Xerox VersaLink B405DN
セキュリティターゲット

Version 1.09

January 2023

― 更新履歴 ―

No.	更新日	バージョン	更新内容
1	2022 年 5 月 26 日	V 1.00	初版
2	2022 年 6 月 14 日	V 1.01	誤記修正
3	2022 年 8 月 10 日	V 1.02	誤記修正
4	2022 年 9 月 26 日	V 1.03	誤記修正
5	2022 年 10 月 5 日	V 1.04	誤記修正
6	2022 年 10 月 18 日	V 1.05	誤記修正
7	2022 年 10 月 19 日	V 1.06	誤記修正
8	2022 年 10 月 20 日	V 1.07	誤記修正
9	2022 年 12 月 2 日	V 1.08	誤記修正
10	2023 年 1 月 19 日	V 1.09	誤記修正

－ 目次 －

1. ST 概説（ST Introduction）..... 1

1.1. ST 参照（ST Reference）..... 1

1.2. TOE 参照（TOE Reference）..... 1

1.3. TOE 概要（TOE Overview）..... 2

1.3.1. TOE の種別（TOE Type）..... 2

1.3.2. TOE の使用法と主要セキュリティ機能（Usage and Major Security Features of TOE）..... 2

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成（Required Non-TOE Hardware and Software）..... 3

1.4. TOE 記述（TOE Description）..... 5

1.4.1. TOE 関連の利用者役割（User Assumptions）..... 5

1.4.2. TOE の論理的範囲（Logical Boundary of the TOE）..... 5

1.4.3. TOE の物理的範囲（Physical Boundary of the TOE）..... 8

2. 適合主張（Conformance Claim）..... 10

2.1. CC 適合主張（CC Conformance Claim）..... 10

2.2. PP 主張、パッケージ主張（PP claim, Package Claim）..... 10

2.2.1. PP 主張（PP Claim）..... 10

2.2.2. パッケージ主張（Package Claim）..... 10

2.2.3. 適合根拠（Conformance Rational）..... 10

3. セキュリティ課題定義（Security Problem Definition）..... 11

3.1. 脅威（Threats）..... 11

3.1.1. TOE 資産（Assets Protected by TOE）..... 11

3.1.2. 脅威（Threats）..... 11

3.2. 組織のセキュリティ方針（Organizational Security Policies）..... 12

3.3. 前提条件（Assumptions）..... 12

4. セキュリティ対策方針（Security Objectives）..... 14

5. 拡張コンポーネント定義（Extended Components Definition）..... 15

5.1. 拡張機能要件定義..... 15

5.1.1. Class FAU: Security Audit 15
5.1.2. Class FCS: Cryptographic Support 16
5.1.3. Class FDP: User Data Protection 22
5.1.4. Class FIA: Identification and Authentication 24
5.1.5. Class FPT: Protection of the TSF 25
6. セキュリティ要件 (Security Requirements) 29
6.1. 表記法 29
6.2. セキュリティ機能要件 (Security Functional Requirements) 29
6.2.1. Class FAU: Security Audit 29
6.2.2. Class FCS: Cryptographic Support 32
6.2.3. Class FDP: User Data Protection 41
6.2.4. Class FIA: Identification and Authentication 45
6.2.5. Class FMT: Security Management 48
6.2.6. Class FPT: Protection of the TSF 51
6.2.7. Class FTA: TOE Access 53
6.2.8. Class FTP: Trusted Paths/Channels 53
6.3. セキュリティ保証要件 (Security Assurance Requirements) 55
6.4. セキュリティ要件根拠 (Security Requirement Rationale) 56
6.4.1. 依存性の検証 (Dependencies of Security Functional Requirements) 56
6.4.2. セキュリティ保証要件根拠 (Security Assurance Requirements Rationale) 60
7. TOE 要約仕様 (TOE Summary Specification) 61
7.1. セキュリティ機能 (Security Functions) 61
7.1.1. 識別認証 63
7.1.2. セキュリティ監査 65
7.1.3. アクセス制御 68
7.1.4. セキュリティ管理 70
7.1.5. 高信頼な運用 72
7.1.6. データ暗号化 73
7.1.7. 高信頼通信 79
7.1.8. PSTN ファクス-ネットワーク間の分離 81
8. ST 略語・用語 (Acronyms And Terminology) 82
8.1. 略語 (Acronyms) 82
8.2. 用語 (Terminology) 83
9. 参照文献 87

― 図表目次 ―

図 1 TOE の想定する運用環境 2
図 2 TOE の論理的構成 6

Table 1 利用者役割 5
Table 2 TOE を構成する物理的コンポーネント(MFD 本体) 8
Table 3 TOE を構成する物理的コンポーネント 8
Table 4 Assets for User Data 11
Table 5 Assets for TSF Data 11
Table 6 Threats 11
Table 7 Organizational Security Policies 12
Table 8 Assumptions 13
Table 9 運用環境のセキュリティ対策方針 14
Table 10 Auditable Events 30
Table 11 D.USER.DOC Access Control SFP 42
Table 12 D.USER.JOB Access Control SFP 43
Table 13 List of Security Functions 48
Table 14 Security Attributes and Authorized Roles 49
Table 15 Management of TSF Data 50
Table 16 Security Management Functions 50
Table 17 セキュリティ保証要件 55
Table 18 セキュリティ機能要件コンポーネントの依存性 56
Table 19 TOE セキュリティ機能とセキュリティ機能要件の対応関係 61
Table 20 監査ログの詳細 66
Table 21 セキュリティ管理機能と操作可能な UI 71
Table 22 平文保存される鍵及び鍵材料の破棄方法 74

1. ST 概説 (ST Introduction)

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 (ST Reference)

本節では ST の識別情報を記述する。

タイトル:	Xerox VersaLink B405DN セキュリティターゲット
バージョン:	V 1.09
発行日:	2023 年 1 月 19 日
作成者:	富士フイルムビジネスイノベーション株式会社

1.2. TOE 参照 (TOE Reference)

本節では TOE の識別情報を記述する。

TOE 名:	Xerox VersaLink B405DN
TOE のバージョン:	Controller ROM Ver. 1.90.3

本 TOE は、以下の商品である。また、本 TOE には英語版のガイダンスが付随する。

商品	バージョン
Xerox VersaLink B405DN	Controller ROM Ver. 1.90.3

1.3. TOE 概要 (TOE Overview)

1.3.1. TOE の種別 (TOE Type)

本 TOE は、有線ローカルエリアネットワーク(LAN)へ接続され、コピー機能、スキャン機能、プリント機能、ファクス機能、をサポートする MFD である。

1.3.2. TOE の使用法と主要セキュリティ機能 (Usage and Major Security Features of TOE)

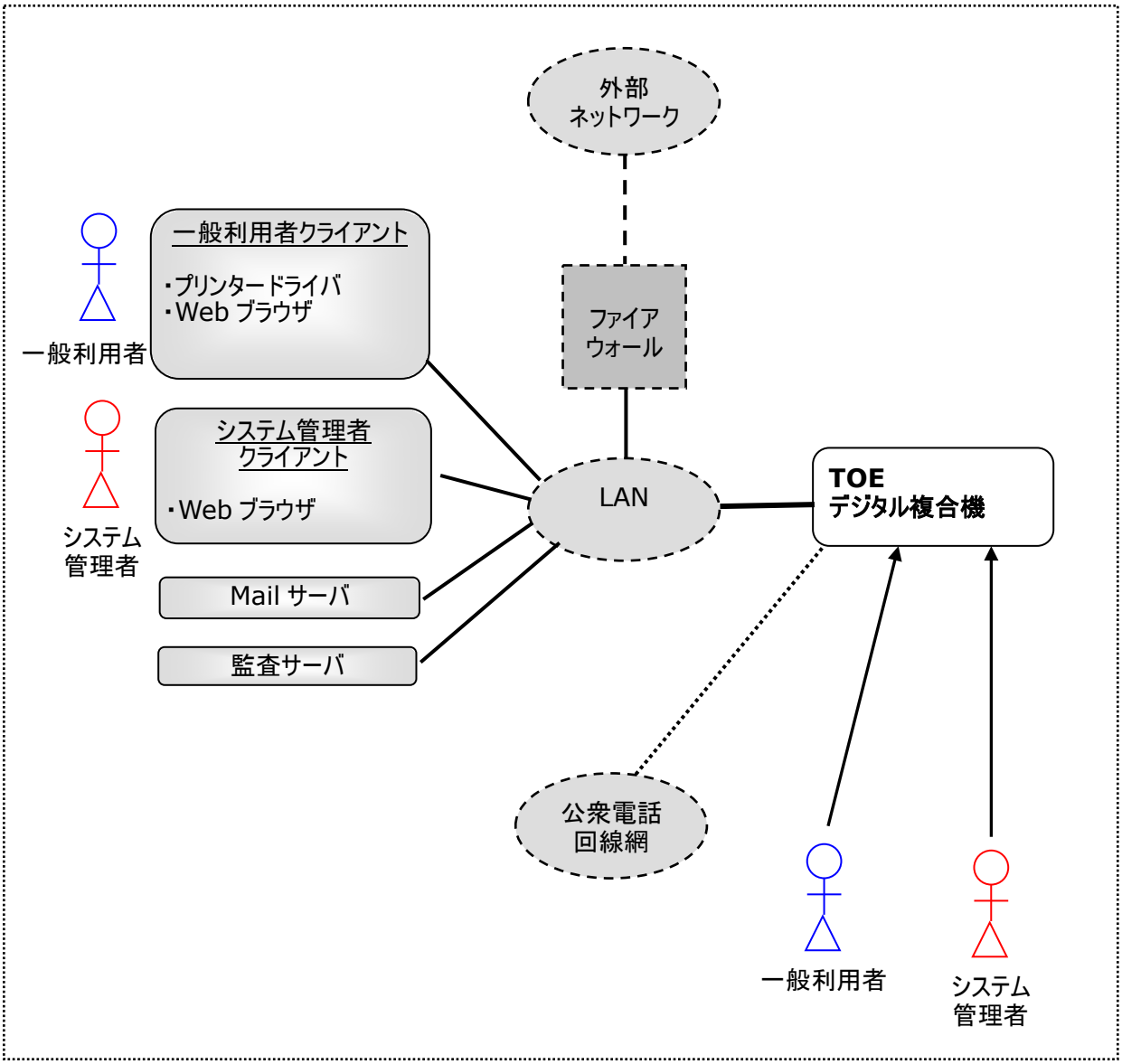


図 1 TOE の想定する運用環境

MFD は、ファイアウォールによって、外部ネットワークから分離された有線ローカルエリアネットワーク（LAN）へ接続された環境で使用される。
また、ファクスを送受信する場合は、公衆電話回線網に接続される。

利用者は、MFD の操作パネルや一般利用者クライアントやシステム管理者クライアントの Web ブラウザやプリンタードライバを介して、MFD の各種基本機能を利用する。
MFD は、利用者の扱う文書に対し、コピー、スキャン送信、プリント出力、ファクスでの送受信、などの機能を有する。これらの文書の改ざん、漏えいを防止するため、MFD は、利用者を識別認証する機能、権限に基づく文書データや機能に対するアクセス制御、MFD 内のストレージに保存・蓄積される設定情報や文書データの暗号化、LAN 上の通信データの保護、管理者に限定したセキュリティ設定機能、MFD の利用履歴を MFD 内部に保存する一方、その利用履歴を MFD 外部の監査サーバからモニタリングするセキュリティ監査機能、TSF 実行コードと TSF データの完全性保証、TSF 実行コードアップグレード時の実行コードの真正性保証、ファクス回線と LAN の分離機能を有する。
なお 本 TOE は ハードディスクを搭載せず eMMC で利用者のデータを取り扱うため、残存画像情報の上書き消去機能は評価対象のセキュリティ機能には含まれていない。
また、本 TOE を構成する製品は、外部認証オプションを追加インストールすることにより、認証方式として、本体認証と外部認証をサポートするが、本 TOE 設定では本体認証のみを使用する。

注）
・利用者が、MFD に個人的なストレージデバイス（ポータブルフラッシュメモリデバイス等）を接続するインタフェースは無効化される。

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成 (Required Non-TOE Hardware and Software)

図 1 に示す利用環境において TOE は MFD であり、下記の TOE 以外のハードウェアおよびソフトウェアが存在する。

(1) 一般利用者クライアント
ハードウェアは汎用の PC である。
プリンタクライアントとして利用する場合は、MFD に対して文書データのプリント要求を行うため、PC にはプリンタードライバをインストールする必要がある。
MFD の Web サーバ機能を利用する場合は、PC にインストールされている Web ブラウザを使用する。

(2) システム管理者クライアント
ハードウェアは汎用の PC である。
TOE に対して TOE 設定データの参照や変更、ファームウェアの更新を行うために、Web ブラウザが必要となる。

(3) Mail サーバ
スキャン文書をメールで送信するには、Mail サーバが必要となる。ハードウェア/OS は汎用の PC またはサーバであり、TLS で保護された SMTP プロトコルをサポートする Mail サービスをインストールする必要がある。

(4) 監査サーバ

MFD で発生した監査事象を収集するため、監査サーバが必要となる。ハードウェア/OS は汎用の PC またはサーバであり、MFD は監査サーバの要求に応じて、HTTPS プロトコルを用いて、TLS に対応している監査サーバに監査ログの送信を行う。

本 TOE の評価では、上記のハードウェアおよびソフトウェアとして、以下を使用する。
(1)、(2)の一般利用者クライアントとシステム管理者クライアントの OS は Windows 10 を、Web ブラウザとして Microsoft Edge を使用する。
(3)の Mail サーバは Cent OS 7.6 と、Postfix version 2.10.1 を使用する。
(4)の監査サーバは Windows 10 と、監査ログ取り出しの実行環境として PowerShell Version 5.1 を使用する。また、システム管理者がガイダンスに従って作成するログ取り出し用の PowerShell スクリプトを設置する必要がある。
(1)において、使用するプリンタードライバは Xerox Corporation が提供する該当機種用の以下ドライバーを使用する。
"PCL6 5.887.3.0"

1.4. TOE 記述 (TOE Description)

本章では、TOE の利用者役割、TOE の論理的範囲、および物理的範囲について記述する。

1.4.1. TOE 関連の利用者役割 (User Assumptions)

本 ST で、TOE に対して想定する利用者役割を Table 1 に記述する。

Table 1 利用者役割

名称	利用者データ種別	定義
U.NORMAL	一般利用者	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.ADMIN	管理者	識別され、認証された利用者で管理者役割を持つ利用者 (TOE の実装では、Key Operator と SA という役割があり、本 ST 上では U.ADMIN として総称される。)

1.4.2. TOE の論理的範囲 (Logical Boundary of the TOE)

図 2 に TOE の論理的構成を記述する。
論理的範囲として示された機能のうち、下線無しの機能は基本機能、下線ありの機能はセキュリティ機能を表す。

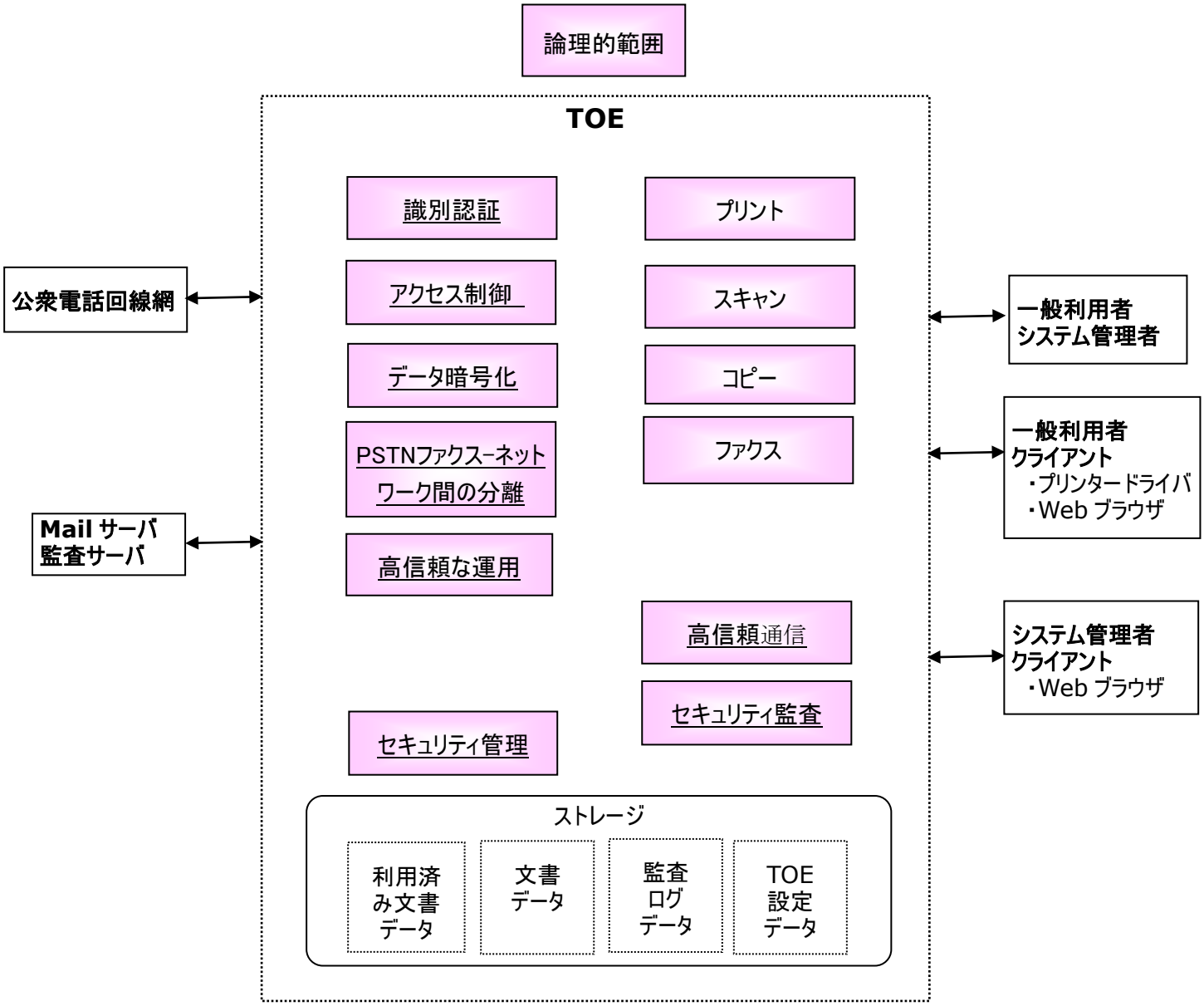


図 2 TOE の論理的構成

1.4.2.1. TOE が提供する基本機能 (Basic Functions)

(1) プリント: 一般利用者クライアントのプリンタードライバから送られた電子文書を受け取る。また、操作パネルからの指示に従い、受け取った電子文書をハードコピー形式へ変換する。

(2) スキャン: 操作パネルからの指示に従い、スキャナー上のハードコピー文書を読み込み、電子形式へ変換する。
本 TOE では、スキャン機能により変換された電子文書に対し、Mail サーバへ送る機能が存在する。

(3) コピー: 操作パネルからの指示に従い、スキャナー上のハードコピー文書を複製する。

(4) PSTN ファクス送信: 操作パネルからの指示に従い、スキャナー上の原稿を読み込み、標準 PSTN ファクスプロトコルを用いて PSTN 経由で PSTN ファクスの宛先へ送信する。

(5) PSTN ファクス受信： PSTN 経由で接続相手機から送られたファクシミリ文書データを受信し、ファクス受信ボックスへ格納する。また、管理者による操作パネルからの指示に基づき、保存されたファクシミリ文書データに対して、以下のような操作を可能とする。印刷：操作パネルからの指示により、ファクス受信ボックスに保存されたファクシミリ文書データをプリントする。削除： 操作パネルからの指示により、保存されたファクシミリ文書データを削除する。

1.4.2.2. TOE が提供するセキュリティ機能 (Security Functions)

1.4.2.1 の基本機能を支援するため、TOE は、以下のセキュリティ機能を提供する。

(1) 識別認証

利用者の識別認証、及び権限付与は、MFD の機能が、管理者によって権限付与された利用者のみにアクセス可能であることを保証する。利用者の識別と認証は、アクセス制御と管理者役割の根拠としても利用され、セキュリティ関連事象と MFD の使用を特定の利用者に関連付ける上での支援にもなる。識別と認証は、MFD によって実行される。

TOE は識別認証するために、操作パネル、利用者クライアントの Web ブラウザ、監査サーバの 3 種類があり、ID とパスワードの入力を促し、パスワード入力時にパスワードを隠すために隠し文字を表示するフィードバックの機能と、認証試行時、連続して認証失敗した場合、認証試行を受け付けなくなる機能を備えている。また、最小パスワード長を設定する機能、ログイン後に一定時間操作の無い場合に自動的にログインをクリアする機能を備えている。

本 TOE を構成する製品は、外部認証オプションを追加インストールすることにより、認証方式として、本体認証と外部認証をサポートするが、本 TOE 設定では本体認証のみを使用する。

(2) アクセス制御

アクセス制御は、文書や文書処理に関連する情報、セキュリティ関連データが、適切なアクセス権限を持つ利用者のみにアクセス可能であることを保証する。

(3) データ暗号化

データ暗号化は、TOE 内部に保存するデータや通信データに対して、攻撃者が不正なインタフェースからアクセスできないことを保証する。

- ポリシーにより、データ暗号化が現地-交換可能な不揮発性ストレージデバイス上の文書及び秘密のシステム情報を保護したり、このようなデバイスが MFD から除去されたりする場合に、このようなデータを保護するために使用される。
- データ暗号化の有効性は、国際的に承認された暗号アルゴリズムの使用により保証される。

(4) 高信頼通信

内部ネットワーク上に存在する文書データ、ジョブ情報、監査ログおよび TOE 設定データといった通信データを保護する。

一般的な暗号化通信プロトコル（TLS/HTTPS, TLS)に対応する。

(5) セキュリティ管理

システム管理者として識別および認証された利用者のみが、操作パネルまたはシステム管理者クライアントから、TOE のセキュリティ機能に関する設定の参照および変更を可能にする。

(6) セキュリティ監査

いつ、誰が、どのような作業を行ったかという事象(例えば、ユーザー操作、障害や構成変更など)は、監査ログとして監査サーバから取得要求を受けると監査サーバへ送信され保存される。監査ログ送信時は

HTTPS プロトコルによって暗号化される。
また、監査ログは TOE 内部にも蓄積することが可能で、システム管理者として識別認証された利用者のみがシステム管理者クライアントの Web ブラウザからもダウンロードすることができる。

(7) 高信頼な運用

MFD へのファームウェアのアップデートは、アップデートの適用前にソフトウェアの真正性を保証するために検証される。また MFD は、その運用が検出可能な故障等により中断されないことを保証するため、自己テストを実行する。

(8) PSTN ファクス-ネットワーク間の分離

MFD は、PSTN ファクス-ネットワーク間の分離に関し、PSTN ファクスモデムが PSTN と LAN 間のデータ・ブリッジを生成するために使えないことを保証する。

1.4.3. TOE の物理的範囲 (Physical Boundary of the TOE)

TOE の物理的な境界は、MFD 製品全体である。フィニシャ等のセキュリティには無関係のオプションやアドオンは、TOE に含まない。Table 2 から Table 3 に TOE を構成する物理的コンポーネントを記述する。
MFD 本体は、起動後の操作パネルに表示される、ベンダー名、および機種名によって識別される。

Table 2 TOE を構成する物理的コンポーネント(MFD 本体)

本体	バージョン	形式	配付方法
Xerox VersaLink B405DN	Controller ROM Ver. 1.90.3	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	現地受け渡し

本 TOE のガイダンスは、Table 3 に示す。

Table 3 TOE を構成する物理的コンポーネント

帳票番号	形式	配付方法	ガイダンス名	ハッシュ値
VERSION 1.6	PDF ファイル	Web 配付	Xerox VersaLink B405 Multifunction Printer User Guide	df04305b315ecf1f52c0d4c22e9ff0a861de63e2a5d561d5cf6e34979bcc4b3a
VERSION 2.1	PDF ファイル	Web 配付	Xerox VersaLink Series Multifunction and Single Function Printers System Administrator Guide	584c82fa73cf1804c501fd59029d6a69940e3d8d69b5d0fd934e1c704fcaef3a
Rev A	紙媒体	現地受け渡し	Xerox VersaLink B405 Quick Use Guide	－
Version 1.0 (20221019)	PDF ファイル	Web 配付	Xerox VersaLink B405DN Multifunction Printer Security Function	a5377681fa23dec865cfa6d584a782ccf27cd56e736e077b

			Supplementary Guide	3b7cab8f6a7b191a

2. 適合主張 (Conformance Claim)

2.1. CC 適合主張 (CC Conformance Claim)

本 ST および TOE の CC 適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン:

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model (April 2017 Version 3.1 Revision 5)
Part 2: Security functional components (April 2017 Version 3.1 Revision 5)
Part 3: Security assurance components (April 2017 Version 3.1 Revision 5)

CC Part2 extended
CC Part3 conformant

2.2. PP 主張、パッケージ主張 (PP claim, Package Claim)

2.2.1. PP 主張 (PP Claim)

本 ST は、下記 HCD-PP への完全適合を主張する。

タイトル: Protection Profile for Hardcopy Devices
バージョン: 1.0 dated September 10, 2015
Errata: Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.2.2. パッケージ主張 (Package Claim)

本 ST および TOE は、パッケージ適合を主張しない。

2.2.3. 適合根拠 (Conformance Rational)

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

- Required Uses

Printing, Scanning, Copying, Network communications, Administration

- Conditionally Mandatory Uses

PSTN faxing, Field-Replaceable Nonvolatile Storage.

- Optional Uses

Internal Audit Log Storage

3. セキュリティ課題定義 (Security Problem Definition)

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威 (Threats)

3.1.1. TOE 資産 (Assets Protected by TOE)

本 TOE が保護する資産は以下のとおりである。

Table 4 Assets for User Data

Designation	User Data type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 5 Assets for TSF Data

Designation	TSF Data type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.1.2. 脅威 (Threats)

本 TOE に対する脅威を、Table 6 に記述する。

Table 6 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF

	Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2. 組織のセキュリティ方針 (Organizational Security Policies)

本 TOE が順守しなければならない組織のセキュリティ方針を Table 7 に記述する。

Table 7 Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory)	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.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

3.3. 前提条件 (Assumptions)

本 TOE の動作、運用、および利用に関する前提条件を、Table 8 に記述する。

Table 8 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4. セキュリティ対策方針 (Security Objectives)

本章では、運用環境のセキュリティ対策方針について記述する。
運用環境のセキュリティ対策方針を Table 9 に記述する。

Table 9 運用環境のセキュリティ対策方針

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

5. 拡張コンポーネント定義 (Extended Components Definition)

この章の拡張コンポーネントは、HCD-PP で定義されたものである。

5.1. 拡張機能要件定義

5.1.1. Class FAU: Security Audit

FAU_STG_EXT Extended: External Audit Trail Storage

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

Component leveling:

FAU_STG_EXT.1 Extended: External Audit Trail Storage	1

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

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

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

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

- There are no auditable events foreseen.

FAU_STG_EXT.1 Protected Audit Trail Storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation, FTP_ITC.1 Inter-TSF trusted channel

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

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

for the transmission of audit data to an External IT Entity.

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

5.1.2. Class FCS: Cryptographic Support

FCS_CKM_EXT Extended: Cryptographic Key Management

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

Component leveling:

FCS_CKM_EXT.4 Extended: Cryptographic Key Material	4

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FCS_CKM_EXT.4 Cryptographic Key Material Destruction

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction

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

Rationale:

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

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

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 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_HTTPS_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.

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.1 Extended: Key Chaining	1

FCS_KYC_EXT.1 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	**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.

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 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.

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 Extended: TLS selected	1

FCS_TLS_EXT.1 TLS selected, requires the TLS protocol implemented as specified.

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

- There are no management actions foreseen.

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

- Failure of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

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

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

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[selection:
None
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Rationale:
TLS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.1.3. Class FDP: User Data Protection

FDP_DSK_EXT Extended: Protection of Data on Disk

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

Component leveling:

FDP_DSK_EXT.1 Extended: Protection of Data on Disk	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FDP_DSK_EXT.1 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.

FDP_FXS_EXT Extended: Fax Separation

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

Component leveling:

FDP_FXS_EXT.1 Extended: Fax Separation	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FDP_FXS_EXT.1 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.

5.1.4. Class FIA: Identification and Authentication

FIA_PMG_EXT Extended: Password Management

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

Component leveling:

FIA PMG EXT.1 Extended: Password Management	1

FIA_PMG _EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FIA_PMG _EXT.1 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.

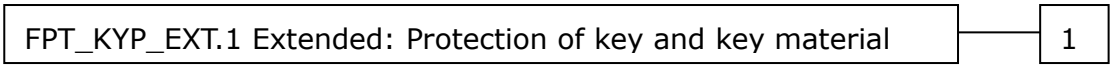
Rationale:
Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.
This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.1.5. Class FPT: Protection of the TSF

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 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.

FPT_SKP_EXT Extended: Protection of TSF Data

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

Component leveling:

FPT_SKP_EXT.1 Extended: Protection of TSF Data	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_SKP_EXT.1 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.

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 Extended: TSF testing	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TST_EXT.1 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.

FPT_TUD_EXT Extended: Trusted Update

Family Behavior:
This family defines requirements for the TSF to ensure that only administrators

can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

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

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

- There are no management actions foreseen.

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

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), 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: *published hash, no other functions*] prior to installing those updates.

Rationale:
Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.
This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6. セキュリティ要件 (Security Requirements)

本章では、セキュリティ機能要件、セキュリティ保証要件およびセキュリティ要件根拠について記述する。
なお、本章で使用する用語の定義は以下のとおりである。

6.1. 表記法

ボールド書体は、HCD-PP で完成または詳細化された SFR の部分を示し、コモンクライテリアパート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している。
ボールドイタリック書体は、HCD-PP で完成または詳細化された SFR の部分を、本セキュリティターゲットにおいて選択され、かつ／または完成された SFR 内のテキストを示す。
アンダーラインつきボールド書体に続く()内の***ボールドイタリック&アンダーライン書体***は、HCD-PP で完成された SFR の部分を、本セキュリティターゲットにおいて詳細化された SFR 内のテキストを示す。
*イタリック書体*は、本セキュリティターゲットにおいて選択され、かつ／または完成された SFR 内のテキストを示す。
*グレーのイタリックの書体*は、本セキュリティターゲットにおいて、選択されなかった SFR 内のテキストを示す。
*イタリック＆アンダーライン書体*は、本セキュリティターゲットにおいて割り付けられた SFR 内のテキストを示す。

繰り返しの(a)、(b)は PP で定義されているもの、さらに繰り返す場合は(a1)、(a2)のようにしている。

6.2. セキュリティ機能要件 (Security Functional Requirements)

本 TOE が提供するセキュリティ機能要件を以下に記述する。

6.2.1. Class FAU: Security Audit

FAU_GEN.1	**Audit data generation** (for O.AUDIT)
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **not specified** level of audit; and c) **All auditable events specified in Table 10**, [assignment: *no other auditable events*].
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 10**, [assignment: *no other relevant information*].

Table 10 Auditable Events

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

FAU_GEN.2 **User identity association**
(for O.AUDIT)

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

FAU_SAR.1 **Audit review**
(for O.AUDIT)

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *U.ADMIN*] with the

	capability to read **all records** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	**Restricted audit review** (for O.AUDIT)
Hierarchical to: Dependencies:	No other components. FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAU_STG.1	**Protected audit trail storage** (for O.AUDIT)
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.
FAU_STG.4	**Prevention of audit data loss** (for O.AUDIT)
Hierarchical to: Dependencies:	FAU_STG.3 Action in case of possible audit data loss FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	**Refinement**: The TSF shall [selection, choose one of: "~~***ignore audited events***~~", "*prevent audited events, except those taken by the authorised user with special rights*", "***overwrite the oldest stored audit records***"] and [assignment: *no other actions to be taken*] if the audit trail is full.
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.

6.2.2. Class FCS: Cryptographic Support

FCS_CKM.1(a)	**Cryptographic Key Generation (for asymmetric keys)** (for O.COMMS_PROTECTION)
Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or FCS_COP.1(i) Cryptographic operation (Key Transport)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_CKM.1.1(a)	Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with** [**selection:** ***· NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*** ***· NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*** ***· NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer***

	Factorization Cryptography" for RSA-based key establishment schemes
	] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.
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), or FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption), or FCS_COP.1(e) Cryptographic Operation (Key Wrapping), or FCS_COP.1(f) Cryptographic operation (Key Encryption), or FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication), or FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
FCS_CKM.1.1(b)	Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: *128 bit, 256 bit*] that meet the following: No Standard.**
FCS_CKM.4	**Cryptographic key destruction** (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or

	FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM.4.1	Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:** ***For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]]*. ***For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;***] that meets the following: [**selection:** ***NIST SP800-88, no standard***].
FCS_CKM_EXT.4	**Cryptographic Key Material Destruction** (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to: Dependencies:	No other components. [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction
FCS_CKM_EXT.4.1	The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.
FCS_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** [**assignment:** *CBC, GCM*] and cryptographic key sizes **128-bits and 256-bits** that meets the following: **FIPS PUB 197, "Advanced Encryption Standard (AES)"** [**Selection:** ***NIST SP 800-38A,*** ***NIST SP 800-38B, NIST SP 800-38C,*** ***NIST SP 800-38D***]
FCS_COP.1(b1)	**Cryptographic Operation (for signature generation/verification)** (for O.UPDATE VERIFICATION)
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(b1)	Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection: ***-Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],*** ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or*** ***-Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]***] that meets the following **[selection:** ***Case: Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: RSA Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"***

	Case: Elliptic Curve Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard" The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard"). **].**
FCS_COP.1(b2)	**Cryptographic Operation (for signature generation/verification)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(b2)	Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [**selection:** ***-Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater]***, ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits, 3072 bits], or*** ***-Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits, 384bits, 521bits]***] that meets the following [**selection:** ***Case: Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: RSA Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard"*** ***Case: Elliptic Curve Digital Signature Algorithm FIPS PUB 186-4, "Digital Signature Standard" The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").*** **].**
FCS_COP.1(c1)	**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(c1)	Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [**selection:** ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].
FCS_COP.1(c2)	**Cryptographic operation (Hash Algorithm)** (for O.COMMS_PROTECTION)
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_COP.1.1(c2)	Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [**selection:** ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].
FCS_COP.1(d)	**Cryptographic operation (AES Data Encryption/Decryption)** (for O. STORAGE_ENCRYPTION)
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(d)	The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection:** ***CBC, GCM, XTS*****] mode** and cryptographic key sizes [**selection:** ***128 bits, 256 bits***] that meet the following: **AES as specified in ISO/IEC 18033-3**, [**selection:** ***CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE1619***].

FCS_COP.1(f)	**Cryptographic operation (Key Encryption)** (selected from FCS_KYC_EXT.1.1)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(f)	Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[selection: *CBC, GCM*] mode**] and cryptographic key sizes [**selection: *128 bits, 256 bits***] that meet the following: [**AES as specified in ISO /IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772***].
FCS_COP.1(g)	**Cryptographic Operation (for keyed-hash message authentication)** (selected with FCS_IPSEC_EXT.1.4)
Hierarchical to: Dependencies:	No other components. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys) FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_COP.1.1(g)	Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC**-[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], key size [assignment: *160, 256, 384*], **and message digest sizes** [**selection: *160, 224, 256, 384, 512***] bits that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard.**"
FCS_HTTPS_EXT.1	**HTTPS selected** (selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to:	No other components.
Dependencies:	FCS_TLS_EXT.1 Extended: TLS selected
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.
FCS_KYC_EXT.1	**Key Chaining** (for O.STORAGE_ENCRYPTION)
Hierarchical to:	No other components.
Dependencies:	[FCS_COP.1(e) Cryptographic operation (Key Wrapping), or FCS_SMC_EXT.1 Extended: Submask Combining, or FCS_COP.1(f) Cryptographic operation (Key Encryption), or FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_KYC_EXT.1.1	The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or DEK;* ***intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s):*** [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1,* ***key encryption as specified in FCS_COP.1(f),*** *key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits,* ***256 bits***].
FCS_RBG_EXT.1	**Cryptographic Operation (Random Bit Generation)** (for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with [selection:

ISO/IEC 18031:2011, NIST SP 800-90A] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment:*1*] 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/IEC18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FCS_TLS_EXT.1 **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 [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
].

6.2.3. Class FDP: User Data Protection

FDP_ACC.1	**Subset access control** (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	Refinement: The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 11 and Table 12**.
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 11 and Table 12**.

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 11 and Table 12***.

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

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

Table 11 D.USER.DOC Access Control SFP

		"Create"	**"Read"**	**"Modify"**	**"Delete"**
Print	***Operation:***	***Submit a document to be printed***	***View image or Release printed output***	***Modify stored document***	***Delete stored document***
	Job owner	**(note 1)**		***denied***	
	U.ADMIN		***denied***	***denied***	***denied***
	U.NORMAL		**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		***denied***	***denied***	
	U.NORMAL		**denied**	**denied**	**denied**
	Unauthenticated	**denied**	**denied**	**denied**	**denied**

Copy	***Operation:***	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	**(note 2)**			
	U.ADMIN		***denied***	***denied***	
	U.NORMAL		**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		***denied***	***denied***	
	U.NORMAL		**denied**	**denied**	**denied**
	Unauthenticated	**denied**	**denied**	**denied**	**denied**
Fax receive	***Operation:***	***Receive a fax and store it***	***Release printed fax output***	***Modify image of received fax***	***Delete image of received fax***
	Fax owner	**(note 3)**		***denied***	
	U.ADMIN	**(note 4)**		***denied***	
	U.NORMAL	**(note 4)**	**denied**	**denied**	**denied**
	Unauthenticated	***(note 4)***	**denied**	**denied**	**denied**

Table 12 D.USER.JOB Access Control SFP

		"Create" *	**"Read"**	**"Modify"**	**"Delete"**
Print	***Operation:***	***Create print job***	***View print queue/log***	***Modify print job***	***Cancel print job***
	Job owner	**(note 1)**		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			**denied**	**denied**
	Unauthenticated	***(condition 1)***	***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			***denied***	
	U.NORMAL			**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			***denied***	
	U.NORMAL			**denied**	**denied**
	Unauthenticated	**denied**	***denied***	**denied**	**denied**
Fax send	***Operation:***	***Create fax send job***	***View fax job status/log***	***Modify fax send job***	***Cancel fax send job***
	Job owner	**(note 2)**		***denied***	
	U.ADMIN			***denied***	
	U.NORMAL			**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***	
	U.ADMIN	**(note 4)**		***denied***	
	U.NORMAL	**(note 4)**		**denied**	**denied**
	Unauthenticated	***(note 4)***	***denied***	**denied**	**denied**

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.
Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print Job.
Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, or fax send Job.
Note 3: Job Owner of received faxes is assigned by default. Ownership of received faxes is assigned to U.ADMIN role.
Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.

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

6.2.4. Class FIA: Identification and Authentication

FIA_AFL.1	**Authentication failure handling** (for O.USER_I&A)
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *1 - 10*]] unsuccessful authentication attempts occur related to [assignment: *User authentication (with local authentication)*].

FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *Identification and authentication of relevant user is inhibited until TOE is cycled.*].
FIA_ATD.1	**User attribute definition** (for O.USER_AUTHORIZATION)
Hierarchical to: Dependencies:	No other components. No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *User Identifier, User Role*].
FIA_PMG_EXT.1	**Password Management** (for O.USER_I&A)
Hierarchical to: Dependencies:	No other components. 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: *" (space)", """, "'", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~"*]]; ・ Minimum password length shall be settable by an **Administrator**, and **have the capability to require** passwords of 15 characters or greater;
FIA_UAU.1	**Timing of authentication** (for O.USER_I&A)
Hierarchical to: Dependencies:	No other components. FIA_UID.1 Timing of identification

FIA_UAU.1.1	Refinement: The TSF shall allow [assignment: *storing the fax data received from public telephone line, storing print data received from print driver*] 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.

FIA_UAU.7 **Protected authentication feedback**
(for O.USER_I&A)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [assignment: ●] to the user while the authentication is in progress.

FIA_UID.1 **Timing of identification**
(for O.USER_I&A and O.ADMIN_ROLES)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	Refinement: The TSF shall allow [assignment: *storing the fax data received from public telephone line*] 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.

FIA_USB.1 **User-subject binding**
(for O.USER_I&A)

Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *User Identifier, User Role*].

FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *none*].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *none*].

6.2.5. Class FMT: Security Management

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 Refinement: The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *List of security functions in Table 13*] to **U.ADMIN**.

Table 13 List of Security Functions

Function	Operation
User Authentication	*enable, disable*
Auditing	*enable, disable*
Trusted communications	*enable, disable, modify the behavior*
Firmware update	*enable, disable*
Self Test	*enable, disable*

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

FMT_MSA.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: creation]*] the security attributes [assignment: *the security attributes listed in Table 14*] to [assignment: *the roles listed in Table 14*].

Table 14 Security Attributes and Authorized Roles

Security attributes	Operation	Role
User identifier (SA and U.NORMAL)	*query, delete, creation*	*U.ADMIN*
User Role (SA and U.NORMAL)	*query, modify*	*U.ADMIN*

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 [selection, choose one of: *restrictive, permissive, [assignment: none]*] default values for security attributes that are used to enforce the SFP.

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

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 15.

Table 15 Management of TSF Data

Data	**Operation**	**Authorised Role(s)**
TSF Data owned by U.NORMAL or associated with documents or jobs owned by U.NORMAL.		
U.NORMAL Password	*modify*	**U.ADMIN, the owning U.NORMAL.**
TSF Data not owned by a U.NORMAL		
Key operator Password	*modify*	**U.Admin** ***(Key Operator)***
SA Password	*modify*	**U.ADMIN**
Data on minimum user password length	*query, modify*	**U.ADMIN**
Data on Secure Print	*query, modify*	**U.ADMIN**
Data on Access denial due to authentication failure	*query, modify*	**U.ADMIN**
Data on Customer Engineer Operation Restriction	*query, modify*	**U.ADMIN**
Data on date and time	*query, modify*	**U.ADMIN**
Data on Autoclear	*query, modify*	**U.ADMIN**
Data on Report Print	*query, modify*	**U.ADMIN**
Software, firmware, and related configuration data		
Controller ROM	*modify*	**U.ADMIN**

FMT_SMF.1 **Specification of Management Functions**
(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

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

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *Security Management Functions listed in Table 16*].

Table 16 Security Management Functions

Management Functions	***Operation***
Registration of U.NORMAL /SA	*query, modify, delete*

	creation
Data on User Authentication	*query, modify*
Key operator Password	*modify*
Data on Secure Print	*query, modify*
Data on Trusted communications	*query, modify*
Data on date and time	*query, modify*
Data on Auditing	*query, modify*
Data on Customer Engineer Operation Restriction	*query, modify*
Data on Self Test	*query, modify*
Data on Access denial due to authentication failure	*query, modify*
Data on minimum user password length	*query, modify*
Data on Autoclear	*query, modify*
Data on Firmware update	*query, modify*
Data on Report Print	*query, modify*
Controller ROM	*modify*

FMT_SMR.1 **Security roles**
(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 Refinement: The TSF shall maintain the roles **U.ADMIN(*U.ADMIN, SA, Key Operator*), U.NORMAL**.

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

6.2.6. Class FPT: Protection of the TSF

FPT_KYP_EXT.1 **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**.
FPT_SKP_EXT.1	**Protection of TSF Data** (for O.COMMS PROTECTION)
Hierarchical to: Dependencies:	No other components. No dependencies.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.
FPT_STM.1	**Reliable time stamps** (for.O.AUDIT)
Hierarchical to: Dependencies:	No other components. No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
FPT_TST_EXT.1	**TSF testing** (for O.TSF_SELF_TEST)
Hierarchical to: Dependencies:	No other components. No dependencies.
FPT_TST_EXT.1.1	The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.
FPT_TUD_EXT.1	**Trusted Update** (for O.UPDATE_VERIFICATION)
Hierarchical to: Dependencies:	No other components. FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), FCS_COP.1(c) Cryptographic operation (Hash Algorithm).
FPT_TUD_EXT.1.1	The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2	The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and **[selection:** *published hash,* ***no other functions***] prior to installing those updates.

6.2.7. Class FTA: TOE Access

FTA_SSL.3	**TSF-initiated termination** (for O.USER_I&A)
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment: *Auto clear time for the control panel：10 ～ 900 seconds* *Login timeout for the Web UI：1 ～ 240minutes* *There is no inactive time with printer driver*].

6.2.8. Class FTP: Trusted Paths/Channels

FTP_ITC.1	**Inter-TSF trusted channel** (for O.COMMS_PROTECTION, O.AUDIT)
Hierarchical to:	No other components.
Dependencies:	[FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_ITC.1.1	Refinement: The TSF shall **use [selection:** *IPsec, SSH,* ***TLS, TLS/HTTPS***] **to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities**: **[selection:** *authentication server,* ***[assignment:*** *Audit Log 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 [assignment: *mail service, and audit transmission service*].
FTP_TRP.1(a)	**Trusted path (for Administrators)** (for O.COMMS_PROTECTION)
Hierarchical to: Dependencies:	No other components. [FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(a)	Refinement: The TSF shall **use [selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide a **trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
FTP_TRP.1.2(a)	Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path
FTP_TRP.1.3(a)	Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.
FTP_TRP.1(b)	**Trusted path (for Non-administrators)** (for O.COMMS_PROTECTION)

Hierarchical to:	No other components.
Dependencies:	[FCS_IPSEC_EXT.1 Extended: IPsec selected, or FCS_TLS_EXT.1 Extended: TLS selected, or FCS_SSH_EXT.1 Extended: SSH selected, or FCS_HTTPS_EXT.1 Extended: HTTPS selected].
FTP_TRP.1.1(b)	Refinement : The TSF shall **use [selection, choose at least one of: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
FTP_TRP.1.2(b)	Refinement: The TSF shall permit [selection: ***the TSF, 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**.

6.3. セキュリティ保証要件 (Security Assurance Requirements)

Table 17 にセキュリティ保証要件を記述する。

Table 17 セキュリティ保証要件

Assurance Class	Assurance Components	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition

Assurance Class	Assurance Components	Assurance Components Description
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

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。

6.4. セキュリティ要件根拠 (Security Requirement Rationale)

6.4.1. 依存性の検証 (Dependencies of Security Functional Requirements)

セキュリティ機能要件が依存している機能要件、および依存関係を満足しない機能要件と、依存関係が満たされなくても問題がない根拠を、Table 18 に記述する。

Table 18 セキュリティ機能要件コンポーネントの依存性

機能要件コンポーネント	依存性の機能要件コンポーネント		
要件および要件名称	PP で規定されている要件	依存性を満足していない要件とその正当性	充足性
FAU_GEN.1 監査データ生成	FPT_STM.1	-	OK
FAU_GEN.2 利用者識別情報の関連付け	FAU_GEN.1 FIA_UID.1	-	OK
FAU_STG_EXT.1 拡張:外部監査証跡格納	FAU_GEN.1 FTP_ITC.1	-	OK
FCS_CKM.1(a) 暗号鍵生成(非対称鍵用)	[FCS_COP.1(b) または FCS_COP.1(i)] FCS_CKM_EXT.4	-	OK
FAU_SAR.1 監査レビュー	FAU_GEN.1	-	OK

機能要件コンポーネント	依存性の機能要件コンポーネント		
要件および要件名称	PP で規定されている要件	依存性を満足していない要件とその正当性	充足性
FAU_SAR.2 限定監査レビュー	FAU_SAR.1	-	OK
FAU_STG.1 保護された監査証跡格納	FAU_GEN.1	-	OK
FAU_STG.4 監査データ損失の防止	FAU_STG.1	-	OK
FCS_CKM.1(b) 暗号鍵生成(対称鍵用)	[FCS_COP.1(a) または FCS_COP.1(d) または FCS_COP.1(e) または FCS_COP.1(f) または FCS_COP.1(g) または FCS_COP.1(h)] FCS_CKM_EXT.4 FCS_RBG_EXT.1	-	OK
FCS_CKM.4 暗号鍵破棄	[FCS_CKM.1(a) または FCS_CKM.1(b)]	-	OK
FCS_CKM_EXT.4 拡張:暗号鍵材料の破棄	[FCS_CKM.1(a) または FCS_CKM.1(b)] FCS_CKM.4	-	OK
FCS_COP.1(a) 暗号操作(対称鍵暗号化／復号)	FCS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(b1) 暗号操作(署名生成／検証)	FCS_CKM.1(a) FCS_CKM_EXT.4	ファームウェアの署名検証で使用される公開鍵ペアは、TOE 外でベンダーが作成し、TOE 内に秘密鍵を持たないため、 FCS_CKM.1(a)、 FCS_CKM_EXT.4 に依存しない。	依存性なし
FCS_COP.1(b2) 暗号操作(署名生成／検証)	FCS_CKM.1(a) FCS_CKM_EXT.4	-	OK
FCS_COP.1(c1) 暗号操作(ハッシュアルゴリズム)	なし	-	-
FCS_COP.1(c2) 暗号操作(ハッシュアルゴリズム)	なし	-	-

機能要件コンポーネント	依存性の機能要件コンポーネント		
要件および要件名称	PP で規定されている要件	依存性を満足していない要件とその正当性	充足性
FCS_COP.1(d) 暗号操作（AES データ暗号化／復号）	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(f) 暗号操作（鍵暗号化）	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_COP.1(g) 暗号操作(鍵付ハッシュメッセージ認証)	CS_CKM.1(b) FCS_CKM_EXT.4	-	OK
FCS_HTTPS_EXT.1 拡張：選択された HTTPS	FCS_TLS_EXT.1	-	OK
FCS_KYC_EXT.1 拡張：鍵チェイン	[FCS_COP.1(e) または FCS_SMC_EXT.1 または FCS_COP.1(i) または FCS_KDF_EXT.1 及び／または FCS_COP.1(f)]	-	OK
FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）	なし		-
FCS_TLS_EXT.1 拡張：選択された TLS	FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1	-	OK
FDP_ACC.1 サブセットアクセス制御	FDP_ACF.1	-	OK
FDP_ACF.1 セキュリティ属性によるアクセス制御	FDP_ACC.1 FMT_MSA.3	-	OK
FDP_DSK_EXT.1 拡張：ディスク上のデータ保護	FCS_COP.1(d)	-	OK
FDP_FXS_EXT.1 拡張：ファクス分離	なし		-
FIA_AFL.1 認証失敗時の取り扱い	FIA_UAU.1	-	OK
FIA_ATD.1 利用者属性定義	なし		-
FIA_PMG_EXT.1 拡張：パスワード管理	なし		-

機能要件コンポーネント	依存性の機能要件コンポーネント		
要件および要件名称	PP で規定されている要件	依存性を満足していない要件とその正当性	充足性
FIA_UAU.1 認証のタイミング	FIA_UID.1	-	OK
FIA_UAU.7 保護されたフィードバック	FIA_UAU.1	-	OK
FIA_UID.1 識別のタイミング	なし		-
FIA_USB.1 利用者・サブジェクト結合	FIA_ATD.1	-	OK
FMT_MOF.1 セキュリティ機能のふるまいの管理	FMT_SMF.1 FMT_SMR.1	-	OK
FMT_MSA.1 セキュリティ属性の管理	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	-	OK
FMT_MSA.3 静的属性初期化	FMT_MSA.1 FMT_SMR.1	-	OK
FMT_MTD.1 TSF データの管理	FMT_SMF.1 FMT_SMR.1	-	OK
FMT_SMF.1 管理機能の特定	なし		-
FMT_SMR.1 セキュリティ役割	FIA_UID.1	-	OK
FPT_KYP_EXT.1 拡張:鍵及び鍵材料の保護	なし		-
FPT_SKP_EXT.1 拡張:TSF データの保護	なし		-
FPT_STM.1 高信頼タイムスタンプ	なし		-
FPT_TST_EXT.1 拡張:TSF テスト	なし		-
FPT_TUD_EXT.1 拡張:高信頼アップデート	FCS_COP.1(b) FCS_COP.1(c)	-	OK
FTA_SSL.3 TSF 起動による終了	なし		-
FTP_ITC.1 TSF 間高信頼チャネル	[FCS_IPSEC_EXT.1、 または FCS_TLS_EXT.1、 または FCS_SSH_EXT.1、 または FCS_HTTPS_EXT.1]	-	OK
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1、	-	OK

機能要件コンポーネント	依存性の機能要件コンポーネント		
要件および要件名称	PP で規定されている要件	依存性を満足していない要件とその正当性	充足性
高信頼パス（管理者用）	または FCS_TLS_EXT.1、 または FCS_SSH_EXT.1、 または FCS_HTTPS_EXT.1]		
FTP_TRP.1(b) 高信頼パス（非管理者用）	[FCS_IPSEC_EXT.1、 または FCS_TLS_EXT.1、 または FCS_SSH_EXT.1、 または FCS_HTTPS_EXT.1]	-	OK

6.4.2. セキュリティ保証要件根拠 (Security Assurance Requirements Rationale)

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。PP 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 が提供するセキュリティ機能の要約仕様について記述する。

7.1. セキュリティ機能 (Security Functions)

Table 19 に TOE セキュリティ機能とセキュリティ機能要件の対応を示す。
本節で説明する TOE セキュリティ機能は 6.1 節に記述されるセキュリティ機能要件を満たすものである。

Table 19 TOE セキュリティ機能とセキュリティ機能要件の対応関係

	セキュリティ機能							
SFRs	識別認証	セキュリティ監査	アクセス制御	セキュリティ管理	高信頼な運用	データ暗号化	高信頼通信	PSTNファクス-ネットワーク間の分離
FAU_GEN.1		✓						
FAU_GEN.2		✓						
FAU_STG_EXT.1		✓						
FAU_SAR.1		✓						
FAU_SAR.2		✓						
FAU_STG.1		✓						
FAU_STG.4		✓						
FCS_CKM.1(a)						✓		
FCS_CKM.1(b)						✓		
FCS_CKM.4						✓		
FCS_CKM_EXT.4						✓		
FCS_COP.1(a)						✓		
FCS_COP.1(b1)						✓		
FCS_COP.1(b2)						✓		
FCS_COP.1(c1)						✓		
FCS_COP.1(c2)						✓		
FCS_COP.1(d)						✓		
FCS_COP.1(f)						✓		

	セキュリティ機能							
SFRs	識別認証	セキュリティ監査	アクセス制御	セキュリティ管理	高信頼な運用	データ暗号化	高信頼通信	PSTNファクス-ネットワーク間の分離
FCS_COP.1(g)						✓		
FCS_HTTPS_EXT.1							✓	
FCS_KYC_EXT.1						✓		
FCS_RBG_EXT.1						✓	✓	
FCS_TLS_EXT.1							✓	
FDP_ACC.1			✓					
FDP_ACF.1			✓					
FDP_DSK_EXT.1						✓		
FDP_FXS_EXT.1								✓
FDP_RIP.1(a)								
FIA_AFL.1	✓							
FIA_ATD.1	✓							
FIA_PMG_EXT.1	✓							
FIA_UAU.1	✓							
FIA_UAU.7	✓							
FIA_UID.1	✓							
FIA_USB.1	✓							
FMT_MOF.1				✓				
FMT_MSA.1				✓				
FMT_MSA.3				✓				
FMT_MTD.1				✓	✓			
FMT_SMF.1				✓	✓			
FMT_SMR.1				✓				
FPT_KYP_EXT.1						✓		
FPT_SKP_EXT.1				✓				
FPT_STM.1		✓						

SFRs	セキュリティ機能							
	識別認証	セキュリティ監査	アクセス制御	セキュリティ管理	高信頼な運用	データ暗号化	高信頼通信	PSTNファクス-ネットワーク間の分離
FPT_TST_EXT.1					✓			
FPT_TUD_EXT.1					✓			
FTA_SSL.3	✓							
FTP_ITC.1							✓	
FTP_TRP.1(a)							✓	
FTP_TRP.1(b)							✓	

7.1.1. 識別認証

識別認証機能は、許可された特定の利用者だけに MFD の機能を使用する権限を持たせるために、操作パネル、利用者クライアントの Web UI(*)からユーザーID とユーザーパスワードを入力させて識別認証する機能である。
MFD に登録されている利用者情報を使用して、識別認証を行う。
(*):利用者クライアント PC の Web ブラウザを介した MFD のサーバ機能。製品上、「Embedded Web Server」という名称で提供されるが、本書においては本項以降、Web UI と呼ぶ。

(1) FIA_AFL.1 Authentication failure handling (認証失敗時の取り扱い)
TOE は利用者が TOE へアクセスする前に、利用者の認証を行うが、認証試行時の認証失敗対応機能を提供している。
利用者の本体認証における認証失敗を検出し、アクセス拒否回数で設定されている回数(1～10 回)の連続失敗に達すると、当該利用者の識別認証に関しては、TOE の電源切断/再投入まで受け付けなくなる。

【関連する TSFI】
操作パネルの識別認証
Web UI の識別認証
外部監査サーバ

(2) FIA_ATD.1 User attribute definition 利用者属性定義
FIA_USB.1 User-subject binding 利用者-サブジェクト結合

TOE は利用者に対して、ユーザーID と役割を属性として定義し、それらを識別認証した利用者に対して割り付ける。

【FIA_ATD.1 に関連する TSFI】
Web UI の管理機能
【FIA_USB.1 に関連する TSFI】
操作パネルの識別認証
Web UI の識別認証
外部監査サーバ

(3) FIA_PMG_EXT.1 Password Management パスワード管理

TOE において、機械管理者のパスワード変更時、または本体認証の利用者登録・変更時のパスワードは、以下の文字の組み合わせで作成することができる。
パスワードに指定可能な文字:
アルファベットの大文字と小文字、数字、及び次の特殊文字
(“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ” (space)”, “”””, “’”, “+”, “,”, “-“, “.“, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “¥”, “]”, “_”, “`”, “{“, “|”, “}”, “~”)
また、システム管理者は最少パスワード長を 0～63 文字の範囲で設定することができる。
TOE はこの設定により 15 文字以上に限定することができる。

【関連する TSFI】
Web UI の管理機能

(4) FIA_UAU.1 Timing of authentication 認証のタイミング、
FIA_UID.1 Timing of identification 識別のタイミング

TOE は利用者の識別認証方式として、本体認証方式をサポートする。
識別認証を要求されるインタフェースには、操作パネル、利用者クライアントの Web ブラウザ、外部監査サーバの 3 種類がある。
操作パネル、利用者クライアントの Web ブラウザでは、MFD 機能の操作を許可する前に、ID とパスワードを入力させて、入力された ID とパスワードが、TOE に登録されている利用者情報と一致することを検証する。
監査サーバでは、システム管理者の ID とパスワードを記述した PowerShell スクリプトをあらかじめ準備し、監査サーバ上でその PowerShell スクリプトを実行する。PowerShell スクリプトを実行することにより、監査サーバから TOE に https プロトコル上で ID とパスワードが送信され、TOE は受信した ID とパスワードに基づき識別認証を実行する。
識別認証を要求されるインタフェースの認証(FIA_UAU.1)と識別(FIA_UID.1)は同時に実行され、識別・認証の両方が成功した時のみ操作が許可される。
クライアント PC のプリンタードライバによる Secure Print は、プリントデータに付与される ID により、識別のみ行われる。
公衆回線からの FAX の受信については、TOE は、識別認証せずに、FAX データを受信する。

【関連する TSFI】
操作パネルの識別認証
Web UI の識別認証
プリンタードライバ
外部監査サーバ
公衆電話回線

(5) FIA_UAU.7 Protected authentication feedback 保護された認証フィードバック
TOE はユーザー認証時に、パスワードを隠すために、パスワードとして入力された文字数と同数の隠し文字"●（bullet）"を、操作パネルや Web ブラウザに表示する機能を提供する。

【関連する TSFI】
操作パネルの識別認証
Web UI の識別認証

(6) FTA_SSL.3 TSF-initiated termination TSF 起動による終了
TOE は Web ブラウザから Web UI に一定時間(1～240 分で設定可能)のアクセスが無い場合はログイン(認証セッション)をクリアし再認証を要求する。
また操作パネルから一定時間(10～900 秒で設定可能)の操作が無い場合は、操作パネルの設定がクリアされ認証画面へ戻る。
プリンタードライバとのセッションは保持せず、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】
操作パネルの識別認証
Web UI の識別認証

7.1.2. セキュリティ監査

セキュリティ監査機能は、システム管理者による設定に従い、すべての TOE 利用者に対して、いつ、誰が、どのような作業を行ったかという事象（例えば、ユーザー操作、障害や構成変更など）を、追跡記録するための機能を提供する。

(1) FAU_GEN.1 Audit data generation （監査データ生成）
FAU_GEN.2 User identity association （利用者識別情報の関連付け）
TOE は、ジョブの終了や利用者の識別認証の失敗、識別認証された利用者による管理機能の利用など、Table 20 に示す監査対象の事象について、監査ログを記録する。また各監査データには、事象発生の日時、事象の種別、事象を引き起こした利用者（可能であれば）、および事象の結果が記録される。
TOE は定義された監査対象事象を監査ログとして記録する時に、その原因となった利用者の識別情報に関連付けて記録している。

【関連する TSFI】
操作パネルの識別認証
Web UI の識別認証
プリンタードライバ
操作パネルの管理機能
Web UI の管理機能
電源ボタン
操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、ファクス受信文書の印刷機能
操作パネルのジョブ状態・履歴の表示機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能
公衆電話回線

Table 20 監査ログの詳細

対象事象	記録される監査事象名	監査事象詳細
監査機能の起動と終了	System Status/ Started normally (cold boot), System Status/ Started normally (warm boot), Shutdown requested	
ジョブの終了	Job Status/ Completed, Job Status/ Canceled by User	Print
		Copy
		Scan
		Fax
		Mailbox
利用者認証失敗 利用者識別失敗 (操作パネル、Web UI、監査サーバから)	Login/ Failed (Invalid UserID), Login/ Failed (Invalid Password)	
利用者識別失敗 (プリンタドライバから)	Job Status/ Print /Aborted	
管理機能の利用	Device Settings/ View Security Setting	
	Device Settings/ Change Security Setting	
	Device Settings/ Switch Authentication Mode	
	Device Settings/ Edit User	

	[変更された属性として"ID", "Password", "Name"が記録される]	
	Device Settings/ Add User	
	Device Settings/ Delete User	
	Device Config/ Software	
	Audit Policy/ Audit Log/ Enable, Audit Policy/ Audit Log/ Disable	
役割の一部である利用者グループの改変	Device Settings/ Edit User [変更された属性として"Role"が記録される]	
時刻の変更	Device Settings/ Adjust Time	
セション確立の失敗 (TLS)	Communication/ Trusted Communication	Failed [プロトコル、通信先、失敗の理由も保存]

(2) FAU_SAR.1 Audit review (監査レビュー)

システム管理者は、Web UI でログイン後、Web UI からの操作により、TOE 内部に保存されたすべての監査ログを読み出すことができる。

監査ログはタブ区切りのテキストファイルとしてダウンロードされる。監査ログをダウンロードする場合は、TLS 通信が有効に設定されている必要がある。

【関連する TSFI】

Web UI の管理機能

(3) FAU_SAR.2 Restricted audit review (限定監査レビュー)

TOE 内部に保存された監査ログの読み出し機能は、認証されたシステム管理者のみに限定される。

また、監査ログへのアクセスは、Web UI のみ使用可能で、操作パネルからアクセスすることは出来ない。

【関連する TSFI】

Web UI の管理機能

(4) FAU_STG.1 Protected audit trail storage (保護された監査証跡格納)

TOE 内部に保存された監査ログへのアクセスは、読み出し機能のみであり、削除および修正機能は存在しない。これにより、監査ログの不正な削除と改変から保護されている。

【関連する TSFI】
Web UI の管理機能

(5) FAU_STG.4 Prevention of audit data loss (監査データ損失の防止)
TOE 内部に保存された監査ログは、最大 15,000 件を保存することが出来る。監査ログが満杯になった場合、最も古く記録された監査データに上書きして、新しい監査ログが損失することなく記録される。

【関連する TSFI】
操作パネルの識別認証
Web UI の識別認証
プリンタードライバ
操作パネルの管理機能
Web UI の管理機能
電源ボタン
操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、ファクス受信文書の印刷機能
操作パネルのジョブ状態・履歴の表示機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能
公衆電話回線

(6) FAU_STG_EXT.1 Extended: External Audit Trail Storage 外部監査証跡格納
TOE は監査サーバから監査ログの取得要求を受けると、TOE に保存されている全監査ログをタブ区切りのテキストファイルとして、監査サーバへ送出する。監査サーバへ送出する際、TLS/HTTPS プロトコルで暗号化される。監査ログの送出は、認証されたシステム管理者のみに限定される。
TOE 内部に一時保存される監査ログ対象のイベントの最大件数と、最大件数を超過した時の動作は、(5) FAU_STG.4 に記述される。

【関連する TSFI】
外部監査サーバ

(7) FPT_STM.1 Reliable time stamps 高信頼タイムスタンプ
定義された監査対象事象を監査ログとして記録する時に、TOE が持っているクロック機能によるタイムスタンプを発行する機能を提供する。
時計の設定変更は FMT_MTD.1 によりシステム管理者のみが可能である。

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

7.1.3. アクセス制御

識別認証が成功した利用者のみが下記の機能を使用可能となる。TSF にアクセスするインタフェースごとに、

利用可能になる機能が異なる。ただし、プリンタードライバでは、識別のみで認証は行われない。

a) 本体操作パネルで制御される機能

コピー機能、ファクス機能(送信)、スキャン機能、プリント機能(*)、機械状態の表示、ジョブ状態・履歴の表示機能、各種 TOE 設定データの参照/設定機能(システム管理者のみ)

(*):プリンタードライバでの Secure Print の設定が条件であり、設定しない場合は印刷されない。また、印刷時に操作パネルで認証が必要となる。

b) Web UI で制御される機能

機械状態の表示、ジョブ状態・履歴の表示機能、TOE 設定データの参照/設定機能(システム管理者のみ)、ファームウェアアップデート機能(システム管理者のみ)

c) 利用者クライアントのプリンタードライバを使用する機能

利用者が利用者クライアントのプリンタードライバで Secure Print を設定した状態でプリント指示をすると、MFD はユーザーID の識別が成功した場合にのみ受信データをビットマップデータに変換(デコンポーズ)してユーザーID ごとの内部リポジトリに蓄積する。

(1) FDP_ACC.1 Subset access control サブセットアクセス制御

FDP_ACF.1 Security attribute based access control セキュリティ属性によるアクセス制御

TOE は、Table 11, Table 12 に従い、各種基本機能のジョブと文書データのアクセス制御をおこなう。以下、文末の()内の note の記述は Table 11, Table 12 の note を参照している。

各種基本機能で扱われる文書データとジョブは、各機能を起動した利用者をオーナーとして割り付ける。

文書データの閲覧、編集は、オーナーだけが実施することができる。文書データの削除は、オーナーまたはシステム管理者が実施することができる。プリントの蓄積文書データの管理者による削除は、実施することができない。ファクス受信の蓄積文書データは、オーナーとして割り付けられたシステム管理者による印刷の実施後に自動的に削除される。ジョブの閲覧は、オーナー、システム管理者または一般利用者が実施することができる。ジョブの削除は、オーナーまたはシステム管理者が実施することができる。

ただしファクス受信中は、システム管理者だけがキャンセルし、削除することができる。クライアント PC から受信途中のデータは、オーナーまたはシステム管理者がキャンセルし、削除することができる。

認証されていない利用者によってクライアント PC から投入されるプリントデータ内には、利用者を特定するためのユーザーID が含まれる。(condition 1)

プリント機能におけるジョブ所有者は、プリントデータに含まれるユーザーID によって特定される。(note 1)

スキャン機能、コピー機能、ファクス送信機能におけるジョブは、操作パネルにログインしたユーザーID が、そのオーナーとして割りつけられる。(note 2)

ファクス受信中のジョブと、ファクス受信して保存されるファクス受信データは、システム管理者がオーナーとして割りつけられる。(note 3)

ファクス受信のジョブもデータも TOE 外から送られるため、TOE の利用者であるいずれのユーザーも、ファクス受信のジョブおよびデータを作成することはできない。(note 4)

プリント機能、ファクス受信機能により蓄積された文書データを編集する機能は提供されない。スキャン機能、コピー機能、ファクス送信機能により蓄積された文書データは、オーナーのみ変更(原稿追加)可能である。

プリント機能、スキャン機能、コピー機能、ファクス送信機能、ファクス受信機能の各種ジョブを改変する機能は提供されない。

【関連する TSFI】
プリンタードライバ
操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、ファクス受信文書の印刷機能
操作パネルのジョブ状態・履歴の表示機能
Web UI のジョブ状態・履歴の表示機能
公衆電話回線

7.1.4. セキュリティ管理

(1) FMT_MOF.1 Management of security functions behavior セキュリティ機能のふるまいの管理
FMT_MTD.1 Management of TSF data TSF データの管理
FMT_SMF.1 Specification of Management Functions 管理機能の特定
FMT_MSA.1 Management of security attributes セキュリティ属性の管理
FMT_MSA.3 Static attribute initialization 静的属性初期化
FMT_SMR.1 Security roles セキュリティの役割
TOE は識別認証されたシステム管理者のみに、下記 Table 21 に示す TOE セキュリティ機能に関係するセキュリティ管理機能の参照と設定変更、および各機能の詳細情報を設定するユーザーインタフェースを提供する。
また、識別認証された一般利用者は自分のパスワード変更のみ可能である。
これらの機能により、要求されるセキュリティ管理機能を提供する。
TOE は、Table 11 Table 12 に従い、各種基本機能で扱われるジョブと文書データの所有者識別情報のデフォルト値として、各機能を起動した利用者識別情報を設定する。詳細は、「7.1.3. アクセス制御 (1) FDP_ACC.1 Subset access control サブセットアクセス制御 FDP_ACF.1 Security attribute based access control セキュリティ属性によるアクセス制御」を参照のこと。
TOE は、機械管理者、SA、システム管理者、一般利用者の役割を正当な利用者に関連付け、それを維持する。役割は、ユーザーID と紐づいており、TOE はログインした利用者にユーザーID に対応する役割を紐づける。役割は、ユーザーID と紐づいており、TOE はログインした利用者にユーザーID に対応する役割を紐づける。
TOE は、利用者役割に関しセキュリティ属性のデフォルト値として、一般利用者を設定する。

【FMT_SMR.1 に関連する TSFI】
Web UI の識別認証
操作パネルの識別認証
【FMT_MOF.1、FMT_MSA.1、FMT_SMR.1、FMT_SMF.1 に関連する TSFI】
Web UI の管理機能
【FMT_MTD.1、FMT_SMF.1 に関連する TSFI】
操作パネルの管理機能
Web UI の管理機能
【FMT_MSA.3 に関連する TSFI】
プリンタードライバ

操作パネルのコピー機能、スキャン機能、ファクス機能
公衆電話回線

Table 21 セキュリティ管理機能と操作可能な UI

セキュリティ管理項目	操作パネル	Web UI
利用者/機械管理者の認証失敗によるアクセス拒否設定を参照し、有効/無効、拒否回数の設定を行う	-	✓
機械管理者のパスワードの設定を行う; 機械管理者のみ可能	-	✓
利用者の作成、ID の参照、削除、およびパスワードの設定を行う。また、利用者に割り当てた役割を参照し、SA 役割または一般利用者役割に変更する。	-	✓
ユーザーパスワードの最小文字数制限を参照し設定を行う	-	✓
通信データ暗号化機能の設定を参照し、有効/無効および詳細情報の設定を行う	-	✓
TLS サーバ証明書の設定を参照し、作成/更新の設定を行う。	-	✓
識別認証機能の設定を参照し、本体認証/無効の設定を行う	-	✓
Secure Print 機能の設定を参照し、蓄積/印刷の設定を行う	-	✓
日付、時刻を参照し設定を行う	✓	✓
自己テスト機能の設定を参照し、有効/無効の設定を行う	-	✓
ファームウェアアップデート機能の設定を参照し、有効/無効の設定を行う	-	✓
オートクリア機能（操作パネルおよび Web UI）の参照と設定	-	✓
レポート出力の設定を参照し、システム管理者限定/利用者の設定を行う	-	✓
カストマーエンジニア操作制限機能の参照と設定を行う(機能の有効/無効/保守パスワード)	-	✓
セキュリティ監査機能の設定を参照し有効/無効の設定を行う）	-	✓

(2) FPT_SKP_EXT.1 Protection of TSF Data TSF データの保護

TOE は、鍵暗号鍵(KEK: Key Encryption Key)を平文で NVRAM2 に保存するが、すべての利用者に対して、この暗号鍵を読みだすためのインタフェースを提供していない。また、NVRAM2 がはんだづけされている基板は、ストレージを目的とした基板ではない。

ストレージ暗号鍵(DEK: Data Encryption Key)は、上記の KEK で AES-CBC 方式で暗号化して、NVRAM1 に保存する。

TOE の起動時、NVRAM1 に保存された暗号化されたストレージ暗号鍵は、NVRAM2 にある鍵暗号鍵で復号化され、稼働中は平文の状態で DRAM に保存される。

ただし、すべての利用者に対して、TOE は、DRAM に保存された平文のストレージ暗号鍵を読みだすインタフェースを提供していない。また、DRAM に保存されている平文のストレージ暗号鍵は、電源を落とすことにより破棄される。

TLS 通信等に使用する秘密鍵付きの証明書は、7.1.6 (15)の機構により暗号化された状態で

NVRAM1 に保存され、すべての利用者に対して秘密鍵を読み出すインタフェースは提供していない。
通信に利用される TLS セッション鍵及び TLS EC Diffie-Hellman 秘密値は平文で DRAM に保存されるが、すべての利用者に対して、TOE は、DRAM に保存された平文のセッション鍵を読みだすインタフェースを提供していない。また、DRAM に保存されている平文のセッション鍵は、電源を落とすことにより破棄される。

【関連する TSFI】
特になし

7.1.5. 高信頼な運用

(1) FPT_TST_EXT.1 TSF testing TSF テスト
TSF はファームウェアである Controller ROM により実現されており、このファームウェアの完全性を検証することにより、TSF の正常動作を保証する。
TOE は、起動時に Controller ROM は 4byte のチェックサムを計算し所定の値と一致するかを確認し、異常時は操作パネルにエラーを表示し起動を停止する。また、DRBG に関して [1]11.3 に記載のヘルステストを実行し、テストが失敗した場合は操作パネルにエラーを表示し起動を停止する。なお DRBG の仕様は 7.1.6 で示す。

【関連する TSFI】
電源ボタン

(2) FPT_TUD_EXT.1 Trusted Update 高信頼アップデート
FMT_MTD.1 Management of TSF data TSF データの管理
FMT_SMF.1 Specification of Management Functions 管理機能の特定
システム管理者は、操作パネルからの操作により、操作パネル上で稼働中のファームウェアバージョンを確認することができる。また、機能設定リストを印字出力することによっても稼働中の TOE を構成するファームウェアのバージョンを確認することができる。
また、識別認証されたシステム管理者のみが、システム管理者クライアントの Web UI から、Controller ROM をパッケージしたバイナリファイルを TOE に送信することにより、ファームウェアをアップデートすることができる。
TOE は、システム管理者クライアントの Web UI から送信されるファームウェアを含むバイナリファイルを受信すると、バイナリファイルに添付された電子署名を検証し、検証に失敗した場合は、アップデートを中止し、操作パネルにエラー通知して停止する。バイナリファイルに付与されている電子署名は、バイナリファイルを SHA-256 でハッシュしたハッシュ値を鍵長 2048bit の秘密鍵で暗号化した RSASSA-PKCS1-v1.5 方式の RSA デジタル署名である。よって検証の手順は、1)バイナリファイルに添付された電子署名をファームウェア署名検証用 RSA 公開鍵にて復号、2)バイナリファイルを SHA-256 でハッシュ、3)復号結果とハッシュ値を比較し、一致すれば検証成功、不一致であれば検証失敗となる。

【FPT_TUD_EXT.1 に関連する TSFI】
操作パネルのファームウェアバージョン確認
Web UI のファームウェアアップデート機能

【FMT_MTD.1、FMT_SMF.1 に関連する TSFI】
Web UI のファームウェアアップデート機能

7.1.6. データ暗号化

(1) FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) 暗号鍵生成(非対称鍵用)

TOE は TLS 暗号通信の鍵確立(EC Diffie-Hellman)で用いる非対称鍵として、 [2]に記載の楕円曲線鍵を用いる。楕円曲線鍵の生成方法は、 [3]5.6.1.2.2 及び [2]Appendix B.4.2 に従う。TLS EC Diffie-Hellman 秘密値は、Linux の/dev/random から得た値をシードとする(14)に記載の AES-256 CTR DRBG で生成した乱数である。楕円曲線として [2]Appendix.D に記載の P-256、P-384、P-521 をサポートし、TLS ネゴシエーション通信で利用する一つが決まる。

TOE は TLS サーバ証明書に利用する非対称鍵として、 [2]に記載の楕円曲線鍵、もしくは、 [4]に記載の RSA 鍵を用いる。これらの非対称鍵は Web UI からのユーザー指示で生成される。楕円曲線鍵の生成方法は [3]5.6.1.2.2 及び [2]Appendix B.4.2 に従う。RSA 鍵は [4]6.3.1.3 節の生成方法に従い、その中で使われる素数は [2]の B.3.3 により生成される。楕円曲線として [2]Appendix.D に記載の P-256、P-384、P-521 を、RSA 鍵長として 2048bit、3072bit をサポートし、Web UI からユーザーがいずれか一つを指定して生成指示する。また、素数候補の乱数生成には(14)に記載の AES-256 CTR DRBG を用いる。

上記の鍵生成において、TOE 特有の拡張や代替の実装はない。

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI の管理機能
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(2) FCS_CKM.1(b) Cryptographic Key Generation (symmetric keys) 暗号鍵生成(対称鍵用)

TOE はストレージ暗号鍵及び高信頼通信のセッション鍵として、所望のビット数の乱数を用いる。具体的には、ストレージ暗号鍵(DEK: Data Encryption Key)の 256 ビット、DEK を暗号化するための鍵暗号鍵(KEK: Key Encryption Key)の 256 ビット、TLS セッション鍵のマスターとしてネゴシエーションで決定した暗号方式に応じて 128-256 ビットをそれぞれ生成する。乱数は(14)に記載の AES-256 CTR DRBG で生成する。なお、この DRBG が呼び出されるのは、(12)に記載した鍵チェインを生成する時点、及び、TLS 通信セッション開始時点である。

【関連する TSFI】

Web UI の識別認証
プリンタードライバ
Web UI の管理機能
電源ボタン
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(3) FCS_CKM.4 Cryptographic key destruction 暗号鍵破棄
FCS_CKM_EXT.4 Cryptographic Key Material Destruction 暗号鍵材料の破棄
TOE は平文保存される鍵及び鍵材料を不要になった時点で破棄する(*)。TOE に平文保存される鍵及び鍵材料とその破棄方法を Table 22 に示す。また、これらの鍵及び鍵材料は暗号処理の実行時に RAM 上のワークメモリへ値がコピーされて利用されるが、RAM 上のデータは TOE の電源断とともに不要となり削除される。

(*)ストレージ暗号鍵は NVRAM1 に保存されるが、(10)に記載の通り暗号化されるため、本要件の対象外とする。また、(1)に記載の TLS サーバ証明書に利用する非対称鍵は、(15)のメカニズムにより NVRAM1 上に暗号化して保存されるため、本要件の対象外とする。ファームウェア署名検証に用いる公開鍵は、秘密鍵、プライベート暗号鍵、暗号クリティカルセキュリティパラメタのいずれにも該当しないため本要件の対象外である。

【関連する TSFI】
操作パネルの管理機能
電源ボタン

Table 22 平文保存される鍵及び鍵材料の破棄方法

鍵種別	保存先	破棄方法と破棄理由
鍵暗号鍵 (KEK:Key Encryption Key)	NVRAM2	操作パネルの管理者メニューから工場出荷時の設定に戻す指示をした際、データを(14)に記載の DRBG で生成した乱数で1回上書きする。 工場出荷時の設定に戻すことはディスク上の全てのデータを破棄することを意味し、データ破棄後は暗号化対象パーティションを同じ暗号鍵で復号する必要がないため、DEK 及び KEK は不要になる。
TLS セッション鍵	RAM (揮発)	TOE の電源断で破棄する。 TOE は電源断の時点で有効な TLS セッションを閉じるため、TLS セッション鍵及び TLS EC Diffie Hellman 秘密値は不要になる。
TLS EC Diffie-Hellman 秘密値		

(4) FCS_COP.1(a)　Cryptographic Operation (Symmetric encryption/decryption)
暗号操作(対称鍵暗号化／復号)

TOE は TLS の対称鍵暗号/復号として [5]に記載の CBC モード及び [6]に記載の GCM モードの AES(128bit、256bit)をサポートする。AES は [7]準拠である。

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI の管理機能
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(5) FCS_COP.1(b1)　Cryptographic Operation (for signature generation/verification)　暗号操作(署名生成／検証)

TOE はファームウェアアップデートの真正性検証において、 [2]に記載の RSA デジタル署名をサポートする。鍵長は 2048bit である。 署名フォーマットは [2]5.5(f)に記載の RSASSA-PKCS1-v1.5 に従う。

【関連する TSFI】
Web UI のファームウェアアップデート機能

(6) FCS_COP.1(b2)　Cryptographic Operation (for signature generation/verification)　暗号操作(署名生成／検証)

TOE は TLS の相手認証、及び、電子署名生成/検証において、 [2]に記載の RSA デジタル署名及び楕円曲線デジタル署名に対応した署名生成及び検証を行う。なお、RSA 鍵長は 2048bit または 3072bit、NIST 楕円曲線は P256、P384、P521 をサポートする。RSA デジタル署名の署名フォーマットは [2]5.5(f)に記載の RSASSA-PKCS1-v1.5 に従う。また、楕円曲線デジタル署名の署名生成/検証は [2]6.4 に従う。これらは TLS 通信時には通信相手とのネゴシエーション、電子署名生成時にはユーザーの指定により、それぞれ使用する署名方式が決まる。

【関連する TSFI】
Web UI の管理機能
操作パネルのスキャン機能

(7) FCS_COP.1(c1)　Cryptographic operation (Hash Algorithm)　暗号操作（ハッシュアルゴリズム）

TOE は、ファームウェアアップデートの真正性検証時のファームウェアアップデートイメージデータのハッシュ計算に SHA256 を利用する。この SHA256 ハッシュ値と署名値の RSA 復号結果を比較することで署名検証を実行する。なお、ハッシュアルゴリズムは [8]に準拠する。

【関連する TSFI】
Web UI のファームウェアアップデート機能

(8) FCS_COP.1(c2) Cryptographic operation (Hash Algorithm) 暗号操作（ハッシュアルゴリズム）
TOE は(11)に記載の TLS における鍵付きメッセージ認証方式のハッシュ計算に SHA1/SHA256/SHA384 をサポートする。通信に使用するハッシュアルゴリズムは相手先とのネゴシエーションによって決定する。また、TOE は電子署名生成/検証のハッシュ計算に SHA256/SHA384/SHA512 をサポートし、署名生成時のユーザーの指定により使用するハッシュアルゴリズムが決定する。
TLS における鍵付きメッセージ認証方式のハッシュ計算と電子署名生成/検証のハッシュ計算は独立しており自由に組み合わせることができる。なお、ハッシュアルゴリズムは [8]に準拠する。

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI の管理機能
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(9) FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption) 暗号操作 （AES データ暗号化／復号）
TOE はストレージ暗号の暗号方式として、 [9]に記載された AES、及び、ブロック暗号モードとして [10]に記載された CBC をサポートする。 鍵長は 256 ビットである。IV はストレージのセクタ番号と DEK を元に算出する。

【関連する TSFI】
プリンタードライバ
操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、ファクス受信文書の印刷機能
操作パネルのジョブ状態・履歴の表示機能
公衆電話回線

(10) FCS_COP.1(f) Cryptographic operation (Key Encryption) 暗号操作（鍵暗号化）
TOE は(12)に記載の通り、ストレージ暗号化機能の DEK(256bit)を [9]に記載された AES 方式で暗号化する。鍵長は 256bit であり、ブロック暗号モードは [10]に記載された CBC をサポートする。鍵長は 256 ビットである。IV は(14)に記載の AES-256 CTR DRBG から得た乱数である。
(12)に記載の通り、ストレージ暗号化機能の DEK(256bit)を暗号化するのは、ストレージ暗号鍵チェインがない TOE の初回起動時である。

【関連する TSFI】
電源ボタン

(11) FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) 暗号操作(鍵付ハッシュメッセージ認証)

TOE は TLS における鍵付きメッセージ認証方式として以下をサポートする。

- 鍵長(bit):160、256、384
- ハッシュ:SHA-1、SHA-256、SHA-384
- メッセージダイジェスト長(bit):160、256、384

ハッシュアルゴリズムは [11]、鍵付きハッシュメッセージ認証アルゴリズム(HMAC)は [12]に準拠する。

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI の管理機能
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(12) FCS_KYC_EXT.1 Key Chaining 鍵チェイン

TOE はストレージ暗号鍵(DEK)及び DEK を暗号化するための鍵暗号鍵(KEK)を鍵チェインとする。具体的には TOE はストレージ暗号鍵チェインがない起動時(具体的には、工場生産初回起動時、または、操作パネルの管理者メニューから工場出荷時の設定に戻す操作をした後の起動時)に(14)に記載の DRBG で DEK と KEK を生成し、DEK は KEK により(10)に従って暗号化し NVRAM1 に、KEK は平文状態で NVRAM2 に、それぞれ保存する。2 回目以降の起動時は、NVRAM1 に暗号化して保存した DEK を NVRAM2 から読み出した KEK で(10)に従って復号する。鍵長は DEK、KEK ともに 256 ビットである。DRBG には(14)に記載した通り十分なエントロピーが供給されるため鍵の強度は 256 ビットであり、鍵チェインの中で 256bit 強度が維持される。

【関連する TSFI】
電源ボタン

(13) FPT_KYP_EXT.1 Protection of Key and Key Material 鍵及び鍵材料の保護

TOE は(12)に記載した通り、ストレージ暗号鍵チェインがない TOE の初回起動時に後述の DRBG で DEK と KEK を生成し、DEK は KEK で暗号化されて NVRAM1 に、KEK は平文状態で NVRAM2 にそれぞれ保存する。その他のストレージに DEK、KEK が保存されることはない。NVRAM2 は現地交換不可能ストレージであるため、(12)の鍵チェインの一部が現地交換可能なストレージに平文で保存されることはない。

【関連する TSFI】

電源ボタン

(14) FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) 暗号操作（乱数ビット生成）

TOE は乱数生成に [1]10.2.1 に準拠した AES-256 CTR DRBG を利用する。この DRBG は Derivation Function、Reseed 機能を有し、Prediction Resistance 機能を持たない。また、Linux カーネルの/dev/random から得た乱数をシードとする。/dev/random の提供元である Linux Random Number Generator(LRNG)及び LRNG に注入するクロックカウンタの読み出し間隔ノイズを含めた全体をエントロピー源とする。このノイズはソフトウェアにより意図的に間隔のばらつきを発生するものである。DRBG は/dev/random から供給されたシードを entropy_input 及び nonce として利用するが、乱数のエントロピー量は 256 ビット×1.5 を超え、 [1]8.6.7 の基準から十分と言える。

TOE はこの DRBG を用いてストレージ暗号鍵、TLS セッション鍵を導出する。

(12)に記載の通り、ストレージ暗号鍵導出のために DRBG が起動されるのは、ストレージ暗号鍵チェインがない TOE の初回起動時である。

【関連する TSFI】

Web UI の識別認証
プリンタードライバ
Web UI の管理機能
電源ボタン
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(15) FDP_DSK_EXT.1 Protection of Data on Disk ディスク上のデータ保護

TOE はストレージデバイス上のデータブロック単位で暗号化/復号化する。具体的には、ストレージデバイス上の暗号化対象パーティションに対するファイル及びメタデータの Read/Write を仲介してデータの復号化/暗号化を施し、当該パーティションに対してデータブロックを Read/Write する。暗号化方式は FCS_COP.1(d)に従う。暗号化対象パーティションを含むストレージデバイスは現地交換可能な NVRAM1 であり、NVRAM1 以外に現地交換可能なストレージデバイスはない。

上記のストレージ暗号化は、TOE 起動時から動作する。暗号化/復号化に利用する DEK は(12)に記載した通り、暗号鍵チェインがない起動時に生成される。

全ての平文の利用者データ、平文の秘密の TSF データは NVRAM1 上の暗号化対象パーティションに書き込まれるため暗号化される。NVRAM1 上の非暗号化対象のパーティションには、プログラムイメージ、制御パラメータや KEK を鍵とし(10)に記載の通り暗号化された DEK のみが格納され、平文の利用者文書データ及び平文の秘密の TSF データを含まない。なお、DEK の暗号化は(12)に記載した通り TOE の暗号鍵チェインがない起動時に行われる。また、平文 KEK の保存先である NVRAM2 は現地交換可能なストレージデバイスではない。

【関連する TSFI】

プリンタードライバ
電源ボタン
操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、ファクス受信文書の印刷機能
操作パネルのジョブ状態・履歴の表示機能
公衆電話回線

7.1.7. 高信頼通信

(1) FCS_HTTPS_EXT.1 HTTPS selected 選択された HTTPS

Web ブラウザ、ならびに監査サーバとの全ての通信トラフィックを HTTPS でセキュアチャネル化するように強制する設定が可能である。この設定は Web UI から管理者のみが行える。HTTPS は [13]に従った実装である。

クライアント PC の Web ブラウザから接続要求を受けると、TOE とクライアント PC 間で TLS 通信のネゴシエーションを確立し、HTTPS 通信を開始する。クライアント PC からの TOE の Web UI における識別認証およびすべてのリモート操作に対して、HTTPS 通信が適用される。また、監査サーバから監査ログデータ取得要求を受け、監査ログデータを監査サーバに送出する際、HTTPS 通信が適用される。

【関連する TSFI】
Web UI の識別認証
Web UI の管理機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(2) FCS_TLS_EXT.1 TLS selected 選択された TLS

TLS 通信として [14]の TLS1.2 をサポートする。

TLS 通信で使用する暗号スイートがクライアント・サーバ間の TLS コネクション中にネゴシエートされる。

TOE は TLS を利用する通信においては、TOE は機能に応じてクライアントにもサーバにもなり得る。例えば、Web UI アクセスではサーバ、スキャン文書メール送信時にはクライアントとして振る舞う。

TOE はクライアントから提案された暗号スイートの中からサポートする適切なものを 1 つ選択する。TOE がサポートする暗号スイートは以下である。

- 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
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_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_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- 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

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI の管理機能
操作パネルのスキャン機能
Web UI のジョブ状態・履歴の表示機能
外部監査サーバ
Web UI のファームウェアアップデート機能

(3) FTP_ITC.1 Inter-TSF trusted channel TSF 間高信頼チャネル
TOE は TOE と監査サーバ、Mail サーバとの間で、以下の高信頼通信プロトコルをサポートする。これにより、エンドポイントの識別と通信データの暴露と改ざんからの保護が保証される。

- 監査サーバ: TLS/HTTPS
- Mail サーバ: TLS

【関連する TSFI】
外部監査サーバ
操作パネルのスキャン機能（Mail サーバ）

(4) FTP_TRP.1(a) Trusted path (for Administrators) 高信頼パス（管理者用）
TOE は管理者のリモートPCからの各アクセスインタフェースに対し、以下の高信頼通信プロトコルをサポートする。これにより、エンドポイントの識別と通信データの暴露と改ざんからの保護が保証される。

- Web UI: TLS/HTTPS

【関連する TSFI】
Web UI の識別認証
Web UI の管理機能
Web UI のジョブ状態・履歴の表示機能
Web UI のファームウェアアップデート機能

(5) FTP_TRP.1(b) Trusted path (for Non-administrators) 高信頼パス（非管理者用）
TOE は非管理者のリモートPCからの各アクセスインタフェースに対し、以下の高信頼通信プロトコルをサポートする。これにより、エンドポイントの識別と通信データの暴露と改ざんからの保護が保証される。

- Web UI: TLS/HTTPS
- プリンタードライバからの印刷: TLS

【関連する TSFI】
Web UI の識別認証
プリンタードライバ
Web UI のジョブ状態・履歴の表示機能

7.1.8. PSTN ファクス-ネットワーク間の分離

(1) FDP_FXS_EXT.1 Fax separation ファクス分離

TOE は、ファクスモデム機能を持ち、公衆電話回線を介して、ファクスデータの送受信機能を提供する。
サポートするプロトコルは ITU-T G3 モードのみである。
ファクスインタフェースで送受信が許されているのは、利用者のファクシミリ文書のみである。
データモデム機能は持たず、外部からの各種データ通信コマンドは一切受け付けないため、ファクス回線から TOE に不正にアクセスすることはできない。また、TOE は、公衆電話回線網と内部ネットワーク間でデータを受け渡す機能をもたないため、公衆電話回線受信が受信した公衆回線データは内部ネットワーク送信に渡らない。

【関連する TSFI】
公衆電話回線

8. ST 略語・用語 (Acronyms And Terminology)

8.1. 略語 (Acronyms)

本 ST における略語を以下に説明する。

略語	定義内容
CC	コモンクライテリア(Common Criteria)
DRAM	ダイナミックランダムアクセスメモリ(Dynamic Randam Access Memory)
FIPS PUB	米国の連邦情報処理標準の出版物(Federal Information Processing Standard publication)
IIT	画像入力ターミナル(Image Input Terminal)
MFD	デジタル複合機(Multi Function Device)
NVRAM	不揮発性ランダムアクセスメモリ(Non Volatile Random Access Memory)
PDL	ページ記述言語(Page Description Language)
PP	プロテクションプロファイル(Protection Profile)
SFP	セキュリティ機能方針(Security Function Policy)
SFR	セキュリティ機能要件(Security Functional Requirement)
SMTP	電子メール送信プロトコル(Simple Mail Transfer Protocol)
ST	セキュリティターゲット(Security Target)
TOE	評価対象(Target of Evaluation)
TSF	TOE セキュリティ機能(TOE Security Function)

8.2. 用語（Terminology）

本 ST における用語を以下に説明する。

用語	説明
破棄する	ファイルシステム、揮発性メモリから対象の関連を辿れないように消去することを指す。
KEK	Key Encryption Key の略。本書では、ストレージ暗号鍵を暗号化するための暗号鍵のことを指す。
DEK	Data Encryption Key の略。本書では、ストレージ暗号鍵のことを指す。
フラッシュメモリ	SD または eMMC を指す。
Web UI	利用者クライアントの Web ブラウザを介して、TOE に対する操作ができるインタフェースである。
ファクス受信ボックス (Faxbox)	ファクス受信ボックスとはファクス受信文書を TOE 内に保存する場所のこと。 またファクス受信ボックスに格納されたファクス受信文書を印刷することが可能である。
Secure Print	プリント機能において、印刷データをデコンポーズして作成したビットマップデータを、MFD のストレージ装置に一旦蓄積し、認証された利用者が操作パネルより指示する事で印刷を開始するプリント方法。
利用済み文書データ	MFD のストレージ装置に蓄積された後、利用が終了しファイルは削除されるが、ストレージ装置内にはデータ部は残存している状態の文書データ。
文書データ (Document data)	一般利用者(U.NORMAL)、SA が MFD のコピー機能、プリント機能、スキャン機能、ファクス機能を利用する際に、MFD 内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。
スキャン文書	スキャン機能によって、電子形式へ変換された文書データ。本 TOE はスキャン文書を Mail サーバへ送信する機能を持つ。
ファクス受信文書	ファクス機能によって受信され、本 TOE で扱われる電子形式の文書データである。本 TOE では、設置時の設定により、受信したファクスデータをファクス受信ボックスに保存することができる。
監査ログ	いつ、誰が、どのような作業を行ったかという事象（例えば、ユーザー操作、障害や構成変更など)を、追跡記録されたデータ。
利用者役割 (User Role)	識別認証した利用者に割り当てられる役割。本 TOE では、機械管理者役割、SA 役割、一般利用者役割が定義されている。
機械管理者役割（Key Operator role）	機械管理者が TOE を利用する際に必要な権限を表す。SFR 内では Key Operator role と表現される。
SA 役割（SA role）	SA が TOE を利用する際に必要な権限を表す。
一般利用者役割（U.NORMAL role）	一般利用者(U.NORMAL)が TOE を利用する際に必要な権限を表す。
利用者識別情報 (User Identifier)	利用者を識別するための情報。ユーザーID。
機械管理者識別情報	機械管理者役割を割り当てられたユーザーID。SFR 内では Key Operator Identifier と表現される。

（Key Operator identifier）	
機械管理者（Key Operator）	MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。
SA	機械管理者あるいは既に作成された SA がアカウントを作成することができ、MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。
システム管理者（U.ADMIN）	Key Operator と SA の総称。
ユーザー認証 (User Authentication)	TOE の各機能を使用する前に、利用者の識別認証を行って TOE の利用範囲に制限をかけるための機能である。 外部認証オプションをインストールすることにより、本体認証と外部認証の2つのモードをサポートするが、本 TOE では本体認証モードで動作する。
本体認証 (Local Authentication)	TOE のユーザー認証を MFD に登録したユーザー情報を使用して認証管理を行うモード。
外部認証 (Remote Authentication)	TOE のユーザー認証を外部認証サーバに登録したユーザー情報を使用して認証管理を行うモード。
ストレージ暗号	保護資産の一部を保存するストレージを暗号化する機能を示す。
デコンポーズ機能	ページ記述言語(PDL)で構成された印刷データを解析し、ビットマップデータに変換する機能。
デコンポーズ	デコンポーズ機能により、ページ記述言語(PDL)で構成されたデータを解析し、ビットマップデータに変換する事。
オートクリア機能 (Auto Clear)	操作パネルおよび Web UI から何も操作をしない状態で一定の時間が経過したとき、自動的に認証がログアウトされる機能である。
カストマーエンジニア (Customer Engineer)	MFD の保守/修理を行うエンジニア。
攻撃者 (attacker)	攻撃者とは、TOE または保護されている資産に不正な手段を講じてアクセスする者である。 攻撃者には、承認された利用者ではあるが、その正体を隠してアクセスする者も含まれる。
操作パネル (Control Panel)	MFD の操作に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネル。
一般利用者クライアント	一般利用者が利用するクライアント。
システム管理者クライアント	システム管理者が利用するクライアント。 システム管理者は Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う。
プリンタードライバ (Printer driver)	一般利用者クライアント上のデータを、MFD が解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウェアで、利用者クライアントで使用する。
印刷データ	MFD が解釈可能なページ記述言語(PDL)で構成されたデータ。 印刷データは、TOE のデコンポーズ機能でビットマップデータに変換される。

ビットマップデータ	コピー機能により読み込まれたデータ、およびプリント機能により利用者クライアントから送信された印刷データをデコンポーズ機能で変換したデータ。 ビットマップデータは独自方式で画像圧縮してストレージ装置に格納される。
原稿	コピー機能で IIT からの読み込みの対象となる文章や絵画、写真などを示す。
TOE 設定データ	これは TSF データの一部であり、TOE によって作成されたか TOE に関して作成されたデータであり、TOE のセキュリティ機能に影響を与える可能性のある設定データ。
暗号鍵	自動生成される 256 ビットのデータ。 ストレージ装置への文書データの保存時に、この鍵データを使用して暗号化を行う。
ネットワーク	外部ネットワークと内部ネットワークを包含する一般的に使用する場合の表現。
外部ネットワーク	TOE を管理する組織では管理が出来ない、内部ネットワーク以外のネットワークを指す。
内部ネットワーク	TOE が設置される組織の内部にあり、外部ネットワークからのセキュリティの脅威に対して保護されているネットワーク内の、MFD と MFD へアクセスが必要なリモートの高信頼なサーバやクライアント PC 間のチャネルを指す。
公衆電話回線 公衆電話回線網 PSTN (public telephone line)	ファクス送信、ファクス受信のデータが流れる回線と構成される網。
公衆回線データ (fax data)	ファクスの公衆回線網を流れる送受信のデータ。
証明書	ITU-T 勧告の X.509 に定義されており、本人情報(所属組織、識別名、名前等)、公開鍵、有効期限、シリアルナンバ、シグネチャ等が含まれている情報。
Data on minimum user password length	TOE 設定データであり、本体認証時における利用者のパスワード設定時の最小文字数の情報
Key operator Password	TOE 設定データであり、機械管理者認証のためのパスワード情報
SA Password	TOE 設定データであり、SA 認証のためのパスワード情報
U.Normal Password	TOE 設定データであり、一般利用者(U.NORMAL)認証のためのパスワード情報
Data on access denial due to authentication failures	TOE 設定データであり、利用者 ID 認証失敗に関係する機能の有効/無効の情報と失敗回数情報
Data on Auditing	TOE 設定データであり、いつ、誰が、どのような作業を行ったかという事象(例えば、ユーザー操作、障害や構成変更など)を、追跡記録する機能の有効/無効の情報。
Data on User Authentication	TOE 設定データであり、MFD のコピー機能、スキャン機能、ファクス機能およびプリント機能を利用する際に、ユーザー認証情報にて認証する機能の有効/無効および設定の情報。
Data on Secure Print	TOE 設定データであり、プリントデータ受信時にSecure Printに蓄積させるか印刷させるかの設定情報。

Data on Trusted communications	TOE 設定データであり、内部ネットワーク上に存在する文書データ、ジョブ情報、監査ログおよび TOE 設定データといった通信データを保護するために対応する一般的な暗号化通信プロトコルの有効/無効および設定の情報および証明書、認証用/暗号化パスワード、共通鍵パスワード情報。
Data on Customer Engineer Operation Restriction	TOE 設定データであり、カストマーエンジニア操作制限機能の有効/無効の情報及び保守パスワードの情報。
Data on date and time	TOE 設定データであり、タイムゾーン/サマータイム設定情報と現在時刻データである。
Data on Auto Clear	TOE 設定データであり、操作パネルオートクリア機能の有効/無効およびクリア時間の情報、および Web UI のオートクリア機能の有効/無効の情報およびクリア時間の情報。
Data on Self Test	TOE 設定データであり、自己テスト機能の有効/無効の情報。
Data on Report Print	TOE 設定データであり、レポート出力機能の設定情報。
Data on Firmwareupdate	TOE 設定データであり、ファームウェアアップデート機能の設定情報。

9. 参照文献

[1] E. Barker , J. Kelsey, “SP 800-90A Rev.1 Recommendation for Random Number Generation UsingDeterministic Random Bit Generators,” June 2015.

[2] National Institute of Standards and Technology, “FIPS 186-4 Digital Signature Standard (DSS),” July 2013.

[3] E. Barker, L. Chen, A. Roginsky, A. Vassilev , R. Davis, “SP 800-56A Rev. 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography,” April 2018.

[4] E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis , S. Simon, “SP 800-56B Rev. 2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography,” March 2019.

[5] M. Dworkin, “SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques,” December 2001.

[6] M. Dworkin, “SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,” November 2007.

[7] National Institute of Standards and Technology, “FIPS 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES),” November 2001.

[8] “ISO/IEC 10118-3:2004,” March 2004.

[9] “ISO/IEC 18033-3:2010,” December 2010.

[10] “ISO/IEC 10116:2017,” July 2017.

[11] National Institute of Standards and Technology, “FIPS 180-3 Secure Hash Standard (SHS),” March 2012.

[12] National Institute of Standards and Technology, “FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC),” July 2008.

[13] “RFC2818 HTTP Over TLS,” May 2000.

[14] “RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.