TOSHIBA

e-STUDIO331AC/401AC

ファクスユニット付モデル
セキュリティターゲット

バージョン 1.02

目　次

表のリスト

図のリスト

1. ST 概説

本章では、ST参照、TOE参照、TOE概要、およびTOE記述について記述する。

1.1. ST参照

本STの識別情報を以下に示す。

タイトル：　TOSHIBA e-STUDIO331AC/401AC　ファクスユニット付モデル
セキュリティターゲット
バージョン：　1.02
作成日：　2025 年 9 月 18 日
作成者：　エトリア株式会社

1.2. TOE参照

TOEの識別情報を以下に示す。

TOE名称：　TOSHIBA e-STUDIO331AC/401AC　ファクスユニット付モデル
バージョン：　SYS V2.0
TOE種別：　デジタル複合機
開発者名称：　エトリア株式会社

上記TOEは、以下Table 1に示すとおり、MFP本体、ファクスユニット、およびソフトウェアで構成される。

Table 1 TOE 構成要素

構成品	TOE識別情報	販売地域
MFP本体	TOSHIBA e-STUDIO331AC、TOSHIBA e-STUDIO401AC のいずれか	北米
ファクスユニット	GD-1370NA-N	
ソフトウェア	SYS V2.0	
MFP本体	TOSHIBA e-STUDIO331AC、TOSHIBA e-STUDIO401AC のいずれか	欧州
ファクスユニット	GD-1370EU	
ソフトウェア	SYS V2.0	

1.3. TOE概要

1.3.1. TOE種別

本TOEは、ネットワーク環境で動作し、プリント機能、コピー機能、スキャン機能、ファクス機能を提供するデジタル複合機である。

1.3.2. TOEの主要なセキュリティ機能と使用方法

本TOEは、一般的なオフィスに設置され、ネットワーク環境で使用することを想定している。利用するネットワーク環境とは、外部ネットワークからの不正なアクセスからファイアーウォールによって保護され

た内部ネットワーク（LAN）内に、クライアントPCやサーバー（FTPサーバー、メールサーバー、SYSLOGサーバー）や公衆電話回線網に接続して利用する。また、利用者はMFPの操作パネルやクライアントPCからWebブラウザやプリンタードライバーを介して、MFPの基本機能を利用する。図 1 に運用環境を示す。

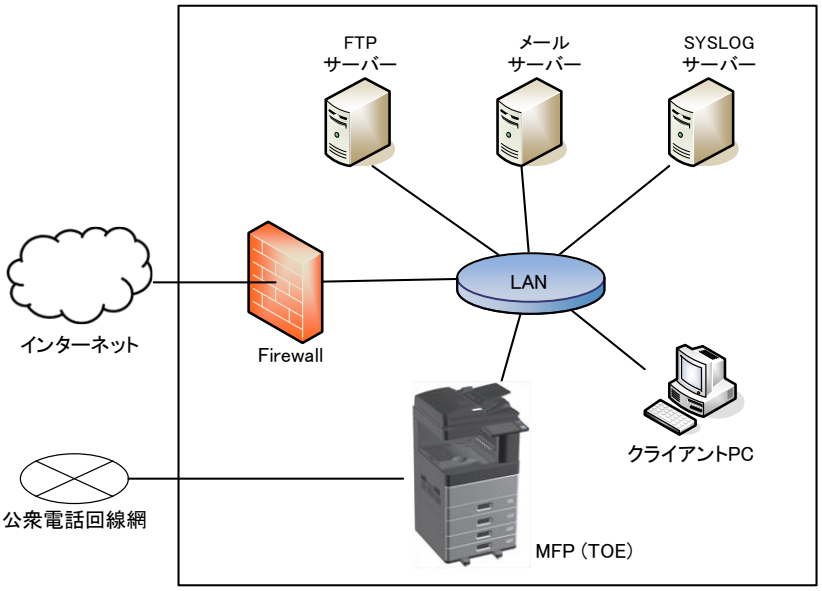


図 1 MFP の利用環境

本TOEは、コピー、プリント、スキャン、ファクスといった基本機能を備えたデジタル複合機である。また、利用者文書データやセキュリティ関連データを保護するために、利用者を識別認証する機能、利用者権限に基づくアクセス制御機能、TOEの利用履歴のログを記録し監査サーバーに送信する機能、TOE内のストレージに保存されているデータを暗号化する機能、LAN上の通信データを保護する機能、セキュリティ設定操作を管理者に限定した設定機能、TOEのセキュリティ機能の正常動作を保証する機能、公衆電話回線網（PSTN）とLAN間のブリッジ接続を禁止する機能を有する。なお、データ消去及び完全削除機能は評価対象のセキュリティ機能には含まない。

1.3.3. TOE以外に要求されるハードウェアおよびファームウェア

TOE以外に要求されるハードウェアおよびファームウェアを以下に示す。

- クライアントPC

  U.NORMAL(a)は、文書データを LAN を介して TOE へ印刷を要求することができる。U.ADMIN(a)は、Web ブラウザを使用して MFP の設定データを参照または変更できる。

  ブラウザとプリンタードライバーは次のとおりである。

  - Web ブラウザ：Microsoft Edge
  - プリンタードライバー：TOSHIBA Universal Printer Driver2　(Version：7.222.5412.313)

- メールサーバー

  メールサーバーは、SMTP を使用して e-mail を送信するサーバーである。 TOE とメールサーバーは TLS 通信で接続されている。（本運用では、Sendmail 8.15.2 を使用したサーバーを想定している。）

- FTPサーバー

  FTP サーバーはファイル転送プロトコル・サーバー・ソフトウェアを送信するサーバー。TOE と FTP サーバーは TLS 通信で接続されている。（本運用では、ProFTPD 1.3.6 を使用したサーバーを想定している。）

- SYSLOGサーバー

  Syslog プロトコルを用いて転送される TOE のログデータを受信・保存するサーバー。TOE と SYSLOG サーバーは TLS 通信で接続されている。（本運用では、Syslog-ng 3.14 を使用したサーバーを想定している。）

1.4. TOE記述

1.4.1. TOEの物理的範囲

TOEは、必須オプションであるファクスユニットを装着したMFP本体とガイダンスである。TOEの構成要素を以下に示す。

Table 2 TOE を構成するハードウェア

MFP本体	ファクスユニット	販売地域	形式	配付方法
TOSHIBA e-STUDIO331AC	GD-1370NA-N	北米	MFP本体とファクスユニットは、それぞれバイナリ形式のファームウェアを組み込んだハードウェアである	MFP本体とファクスユニットは、それぞれ個別の配付物として、段ボールに梱包された状態で輸送業者によって利用者に配送される
TOSHIBA e-STUDIO401AC	GD-1370NA-N			
TOSHIBA e-STUDIO331AC	GD-1370EU	欧州		
TOSHIBA e-STUDIO401AC	GD-1370EU			

MFP本体のバージョンは以下の通り。

- SYSTEM FIRMWARE： TM20SF0W2005
- SYSTEM SOFTWARE： TM20SD0W2005
- ENGINE FIRMWARE： TK250MWW02
- SCANNER FIRMWARE： TK250SLGWW03

ファクスユニットのバージョンは以下の通り。

- FAX1 FIRMWARE： FAXH625TA13

Table 3 TOE を構成するガイダンス

タイトル	識別子	形式	配付方法	販売地域
Quick Start Guide	OME24000700	PDF形式ファイルおよび印刷物	MFP本体に同梱された状態で利用者に配付される。	北米 欧州
Safety Information	OME24001000	PDF形式ファイルおよび印刷物		
Copy	OME24001300	PDF形式ファイル		
Scan	OME24001400	PDF形式ファイル		
User Functions	OME24001900	PDF形式ファイル		
Installation	OME24002300	PDF形式ファイル		
Print	OME24002400	PDF形式ファイル		
TopAccess	OME24002100	PDF形式ファイル		
Frequently Asked Questions	OME24002000	PDF形式ファイル		
Troubleshooting	OME24000900	PDF形式ファイル		
High Security Mode	OME24002500	PDF形式ファイル		
Preparation of Paper	OME24000800	PDF形式ファイル		
Information About Equipment	OME24001100	PDF形式ファイル		
Specifications	OME24001200	PDF形式ファイル		
Fax	OME24001500	PDF形式ファイル		
Information to our customers	OME25007100	印刷物		

1.4.2. TOEの論理的範囲

TOEの論理的な境界は、次のセクションによって記述されるセキュリティ機能および基本機能によって定義される。

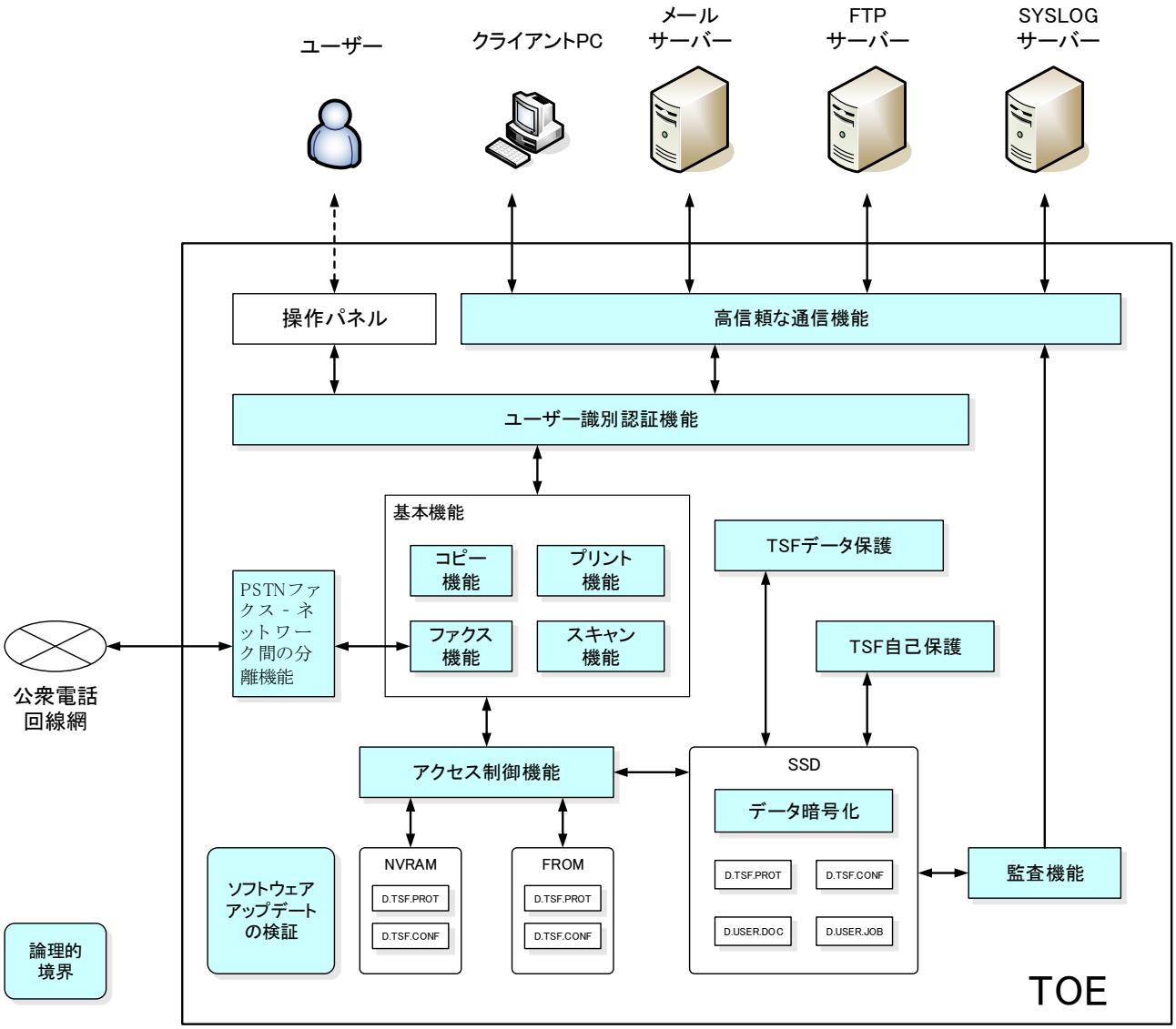


図 2 論理的境界

1.4.2.1. 基本機能

TOEは基本的な機能として、コピー、プリント、スキャンなどの画像に関する一連の機能を有し、これらの機能を統合的に制御する。

- コピー機能

  ユーザーが操作パネルを操作して、スキャナー部で紙文書を読み取り、複写印刷する機能である。

- プリント機能

  クライアント PC からのプリントデータを、LAN を介して TOE に送り、紙に印刷する機能である。

- スキャン機能

  ユーザーが操作パネルを操作し、紙文書をスキャナー部で読取り、その画像データをメールに添付し送信したり、FTP サーバーに送信したりすることができる。

- ファクス機能

  ファクス機能とは、ファクス送信機能とファクス受信機能からなる。

  ファクス送信機能は、スキャナー部で読み取った紙文書データを、PSTN を介して外部のファクス機に送信する機能である。また、ファクス受信機能は、PSTN を介して外部ファクス機から送信されてきた文書データを受信する機能である。

1.4.2.2. セキュリティ機能

TOEによって提供されるセキュリティ機能は以下のとおりである。

- 識別、認証、及びHCD機能を使用するための付与機能

  ユーザー識別、認証機能は、TOE を利用しようするユーザーが、TOE を利用することができるユーザーであるかどうかを検証し、利用できるユーザーである事が確認された場合のみ利用許可を与える機能である。

  TOE は、ユーザー認証するために、操作パネルまたはクライアント PC からのユーザーID とユーザーパスワードを入力するようにユーザーに促し、ユーザーパスワード入力時にダミー文字を表示するフィードバックの保護機能と、認証に失敗したユーザーをロックアウト機能を備えています。また、ログイン後に無操作状態が所定の時間続いた場合、自動的にログアウトする機能を備えている。

- アクセス制御機能

  TOE は、許可されたユーザーに安全な資産であるユーザーデータ及び機能へのアクセスを制御します。

- 監査機能

  TOE は、装置の状態を追跡するための監査ログを生成する。イベント毎に記録されたすべてのログは、監査サーバーへ送信され、監査サーバーで閲覧することができる。

- 高信頼な通信機能

  TOE は、LAN に接続し通信する際に、ネットワーク上の通信データの漏洩や改ざんを防止するため、暗号通信プロトコルをサポートする。

  TOE の運用環境では、クライアント PC、メールサーバー、SYSLOG サーバー、FTP サーバーと通信するが、データを暗号化するために TLS を使用する。また、クライアント PC からプリンタードライバーを使って IPP 印刷する場合も、TOE はクライアント PC との通信に TLS を使ってプリントプロトコルの IPPS を使ってプリントデータを保護している。

- TSF自己保護

  TOE は、既知のシグネチャに対するデジタル署名の検証を使用して、静的実行可能ファイルと構成ファイルの完全性テストを実行します。 これにより、TOE は信頼できる状態から改ざんされたかを検出することができる。

- TSFデータ保護

  識別認証機能により認証された管理者のみが、操作パネルまたは TopAccess から TSF データに関する操作を実行できる機能。例えば、日時の変更やユーザーの登録/削除、使用可能なサービスとプロトコルを有効または無効に設定することができる。

- データ暗号化

  SSD に保存されるユーザーデータの漏洩を防止するために、これらのデータを暗号する機能である。

- PSTNファクス - ネットワーク間の分離機能

  PSTN からの入力をファクス受信に制限することにより、公衆電話回線網と LAN 間のブリッジ接続を禁止する機能である。

- ソフトウェアアップデートの検証

  TOE のソフトウェアをアップデートする時に、アップデートするソフトウェアが正規なものかどうかを検証する機能である。

1.4.2.3. 用語

本STに関連する特定の用語の内、2章で適合主張しているCCおよびPPで定義されている用語については、その定義に従う。それ以外の用語をTable 4に定義する。

Table 4 用語

用語	定義
ユーザーID	一般ユーザー、MFP管理者に付与される識別子。TOEはこの識別子によりユーザーを特定する。
ユーザーパスワード	各ユーザーがTOEにログインする際に使用するパスワード。
ジョブログ	プリントジョブ、送信管理記録、受信管理記録およびスキャンジョブのようなジョブ情報
メッセージログ	MFPの機器情報あるいはユーザーにより実行された操作に関するログ
TopAccess	Webベースのジョブおよびデバイス管理ツールである。このツールを使用するとネットワークを介してMFPの情報を取得することができる。
自動ログアウト時間	ログインしているユーザーが一定時間MFPの操作をしなかった場合に自動的にログアウトされるまでの時間。
ロックアウト時間	ロックアウトされたアカウントが解放されるまでの時間。
日付/時刻	ログ管理のための時間情報。年／月／日／時／分／秒
役割	U.NORMAL、U.ADMIN。 U.NORMALはU.NORMAL(a)とU.FAXOPERATOR、U.ADMINはU.ADMIN(a)、U.ACCOUNTMANAGER、U.ADDRESSBOOKOPERATORに詳細化される。
ファームウェア	ハードウェアを制御するために機器に組み込まれたソフトウェア
Cipher Suite	TLS通信で使用する暗号アルゴリズムの組合せのこと。 「鍵交換_署名_暗号化_ハッシュ関数」の組によって構成される。
アドレス帳	ファクス番号、e-mailアドレスを宛先一覧として登録、表示することでき、ファクス送信やスキャンのe-mail送信の宛先を簡単に指定することができる。
ユーザー認証失敗処理の管理	管理者により、ログインパスワードの入力リトライ回数の変更や、ロックアウト時間の変更、ロックアウトされたアカウントステータスをクリアーにすることができる。
セキュアチャネル	第三者に盗聴されないようにデータを暗号化した通信チャネル。
欧州特殊文字	ドイツ語のウムラウトとフランス語のセディラを持つ文字

2. 適合主張

2.1. CC適合主張

本STおよびTOEのCC適合主張は以下のとおりである。

Common Criteria version: Version 3.1 Release 5

- Part1： Introduction and general model April 2017 Version 3.1 Revision 5
- Part2： Security functional components April 2017 Version 3.1 Revision 5
- Part3： Security assurance components April 2017 Version 3.1 Revision 5
- CC part2に対するSTの適合： CC part 2 Extended
- CC part3に対するSTの適合： CC part 3 Conformant

2.2. PP適合主張

本STおよびTOEが適合しているPPは以下のとおりである。

PP名称：	Protection Profile for Hardcopy Devices
PPバージョン：	1.0 dated September 10, 2015
認識識別：	JISEC-C0553
Errata：	Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. パッケージ適合主張

本STはパッケージへの適合主張はしない。

2.4. 適合主張根拠

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

- Required Uses

  Printing, Scanning, Copying、Networking communications, Addministration

- Conditionally Mandatory Uses

  PSTN faxing, Fileld-Replaceable Nonvolatile Storage

- Optional Uses

  なし

3. セキュリティ課題定義

3.1. ユーザー

本STでは、下表のようにTOEのユーザーと役割を定義する

Table 5 ユーザー分類

役割		分類名	定義
U.NORMAL 識別され、認証された利用者で、管理者役割を持たない利用者	U.NORMAL(a)	一般ユーザー	TOEの基本機能であるコピー機能・プリント機能・スキャン機能・ファクス送信機能を実行できるユーザー。一般ユーザーは、基本機能ごとに操作権限を付与され、付与された機能だけを実行できる。
	U.FAXOPERATOR	一般ユーザー	ファクス送受信機能を実行できるユーザー。
U.ADMIN 識別され、認証された利用者で管理者役割を持つ利用者	U.ADMIN(a)	管理者	TOEのセキュリティ機能に係わる設定、ユーザーのアカウント情報の変更、監査ログの閲覧など、TOE 全般の管理権限を持つ管理者。
	U.ACCOUNTMANAGER	管理者	ユーザーのアカウント管理(ユーザーのユーザーIDや役割設定、基本機能の操作権限など)の設定が行える管理者。
	U.ADDRESSBOOKOPERATOR	管理者	アドレス帳を編集できるユーザー。

3.2. 資産

STでは2つの資産分類を定義する。

Table 6 資産分類

Designation	Asset category	Definition
D.USER	User Data 利用者データ	Data created by and for Users that do not affect the operation of the TSF TSF の操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ
D.TSF	TSF Data TSFデータ	Data created by and for the TOE that might affect the operation of the TSF TSF の操作に影響を与えるかもしれないTOEのためのTOEによって作成されたデータ

3.2.1. ユーザーデータ

本STでは2つのユーザーデータを定義する。

Table 7 ユーザーデータ種別

名称	資産分類	定義	詳細
D.USER.DOC	User Document Data 利用者文書データ	Information contained in a User’s Document, in electronic or hardcopy form. 電子的またはハードコピーの形式で、利用者の文書に含まれる情報	コピー文書データ
			プリント文書データ
			スキャン文書データ
			ファクス送信文書データ
			ファクス受信文書データ
D.USER.JOB	User Job Data 利用者ジョブデータ	Information related to a User’s Document or Document Processing Job. 利用者の文書または文書処理ジョブに関連する情報	プリントジョブ
			スキャンジョブ
			コピージョブ
			ファクス送信ジョブ
			ファクス受信ジョブ

3.2.2. TSFデータ

TSFデータは、2つの種別から構成される。

Table 8 TSF データ種別

名称	資産分類	定義	詳細
D.TSF.PROT	Protected TSF Data 保護されたTSFデータ	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. データの所有者でもなく、または管理者役割も持たない利用者によって、改ざんされたTSFデータがTOEのセキュリティ影響を及ぼすかもしれないが、暴露については容認できるようなTSFデータ。	セキュアチャネルの有効/無効
			ユーザーID
			役割
			ログインパスワードのリトライ回数
			ロックアウト時間
			ロックされたアカウントステータス
			オートログアウト時間
			日時情報
			最小パスワード長
			アドレス帳
			SYSLOGサーバーの設定
			FTPサーバーの設定
			ソフトウェアのアップデート

名称	資産分類	定義	詳細
D.TSF.CONF	Confidential TSF Data 秘密のTSFデータ	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. データの所有者でもなく、管理者役割も持たない利用者によって、暴露または改ざんされたTSFデータが、TOEのセキュリティに影響を及ぼすかもしれないようなTSFデータ。	ユーザーパスワード
			暗号鍵

3.3. 脅威

適合製品が対抗するTOEに対する脅威は、以下のとおりである。

脅威は、TOEのセキュリティ方針を危殆化する可能性のある結果をもたらすアクションを実行する脅威エージェントによって定義される。

Table 9 脅威の定義

名称	定義
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. 攻撃者は、TOEのインタフェースを通じて、TOE内の利用者文書データへアクセス（閲覧、改変、または削除）、または利用者ジョブデータを変更（改変または削除）するかもしれない。
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE’s interfaces. 攻撃者は、TOEのインタフェースを通じて、TOE内のTSFデータへの不正なアクセスを得るかもしれない。
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate. TOEの操作が許可された場合、TSFの誤作動によって、セキュリティの損失を引き起こすかもしれない。
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE. 攻撃者は、TOEに不正なソフトウェアをインストールするかもしれない。

名称	定義
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication. 攻撃者は、ネットワーク通信をモニターしたり操作したりすることで、送信中のデータにアクセスしたり、TOEのセキュリティを侵害したりするかもしれない。

3.4. 組織のセキュリティ方針

以下は、適合する製品が掲げる組織のセキュリティ方針（OSP）である。

3.4.1. 組織のセキュリティ方針の定義

組織のセキュリティ方針は、資産に対する脅威に基づいて定義するのは実用的ではない、または主に顧客の期待から生じる、セキュリティ対策方針の基礎を提供するために使用される。

Table 10 組織のセキュリティ方針の定義

名称	定義
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions. 利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity. セキュリティ関連アクティビティは監査されなければならず、またこのようなアクションのログは保護され、外部ITエンティティへ送信されなければならない。
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN. TOEは、LAN上の他のデバイスと自身を識別できなければならない。
P.STORAGE_ENCRYPTION （条件付き必須）	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. TOEが利用者文書データまたは秘密のTSFデータを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOEはそれらのデバイス上のこのようなデータを暗号化すること。
P.KEY_MATERIAL （条件付き必須）	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.

名称	定義
	利用者文書データまたは秘密のTSFデータの現地交換可能な不揮発性ストレージのための暗号鍵の生成に寄与するような、平文の鍵、サブマスク、乱数、またはその他のあらゆる値は、不正なアクセスから保護されなければならない、かつそのストレージデバイス上に保存されてはならない。
P.FAX_FLOW （条件付き必須）	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN. TOEがPSTNファクス機能を提供する場合、PSTNファクス回線とLANの間に分離を保証する。

3.5. 前提条件

前提条件は、セキュリティ対策方針やセキュリティ機能要件が有効であるために、満たされなければならない条件である。

Table 11 前提条件

名称	定義
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. TOE、及びTOEが保存または処理するデータの価値に見合った物理セキュリティが、その環境によって提供されることを想定する。
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface. 運用環境は、LANインタフェースへの外部からの直接のアクセスからTOEを保護することを想定する。
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies. TOE管理者は、サイトセキュリティ方針に従ってTOEを管理すると、信頼されている。
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies. 許可された利用者は、サイトセキュリティ方針に従ってTOEを使用するよう教育訓練を受けている。

4. セキュリティ対策方針

4.1. 運用環境セキュリティ対策方針

運用環境セキュリティ対策方針についての詳細情報をTable 12に記述する。

Table 12 運用環境のセキュリティ対策方針

名称	定義
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes. 運用環境は、TOE、及びTOEが保存または処理するデータの価値に見合った物理セキュリティを提供しなければならない。
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface. 運用環境は、LANインタフェースへの外部からの直接のアクセスからTOEを保護するためにネットワークセキュリティを提供しなければならない。
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes. TOE所有者は、管理者がその権限を悪意ある目的に使用しないという信頼を確立しなければならない。
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them. TOE所有者は、利用者がサイトセキュリティ方針を理解し、それに従う力量を持っていることを保証しなければならない。
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. TOE所有者は、管理者がサイトセキュリティ方針を理解し、TOEを正しく設定し、パスワードと鍵を相応に保護するために製造者のガイダンスを活用する力量を持っていることを保証しなければならない。

5. Extended Component Definitions

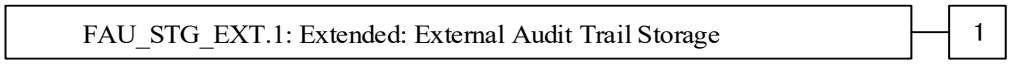
Extended component definitions are listed below.

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:

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

Component leveling:



FAU_STG_EXT.1 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 audits records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

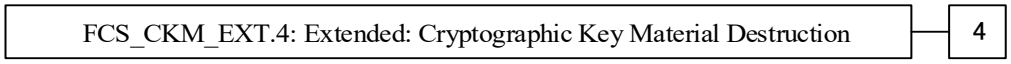
This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2. FCS_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or

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

FCS_CKM.4 Cryptographic key destruction

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 Behavior:

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: No dependencies.

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_KDF_EXT Extended: Cryptographic Key Derivation

Family Behavior:

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

Component leveling:

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Hierarchical to: No other components.

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

[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

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

Rationale:

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

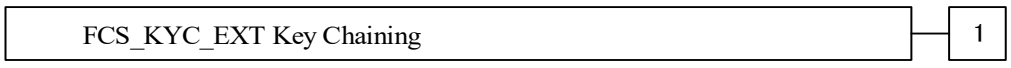
This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.5. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.

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

FCS_SMC_EXT.1 Extended: Submask Combining,

FCS_COP.1(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 BEVor 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 Behavior:

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

Component leveling:

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Rationale:

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

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

5.7. FCS_SMC_EXT Extended: Submask Combining

Family Behavior:

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)

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.

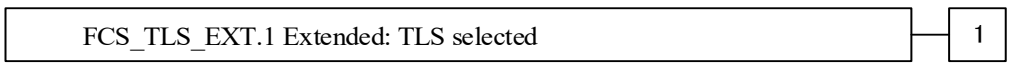
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.8. FCS_TLS_EXT Extended: TLS selected

Family Behavior:

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: No dependencies.

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.

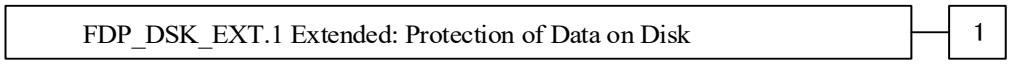
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.9. FDP_DSK_EXT Extended: Protection of Data on Disk

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

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

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

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

Rationale:

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

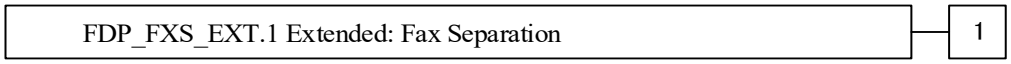
This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.10. FDP_FXS_EXT Extended: Fax Separation

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_FXS_EXT.1 Extended: Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.11. FIA_PMG_EXT Extended: Password Management

Family Behavior:

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

Component leveling:

FIA_PMG _EXT.1 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 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.

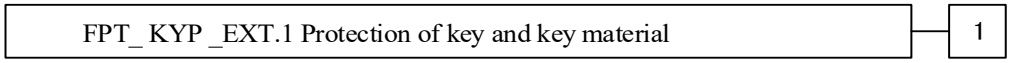
This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.12. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ KYP _EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, 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.

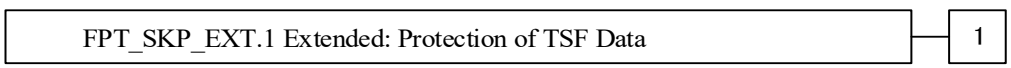
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.13. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

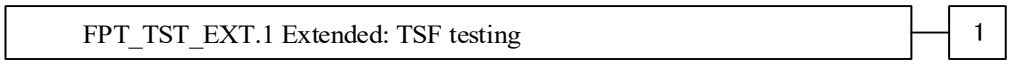
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.14. FPT_TST_EXT Extended: TSF testing

Family Behavior:

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

Component leveling:



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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.15. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:

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

Component leveling:

FPT_TUD_EXT.1 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), or

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: no other functions] prior to installing those updates.

Rationale:

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

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

6. SECURITY REQUIREMENTS

6.1. 表記法

- **ボールド書体**は、PPで“完成”または“詳細化”された部分を示す。
  - ***ボールドイタリック***書体は、本STで“割付”、“選択”、または“詳細化”されたことを示す。
- ［］内は、“割付”または“選択”された結果を示す。
- （）内に文字、例えば、(a)、(b)、....と続くようなSFRコンポーネントは、必須の繰返しを示す。

6.2. Class FAU: Security Audit

6.2.1. FAU_GEN.1 Audit data generation

(for O.AUDIT)
Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **All auditable events specified in Table 13**, [*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 13,** [*none*].

Table 13 監査対象事象

監査対象事象	関連SFR	追加情報
ジョブの終了 Job completion	FDP_ACF.1	ジョブの種別
ユーザー認証失敗 Unsuccessful User authentication	FIA_UAU.1	なし

監査対象事象	関連SFR	追加情報
ユーザー識別失敗 Unsuccessful User identification	FIA_UID.1	なし
管理機能の利用 Use of management functions	FMT_SMF.1	なし
役割の一部であるユーザーグループの改変 Modification to the group of Users that are part of a role	FMT_SMR.1	なし
時刻の変更 Changes to the time	FPT_STM.1	なし
セション確立の失敗 Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	失敗の理由

6.2.2. FAU_GEN.2　User identity association

(for O.AUDIT)
Hierarchical to: No other components.

Dependencies: FAU_GEN.1　Audit data generation

FIA_UID.1Timing 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.

6.2.3. FAU_STG_EXT.1　Extended: External Audit Trail Storage

(for O.AUDIT)
Hierarchical to: No other components.

Dependencies: FAU_GEN.1　Audit data generation,

FTP_ITC.1　Inter-TSF trusted channel.

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

6.3. Class FCS: Cryptographic Support

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

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

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

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

- ***NIST Special Publication 800-56B, "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.

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

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

6.3.3. FCS_CKM.4 Cryptographic key destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA))
Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or

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

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

For volatile memory, the destruction shall be executed by [*powering off a device*].

For nonvolatile storage, the destruction shall be executed by a [*single*] overwrite of key data storage location consisting of *[a static pattern],* followed by a [*none*]. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: [*no standard*].

6.3.4. FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to: No other components.

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

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

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

(for O.COMMS_PROTECTION)
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(a) **Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [*CBC modes*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[*NIST SP 800-38A*]**

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

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)
Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic key generation]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: No dependencies.

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

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

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

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: No dependencies.

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

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

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

(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.

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

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [*CBC*] mode** and cryptographic key sizes **[*128 bits*]** that meet the following: **AES as specified in ISO/IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

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

(selected from FCS_KYC_EXT.1.1)
Hierarchical to: No other components.

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

FCS_COP.1.1(f) Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[*CBC*] mode]** and cryptographic key sizes **[*128 bits*]** that meet the following: [**AES as specified in ISO /IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

6.3.12. FCS_SMC_EXT.1 Extended: Submask Combining

(selected in FCS_KYC_EXT.1.1)

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 [***exclusive OR (XOR)***] to generate an intermediary key or BEV.

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

(selected with FCS_IPSEC_EXT.1.4)

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-[*SHA-1, SHA-256*], key size [*160, 256*]bits, and message digest sizes [*160, 256*] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."

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

(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)
Hierarchical to: No other components.

Dependencies: FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_COP.1(c) Cryptographic operation (Hash Algorithm),
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(h) Refinement: The TSF shall perform [**keyed-hash message authentication**] in accordance with [*HMAC-SHA-256*] and cryptographic key sizes [256] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**; ISO/IEC 10118].

6.3.15. FCS_TLS_EXT.1 Extended: TLS selected

(selected in FTP_ITC.1.1, FTP_TRP.1.1)
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 [*TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[

- *TLS_RSA_WITH_AES_256_CBC_SHA*

- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*

].

6.3.16. FCS_HTTPS_EXT.1 Extended: HTTPS selected

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

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.

6.3.17. FCS_KDF_EXT Extended: Cryptographic Key Derivation

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),
[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

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

6.3.18. FCS_KYC_EXT.1 Extended: Key Chaining

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(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: [*intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)*: [*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]] while maintaining an effective strength of [*128 bits*].

6.4. Class FDP: User Data Protection

6.4.1. FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 14** and **Table 15.**

Table 14 D.USER.DOC アクセス制御 SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation:*	*Submit a document to be printed*	*View image or Release printed output*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	*Operation:*	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	

		"Create"	"Read"	"Modify"	"Delete"
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	*Operation:*	*Submit a document for copying*	*View scanned image or Release printed copy output*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	*Operation:*	*Submit a document to send as a fax*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied

		"Create"	"Read"	"Modify"	"Delete"
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR		denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	*Operation:*	*Receive a fax and store it*	*View fax image or Release printed fax output*	*Modify image of received fax*	*Delete image of received fax*
	Job owner	(note 3)		denied	
	U.ADMIN(a)	(note 4)		denied	
	U.NORMAL(a)	(note 4)	denied	denied	denied
	U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
	U.FAXOPERATOR	(note 4)		denied	
	U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied

Table 15 D.USER.JOB アクセス制御 SFP

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

		"Create" *	"Read"	"Modify"	"Delete"
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated		denied	denied	denied
Scan	*Operation:*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	*Operation:*	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	*Operation:*	*Create fax send job*	*View fax job queue / log*	*Modify fax send job*	*Cancel fax send job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	

		"Create" *	"Read"	"Modify"	"Delete"
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR			denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	*Operation:*	*Create fax receive job*	*View fax receive status / log*	*Modify fax receive job*	*Cancel fax receive job*
	Fax owner	(note 3)		denied	denied
	U.ADMIN(a)	(note 4)		denied	denied
	U.NORMAL(a)	(note 4)	denied	denied	denied
	U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
	U.FAXOPERATOR	(note 4)		denied	denied
	U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied

Application note:

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

Note 1: *Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.*

Note 2: *Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.*

Note 3: *Job Owner of received faxes is assigned by default or configuration. Ownership of received faxes is assigned to U.FAXOPERATOR and U.ADMIN(a) role.*

Note 4: *PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.*

6.4.2. FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 14** and **Table 15**.

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 14 and Table 15***.

FDP_ACF.1.3 **Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***].

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***].

6.4.3. FDP_FXS_EXT.1 Extended: Fax separation

(for O.FAX_NET_SEPARATION)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.4.4. FDP_DSK_EXT.1 Extended: Protection of Data on Disk

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

FDP_DSK_EXT.1.1 The TSF shall [***perform encryption in accordane with FCS_COP.1(d)***], 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.

6.5. Class FIA: Identification and Authentication

6.5.1. FIA_AFL.1 Authentication failure handling

(for O.USER_I&A)
Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within [1 - 30]*] unsuccessful authentication attempts occur related to [*the unsuccessful user authentication attempts of following the last successful authentication or clear of user account lock*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*lockout each account in lockout time, U.ADMIN(a) and U.ACCOUNTMANAGER can release a lockout account*].

6.5.2. FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)
Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*ユーザーID, 役割*].

6.5.3. FIA_PMG_EXT Extended:Password Management

(for O.USER_I&A)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!", "@", "#", "$", "^", "*", "(", ")", [refer to Table 16]*];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

Table 16 その他使用可能文字

文字タイプ	使用可能文字
句読点	+ , - . / : ; = ? \ _ ` { | } ~ スペース
欧州特殊文字	¢£§ª°µ¿₮€ ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõöøùú ûüýþÿĀāĂăĄąĆćČčĎďĐđĒēĖėĘęĚěĞğĢģĪīĮįİıĶĹĺĻļĽľŁłŃŇňŌōŐőŒœŔŕŖŗŘřŚśŞŠš ŢţŤťŪūŮŰűŲųŸŹźŻżŽžƒЁЂЃЄЅІЇЈЉЊЋЌЎЏАБВГДЕЖЗИЙКЛ МНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдежзийклмноп туфхцчшщъыьэюяёђѓєѕіїјљњћќўџҐҒӘӨҰҲҺ

文字タイプ	使用可能文字
	ΐ ά έ ή ί ΰ α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ ς σ τ υ φ χ ψ ω ϊ ϋ ό ύ ώ

6.5.4. FIA_UAU.1　Timing of authentication

(for O.USER_I&A)
Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **Refinement:** The TSF shall allow [*storing the document data from printer driver, receive PSTN Fax data*] on behalf of the user to be performed before the user is authenticated.

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

6.5.5. FIA_UAU.7　Protected authentication feedback

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1　Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*display dummy characters*] to the user while the authentication is in progress.

6.5.6. FIA_UID.1 Timing of identification

(for O.USER_I&A and O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 **Refinement:** The TSF shall allow [*receive PSTN fax data*] on behalf of the user to be performed before the user is identified.

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

6.5.7. FIA_USB.1 User-subject binding

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_ATD.1　User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*ユーザーID, 役割*].

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: [*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: [*none*].

6.6. Class FMT: Security Management

6.6.1. FMT_MOF.1 Management of security functions behavior

(for O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable*] the functions [*Secure Channel*] to *U.ADMIN(a)*.

6.6.2. FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control,

~~FDP_IFC.1 Subset information flow control~~]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [*query, modify, delete, [create, export]*] the security attributes [*ユーザーID,役割*] to [*Table 17参照*].

Table 17 セキュリティ属性リスト

セキュリティ属性	操作	役割
ユーザーID	*create, modify, query , delete, export*	*U.ADMIN(a)*
	query, export	*U.ACCOUNTMANAGER*
	query	*U.NORMAL,* *U.ADDRESSBOOKOPERATOR*
ユーザーID (U.ADMIN(a)を除く)	*create, modify, delete*	*U.ACCOUNTMANAGER*

セキュリティ属性	操作	役割
役割	*create, modify, query, delete, export*	*U.ADMIN(a)*
	query, export	*U.ACCOUNTMANAGER*
	query	*U.NORMAL* *U.ADDRESSBOOKOPERATOR*
役割 (U.ADMIN(a)を除く)	*create, modify, delete*	*U.ACCOUNTMANAGER*

6.6.3. FMT_MSA.3 Static attribute initialization

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

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

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

6.6.4. FMT_MTD.1 Management of TSF data

(for O.ACCESS CONTROL)
Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 18.**

Table 18 TSF データの管理

Data	Operation	Authorised role(s)
U.NORMAL のユーザーパスワード	*modify*	***the owning U.NORMAL***
	modify, export	*U.ADMIN(a)* *U.ACCOUNTMANAGER*

Data	Operation	Authorised role(s)
*U.ADMIN(a)*のユーザーパスワード	*modify, export*	***U.ADMIN(a)***
U.ACCOUNTMANAGER のユーザーパスワード	*modify, export*	***U.ADMIN(a),*** ***U.ACCOUNTMANAGER***
U.ADDRESSBOOKOPERATOR のユーザーパスワード	modify	***the owning U.ADDRESSBOOKOPERATOR***
	modify, export	***U.ADMIN(a),*** ***U.ACCOUNTMANGER***
ログインパスワードの入力リトライ回数	modify	***U.ADMIN(a)***
ロックアウト時間	modify	***U.ADMIN(a)***
ロックアウトされたアカウントステータス	clear	***U.ADMIN(a),*** ***U.ACCOUNTMANGER***
オートログアウト時間	modify	***U.ADMIN(a)***
日時情報	modify	***U.ADMIN(a)***
最小パスワード長	modify	***U.ADMIN(a)***
アドレス帳	create, modify, delete	***U.ADMIN(a),*** ***U.ADDRESSBOOKOPERATOR***
SYSLOG サーバーの設定	modify	***U.ADMIN(a)***
FTP サーバーの設定	modify	***U.ADMIN(a)***
ソフトウェア	query, modify	***U.ADMIN(a)***

6.6.5. FMT_SMF.1　Specification of Management Functions

(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)
Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [*refer to* ***Table 19***].

Table 19 管理機能

SFR	管理	管理機能	理由
FAU_GEN.1	予見される管理アクティビティはない	なし	-
FAU_GEN.2	予見される管理アクティビティはない	なし	-
FAU_STG_EXT.1	TSF は、暗号機能を設定する能力を持っていなければならない。	なし	この機能は提供されない
FCS_CKM.1(b)	予見される管理アクティビティはない	なし	-
FCS_CKM.4	予見される管理アクティビティはない	なし	-
FCS_CKM_EXT.4	予見される管理アクティビティはない	なし	-
FCS_COP.1(b)	予見される管理アクティビティはない	なし	-
FCS_COP.1(c)	予見される管理アクティビティはない	なし	-
FCS_COP.1(d)	予見される管理アクティビティはない	なし	-
FCS_COP.1(f)	予見される管理アクティビティはない	なし	-
FCS_COP.1(g)	予見される管理アクティビティはない	なし	-
FCS_COP.1(h)	予見される管理アクティビティはない	なし	-
FCS_RBG_EXT.1(a)	予見される管理アクティビティはない	なし	-
FCS_RBG_EXT.1(b)	予見される管理アクティビティはない	なし	-
FCS_TLS_EXT.1	予見される管理アクティビティはない	なし	-
FCS_HTTPS_EXT.1	予見される管理アクティビティはない	なし	-
FCS_KDF_EXT.1	予見される管理アクティビティはない	なし	-
FCS_KYC_EXT.1	予見される管理アクティビティはない	なし	-
FDP_ACC.1	予見される管理アクティビティはない	なし	-
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	なし	属性の初期値は固定され変更はできない
FDP_FXS_EXT.1	予見される管理アクティビティはない	なし	-
FDP_DSK_EXT.1	予見される管理アクティビティはない	なし	-

SFR	管理	管理機能	理由
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理	ユーザー認証失敗処理の管理	-
	b) 認証失敗の事象においてとられるアクションの管理	なし	所定のアクションため管理されていません
FIA_ATD.1	a) もし割付に示されていれば、許可管理者はユーザーに対する追加のセキュリティ属性を定義することができる	なし	この機能は提供されない
FIA_PMG_EXT.1	予見される管理アクティビティはない	最小パスワード長の管理	-
FIA_UAU.1	a) 管理者による認証データの管理	・ユーザーパスワードの管理 (U.ACCOUNTMANAGER/U.ADMIN(a)/U.NORMAL /U.ADDRESSBOOKOPERATOR) by U.ADMIN(a). ・ユーザーパスワードの管理 (U.ACCOUNTMANAGER/U.NORMAL /U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER	-

SFR	管理	管理機能	理由
	b) 関係するユーザーによる認証データの管理	・U.NORMALによる自身のユーザパスワードの管理 ・U.ADDRESSBOOKOPERATORによる自身のユーザパスワードの管理	-
	c) ユーザーが認証される前にとられるアクションのリストを管理すること	なし	所定のアクションため管理されない
FIA_UAU.7	予見される管理アクティビティはない	なし	-
FIA_UID.1	a) ユーザー識別情報の管理	ユーザーIDの管理	-
	b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	なし	所定のアクションため管理されない
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる	なし	許可された役割はない
	b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる	なし	許可された役割はない
FMT_MOF.1	a) TSFの機能と相互に影響を及ぼし得る役割のグループを管理すること	なし	所定のアクションため管理されない
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること	なし	所定のアクションため管理されない
	b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること	なし	所定のアクションため管理されない
FMT_MSA.3	a) 初期値を特定し得る役割のグループを管理すること	なし	初期値を指定できる役割はない

SFR	管理	管理機能	理由
	b) 所定のアクセス制御SFPに対するデフォルト値の許可的あるいは制限的設定を管理すること	なし	初期値は固定されており、変更できない
	c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること	なし	規則を変更すはできない
FMT_MTD.1	a) TSFデータと相互に影響を及ぼし得る役割のグループを管理すること	なし	所定のアクションため管理されない
FMT_SMF.1	予見される管理アクティビティはない	なし	-
FMT_SMR.1	a) 役割の一部をなすユーザーのグループの管理	なし	所定のアクションため管理されない
FPT_SKP_EXT.1	予見される管理アクティビティはない	なし	-
FPT_STM.1	a) 時間の管理	タイムスタンプ設定の管理。	-
FPT_TST_EXT.1	予見される管理アクティビティはない	なし	-
FPT_TUD_EXT.1	予見される管理アクティビティはない	ソフトウェアの管理	-
FTA_SSL.3	a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定	なし	ユーザー個々に設定できない
	b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定	セッション終了後のユーザーの非アクティブのデフォルト時間の指定	-
FTP_ITC.1	a) もしサポートされていれば、高信チャネルを要求するアクションの構成	セキュアチャネル設定	-
FTP_TRP.1(a)	a) もしサポートされていれば、高信頼パスを要求するアクションの構成	なし	所定のアクションため管理されない
FTP_TRP.1(b)	a) もしサポートされていれば、高信頼パスを要求するアクションの構成	なし	所定のアクションため管理されない

SFR	管理	管理機能	理由
-	-	·アドレス帳の管理 ·SYSLOGサーバーの設定 ·FTPサーバーの設定	-

6.6.6. FMT_SMR.1 Security roles

(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)
Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles *U.ADMIN(a), U.ACCOUNTMANAGER, U.ADDRESSBOOKOPERATOR, and U.NORMAL*.

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

6.7. Class FPT: Protection of the TSF

6.7.1. FPT_SKP_EXT.1 Extended: Protection of TSF Data

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.7.2. FPT_STM.1 Reliable time stamps

(for O.AUDIT)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.7.3. FPT_TST_EXT.1 Extended: TSF testing

(for O.TSF_SELF_TEST)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.7.4. FPT_TUD_EXT.1 Extended: Trusted Update

(for O.UPDATE_VERIFICATION)
Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),

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

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

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

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

6.7.5. FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

(for O.KEY_MATERIAL)
Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.8. Class FTA: TOE Access

6.8.1. FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)
Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*refer to Table 20*].

Table 20 利用者の非アクティブ時間間隔

インタフェース	オートログアウト時間
操作パネル	15 - 150 秒
Webブラウザ	5 - 999 分
プリンタードライバー	対話セッションはない

6.9. Class FTP: Trusted Paths/Channels

6.9.1. FTP_ITC.1 Inter-TSF trusted channel

(for O.COMMS_PROTECTION, O.AUDIT)
Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or

FCS_SSH_EXT.1 Extended: SSH selected, or

FCS_HTTPS_EXT.1 Extended: HTTPS selected].

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

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

FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [*SYSLOG service, FTP service, mail service*].

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

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or

FCS_SSH_EXT.1 Extended: SSH selected, or

FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) **Refinement:** The TSF shall **use** [*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**.

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**.

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

(for O.COMMS_PROTECTION))
Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or

FCS_SSH_EXT.1 Extended: SSH selected, or

FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) **Refinement:** The TSF shall **use** [*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**.

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

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

6.10. セキュリティ保証要件

Table 21にProtection Profile for Hardcopy Devices – v1.0のセキュリティ保証要件を示す。これは、評価保証レベルのEAL1に定義されたコンポーネントセットにASE_SPD.1を追加したものである。

Table 21 TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネント記述
セキュリティターゲット評価 Security Target Evaluation	ASE_CCL.1	適合主張 Conformance claims
	ASE_ECD.1	拡張コンポーネント定義 Extended components definition
	ASE_INT.1	ST概説 ST introduction
	ASE_OBJ.1	運用環境のセキュリティ対策方針 Security objectives for the operational environment
	ASE_REQ.1	主張されたセキュリティ要件 Stated security requirements
	ASE_SPD.1	セキュリティ課題定義 Security Problem Definition
	ASE_TSS.1	TOE要約仕様 TOE Summary Specification
開発 Development	ADV_FSP.1	基本機能定義 Basic functional specification
ガイダンス文書 Guidance Documents	AGD_OPE.1	ユーザー操作ガンダンス Operational user guidance
	AGD_PRE.1	準備手続き Preparative procedures
ライフサイクルサポート Assurance Class	ALC_CMC.1	TOEのラベル付け Labelling of the TOE
	ALC_CMS.1	TOEのCM範囲 TOE CM coverage
テスト Tests	ATE_IND.1	独立テスト-適合 Independent testing – Conformance
脆弱性評定 Vulnerability assessment	AVA_VAN.1	脆弱性調査 Vulnerability survey

6.11. セキュリティ機能要件根拠

6.11.1. セキュリティ機能要件書の依存関係

TOEセキュリティ機能要件について、本STにおける依存性の分析結果をTable 22に示す。

Table 22 セキュリティ機能要件の依存性分析結果

TOEセキュリティ機能要件	CCおよびPPPで要求される依存性	STで満たしている依存性	STで満たしていない依存性	理由
FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	なし	
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	なし	
FCS_CKM.1(a)	[FCS_COP.1(b), or FCS_COP.1(i)], FCS_CKM_EXT.4	FCS_COP.1(b), FCS_CKM_EXT.4	なし	
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(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1(a), FCS_RBG_EXT.1(b)	なし	
FCS_CKM.4	[FCS_CKM.1(a), or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	なし	
FCS_CKM_EXT.4	[FCS_CKM.1(a) or FCS_CKM.1(b)], FCS_CKM.4	FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4	なし	

TOEセキュリティ機能要件	CCおよびPPPで要求される依存性	STで満たしている依存性	STで満たしていない依存性	理由
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	なし	
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	なし	
FCS_COP.1(c)	なし	なし	なし	
FCS_COP.1(d)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	なし	
FCS_COP.1(f)	FCS_CKM.1(b), FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	なし	
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	なし	
FCS_COP.1(h)	FCS_CKM.1(b), FCS_COP.1(c), FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_COP.1(c), FCS_CKM_EXT.4	なし	
FCS_SMC_EXT. 1	FCS_COP.1(c)	FCS_COP.1(C)	なし	
FCS_RBG_EXT.1(a)	なし	なし	なし	
FCS_RBG_EXT.1(b)	なし	なし	なし	
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), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1(b)	なし	
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	なし	
FPT_KYP_EXT.1	なし	なし	なし	
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(i),	FCS_KDF_EXT.1, FCS_SMC_EXT.1,	なし	

TOEセキュリティ機能要件	CCおよびPPPで要求される依存性	STで満たしている依存性	STで満たしていない依存性	理由
	FCS_KDF_EXT.1, and/or FCS_COP.1(f)]	FCS_COP.1(f)		
FCS_KDF_EXT.1	FCS_COP.1(h)	FCS_COP.1(h)	なし	
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	なし	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし	
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	なし	
FDP_FXS_EXT.1	なし	なし	なし	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	なし	
FIA_ATD.1	なし	なし	なし	
FIA_PMG_EXT.1	なし	なし	なし	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	なし	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	なし	
FIA_UID.1	なし	なし	なし	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	なし	
FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	なし	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	なし	
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	なし	
FMT_SMF.1	なし	なし	なし	

TOEセキュリティ機能要件	CCおよびPPPで要求される依存性	STで満たしている依存性	STで満たしていない依存性	理由
FMT_SMR.1	FIA_UID.1	FIA_UID.1	なし	
FPT_SKP_EXT.1	なし	なし	なし	
FPT_STM.1	なし	なし	なし	
FPT_TST_EXT.1	なし	なし	なし	
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b), FCS_COP.1(c)	なし	
FTA_SSL.3	なし	なし	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_TLS_EXT.1, FCS_HTTPS_EXT.1	なし	
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	なし	
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	なし	

6.11.2. セキュリティ保証要件根拠

これらのセキュリティ保証要件を選択する根拠は、最小限のセキュリティベースラインが攻撃者の想定される脅威レベルに基づいていること、TOEにおける運用環境のセキュリティが配備されており、かつTOE自身の価値に見合っていると定義されていることである。STのあらゆるところにある保証アクティビティはセキュリティ保証要件を達成するための明確な期待値についての特注のガイダンスを提供するために使用されている。

7. TOE要約仕様（TOE Summary Specification）

本章では、TOEセキュキュリティ機能（TSF）の要約仕様を記述する。

7.1. 監査

以下にクラスFAUの要件に関する要約仕様を記述する。

FAU_GEN.1

TOE は、監査イベントが発生したときに監査ログを作成し、監査ログファイルに記録する。これにより FAU_GEN.1 を実現している。

Table 23 記録されたイベントおよび監査ログ

監査対象事象	イベント	記録される ユーザーID	結果
監査機能の起動	MFP の電源オン	なし	なし
監査機能の終了	MFP の電源オフ	なし	なし
ジョブの終了	プリントジョブの終了	ジョブ所有者	成功、または失敗
	スキャンジョブの終了	ジョブ所有者	成功、または失敗
	コピージョブの終了	ジョブ所有者	成功、または失敗
	ファクス送信ジョブの終了	ジョブ所有者	成功、または失敗
	ファクス受信ジョブの終了	ジョブ所有者	成功、または削除
ユーザー認証失敗 ユーザー識別失敗	ログインの失敗	ログインしたユーザー	成功、または失敗
ユーザー識別失敗	ログインの失敗（プリントジョブ）	TOE に登録されていないユーザー	失敗
管理機能の利用	ユーザーの追加	変更を行ったユーザー	成功、または失敗
	ユーザーID の変更	変更を行ったユーザー	成功、または失敗
	ユーザーの削除	変更を行ったユーザー	成功
	ユーザー認証失敗処理の管理、最小パスワード長の管理、ユーザーパスワードの管理 (U.ACCOUNTMANAGER/ U.ADMIN(a) /U.NORMAL/ U.ADDRESSBOOKOPERATOR) by U.ADMIN(a)、ユーザーパスワードの管理 (U.ACCOUNTMANAGER/U.NORMAL/ U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER、U.NORMAL による自身のユーザパスワードの管理、U.ADDRESSBOOKOPERATOR による自身のユーザパスワードの管理、ソフトウェアの管理、セッショ	変更を行ったユーザー	成功

監査対象事象	イベント	記録される ユーザーID	結果
	ン終了後のユーザーの非アクティブのデフォルト時間の指定、 セキュアチャネル設定、アドレス帳の管理、SYSLOG サーバー設定、FTP サーバーの設定		
役割の一部であるユーザーグループの改変	役割情報の変更	変更を行ったユーザー	成功
時刻の変更	時間の修正	変更を行ったユーザー	成功
セション確立の失敗	TLS セッション確立の失敗	なし	成功、または失敗

TOE は、監査されるイベントに以下のデータを追加する。

- 日付/時刻： エラー/イベントが発生した時刻
- メッセージ： イベントの内容を説明する文章（セション失敗の場合は、失敗の理由も表示）
- エラーコード： イベントはコードとして定義され、4 桁の 16 進数で表されます。
- ユーザーID： ログインしたユーザーの識別子
- 結果： イベントの実施結果

【関連するTSFI】

- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定、電源キー
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：プリント要求に対するインタフェース
- その他：メインスイッチ、PSTN ファクスインタフェース

FAU_GEN.2

TOE は、監査対象のイベントが発生すると、そのイベントの事由となったユーザーのユーザーID を監査ログに付加することで、FAU_GEN.2 を実現している。

【関連するTSFI】

- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定、電源キー
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：プリント要求に対するインタフェース
- その他：メインスイッチ、PSTN ファクスインタフェース

FAU_STG_EXT.1

U.ADMIN(a)は TopAccess の管理者設定から、SYSLOG サーバーを転送するサーバーとして設定できる。

TOE は、生成された監査データをまず内部ストレージデバイスに保存し、通信プロトコル TLS1.2 を使用して外部監査ログサーバーである SYSLOG サーバーに送信することができる。内部ストレージの

監査ログの保存領域は、ログの最大記録件数は各々メッセージログ：10,000 件、印刷ログ：5,000 件、スキャンログ：5,000 件、ファクスの送信管理記録：5,000 件、ファクスの受信管理記録：5,000 件を保存できる。各々のログの最大記録数が満杯になった場合、各々のログの最も古い監査データが削除され新しい監査データを保存することできる。
内部ストレージに保存された全ての監査ログは、U.ADMIN(a)だけが参照することができ、その他のユーザーは、自身のジョブログしか参照させないアクセス制御を行っている。

【関連するTSFI】
- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定、電源キー
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：　プリント要求に対するインタフェース
- その他：メインスイッチ、PSTN ファクスインタフェース

7.2. 暗号サポート

以下にクラスFCSの要件に関する要約仕様を記述する。

FCS_CKM.1(a)

TOEは、TLS通信のサーバー証明書に用いる非対称暗号鍵として、NIST SP 800-56B,Revision 1の6.3.1.3節に記載のrsakpg1-crt方式でRSA鍵ペアを生成する。鍵の生成に使用する乱数はFCS_RBG_EXT.1(b)に従い、CTR_DRBG(AES)で生成する。生成された公開鍵を含むサーバー証明書とサーバー秘密鍵は、FDP_DSK_EXT.1とFCS_CKM.1(d)に従って暗号化されてSSDに保存される。
なお、TOEは、本TSFに関し、TOE特有の拡張やHCD-PPに記載のない独自処理、あるいは許容された別実装を含んでいない。
本要件に関するTSFIは、以下に示す通りである。

【関連するTSFI】
- TopAccess：管理者設定

FCS_CKM.1(b)

TSFは、TLS通信のネゴシエーションにおいて、通信用のセッション鍵とHMACの鍵を生成する。セッション鍵とHMACの鍵は、サーバ・クライアント間で共有する乱数から生成される。乱数は、FCS_RBG_EXT.1(b)に従い、CTR_DRBG(AES)で生成する。各鍵のパラメータは、選択されたCipher Suiteによって、以下に示す通りである。

- セッション鍵
  通信データを暗号化するのに利用され、選択されたCipher Suiteによって、使用する暗号アルゴリズムと鍵の長さが異なる。暗号アルゴリズムはAES-CBCを使用し、セッション鍵の長さは128bitと256bitが選択できる。
- HMACの鍵
  通信データの改竄検証のために利用され、選択されたCipher Suiteによって、使用する暗号アルゴリズムと鍵の長さが異なる。暗号アルゴリズムにはFCS_COP.1(g)に従ったHMAC-SHA-1またはHMAC-SHA-256を使用し、HMACの鍵の長さはそれぞれ160bitと256bitである。

これらの鍵は、揮発性メモリ内に保存し、電源断で消去される。

【関連するTSFI】

- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定、電源キー
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：プリント要求に対するインタフェース
- その他：メインスイッチ、PSTN ファクスインタフェース

TSFは、ストレージ暗号化のための以下の鍵を生成する。これらの鍵はFPT_KYP_EXT.1に従って保護される。

- KEK導出鍵と鍵材料暗号化鍵
  鍵および鍵材料の保護のために使われる鍵であり、TOE設定時にそれぞれTOEでひとつ生成する。FCS_RBG_EXT.1(a)に従いHash_DRBG(SHA-512)を用いて生成した256bitの乱数を128bitずつに分割し、128bitのKEK導出鍵と128bitの鍵材料暗号化鍵として、揮発性メモリとFROMに保存する。
- DEK
  利用者文書データおよび秘密のTSFデータの保護のために使われる鍵であり、TOE設定時に暗号化パーティションごとに個別に生成する。FCS_RBG_EXT.1(b)に従いCTR_DRBG(AES)で生成した128bitの乱数を、その暗号化パーティションのDEKとして揮発性メモリに保存する。DEKを含む鍵材料はFPT_KYP_EXT.1とFCS_COP.1(f)に従って暗号化されてSSDには暗号文状態で保存される。
- スワッピングパーティション用DEK
  スワップアウトデータの保護のために使われる鍵であり、TOE状態で起動時にひとつ生成する。FCS_RBG_EXT.1(b)に従いCTR_DRBG(AES)で生成した128bitの乱数を、スワッピングパーティション用DEKとして揮発性メモリのみに保存する。この鍵はTOE起動ごとに変更される。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FCS_CKM_EXT.4/FCS_CKM.4

TSFが扱う以下の平文の秘密鍵及びプライベート暗号鍵及び暗号クリティカルパラメータは、不要となった時に破棄される。

- FROM内のKEK導出鍵、鍵材料暗号化鍵
  暗号文状態でSSDに保存された利用者データおよび秘密のTSFデータを復号するために使用され、TOE廃棄時にこれらのデータは不要となるため、復号に用いるすべてのCSPが不要となる。TOEの廃棄時に、不要な鍵または鍵材料として扱われ、鍵が保存されているFROMの領域を、固定の値で1回上書きすることにより破棄する。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

● 揮発メモリ内のKEK導出鍵、鍵材料暗号化鍵、KEK、DEK、スワップパーティション用DEK、サブマスク、LUKS鍵、KEK導出用コンテキスト、通信用のセッション鍵及びHMACの鍵、サーバー秘密鍵

利用者データおよび秘密のTSFデータの暗号処理に使用されるすべてのCSPと、通信用のすべてのCSPは、TOEの電源がOFFからONまでの間は不要となる。電源OFF時に、不要な鍵または鍵材料として扱われ、揮発性メモリ内に格納されたこれら平文の秘密鍵及び暗号クリティカルパラメータは、電源断で消去される。

【関連するTSFI】
- 操作パネル：電源キー
- その他：メインスイッチ

FCS_COP.1(a)

TSFは、FTP_ITC.1、FTP_TRP.1(a)及びFTP_TRP.1(b)における通信データ保護のために、FCS_CKM.1(b)により生成した128bitまたは256bitの暗号鍵とFIPS PUB197に準拠するAES暗号アルゴリズムをNIST SP 800-38Aに準拠するCBCモードで動作させることにより、通信データの暗号化及び復号を行う。
本要件に関するTSFIは、以下に示す通りである。

【関連するTSFI】
- FTP_ITC.1、FTP_TRP.1(a)、FTP_TRP.1(b)の TSFI に準ずる

FCS_COP.1(b)

TSFは、機器証明書作成における署名生成、FTP_ITC.1によるサーバー証明書及びFPT_TUD_EXT.1によるファームウェアのアップデート検証において、FIPS PUB 186-4に規定されたDigital Signature Standardに準拠した鍵長が2048bitのRSAデジタル署名アルゴリズム(rDSA)を使用する。TSFは、機器証明書作成における署名生成及びサーバー証明書の検証ではRSASSA-PKCS1-v1_5を、ファームウェアアップデート検証ではRSASSA-PSSを用いる。また、証明書の作成はFCS_CKM.1(a)により生成されたRSA鍵を使用する。
本要件に関するTSFIは、以下に示す通りである。

【関連するTSFI】
- FTP_ITC.1 および FPT_TUD_EXT.1 の TSFI に準ずる
- TopAccess：管理者設定

FCS_RBG_EXT.1(a)

TSFは、TOEのストレージ暗号化のためのKEK導出鍵と鍵材料暗号化鍵の生成にあたって、エントロピー源およびDRBGを用いて乱数を生成する。このDRBGは、NIST SP 800-90Aに従ってHash_DRBG (SHA-512)を用いて乱数を生成する。エントロピー源は、一つのハードウェアベースによるノイズ源を含み、DRBGに供給されるエントロピー量は後述する。ノイズ源はTOEのSoC（Intel Atomプロセッサーx5-E3930）が内蔵するハードウェアのESを使用する。ノイズ源からの出力は、SoC内のDRBGのシードに用いられ、NIST SP 800-90AのCTR_DRBG(AES)に従った処理を行ってRDRAND命令で出力される。ノイズ源は、1bitあたり0.5bit以上の最小エントロピーを含むことが

[Rambus 2012]の記述から分かっており、RDRAND命令はノイズ源からの256ビットエントロピーのシードで初期化されたセキュリティ強度128ビットのDRBGの出力である。RDRAND命令は128bitを511個分出力するとESからリシードされる仕様であるので、エントロピー源を構成するrngdデーモンプロセスはRDRAND命令で取得した128*512=65,536bit=8,192byteをAES-CBC-MAC処理で16byteに圧縮することで、16byteごとにシードが異なるRDRAND命令出力を収集し、rngdの2,500byteの3つのバッファにほぼフルエントロピーのデータを一時的に蓄積する。このTSFが使用されるとき、Linux PRNGが2048bit以上のエントロピーを保持する状態にパラメータを設定されているので、TSFのHash_DRBG(SHA-512)がLinux PRNGの/dev/urandom出力から読み出す128byteのデータはほぼフルエントロピーの状態と推定する。この128byteのうち96byteの部分をEntropy InputとNonceとし、Hash_DRBG(SHA-512)のシード値として供給する。

TSFの開発者はNIST SP800-90Bの6節の最小エントロピー見積もりにより、TOEの動作条件の範囲で、/dev/urandom出力が1bitあたり0.85bit以上の最小エントロピーを含むことを確認した。フルエントロピーでないと悲観的に見積もっても、NIST SP800-90Bの3.1.5節に従ったエントロピー量の下限評価により、/dev/urandom出力の96byteのビット列には652.80(=96*8*0.85)bitのエントロピーが含まれると推定する。このビット列をEntropy InputとNonceとし、Hash_DRBG(SHA-512)にシード値を供給する事により、FCS_RGB_EXT.1(a)を実現している。

【関連するTSFI】

- 操作パネル：電源キー（TOE 設置後の初回起動に限る）
- その他：メインスイッチ（TOE 設置後の初回起動に限る）

FCS_RBG_EXT.1(b)

TSFは、TOEのストレージ暗号化のための暗号化パーティションごとの鍵および鍵材料（KEK導出用コンテキスト、DEK、サブマスクとLUKS鍵）の生成のため、FTP_ITC.1、FTP_TRP.1(a)及びFTP_TRP.1(b)における通信データ保護のため、TLS通信のサーバー秘密鍵生成ならびにTLS通信のネゴシエーションのために、エントロピー源およびDRBGを用いて乱数を生成する。TOEのCTR_DRBGはNIST SP 800-90Aに従ったCTR_DRBG (AES)の同じ構造を持つプライマリーDRBGとプライベートDRBGの2段構成になっており、プライベートDRBGの出力が鍵および鍵材料を生成するためのTSFによる乱数出力である。エントロピー源は、一つのハードウェアベースによるノイズ源を含み、DRBGに供給されるエントロピー量は後述する。ノイズ源はTOEのSoC（Intel Atomプロセッサーx5-E3930）が内蔵するハードウェアのESを使用する。ノイズ源からの出力は、SoC内のDRBGのシードに用いられ、NIST SP 800-90AのCTR_DRBG(AES)に従った処理を行ってRDRAND命令で出力される。ノイズ源は、1bitあたり0.5bit以上の最小エントロピーを含むことが[Rambus 2012]の記述から分かっており、RDRAND命令はノイズ源からの256ビットエントロピーのシードで初期化されたセキュリティ強度128ビットのDRBGの出力である。RDRAND命令は128bitを511個分出力するとESからリシードされる仕様であるので、エントロピー源を構成するrngdデーモンプロセスはRDRAND命令で取得した128*512=65,536bit=8,192byteをAES-CBC-MAC処理で16byteに圧縮することで、16byteごとにシードが異なるRDRAND命令出力を収集し、rngdの2,500byteの3つのバッファにほぼフルエントロピーのデータを一時的に蓄積する。rngdからLinux PRNGに必要なエントロピーが十分に供給されるので、TSFがLinux PRNGの/dev/random出力から読み出すデータはほぼフルエントロピーの状態と推定する。TSFの開発者はNIST SP800-90Bの6節の最小エントロピー見積もりにより、TOEの動作条件の範囲で、/dev/random出力が1bitあたり0.82bit以上の最小エントロピーを含むことを確認した。フ

ルエントロピーでないと悲観的に見積もっても、NIST SP800-90Bの3.1.5節に従ったエントロピー量の下限評価により、/dev/random出力の32byteのビット列には209.92(=32*8*0.82)bitのエントロピーが含まれると推定する。同様に/dev/random出力の16byteのビット列には104.96(=16*8*0.82)bitのエントロピーが含まれると推定する。この合計48byteのビット列をプライマリーDRBGと呼ぶCTR_DRBG(AES)の初期化の32byteのentropy_inputと16byteのnonceを連結して入力する48byteのシードに用いる。プライマリーDRBGのCTR_DRBG(AES)は128ビットのセキュリティ強度を持つ。さらにプライベートDRBGは同じく32byteのentropy_inputと16byteのnonceをプライマリーDRBGから供給される。プライベートDRBGも同様に128bitのセキュリティを持つと考えられる。FCS_RBG_EXT.1(b)の利用はプライベートDRBGのCTR_DRBG(AES)の乱数生成関数を呼び出す。リシードに関してはプライベートDRBGへの2^{32}回の呼び出しまでにプライマリーDRBGが/dev/random出力による32byteのentropy_inputによるリシードと、プライマリーDRBG出力を用いたプライベートDRBGの32byteのentropy_inputによるリシード処理が行われる。これらにより、プライベートDRBGは128ビットのセキュリティ強度を持つFCS_RGB_EXT.1(b)を実現している。

【関連するTSFI】

- FTP_TRP.1(a)、FTP_TRP.1(b)および FTP_ITC.1 の TSFI に準ずる
- 操作パネル：電源キー（TOE 設置後の初回起動に限る）
- その他：メインスイッチ（TOE 設置後の初回起動に限る）

7.3. ストレージ暗号化（条件付き必須要件）

以下に条件付き必須要件B.1に関する要約仕様を記述する。

FPT_KYP_EXT.1

TOE 設定時に FCS_KYC_EXT.1 の鍵チェインで特定される鍵および鍵材料が生成され、TOE 廃棄まで保護される。鍵の保存場所と保護の状態は以下のとおりであり、現地交換な不揮性ストレージデバイスである FRAM または SSD に平文状態の鍵は保存されない。鍵および鍵材料のサイズは FCS_KYC_EXT.1 の TSS に記述する。

- KEK導出鍵と鍵材料暗号化鍵
  KEK 導出鍵と鍵材料暗号化鍵はそれぞれ TOE でひとつの鍵が FCS_COP.1(b)に従って生成され、揮発性メモリへの保存と現地交換不可能な不揮発性ストレージである FROM に平文状態で保存が行われる。

- KEK 導出用コンテキスト
  KEK 導出用コンテキストは、利用者データまたは秘密の TSF データを保存する SSD の暗号化パーティションごとに個別に乱数から生成され、揮発性メモリに保存される。KEK 導出用コンテキストは FCS_COP.1(f)に従って鍵材料暗号化鍵で暗号化されてから、SSD の暗号化パーティションの先頭部の管理ヘッダ領域内に暗号文状態で保存される。

- KEK
  KEK は、利用者データまたは秘密の TSF データを保存する SSD の暗号化パーティションごとに個別に FCS_KDF_EXT.1 に従って KEK 導出鍵と鍵材料暗号化鍵および KEK 導出用コンテキストから生成され、揮発性メモリのみに保存される。

- DEK
  DEK は利用者データまたは秘密の TSF データを保存する SSD の暗号化パーティションごとに個別の鍵が FCS_COP.1(b)に従って生成され、揮発性メモリのみに保存される。

● サブマスクと LUKS 鍵
サブマスクの導出に用いる LUKS データは、利用者データまたは秘密の TSF データを保存する SSD の暗号化パーティションごとに乱数から個別に生成され、揮発性メモリに保存される。サブマスクは LUKS データの特定範囲から符号生成ルールに従って導出され、揮発性メモリのみに保存される。
LUKS 鍵の生成にあたっては FCS_SMC_EXT.1 に従って DEK にサブマスクを XOR することで LUKS 鍵が導出され、LUKS 鍵は LUKS データ末尾（未使用部分）の揮発性メモリに保存される。
LUKS 鍵を含む LUKS データは FCS_COP.1(f)に従って KEK で暗号化されてから、SSD の暗号化パーティションの先頭部の管理ヘッダ領域内に暗号文状態で保存される。

【関連するTSFI】
・ なし

FCS_KYC_EXT.1

TOE の鍵チェイン FCS_KYC_EXT.1 における BEV は、ストレージデータ暗号化鍵（DEK）である。TOE 設定時に FCS_KYC_EXT.1 の鍵チェインを構成する鍵および鍵材料を生成する。鍵チェインは以下の鍵および鍵材料から構成される。

● KEK導出鍵と鍵材料暗号化鍵
TOE 設定時に、FCS_RBG_EXT.1(a)に従い Hash_DRBG(SHA-512)を用いて生成した 256bit の乱数を 128bit ずつに分割し、KEK 導出鍵と鍵材料暗号化鍵を生成する。KEK 導出鍵と鍵材料暗号化鍵は、揮発性メモリおよび FROM に平文状態で保存される。なお、FROM は現地交換不可能な不揮発性ストレージである。TOE 状態の起動時では、FROM から読み出した KEK 導出鍵と鍵材料暗号化鍵を使用する。

● KEK導出用コンテキスト
TOE 設定時に、FCS_RBG_EXT.1(b)に従って CTR_DRBG(AES)を用いて生成した 256bit の乱数が KEK 導出用コンテキストである。暗号化パーティションごとに生成され、揮発性メモリへの保存と SSD への暗号文状態での保存が行われる。KEK 導出用コンテキストは、FCS_COP.1(f)に従い AES-CBC で 128bit の鍵材料暗号化鍵を用いて暗号化される管理ヘッダに含まれ、暗号文状態で SSD に保存される。TOE 状態の起動時では、SSD から読み出した暗号文状態の管理ヘッダを FCS_COP.1(f)に従い AES-CBC で鍵材料暗号化鍵を用いて復号した結果から KEK 導出用コンテキストを取り出すことにより揮発性メモリに保存される。

● KEK
TOE 設定時に、FCS_KDF_EXT.1 に従って揮発メモリに保存された KEK 導出鍵と鍵材料暗号化鍵と KEK 導出用コンテキストを用い、SP800-108 の KDF カウンターモードに定義されるとおり、FCS_COP.1(h)で特定される HMAC-SHA-256 を用いて 128bit の鍵が導出され、KEK として揮発性メモリに保存される。TOE 状態の起動時は同じ処理手順で 128bit の鍵が導出され、KEK として揮発性メモリに保存される。

● DEKとサブマスクとLUKS鍵
TOE 設定時に、FCS_RBG_EXT.1(b)に従って CTR_DRBG(AES)を用いて生成した 128bit の乱数を DEK とする。DEK は暗号化パーティションごとに生成され、揮発性メモリに保存される。次に、FCS_RBG_EXT.1(b)に従って CTR_DRBG(AES)を用いて生成された 63984 バイトの乱数を揮発性メモリの LUKS データに保存する。LUKS データの特定範囲から符号生成ルールに従ってから 128bit のサブマスクを導出し、揮発メモリに保存する。LUKS 鍵の生成にあたっては

FCS_SMC_EXT.1 に従って 128bit の DEK に 128bit のサブマスクを XOR することで 128bit の LUKS 鍵を導出し、LUKS 鍵を LUKS データの末尾（未使用部分）の揮発性メモリに保存する。つぎに LUKS 鍵を含む 64000 バイトの LUKS データを、FCS_COP.1(f)に従い AES-CBC で 128bit の KEK を用いて暗号化し、暗号文状態で SSD に保存する。TOE 状態の起動時では、SSD から読み出した暗号文状態の LUKS データを FCS_COP.1(f)に従い AES-CBC で 128bit の KEK を用いて復号した結果からサブマスクの導出と LUKS 鍵の取り出しを行う。DEK の生成にあたっては FCS_SMC_EXT.1 に従って 128bit の LUKS 鍵に 128bit のサブマスクを XOR することで 128bit の DEK を導出し、DEK を揮発性メモリに保存する。

- 鍵チェインの強度

KEK 導出鍵と鍵材料暗号化鍵はそれぞれ 128bit であり、FCS_RBG_EXT.1(a)と FCS_RBG_EXT.1(b)にはそれぞれ十分なエントロピー十分なエントロピーが供給されているため鍵の強度は 128bit である。鍵導出の FCS_KDF_EXT.1 および FCS_COP.1(f)が 128bit のセキュリティ強度であるため、鍵チェインの各段階にて 128bit のセキュリティ強度を確保している。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FDP_DSK_EXT.1

TOE の現地交換可能な不揮発性ストレージは FRAM と SSD の 2 つである。TOE 状態では FRAM には MFP の印刷設定値や調整値等の秘密でないデータのみが保存されており、TOE はディスク上のデータ保護の対象の利用者文書データ及び秘密の TSF データを書き込むことはない。利用者文書データ及び秘密の TSF データは SSD にのみ暗号文状態で保存する。SSD はパーティションで分割されてそれぞれファイルシステムが作成される。以下に SSD の 3 つのパーティションの種別と暗号化されない領域について記述する。使用する鍵および鍵材料の詳細は TSS の FCS_KYC_EXT.1 の項に従う。

- 非暗号化パーティション

利用文書データおよび秘密の TSF データでない任意のデータを保存するパーティションの種別であり、本要件によるディスク上のデータ保護の対象のデータを含まない。

- 暗号化パーティション

利用者文書データおよび秘密の TSF データおよびそれらに関連するコアダンプ等のデータを保存するパーティションの種別である。暗号化パーティションに対する透過的暗号化機能は暗号化パーティションをマウントするときに開始される。TOE はこのパーティションに作成された通常ファイルシステムに書き込まれるすべてのファイルおよびメタデータは、必ず FCS_COP.1(d)に従って暗号化されてからブロックデバイスドライバを経由して SSD に暗号文状態で保存される。読み出し処理では逆の手順により FCS_COP.1(d)に従って復号され、平文状態でファイルシステムから読み出される。ここで FCS_COP.1(d)に従った暗号化と復号には暗号化パーティションごとの 128bit の DEK が使用される。

TOE 設置時には鍵および鍵材料が生成される。まず TOE でひとつの KEK 導出鍵と鍵材料暗号化鍵が生成され、揮発性メモリと現地交換可能な不揮発性ストレージではない FROM に平文状態で保存される。次に利用者データおよび秘密の TSF データを保存するそれぞれの暗号化パーティションの透過的な暗号化機能が有効化される。このとき暗号化パーティションごとに KEK 導出用コンテキスト、KEK、DEK、LUKS データ、サブマスク、LUKS 鍵が生成される。KEK と DEK と LUKS デー

タから導出されるサブマスクを除く、KEK 導出用コンテキストと、LUKS 鍵を含む LUKS データがそれぞれ暗号文状態で SSD に保存される。まず FCS_KDF_EXT.1 に従って KEK 導出鍵と鍵材料暗号化鍵と KEK 導出用コンテキストから 128bit の KEK を導出し揮発性メモリに保存する。KEK 導出用コンテキストを含む管理ヘッダは FCS_COP.1(f)に従って鍵材料暗号化鍵で暗号化され、LUKS 鍵を含む LUKS データは FCS_COP.1(f)に従って KEK で暗号化され、それぞれの暗号文は暗号化パーティション先頭の管理ヘッダ領域の特定の場所に暗号文状態で保存される。最後に透過的暗号化機能が有効化された暗号化パーティションにファイルシステムを作成する。

TOE 状態では起動時に FROM から KEK 導出鍵と鍵材料暗号化鍵を読み出して揮発性メモリに保存する。次に暗号化パーティション先頭の管理ヘッダ領域から暗号文状態の KEK 導出用コンテキストを含む暗号文と LUKS 鍵を含む LUKS データの暗号文を読み出して揮発性メモリに保存する。KEK 導出用コンテキストを含む暗号文は FCS_COP.1(f)に従って鍵材料暗号化鍵で復号し、KEK 導出用コンテキストを揮発性メモリに保存する。次に FCS_KDF_EXT.1 に従って KEK 導出鍵と鍵材料暗号化鍵と KEK 導出用コンテキストから 128bit の KEK を導出し揮発性メモリに保存する。次に LUKS 鍵を含む LUKS データの暗号文を FCS_COP.1(f)に従って KEK で復号し、LUKS データと LUKS 鍵を揮発性メモリに保存する。LUKS 鍵に LUKS データから導出したサブマスクを XOR して導出した DEK を揮発性メモリに保存する。この一連の処理で導出した DEK を用いて透過的暗号化機能の FCS_COP.1(d)に従った暗号化と復号が開始される。

- スワップパーティション

TOE のスワップ機能が、TOE の揮発性メモリがひっ迫したときに優先度の低いデータ（スワップアウトデータ）を保存するパーティションの種別である。スワップパーティションに対する透過的暗号化機能はスワップパーティションをマウントするときに開始される。このパーティションのスワップファイルシステムに書き込まれるすべてのスワップアウトデータおよびメタデータは、必ず FCS_COP.1(d)に従って暗号化されてからブロックデバイスドライバを経由して SSD に暗号文状態で保存される。これによりスワップアウトデータに利用者文書データおよび秘密の TSF データが含まれる場合であっても FDP_DSK_EXT の保護を供する。読み出し処理では逆の手順により FCS_COP.1(d)に従って復号され、スワップアウトデータは平文状態でファイルシステムから読み出される。

TOE 設定時および TOE 状態の起動時にスワップパーティションの透過的な暗号化機能を有効化する。FCS_RBG_EXT.1(b)に従って CTR_DRBG(AES)を用いて生成した 128bit の乱数をスワップパーティション用 DEK として揮発性メモリに保存する。このスワップパーティション用 DEK を用いて透過的暗号化機能の FCS_COP.1(d)に従った暗号化と復号が開始される。そのあとスワップファイルシステムを作成してスワップパーティションとしての使用を開始する。

- 暗号化されない領域

SSD の暗号化されない領域は、ブートローダ、パーティションテーブル、利用者文書データおよび秘密の TSF データでないデータを格納するパーティション、利用者文書データおよび秘密の TSF データを格納する各パーティション先頭の管理ヘッダ用領域の非暗号化領域である。より詳細には SSD の各暗号化パーティション先頭の 1MiB が管理ヘッダ用領域であり、暗号文状態で保存されている管理ヘッダは先頭から 1KiB からの 1KiB、暗号文状態で保存されている LUKS データは先頭から 4KiB からの 64000 バイトである。管理ヘッダ用領域のそれ以外の領域は暗号化されない領域であるが、秘密のデータが保存されることはない。

【関連するTSFI】

- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：プリント要求に対するインタフェース
- その他：PSTN ファクスインタフェース

7.4. ストレージ暗号化（選択要件）

以下にストレージ暗号化で選択した要件D.1とD.4に関する要約仕様を記述する。

FCS_COP.1(f)

TSFは、平文状態の管理ヘッダ（KEK導出用コンテキストを含む）と平文状態のLUKSデータ（LUKS鍵を含む）に対する処理と、SSDから読み込んだ暗号文状態の管理ヘッダ（KEK導出用コンテキストを含む）と暗号文状態のLUKSデータ（LUKS鍵を含む）に対する処理に用いられる。

TSFは、TOE設置時はFCS_KYC_EXT.1のTSSに従って生成した128bitの鍵材料暗号化鍵を用い、平文状態の管理ヘッダをISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで暗号化し、暗号文状態の管理ヘッダをSSDに保存する。

TSFは、TOE設置時はFCS_KYC_EXT.1のTSSに従って生成した128bitのKEKを用い、平文状態のLUKSデータをISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで暗号化し、暗号文状態のLUKSデータをSSDに保存する。

TSFは、TOE状態の起動時にはFCS_KYC_EXT.1のTSSに従ってFROMから読み込んだ128bitの鍵材料暗号化鍵を用い、SSDから読み込んだ暗号文状態の管理ヘッダをISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで復号し、平文状態の管理ヘッダを揮発性メモリに保存する。

TSFは、TOE状態の起動時にはFCS_KYC_EXT.1のTSSに従って生成した128bitのKEKを用い、SSDから読み込んだ暗号文状態のLUKSデータをISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで復号し、平文状態のLUKSデータを揮発性メモリに保存する。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FCS_KDF_EXT.1

TSF は、NIST SP800-108 のカウンターモード KDF であって、その PRF に FCS_COP.1(h)で特定される鍵付きハッシュ関数として HMAC-SHA-256 を用いて 128bit の KEK を導出する。NIST SP800-108 のカウンターモード KDF への入力のサブマスクは、FCS_RBG_EXT.1(a)に従い Hash_DRBG(SHA-512)を用いて生成した 256bit の乱数を 128bit ずつに分割した KEK 導出鍵と鍵材料暗号化鍵を連結した 256bit を K_{IN} とし、FCS_RBG_EXT.1(b)に従い CTR_DRBG(AES)を用いて生成した乱数による 256bit の KEK 導出用コンテキストを Context とするので、出力は 128bit のセキュリティ強度の条件を満足する。ここで K_{IN} と Context はどちらも FCS_RBG_EXT.1 で特定された RNG が生成したサブマスクであるので、SFR の要求を満足する。

TOE 設定時には、KEK 導出鍵と鍵材料暗号化鍵を連結した 256bit と、KEK 導出用コンテキストを TSF の入力のサブマスクに用いる。TOE 設置後の起動時には、FROM から読み込んだ KEK 導出鍵と鍵材料暗号化鍵を連結した 256bit と、SSD から読み出した暗号文を復号した KEK 導出用コンテキストを TSF の入力のサブマスクに用いる。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FCS_SMC_EXT.1

TSFは、TOE設定時はLUKS鍵を生成するために、128bitのDEKに128bitのサブマスクをXORして128bitのLUKS鍵を生成する。

TSFは、TOE状態での起動時にはDEKを生成するために、128bitのLUKS鍵に128bitのサブマスクをXORして128bitのDEKを生成する。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FCS_COP.1(h)

TSF は、KEK 導出鍵と鍵材料暗号化鍵と KEK 導出用コンテキストから KEK を導出する際に、FCS_KDF_EXT.1 の鍵付きハッシュメッセージ関数の計算に、ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”; ISO/IEC 10118 に準拠した HMAC-SHA-256 を使用する。HMAC の鍵長は 256bit、ハッシュ関数は SHA-256、ブロック長は 512bit、出力される MAC 長は 256bit である。

【関連するTSFI】

- 操作パネル：電源キー
- その他：メインスイッチ

FCS_COP.1(d)

TSFは、利用者文書データおよび秘密のTSFデータおよびそれらに関連するコアダンプ等を種別ごとに割り当てられたSSDの暗号化パーティションに書き込むときに透過的に暗号化を行う。ストレージ暗号化の暗号方式としてSSDへの書き込みデータの暗号化とSSDからの読み出しデータの復号を透過的に行うため、TOE状態での起動時にFCS_CKM.1(b)に従って鍵生成されたFCS_KYC_EXT.1で特定される128bitのDEKを鍵に用い、ISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで暗号化および復号を実行する。

TSFは、メインメモリからスワップアウトされたスワップアウトデータをSSDのスワップパーティションに書き込むときに透過的に暗号化を行う。ストレージ暗号化の暗号方式としてSSDへの書き込みデータの暗号化とSSDからの読み出しデータの復号を透過的に行うため、TOE状態での起動時に

FCS_CKM.1(b)に従って鍵生成される128bitのスワップパーティション用DEKを鍵に用い、ISO/IEC 18033-3のAESとISO/IEC 10116のCBCの組み合わせによるAES-CBCで暗号化および復号を実行する。

【関連するTSFI】

- 操作パネル：ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信、プリント、ジョブ表示およびログ表示、管理者設定、電源キー
- TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
- プリンタードライバー：プリント要求に対するインタフェース
- その他：その他：メインスイッチ、PSTN ファクスインタフェース

7.5. 通信の保護（選択要件）

以下に選択要件D.2に関する要約仕様を記述する。

FCS_TLS_EXT.1

TSF は、FTP_ITC.1 に示す各種サーバーとの通信及び FTP_TRP.1(a)/FTP_TRP.1(b)に示すクライアント PC との通信において、TLS 通信をサポートする。TSF がサポートする TLS 通信は TLS1.2(RFC 5246)である。

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

TSFがクライアントPCと通信する場合の動作

- TSFは、FCS_RBG_EXT.1(b)及びFCS_CKM.1(a)に従い、TLS通信で用いるRSAのサーバー秘密鍵および公開鍵を生成する。FCS_COP.1(b)及びFCS_COP.1(c)に従い、この秘密鍵とハッシュアルゴリズムを用いてサーバー証明書の署名を生成する。
- 秘密の乱数データを共有する方法は以下の通りである。
  - ✧ TSF は、サーバー秘密鍵を用いて、クライアント PC から送られてきた RSA 公開鍵で暗号化されている秘密の乱数を復号する。FCS_COP.1(c)及び FCS_COP.1(g)に従い、メッセージ認証のための鍵付ハッシング(HMAC)を用いて、秘密の乱数からセッション鍵や HMAC の鍵を生成する。
- TSFが、通信データの暗号化及び検証をする方法は以下の通りである。
  - ✧ TSF は、FCS_COP.1(c)及び FCS_COP.1(g)に従い、HMAC の鍵を用いて、通信データの改竄検証を行う。

✧ TSF は、FCS_COP.1(a)に従い、AES-CBC モードで通信データの暗号化及び復号を行う。

【関連するTSFI】

・ FTP_TRP.1(a)、FTP_TRP.1(b)の TSFI に準ずる

TSFが各種サーバーとの通信を行う場合の動作

- TSFが、各種サーバーから送られてきたサーバー証明書のデジタル署名を検証する方法は以下の通りである。

  ✧ TSF は、FCS_COP.1(c)に従いサーバー証明書検証のためのハッシュ値を計算する。

  ✧TSF は、FCS_COP.1(b)に従う RSA 署名検証によりサーバー証明書のデジタル署名を復号し、前記のサーバー証明書検証のためのハッシュ値と比較することでサーバー証明書の改竄検証を行う。

- 秘密の乱数データを共有する方法は以下の通りである。

  ✧ TSF は、セッション鍵や HMAC の鍵を生成するため、FCS_RBG_EXT.1(b)に従って秘密の乱数を生成する。

  ✧ TSF は、各種サーバーから送られてきたサーバー証明書に含まれる RSA 公開鍵を用いて、秘密の乱数を暗号化する。FCS_COP.1(c)及び FCS_COP.1(g)に従い、メッセージ認証のための鍵付ハッシング(HMAC)を用いて、秘密の乱数からセッション鍵や HMAC の鍵を生成する。

- TSFが、通信データの暗号化及び検証をする方法は以下の通りである。

  ✧ TSF は、FCS_COP.1(c)及び FCS_COP.1(g)に従い、HMAC の鍵を用いて、通信データの改竄検証を行う。

  ✧ TSF は、FCS_COP.1(a)に従い、AES-CBC モードで通信データの暗号化及び復号を行う。

【関連するTSFI】

・ FTP_ITC.1 の TSFI に準ずる

TSFがクライアントPCとIPPSを用いて通信する場合の動作

- TSFは、FCS_RBG_EXT.1(b)及びFCS_CKM.1(a)に従い、TLS通信で用いるRSAのサーバー秘密鍵および公開鍵を生成する。FCS_COP.1(b)及びFCS_COP.1(c)に従い、この秘密鍵とハッシュアルゴリズムを用いてサーバー証明書の署名を生成する。

- TSFは、サーバー秘密鍵を用いて、クライアントPCから送られてきたRSA公開鍵で暗号化されている秘密の乱数を復号する。FCS_COP.1(c)及びFCS_COP.1(g)に従い、メッセージ認証のための鍵付ハッシング(HMAC)を用いて、秘密の乱数からセッション鍵やHMACの鍵を生成する。

- TSFは、FCS_COP.1(c)及びFCS_COP.1(g)に従い、HMACの鍵を用いて、通信データの改

竄検証を行う。

- TSFは、FCS_COP.1(a)に従い、AES-CBCモードで通信データの暗号化及び復号を行う。

【関連するTSFI】
・ プリンタードライバー：プリント要求に対すインタフェース

FCS_HTTPS_EXT.1

TOE とリモート利用者とを高信頼通信パスを確立するために、RFC2818 に適合した HTTPS プロトコルを実装している。また、FCS_TLS_EXT.1 で指定された TLS プロトコルを用いた HTTPS 通信を可能にする事により FCS_HTTPS_EXT.1 を実現している。

【関連するTSFI】
・ TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定

FCS_COP.1(g)

TSFは、TLS通信において秘密の乱数からセッション鍵やHMACの鍵を生成する処理に含まれるHMACで使用される。また、TSFはTLS通信において通信データの改竄検証をするためのHMACで使用される。FIPS PUB 198-1、「The Keyed-Hash Message Authentication Code」、及びFIPSPUB 180-3、「Secure Hash Standard」を満たすメッセージ長及び鍵長が160bitのHMAC-SHA-1、メッセージ長及び鍵長が256bitのHMAC-SHA256に従って鍵付ハッシュメッセージ認証は実行される。この際に使用されるハッシュ関数は、FCS_COP.1(c)に従っている。これにより、FCS_COP.1(g)は実現される。

【関連するTSFI】
・ FTP_TRP.1(a)、FTP_TRP.1(b)および FTP_ITC. 1 の TSFI に準ずる

7.6. 高信頼アップデート（選択要件）

以下に選択要件D.3に関する要約仕様を記述する。

FCS_COP.1(c)

TSFは、以下の3つ処理に用いられる。

TSFは、FPT_TUD_EXT.1におけるファームウェアのアップデートの際にファームウェアの真正性を検証するために、ファームウェアにはデジタル署名が必ず付けられる。その暗号ハッシュ関数は、ISO/IEC 10118-3:2004に合致するSHA-256に従っている。
TSFは、FCS_TLS_EXT.1に従いTLS通信のサーバー証明書の署名生成または検証に行う。その際に使われる暗号ハッシュ関数は、ISO/IEC 10118-3:2004に合致するSHA-1、SHA-256、SHA-384又はSHA-512に従っている。
TSFは、通信データの完全性を検証する際に、FCS_COP.1(g)に従い鍵付ハッシュメッセージ認証を実行する。その際に使われる暗号ハッシュ関数は、ISO/IEC 10118-3:2004に合致するSHA-1及びSHA-256に従っている。
以上より、FCS_COP.1(c)は実現される。

【関連するTSFI】
・ FTP_TRP.1(a)、FTP_TRP.1(b)および FTP_ITC.1 に準ずる

7.7. 利用者データ保護

以下にクラスFDPの要件に関する要約仕様を記述する。

FDP_ACC.1/FDP_ACF.1

TOEは、ユーザー文書データへのアクセス制御と、ユーザー文書データの操作へのアクセス制御を行う。ユーザー文書データへのアクセス制御は、その文書データに紐付けされたユーザーIDと、ログインで識別認証されたユーザーのユーザーIDが一致した場合にのみアクセスを許可する。また、ユーザー文書の操作へのアクセス制御は、Table 14およびTable 15で示される規則とおり、ユーザーが持つ役割に従い、操作が実施される。

FCC_ACC.1およびFDP.AFC.1は下表のアクセス制御によって実現されている。

Table 24 D.USER.DOC のプリントアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・ U.ADMIN(a)と U.NORMAL(a)をプリントする文書の投入のジョブ所有者として割付ける。 ・ 自身の投入した文書の閲覧および出力を許可する。 ・ 自身の投入した文書の改変は拒否する。 ・ 自身の投入した文書の削除は許可する。
U.ADMIN(a)	・ プリントする文書の投入を許可する。 ・ 他のユーザーが投入したプリント文書の閲覧を拒否する。 ・ 他のユーザーが投入したプリント文書の改変を拒否する。 ・ 他のユーザーが保存したプリント文書の削除を許可する。
U.NORMAL(a)	・ プリントする文書の投入を許可する。 ・ 他のユーザーが投入したプリント文書の閲覧を拒否する。 ・ 他のユーザーが投入したプリント文書の改変を拒否する。 ・ 他のユーザーが保存したプリント文書の削除を拒否する。
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・ プリントする文書の投入を拒否する。 ・ 全ての投入したプリント文書の閲覧を拒否する。 ・ 全ての投入したプリント文書の改変を拒否する。 ・ 全ての保存したプリント文書の削除を拒否する。
未認証ユーザー	・ 識別された U.ADMIN(a)、U.NORMAL(a)からプリント文書の投入は許可する。 ・ 全ての投入したプリント文書の閲覧を拒否する。 ・ 全ての投入したプリント文書の改変を拒否する。 ・ 全ての保存したプリント文書の削除を拒否する。

【関連するTSFI】

- 操作パネル：プリント
- プリンタードライバー：プリント要求に対するインタフェース

Table 25 D.USER.DOC のスキャンアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.NORMAL(a)をスキャンする文書の投入のジョブ所有者として割付ける。 ・自身がスキャンした画像の閲覧を許可する。 ・自身がスキャンした画像の改変および削除は許可する。
U.ADMIN(a)	・スキャンする文書の投入を許可する。 ・他のユーザーがスキャンした画像の閲覧を拒否する。 ・全てのユーザーがスキャンした画像の改変は拒否する。 ・自身のスキャンした画像の削除は許可し、他のユーザーのスキャンした画像の削除は拒否する。
U.NORMAL(a)	・スキャンする文書の投入を許可する。 ・他のユーザーがスキャンした画像の閲覧を拒否する。 ・他のユーザーがスキャンした画像の改変および削除は拒否する。
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・スキャンする文書の投入を拒否する。 ・全てのスキャンした画像の閲覧を拒否する。 ・全てのユーザーがスキャンした画像の改変および削除は拒否する。
未認証ユーザー	・スキャンする文書の投入を拒否する。 ・全てのスキャンした画像の閲覧を拒否する。 ・全てのスキャンした画像の改変および削除は拒否する。

【関連するTSFI】

・操作パネル：スキャン、かんたんスキャン

Table 26 D.USER.DOC のコピーアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.ADMIN(a)と U.NORMAL(a)をコピーする文書の投入のジョブ所有者として割付ける。 ・自身が印刷したコピーの出力を許可する。 ・自身が保存した画像の改変を拒否する。 ・自身が保存した画像の削除を許可する。
U.ADMIN(a)	・コピーする文書の投入を許可する。 ・他のユーザーがコピーした画像の閲覧を拒否する。 ・他のユーザーがコピーし保存した画像の改変を拒否する。 ・他のユーザーがコピーし保存した画像の削除を許可する。
U.NORMAL(a)	・コピーする文書の投入を許可する。 ・他のユーザーがコピーした画像の閲覧を拒否する。 ・他のユーザーがコピーし保存した画像の改変を拒否する。 ・他のユーザーがコピーし保存した画像の削除を拒否する。

ユーザー	アクセス制御規則
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・ コピーする文書の投入を拒否する。 ・ 全てのコピーした画像の閲覧を拒否する。 ・ 全てのコピーし保存した画像の改変を拒否する。 ・ 全てのコピーし保存した画像の削除を拒否する。
未認証ユーザー	・ コピーする文書の投入を拒否する。 ・ 全てのコピーした画像の閲覧を拒否する。 ・ 全てのコピーし保存した画像の改変を拒否する。 ・ 全てのコピーし保存した画像の削除を拒否する。

【関連するTSFI】

・ 操作パネル：コピー、かんたんコピー、ジョブ表示およびログ表示

Table 27 D.USER.DOC のファクス送信アクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・ U.ADMIN(a)と U.NORMAL(a)と U.FAXOPERATOR をファクス送信文書のジョブ所有者として割付ける。 ・ 自身がスキャンした画像の閲覧を許可する。 ・ 自身が保存した画像の改変を許可する。 ・ 自身が保存した画像の削除を許可する。
U.ADMIN(a)	・ ファクス送信文書の投入を許可する。 ・ 他のユーザーのスキャン画像の閲覧を拒否する。 ・ 他のユーザーの保存した画像の改変を拒否する。 ・ 他のユーザーが保存した画像の削除を許可する。
U.NORMAL(a) U.FAXOPERATOR	・ ファクス送信文書の投入を許可する。 ・ 他のユーザーがスキャンした画像の閲覧を拒否する。 ・ 他のユーザーが保存した画像の改変を拒否する。 ・ 他のユーザーが保存した画像の削除を拒否する。
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・ ファクス送信文書の投入を拒否する。 ・ 全てのスキャン画像の閲覧を拒否する。 ・ 全ての保存した画像の改変を拒否する。 ・ 全ての保存した画像の削除を拒否する。
未認証ユーザー	・ ファクス送信文書の投入を拒否する。 ・ 全てのスキャン画像の閲覧を拒否する。 ・ 全ての保存した画像の改変を拒否する。 ・ 全ての保存した画像の削除を拒否する。

【関連する TSFI】

・ 操作パネル：ファクス送信、ジョブ表示およびログ表示

Table 28 D.USER.DOC ファクス受信アクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.ADMIN(a)と U.FAXOPERATOR をファクス受信文書のジョブ所有者として割付ける。 ・全てのファクス受信文書の閲覧および印刷を許可する。 ・全てのファクス受信文書の改変を拒否する。 ・全てのファクス受信文書の削除を許可する。
U.ADMIN(a) U.FAXOPERATOR	・全てのファクス受信はユーザーの操作によらず受信を許可する。 ・全てのファクス受信文書の閲覧および印刷を許可する。 ・全てのファクス受信文書の改変を拒否する。 ・全てのファクス受信文書の削除を許可する。
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・全てのファクス受信はユーザーの操作によらず受信を許可する。 ・全てのファクス受信画像の閲覧および印刷を拒否する。 ・全てのファクス受信画像の改変を拒否する。 ・全てのファクス受信画像の削除を拒否する。
未認証ユーザー	・全てのファクス受信はユーザーの操作によらず受信を許可する。 ・全てのファクス受信画像の閲覧および印刷を拒否する。 ・全てのファクス受信画像の改変を拒否する。 ・全てのファクス受信画像の削除を拒否する。
なし	・全てのファクス受信文書はユーザーの操作によらず TOE の外部から受信される。

【関連するTSFI】

- 操作パネル：プリント
- その他：PSTN ファクスインタフェース

Table 29 D.USER.JOB のプリントアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.ADMIN(a)と U.NORMAL(a)は自身がプリント実行したジョブのジョブ所有者として割付けられる。
U.ADMIN(a)	・プリントジョブの作成を許可する。 ・全てのプリントジョブの閲覧を許可する。 ・全てのプリントジョブの改変を拒否する。 ・全てのプリントジョブの取消しを許可する。
U.NORMAL(a)	・プリントジョブの作成を許可する。 ・全てのプリントジョブの閲覧を許可する。 ・全てのプリントジョブの改変を拒否する。 ・自身のプリントジョブの取消しは許可するが、他のユーザーのプリントジョブの取消しは拒否する。

ユーザー	アクセス制御規則
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・ プリントジョブの作成を拒否する。 ・ 全てのプリントジョブの閲覧を許可する。 ・ 全てのプリントジョブの改変を拒否する。 ・ 全てのプリントジョブの取消しを拒否する。
未認証ユーザー	・ 識別された U.ADMIN(a)、U.NORMAL(a)によるプリントジョブの作成は許可する。 ・ プリントジョブの作成を許可する。 ・ 全てのプリントジョブの閲覧を拒否する。 ・ 全てのプリントジョブの改変を拒否する。 ・ 全てのプリントジョブの取消しを拒否する。

【関連するTSFI】

- 操作パネル：プリント、ジョブ表示およびログ表示
- TopAccess：ジョブステータス
- プリンタードライバー：プリント要求に対するインタフェース

Table 30 D.USER.JOB のスキャンアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・ U.ADMIN(a)と U.NORMAL(a)は自身がスキャン実行したジョブのジョブ所有者として割付けられる。
U.ADMIN(a)	・ スキャンジョブの作成を許可する。 ・ 全てのスキャンジョブの閲覧を許可する。 ・ 全てのスキャンジョブの改変を拒否する。 ・ 全てのスキャンジョブの取消しを許可する。
U.NORMAL(a)	・ スキャンジョブの作成を許可する。 ・ 全てのスキャンジョブの閲覧を許可する。 ・ 全てのスキャンジョブの改変を拒否する。 ・ 自身のスキャンジョブの取消しは許可するが、他のユーザーのスキャンジョブの取消しは拒否する。
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR U.FAXOPERATOR	・ スキャンジョブの作成を拒否する。 ・ 全てのスキャンジョブの閲覧を許可する。 ・ 全てのスキャンジョブの改変を拒否する。 ・ 全てのスキャンジョブの取消しを拒否する。
未認証ユーザー	・ スキャンジョブの作成を拒否する。 ・ 全てのスキャンジョブの閲覧を拒否する。 ・ 全てのスキャンジョブの改変を拒否する。 ・ 全てのスキャンジョブの取消しを拒否する。

【関連するTSFI】

- 操作パネル：スキャン、かんたんスキャン、ジョブ表示およびログ表示
- TopAccess：ジョブステータス

Table 31 D.USER.JOB のコピーアクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.ADMIN(a)と U.NORMAL(a)を自身が実行したコピージョブのジョブ所有者として割付ける。
U.ADMIN(a)	・コピージョブの作成を許可する。 ・全てのコピージョブの閲覧を許可する。 ・全てのコピージョブの改変を拒否する。 ・全てのコピージョブの取消しを許可する。
U.NORMAL(a)	・コピージョブの作成を許可する。 ・全てのコピージョブの閲覧を許可する。 ・全てのコピージョブの改変を拒否する。 ・自身のコピージョブの取消しは許可するが、他のユーザーのコピージョブの取消しは拒否する。
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・コピージョブの作成を拒否する。 ・全てのコピージョブの閲覧を許可する。 ・全てのコピージョブの改変を拒否する。 ・全てのコピージョブの取消しを拒否する。
未認証ユーザー	・コピージョブの作成を拒否する。 ・全てのコピージョブの閲覧を拒否する。 ・全てのコピージョブの改変を拒否する。 ・全てのコピージョブの取消しを拒否する。

【関連するTSFI】

- 操作パネル：コピー、かんたんコピー、ジョブ表示およびログ表示
- TopAccess：ジョブステータス

Table 32 D.USER.JOB のファクス送信アクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・U.ADMIN(a)と U.NORMAL(a)と U.FAXOPERATOR を自身が実行したファクス送信ジョブのジョブ所有者として割付ける。
U.ADMIN(a)	・ファクス送信ジョブの作成を許可する。 ・全てのファクス送信ジョブの閲覧を許可する。 ・全てのファクス送信ジョブの改変を拒否する。 ・全てのファクス送信ジョブの取消しを許可する。
U.NORMAL(a)	・ファクス送信ジョブの作成を許可する。 ・全てのファクス送信ジョブの閲覧を許可する。 ・全てのファクス送信ジョブの改変を拒否する。 ・自身のファクス送信ジョブの取消しは許可するが、他のユーザーのファクス送信ジョブの取消しは拒否する。
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・ファクス送信ジョブの作成を拒否する。 ・全てのファクス送信ジョブの閲覧を許可する。 ・全てのファクス送信ジョブの改変を拒否する。 ・全てのファクス送信ジョブの取消しを拒否する。

ユーザー	アクセス制御規則
U.FAXOPERATOR	・ ファクス送信ジョブの作成を許可する。 ・ 全てのファクス送信ジョブの閲覧は許可する。 ・ 全てのファクス送信ジョブの改変を拒否する。 ・ 自身のファクス送信ジョブの取消しは許可するが、他のユーザーのファクス送信ジョブの取消しは拒否する。
未認証ユーザー	・ ファクス送信ジョブの作成を拒否する。 ・ 全てのファクス送信ジョブの閲覧を拒否する。 ・ 全てのファクス送信ジョブの改変を拒否する。 ・ 全てのファクス送信ジョブの取消しを拒否する。

【関連するTSFI】

- 操作パネル：ファクス送信、ジョブ表示およびログ表示
- TopAccess：ジョブステータス

Table 33 D.USER.JOB のファクス受信アクセス制御

ユーザー	アクセス制御規則
ジョブ所有者	・ U.ADMIN(a)と U.FAXOPERATOR をファクス受信ジョブのジョブ所有者として割付ける。
U.ADMIN(a) U.FAXOPERATOR	・ ユーザーの操作によらず全てのファクス受信ジョブの作成を許可する。 ・ 全てのファクス受信ジョブの閲覧を許可する。 ・ 全てのファクス受信ジョブの改変を拒否する。 ・ 全てのファクス受信ジョブの取消しを拒否する。
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・ ユーザーの操作によらず全てのファクス受信ジョブの作成を許可する。 ・ 全てのファクス受信ジョブの閲覧を拒否する。 ・ 全てのファクス受信ジョブの改変を拒否する。 ・ 全てのファクス受信ジョブの取消しを拒否する。
未認証ユーザー	・ ユーザーの操作によらず全てのファクス受信ジョブの作成を許可する。 ・ 全てのファクス受信ジョブの閲覧を拒否する。 ・ 全てのファクス受信ジョブの改変を拒否する。 ・ 全てのファクス受信ジョブの取消しを拒否する。

【関連するTSFI】

- 操作パネル：ジョブ表示およびログ表示
- TopAccess：ジョブステータス
- その他：PSTN ファクスインタフェース

7.8. PSTNファクス-ネットワーク間の分離

以下に条件付き必須B.2要件に関する要約仕様を記述する。

FDP_FXS_EXT.1

ファクスモデムの機能は、ファクス送信およびファクス受信のみである。
TOE のファクスインタフェースは、外部ファクス機とファクス文書データの送受信のみに使用され、その他の目的でファクスインタフェースを使用する事はない。
TOE のファクスインタフェースは、送受信プロトコルとして ITU-T 準拠 G3 のみサポートする。そのため、TOE と PSTN との通信は、ファクスプロトコルを使った送受信のみ受付けるが、フェーズ B のネゴシエーションが成立しない通信は、それ以降のフェーズに移行せず通信エラーになるため、TOE は通信回線を切断する。
これにより、PSTN と LAN 間のブリッジ接続を禁止している。

【関連するTSFI】
- 操作パネル：ファクス送信
- その他：PSTN ファクスインタフェース

7.9. 識別と認証

以下にクラスFIAの要件に関する要約仕様を記述する。

FIA_AFL.1

- TOE は、操作パネルおよび TopAccess からユーザーがログインする際に、最後に成功した認証またはアカウントロック解除後のログインから数えた認証失敗回数が、U.ADMIN(a)によって設定された回数（1～30）に達した時、該当のユーザーID を所定の時間ロックアウトする。
- ロックアウト状態にあるユーザーのロックアウトを解除する機能を U.ADMIN(a)と U.ACCOUNTMANAGER に提供する。

【関連するTSFI】
- 操作パネル：ログイン
- TopAccess：ログイン、管理者設定

FIA_ATD.1

- TOE は、セキュリティ属性としてユーザーID と役割をユーザーに関連付け登録し維持する。

【関連するTSFI】
- TopAccess：ユーザー管理

FIA_PMG_EXT.1

TOE は、ユーザーパスワードの登録、変更の時にユーザーパスワードを検査する機能を提供する。パスワードとして許容される文字タイプは、アルファベットの大文字、小文字、数字、句読点（+ , - . / : ; = ? \ _ ` { | } ~ スペース）、特殊文字 (! @ # $ ^ * ( ))、および欧州特殊文字（ドイツ語のウムラウトとフランス語のセディラを持つ文字：詳細は Table 16 参照）である。また、U.ADMIN(a)によってパスワード最小桁数を 15 文字以上に設定する事が可能である。

【関連するTSFI】
- 操作パネル：ホーム画面、ログイン、管理者設定
- TopAccess：ログイン、アカウント

FIA_UAU.7

TOEは、操作パネルからユーザーがパスワードを入力すると、操作画面上の入力文字の代わりにダミー文字として“●”を表示し、入力した文字は表示しない。また同様に、Webブラウザからユーザーがパスワードを入力する場合も、入力した文字の代わりに代替文字を表示する。ただし、代替文字は使用するブラウザに依存した文字を表示する。

【関連するTSFI】
- 操作パネル：ログイン
- TopAccess：ログイン

FIA_UAU.1/FIA_UID.1

TOEは、ユーザーを識別・認証することを要求する。ユーザーアカウントのデータベースに対してユーザーの識別と認証が実行され、ユーザーIDとパスワードが内部的に保存されているクレデンシャルデータと一致しない場合ログインは拒否され、ユーザーに再度入力プロンプトが表示される。
クライアントPCからプリンタードライバーを介して実行されるプリントの場合は、プリントジョブにはジョブオーナーのユーザーIDが紐付けされており、TOEはプリントジョブを受信した時にそのユーザーIDを識別しプリントホールドキューにプリントジョブを格納する。
また、TOEは、ファクス受信する際には、ファクス受信ジョブの識別と認証を行わずにファクス受信データをTOEに保存する。

【関連するTSFI】
- 操作パネル：ログイン
- TopAccess：ログイン
- プリントドライバー：プリント要求に対するインタフェース
- その他：PSTN ファクスインタフェース

FIA_USB.1

- TOE は、識別と認証に成功したユーザーとユーザーID、役割を関連付ける。

【関連するTSFI】
- 操作パネル：ログイン
- TopAccess：ログイン

7.10. セキュリティ管理

以下にクラス FMT の要件に関する要約仕様を記述する。

FMT_MOF.1

TOEは、U.ADMIN(a)のみに、セキュアチャネルの機能設定の有効/無効設定を切り替える機能を提供する。

【関連するTSFI】
- 操作パネル：管理者設定
- TopAccess：管理者設定

FMT_MSA.1

TOEは、U.ADMIN(a)に以下の機能を提供する。
- 全ユーザーID の作成、変更、問合せ、削除、エクスポート
- 全役割の作成、変更、問合せ、削除、エクスポート

TOEは、U.ACCOUNTMANAGERに以下の機能を提供する。
- 全ユーザーID の問合せ、エクスポート
- U.ADMIN(a)を除くユーザーID の作成、変更、削除
- U.ADMIN(a)を除く役割の作成、変更、削除

TOEは、U.NORMAL、U.ADDRESSBOOKOPERATORに以下の機能を提供する。
- 自身のユーザーID の問合せ
- 自身の役割の問合せ

【関連するTSFI】
- TopAccess：ユーザー管理

FMT_MSA.3

TOEは、D.USER.DOCおよびD.USER.JOBが新規に作成される時、そのセキュリティ属性の初期値としてそれを作成したユーザーのユーザーIDを割当てる。
TOEは、D.USER.DOCおよびD.USER.JOBが生成される際、そのセキュリティ属性であるユーザーIDの初期値を上書きする機能は提供しない。

【関連するTSFI】
- 操作パネル：コピー、かんたんコピー、スキャン、かんたんスキャン、ファクス送信
- TopAccess：ユーザー管理
- プリンタードライバー：プリント要求に対するインタフェース

FMT_MTD.1

TOEは、U.ADMIN(a)に以下の操作機能を提供する。
- U.ADMIN(a)のユーザーパスワードの変更とエクスポート
- U.ACCOUNTMANAGER のユーザーパスワードの変更とエクスポート
- U.ADDRESSBOOKOPERATOR のユーザーパスワードの変更とエクスポート
- U.NORMAL のユーザーパスワードの変更とエクスポート
- ログインパスワードの入力リトライ回数の変更
- ロックアウト時間の変更
- ロックアウトされた全アカウントのステータスクリア
- オートログアウト時間の変更
- 日時情報の変更
- 最小パスワード長の変更
- アドレス帳の作成、変更、削除
- SYSLOG サーバーの設定の変更
- FTP サーバーの設定の変更
- ソフトウェアのバージョン確認とアップデート

TOEは、以下の操作機能をU.ACCOUNTMANAGERに提供する。
- U.ACCOUNTMANAGER のユーザーパスワードの変更とエクスポート
- U.ADDRESSBOOKOPERATOR のユーザーパスワードの変更とエクスポート
- U.NORMAL のユーザーパスワードの変更とエクスポート
- U.ADMIN(a)以外のロックアウトされたアカウントのステータスクリア

TOEは、以下の操作機能をU.NORMALに提供する。
- 自身のユーザーパスワードの変更

TOEは、以下の操作機能にU.ADDRESSBOOKOPERATORを提供する。
- 自身のユーザーパスワードの変更

【関連するTSFI】
- 操作パネル：ログイン、ホーム画面、ジョブ表示およびログ表示、管理者設定
- TopAccess:ログイン、アカウント、ユーザー管理、管理設定

FMT_SMF.1

TOEは、以下のセキュリティ管理機能を提供することにより、FMT_SMF.1を実現する。

タイムスタンプ設定の管理：
- U.ADMIN(a)による日時情報の変更操作。

ユーザーIDの管理：
- U.ADMIN(a)または U.ACCOUNTMANAGER によるユーザーID の変更操作。

ユーザーパスワードの管理：
- U.ADMIN(a)による U.ACCOUNTMANAGER、U.NORMAL、U.ADMIN(a)および U.ADDRESSBOOKOPERATOR のユーザーパスワードの変更およびエクスポート操作。
- U.ACCOUNTMANAGER による U.ACCOUNTMANAGER、U.NORMAL、および U.ADDRESSBOOKOPERATOR のユーザーパスワードの変更およびエクスポート操作。
- U.NORMAL による自己のユーザーパスワードの変更操作。
- U.ADDRESSBOOKOPERATOR によるユーザーパスワードの変更操作。

ユーザー認証失敗処理の管理：
- U.ADMIN(a)によるログインパスワードの入力回数の変更操作。
- U.ADMIN(a)によるロックアウト時間の変更操作。
- U.ADMIN(a)または U.ACCOUNTMANAGER によるロックアウトされたアカウントステータスのクリアー操作。

最小パスワード長の管理：
- U.ADMIN(a)による最小パスワード長の変更操作。

対話セッションが終了した後のユーザーの非アクティブの既定時間の指定：
- U.ADMIN(a)による自動ログアウト時間の変更操作。

セキュアチャネル設定：
・ U.ADMIN(a)による TLS 通信の有効/無効の変更操作。

アドレス帳の管理：
・ U.ADMIN(a)によるアドレス帳の変更操作。

SYSLOGサーバー：
・ U.ADMIN(a)による SYSLOG サーバー設定の変更操作。

FTPサーバー：
・ U.ADMIN(a)による FTP サーバー設定の変更操作。

ソフトウェア：
・ U.ADMIN(a)によるソフトウェアのバージョン確認とアップデート。

【関連するTSFI】
・ 操作パネル：ログイン、ホーム画面、ジョブ表示およびログ表示、管理者設定
・ TopAccess：ログイン、アカウント、ユーザー管理、管理者設定

FMT_SMR.1

TOEは、U.ADMIN(a)、U.ACCOUNTMANAGER、U.NORMALおよびU.ADDRESSBOOKOPERATORに関連する役割を保持し、ユーザーを登録する時にその役割を適切なユーザーに関連付ける。

【関連するTSFI】
・ 操作パネル：ログイン
・ TopAccess：ログイン、ユーザー管理

7.11. TSFの保護

以下にクラス FPT の要件に関する要約仕様を記述する。

FPT_SKP_EXT.1

・ TSF は、FCS_CKM.1(a)の TSS に記述のサーバー秘密鍵を揮発性メモリに平文で保存するが全てのユーザーにアクセスする機能は提供してない。また、これらのサーバー秘密鍵は電源断で消去される。
・ TSF は、FCS_CKM.1(a)の TSS に記述のサーバー秘密鍵を現地交換可能な不揮発性ストレージである SSD に保存するときには、FDP_DSK_EXT.1 に従った FCS_COP.1(d)により 128bit の DEK を用いた AES-CBC で暗号化して暗号文状態で保存する。復号に必要な DEK に対しては、全てのユーザーにアクセスする機能を提供していない。また、これらの DEK は電源断で消去される
・ TSF は、FCS_KYC_EXT.1 の TSS に記述の鍵および鍵材料（KEK 導出鍵、鍵材料暗号化鍵、KEK 導出用コンテキスト、KEK、DEK、サブマスク、LUKS 鍵）を揮発性メモリに平文で保存するが、全てのユーザーにアクセスする機能を提供していない。また、これらの CSP は電源断で消去される。

・ TSF は、スワッピングパーティション用 DEK を揮発性メモリに平文で保存するが、全てのユーザーにアクセスする機能を提供していない。また、これらの CSP は電源断で消去される。
・ TSF は、FCS_CKM.1(b)の TSS に記述の KEK 導出鍵と鍵材料暗号化鍵を FROM に平文で保存するが、全てのユーザーにアクセスする機能は提供していない。
・ TSF は、FCS_CKM.1(b)の TSS に記述の TLS 通信用のセッション鍵および HMAC の鍵を揮発性メモリに平文で保存するが、全てのユーザーにアクセスする機能を提供してない。また、これらの共通鍵は、電源断で消去される。

これによりFPT_SKP_EXT.1を実現している。

【関連するTSFI】
なし

FPT_STM.1

TOEは、監査ログを記録するためにTOEに内蔵されるリアルクロックICが提供する「年」、「月」、「日」、「時」、「分」、「秒」をタイムスタンプとして使用することにより、FPT_STM.1を実現している。

【関連するTSFI】
FAU_GEN.1、FAU_GEN. 2 の関連 TSFI に準ずる

FPT_TST_EXT.1

TOE は、電源起動時に以下のセルフテストを実行する。

・ TSF イメージの検証
TSF は MFP を制御するソフトウェア（SYSTEM FIRMWARE、SYSTEM SOFTWARE）で実現されており、TSF の正当性を検証するためにシステムファームウェアとシステムソフトウェアのそれぞれのイメージファイルに対して、公開鍵方式に RSA、ハッシュ関数に SHA-256 を使用した電子署名方式による検証を実施することにより TSF の正常動作を保証している。また、プリンターユニット部のファームウェア（ENGINE FIRMWARE）、スキャナーユニット部のファームウェア（SCANNER FIRMWARE）、ファクスユニット部のファームウェア（FAX1 FIRMWARE）は、各々16bit のチェックサムを計算し、ファームウェアの実装の故障を検知するためにイメージファイルの自己検証を行っている。イメージファイルの検証で異常が検出されたイメージファイルは起動されず、TOE のパネルのメッセージ表示エリアにはサービスマンコールが表示され、TOE は起動を中止しユーザーは TOE を使用できなくなる

・ エントロピー源のヘルステスト
MFP を制御するソフトウェア（SYSTEM SOFTWARE）は電源起動時に rngd のプロセスを開始した後、Linux PRNG の/dev/random から 4096 バイトを取得して NIST SP 800-90B にならった自己検証を行う。このとき Linux PRNG にエントロピーを供給するため、rngd はタイトループのリトライで RDRAND 命令を複数回呼び出す。この呼び出しで 10 回の連続エラー(CF=0)を検知すると、異常検出のログを出力して rngd プロセスを終了させる。プロセス監視タスクの常時監視が直ちに rngd のプロセス終了を検知すると、パネルのメッセージ表示エリアにはサービスマンコールが表示され、TOE は運用を停止する。このヘルステストの目的は乱数生成器のエントロピー源にかかわるソフトウェアの予期しない故障を検知するためである。

また、CPU の RDRAND 命令が呼び出されると、エントロピー源の中にあるノイズ源が故障していないことを保証するために、SoC 内蔵の Online Health Test (OHT)による継続的なヘルステストが正常に実施されていることを検証する Buit in Self Test（BIST）が自動で行われる。この BIST で異常を検知すると RDRAND 命令は常に CF=0 でエラーを返し、MFP を制御するソフトウェアはノイズ源の故障を検知する。上記のヘルステストで異常が検出された場合、コントロールパネルにエラーコードが表示され、TOE は動作を中止しユーザーは TOE を使用できなくなる。

・ DRBG のヘルステスト
DRBG の FCS_RBG_EXT.1(a)と FCS_RBG_EXT.1(b)はそれぞれ NIST SP 800-90A に準拠しており、TOE 起動後それぞれの TSF を最初に呼び出すときに NIST SP 800-90A rev.1 の 11.3 節のヘルステストが自動実行される。上記のヘルステストで異常が検出された場合、コントロールパネルにエラーコードが表示され、TOE は動作を中止しユーザーは TOE を使用できなくなる。

【関連するTSFI】
- 操作パネル：電源キー
- その他：メインスイッチ

FPT_TUD_EXT.1

TSFは、U.ADMIN(a)に、TOEの現在のソフトウェアバージョン情報を確認するためのインタフェースとして操作パネルのホーム画面の管理者設定画面を提供し、ソフトウェアをアップデートするインタフェースとして操作パネルの管理者設定画面とTopAccessの管理者設定画面を提供する。
また、アップデート開始前にアップデートするソフトウェアの真正性を検証するデジタル署名検証の機能を提供する。その検証方法は、アップデートする各ファームウェア（SYSTEM SOTWAER、SYSTEM FIRMWARE、ENGINE FIRMWARE、SCNNER FIRMARE、FAX1 FIRMWARE）ファイルに付随して提供されるデジタル署名から、FCS_COP.1(b)に従ったRSASSA-PSSにより復号したハッシュ値と、アップデートしようとする各ファームウェアからFCS_COP.1(c)に従ってSHA-256で導出したハッシュ値を比較し、双方が一致することを確認する事で正しいファームウェアかどうかを検証する。

【関連するTSFI】
- 操作パネル：ホーム画面、管理者設定
- TopAccess：管理者設定

7.12. TOEアクセス

以下にクラス FTA の要件に関する要約仕様を記述する。

FTA_SSL.3

TOEは、ユーザーが一定時間操作パネルを操作しないと、強制的にログアウトします。 設定時間は15～150秒の間で設定できる。 また、Webブラウザを使用してTOEにアクセスし、一定時間操作が無いと、セッションを強制的に終了しログアウトする。 設定時間は5～999分の間で設定できる。
TOEは、プリンタードライバーからのプリントジョブの投入には対話セッションの生成は行わず、プリントの要求処理後ただちにセッションを終了する。

【関連するTSFI】
- 操作パネル：ログイン

・ TopAccess：ログイン

7.13. 高信頼パス/チャネル

以下にクラス FTP の要件に関する要約仕様を記述する。

FTP_ITC.1

TOEは、各サーバー間の通信中のデータ保護のためTLS1.2を使用して通信を開始する。TOEが高信頼チャネルを介してメールサーバー、SYSLOGサーバー、FTPサーバーへのアクセスする場合には、TLS通信の開始を各サーバーへ要求する。

【関連するTSFI】

・ 操作パネル：電源キー、ログイン、ホーム画面、コピー、かんたんコピー、スキャン、かんたんスキャン、プリント、ファクス送信、ジョブ表示およびログ表示、管理者設定、
・ TopAccess：ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
・ プリンタードライバー：プリント要求に対するインタフェース
・ その他：メインスイッチ、PSTN ファクスインタフェース

FTP_TRP.1(a)、FTP_TRP.1(b)

TSFは、TOEとリモート管理者およびリモート利用者間の通信経路において、通信データの漏洩からの保護と通信データの改変の検知する高信頼パスを提供するために、以下の機能を提供する。

WEBページとの通信：

・ クライアントPCからTOEのWEBページへの高信頼パスを確立するために、HTTPSネットワークプロトコルで接続する。
・ リモート管理者およびリモート利用者がクライアントPCからWEBブラウザを使って、TOEのWEBページに接続する場合は、HTTPSプロトコルを用いた接続に限り通信が開始される。
・ クライアントPCからの最初の管理者認証とユーザー認証およびすべてのリモート利用者アクションは、HTTPSプロトコルを用いた接続に限り実行される。

クライアントPCからのプリント：

・ クライアントPCからプリンタードライバーを使ったプリントの場合、TOEへの接続で高信頼パスを確立するためには、TLS通信プロトコルで接続する。

【関連するTSFI】

・ TopAccess： ログイン、ジョブステータス、アカウント、ユーザー管理、管理者設定
プリンタードライバー：プリント要求に対するインタフェース

本章に関連する TSFI について、以下の Table 34 に示す。

Table 34 TSFI の定義

TSFI名		詳細
操作パネル		
	電源キー	メインスイッチによりMFPに電源投入後、MFPを起動したり、MFPをシャットダウンしたりするためのインタフェース。
	ログイン	操作パネルからアクセスするユーザーを識別認証するためのインタフェース。
	ホーム画面	ユーザーパスワードの変更操作、およびTOEのバージョンを確認するためのインタフェース。
	コピー	文書を複写するためのインタフェース。
	かんたんコピー	文書を複写するためのインタフェース。
	スキャン	原稿を画像データとしてスキャンし、スキャンした画像データをプレビュー、ページ削除・差し替え・挿入したり、FTPサーバーのフォルダに保存したり、指定のe-mailアドレスへ送信したりするためのインタフェース。
	かんたんスキャン	原稿を画像データとしてスキャンし、スキャンした画像データをプレビュー、ページ削除したり、また、スキャンしたデータを添付ファイルとして指定のe-mailアドレスへ送信したりするためのインタフェース。
	プリント	クライアントPCから送られMFP内のホールドキューに格納された原稿や、ファクス受信データを印刷するためのインタフェース。
	ファクス送信	原稿を画像データとしてスキャンし、スキャンした画像データをプレビュー、ページ削除・差し替え・挿入およびファクス送信するためのインタフェース。
	ジョブ表示およびログ表示	印刷、スキャンの実行状況やアドレス帳のデータを操作するためのインタフェース。
	管理者設定	管理者のパスワードの変更、アドレス帳のデータの操作等の管理者がセキュリティに関する操作を行うためのインタフェース。
TopAccess		
	ログイン	クライアントPCからアクセスするユーザーを識別認証するためのインタフェース。
	ジョブステータス	実行中のプリントジョブ、スキャンジョブを操作するためのインタフェース。
	アカウント	自身のパスワード変更や設定されている役割情報を表示するためのインタフェース。
	ユーザー管理	ユーザー情報の登録等のユーザーに関する管理を行うためのインタフェース。
	管理者設定	オートクリア設定等のMFPの設定、パスワードポリシーの設定、アドレス帳のインポート等のMFPの管理を行うためのインタフェース。
プリンタードライバー		
	プリント要求に対すインタフェース	クライアントPCからプリントデータをMFPにホールド(保存)するためのインタフェースである。
その他		
	PSTNファクスインタフェース	外部ファクス機からのファクスデータを受信するインタフェース。
	メインスイッチ	MFPに電源を投入して、ログの取得を開始し、TOEを使用できる状態にするためのインタフェース。

Apendix

Appendix では、略語の定義と参考文献を示す。

Table 35 略語の定義

略語	定義
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
EE	Encryption Engine
FDE	Full Drive Encryption
FIPS PUB	Federal Information Processing Standards Publication
FRAM	Ferroelectric Random Access Memory
FROM	Flash ROM
FTP	File Transfer Protocol
GCM	Galois Counter Mode
HCD	Hardcopy Device
SSD	Solid State Drive
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol over SSL
IPP	Internet Printing Protocol
IPPS	IPP over SSL
IT	Information Technology
ISO/IEC	International Organization for Standardization / International

略語	定義
	Electrotechnical Commission
LAN	Local Area Network
LCD	Liquid crystal display
LED	light emitting diode
MFP	Multifunction Product
NCU	Network control unit
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
PC	Personal Computer
PP	Protection Profile
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
Soc	System-on-a-chip
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

- 参考文献
  - [Rambus 2012]
    - Analysis of Intel's Ivy Bridge Digital Random Number Generator, Cryptography Research a division of Rambus, 2012.
    - Available: https://www.rambus.com/intel-ivy-bridge-random-number-generator/.