拠

TOE は、PP に定義されている以下の要件を満足し、PP の要求通り完全適合(Exact Conformance)している。そのため TOE 種別は PP と一貫している。

- Required Uses
Printing, Scanning, Copying, Network communications, Administration
- Conditionally Mandatory Uses
Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
Internal Audit Log Storage

3 セキュリティ課題定義

3.1 TOE のユーザー

TOE の利用者は、以下の2種類の利用者分類に定義されている。

Table 6—Users

Designation	Category name	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 資産

資産には、以下の2つの資産分類が定義されている。

Table 7—資産

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 利用者データ

利用者データは、以下の2種類に分類されている。

Table 8—利用者データ

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 データ

TSF データには、以下の2種類に分類されている。

Table 9—TSF データ

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

本 TOE で扱う TSF Data を以下に示す。

Table 10 — TSF Data の具体化

タイプ	TSF Data	内容	保存先
D.TSF.PROT	ユーザー名	ユーザー識別認証機能で利用するユーザーの識別情報	SSD
	ロール	アクセス制御機能で利用するユーザーの権限情報	SSD
	ロックアウトポリシー設定	ロックアウト機能の設定情報であり、ロックアウトの許容回数とロックアウト時間の設定情報	SSD
	パスワードポリシー設定	ユーザー認証機能で利用するパスワードの設定情報であり、最小パスワード長、使用可能文字に関する制約の設定情報	SSD
	自動ログアウト設定	操作パネルやリモートUIからログインしたユーザーが無操作状態のときに、自動的にログアウトさせるまでのタイムアウト時間	SSD
	日付/時刻設定	日付と時刻の設定情報	RTC
	IPSec 設定	LAN データ保護機能に関する設定情報	SSD
	TLS 設定	LAN データ保護機能に関する設定情報であり、機能の有効/無効化に関する設定情報	SSD
	監査ログ送信設定	監査ログを外部 IT 機器へ送信するための設定情報	SSD
	タイムサーバー接続設定	TOE の日時と時刻の設定情報を外部 IT 機器と同期させるための設定情報	SSD
D.TSF.CONF	パスワード	ユーザー識別認証機能で利用するユーザーの認証情報	SSD
	SSD 暗号鍵	SSD 暗号化機能で用いる暗号鍵	暗号化チップ内 RAM
	鍵シード	DRBG の内部状態であり、AES 暗号鍵生成に使用するシード値。	暗号化チップ内の FLASH メモリー
	LAN データ保護暗号鍵	LAN データ保護機能で用いる暗号鍵	SSD
	監査ログ	監査ログ機能で生成される動作記録。日時、ユーザー名、結果、動作内容等が含まれる。	SSD

3.3 脅威

Table 11 に脅威を示す。

Table 11 — 脅威

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

3.4 TOE に関する組織のセキュリティ方針

Table 12 に組織のセキュリティ方針を示す。

Table 12 — 組織のセキュリティ方針

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

3.5 前提条件

Table 13 に前提条件を示す。

Table 13 — 前提条件

Assumption	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 セキュリティ対策方針

4.1 運用環境のセキュリティ対策方針

Table 14 に運用環境のセキュリティ対策方針を示す。

Table 14 — 運用環境のセキュリティ対策方針

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

5 Extended components definition

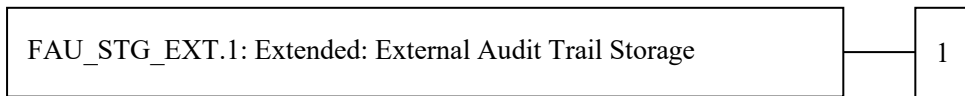
本STでは以下のセキュリティ機能要件を定義する。これらの拡張コンポーネントは全て2.2章記載のPPにて定義されているものである。

5.1 FAU_STG_EXT Extended: External Audit Trail Storage

Family behaviour:

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

Management:

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

- The TSF shall have the ability to configure the cryptographic functionality.

Audit:

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

- There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel

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

Rationale:

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

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

5.2 FCS_CKM_EXT Extended: Cryptographic Key Management

Family behaviour:

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 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.

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.

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.

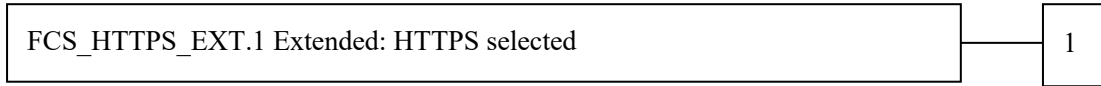
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3 FCS_HTTPS_EXT Extended: HTTPS selected

Family behaviour:

Components in this family define requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component leveling:



FCS_HTTPS_EXT.1 HTTPS selected, requires that HTTPS be implemented according to RFC 2818 and supports TLS.

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 of HTTPS session establishment

FCS_HTTPS_EXT.1 **Extended: HTTPS selected**

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 Extended: TLS selected

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Rationale:

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

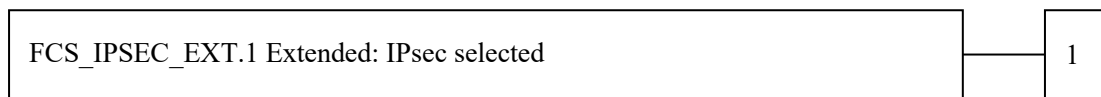
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4 FCS_IPSEC_EXT Extended: IPsec selected

Family behaviour:

This family addresses requirements for protecting communications using IPsec.

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components

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

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

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

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

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

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

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

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

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

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

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

Rationale:

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

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

5.5 FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family behaviour:

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

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.

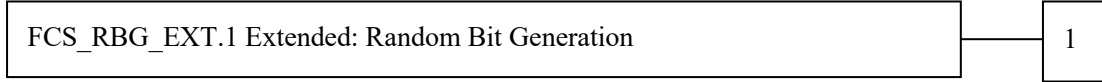
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.6 FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family behaviour:

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 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:

- Failure of HTTPS session establishment

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components

Dependencies: No dependencies.

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

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

Rationale:

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

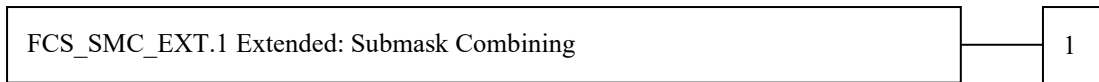
This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.7 FCS_SMC_EXT Extended: Submask Combining

Family behaviour:

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

Component leveling:



FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion.

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_SMC_EXT.1 Extended: Submask Combining

Hierarchical to: No other components.

Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm) dependencies.

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: exclusive OR (XOR), SHA-256, SHA-512] to generate an intermediary key or BEV.

Rationale:

Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.

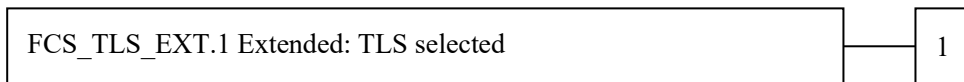
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.8 FCS_TLS_EXT Extended: TLS selected

Family behaviour:

This family addresses the ability for a server and/or a client to use TLS to protect data between a client and the server using the TLS protocol.

Component leveling:



FCS_TLS_EXT.1 TLS selected, requires the TLS protocol 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 of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components

Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
 FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
 FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)

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

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

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: *TLS 1.0 (RFC 2246)*, *TLS 1.1 (RFC 4346)*, *TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- *TLS_RSA_WITH_AES_128_CBC_SHA*

Optional Ciphersuites:

[selection:

- *None*
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*

].

Rationale:

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

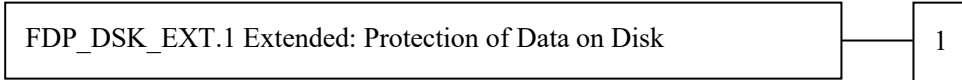
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.9 FDP_DSK_EXT Extended: Protection of Data on Disk

Family behaviour:

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 behaviour:

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 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 behaviour:

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

Component leveling:



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.

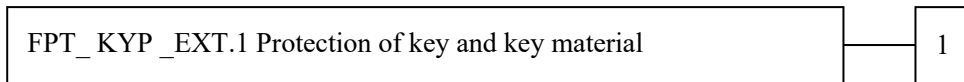
This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.12 FPT_KYP_EXT Extended: Protection of Key and Key Material

Family behaviour:

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, and not store any such plaintext key on a device that uses the key for its encryption.

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 behaviour:

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: Extended: Protection of TSF Data

Hierarchical to: No other components

Dependencies: No dependencies.

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

Rationale:

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

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

5.14 FPT_TST_EXT Extended: TSF testing

Family behaviour:

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 behaviour:

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 Trusted Update, ensures authenticity and access control for updates.

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

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

FPT_TUD_EXT.1 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 セキュリティ要件

6.1 表記法

- ・ **ボールド書体**は、HCD PP で“完成”または“詳細化”された部分を示し、コモンクライテリアパート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している。
- ・ **イタリック書体**は、本 ST にて選択され、かつ/または完成されなければならない SFR 内のテキストを示す。
- ・ **ボールドイタリック書体**は、HCD PP で“割付”または“選択”が完了または詳細化された部分を示し、本 ST にて選択され、かつ/または完成されなければならない SFR 内のテキストを示す。
- ・ []内は、“割付”または“選択”を指示している部分を示す。本 ST での“割付”または“選択”の結果は、[]部を本文後に抜き出し、その後に示す。
- ・ ()内に文字、例えば、(a)、(b)と続く SFR コンポーネントは、HCDPP で繰返しが定義されたことを示す。ST でさらに繰返す場合は、(a)(ssd)のように定義する。

6.2 セキュリティ機能要件

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps

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

- 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 15**, [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 15**, [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- None

Table 15 —Auditable Events

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *an Administrator*] with the capability to read **all records** from the audit records.

[assignment: *an Administrator*]
- U. ADMIN

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

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

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

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

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

- “overwrite the oldest stored audit records”

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

- None

FAU_STG_EXT.1 Extended: External 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.

6.2.2 Class FCO: Communication

There are no class FCO requirements.

6.2.3 Class FCS: Cryptographic Support

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

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution~~, or
FCS_COP.1(b) Cryptographic Operation (for signature generation/

verification),
 FCS_COP.1(i) Cryptographic operation (Key Transport)]
 FCS_CKM_EXT.4 Extended: Cryptographic Key Material
 Destruction

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

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

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

[selection:

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

|

- NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for 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

[selection: P-521, no other curves]

- no other curves

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

- Hierarchical to:** No other components.
- Dependencies:** [~~FCS_CKM.2 Cryptographic key distribution~~, or
 FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
 FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
 FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
 FCS_COP.1(f) Cryptographic operation (Key Encryption)
 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
 FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

- [selection: 128 bit, 256 bit]
 - 128 bit, 256 bit

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

- 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

- Hierarchical to:** No other components.
- Dependencies:** [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
 FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [selection:

For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].

For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: [selection: NIST SP800-88, no standard].

[selection:

For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].

For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

]

- For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].
- For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

[selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]]

- powering off a device

[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)

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, GCM

[Selection: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*]

- NIST SP 800-38A, NIST SP 800-38D

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

Hierarchical to: No other components.

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

FCS_COP.1.1(b) (update) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*

that meets the following [selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

]

[selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*

- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*
- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]

[assignment: 2048 bits or greater]

- 2048 bits

[selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

]

- Case: RSA Digital Signature Algorithm
 - FIPS PUB 186-4, “Digital Signature Standard”

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

Hierarchical to: No other components.

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

FCS_COP.1.1(b)(tls) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*

that meets the following [selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

|

[selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*
- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]

[assignment: 2048 bits or greater]

- 2048 bits

[assignment: 256 bits or greater]

- 256 bits, 384 bits

[selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

|

- Case: RSA Digital Signature Algorithm
 - FIPS PUB 186-4, “Digital Signature Standard”
- Case: Elliptic Curve Digital Signature Algorithm
 - FIPS PUB 186-4, “Digital Signature Standard”
 - The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).

[selection: P521, no other curves]

- no other curves

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

Hierarchical to: No other components.

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

FCS_COP.1.1(b)(ipsec) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*

that meets the following [selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

]

[selection:

- *Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*
- *RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*
- *Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]*

- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]

[assignment: 2048 bits or greater]

- 2048 bits

[assignment: 256 bits or greater]

- 256 bits, 384 bits

[selection:

Case: Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-4, “Digital Signature Standard”*
- *The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).*

]

- Case: RSA Digital Signature Algorithm
 - FIPS PUB 186-4, “Digital Signature Standard”
- Case: Elliptic Curve Digital Signature Algorithm
 - FIPS PUB 186-4, “Digital Signature Standard”
 - The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).

[selection: P521, no other curves]

- no other curves

FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_COP.1.1(c) Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [selection: *SHA-1, SHA-256, SHA-384, SHA-512*] that meet the following: [ISO/IEC 10118-3:2004].

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

- SHA-1, SHA-256, SHA-384, SHA-512

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

Hierarchical to: No other components.

Dependencies: 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*]

- XTS

[selection: *128 bits, 256 bits*]

- 256 bits

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

- XTS as specified in IEEE 1619

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

Hierarchical to: No other components.

Dependencies: 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

[assignment: *key size (in bits) used in HMAC*]

- 160, 256, 384 bits

[selection: *160, 224, 256, 384, 512*]

- 160, 256, 384

FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 Extended: TLS selected

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

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

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

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

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

[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, 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*]].

[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*]]

- 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*]]

[selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*]

- RFC 4304 for extended sequence numbers

[selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]

- RFC 4868 for hash functions

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

[selection: *IKEv1, IKEv2*]

- IKEv1

[selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*]

- no other algorithm

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

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

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

- IKEv1 SA lifetimes can be established based on [selection: *number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]

[selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]

- length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs

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

[selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 5 (1536-bit MODP)*], [assignment: *other DH groups that are implemented by the TOE*], *no other DH groups*]

- 19 (256-bit Random ECP), 20 (384-bit Random ECP)

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, ECDSA

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*].

[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)]*]

- 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 combining as specified in FCS_SMC_EXT.1

[selection: *128 bits, 256 bits*]

- 256 bits

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*]

- NIST SP 800-90A

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

- CTR_DRBG (AES)

FCS_RBG_EXT.1.2(network): The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*]] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-

based noise source(s)] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

[selection: [assignment: *number of software-based sources*] software-based noise source(s),
[assignment: *number of hardware-based sources*] hardware-based noise source(s)]

- [assignment: *number of software-based sources*] software-based noise source(s)

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

- 1

[selection: *128 bits, 256 bits*]

- 256 bits

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*]

- NIST SP 800-90A

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

- Hash_DRBG (SHA-256)

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

[selection: [assignment: *number of software-based sources*] software-based noise source(s),
[assignment: *number of hardware-based sources*] hardware-based noise source(s)]

- [assignment: *number of hardware-based sources*] hardware-based noise source(s)

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

- 1

[selection: *128 bits, 256 bits*]

- 256 bits

FCS_SMC_EXT.1 Extended: Submask Combining

Hierarchical to: No other components.

Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

FCS_SMC_EXT.1.1: The TSF shall combine submasks using the following method [selection: *exclusive OR (XOR), SHA-256, SHA-512*] to generate an intermediary key or BEV.

[selection: *exclusive OR (XOR), SHA-256, SHA-512*]

- SHA-256

FCS_TLS_EXT.1 Extended: TLS selected

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

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: *TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:

- None
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

[selection: *TLS 1.0 (RFC 2246)*, *TLS 1.1 (RFC 4346)*, *TLS 1.2 (RFC 5246)*]
 - TLS 1.2 (RFC 5246)

[selection:

None
 TLS_RSA_WITH_AES_256_CBC_SHA
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 TLS_RSA_WITH_AES_128_CBC_SHA256
 TLS_RSA_WITH_AES_256_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

TLS_RSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

6.2.4 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

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 16 and Table 17**.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 16** and **Table 17**.

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 16 and Table 17*.

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*]

- None

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*]

- None

Table 16 — D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	Operation:	<i>Submit a document to be printed</i>	<i>View image or Release printed output</i>	<i>Modify stored document</i>	<i>Delete stored document</i>
	Job owner	(note 1) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	Operation:	<i>Submit a document for scanning</i>	<i>View scanned image</i>	<i>Modify stored image</i>	<i>Delete stored image</i>
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	Operation:	<i>Submit a document for</i>	<i>View scanned image or</i>	<i>Modify stored</i>	<i>Delete stored</i>

		<i>copying</i>	<i>Release printed copy output</i>	<i>image</i>	<i>image</i>
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage / retrieval	Operation:	<i>Store document</i>	<i>Retrieve stored document</i>	<i>Modify stored document</i>	<i>Delete stored document</i>
	Job owner	(note 1) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Table 17 — D.USER.JOB Access Control SFP

		"Create" *	"Read"	"Modify"	"Delete"
Print	Operation:	<i>Create print job</i>	<i>View print queue / log</i>	<i>Modify print job</i>	<i>Cancel print job</i>
	Job owner	(note 1) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	Operation:	<i>Create scan job</i>	<i>View scan status / log</i>	<i>Modify scan job</i>	<i>Cancel scan job</i>
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	allowed	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	Operation:	<i>Create copy job</i>	<i>View copy status / log</i>	<i>Modify copy job</i>	<i>Cancel copy job</i>
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage / retrieval	Operation:	<i>Create storage / retrieval job</i>	<i>View storage / retrieval log</i>	<i>Modify storage / retrieval job</i>	<i>Cancel storage / retrieval job</i>
	Job owner	(note 2) allowed	allowed	denied	allowed

	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	denied	denied	denied

Application notes:

The following Notes that are referenced in Table 16 and Table 17:

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.

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.

[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.

6.2.5 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

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

- an administrator configurable positive integer within [assignment: range of acceptable values]

[assignment: *range of acceptable values*]

- 1 から 10 内における正の整数値

[assignment: *list of authentication events*]

- 操作パネルを使ったログイン試行、リモートUIを使ったログイン試行、プリンタードライバからの認証試行

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

[selection: met, surpassed]

- met

[assignment: *list of actions*]

- 1-60分で設定した時間を経過するまでロックアウト

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[assignment: *list of security attributes*]

- User Name, Role

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;

[selection: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, [assignment: *other characters*]]

- “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, [assignment: *other characters*]

[assignment: *other characters*]

- “(space)”, “””, “””, “+”, “,”, “-”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “¥”, “]”, “_”, “~”, “{”, “|”, “}”, “~”

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 “)”).

[selection: [assignment: *other supported lengths*], *no other lengths*]

- [assignment: *other supported lengths*]

[assignment: *other supported lengths*]

- 24 文字以内の文字

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*, [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*

FIA_UAU.1 Timing of authentication

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*]

- none

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

[assignment: *list of feedback*]

- *, ●

FIA_UID.1 Timing of identification

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*]

- none

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

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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

[assignment: list of user security attributes]

- User Name, Role

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

[assignment: rules for the initial association of attributes]

- None

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

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

- None

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

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*]

- disable, enable

[assignment: *list of functions*]

- TLS 暗号化機能

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies:

FDP_ACC.1	Subset access 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]*]

- query, modify, delete, [assignment: other operations]

[assignment: *other operations*]

- create

[assignment: *list of security attributes*]

- Table 18: Management security attributes の「Security attributes」の項

[assignment: *the authorised identified roles*]

- Table 18: Management security attributes の「Authorised role(s)」の項

Table 18 - Management of security attributes

Security attributes	Operation	Authorised role(s)
User Name	query	U.ADMIN, the owning U.NORMAL
	create,delete	U.ADMIN
Role	query	U.ADMIN
	create,modify,delete	U.ADMIN

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies:

FMT_MSA.1	Management of security attributes
FMT_SMR.1	Security roles

FMT_MSA.3.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

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

- restrictive

FMT_MSA.3.2 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

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 19.**

Table 19 - Device management Function

Data	Operation	Authorised role(s)
ユーザーパスワード	create, delete	U.ADMIN
	modify	U.ADMIN, the owning U.NORMAL
監査ログ	query	U.ADMIN
日付/時刻設定	modify	U.ADMIN
IPSec 設定	query, modify	U.ADMIN
TLS 設定	query, modify	U.ADMIN
自動ログアウト設定	query, modify	U.ADMIN
ロックアウトポリシー設定	query, modify	U.ADMIN
パスワードポリシー設定	query, modify	U.ADMIN
監査ログ設定	query, modify	U.ADMIN
ファームウェア	modify	U.ADMIN

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

- Table 20 を参照

Table 20 – Management Functions

Management Functions
ユーザー管理機能
日付/時刻設定の管理機能
IPSec 設定の管理機能
TLS 設定の管理機能
自動ログアウト設定の管理機能
ロックアウトポリシー設定の管理機能
パスワードポリシー設定の管理機能
監査ログ管理機能
高信頼アップデート管理機能

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

6.2.7 Class FPR: Privacy

There are no class FPR requirements.

6.2.8 Class FPT: Protection of the TSF

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST_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.

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.

[selection: *published hash, no other functions*]
- no other functions

6.2.9 Class FRU: Resource Utilization

There are no class FRU requirements.

6.2.10 Class FTA: TOE Access

FTA_SSL.3 (LUI) TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[assignment: *time interval of user inactivity*]
- 操作パネルを操作しない状態が、設定時間経過

FTA_SSL.3 (RUI) TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[assignment: time interval of user inactivity]

- リモート UI を操作しない状態が、設定時間経過

6.2.11 Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

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

FTP_ITC.1.1 Refinement: The TSF shall use [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

[selection: *IPsec, SSH, TLS, TLS/HTTPS*]

- IPsec

[selection: *authentication server, [assignment: other capabilities]*]

- [assignment: *other capabilities*]

[assignment: *other capabilities*]

- ファイルサーバー、監査ログサーバー、タイムサーバー

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

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for [assignment: *list of services for which the TSF is able to initiate communications*].

[assignment: *list of services for which the TSF is able to initiate communications*]

- 送信サービス、監査ログサービス、タイムサービス

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

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, TLS/HTTPS

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)

Hierarchical to: No other components.

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

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

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

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

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

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

6.3 セキュリティ保証要件

Table 21 lists the Security Assurance Requirements for Protection Profile for Hardcopy Devices, and related EAL1 augmented by ASE_SPD.1.

Table 21 —TOE Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: 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
ATE: Tests	ATE_IND.1 Independent testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6.4 セキュリティ機能要件根拠

6.4.1 The dependencies of security requirements

本章では、ST で機能要件の依存性を満たしていても問題のない理由を記述する。

Table 22 — The dependencies of security requirements

機能要件	PP で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A (依存性を満たしている)
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	N/A (依存性を満たしている)
	FIA_UID.1	FIA_UID.1	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A (依存性を満たしている)
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A (依存性を満たしている)
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A (依存性を満たしている)
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A (依存性を満たしている)
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1	N/A (依存性を満たしている)
	FTP_ITC.1	FTP_ITC.1	
FCS_CKM.1(a)	FCS_COP.1(b)	FCS_COP.1(b)	N/A (依存性を満たしている)
	FCS_CKM_EXT.4	FCS_CKM_EXT.4	
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)] FCS_CKM_EXT.4 FCS_RBG_EXT.1	FCS_COP.1(a) FCS_COP.1(d) FCS_COP.1(g) FCS_CKM_EXT.4 FCS_RBG_EXT.1(network) FCS_RBG_EXT.1(ssd)	N/A (依存性を満たしている)
FCS_CKM_EXT.4	[FCS_CKM.1(a) or FCS_CKM.1(b)]	FCS_CKM.1(a) FCS_CKM.1(b)	N/A (依存性を満たしている)

機能要件	PP で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
	FCS_CKM.4	FCS_CKM.4	
FCS_CKM.4	[FCS_CKM.1(a) or FCS_CKM.1(b)]	FCS_CKM.1(a) FCS_CKM.1(b)	N/A (依存性を満たしている)
FCS_COP.1(a)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (依存性を満たしている)
FCS_COP.1(b)(update)	FCS_CKM.1(a) FCS_CKM_EXT.4	No dependencies	予め埋め込まれた公開鍵で検証するのみであるため、暗号鍵生成及び破棄は不要。
FCS_COP.1(b)(tls)	FCS_CKM.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	N/A (依存性を満たしている)
FCS_COP.1(b)(ipsec)	FCS_CKM.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	N/A (依存性を満たしている)
FCS_COP.1(c)	No dependencies	No dependencies	N/A (依存性の要求なし)
FCS_COP.1(d)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (依存性を満たしている)
FCS_COP.1(g)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (依存性を満たしている)
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	N/A (依存性を満たしている)
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) (ipsec) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1(network)	N/A (依存性を満たしている)
FCS_KYC_EXT.1	[FCS_COP.1(e), or FCS_SMC_EXT.1, or FCS_COP.1(f), or FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_SMC_EXT.1	N/A (依存性を満たしている)
FCS_RBG_EXT.1 (network)	No dependencies	No dependencies	N/A (依存性の要求なし)
FCS_RBG_EXT.1(ssd)	No dependencies	No dependencies	N/A (依存性の要求なし)
FCS_SMC_EXT.1	FCS_COP.1(c)	FCS_COP.1(c)	N/A (依存性を満たしている)
FCS_TLS_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	FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b)(tls) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1(network)	N/A (依存性を満たしている)
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A (依存性を満たしている)
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	N/A (依存性を満たしている)
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	N/A (依存性を満たしている)

機能要件	PP で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A (依存性を満たしている)
FIA_ATD.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FIA_PMG_EXT.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FIA_PSK_EXT.1	FCS_RBG_EXT.1	No dependencies	FCS_RBG_EXT.1 を主張していない理由: SFR で選択していないため不要。
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A (依存性を満たしている)
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A (依存性を満たしている)
FIA_UID.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A (依存性を満たしている)
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (依存性を満たしている)
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	N/A (依存性を満たしている)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	N/A (依存性を満たしている)
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (依存性を満たしている)
FMT_SMF.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A (依存性を満たしている)
FPT_KYP_EXT.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FPT_SKP_EXT.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FPT_STM.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FPT_TST_EXT.1	No dependencies	No dependencies	N/A (依存性の要求なし)
FPT_TUD_EXT.1	FCS_COP.1(b) FCS_COP.1(c)	FCS_COP.1(b) (update) FCS_COP.1(c)	N/A (依存性を満たしている)
FTA_SSL.3(LUI)	No dependencies	No dependencies	N/A (依存性の要求なし)
FTA_SSL.3(RUI)	No dependencies	No dependencies	N/A (依存性の要求なし)
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1	N/A (依存性を満たしている)
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 FCS_TLS_EXT.1 FCS_HTTPS_EXT.1	N/A (依存性を満たしている)
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 (依存性を満たしている)

7 TOE 要約仕様

7.1 ユーザー認証機能

- 対応する機能要件: **FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1, FIA_USB.1, FIA_AFL.1, FTA_SSL.3(LUI), FTA_SSL.3(RUI)**

TOE は、正規のユーザーを識別認証するために、ユーザーが操作パネルやリモート UI においてデジタル複合機を操作する前にユーザーの識別認証を要求する。また、プリントジョブ投入時は、クライアント PC 上のプリンタードライバを通して要求されるユーザーの識別認証を行う。[**FIA_UAU.1, FIA_UID.1**]

ユーザー認証は、以下の認証方式をサポートする。

- 内部認証方式
デバイスに登録されているユーザー情報を利用する認証方式。

TOE はユーザー認証として、操作パネル及びリモート UI のログイン画面からユーザー名・パスワード・認証先であるログイン先の入力を要求して、指定したログイン先にてユーザー名・パスワードが合致した場合のみユーザーを識別認証する。パスワード入力の際のパスワードテキストエリアは、操作パネル”*”、リモート UI は”●”と表示する。[**FIA_UAU.7**]

TOE は利用者に対して、ユーザー名とロールを属性として維持する。TOE は、ユーザーの識別認証に成功すると、ユーザーごとに Access Control Token(以後 ACT)を発行することで属性を割り付ける。

[**FIA_ATD.1, FIA_USB.1**]

操作パネル:	- 設定/登録>機器設定>管理設定>ユーザー管理>認証管理>認証ユーザーの登録/編集
リモート UI:	- 設定/登録>管理設定>ユーザー管理>認証管理

TOE は、操作パネル、リモート UI 及びプリンタードライバにおけるユーザー認証において、不正なログイン試行を減らすためロックアウト機能を提供する。[**FIA_AFL.1**]

ロックアウト機能の動作設定は U.ADMIN のみ可能で以下の操作で変更できる。

操作パネル:	- 設定/登録>機器設定>管理設定>セキュリティ設定>認証/パスワード設定>認証機能の設定
リモート UI:	- 設定/登録>管理設定>セキュリティ設定>認証/パスワード設定>認証機能の設定

ロックアウト機能は以下の条件が設定でき、条件に合致するとそのアカウントはロックアウトされる。

- 操作パネル/リモート UI/プリンタードライバからのログイン試行の失敗回数を積算し、設定したログイン試行の許容回数に達した場合、ログインに失敗したアカウントをロックアウトし、ログインを認めない。ログイン試行の許容回数は、1~10 回から選択できるうち 3 回以下を設定する。
- ロックアウト時間は 1-60 分から選択できるうち、3 分以上を設定する。設定したロックアウト時間が経過するまで、該当ユーザーのログインを認めない

TOE は、ログインしたユーザーが指定時間操作しない場合、自動的にログアウトさせる自動ログアウト機能を持つ。操作パネルからログインされた場合はオートクリア移行時間設定により、リモート UI からログインさ

れた場合はセッション設定により、管理者はそれぞれの自動ログアウト時間を設定できる。

[FTA_SSL.3(LUD)] [FTA_SSL.3(RUD)]

オートクリア移行時間の設定は U.ADMIN のみ可能で以下の操作で変更できる。

操作パネル:	<ul style="list-style-type: none"> - 設定/登録>機器設定>環境設定>タイマー/電力設定>オートクリア移行時間 - 設定/登録>機器設定>環境設定>タイマー/電力設定>オートクリア移行時間の制限
リモート UI:	<ul style="list-style-type: none"> - 設定/登録>環境設定>タイマー/電力設定>省電力設定>オートクリア移行時間 - 設定/登録>環境設定>タイマー/電力設定>オートクリア移行時間の制限

オートクリア移行時間は以下の条件が設定でき、条件に合致するとそのアカウントはログアウトされる。

- 操作パネルを操作しない状態が、オートクリア移行時間設定にて設定されたタイムアウト時間経過した場合。タイムアウト時間は、10 秒-9 分の範囲で指定できる。(初期値は 2 分)

セッション設定は U.ADMIN のみ可能で以下の操作で変更できる。

リモート UI:	- 設定/登録>環境設定>ネットワーク>セッション設定
----------	-----------------------------

セッション設定は以下の条件が設定でき、条件に合致するとそのアカウントはログアウトされる。

- リモート UI を操作しない状態が、セッション設定にて設定されたタイムアウト時間を経過した場合。タイムアウト時間は、15 分-150 分から選択できる。(初期値は 15 分)。

7.2 アクセス制御機能

TOE は、TOE が持つプリント機能、スキャン機能、コピー機能、文書の保存と取り出し機能で処理するジョブ及びジョブ中の電子文書に対して、以下のアクセス制御機能を有している。

- プリント機能 : プリント処理制御機能
- スキャン機能 : スキャン処理制御機能
- コピー機能 : コピー処理制御機能
- 文書の保存と取り出し機能 : 文書の保存と取り出し処理制御機能

TOE は、識別認証されたユーザーに発行された ACT の内容に応じて、ユーザー名の識別及びユーザーに割り当てられたロールの識別を行なうことで、これらのアクセス制御機能を実行する。

7.2.1 プリント処理制御機能

- 対応する機能要件:FDP_ACC.1, FDP_ACF.1, FMT_MSA.3

TOE はプリント処理について、以下のアクセス制御機能を提供する。プリント文書及びプリントジョブに付与されるユーザー名は、投入ジョブ生成時にそのジョブを生成したユーザー名で初期化されている。また、プリント文書及びプリントジョブに付与されたユーザー名ほどのユーザーも変更することはできない。

TOE は、プリントジョブが投入されると、そのままプリントせずに一時保存する。更に、プリントジョブに付与されたユーザー名でそのプリントジョブの所有者を判断し、以下のアクセス制御を実現している。

[プリント文書の投入・プリントジョブの作成]

TOE はプリント文書の投入及びプリントジョブの作成を全ての認証ユーザー(ジョブ所有者、U.ADMIN、U.NORMAL)に許可している。未認証ユーザーには許可しない。

プリント文書の投入及びプリントジョブの作成は以下の手段で行われ、印刷指示されたデータは、プリント機能に留め置かれる。

- ・ユーザーはクライアント PC からプリンタードライバーを通してプリントジョブを投入する。ジョブ投入時に識別認証を行い、識別認証に失敗すると TOE にジョブを投入することはできない。

[画像の閲覧、印刷]

TOE は、ジョブ所有者(自身のユーザー名とプリントジョブのユーザー名が一致した場合)について、一時保存したプリントジョブの電子文書の画像の閲覧、印刷を許可している。

画像の閲覧、印刷指示は以下の手段で行われる。

- ・操作パネルにログインし、「プリント」を選択すると、自分用に留め置かれたデータがリストアップされる。プリント機能は留め置かれたデータの画像表示ができる。
- ・プリント機能で留め置かれたデータの印刷指示ができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外の一時保存したプリントジョブの電子文書をインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、画像の閲覧、印刷を許可しない。

[プリントキュー/ログを閲覧]

TOE は、ジョブ所有者、U.ADMIN に、プリントキュー/ログの閲覧を許可している。

プリントキュー/ログの閲覧は以下の手段で行われる。

- ・ジョブ所有者及び U.ADMIN は操作パネルにログインし、状況確認画面から印刷中・印刷待ちジョブのリスト、およびジョブログを確認することができる。ただし、ジョブ所有者は、自身がジョブ所有者(自身のユーザー名とプリントジョブのユーザー名が一致した場合)となっているもののみ表示される。自身がジョブ所有者でないジョブについては、ジョブ名・ユーザー名などがマスクされるためプリントキュー/ログの閲覧はできない。
- ・ジョブ所有者は、操作パネルにログインし、「プリント」を選択すると、自分用に留め置かれたデータがリストアップされる。
- ・U.ADMIN はリモート UI にログインし、状況確認画面から印刷中・印刷待ちジョブのリスト、およびジョブログを確認することができる。

TOE は、U.NORMAL に対しては、自身のユーザー名と付与されたユーザー名が一致しないプリントジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、プリントキュー/ログの閲覧を許可しない。

[プリント文書、プリントジョブの改変]

TOE は、ジョブ所有者へ、自分自身が所有するプリント文書及びプリントジョブの改変を許可している。

プリント文書及びプリントジョブの改変は以下の手段で行われる。

- ・操作パネルにログインし、「プリント」を選択すると、自分用に留め置かれたデータがリストアップされる。プリント機能の画像表示機能から、ページ単位の改変(削除)ができる。
- ・操作パネルにログインし、「プリント」を選択すると、自分用に留め置かれたデータがリストアップされる。ジョブを選択すると、ジョブ条件(印刷部数や印刷範囲等)を変更することができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外のプリント文書及びプリントジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、プリント文書及びプリントジョブの改変を許可しない。

[削除]

TOE は、ジョブ所有者、U.ADMIN に、プリント文書及びプリントジョブに対する削除を許可している。

プリント文書及びプリントジョブの削除は以下の手段で行われる。

- ・ジョブ所有者は、操作パネルにログインし「プリント」を選択すると、自分用に留め置かれたプリントジョブがリストアップされる。プリント機能のジョブ削除機能から、プリントジョブ及びプリント文書を全て削除できる。
- ・操作パネルにログインし、状況確認画面からプリントジョブを選択して中止することで、プリント文書が削除できる。ジョブ所有者は所有しているプリントジョブ、U.ADMIN は全ユーザーのプリントジョブ及びプリント文書を削除できる。
- ・U.ADMIN はリモート UI にログインし、状況確認画面から全ユーザーのプリントジョブ及びプリント文書を削除できる。

TOE は、U.NORMAL に対しては、自身のユーザー名と付与されたユーザー名が一致しないプリント文書及びプリントジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、プリント文書及びプリントジョブの削除を許可しない。

7.2.2 スキャン処理制御機能

- 対応する機能要件:FDP_ACC.1, FDP_ACF.1, FMT_MSA.3

TOE はスキャン処理について、以下のアクセス制御機能を提供する。スキャン文書及びスキャンジョブに付与されるユーザー名は、スキャンジョブ生成時にそのジョブを生成したユーザー名で初期化されている。また、スキャン文書及びスキャンジョブに付与されたユーザー名はどのユーザーも変更することはできない。

スキャンジョブには一時保存するためのスキャンジョブ一時保存機能として、「タイマー送信」と「プレビュー」がある。

[スキャン文書の投入・スキャンジョブの作成]

TOE はスキャン文書の投入及びスキャンジョブの作成をジョブ所有者、U.ADMIN、U.NORMAL に許可している。

スキャン文書の投入及びスキャンジョブの作成は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択しスタートボタンを押す。宛先にはファイルサーバーを指定できる。スキャンジョブが生成され、原稿が読み込まれ画像データが格納される。その後、TOE に接続された LAN より、ファイルサーバーへ送信される。

TOE は、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャン文書の投入及びスキャンジョブの作成を許可しない。

[スキャン画像の閲覧]

TOE はスキャン画像の閲覧権限をジョブ所有者に許可している。

スキャン画像の閲覧は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択する。その他設定で、「プレビュー」を有効にしてスタートボタンを押す。原稿が読み込まれ、画像データが操作パネルに表示される。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外のスキャン文書をインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャン画像の閲覧を許可しない。

[スキャンジョブ状況/ログの閲覧]

TOE はスキャンジョブ状況/ログの閲覧権限をジョブ所有者、U.ADMIN、U.NORMAL に許可している。

スキャンジョブ状況/ログの閲覧は以下の手段で行われる。

- ・操作パネルにログインし、状況確認画面の「送信」で、ジョブ状況やジョブ履歴が確認できる。ただし、U.NORMAL の場合、ジョブ状況に他人のジョブを含んだジョブリストを表示できるが、他人のジョブの宛先等詳細は表示されない。また、ジョブ履歴にも自分のジョブ以外表示されない。
- ・U.ADMIN は、リモート UI にログインし、状況確認画面の「送信」で、ジョブ状況やジョブ履歴が確認できる。

TOE は、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャンジョブ状況/ログの閲覧を許可しない。

[スキャン文書の改変]

TOE はスキャン文書の改変権限をジョブ所有者に許可している。

スキャン文書の改変は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択する。「その他の機能」設定で、プレビューを有効にしてスタートボタンを押す。原稿が読み込まれ、画像データが操作パネルに表示されている状態で、ページの削除や移動ができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外のスキャン文書をインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャン文書の改変を許可しない。

[スキャンジョブの改変]

TOE はスキャンジョブの改変権限をジョブ所有者、U.ADMIN に許可している。

スキャンジョブの改変は以下の手段で行われる。

- ・操作パネルにログインし、状況確認画面の「送信」の「ジョブ状況」画面でジョブを選択する。「詳細情報」を表示させると宛先を変更することができる。

TOE は、U.NORMAL に対しては、ジョブ所有者以外のスキャンジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャンジョブの改変を許可しない。

[スキャン文書の削除・スキャンジョブの削除]

TOE は、スキャン文書及びスキャンジョブに対する削除をジョブ所有者、U.ADMIN に許可している。

スキャン文書及びスキャンジョブの削除は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択しスタートボタンを押す。読込中画面で中止ボタンを押すことで、それまで読込んだスキャン文書が削除され、スキャンジョブも削除される。
- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択する。「その他の機能」設定で、プレビューを有効にしてスタートボタンを押す。原稿が読み込まれ、スキャン文書が操作パネルに表示されている状態で、送信ジョブの停止をすることでスキャン文書が削除され、スキャンジョブが削除される。
- ・スキャナに原稿を載せ、操作パネルにログインして「スキャンして送信」を選択し、宛先を選択する。「その他の機能」設定で、タイマー送信を有効にしてスタートボタンを押す。原稿が読み込まれた後、状況確認画面の送信ジョブ状況を表示させる。スキャンジョブを選択し、中止ボタンを押すことでスキャン文書が削除され、スキャンジョブが削除される。ただし、ジョブ所有者の場合は、自身のユーザー名とスキャンジョブのユーザー名が一致したジョブのみ削除できる。
- ・U.ADMIN はリモート UI にログインし、状況確認画面から送信ジョブを選択して中止することで、スキャン文書が削除され、スキャンジョブが削除される。

TOE は、U.NORMAL に対しては、自身のユーザー名と付与されたユーザー名が一致しないスキャン文書及びスキャンジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、スキャン文書及びスキャンジョブの削除を許可しない。

7.2.3 コピー処理制御機能

- 対応する機能要件: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3

TOE はコピー処理について、以下のアクセス制御機能を提供する。コピー文書及びコピージョブに付与されるユーザー名は、コピージョブ生成時にそのジョブを生成したユーザー名で初期化されている。また、コピー文書及びコピージョブに付与されたユーザー名はどのユーザーも変更することはできない。

[コピー文書の投入・コピージョブの作成]

TOE はコピー文書の投入及びコピージョブの作成をジョブ所有者、U.ADMIN、U.NORMAL に許可している。

コピー文書の投入及びコピージョブの作成は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「コピー」を選択する。場合により必要な設定を行い、スタートボタンを押す。コピージョブが生成され、原稿が読み込まれる。

TOE は、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、コピー文書の投入及びコピージョブの作成を許可しない。

[画像の閲覧]

TOE は、コピー画像の閲覧をジョブ所有者に許可している。

画像の閲覧は以下の手段で行われる。

- ・スキャナに原稿を載せ、操作パネルにログインして「コピー」を選択し、その他の機能からジョブ結合を指定する。スタートボタンを押して読み込んだジョブを選択し、その他の動作からプレビューを選択することで、画像を表示することができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外のコピー画像をインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、画像の閲覧を許可しない。

[コピージョブ状況/ログの閲覧]

TOE はコピージョブ状況/ログの閲覧権限をジョブ所有者、U.ADMIN に許可している。

コピージョブ状況/ログの閲覧は以下の手段で行われる。

- 操作パネルにログインし、状況確認画面の「コピー/プリント」画面で、ジョブ状況やジョブ履歴が確認できる。ただし、ジョブ所有者の場合は、ジョブ履歴には自身がジョブ所有者となっている以外のジョブは表示されない。
- U.ADMIN は、リモート UI にログインし、状況確認画面の「コピー/プリント」画面で、ジョブ状況やジョブ履歴が確認できる。

TOE は、U.NORMAL に対しては、自身のユーザー名と付与されたユーザー名が一致しないコピージョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、コピージョブ状況/ログの閲覧を許可しない。

[コピー文書の改変]

TOE はコピー文書の改変権限をジョブ所有者に許可している。

コピー文書の改変は以下の手段で行われる。

- スキャナに原稿を載せ、操作パネルにログインして「コピー」を選択し、その他の機能からジョブ結合を指定する。スタートボタンを押し読込んだジョブのページを指定して削除することができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外のコピー文書をインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、コピー文書の改変を許可しない。

[コピージョブの改変]

TOE はコピージョブの改変機能を持たない。

よって TOE は、ジョブ所有者、U.ADMIN、U.NORMAL、未認証ユーザーに対して、コピージョブの改変を許可しない。

[削除]

TOE は、コピー文書及びコピージョブに対する削除をジョブ所有者、U.ADMIN に許可している。

コピー文書及びコピージョブの削除は以下の手段で行われる。

- スキャナに原稿を載せ、操作パネルにログインして「コピー」を選択し、スタートボタンを押す。ジョブ所有者は、原稿読込中画面で中止ボタンを押すことで、コピージョブを中止し、読込んだ画像データが削除される。
- スキャナに原稿を載せ、操作パネルにログインして「コピー」を選択し、スタートボタンを押す。原稿が読み込まれコピーが実行される。状況確認画面で、実行中のコピージョブの中止を指示することで、コピージョブを中止し、読込んだ画像データが削除される。
- U.ADMIN はリモート UI にログインし、状況確認画面からジョブを選択して中止することで、コピージョブを中止し、読込んだ画像データが削除される。

TOE は、U.NORMAL に対しては、自身のユーザー名と付与されたユーザー名が一致しないコピー文書及びコピージョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、コピー文書及びコピージョブの削除を許可しない。

7.2.4 文書の保存と取り出し処理制御機能

- 対応する機能要件: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3

TOE は文書の保存と取り出し処理について、以下のアクセス制御機能を提供する。文書の保存と取り出しの文書及びジョブに付与されるユーザー名は、文書の保存と取り出しジョブ生成時にそのジョブを生成したユーザー名で初期化されている。また、文書及びジョブに付与されたユーザー名はどのユーザーも変更することはできない。

TOE は、スキャナから読み込んだ電子文書を、アドバンスドボックスに保存する機能と、保存した文書を取り出す機能を提供する。保存先は、アドバンスドボックス内の、ログインしたユーザーのみがアクセスできるようアクセス制御された、個人スペースを使用する。

[文書の保存・保存ジョブの作成]

TOE は文書の保存及び保存ジョブの作成をジョブ所有者、U.ADMIN、U.NORMAL に許可している。

文書の保存及び保存ジョブの作成は以下の手段で行われる。

- ・保存ジョブは、スキャナに原稿を載せ、操作パネルにログインして「スキャンして保存」-「アドバンスドボックス」-「個人スペース」を選択し、ユーザーの個人スペースを指定する。スタートボタンを押すと保存ジョブが生成され、原稿が読み込まれ画像データファイルが個人スペースに生成・保存される。

TOE は、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、文書の保存及び保存ジョブの作成を許可しない。

[文書の取り出し・取り出しジョブの作成]

TOE は文書の取り出し及び取り出しジョブの作成をジョブ所有者、U.ADMIN に許可している。

文書の取り出し及び取り出しジョブの作成は以下の手段で行われる。

- ・取り出しジョブは、操作パネルにログインし、「保存ファイルの利用」-「アドバンスドボックス」-「個人スペース」を指定し、保存されているファイルを選択する。「プリントする」ボタンを押すことで、文書を取り出す印刷ジョブを作成することができる。

TOE は、U.NORMAL に対しては、自身の個人スペース以外のスペースをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、文書の取り出し及び取り出しジョブの作成を許可しない。

[保存/取り出しログの閲覧]

TOE は保存/取り出しログの閲覧権限をジョブ所有者、U.ADMIN、U.NORMAL に許可している。

保存/取り出しログの閲覧は以下の手段で行われる。

- 保存ログは、操作パネルにログインし、状況確認画面の「保存/ジョブ履歴」画面に表示できる。
- 保存ログは、U.ADMIN ではさらに、リモート UI にログインし、状況確認画面の「保存コピー/プリント」画面の「ジョブ履歴」画面のローカルプリント表示にて、保存した際のジョブログが表示できる。
- 取り出しログは、操作パネルにログインし、状況確認画面の「コピー/プリント」画面の「ジョブ履歴」画面のローカルプリント表示にて表示できる。
- 取り出しログは、U.ADMIN ではさらに、リモート UI にログインし、状況確認画面の「コピー/プリント」画面の「ジョブ履歴」画面のローカルプリント表示にて表示できる。

TOE は、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表さないことで、保存/取り出しログの閲覧を許可しない。

[保存文書の改変]

TOE は保存文書の改変権限をジョブ所有者に許可している。

保存文書の改変は以下の手段で行われる。

- 操作パネルにログインし、「保存ファイルの利用」-「アドバンスドボックス」-「個人スペース」を指定し、ファイルを選択して「ファイル編集」-「ファイル名変更」を指定することで、ファイル名の変更ができる。

TOE は、U.ADMIN 及び U.NORMAL に対しては、ジョブ所有者以外の個人スペースをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、保存文書の改変を許可しない。

[保存/取り出しジョブの改変]

TOE は保存/取り出しジョブの改変機能を持たない。

TOE は、ジョブ所有者、U.ADMIN、U.NORMAL、未認証ユーザーに対して、保存/取り出しジョブの改変を許可しない。

[保存文書の削除]

TOE は、保存文書対する削除をジョブ所有者、U.ADMIN に許可している。

保存文書の削除は以下の手段で行われる。

- ジョブ所有者は、操作パネルにログインし、「保存ファイルの利用」-「アドバンスドボックス」-「個人スペース」を指定し、ファイルを選択して「ファイル編集」-「削除」を指定することで、保存文書の削除ができる。
- U.ADMIN は、操作パネルにログインし、「設定/登録」-「ファンクション設定」-「ファイル保存/利用」-「アドバンスドボックス設定」-「個人スペースの一括削除」を指定することで、保存文書の削除ができる。

- ・U.ADMIN は、リモート UI にログインし、「設定/登録」-「ファイル保存/利用」-「アドバンスドボックスの設定」-「個人スペースの削除」より、保存文書の削除ができる。

TOE は、U.NORMAL に対しては、自身の個人スペース以外のスペースをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、保存文書の削除を許可しない。

[保存/取り出しジョブの削除]

TOE は、保存/取り出しジョブに対する削除をジョブ所有者、U.ADMIN に許可している。

保存/取り出しジョブの削除は以下の手段で行われる。

- ・ジョブ所有者は、保存ジョブの生成後、操作パネルに表示される中止もしくはストップボタンを押すことで保存ジョブの削除ができる。また、状況確認画面の「保存」もしくは「コピー/プリント」のジョブ状況画面にて中止を指定し、保存ジョブの削除ができる。
- ・U.ADMIN は、リモート UI にログインし、状況確認画面の「保存/ジョブ状況」にて中止を指定することで、保存ジョブの削除ができる。

TOE は、U.NORMAL に対しては、自身のジョブ以外のジョブをインターフェース上に表示しないことで、未認証ユーザーに対しては、識別認証の失敗により操作するためのインターフェースを表示しないことで、保存/取り出しジョブの削除を許可しない。

7.3 SSD 暗号化機能

- 対応する機能要件: FDP_DSK_EXT.1

TOE 内蔵 SSD へのアクセスは、全て TOE のコントローラーボード上に実装される SSD 暗号化チップを経由する。これにより、コントローラーボードと TOE 内蔵 SSD との間で入出力されるユーザーデータおよび TSF データを含む全データは暗号化され、TOE 内蔵 SSD へは暗号化されたデータが保存される。

[FDP_DSK_EXT.1.1]

SSD 暗号化機能は、TOE に SSD を接続して最初に起動した時から自動的に有効になり、動作を制御するインターフェースは存在しないことから、U.ADMIN や利用者は TOE の SSD 暗号化機能に対して何ら設定する必要はない。[FDP_DSK_EXT.1.2]

ユーザーデータや TSF データを含め TOE 内蔵 SSD へ書き込む際は、必ず SSD 暗号化チップを経由し暗号化を行ってから TOE 内蔵 SSD に書き込まれる。また、TOE 内蔵 SSD から読み出す際も全ての読み込みが SSD 暗号化チップを経由して復号を行う。暗号化/復号機能によって、TOE 内蔵 SSD に格納されるユーザーデータおよび TSF データを含む全データの機密性を確保する。

7.3.1 暗号化/復号機能

- 対応する機能要件: FCS_COP.1(d)

TOE は、すべてのインターフェースから TOE 内蔵 SSD に格納されるユーザーデータおよび TSF データの機密性を確保するために、次の暗号操作を行い TOE 内蔵 SSD に格納される全てのデータを暗号化する。[FCS_COP.1(d)]

- TOE 内蔵 SSD へ書き込まれるデータを暗号化する。
- TOE 内蔵 SSD から読み出されるデータを復号する。

暗号操作に用いる暗号アルゴリズム、暗号鍵は以下のとおりである。

- ISO/IEC 18033-3 に従った「AES アルゴリズム」
- IEEE1619 で指定された XTS モード
- AES の鍵長が「256 ビット」の暗号鍵

7.3.2 暗号鍵管理機能

- 対応する機能要件: **FCS_CKM.1(b), FCS_CKM.4, FCS_CKM.1(c), FCS_CKM_EXT.4, FCS_RBG_EXT.1(ssd), FCS_KYC_EXT.1, FCS_SMC_EXT.1, FPT_KYP_EXT.1, FPT_SKP_EXT.1**

SSD 暗号化機能が取り扱う CSP (Critical Security Parameter) について説明する。

CSP 識別	説明	格納場所	格納状態	破棄方法
暗号鍵	暗号のための鍵。	暗号化チップ内の RAM	平文	TOE の電源断により消失
鍵シード	DRBG の内部状態 V 及び C であり、AES 暗号鍵生成に使用するシード値。	暗号化チップ内の FLASH メモリー	平文	固定値(0xFF)で 1 回上書き

次に、暗号鍵のライフサイクル(生成、管理、破棄方法)について記載する。

[暗号鍵の生成方法]

TOE は、暗号化チップと TOE コントローラとの初回接続時(つまり、TOE 製造時) もしくは TOE 廃棄時など管理者が鍵シードの破棄・再生成を指示した場合に、次の仕様に基づき、SSD 暗号化機能で使用する鍵シードを生成する。

暗号化チップは、リングオシレータを用いた乱数生成器を 1 個のハードウェアベースのノイズ源とするエントロピー生成機能を用いて、DRBG へ入力する Entropy Input (640 ビット)、Nonce(256 ビット)を生成する。エントロピー生成機能によって生成される Entropy Input は、400 ビット、Nonce は 160 ビットのエントロピーを最低限持っている。これらの値を DRBG に入力することで DRBG の内部状態 V,C を初期化する。そして、DRBG 内部状態 V,C を暗号鍵の元となる鍵シードとして暗号化チップ内の FLASH メモリーに保存する。

[FCS_RBG_EXT.1(ssd)]

TOE は鍵シード(DRBG 内部状態 V,C)を DRBG に入力し、1 回目に生成される乱数を破棄し、2 回目、3 回目の乱数生成において内部状態 V,C をサブマスクとして SHA-256 を用いたサブマスク結合を行うことにより 256 ビットの暗号鍵を 2 本算出する。[FCS_SMC_EXT.1, FCS_COP.1(c), FCS_CKM.1(b)]

以降 TOE は、TOE 内蔵 SSD に格納する全てのデータを暗号化する。

次回電源 ON 時に、暗号化チップは鍵シードを元に自動的に暗号鍵を再構成し、RAM に格納する。

[暗号鍵の管理方法]

サブマスクである DRBG 内部状態 V,C には、エントロピー生成機能を用いて十分なエントロピーが供給されている。このサブマスクに対してサブマスク結合 (SP800-90A に基づく Hash DRBG による内部処理) を行うことにより 256bit 長の暗号鍵を構成していることから鍵チェーンの各段階において暗号鍵の強度 (256bit) は維持される。[FCS_KYC_EXT.1]

TOE は、暗号鍵の元となる鍵シードを平文で暗号化チップ内の FLASH メモリーに保存する。また、暗号鍵は暗号化チップ内の RAM 上にもみ格納され、FLASH メモリーには格納されない。

暗号化チップは TOE のコントローラーボードに実装されており、暗号化チップ内の FLASH メモリーは「現地交換可能な不揮発性ストレージデバイス」ではないため、鍵チェーンの一部が平文で現地交換可能な不揮発性ストレージデバイスに保存されることはない。[FPT_KYP_EXT.1]

暗号化チップ内の FLASH メモリーから暗号化チップ外に鍵シードを読み出す TOE のインターフェースはない。また暗号化チップ内の RAM から暗号化チップ外に暗号鍵を読み出すインターフェースはないため、鍵シードおよび暗号鍵を暴露から保護している。[FPT_SKP_EXT.1]

[暗号鍵の破棄方法]

暗号鍵は暗号化チップ内の RAM 上にもみ存在する。暗号鍵は電源断時に不要となるので、電源断により消失する。[FCS_CKM_EXT.4/ FCS_CKM.4]

鍵シードは、TOE 廃棄時など管理者が暗号鍵の変更が必要だと判断した際に不要となる。鍵シードの破棄は、操作パネルからの指示で実行される。鍵シードに対して固定値(0xFF)で 1 回上書きすることで鍵シードを破棄する。[FCS_CKM_EXT.4/ FCS_CKM.4]

7.4 LAN データ保護機能

7.4.1 IPsec 暗号化機能

- 対応する機能要件: FCS_COP.1(a), FCS_COP.1(c), FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b), FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_COP.1(g)

TOE は、ファイルサーバー/監査ログサーバー/タイムサーバーと TOE 間で送受信するユーザーデータおよび TSF データの機密性、完全性の確保のために、すべての IP パケットを RFC4301 で規定された IPsec にて以下のように暗号化/復号する。[FTP_ITC.1, FCS_IPSEC_EXT.1.1]

- LAN へ送信する IP パケットの暗号化操作
- LAN から受信する IP パケットの復号操作

一般利用者が、クライアント PC よりプリンタードライバーを使い印刷を行う際に、クライアント PC から TOE へと送信するユーザーデータおよび TSF データの機密性、完全性の確保のために、TOE はすべての IP パケットを RFC4301 で規定された IPsec にて以下のように暗号化/復号する。[FTP_TRP.1(b), FCS_IPSEC_EXT.1.1]

- LAN へ送信する IP パケットの暗号化操作
- LAN から受信する IP パケットの復号操作

管理者が、クライアント PC より Web ブラウザを使いリモート UI のページ操作を行う際に、クライアント PC から TOE へと送受信するユーザーデータおよび TSF データの機密性、完全性の確保のために、TOE はすべての IP パケットを RFC4301 で規定された IPSec にて以下のように暗号化/復号する。なおリモート UI 操作の保護については、IPSec 暗号化機能だけではなくさらに 7.4.3 記載の TLS 暗号化機能を合わせて用いることもできる。[FTP_TRP.1(a), FCS_IPSEC_EXT.1.1]

- LAN へ送信する IP パケットの暗号化操作
- LAN から受信する IP パケットの復号操作

下記の暗号アルゴリズム、暗号鍵を用いて、RFC4303 に定義された IPSec プロトコル ESP を実現している。[FCS_COP.1(a), FCS_COP.1(c)]

cryptographic algorithm	cryptographic key sizes	list of standards
AES-CBC+HMAC	128 bit, 256 bit	FIPS PUB 197(AES) NIST SP800-38A(CBC) FIPS PUB198-1(HMAC)
AES-GCM	128 bit, 256 bit	FIPS PUB 197(AES) NIST SP800-38D(GCM)

- 上記の HMAC で利用するセキュアハッシュアルゴリズム(SHA)は SHA-1。SHA-1 は、FIPS PUB198-1 に規定された The Keyed-Hash Message Authentication Code および FIPS PUB180-3 に規定された Secure Hash Standard を満たす。メッセージダイジェスト長は 160 ビット。HMAC で利用される鍵長は 160bit。[FCS_COP.1(g)]

IPSec の動作モードは、トランスポートモードのみをサポートしている。[FCS_IPSEC_EXT.1.2]

IPSec 接続設定は、Security Policy Database(SPD)として複数のルールを優先順位をつけて定義している。SPD には、ルールを適用する通信相手条件(IP アドレス、ポート番号)と、通信相手との通信方式(IKE 設定や IPSec 設定)、ルールそのものの有効/無効が定義されている。

IP パケットを送受信する場合、SPD の優先順位に従い、有効なルールから IKE のネゴシエーションを試みる。IKE が確立しなければパケットは破棄される。

IKE が確立した場合、確立した IKE を維持したまま SPD の優先順位の最上位から有効なルールの通信相手条件の合致を確認し、最初に合致したルールの IPSec 設定により通信を行う。全ての SPD の通信相手条件に合致しない IP パケットは破棄される。

最初に合致したルールで通信ができなかった場合は、パケットは破棄され、さらに優先順位の低いルールとの通信相手条件の合致は確認しない。[FCS_IPSEC_EXT.1.3]

IPSec で対応するプロトコルの仕様は以下の通りである。[FCS_IPSEC_EXT.1.4-7,9]

- RFC2407、2408、2409、4109、拡張シーケンス番号のための RFC4304 及びハッシュ関数の RFC4868 で定義された IKEv1
- IKEv1 のペイロード暗号:RFC3602 で規定された AES-CBC-128/AES-CBC-256
- IPSec ESP のペイロード暗号:RFC3602 で規定された AES-CBC-128/AES-CBC-256 及び RFC4106 で規定された AES-GCM-128/AES-GCM-256
- IKEv1 フェーズ 1 鍵交換はメインモードのみを使用する(アグレッシブモードは使用しない)

- サポートする DH グループは Group14(2048bit)、ECDH256bit、ECDH384bit であり、どれを利用するかを U.ADMIN が設定する。その後通信時に鍵交換及び鍵確立の実施により決定される。

IKEv1 の SA ライフタイムは、フェーズ 1 の SA で 24 時間以内とフェーズ 2 の SA で 8 時間以内時間を指定することで制限することができる。[FCS_IPSEC_EXT.1.8]

全ての IKE プロトコルは、RSA アルゴリズム、ECDSA アルゴリズム、事前共有鍵のいずれかを用いて、ピア認証を実行する。[FCS_IPSEC_EXT.1.10]

IPSec の事前共有鍵は、SPD のルールごとに設定することが可能である。[FIA_PSK_EXT.1.1]

事前共有鍵の文字数は、22 文字以上 24 文字以内で設定可能である。使用できる文字は、大文字・小文字・数字・特殊文字(「!」、「@」、「#」、「\$」、「%」、「^」、「&」、「*」、「(」、「)」)の組み合わせから作成可能である。[FIA_PSK_EXT.1.2]

事前共有鍵はテキストベースで作成されたもののみを、SHA-1、SHA-256、SHA-384 で条件つけて使用する。なお条件づけに用いるハッシュアルゴリズムは、IKE フェーズ 1 のネゴシエーションにより SHA-1、SHA-256、SHA-384 の中からいずれか一つが選択され使用される。[FIA_PSK_EXT.1.3]

IPsec 暗号化機能の設定は、操作パネルもしくはリモート UI より、U.ADMIN により管理機能から設定される。

操作パネル:	- 設定/登録>機器設定>環境設定>ネットワーク>TCP/IP 設定>IPSec 設定
リモート UI:	- 設定/登録>環境設定>ネットワーク>IPSec 設定 - 設定/登録>環境設定>ネットワーク>IPSec ポリシー一覧

7.4.2 IPSec 暗号鍵管理機能

- 対応する機能要件: FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM_EXT.4, FCS_CKM.4, FPT_SKP_EXT.1

IPSec 暗号鍵管理機能が取り扱う CSP について、以下に説明する。

CSP 識別	説明	格納場所	格納状態	破棄方法
事前共有鍵	IKEv1 にて事前共有鍵方式での認証で利用する共有鍵	SSD	暗号化	無し
MFP 鍵ペア	IKEv1 にてデジタル署名方式 (RSA、ECDSA) での認証で利用する TOE の鍵ペア	SSD	暗号化	無し
IKE 暗号鍵	IKEv1 で使用する暗号のための暗号鍵	RAM	平文	TOE の電源断により消失
DH 鍵ペア ECDH 鍵ペア	DH/ECDH による鍵交換の際に生成する公開鍵/秘密鍵	RAM	平文	TOE の電源断により消失
IPSec 暗号鍵	IPSec ESP で使用する暗号のための暗号鍵	RAM	平文	TOE の電源断により消失

IPSec 認証鍵	IPSec ESP で使用する認証のための鍵	RAM	平文	TOE の電源断により消失
DRBG 内部状態	乱数を生成するための DRBG 内部状態。	RAM	平文	TOE の電源断により消失

次に CSP のライフサイクルについて記載する。

[暗号鍵の生成方法]

TOE は、次の仕様に基づき、IPSec 暗号化機能で使用する暗号鍵を生成する。

CSP 識別	暗号アルゴリズム/鍵確立アルゴリズム	標準
MFP 鍵ペア	RSA(2048 ビット)	NIST SP800-56B Rev1:6.3.1.1 rsakpg1-basic
	ECDSA(P-256、P-384)	FIPS PUB 186-4 NIST SP800-56A Rev3: 5.6.1.2.2
IKE 暗号鍵	AES-CBC	FIPS PUB 197(AES) NIST SP800-38A(CBC)
DH 鍵ペア	DH(Group14)	NIST SP800-56A Rev3: 5.6.1.1 Approved Safe-Prime Groups
ECDH 鍵ペア	ECDH(P-256、P-384)	NIST SP800-56A Rev3: 5.7.1.2
IPSec 暗号鍵	AES-CBC	FIPS PUB 197(AES) NIST SP800-38A(CBC)
	AES_GCM	FIPS PUB 197(AES) NIST SP800-38D(GCM)
IPSec 認証鍵	HMAC	FIPS PUB 198-1

事前共有鍵は、操作パネル、もしくはリモート UI より TOE の管理機能を利用して U.ADMIN によって設定 (登録/変更/削除)される。なお事前共有鍵のテキストエリアは、操作パネルでは”*”, リモート UI では”●”で表示する。[FPT_SKP_EXT.1]

IPSec 認証鍵/DH 鍵ペア/ECDH 鍵ペアは IPSec 通信時のネゴシエーションによって生成される。MFP 鍵ペアは、操作パネルもしくはリモート UI から TOE の管理機能を利用して U.ADMIN が生成可能である。

[FCS_CKM.1(a)]

TOE は IKE 暗号鍵として、IPSec 通信のネゴシエーション時に 7.4.5 乱数生成機能を用いて 128bit もしくは 256bit の AES-CBC の暗号鍵を生成する。TOE は IPSec 暗号鍵として、IPSec 通信のネゴシエーション時に 7.4.5 乱数生成機能を用いて鍵長 128bit もしくは 256bit である、AES-CBC もしくは AES_GCM 暗号鍵を生成する。[FCS_CKM.1(b)]

[暗号鍵の管理方法]

CSP 識別	管理方法
--------	------

事前共有鍵及び MFP 鍵ペア	SSD 暗号化機能により暗号化し TOE 内蔵 SSD に格納する。
IKE 暗号鍵/ IPsec 暗号鍵/ IPsec 認証鍵/ DH 鍵ペア/ DRBG 内部状態	RAM 上に平文で格納する。

操作パネル、もしくはリモート UI より TOE の管理機能を利用しても、事前共有鍵及び MFP 鍵ペア/IKE 暗号鍵/ IPsec 暗号鍵/ IPsec 認証鍵/DH 鍵ペア/ ECDH 鍵ペアを読み出す、もしくは閲覧する機能はない。
[FPT_SKP_EXT.1]

[暗号鍵の破棄方法]

事前共有鍵及び MFP 鍵ペアは、暗号化して TOE 内蔵 SSD に保存している。そのため破棄は必要ない。

IKE 暗号鍵/ IPsec 暗号鍵/ IPsec 認証鍵/DH 鍵ペア/ ECDH 鍵ペア/ DRBG 内部状態は、IPsec 通信終了後 TOE の電源断時に不要となり、電源断により消失する。[FCS_CKM_EXT.4/FCS_CKM.4]

7.4.3 TLS 暗号化機能

- 対応する機能要件： FCS_COP.1(a), FCS_COP.1(c), FCS_COP.1(g), FTP_TRP.1(a), FCS_TLS_EXT.1, FCS_HTTPS_EXT.1

TOE は、U.ADMIN が以下の用途で TOE を利用する際に、送受信されるユーザーデータおよび TSF データの機密性、完全性の確保のために、TLS にて暗号化/復号する。

用途	対象ユーザー	プロトコル
Web ブラウザを使ったリモート UI のページ操作	U.ADMIN	TLS/HTTPS

TSF は、U.ADMIN によってクライアント PC 上の Web ブラウザーから TOE の Web ページに対して接続要求が行われた場合に、TOE とクライアント PC との間で TLS 通信のネゴシエーションを行い、TLS プロトコルによるサーバー認証が行なわれ、TLS によるセッションが確立された後、HTTPS 通信(RFC2818 適合)を開始する。[FCS_HTTPS_EXT.1]

ただしリモート UI 操作については、IPsec 暗号化機能が常に用いられており、TLS 暗号化機能は使わなくとも保護される。[FTP_TRP.1(a)]

暗号操作に用いる暗号アルゴリズム、暗号鍵は以下のとおりである。なお、AES 暗号アルゴリズムは FIPS PUB 197 に準拠している。[FCS_COP.1(a)]

cryptographic algorithm	cryptographic key sizes	list of standards
AES-CBC	128 bit, 256 bit	NIST SP800-38A
AES-GCM	128 bit, 256 bit	NIST SP800-38D

TLS では、以下のプロトコルに対応している。[FCS_TLS_EXT.1]

- TLS 1.2(RFC 5246)

TLS では、以下のサイフアスイートをサポートしている。[FCS_COP.1(a), FCS_COP.1(c), FCS_COP.1(g), FCS_TLS_EXT.1]

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS 暗号化機能の設定は、操作パネルもしくはリモート UI より、U.ADMIN により管理機能から設定される。

操作パネル:	- 設定/登録>機器設定>環境設定>ネットワーク>TCP/IP 設定>TLS 設定
リモート UI:	- 設定/登録>環境設定>ネットワーク>TLS 設定

7.4.4 TLS 暗号鍵管理機能

- 対応する機能要件: FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4, FCS_CKM_EXT.4, FPT_SKP_EXT.1

TLS 鍵管理機能が取り扱う CSP について、以下に説明する。

CSP 識別	説明	格納場所	格納状態	破棄方法
MFP 鍵ペア	デジタル署名方式(RSA または ECDSA)での認証で利用する TOE の鍵ペア	SSD	暗号化	無し
ECDH 鍵ペア	ECDH の際に生成する公開鍵/秘密鍵	RAM	平文	TOE 電源断により消去
TLS プリマスタシークレット	TLS 通信に利用するプリマスタシークレット	RAM	平文	TOE 電源断により消去
TLS セッション鍵	通信暗号のための暗号鍵	RAM	平文	TOE 電源断により消去
DRBG 内部状態	乱数を生成するための DRBG 内部状態。	RAM	平文	TOE の電源断により消失

次に CSP のライフサイクルについて記載する。

[暗号鍵の生成方法]

TOE は、次の仕様に基づき、TLS 暗号化機能で使用する暗号鍵を生成する。

CSP 識別	暗号アルゴリズム/鍵確立アルゴリズム	標準
MFP 鍵ペア	RSA(2048 ビット)	NIST SP800-56B Rev1:6.3.1.1 rsakpg1-basic
	ECDSA(P-256, P-384)	FIPS PUB 186-4 NIST SP800-56A Rev3: 5.6.1.2.2
ECDH 鍵ペア	ECDH(P-256, P-384)	NIST SP800-56A Rev3: 5.7.1.2
TLS セッション鍵	AES-CBC(128 ビット、256 ビット)	FIPS PUB 197(AES) NIST SP800-38A(CBC)
	AES-GCM(128 ビット、256 ビット)	FIPS PUB 197(AES) NIST SP800-38D(GCM)

MFP 鍵ペアは、操作パネルもしくはリモート UI から TOE の管理機能を利用して U.ADMIN が生成可能である。[FCS_CKM.1(a)]

TOE は TLS セッション鍵/ TLS プリマスタシークレット/ ECDH 鍵ペアを TLS 通信開始時に 7.4.5 乱数生成機能を用いて生成する。[FCS_CKM.1(a), FCS_CKM.1(b)]

[暗号鍵の管理方法]

CSP 識別	管理方法
MFP 鍵ペア	SSD 暗号化機能により暗号化し TOE 内蔵 SSD に格納する。
TLS セッション鍵/ TLS プリマスタシークレット/ ECDH 鍵ペア/ DRBG 内部状態	RAM 上に平文で格納する。

操作パネル、もしくはリモート UI より TOE の管理機能を利用しても、TLS セッション鍵/ TLS プリマスタシークレット/ ECDH 鍵ペア/ TOE 内蔵 SSD に保存されている MFP 鍵ペアを、読み出すもしくは閲覧する機能はない。[FPT_SKP_EXT.1]

[暗号鍵の破棄方法]

MFP 鍵ペアは、暗号化して TOE 内蔵 SSD に保存している。そのため破棄は必要ない。

TLS セッション鍵/ TLS プリマスタシークレット/ ECDH 鍵ペア/ DRBG 内部状態は、TOE の電源断時に不要となり、電源断により消失する。[FCS_CKM_EXT.4/FCS_CKM.4]

7.4.5 乱数生成機能

- 対応する機能要件: FCS_RB_G_EXT.1(network), FCS_COP.1(c)

TOE は、次の仕様に基づき、乱数生成を実行する。乱数生成機能によって生成された乱数は、IPSec 暗号化機能及び TLS 暗号化機能で使用される。

乱数生成アルゴリズム	標準
------------	----

CTR_DRBG(AES)	NIST SP800-90A
---------------	----------------

TOE は NIST SP800-90A に従って CTR_DRBG にエントロピー列を入力することで乱数生成を行う。

[FCS_RBG_EXT.1.1(network)]

TOE は、乱数生成の要求を受けると、CTR_DRBG を用いて 256 ビットの乱数を生成する。

[FCS_RBG_EXT.1.2(network)]

TOE はノイズ源としては、1 つのソフトウェアベースによるノイズ源を使用する。

TOE はノイズ源から取得したビット列(エントロピー:1,024 ビット、ナンス:256 ビット)をシードとして CTR_DRBG に入力する。

CTR_DRBG に入力するシードのエントロピー量は 256 ビットの乱数に求められるセキュリティ強度 384 ビットを越えており、SP800-90A 8.6.7 に定められた基準を満たしている。

7.5 署名検証/生成機能

7.5.1 TLS 署名生成機能

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

TLS のセッション確立時において、FIPS PUB 186-4 に基づく以下のアルゴリズムを用いて、署名生成を行なう。[FCS_COP.1(b)(tls)]

- RSA デジタル署名アルゴリズム(rDSA)で鍵長が 2048 ビットのもの
- 楕円曲線デジタル署名アルゴリズム(ECDSA)で鍵長が 256 ビット、384 ビットのもの

署名生成には SHA-256、SHA-384、SHA-512 を用いる。[FCS_COP.1(c)]

以下に使用可能な署名アルゴリズムとハッシュの組み合わせを示す。

- RSA2048 : SHA-256, RSA2048 : SHA-384, RSA2048 : SHA-512
- ECDSA-256: SHA-256
- ECDSA-384: SHA-384

7.5.2 IPSec 署名検証/生成機能

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

IPSec の IKEv1 での証明書を用いた認証において、FIPS PUB 186-4 に基づく以下のアルゴリズムで署名検証/生成を行なう。[FCS_COP.1(b)(ipsec)]

- RSA デジタル署名アルゴリズム(rDSA)で鍵長が 2048 ビットのもの
- 楕円曲線デジタル署名アルゴリズム(ECDSA)で鍵長が 256 ビット、384 ビットのもの

署名検証/生成には SHA-256 もしくは SHA-384 で算出したハッシュ値を用いる。[FCS_COP.1(c)]

以下に使用可能な署名アルゴリズムとハッシュの組み合わせを示す。

- RSA2048: SHA-256, RSA2048: SHA-384

- ECDSA-256:SHA-256
- ECDSA-384:SHA-384

7.6 自己テスト機能

- 対応する機能要件: **FPT_TST_EXT.1, FCS_COP.1(b)(update), FCS_COP.1(c)**

TOE は、起動時に以下の自己テストを実施する。[FPT_TST_EXT.1]

以下の自己テストでエラーが検出された場合、TOE は操作パネルにエラーコードを表示し、TOE の起動を中止する。

ファームウェアの完全性チェック

- ファームウェアには、あらかじめ FIPS PUB 186-4 に基づく RSA(鍵長 2048bit)、SHA-256 を用いて署名が付与されており、あらかじめ保持する公開鍵を用いて署名を復号して得られたハッシュ値と、ファームウェア自身から算出したハッシュ値を比較して完全性を検証する。
[FCS_COP.1(b)(update), FCS_COP.1(c)]

7.7 監査ログ機能

- 対応する機能要件: **FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FAU_STG_EXT.1, FMT_MTD.1**

TOE は、以下のイベントが生じた際に監査ログを生成する。[FAU_GEN.1]

監査ログの項目は以下である。[FAU_GEN.2]

- 日時、ユーザー名、イベント種別、結果(成功/失敗)

但し、以下のイベントの際には以下の項目も追加する。

- ジョブ完了の監査ログには、ジョブ種
- 認証失敗の監査ログには、認証試行したユーザー名
- セッションの確立失敗時の監査ログには、セッション確立失敗の理由

監査ログ対象事象	対象事象詳細及びインターフェース
監査機能の起動	TOE 電源 ON (本体電源スイッチ、操作パネル、リモート UI)
監査機能の終了	TOE 電源 OFF (本体電源スイッチ、操作パネル、リモート UI)
ジョブ完了	プリントジョブの終了 スキャンジョブの終了 コピージョブの終了 文書の保存ジョブの終了

	※上記は全て、FDP_ACC.1/FDP_ACF.1 に関連するインターフェース
ユーザー識別認証の失敗	操作パネルからのログイン試行 リモート UI からのログイン試行 プリンタードライバーからの認証試行
デバイス管理機能の利用	FMT_SMF.1 に関連するインターフェース使用
ユーザー管理機能の利用	FMT_SMF.1 に関連するインターフェース使用
利用者グループの改変	ロールの登録/変更/削除に関連するインターフェース使用
時刻の変更	日付/時刻設定の管理機能に関連するインターフェース使用
セッションの確立失敗	ネットワーク通信での IPSec セッション確立の失敗 ネットワーク通信での TLS セッション確立の失敗

監査ログに記録される日時情報は、TOE から提供される。TOE の日時情報は、下記管理機能の利用により手動で設定、もしくはタイムサーバーから正確な日時を取得して時刻同期することで設定される。なお、タイムサーバーはユーザーのオフィス環境内に構築されており、TOE とタイムサーバーとの通信は、LAN データ保護機能により、全ての IP パケットに対して IPSec による暗号化/復号が行なわれる。また、TOE の時刻管理にタイムサーバーを利用する設定は、操作パネルもしくはリモート UI より U.ADMIN のみが管理機能より設定することができる。[FPT_STM.1]

操作パネル:	- 設定/登録>機器設定>環境設定>タイマー/電力設定>日付/時刻設定 - 設定/登録>機器設定>環境設定>ネットワーク>TCP/IP 設定>SNTP 設定
リモート UI:	- 設定/登録>環境設定>タイマー/電力設定>日付/時刻の設定 - 設定/登録>環境設定>ネットワーク>SNTP 設定

TOE は監査ログサーバーへ監査ログを送信する機能として以下を提供する。

監査ログの送信機能の設定は、リモート UI より、U.ADMIN のみが管理機能から設定される。

リモート UI:	- 設定/登録>管理設定>デバイス管理>監査ログのエクスポート/クリア>監査ログの自動エクスポート設定
----------	---

監査ログは SMB プロトコルを用い csv 形式のファイルとして監査ログサーバーへ送信される。監査ログは指定時間に送信されるが、監査ログが本体保存容量(4万件)の 95%に達した場合は、指定時刻に関係なく監査ログサーバーに送信される。送信に成功すると、送信した監査ログは自動的に削除される。送信に失敗した場合は、複数回リトライを行う。それでも失敗した場合は次の送信指定時間に送信される。TOE と監査ログサーバーとの通信は、IPSec 暗号化機能により、全て暗号化/復号化が行なわれる。

[FAU_STG_EXT.1]

TOE は内部監査ログ格納機能として以下を提供する。

管理者は、リモート UI の以下の操作から監査ログを CSV ファイル形式で出力し、閲覧することができる。この機能は U.ADMIN のみに利用を許可している。[FAU_SAR.1][FAU_SAR.2] [FMT_MTD.1]

リモート UI:	- 設定/登録 > 管理設定 > デバイス管理 > 監査ログのエクスポート/クリア > 監査ログのエクスポート
----------	---

本体内の監査ログデータは TOE 内蔵 SSD に格納されており、SSD 暗号化機能によって機密性が守られている。本 TOE には監査ログの内容を改変する機能及びインターフェースはない。自動エクスポート機能を有効にしているため、監査ログを手動で削除することはできない。[FAU_STG.1]

監査ログは最大4万件が保持される。監査ログの記録上限数に達した場合は、最も古く格納された監査ログを削除し、新しい監査ログを保存する。[FAU_STG.4]

7.8 高信頼アップデート機能

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

【バージョン問合せ】

TOE は、TOE ファームウェアの現在のバージョンを問い合わせる能力を U.ADMIN に許可する。U.ADMIN は以下の操作でリモート UI 及び操作パネルからファームウェアの現在のバージョンを確認することができる。[FPT_TUD_EXT.1.1]

操作パネル:	- カウンター/機器情報キー > 機器情報/その他 > デバイス構成確認
リモート UI:	- 状況確認/中止 > デバイス情報

【アップデート開始能力】

TOE は、TOE ファームウェアのアップデートを開始する能力を U.ADMIN に許可する。U.ADMIN はリモート UI の以下の操作でアップデートを行なうファームウェアを指定し、手動アップデートすることができる。[FPT_TUD_EXT.1.2]

リモート UI:	- 設定登録 > 管理設定 > ライセンス/その他 > ソフトウェアの登録/更新 > 手動アップデート
----------	---

【ファームウェア検証】

TOE は、手動アップデート手順の中で、デジタル署名メカニズム(FIPS PUB 186-4 に基づく RSA(鍵長 2048bit)と SHA-256 による署名検証)を用いてアップデートに使用するファームウェアの検証を行なう。ファームウェアの検証に失敗した場合は、リモート UI にエラーメッセージが表示され、アップデートは中止される。ファームウェアはアップデート開始前の状態に維持される。[FPT_TUD_EXT.1.3, FCS_COP.1(b)(update), FCS_COP.1(c)]

7.9 管理機能

7.9.1 ユーザー管理機能

- 対応する機能要件: FIA_PMG_EXT.1, FMT_MTD.1, FMT_MSA.1, FMT_SMR.1, FMT_SMF.1

TOEは、以下のセキュリティ属性に対する操作を、認可されたロールに限定する。操作は、リモート UI もしくは操作パネルから下記の操作で行うことができる。[FMT_MSA.1, FMT_SMF.1]

操作パネル:	- ユーザー名はログイン後操作パネルの右上に表示される - 設定/登録>機器設定>管理設定>ユーザー管理>認証管理>認証ユーザーの登録/編集 (U.ADMIN のみ)
リモート UI:	- 設定/登録>管理設定>ユーザー管理>認証管理 (U.ADMIN のみ)

セキュリティ属性	操作	認可されたロール
ユーザー名	問い合わせ	U.ADMIN、所有する U.NORMAL
	追加、削除	U.ADMIN
ロール	問い合わせ	U.ADMIN
	追加、変更、削除	U.ADMIN

TOEは、以下のデータに対する操作を、それぞれ認可されたロールに限定する。操作は、リモート UI もしくは操作パネルから下記の操作で行うことができる。[FMT_MTD.1, FMT_SMF.1]

操作パネル:	- 設定/登録>管理設定>ユーザー管理>認証管理>パスワードの変更 (所有する U.NORMAL) - 設定/登録>機器設定>管理設定>ユーザー管理>認証管理>認証ユーザーの登録/編集 (U.ADMIN のみ)
リモート UI:	- 設定/登録>管理設定>ユーザー管理>認証管理 (U.ADMIN のみ)

データ	操作	認可されたロール
ユーザーパスワード	変更	所有する U.NORMAL
	追加、変更、削除	U.ADMIN

【ユーザーパスワード】

ユーザーパスワードに指定可能な文字は、アルファベットの大文字、小文字、数字、および特殊文字 (“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, “(space)”, “””, “””, “+”, “;”, “_”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “¥”, “]”, “_”, “`”, “{”, “|”, “}”, “~” を含む)である。また、最小文字数は、U.ADMIN により 15 文字以上に設定可能である。[FIA_PMG_EXT.1]

【ロール】

ロールには、あらかじめ「ベースロール」と呼ばれる、“Administrator”, “Power User”, “General User”, “Limited User”, “Guest User”の 5 種類のロールが存在している。“Administrator”は管理者向けベースロールであり、それ以外のベースロールは一般利用者向けロールである。

「ベースロール」以外の新規の「カスタムロール」を作成する場合には、“Guest User”ロールを除く4種類の「ベースロール」を複製編集して、登録することができる。ただし、“Administrator”ロールをベースとしたカスタムロールや、あらかじめカスタムロール(管理者)として登録されている“DeviceAdmin”, “NetworkAdmin”ロールは、一部の管理権限を許可されているため使用しない。

本構成では、以下の2種類のロール(U.ADMIN、U.NORMAL)を使用する。TOEは、これらの役割を正当な利用者に関連付け、リモートUI及び操作パネルでのログイン中はそれを維持する。[FMT_SMR.1]

- U.ADMIN
管理権限を有するロール。“Administrator”ロールを使用する。
- U.NORMAL
管理権限を持たないロール。ベースロール“General User”から作成されるカスタムロールを使用する。

ロールの設定は、リモートUIもしくは操作パネルから下記の操作で行うことができる。[FMT_SMR.1]

操作パネル:	- 設定/登録>機器設定>管理設定>ユーザー管理>認証管理>認証ユーザーの登録/編集 (U.ADMINのみ)
リモートUI:	- 設定/登録>管理設定>ユーザー管理>認証管理 (U.ADMINのみ)

7.9.2 デバイス管理機能

- 対応する機能要件: FMT_MTD.1, FMT_SMF.1, FMT_MOF.1, FIA_PMG_EXT.1

TOEは、セキュリティ機能を有効に機能させるべく、以下の管理機能を実行することができる。操作は、リモートUIもしくは操作パネルの設定/登録>機器設定から行うことができる。[FMT_SMF.1]

またセキュリティ機能[TLS暗号機能]を動作または停止する能力をU.ADMINに制限している。
[FMT_MOF.1]

管理機能	項目	詳細
日付/時刻設定の管理機能	内容	日時情報を設定できる。 また、タイムサーバーと同期する設定ができる。
	操作方法	操作パネル: 設定/登録>機器設定>環境設定>タイマー/電力設定>日付/時刻設定 操作パネル: 設定/登録>機器設定>環境設定>ネットワーク>TCP/IP設定>SNTP設定 リモートUI: 設定/登録>環境設定>タイマー/電力設定>日付/時刻の設定 リモートUI: 設定/登録>環境設定>ネットワーク>SNTP設定
IPSec設定の管理機能	内容	IPSec接続を定義するSecurity Policy Database (SPD)を管理する。SPDには、条件を適用する通信相手の条件、ネゴシエーションや暗号化方法、設定の有効/無効が定義される。 SPD内のIKE設定では、認証方式として事前共有鍵の登録や証明書の選択を行うことができる。また認証/暗号化アルゴリズムの設定では、認証用ハッシュとしてSHA1, SHA2(SHA256, SHA384)の選択、暗号方式としてAES-CBCの設定、さらにDHグループの選択ができる。またIKE SAの有効期間を設定できる。 SPD内のIPSec通信設定では、IPSec SA有効期間の指定と、認証/暗号化アルゴリズムの指定として、ESP(SHA1, AES-CBC)の指定ができる。

	操作方法	<p>操作パネル:設定/登録>機器設定>環境設定>ネットワーク>TCP/IP 設定>IPSec 設定</p> <p>リモート UI:設定/登録>環境設定>ネットワーク>IPSec 設定</p> <p>リモート UI:設定/登録>環境設定>ネットワーク>IPSec ポリシー一覧</p>
TLS 設定の管理機能	内容	<p>TLS 暗号機能の動作開始または停止が定義される。</p> <p>また、TLS の暗号通信に用いる暗号鍵と証明書を選択することができる。この選択によって、TLS のセッション確立時に用いるデジタル署名アルゴリズムと鍵長が決定される。</p>
	操作方法	<p>操作パネル:設定/登録>機器設定>管理設定>ライセンス/その他>リモート UI の ON/OFF</p> <p>操作パネル:設定/登録>機器設定>環境設定>ネットワーク>TCP/IP 設定>TLS 設定</p> <p>リモート UI:設定/登録>管理設定>ライセンス/その他>リモート UI 設定</p> <p>リモート UI:設定/登録>環境設定>ネットワーク>TLS 設定</p>
自動ログアウト設定の管理機能	内容	<p>操作パネルからログインされた場合はオートクリア移行時間により、リモート UI からログインされた場合はセッション設定により、管理者はそれぞれの自動ログアウト時間を設定できる。</p> <ul style="list-style-type: none"> - オートクリア移行時間: 10 秒から 9 分 (初期値 2 分) - セッション設定: 15 分から 150 分 (初期値 15 分)
	操作方法	<p>操作パネル:設定/登録>機器設定>環境設定>タイマー/電力設定>オートクリア移行時間</p> <p>操作パネル:設定/登録>機器設定>環境設定>タイマー/電力設定>オートクリア移行時間の制限</p> <p>リモート UI:設定/登録>環境設定>タイマー/電力設定>省電力設定>オートクリア移行時間</p> <p>リモート UI:設定/登録>環境設定>タイマー/電力設定>オートクリア移行時間の制限</p> <p>リモート UI:設定/登録>環境設定>ネットワーク>セッション設定</p>
ロックアウトポリシー設定の管理機能	内容	<p>ロックアウト許容回数とロックアウト時間の設定ができる。</p> <ul style="list-style-type: none"> -ロックアウト許容回数: 1 から 10 回 (設定値は初期値 5 回だが、3 回またはそれ以下) -ロックアウト時間: 1 分から 60 分 (設定値は初期値 3 分、またはそれ以上)
	操作方法	<p>操作パネル:設定/登録>機器設定>管理設定>セキュリティー設定>認証/パスワード設定>認証機能の設定</p> <p>リモート UI:設定/登録>管理設定>セキュリティー設定>認証/パスワード設定>認証機能の設定</p>
パスワードポリシー設定の管理機能	内容	<p>堅牢なパスワードの設定をユーザーに求めるために、以下のようなパスワードの品質を担保する機能を提供する。</p>

		<p>-最小パスワード長を 15 文字以上 32 文字以下に設定できる機能</p> <p>-使用可能文字 アルファベットの大文字、小文字、数字、および特殊文字 (“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, “(space)”, “,”, “.”, “+”, “=”, “-”, “/”, “:”, “;”, “<”, “=”, “>”, “?” , “[”, “¥”, “]”, “_”, “~”, “{”, “ ”, “}”, “~”)</p>
	操作方法	<p>操作パネル: 設定/登録>機器設定>管理設定>セキュリティ設定>認証/パスワード設定>パスワード設定</p> <p>リモート UI: 設定/登録>管理設定>セキュリティ設定>認証/パスワード設定>パスワード設定</p>
監査ログ管理機能	内容	<p>内部に格納されている監査ログの取り出しができる</p> <p>監査ログサーバーへ監査ログを送信するための、送信先設定をすることができる。</p>
	操作方法	<p>リモート UI: 設定/登録>管理設定>デバイス管理>監査ログのエクスポート/クリア</p>
高信頼アップデート管理機能	内容	<p>更新するファームウェアを指定する</p>
	操作方法	<p>リモート UI: 設定登録>管理設定>ライセンス/その他>ソフトウェアの登録/更新>手動アップデート</p>

8 参考文献

[Rambus 2012]

Analysis of Intel's Ivy Bridge Digital Random Number Generator, Cryptography Research a division of Rambus, 2012.

<https://www.rambus.com/intel-ivy-bridge-random-number-generator/>

以上