SHARP

MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U

セキュリティターゲット

Version 1.04

シャープ株式会社

履歴

日付	Ver.	変更点	承認者	作成者
2017-10-18	0.90	• 初版作成	中平	小川
2017-12-01	1.00	• 誤記修正	中平	小川
2018-01-10	1.01	• ガイダンスのバージョン変更	中平	小川
2018-01-18	1.02	• TOEバージョンの変更	中平	小川
2018-02-13	1.03	• 指摘事項修正	中平	小川
2018-03-27	1.04	• ガイダンスのバージョン変更	中平	小川

目次

表のリスト

図のリスト

1 ST 概説

本書は、MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U のセキュリティについて述べたセキュリティターゲット (ST) である。MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U は、2.1 節に示す IT セキュリティ国際標準 (コモンクライテリア、CC) に基づき、本 ST への適合を主張する CC 評価対象 (TOE) である。本 ST では、8.1 節および 8.2 節に示す用語を使用している。本 ST は、2.1 節に示す PP への適合を主張する。

本章では、本 ST および TOE に関し、ST 参照、TOE 参照、TOE 概要、および TOE 記述を記載する。

1.1 ST 参照

本セキュリティターゲット (ST) を識別するための情報を記載する。

名称: MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U セキュリティターゲット

バージョン: 1.04

発行日: 2018-03-27

作成者: シャープ株式会社

1.2 TOE 参照

本 ST への適合を主張する CC 評価対象 (TOE) を識別するための情報を記載する。

TOE 全体を、次のとおり識別する。

名称: MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U

バージョン: 0210zc00

開発者: シャープ株式会社

上記 TOE は、Table 1.1 に示す本体および必須オプションの組み合わせから成る。

Table 1.1: TOE構成要素

本体			必須オプション
型番	ファクス機能	販売地域	
MX-M3070, MX-M3570, MX-M4070, MX-M5070, or MX-M6070	オプション	日本以外	MX-FR57U

1.3 TOE 概要

1.3.1 TOE の種別

本 TOE は IT 製品であり、コピー機能、プリンター機能、スキャナー機能に加え、文書を保存/取り出す機能 (本 TOE では、ドキュメントファイリング機能と称す) を備えたデジタル複合機 (Multifunction device: 略称 MFD) である。

1.3.2 TOE の使用法

TOE は、ローカルエリアネットワーク (LAN) に接続されて、ネットワーク環境で使用される。ネットワーク環境では、ファイアウォールにより外部ネットワークの不正アクセスから保護された内部ネットワークでクライアント PC、サーバーと接続されて使用されることを想定している。

この利用環境において、利用者は、TOE が備える操作パネル、または LAN を介したクライアント PC からの通信によって、TOE を操作することができる。

TOE の主な使用用途は、以下に示すとおりである。

- 紙文書をスキャンして読み込んだ文書データを複写印刷する (コピー機能)
- クライアント PC から文書データを送信して印刷する (プリンター機能)
- 紙文書をスキャンして読み込んだ文書データを、クライアント PC や FTP サーバーに送信する (スキャナー機能)
- 紙文書をスキャンして読み込んだ文書データや外部より受信した文書データを TOE 内に保存し、後にそれらを取り出して印刷、または送信する (ドキュメントファイリング機能)
- 操作パネルから MFD の各種設定を行う
- クライアント PC 上の Web ブラウザーから MFD の各種設定を行う (Web ページ設定)

1.3.3 TOE の主要なセキュリティ機能

TOE は、文書データを TOE 内に蓄積、または LAN に接続された IT 機器との間で送受信する。TOE は、これら文書データや TOE 内に保存される秘密のシステム情報等を不正な暴露や改ざんから保護するため、以下に記すようなセキュリティ機能を備える。

- 識別認証機能: TOE を利用しようとする者が TOE の許可利用者であるかを識別認証する機能
- アクセス制御機能: TOE 内に保存されたデータへのアクセスを制限する機能
- 蓄積データ暗号化機能: TOE 内の現地交換可能な不揮発性ストレージデバイス上のデータを暗号化する機能
- ネットワーク保護機能: LAN 利用時に通信経路上を保護する機能
- セキュリティ管理機能: TSF データに対する操作を管理者のみに制限する機能
- 監査機能: TOE の使用およびセキュリティに関連する事象のログを記録し、監査する機能
- ソフトウェア検証機能: TOE のソフトウェアアップデート前にファームウェアの真正性を検証する機能
- 自己テスト機能: TOE 起動時に TSF の正常動作を実証する機能
- 残存情報消去機能: 残存情報を上書き消去して再利用を防止する機能
- データ完全消去機能: すべての利用者データおよび TSF データを完全消去する機能

1.3.4 要求される TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE の一般的な利用環境を Figure 1 に示す。

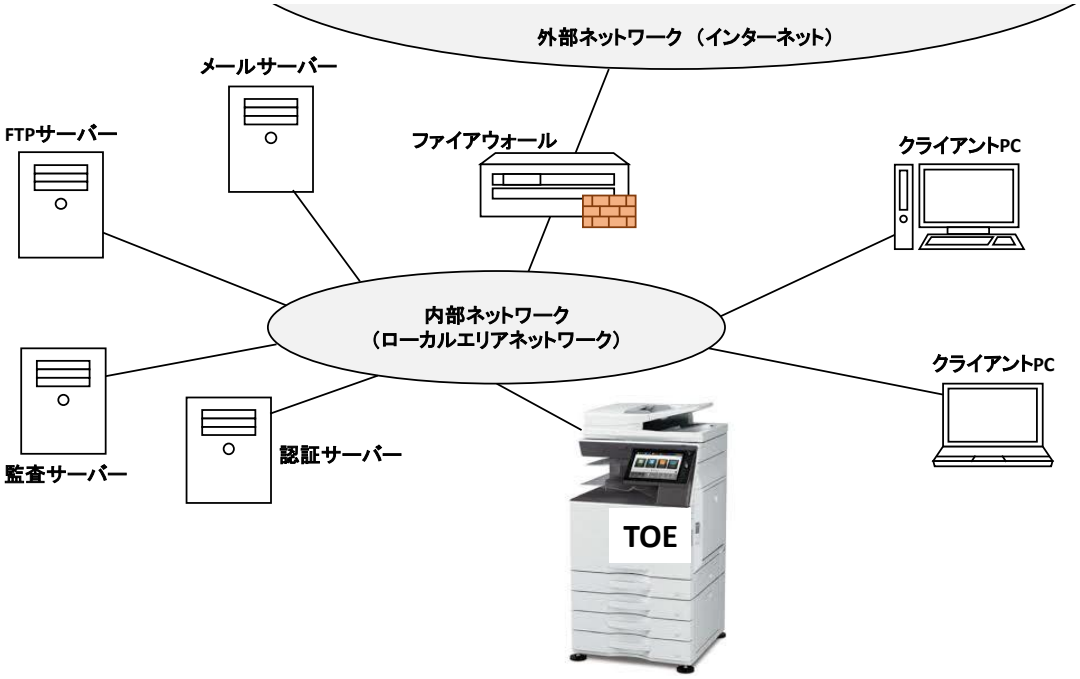

Figure 1: TOE の利用環境

TOE の動作には、少なくともローカルエリアネットワークおよび syslog プロトコルを使用して TLS v1.2 に対応している監査サーバーが必要である。TOE 評価では rsyslog で構成された監査サーバーを使用する。TOE の機能を利用するにあたり必要となるハードウェア、ソフトウェア、またはファームウェアについては、Table1.3 に示す。なお、各種サーバーおよび Web ブラウザーは TLS v1.2 に対応している必要があり、プリンタードライバーは IPP-SSL 機能の使用が必要である。
また、TOE を外部ネットワークに接続するためには、ファイアウォールを設置して外部ネットワークの不正アクセスから TOE を保護する必要がある。

Table 1.2: TOE 機能利用に必要なハードウェア/ソフトウェア/ファームウェア

TOE 機能	必要なハードウェア/ソフトウェア/ファームウェア	TOE 評価で使用した構成
ネットワーク認証	認証サーバー	openLDAP (2.4)
Web ページ設定	クライアント PC	Windows 8.1
	Web ブラウザー	Internet Explorer 11
プリンタードライバーからのプリント	クライアント PC	Windows 8.1
	プリンタードライバー	SHARP <本体名> PCL6 ドライバー
E-mail 送信スキャン	メールサーバー	Postfix (2.10)
ファイルサーバー送信スキャン	FTP サーバー	Windows 8.1 に搭載の Microsoft Internet Information Services

1.4 TOE 記述

1.4.1 TOE の物理的構成

TOE の物理的範囲は Figure 2 に示す MFD 全体であり、操作パネル、スキャナーユニット、エンジンユニット、コントローラーユニット、内部ストレージで構成される。これは、Table 1.1 に示す MFD 本体のいずれかに対応する必須オプションを取り付けた後、ガイダンスの指示に従い、高度なセキュリティの設定を実行したものである。なお、MFD にフィニッシャーや給紙トレイ等を追加することも可能であるが、それらは TOE に含まない。

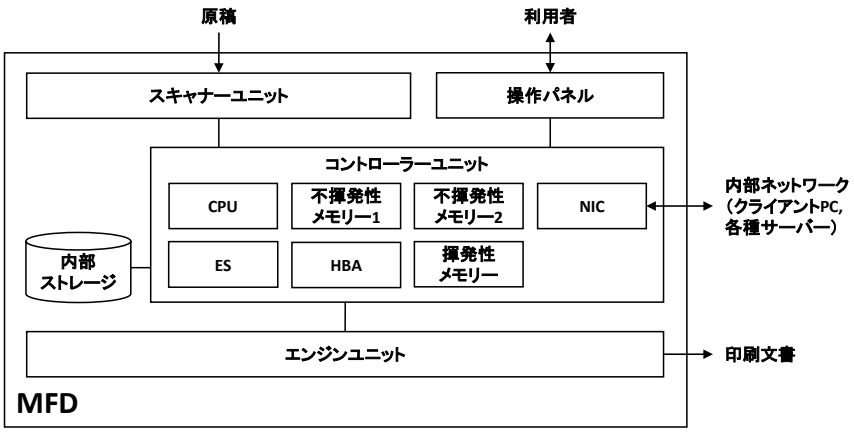

Figure 2: TOE の物理的構成

- 操作パネル: タッチパネル液晶ディスプレイ、ハードキー、LED を備えた TOE を操作するためのコントロール装置。
- スキャナーユニット: 紙文書を読み込み電子データに変換するための装置。スキャナー動作の制御を行うスキャナー制御ファームウェアが、本装置内の ROM に格納されている。なお、ファームウェアは、必須オプションの MX-FR57U が取り付けられる際にアップデートされる。

- エンジンユニット: 給紙機能、排紙機能の機構を含み、紙文書を印刷し排出するための装置。プリント動作の制御を行うプリント制御ファームウェアが、本装置内の ROM に格納されている。なお、ファームウェアは、必須オプションの MX-FR57U が取り付けられる際にアップデートされる。
- コントローラーユニット: 以下に示す TOE のファームウェアを実行するための集積回路や記憶装置等を備えた、MFD 全体を制御するための装置。
  - CPU: MFD 動作における基本的な演算処理を行う中央演算処理装置。
  - 揮発性メモリー: 作業領域として利用される、揮発性の記憶装置。
  - NIC: Ethernet (10Base-T, 100Base-TX, 1000Base-T) をサポートしたネットワークインタフェース装置。
  - HBA (ホストバスアダプタ): コントローラーユニットと内部ストレージを接続する、暗号回路を搭載したインタフェース装置。
  - ES (エントロピー源): 乱数発生器を初期化するために使用する、ランダムビット列を発生する回路。
  - 不揮発性メモリー1: MFD 本体の Boot 制御を行う本体制御ファームウェア、および鍵暗号化に使用する鍵暗号鍵を格納する、基板上に半田付けされた不揮発性の記憶装置。なお、ファームウェアは、必須オプションの MX-FR57U が取り付けられる際にアップデートされる。
  - 不揮発性メモリー2: 内部ストレージ上の利用者データおよび TSF データの暗号化に使用する暗号鍵を格納する、不揮発性の記憶装置。格納される暗号鍵は、不揮発性メモリー1 に格納された鍵暗号鍵によって鍵暗号化されている。本装置は、必須オプションの MX-FR57U によって取り付けられる。
- 内部ストレージ: 文書データ等の利用者データ、TSF データ、および MFD 本体のメイン制御を行う本体制御ファームウェアを格納する、現地交換可能な不揮発性の記憶装置。HDD および eMMC から構成されている。なお、ファームウェアは、必須オプションの MX-FR57U が取り付けられる際にアップデートされる。

1.4.2 ガイダンス

本 TOE を構成するガイダンスの一覧を Table 1.3 に示す。

Table 1.3: TOE を構成するガイダンス

名称	バージョン	言語
Start Guide	TINSX5397FCZZ YT1	英語
Quick Start Guide	2018B-EX1	英語
User's Manual	2018B-EX1	英語
Web Page Settings Guide	2017H-EN1	英語
Software Setup Guide	2017L-EN1	英語
Troubleshooting	2018B-EN1	英語
MX-FR57U Data Security Kit Operation Guide	EX1	英語
MX-FR57U Data Security Kit Notice	2.0	英語
How to set up MX-FR57U to be the "Protection Profile for Hardcopy Devices" compliant	V1.0	英語

1.4.3 TOE の論理的構成

TOE の論理的構成を Figure 3 に示す。TOE のセキュリティ機能は網掛けで示す部分である。

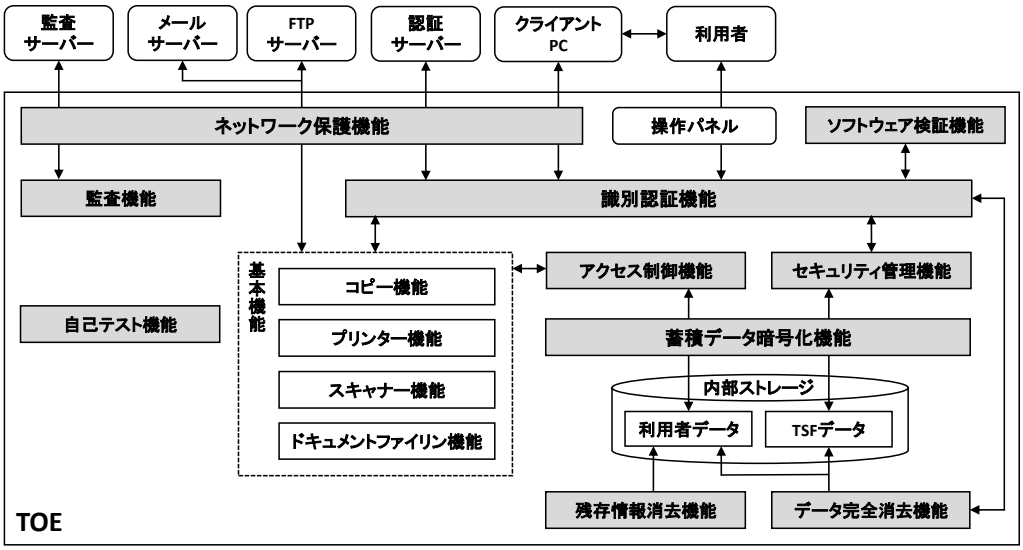

Figure 3: TOE の論理的構成

1.4.3.1 TOE が提供する基本機能

TOE は、基本機能として以下に示す機能を提供する。

- コピー機能
  利用者による操作パネルからの操作によって、紙文書をスキャンして読み込んだ文書データを複写印刷する機能。
- プリンター機能
  LAN 経由で外部から受信した文書データを印刷する機能で、プリンタードライバーによるプリント機能からなる。
  プリンタードライバーによるプリント機能は、クライアント PC のプリンタードライバーから送信された文書データを受信し、利用者による操作パネルからの操作によって印刷する機能である。
- スキャナー機能
  利用者による操作パネルからの操作によって、紙文書をスキャンして読み込んだ文書データをクライアント PC、または FTP サーバーに送信する機能。
  送信方法は、以下に示すとおりで、管理者が TOE 内のアドレス帳に登録している E-mail アドレスおよび FTP サーバーに対してのみ送信を行うことができる。
  - E-mail 送信: E-mail 添付ファイルとして指定のアドレスに送信
  - ファイルサーバー送信: 指定の FTP サーバーに送信
- ドキュメントファイリング機能
  内部ストレージに文書データを保存し、利用者による操作パネルからの操作、または LAN 経由によるクライアント PC からの操作によって、保存されたデータを再操作する機能で、ファイリング機能、スキャン保存機能、再操作機能からなる。
  ファイリング機能は、利用者がコピー機能、プリンター機能、またはスキャナー機能を使用する際、印刷、または送信する文書データを同時に内部ストレージに保存する機能である。
  スキャン保存機能は、利用者による操作パネルからの操作によって、紙文書をスキャンして読み込んだ文書データを内部ストレージに保存する機能である。この機能では保存のみを行い、印刷および送信は行わない。
  再操作機能は、利用者が内部ストレージに保存された文書データを取り出し、以下に示す操作を行う機能である。
  - 印刷: 利用者による操作パネルからの操作によって、文書データを紙文書に印刷する
  - 送信: 利用者による操作パネルからの操作によって、文書データを E-mail 送信、またはファイルサーバー送信する

- プレビュー: 利用者による操作パネルからの操作、または LAN 経由によるクライアント PC からの操作によって、文書データの概略を表示する
- 削除: 利用者による操作パネルからの操作、または LAN 経由によるクライアント PC からの操作によって、不要になった文書データを内部ストレージから取り除き、上書き消去する

1.4.3.2 TOE が提供するセキュリティ機能

TOE は、セキュリティ機能として以下に示す機能を提供する。

- 識別認証機能
  TOE を利用しようとする者が TOE の許可利用者であるかをログイン名とパスワードによって検証し、TOE の許可利用者であることが確認できた場合に TOE の利用を許可する機能。
  検証方法には、TOE 内の利用者登録による内部認証と、外部の認証サーバーを利用したネットワーク認証がある。
  本機能には、操作パネルからパスワードを入力する際にパスワードをダミー文字で表示する機能が含まれる。さらに、連続した認証失敗回数が設定値に達した場合に認証機能をロックする機能、パスワードの品質を保護するために管理者が予め設定したパスワードの最小桁数等の条件を満たしたパスワードだけを登録する機能、ログイン(識別認証)後に一定時間無操作状態が続いた場合に自動的にログアウトする機能も本機能に含まれる。
- アクセス制御機能
  TOE 内の保護資産に対し、許可された利用者のみがアクセス可能となるように、保護資産へのアクセスを制限する機能。
- 蓄積データ暗号化機能
  内部ストレージに保存された保護資産を不正アクセスから保護するため、それらを暗号化する機能。
  本機能には、暗号鍵を生成する機能も含まれる。暗号鍵は、TOE 起動毎に不揮発性メモリー2 に格納された鍵暗号化された暗号鍵を不揮発性メモリー1に格納された鍵暗号鍵を使用して復号することで生成され、揮発性メモリーに保存される。
- ネットワーク保護機能
  LAN 利用時にネットワーク上を流れる通信データが盗聴などにより漏洩、改ざんされることを防止するため、通信経路上を保護する機能。
  クライアントPC、監査サーバー、認証サーバー、FTP サーバー、およびメールサーバーと通信する際、接続先の正当性を検証し、ネットワーク上を流れる保護資産を暗号化することで保護する。
- セキュリティ管理機能
  認証識別機能により認証された TOE の管理者のみが、操作パネル、または LAN 経由によるクライアント PC から以下に示す TSF データの操作を行えることを制御する機能。
  - 内部認証利用者の登録/削除
  - 内部認証利用者の利用者ログイン名/パスワード/役割の変更 (ただし、パスワードは利用者自身でも変更可能)
  - 利用者パスワードの最小パスワード長の変更
  - 識別認証方式の変更
  - 権限グループの登録/変更/削除
  - 日付/時刻の変更
  - 監査ログ送信先の問い合わせ/変更
  - 自動ログアウト時間の問い合わせ/変更
  - アドレス帳データの登録/変更/削除
  - 利用可能な LDAP 認証サーバーの登録/変更/削除
  - IP アドレス設定の変更
  - メール送信サーバー設定の問い合わせ/変更
- 監査機能
  TOE の使用およびセキュリティに関連する事象のログを日時情報等とともに監査ログとして記録し、記録した監査ログを監査できる形式で提供する機能。

記録した監査ログは、ネットワーク保護機能を使用して監査サーバーに送信され、監査サーバーから閲覧することができる。

- ソフトウェア検証機能
  TOE のファームウェアアップデートを開始する前に、アップデート対象のファームウェアの真正性を検証し、それが正規のものであることを確認する機能。
- 自己テスト機能
  TOE 起動時に TSF 実行コードおよび TSF データの完全性を検証し、TSF の正常動作を実証する機能。
- 残存情報消去機能
  残存情報の再利用を不可能な状態にするため、内部ストレージから削除された文書データ、基本機能使用時に内部ストレージにスプール保存された文書あるいはその断片に対し、特定のデータで上書き消去する機能。
- データ完全消去機能
  管理者の要求に応じ、内部ストレージに保存されているすべての利用者データおよび TSF データに対し、特定のデータで上書き消去する機能。

1.4.4 TOE の保護資産

本 TOE が対象とする保護資産は、以下のように分類される。

- D.USER (利用者データ)
  TSF の操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ。
- D.TSF (TSF データ)
  TSF の操作に影響を与えるかもしれない TOE のための TOE によって作成されたデータ。

上記の利用者データは、以下の二つの種別から構成される。

- D.USER.DOC (利用者文書データ)
  電子的またはハードコピーの形式で、利用者の文書に含まれる情報
- D.USER.JOB (利用者ジョブデータ)
  利用者の文書または文書処理ジョブに関連する情報

上記の TSF データは、以下の二つの種別から構成される。

- D.TSF.PROT (保護された TSF データ)
  データの所有者でもなく、または管理者役割も持たない利用者によって、改ざんされた TSF データが TOE のセキュリティに影響を及ぼすかもしれないが、暴露については容認できるような TSF データ。本 TOE で扱うデータは以下の通り。
  - 内部認証利用者ログイン名、内部認証利用者役割、監査ログ、監査ログ送信先設定、最小パスワード長、識別認証方式、権限グループ、日付/時刻、自動ログアウト時間、アドレス帳、認証サーバー設定、IP アドレス設定、メール送信サーバー設定
- D.TSF.CONF (秘密の TSF データ)
  データの所有者でもなく、管理者役割も持たない利用者によって、改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないような TSF データ。本 TOE で扱うデータは以下の通り。
  - 内部認証利用者パスワード、暗号鍵

1.4.5 TOE の利用者

本 TOE の利用者 (U.USER) は、以下のように分類される。

- U.NORMAL (一般利用者 / a normal user)
  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 / an administrator)
  識別され、認証された利用者で、管理者役割を持つ利用者。工場出荷時に本機に組み込まれた管理者(以降、組込み管理者と呼ぶ)アカウントを含む。

2 適合主張

本 ST は以下を満たしている。

2.1 CC 適合主張

本 ST および TOE が適合を主張する CC のバージョン、および本 ST の CC パート 2 およびパート 3 適合性は、以下に示すとおりである。

CC Conformance: Common Criteria version: Version 3.1, Release 4,
Part 2 (CCMB-2012-09-002) Extended, and
Part 3 (CCMB-2012-09-003) Conformant.

2.2 PP 主張

本 ST および TOE が適合する PP は以下に示すとおりである。

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

本 ST 内において、特に断りのない限り上記を単に PP と呼ぶ。

2.3 パッケージ主張

本 ST および TOE は、パッケージ適合を主張しない。

2.4 適合根拠

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

- Required Uses
  - Printing, Scanning, Copying, Network communications, Administration
- Conditionally Mandatory Uses
  - Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
  - Image Overwrite, Purge Data

3 セキュリティ課題定義

本章は、TOE のセキュリティ課題を定義する。

3.1 脅威

TOE に対する脅威を Table 3.1 に示す。

Table 3.1: 脅威

名称	定義
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces. 攻撃者は、TOEのインタフェースを通じて、TOE内の利用者文書データへアクセス(閲覧、改変、または削除)、または利用者ジョブデータを変更(改変または削除)するかもしれない。
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces. 攻撃者は、TOEのインタフェースを通じて、TOE内のTSFデータへの不正なアクセスを得るかもしれない。
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate. TOEの操作が許可された場合、TSFの誤作動によって、セキュリティの損失を引き起こすかもしれない。
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE. 攻撃者は、TOEに不正なソフトウェアをインストールするかもしれない。
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication. 攻撃者は、ネットワーク通信をモニターしたり操作したりすることで、送信中のデータにアクセスしたり、TOEのセキュリティを侵害したりするかもしれない。

3.2 組織のセキュリティ方針

組織のセキュリティ方針を Table 3.2 に示す。

Table 3.2: 組織のセキュリティ方針

名称	定義
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions. 利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity. セキュリティ関連アクティビティは監査されなければならず、またこのようなアクションのログは保護され、外部ITエンティティへ送信されなければならない。

名称	定義
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN. TOEは、LAN上の他のデバイスとそれ自身を識別できなければならない。
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices. TOEが利用者文書データまたは秘密のTSFデータを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOEはそれらのデバイス上のこのようなデータを暗号化すること。
P.KEY_MATERIAL	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. 利用者文書データまたは秘密のTSFデータの現地交換可能な不揮発性ストレージのための暗号鍵の生成に寄与するような、平文の鍵、サブマスク、乱数、またはその他のあらゆる値は、不正なアクセスから保護されなければならない、かつそのストレージデバイス上に保存されてはならない。
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices. 画像処理ジョブの終了または中止の際に、TOEはその現地交換可能な不揮発性ストレージデバイス上の残存画像データを上書き消去しなければならない。
P.PURGE_DATA	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices. TOEは、権限付与された者が、不揮発性大容量ストレージデバイス上のすべての顧客が供給する利用者データ及びTSFデータを永久に取り出しできないようにすることができる起動を提供しなければならない。

3.3 前提条件

TOE の使用、運用時に、Table 3.3 で詳述する環境が必要となる。

Table 3.3: 前提条件

名称	定義
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment. TOE、及びTOEが保存または処理するデータの価値に見合った物理セキュリティが、その環境によって提供されることを想定する。
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface. 運用環境は、LANインタフェースへの外部からの直接のアクセスからTOEを保護することを想定する。
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies. TOE管理者は、サイトセキュリティ方針に従ってTOEを管理すると、信頼されている。

A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies. 許可された利用者は、サイトセキュリティ方針に従ってTOEを使用するよう教育訓練を受けている。

4 セキュリティ対策方針

本章は、セキュリティ対策方針における施策について述べる。

運用環境のセキュリティ対策方針を Table 4.1 に示す。

Table 4.1: 運用環境のセキュリティ対策方針

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

5 拡張コンポーネント定義

本 ST は以下の拡張コンポーネントを定義する。これらは PP で定義されたものの一部である。

5.1 FAU_STG_EXT　Extended: External Audit Trail Storage

Family Behavior:

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

Component leveling:

FAU_STG_EXT.1: External Audit Trail Storage	1

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

Management:

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

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

Audit:

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

- There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components.

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

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

Rationale:

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

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

5.2 FCS_CKM_EXT　Extended: Cryptographic Key Management

Family Behavior:

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

Component leveling:

FCS_CKM_EXT.4: Cryptographic Key Material Destruction	4

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

Management:

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

- There are no management actions foreseen.

Audit:

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

● There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

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

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

Rationale:

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

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

5.3 FCS_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	1

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

Management:

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

● There are no management actions foreseen.

Audit:

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

● Failure of HTTPS session establishment

FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 Extended: TLS selected

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

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

Rationale:

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

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

5.4 FCS_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: Key Chaining	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.

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

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

Rationale:

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.

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

5.5 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	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Rationale:

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

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

5.6 FCS_TLS_EXT Extended: TLS selected

Family Behavior:

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

Component leveling:

FCS_TLS_EXT.1: TLS selected	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.

5.7 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: Protection of Data on Disk	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

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

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

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

Rationale:

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

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

5.8 FIA_PMG_EXT Extended: Password Management

Family Behavior:

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

Component leveling:

FIA_PMG _EXT.1: Password Management	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

- There are no auditable events foreseen.

FIA_PMG _EXT.1 Extended: Password management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG _EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

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

Rationale:

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

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

5.9 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: Protection of key and key material	1

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

Management:

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

- There are no management actions foreseen.

Audit:

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

● There are no auditable events foreseen.

FPT_ KYP _EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ KYP _EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such plaintext key on a device that uses the key for its encryption.

Rationale:

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

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

5.10 FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:

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

Component leveling:

FPT_SKP_EXT.1: Protection of TSF Data	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 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.11 FPT_TST_EXT Extended: TSF Testing

Family Behavior:

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

Component leveling:

FPT_TST_EXT.1: TSF testing	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 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Rationale:

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

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

5.12 FPT_TUD_EXT Extended: Trusted Update

Family Behavior:

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

Component leveling:

FPT_TUD_EXT.1: Trusted Update	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), 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

本章は、セキュリティ要件を記述する。

6.1 表記法

- PP で操作完了または詳細化した部分は**ボールド書体**で示す。
- 本 ST で”割付”、”選択”、または”詳細化”した部分は***ボールドイタリック書体***で示し、”割付”した値はイタリック書体でないブラケット [ ] 内に、”選択”した値はイタリック書体のブラケット *[ ]* 内に示す。
- PP による”繰返し”については、コンポーネントの名称、コンポーネントのラベル、およびエレメントのラベルに対し、丸括弧入り英小文字 (a), (b), … を後置することで、固有識別とする。
- 要件操作に関係なく、単に記述を強調している部分については、*イタリック書体*で示す。

6.2 セキュリティ機能要件

本節では TOE が満たすべきセキュリティ機能要件 (SFR) を PP の分類ごとに記述する。

6.2.1 必須 FAU 要件

本節では、PP が定める必須用途に関わる FAU (Security Audit / セキュリティ監査) クラスの機能要件を記述する。

FAU_GEN.1 Audit data generation (for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) **All auditable events specified in Table 6.1, [and *Table 6.2*]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 6.1, [*and Table 6.2*]**.

Table 6.1: Auditable Events the PP Requires

Auditable event	Relevant SFR	Additional information
Job completion / ジョブの終了	FDP_ACF.1	Type of job / ジョブ種別
Unsuccessful User authentication / 利用者認証失敗	FIA_UAU.1	None
Unsuccessful User identification / 利用者識別失敗	FIA_UID.1	None
Use of management functions / 管理機能の利用	FMT_SMF.1	None
Modification to the group of Users that are part of a role / 役割の一部である利用者グループの改変	FMT_SMR.1	None
Changes to the time / 時刻の変更	FPT_STM.1	None
Failure to establish session / セション確立の失敗	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure / 失敗の理由

Note: 利用者識別事象は利用者認証事象と分離されず、監査目的として1つの事象とみなす。

Table 6.2: Auditable Events this ST Provides

Auditable event	Relevant SFR	Additional information
Software update / ソフトウェアアップデート	FPT_TUD_EXT.1	新旧バージョン

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

FAU_STG_EXT.1 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 必須 FCS 要件

本節では、PP が定める必須用途に関わる FCS (Cryptographic Support / 暗号サポート) クラスの機能要件を記述する。他に 6.2.9, 6.2.12, 6.2.13 および 6.2.14 の各節にも一部の FCS 要件がある。

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

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) **Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with *[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_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

FCS_CKM_EXT.4 Cryptographic Key Material Destruction (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

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

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

FCS_CKM.4 Cryptographic key destruction (for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

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

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

- ***For volatile memory, the destruction shall be executed by [powering off a device].***
- ***For nonvolatile storage, the destruction shall be executed by a [single] overwrite of key data storage location consisting of [a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [none]. If read-verification of the overwritten data fails, the process shall be repeated again;***

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

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption) (for O.COMMS_PROTECTION)

Hierarchical to: No other components.

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

FCS_COP.1.1(a) **Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [** ***CBC mode*** **]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

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

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) (for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

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

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

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 ***[NIST SP 800-90A]*** using ***[CTR_DRBG (AES)]***.

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

6.2.3 必須 FDP 要件

本節では、PP が定める必須用途に関わる FDP (User Data Protection / 利用者データ保護) クラスの機能要件を記述する。他に 6.2.9, 6.2.10 および 6.2.11 の各節にも一部の FDP 要件がある。

FDP_ACC.1 Subset access control (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** on **subjects, objects, and operations among subjects and objects specified in Table 6.3 and Table 6.4**.

FDP_ACF.1 Security attribute based access control (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute 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 6.3 and Table 6.4**.

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 6.3 and Table 6.4**.

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

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

Table 6.3: D.USER.DOC Access Control SFP

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

Table 6.4: D.USER.JOB Access Control SFP

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

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

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

6.2.4 必須 FIA 要件

本節では、PP が定める必須用途に関わる FIA (Identification and Authentication / 識別と認証) クラスの機能要件を記述する。他に 6.2.13 節にも一部の FIA 要件がある。

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 *[* [***3***] *]* unsuccessful authentication attempts occur related to [***the unsuccessful user (including administrator) internal authentication attempts following the last successful authentication***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *[* ***met*** *]*, the TSF shall [

- ***Unsuccessful authentication reached three times: Reception of authentication trials stops for five minutes***
- ***Five minutes later after stopping: the number of times authentication was unsuccessful is cleared, and the reception of authentication trials is recovered***

].

FIA_ATD.1 User attribute definition (for O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*利用者ログイン名, 利用者役割*].

FIA_PMG_EXT.1 Password Management (for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: *["!", "@", "#", "$", "%", "^", "&", "*", "(", ")",* **[** ***no other characters*** **]** *]*;
- 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: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **Refinement:** The TSF shall allow [***nothing***] 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 [***substitute characters as many as ones that are provided***] 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 [***nothing***] 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: [*利用者ログイン名, 利用者役割*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***no rules***].

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: [***no rules***].

6.2.5 必須 FMT 要件

本節では、PP が定める必須用途に関わる FMT (Security Management / セキュリティ管理) クラスの機能要件を記述する。

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 *[**enable**]* the functions [
● ***Initialize Private Data / Data in Machine (個人情報及び本機内データの初期化)***
] to **U.ADMIN**.

FMT_MSA.1 Management of security attributes (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control~~, or FDP_IFC.1 Subset information flow control~~]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to *[**query**, **modify**, **delete**, [**create**]]* the security attributes [***Security attributes specified in Table 6.5***] to [***Authorised roles specified in Table 6.5***].

Table 6.5: List of Security attributes

Security attributes	Operation	Authorised roles
内部認証利用者ログイン名	***create, modify, delete***	**U.ADMIN**
	query	**U.ADMIN, the owning U.NORMAL**
内部認証利用者役割	***create, modify, delete***	**U.ADMIN**
	query	**U.ADMIN, the owning U.NORMAL**

FMT_MSA.3 Static attribute initialization (for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

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

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

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

FMT_MTD.1 Management of TSF data (for O.ACCESS_CONTROL)

Hierarchical to: No other components.

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

FMT_MTD.1.1 **Refinement:** The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 6.6**.

Table 6.6: Management of TSF Data

TSF Data	Operation	Authorised role(s)
内部認証利用者パスワード	***create, delete***	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
最小パスワード長	***modify***	**U.ADMIN**
識別認証方式	***modify***	**U.ADMIN**
日付/時刻	***modify***	**U.ADMIN**
監査ログ送信先設定	***query, modify***	**U.ADMIN**
自動ログアウト時間	***query, modify***	**U.ADMIN**
アドレス帳	***create, modify, delete***	**U.ADMIN**
認証サーバー設定	***create, modify, delete***	**U.ADMIN**
IPアドレス設定	***modify***	**U.ADMIN**
メール送信サーバー設定	***query, modify***	**U.ADMIN**

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 **Refinement:** The TSF shall be capable of performing the following management functions: [***management functions specified in Table 6.7, Table 6.8, Table 6.9, and Table 6.10***].

Table 6.7: List of Management Functions Provided by the TSF (1)

機能要件/SFR	管理機能/management functions	備考/notes
FAU_GEN.1	None	—
FAU_GEN.2	None	—
FAU_STG_EXT.1	• 監査ログ送信先の設定	暗号機能はTLS使用に固定
FCS_CKM.1(a)	None	—
FCS_CKM.1(b)	None	—
FCS_CKM_EXT.4	None	—
FCS_CKM.4	None	—
FCS_COP.1(a)	None	—
FCS_COP.1(b)	None	—
FCS_RBG_EXT.1	None	—
FDP_ACC.1	None	—
FDP_ACF.1	None	明示的な許可/拒否の規則なし
FIA_AFL.1	None	閾値とアクションは固定
FIA_ATD.1	• 内部認証利用者の登録 • 内部認証利用者役割の変更	—
FIA_PMG_EXT.1	• 最小パスワード長の変更	—
FIA_UAU.1	• 識別認証方式の変更 • 認証サーバーの設定 • 内部認証利用者パスワードの変更	認証前アクションは固定
FIA_UAU.7	None	—
FIA_UID.1	• 識別認証方式の変更 • 認証サーバーの設定 • 内部認証利用者の登録/削除 • 内部認証利用者ログイン名の変更	識別前アクションは固定
FIA_USB.1	None	サブジェクト属性は固定

Table 6.8: List of Management Functions Provided by the TSF (2)

機能要件/SFR	管理機能/management functions	備考/notes
FMT_MOF.1	None	役割グループは固定
FMT_MSA.1	None	役割グループと規則は固定
FMT_MSA.3	None	役割グループ、デフォルト設定、および、規則は固定
FMT_MTD.1	None	役割グループは固定
FMT_SMF.1	None	—
FMT_SMR.1	• 権限グループの管理	—
FPT_SKP_EXT.1	None	—
FPT_STM.1	• 日付/時刻の設定	—
FPT_TST_EXT.1	None	—
FPT_TUD_EXT.1	None	—
FTA_SSL.3	• 自動ログアウト時間の設定	—
FTP_ITC.1	None	—
FTP_TRP.1(a)	None	—
FTP_TRP.1(b)	None	—

Table 6.9: List of Management Functions Provided by the TSF (3)

機能要件/SFR	管理機能/management functions	備考/notes
FPT_KYP_EXT.1	None	—
FCS_KYC_EXT.1	None	—
FDP_DSK_EXT.1	None	—
FDP_RIP.1(a)	None	残存情報保護の実施タイミングは、割当て解除時に固定
FDP_RIP.1(b)	• 個人情報及び本機内データの初期化の起動	—
FCS_COP.1(d)	None	—
FCS_COP.1(f)	None	—
FCS_TLS_EXT.1	None	—
FCS_HTTPS_EXT.1	None	—
FCS_COP.1(c)	None	—

Table 6.10: List of Management Functions Provided by the TSF (4)

機能要件/SFR	管理機能/management functions	備考/notes
—	• アドレス帳の管理	—
—	• IPアドレスの設定	—
—	• メール送信サーバーの設定	—

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.NORMAL**.

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

6.2.6 必須 FPT 要件

本節では、PP が定める必須用途に関わる FPT (Protection of the TSF / TSF の保護) クラスの機能要件を記述する。他に 6.2.9 節にも一部の FPT 要件がある。

FPT_SKP_EXT.1 Protection of TSF Data (for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_STM.1 Reliable time stamps (for O.AUDIT)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST_EXT.1 TSF testing (for O.TSF_SELF_TEST)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TUD_EXT.1 Trusted Update (for O.UPDATE_VERIFICATION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation / verification)
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

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

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

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

6.2.7 必須 FTA 要件

本節では、PP が定める必須用途に関わる FTA (TOE Access / TOE アクセス) クラスの機能要件を記述する。

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 [***user inactivity for:***
- ***240 seconds or shorter, specified by U.ADMIN, for sessions via the operation panel***
- ***300 seconds, for sessions via web interfaces***

].

6.2.8 必須 FTP 要件

本節では、PP が定める必須用途に関わる FTP (Trusted Paths/Channels / 高信頼パス/チャネル) クラスの機能要件を記述する。

FTP_ITC.1 Inter-TSF trusted channel (for O.COMMS_PROTECTION, O.AUDIT)

Hierarchical to: No other components.

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

FTP_ITC.1.1 **Refinement:** The TSF shall **use** ***[TLS]*** **to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities:** ***[authentication server,*** **[** ***audit log server, ftp server, mail server*** **]** ***]*** that is logically distinct from other communication channels and provides assured identification of its end

points and protection of the channel data from **disclosure and detection of modification of the channel data**.

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

FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [***authentication service, audit log service, ftp service, mail service***].

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

Hierarchical to: No other components.

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

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

FTP_TRP.1.2(a) **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

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

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

Hierarchical to: No other components.

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

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

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

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

6.2.9 条件付き必須要件 B1

本節では、PP が定める条件付き必須用途のうち、現地交換可能な不揮発性ストレージデバイス上の秘密のデータに関わる機能要件を記述する。他に 6.2.12 節にも、本節に関する機能要件の一部がある。

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**.

FCS_KYC_EXT.1 Key Chaining (for O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,

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

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: *[**intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method: [key encryption as specified in FCS_COP.1(f)]**]* while maintaining an effective strength of *[**256 bits**]*.

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 *[**perform encryption in accordance with FCS_COP.1(d)**]* such that any Field- Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.

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

6.2.10オプション要件 C2

本節では、PP が定めるオプション用途のうち、画像上書きに関わる機能要件を記述する。

FDP_RIP.1(a) Subset residual information protection (for O.IMAGE_OVERWRITE)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(a) **Refinement:** The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects: **D.USER.DOC**.

6.2.11オプション要件 C3

本節では、PP が定めるオプション用途のうち、データの完全削除に関わる機能要件を記述する。

FDP_RIP.1(b) Subset residual information protection (for O.PURGE_DATA)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1(b) **Refinement:** The TSF shall ensure that any previous **customer-supplied** information content of a resource is made unavailable upon the **request of an Administrator to** the following objects: **D.USER, D.TSF**.

6.2.12選択ベース要件 D1

本節では、PP が定める選択ベース要件のうち、現地交換可能な不揮発性ストレージデバイス上の秘密のデータに関わる機能要件を記述する。他に 6.2.9 節にも、本節に関する機能要件の一部がある。

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

Hierarchical to: No other components.

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

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in *[CBC]* mode** and cryptographic key sizes *[**256 bits**]* that meet the following: **AES as specified in ISO/IEC 18033-3, *[CBC as specified in ISO/IEC 10116]***.

FCS_COP.1(f) Cryptographic operation (Key Encryption) (selected from FCS_KYC_EXT.1.1)

Hierarchical to: No other components.

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

FCS_COP.1.1(f) **Refinement:** The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in *[CBC]* mode** and cryptographic key sizes ***[256 bits]*** that meet the following: **AES as specified in ISO/IEC 18033-3, *[CBC as specified in ISO/IEC 10116]***.

6.2.13選択ベース要件 D2

本節では、PP が定める選択ベース要件のうち、保護された通信に関わる機能要件を記述する。

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 ***[TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[

- ***TLS_RSA_WITH_AES_256_CBC_SHA***
- ***TLS_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***

].

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_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) (selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

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

FCS_COP.1.1(g) **Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-*[SHA-1, SHA-256]*, key size [*160,***

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

6.2.14選択ベース要件 D3

本節では、PP が定める選択ベース要件のうち、高信頼アップデートに関わる機能要件を記述する。

FCS_COP.1(c) Cryptographic operation (Hash Algorithm) (selected in FPT_TUD_EXT.1.3)

Hierarchical to: No other components.

Dependencies: No dependencies

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

6.2.15セキュリティ機能要件根拠

上記、本 ST が主張する SFR は、PP が規定する SFR の部分集合である。割り付けおよび選択はすべて完了している。また、以下に述べるとおり、依存性について問題はない。

6.2.15.1 セキュリティ機能要件の依存性根拠

Table 6.11, Table 6.12, および Table 6.13 は、CC および PP が規定する SFR が満足すべき依存性と、本 TOE が満足している依存性、満足していない依存性、および依存性不満足の正当性を示す。

Table 6.11: セキュリティ機能要件の依存性 (1)

依存性 機能要件	満足すべき	満足している	不満足	備考
FAU_GEN.1	FPT_STM.1	FPT_STM.1	—	—
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	—	—
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	—	—
FCS_CKM.1(a)	[FCS_COP.1(b), or FCS_COP.1(i)], FCS_CKM_EXT.4	FCS_COP.1(b), FCS_CKM_EXT.4	—	—
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)], FCS_CKM_EXT.4, FCS_RBG_EXT.1	FCS_COP.1(a), FCS_COP.1(d), FCS_COP.1(f), FCS_COP.1(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1	—	—
FCS_CKM_EXT.4	[FCS_CKM.1(a) or FCS_CKM.1(b)], FCS_CKM.4	FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4	—	—
FCS_CKM.4	[FCS_CKM.1(a) or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	—	—
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a), FCS_CKM_EXT.4	—	—
FCS_RBG_EXT.1	—	—	—	—
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	—	—
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	—	—
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	—	—
FIA_ATD.1	—	—	—	—
FIA_PMG_EXT.1	—	—	—	—
FIA_UAU.1	FIA_UID.1	FIA_UID.1	—	—
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	—	—
FIA_UID.1	—	—	—	—
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	—	—

Table 6.12: セキュリティ機能要件の依存性 (2)

依存性 機能要件	満足すべき	満足している	不満足	備考
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	—	—
FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	—	—
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	—	—
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1	FIA_UID.1	—	—
FPT_SKP_EXT.1	—	—	—	—
FPT_STM.1	—	—	—	—
FPT_TST_EXT.1	—	—	—	—
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b), FCS_COP.1(c)	—	—
FTA_SSL.3	—	—	—	—
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1	—	—
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	—	—
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	—	—

Table 6.13: セキュリティ機能要件の依存性 (3)

依存性 機能要件	満足すべき	満足している	不満足	備考
FPT_KYP_EXT.1	—	—	—	—
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_COP.1(f)	—	—
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	—	—
FDP_RIP.1(a)	—	—	—	—
FDP_RIP.1(b)	—	—	—	—
FCS_COP.1(d)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(f)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_TLS_EXT.1	FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1	FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1	—	—
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	—	—
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	—	—
FCS_COP.1(c)	—	—	—	—

6.3 セキュリティ保証要件

以下、本 ST が主張するセキュリティ保証要件 (SAR) を、CC パート 3 の保証クラス別に示す。本 ST は、CC パート 3 に定義され、PP に記述されたセキュリティ保証コンポーネントを、そのまま SAR として使用する。

6.3.1 Class ASE: Security Target Evaluation

- Conformance claims: ASE_CCL.1 — Conformance claims
- Extended components definition: ASE_ECD.1 — Extended components definition
- ST introduction: ASE_INT.1 — ST introduction
- Security objectives: ASE_OBJ.1 — Security objectives for the operational environment
- Security requirements: ASE_REQ.1 — Stated security requirements
- Security problem definition ASE_SPD.1 — Security problem definition
- TOE summary specification ASE_TSS.1 — TOE summary specification

6.3.2 Class ADV: Development

- Functional Specification: ADV_FSP.1 — Basic functional specification

6.3.3 Class AGD: Guidance Documents

- Operational user guidance: AGD_OPE.1 — Operational user guidance
- Preparative procedures: AGD_PRE.1 — Preparative procedures

6.3.4 Class ALC: Life-cycle Support

- CM capabilities: ALC_CMC.1 — Labelling of the TOE
- CM scope: ALC_CMS.1 — TOE CM coverage

6.3.5 Class ATE: Tests

- Independent testing: ATE_IND.1 — Independent testing - conformance

6.3.6 Class AVA: Vulnerability Assessment

- Vulnerability analysis: AVA_VAN.1 — Vulnerability survey

6.3.7 セキュリティ保証要件根拠

上記、本 ST が主張する SAR は、PP が規定する SAR と完全に一致している。

7 TOE 要約仕様

本章は、TOE セキュリティ機能 (TSF) の要約仕様を記述することにより、セキュリティ機能要件 (SFR) が満たされることを示す。

7.1 セキュリティ監査

本節では主に、6.2.1 節の必須 FAU 要件に関する要約仕様を記述する。

FAU_GEN.1 / FAU_GEN.2

TSF は、監査の起動と終了に加え、Table 6.1 および Table 6.2 に記述した監査イベントのログを監査データとして生成する。
TSF は、監査の起動/終了を含む監査イベントが発生した日付(年/月/日)および時刻(時/分/秒)を TOE のシステムクロックから取得し、監査データに記録する。
TSF は、特定の利用者が発生させたイベントには、その利用者のログイン名(ログイン名の全体または先頭部分)を、監査イベントに関連するサブジェクト識別情報として監査データに記録する。ただし、TOE 自身がイベントを発生させた場合は“SYSTEM”、サブジェクトが特定できない場合は“N/A”と記録する。
TSF が監査データに記録する情報に関する内容について、Table 7.1 に示す。

Table 7.1: 監査データに記録する情報

イベント名	日時 (*1)	操作 I/F (*2)	ログイン名	結果 (*3)	追加情報
監査の起動 (Audit Start)	○	N/A	N/A	○	N/A
監査の終了 (Audit End)	○	N/A	N/A	○	N/A
ジョブの終了 (Job Completion)	○	○	ジョブ所有者	○	終了したジョブ名
識別認証の失敗 (I&A Failure)	○	○	ログイン名として入力された文字列	N/A	N/A
ユーザーの追加 (Add User)	○	○	追加を行った利用者	○	追加したログイン名
パスワードの変更 (Change Password)	○	○	変更を行った利用者	○	パスワード変更された利用者のログイン名
ログイン名の変更 (Change Login Name)	○	○	変更を行った利用者	○	変更後のログイン名
ユーザーの削除 (Delete user)	○	○	削除を行った利用者	○	削除したログイン名(全ユーザー一括削除の場合は All)
権限グループの追加 (Add Auth Group)	○	○	追加を行った利用者	○	追加した権限グループ名
利用者の所属する権限グループの変更 (Change Role)	○	○	変更を行った利用者	○	・所属する権限グループを変更された利用者のログイン名 ・変更後の権限グループ名
権限グループの設定の変更 (Change Auth Group Setting)	○	○	変更を行った利用者	○	設定変更された権限グループ名
日付/時刻の変更 (Change Time Setting)	○	○	変更を行った利用者	○	N/A
設定値の変更 (Change Setting)	○	○	変更した利用者	○	・設定変更された設定項目 ・変更後の設定値
TLS 通信の失敗 (Comm Failure) *通信相手が監査サ	○	N/A	SYSTEM	N/A	・失敗の理由

ーバー					
TLS 通信の失敗 (Comm Failure) *通信相手が監査サーバー以外	○	Net	N/A	N/A	・通信開始者の IP アドレス ・通信相手の IP アドレス ・通信方向 ・失敗の理由
アドレス帳の更新 (Modify Addr Book)	○	○	更新を行った利用者	○	追加時: 追加されたエントリの内部管理 ID および宛先名 削除/変更時: 削除/変更されたエントリの内部管理 ID
ファームウェアアップデート (Firm Update)	○	○	アップデートを行った利用者	○	・ファームウェア名 ・アップデート前のファームウェアバージョン ・アップデート後のファームウェアバージョン

*1 イベント発生日時がISO 8601の拡張形式で表記される
*2 操作インタフェースとして、操作パネル/Webページ/ネットワークのいずれかが表記される。ただし、表中で"N/A"となっているものは、"N/A"と表記される。
*3 イベント実施結果として、成功/失敗のいずれかが表記される。ただし、表中で"N/A"となっているものは、"N/A"と表記される。

本要件に関する TSF インタフェースは、Table 7.2 に示すとおりである。

Table 7.2: FAU_GEN.1/FAU_GEN.2 に関する TSF インタフェース

イベント名	インタフェース
監査の起動	• MFDの電源ON (停電からの復旧も同等)
監査の終了	• MFDの電源OFF
ジョブの終了	• FDP_ACC.1/FDP_ACF.1のTSFインタフェースに準じ、コピー/プリント/スキャン/ドキュメントファイリング機能からジョブを生成
識別認証の失敗	• 操作パネル/Webページのユーザー認証画面でログイン操作
ユーザーの追加	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録
パスワードの変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
ログイン名の変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
ユーザーの削除	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを削除
権限グループの追加	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[権限グループ]から権限グループを登録
利用者の所属する権限グループの変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
権限グループの設定の変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[権限グループ]から権限グループを修正
日付/時刻の変更	• 操作パネルの設定モード/Webページで、[システム設定]→[共通設定]→[日付/時刻設定]から日付と時刻を設定
設定値の変更	• 操作パネルの設定モード/Webページで、各種設定から設定値を変更
TLS 通信の失敗	• FTP_ITC.1のTSFインタフェースに準じ、認証サーバー/監査サーバー/FTPサーバー/メールサーバーとの通信を実行
アドレス帳の更新	• 操作パネルで、[アドレス帳]から新規登録/編集/削除を実行 • Webページで、[アドレス帳]→[アドレス帳]から新規登録/編集/削除を実行
ファームウェアアップデート	• 操作パネルからメンテナンス用モードへ移行し、ファームウェアアップデートを実行

FAU_STG_EXT.1

生成された監査データは、FTP_ITC.1 に従い、Syslog プロトコルおよび TLS1.2 を用いて監査サーバーに送信される。そのデータは、送信が成功するまで、内部ストレージに準備されたバッファ領域に保存される。このバッファ領域には、4 万件の監査データを保存することができる。監査データの送信は、新たにデータが生成されたタイミングで行われる。
監査サーバーへの送信が失敗したとき、操作パネルおよび Web ページの画面上に警告メッセージを表示し、成功するまで定期的に監査サーバーへの送信を再試行する。警告メッセージには、監査サーバーに接続されていないこととその影響が表記され、管理者への連絡を要請する。
バッファ領域の使用率が 80%以上に達すると、組込み管理者以外はログインできないように制限される。この制限は、バッファ領域の使用率が 70%未満になった時点で解除される。バッファ領域が満杯、つまりバッファ領域に 4 万件の監査データが保存された状態では、新たに生成された監査データはバッファ領域に保存されず、削除される。
バッファ領域に保存された監査データは、FDP_DSK_EXT.1 に従い暗号化して保存される。また、利用者役割に関わらず、すべての利用者はバッファ領域に保存された監査データにアクセスすることができない。
本要件に関する TSF インタフェースは、FAU_GEN.1/FAU_GEN.2 の TSF インタフェースに準じる。

7.2 暗号サポート

本節では主に、6.2.2 節の必須 FCS 要件に関する要約仕様を記述する。

FCS_CKM.1(a)

TSF は、暗号通信の鍵確立で用いる非対称鍵として、標準文書 NIST SP 800-56B, Revision 1 の 6.3.1.1 節に記載の rsakpg1-basic 方式で RSA 鍵を生成する。その際に必要となる乱数は FCS_RBG_EXT.1 に従って生成する。TOE は本 TSF に関し、TOE 特有の拡張や同標準外の独自処理、あるいは許容された別実装を含んでいない。この鍵は、管理者の操作により削除されるまで、内部ストレージに保存される。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- FCS_CKM_EXT.4 の TSF インタフェースに準じ、非対称鍵を破棄した後、再度 MFD の電源 ON (停電からの復旧も同等)

FCS_CKM.1(b)

TSF は、暗号通信のネゴシエーションにおいて、通信用のセション鍵を生成する。セション鍵は、TLS 通信を行うたびにサーバー・クライアント間で共有される複数の鍵から構成され、データを暗号化/復号するための対称鍵とデータを検証するための MAC 鍵を含む。TSF は、FCS_RBG_EXT.1 による RBG で生成された乱数を用いて、AES-128 の暗号スイートを使用する場合は 128 ビット長の、AES-256 の暗号スイートを使用する場合は 256 ビット長の対称鍵を生成し、揮発性メモリー内に保存する。また、
FCS_RBG_EXT.1 による RBG で生成された乱数を用いて、SHA-1 の暗号スイートを使用する場合は 160 ビット長の、SHA-256 の暗号スイートを使用する場合は 256 ビット長の MAC 鍵を生成し、揮発性メモリー内に保存する。
本要件に関する TSF インタフェースは、FTP_ITC.1 の TSF インタフェースに準じる。

TSF は、TOE 設置後の初回起動時および TOE 初期化後の再起動時に、ストレージ鍵を暗号化するための対称鍵として、FCS_RBG_EXT.1 による RBG で生成された乱数を用いて 256 ビット長の鍵暗号鍵を生成し、不揮発性メモリー1 内に保存する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- TOE 設置作業後の初回起動
- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行後、TOE を再起動

TSF は、TOE 設置後の初回起動時および TOE 初期化後の再起動時に、内部ストレージに保存するデータを暗号化するための暗号鍵として、FCS_RBG_EXT.1 による RBG で生成された乱数を用いて 256 ビット長のストレージ鍵を生成し、FCS_COP.1(f)による鍵暗号化を用いて不揮発性メモリー1 に保存された鍵暗号鍵で暗号化した状態で不揮発性メモリー2 内に保存する。

本要件に関する TSF インタフェースは、以下に示すとおりである。

- TOE 設置作業後の初回起動
- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行後、TOE を再起動

また、TSF は、TOE の電源 ON 時に、不揮発性メモリー2 に保存された暗号化されたストレージ鍵を読み出し、FCS_COP.1(f)による鍵暗号化を用いて不揮発性メモリー1 に保存された鍵暗号鍵で復号したストレージ鍵を、暗号アルゴリズム AES Rijndael で使用するため、TOE の電源断までの間、揮発性メモリー内に保存する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- MFD の電源 ON (停電からの復旧も同等)

FCS_CKM_EXT.4 / FCS_CKM.4

TSF が扱う以下の鍵は、不要となった後に破棄される。

- 通信用の非対称鍵:
  管理者が TOE の機器証明書の削除を実行した時、不要な鍵として扱われ、鍵が保存されている領域をゼロビット列で1回上書きすることにより破棄される。
  本要件に関する TSF インタフェースは、以下に示すとおりである。
  - 操作パネルの設定モード/Web ページで、[システム設定]→[セキュリティ設定]→[SSL 設定]から機器証明書を削除
- 通信用のセション鍵:
  TLS 通信が切断された時、不要な鍵として扱われ、鍵が保存されている領域を簡易的な疑似乱数で上書きすることにより破棄される。また、揮発性メモリー上にあるため、TOE の電源断で揮発し、破棄される。
  本要件に関する TSF インタフェースは、以下に示すとおりである。
  - FTP_ITC.1 の TSF インタフェースに準じて開始した TLS 通信の切断
  - MFD の電源 OFF
- 鍵暗号鍵:
  管理者が個人情報及び本機内データの初期化(Initialize Private Data / Data in Machine)を実行した時、暗号化された利用者データおよび TSF データがすべて消去されることから、ストレージ鍵は不要な鍵として扱われ、ストレージ鍵の暗号化/復号に使用している鍵暗号鍵も同様に不要な鍵として扱われ、FCS_RBG_EXT.1 による RBG で生成された乱数で 1 回上書きすることにより破棄される。
  本要件に関する TSF インタフェースは、以下に示すとおりである。
  - 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行
- ストレージ鍵:
  管理者が個人情報及び本機内データの初期化(Initialize Private Data / Data in Machine)を実行した時、暗号化された利用者データおよび TSF データがすべて消去されることから、不要な鍵として扱われ、不揮発性メモリー2 に保存された暗号化されたストレージ鍵は FCS_RBG_EXT.1 による RBG で生成された乱数で 1 回上書きすることにより破棄される。
  本要件に関する TSF インタフェースは、以下に示すとおりである。
  - 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行

  また、TOE の電源 ON 時に復号されたストレージ鍵は TOE の電源断で不要な鍵として扱われ、揮発性メモリー上にあるため、TOE の電源断で揮発し、破棄される。
  本要件に関する TSF インタフェースは、以下に示すとおりである。
  - MFD の電源 OFF

FCS_COP.1(a)

TSF は、FTP_ITC.1, FTP_TRP.1(a) および FTP_TRP.1(b) における通信データ暗号化のために、FCS_CKM.1(b)により生成した 128 ビット長または 256 ビット長の暗号鍵と FIPS PUB 197 に準拠する AES 暗号アルゴリズムを NIST SP 800-38A に準拠する CBC モードで動作することにより通信データの暗号化および復号を行う。
本要件に関する TSF インタフェースは、FTP_ITC.1 および FTP_TRP.1(a)/FTP_TRP.1(b) の TSF インタフェースに準じる。

FCS_COP.1(b)

TSF は、TOE の機器証明書導入による証明書生成における署名生成、FTP_ITC.1 によるサーバー証明書検証および FPT_TUD_EXT.1 によるアップデート検証において、FIPS PUB 186-4 に規定された Digital Signature Standard を満たす鍵長が 2048 ビットの RSA デジタル署名アルゴリズム(rDSA)を使用する。また、TOE の機器証明書導入による証明書生成における署名生成において、FCS_CKM.1(a)により生成された RSA 鍵を使用する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- TOE の機器証明書導入:
  - [システム設定]→[セキュリティ設定]→[SSL 設定]において機器証明書が導入されていない状態で、TOE を再起動
  - Web ページで、[システム設定]→[セキュリティ設定]→[SSL 設定]内の機器証明書において、[導入]を実行
- サーバー証明書検証:
  - FTP_ITC.1 の TSF インタフェースに準じる
- アップデート検証:
  - FPT_TUD_EXT.1 の TSF インタフェースに準じる

FCS_RBG_EXT.1

TSF は、DRBG および ES から構成された RBG を含む。DRBG は、384 ビットのエントロピーを持つ乱数シード(Entropy Input)を必要とする、NIST SP 800-90A を満たす CTR_DRBG (AES-256)である。これは導出関数(derivation function)を使用しない CTR_DRBG であり、他のシード材料(nonce 等)は使用しない。
ES は、1 個のハードウェアベースのノイズ源を含む自社開発の回路であり、DRBG に入力する 384 ビットのエントロピーを持つ乱数シードを生成する。
TSF は、ES に対して乱数生成要求および乱数読み出しを繰り返し行うことで 384 ビット以上のエントロピーを蓄え、それを基に 384 ビットのエントロピーを持つ乱数シードを生成する。これを DRBG に与えることで暗号鍵生成に利用する乱数を生成する。
本要件に関する TSF インタフェースは、FCS_CKM.1(a)および FCS_CKM.1(b)の TSF インタフェースに準じる。

7.3 利用者データ保護

本節では主に、6.2.3 節の必須 FDP 要件に関する要約仕様を記述する。

FDP_ACC.1 / FDP_ACF.1

TSF は、利用者データおよび利用者データの操作へのアクセス制御を行う。
利用者データへのアクセスを、識別認証された管理者(U.ADMIN)、および利用者データに付属する所有者情報として紐づけられた利用者ログイン名と一致する識別認証された利用者のみに許可することで、利用者データへの操作について、Table 6.3 および Table 6.4 に基づいた利用者およびジョブオーナーに基づくアクセス管理規則を実施する。
D.USER.DOC アクセス制御に関する TSF インタフェースは、Table 7.3 に示すとおりである。

Table 7.3: D.USER.DOC アクセス制御に関する TSF インタフェース

機能	操作	インタフェース
Print (プリント)	Create	• クライアントPCから印刷する文書を選択し、プリンタードライバーの設

		定画面から印刷を実行
	Read	• 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、印刷を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、[画像を確認する]を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、[設定を変更して印刷する]を実行 • 上記操作後に印刷を実行
	Modify	• 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、[設定を変更して印刷する]から編集を実行
	Delete	• 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、[削除]を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作によりホールドされたファイルを選択し、印刷後にデータを削除する設定を有効にして印刷を実行 • Create操作を実行後、操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[データエリア消去]→[ドキュメントファイリングデータ消去]から消去を実行 (組込み管理者のみ操作可能)
Scan (スキャン)	Create	• MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルスキャン]からプレビューを実行 (以下、本操作をCreate操作Sc1と呼ぶ) • MFDのスキャナーユニットに原稿をセットして、[E-Mail]、または[FTP/Desktop]からプレビューを実行 (以下、本操作をCreate操作Sc2と呼ぶ) • MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルスキャン]、[E-Mail]、または[FTP/Desktop]からスキャンを実行 (以下、本操作をCreate操作Sc3と呼ぶ)
	Read	• Create操作Sc1、またはCreate操作Sc2を実行
	Modify	• Create操作Sc2を実行後、プレビュー画面から編集を実行
	Delete	• Create操作Sc1、またはCreate操作Sc2を実行後、[読込のみしなおす]、または[リセット]を実行 • Create操作Sc1、またはCreate操作Sc2を実行後、[ホーム画面]ボタンを押す • Create操作Sc1、またはCreate操作Sc2を実行後、モード表示部からモードを切り替える • Create操作Sc3を実行後、操作パネルで、[リセット]、または[読み込み中止]を実行 • スキャン実行後、操作パネルで、[ジョブ状況]→[スキャナー]→[予約/実行中のジョブ]からスキャン実行で作成されたジョブを中止/削除
Copy (コピー)	Create	• MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルコピー]からプレビューを実行 (以下、本操作をCreate操作C1と呼ぶ) • MFDのスキャナーユニットに原稿をセットして、操作パネルで、[コピー]からプレビューを実行 (以下、本操作をCreate操作C2と呼ぶ) • MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルコピー]、または[コピー]からコピーを実行 (以下、本操作をCreate操作C3と呼ぶ)
	Read	• Create操作C1、またはCreate操作C2を実行 • 上記操作後にコピーを実行 • Create操作C3を実行
	Modify	• Create操作C2を実行後、プレビュー画面から編集を実行
	Delete	• Create操作C1、またはCreate操作C2を実行後、[読込のみしなおす]、[設定を変更せず原稿を読み込みしなおす]、または[リセット]を実行 • Create操作C1、またはCreate操作C2を実行後、[ホーム画面]ボタンを押す

		• Create操作C1、またはCreate操作C2を実行後、モード表示部からモードを切り替える • Create操作C3を実行後、操作パネルで、[リセット]、または[コピー中止]を実行 • コピー実行後、操作パネルで、[印刷中止]、または[ジョブ状況]→[プリント]→[予約/実行中のジョブ]からコピー実行で作成されたジョブを中止/削除
Storage/retrieval (保存/取り出し: ドキュメントファイリング)	Create	• MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルスキャン]→[本体/デバイス保存]、[スキャン保存]、または[ドキュメントファイリング]→[本体HDDにスキャン保存する]からスキャン保存を実行 • ファイリング設定をONに設定して、スキャン、または、コピーを実行
	Read	• 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[今すぐ印刷]、または[設定を変更して印刷する]から印刷を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[送信する]から送信を実行
	Modify	• 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[設定を変更して印刷する]から編集を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[送信する]から編集を実行
	Delete	• 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[削除]を実行 • Webページで、[ファイル操作]→[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、[削除]を実行 • 操作パネルで、[ドキュメントファイリング]からCreate操作で保存されたファイルを選択し、印刷後にデータを削除する設定を有効にして印刷を実行 • 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[データエリア消去]→[ドキュメントファイリングデータ消去]から消去を実行 (組込み管理者のみ操作可能)

D.USER.JOB アクセス制御に関する TSF インタフェースは、Table 7.4 に示すとおりである。

Table 7.4: D.USER.JOB アクセス制御に関する TSF インタフェース

機能	操作	インタフェース
Print (プリント)	Create	• クライアントPCから印刷する文書を選択し、プリンタードライバーの設定画面から印刷を実行後、操作パネルで、[ドキュメントファイリング]からクライアントPCからの印刷実行でホールドされたファイルを選択し、印刷を実行
	Read	• 操作パネルで、[ジョブ状況]→[プリント]→[予約/実行中のジョブ]を選択
	Modify	N/A
	Delete	• 操作パネルで、 [印刷中止]、または[ジョブ状況]→[プリント]→[予約/実行中のジョブ]からCreate操作で作成されたジョブを中止/削除
Scan (スキャン)	Create	• MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルスキャン]、[E-Mail]、または[FTP/Desktop]からスキャンを実行
	Read	• 操作パネルで、[ジョブ状況]→[スキャナー]→[予約/実行中のジョブ]を選択
	Modify	N/A
	Delete	• 操作パネルで、[ジョブ状況]→[スキャナー]→[予約/実行中のジョブ]からCreate操作で作成されたジョブを中止/削除
Copy (コピー)	Create	• MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルコピー]、または[コピー]からコピーを実行
	Read	• 操作パネルで、[ジョブ状況]→[プリント]→[予約/実行中のジョブ]を選択

	Modify	N/A
	Delete	• コピー実行後、原稿読み込み中に操作パネルで、[リセット]、または[コピー中止]を実行 • 操作パネルで、[印刷中止]、または[ジョブ状況]→[プリント]→[予約/実行中のジョブ]からCreate操作で作成されたジョブを中止/削除
Storage/retrieval (保存/取り出し: ドキュメントファイリング)	Create	(保存ジョブ) • MFDのスキャナーユニットに原稿をセットして、操作パネルで、[シンプルスキャン]→[本体/デバイス保存]、[スキャン保存]、または[ドキュメントファイリング]→[本体HDDにスキャン保存する]からスキャン保存を実行 (以下、本操作をCreate操作S1と呼ぶ) • ファイリング設定をONに設定して、スキャン、またはコピーを実行 (以下、本操作をCreate操作S2と呼ぶ) (取り出しジョブ) • 操作パネルで、[ドキュメントファイリング]からTable 7.3で記述しているStorage/retrievalのCreate操作で保存されたファイルを選択し、[今すぐ印刷]、または[設定を変更して印刷する]から印刷を実行 • 操作パネルで、[ドキュメントファイリング]からTable 7.3で記述しているStorage/retrievalのCreate操作で保存されたファイルを選択し、[送信する]から送信を実行
	Read	(保存ジョブ) • Create操作S2を実行後、操作パネルで、[ジョブ状況]の、コピー時は[プリント]、スキャン時は[スキャナー]から[予約/実行中のジョブ]を選択 (取り出しジョブ) • 操作パネルで、[ジョブ状況]の、印刷時は[プリント]、送信時は[スキャナー]から[予約/実行中のジョブ]を選択
	Modify	N/A
	Delete	(保存ジョブ) • Create操作S1を実行後、原稿読み込み中に操作パネルで、[リセット]、または[読み込み中止]を実行 • Create操作S2を実行後、スキャン時はScanジョブ、コピー時はCopyジョブのDeleteを実行 (取り出しジョブ) • 印刷実行後、操作パネルで、[印刷中止]、または[ジョブ状況]→[プリント]→[予約/実行中のジョブ]からCreate操作で作成されたジョブを中止/削除 • 送信実行後、操作パネルで、[ジョブ状況]→[スキャナー]→[予約/実行中のジョブ]からCreate操作で作成されたジョブを中止/削除

7.4 識別と認証

本節では主に、6.2.4 節の必須 FIA 要件に関する要約仕様を記述する。

FIA_AFL.1

操作パネルおよびWebページからTOEを操作、またはクライアントPCからプリンタードライバーを介した印刷を実行する際に要求される利用者パスワード認証において、連続して3回認証に失敗した場合、認証受付を停止、すなわち利用者パスワードをロックする。ロックからの経過時間が5分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアして認証受付が停止された状態から復帰する。本要件は内部認証にのみ適用される。

本要件に関するTSFインタフェースは、以下に示すとおりである。

- 操作パネル/Webページのユーザー認証画面でログイン操作
- MFD用のプリンタードライバーがインストールされているPCから印刷を実行

FIA_ATD.1

TSFは、利用者ログイン名、利用者役割の利用者属性を定義し、維持することができる。

本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録/修正

FIA_PMG_EXT.1

TSF は新規利用者登録における利用者パスワードの登録、および登録済み利用者の利用者パスワードの変更を行う管理機能を持つ。このとき、アルファベットの大文字、小文字、数字、および特殊文字 (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” を含む) からなるパスワードのみを受け入れる。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録/修正

最小パスワード長は、組込み管理者により 15 文字以上に設定可能である。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[システム設定]→[セキュリティ設定]→[パスワードの変更]から最小パスワード長を変更

FIA_UAU.1 / FIA_UID.1

TSF は、操作パネルおよび Web ページから TOE を操作、またはクライアント PC からプリンタードライバーを介した印刷を実行する際に、管理者を含む利用者の識別認証を行う。
TSF は、以下の 2 種類の識別認証方式をサポートする。

- 内部認証方式: TOE 本体内に登録されている利用者情報を利用する認証方式。常に有効。
- ネットワーク認証方式: 外部の LDAP 認証サーバーに登録されている利用者情報を利用する認証方式。管理者の設定により、有効/無効を変更可能。

操作パネルおよび Web ページから TOE を操作する場合、TSF は TOE の操作を許可する前に利用者ログイン名、利用者パスワードおよび認証先の入力を要求する。認証先は、ネットワーク認証方式が無効の場合は TOE 本体内のみ、ネットワーク認証方式が有効の場合は TOE 本体内および TOE に登録されている LDAP 認証サーバーから選択する。入力された利用者ログイン名および利用者パスワードが、選択された認証先に登録されている利用者情報と合致することを選択された認証先で検証する。ただし、入力された利用者ログイン名が TOE の組込み管理者(admin)である場合は、認証先に関わらず、TOE 本体内に登録されている組込み管理者情報と合致することを TOE 本体内で検証する。検証の結果、登録されている利用者情報と合致した場合のみ、TSF は識別認証された利用者と判断し、その利用者に割り当てられた利用者役割の範囲内で TOE の操作を許可する。ただし、認証先が LDAP 認証サーバーで、識別認証された利用者に利用者役割が割り当てられていない場合は、一般利用者(U.NORMAL)の範囲内で TOE の操作を許可する。
クライアント PC からプリンタードライバーを介した印刷を実行する場合、TSF はプリンタードライバーから文書データと併せてプリンタードライバーの設定画面で入力された利用者ログイン名および利用者パスワードの情報を受信する。受信した利用者ログイン名および利用者パスワードが、ネットワーク認証方式が無効の場合は TOE 本体内に登録されている利用者情報と合致することを TOE 本体内で、ネットワーク認証方式が有効の場合はデフォルト接続先に設定されている LDAP 認証サーバーに登録されている利用者情報と合致することを LDAP 認証サーバーで検証する。ただし、受信した利用者ログイン名が TOE の組込み管理者(admin)である場合は、ネットワーク認証方式の有効/無効に関わらず、TOE 本体内に登録されている組込み管理者情報と合致することを TOE 本体内で検証する。検証の結果、登録されている利用者情報と合致した場合のみ、TSF は受信した文書データを識別認証された利用者により投入された利用者データと判断し、TOE 本体内に格納する。それ以外の場合、TSF は受信した文書データを TOE 本体内に格納せず、上書き消去により破棄する。
いずれの識別認証方式またはインタフェースにおいても、識別認証される前に許可されるアクションはない。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネル/Web ページのユーザー認証画面でログイン操作
- MFD 用のプリンタードライバーがインストールされている PC から印刷を実行

FIA_UAU.7

操作パネルでの認証試行時、入力したパスワードの文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。
Web ページでの認証試行時は、クライアントに対しパスワード形式の入力を指定する。これは、クライアントの Web ブラウザーに対し、利用者が入力した文字を代替文字のような方式で隠蔽するよう要求する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネル/Web ページのユーザー認証画面でログイン操作

FIA_USB.1

TSF は利用者識別認証により、各利用者を特定し、利用者ログイン名、利用者役割の利用者属性をサブジェクトに関連づける。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネル/Web ページのユーザー認証画面でログイン操作

7.5 セキュリティ管理

本節では主に、6.2.5 節の必須 FMT 要件に関する要約仕様を記述する。

FMT_MOF.1

TSF は以下の管理機能について、識別認証された管理者(U.ADMIN)のみに使用を許可する。

- 個人情報及び本機内データの初期化 (Initialize Private Data / Data in Machine)

本要件に関する TSF インタフェースは、以下に示すとおりである

- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を起動

FMT_MSA.1

TSF は、自身の利用者ログイン名および利用者役割を問い合わせる機能を、識別認証された全ての内部認証利用者に提供する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]から自身のユーザーを問い合わせ

TSF は、内部認証利用者の利用者ログイン名および利用者役割を作成、改変および削除する機能と、自身以外の内部認証利用者の利用者ログイン名および利用者役割を問い合わせる機能を、識別認証された管理者(U.ADMIN)のみに提供する。なお、作成する機能は内部認証利用者を新規に登録する時にのみ提供され、削除する機能は登録された内部認証利用者を削除する時にのみ提供される。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録/修正/問い合わせ/削除

FMT_MSA.3

TSF は、内部認証利用者を新規に登録する時、利用者役割である所属権限グループの初期値を User すなわち U.NORMAL とする。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録

TSF は、利用者データを生成する時、それを生成した利用者の利用者ログイン名を利用者データの所有者情報の初期値として割り当てる。
本要件に関する TSF インタフェースは、FDP_ACC.1/FDP_ACF.1 の TSF インタフェースに準じる。

FMT_MTD.1

TSF は、自身の利用者パスワードを変更する管理機能を、識別認証された全ての内部認証利用者に提供する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]から自身のユーザーを修正

TSF は、内部認証利用者の利用者パスワードを作成および削除する機能と、自身以外の内部認証利用者の利用者パスワードを変更する管理機能を管理者のみに提供する。なお、作成する機能は内部認証利用者を新規に登録する時にのみ提供され、削除する機能は登録された内部認証利用者を削除する時にのみ提供される。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録/修正/削除

TSF は、上記に加え、以下の TSF データを管理する機能を管理者のみに提供する。

- 最小パスワード長 (改変) ※組込み管理者のみに提供
- 識別認証方式 (改変)
- 日付/時刻 (改変)
- 監査ログ送信先 (問い合わせ/改変)
- 自動ログアウト時間 (問い合わせ/改変)
- アドレス帳 (登録/改変/削除)
- 認証サーバー設定 (登録/改変/削除)
- IP アドレス設定 (改変)
- メール送信サーバー設定 (問い合わせ/改変)

本要件に関する TSF インタフェースは、Table 7.5 に示すとおりである。

Table 7.5: FMT_MTD.1 に関する TSF インタフェース

管理機能	インタフェース
最小パスワード長の変更	• 操作パネルの設定モード/Webページで、[システム設定]→[セキュリティ設定]→[パスワードの変更]から最小パスワード長を変更
識別認証方式の変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[初期設定]から認証先設定を変更
日付/時刻の設定	• 操作パネルの設定モード/Webページで、[システム設定]→[共通設定]→[日付/時刻設定]から日時を設定
監査ログ送信先の設定	• 操作パネルの設定モード/Webページで、[システム設定]→[セキュリティ設定]→[監査ログ]→[ストレージ/送信設定]から送信先を設定
自動ログアウト時間の設定	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[初期設定]から自動ログアウト設定を変更
アドレス帳の管理	• 操作パネルで、[アドレス帳]から新規登録/編集/削除を実行 • Webページで、[アドレス帳]→[アドレス帳]から新規登録/編集/削除を実行
認証サーバーの設定	• 操作パネルの設定モード/Webページで、[システム設定]→[ネットワーク設定]→[LDAP設定]からLDAP認証サーバーを登録/修正/削除
IP アドレスの設定	• 操作パネルの設定モード/Webページで、[システム設定]→[ネットワーク設定]→[プロトコル設定]からIPv4を設定
メール送信サーバーの設定	• 操作パネルの設定モード/Webページで、[システム設定]→[ネットワーク設定]→[サービス設定]の[SMTP]タブから設定

FMT_SMF.1

TSF は、以下の管理機能を提供する。

- 内部認証利用者の登録/削除

- 内部認証利用者の利用者パスワードの変更
- 内部認証利用者の利用者ログイン名の変更
- 内部認証利用者の利用者役割の変更
- 監査ログ送信先の設定
- 最小パスワード長の変更
- 識別認証方式の変更
- 権限グループの管理
- 日付/時刻の設定
- 自動ログアウト時間の設定
- 個人情報及び本機内データの初期化の起動
- アドレス帳の管理
- 認証サーバーの設定
- IP アドレスの設定
- メール送信サーバーの設定

本要件に関する TSF インタフェースは、Table 7.6 に示すとおりである。

Table 7.6: FMT_SMF.1 に関する TSF インタフェース

管理機能	インタフェース
内部認証利用者の登録/削除	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを登録/削除
内部認証利用者の利用者パスワードの変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
内部認証利用者の利用者ログイン名の変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
内部認証利用者の利用者役割の変更	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正
最小パスワード長の変更	• FMT_MTD.1のTSFインタフェースに準じる
識別認証方式の変更	• FMT_MTD.1のTSFインタフェースに準じる
権限グループの管理	• 操作パネルの設定モード/Webページで、[ユーザー管理]→[権限グループリスト]から権限グループを登録/修正、またはグループを工場出荷値に戻す
日付/時刻の設定	• FMT_MTD.1のTSFインタフェースに準じる
監査ログ送信先の設定	• FMT_MTD.1のTSFインタフェースに準じる
自動ログアウト時間の設定	• FMT_MTD.1のTSFインタフェースに準じる
個人情報及び本機内データの初期化の起動	• FMT_MOF.1のTSFインタフェースに準じる
アドレス帳の管理	• FMT_MTD.1のTSFインタフェースに準じる
認証サーバーの設定	• FMT_MTD.1のTSFインタフェースに準じる
IP アドレスの設定	• FMT_MTD.1のTSFインタフェースに準じる
メール送信サーバーの設定	• FMT_MTD.1のTSFインタフェースに準じる

なお、TSF はストレージ暗号化に関する管理機能を提供しない。ストレージ暗号化は常に行われるからである。

FMT_SMR.1

TSF は、役割に関し、権限グループ (authority groups) の機能を持つ。
組込の権限グループとして、管理者権限 (Admin) およびユーザー権限 (User) という二つのグループを持ち、各々U.ADMIN および U.NORMAL に相当する。組込の権限グループを改変または削除することはできない。
これに加え、管理者は追加の権限グループを作成可能である。権限グループを作成する際、組込のユーザー権限をモデルとして、その任意の部分を制限できる。

各利用者を各権限グループに割り当てること、および、権限グループを作成、改変、または削除することは、管理者だけに可能である。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[権限グループリスト]から権限グループを修正、またはグループを工場出荷値に戻す
- 操作パネルの設定モード/Web ページで、[ユーザー管理]→[ユーザーリスト]からユーザーを修正

7.6 TSF の保護

本節では主に、6.2.6 節の必須 FPT 要件に関する要約仕様を記述する。

FPT_SKP_EXT.1

TSF は、対称鍵である鍵暗号鍵を平文で不揮発性メモリー1 に保存するが、管理者を含む全ての利用者にこの鍵暗号鍵を読み出すための機能を提供していない。また、不揮発性メモリー1は基板上に半田付けされているため、取り外しは不可能である。
TSF は、対称鍵であるストレージ鍵を鍵暗号鍵で暗号化して不揮発性メモリー2 に保存し、TOE の電源 ON 時にこの暗号化されたストレージ鍵を読み出して鍵暗号鍵で復号した平文のストレージ鍵を揮発性メモリーに保存するが、管理者を含む全ての利用者にこれらストレージ鍵を読み出すための機能を提供していない。また、平文のストレージ鍵は電源断で揮発して破棄される。
TSF は、対称鍵および MAC 鍵を含むセション鍵を平文で揮発性メモリーに保存するが、管理者を含む全ての利用者にこのセション鍵を読み出すための機能を提供していない。また、このセション鍵は電源断で揮発して破棄される。
TSF は、TLS 鍵ペアのプライベート鍵をストレージ暗号鍵で暗号化して内部ストレージに保存するが、このプライベート鍵を読み出すための機能を提供していない。

FPT_STM.1

TSF は、FAU_GEN.1/FAU_GEN.2 で示した監査対象イベントを監査ログとして記録する際、TOE のシステムクロックからタイムスタンプを発行する。
本要件に関する TSF インタフェースは、FAU_GEN.1/FAU_GEN.2 の TSF インタフェースに準じる。

FPT_TST_EXT.1

TSF は、TOE 起動時に以下の自己テストを行う。

- エントロピー源のヘルステスト: ES が故障していないことを保証するため、乱数生成要求および乱数読み出しを繰り返し実行することで 4096 ビットの乱数を発生させ、乱数生成が所定の時間内に完了すること、連続した同一ビット値の長さが所定の閾値以下であること、および出現ビット値の偏りが所定の許容範囲を超えないことを確認する。
- DRBG のヘルステスト: NIST SP 800-90A に基づき、Instantiate、Generate および Reseed の機能について既知解テストを行う。
- HBA 暗号回路のテスト: 暗号回路が故障していないことを保証するため、AES 公募要件(http://csrc.nist.gov/archive/aes/katmct/katmct.htm)の既知解テストを行う。
- TSF イメージ検証: TSF を実装するファームウェアに毀損がないことを保証するため、コントローラーファームウェアはハッシュ(SHA-256)、その他のファームウェアは 16bit 誤り検出符号(チェックサム)により自己検証を行う。

以上の自己テストの全部または一部にエラーが検出されれば、TOE は起動を中止し、電源断まで動作を停止する。
TSF は、ハードウェア TSF とソフトウェア TSF から構成されている。ハードウェア TSF はエントロピー源および HBA 暗号回路であり、エントロピー源のヘルステストおよび HBA 暗号回路のテストにより、それらを実際に動作させて故障の検出を行っている。ソフトウェア TSF はファームウェア上に実装されており、TSF イメージ検証により、TSF 実行コードの完全性を検証している。また、TOE が従う標準のうち NIST SP 800-90A が自己テストの実施を要求しているが、これは DRBG のヘルステストにより満たされる。以上のことから、TSF が正しく動作していることを実証するためにテストが十分なものであると言える。

本要件に関する TSF インタフェースは、以下に示すとおりである。

- MFD の電源 ON (停電からの復旧も同等)

FPT_TUD_EXT.1

TSF は、TOE のファームウェアバージョンを問い合わせる能力を管理者に、TOE のファームウェアに対するアップデートを開始する能力を組込み管理者に提供する。
TSF は、上記ファームウェアアップデートを開始する前に、アップデート対象のファームウェアの真正性を検証する手段を組込み管理者に提供する。ファームウェア本体と共にファームウェアファイルの一部として提供されるデジタル署名から FCS_COP.1(b)に従う RSA 署名検証により復号されたハッシュ値と、アップデート対象のファームウェアを全てまとめた状態から FCS_COP.1(c)に従う SHA-256 の暗号ハッシングサービスにより算出されたハッシュ値を照合し、その値が一致することを確認することにより、ファームウェア真正性を検証する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モード/Web ページで、[ステータス]→[ファームウェアバージョン]からファームウェアバージョンを問い合わせ
- 操作パネルからメンテナンス用モードへ移行し、ファームウェアアップデートを実行

7.7 TOE アクセス

本節では主に、6.2.7 節の必須 FTA 要件に関する要約仕様を記述する。

FTA_SSL.3

TSF は、操作パネルでログイン (識別認証) した利用者について、無操作の後に自動ログアウトする機能を提供する。その猶予時間は管理者により設定された時間であり、最小で 10 秒、最大で 240 秒(4 分)である。
TSF は、Web ページでログイン (識別認証) した利用者について、無操作の後に自動ログアウトする機能を提供する。その猶予時間は 300 秒間 (5 分間) 固定である。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネル/Web ページで、ユーザー認証画面からログインした状態で無操作

7.8 高信頼パス/チャネル

本節では主に、6.2.8 節の必須 FTP 要件に関する要約仕様を記述する。

FTP_ITC.1

TSF は、高信頼 IT 製品である認証サーバー、監査サーバー、FTP サーバーおよびメールサーバーとの通信を保護するため、それらと通信を行う際に、FCS_TLS_EXT.1 に則った TLS1.2 を使用した高信頼チャネルを介して通信を開始する。この通信は、TOE と高信頼 IT 製品のどちらからでも開始することができる。
TSF は、以下の機能を利用する際に、高信頼チャネルを介して高信頼 IT 製品との通信を開始する。

- ネットワーク認証による識別認証
- 監査ログデータの送信
- ファイルサーバー送信
- E-mail 送信

本要件に関する TSF インタフェースは、以下に示すとおりである。

- 認証サーバーとの通信:
  - 操作パネル/Web ページのユーザー認証画面でログイン操作
- 監査サーバーとの通信:
  - FAU_GEN.1/FAU_GEN.2 の TSF インタフェースに準じる
- FTP サーバーとの通信:

  - MFD のスキャナーユニットに原稿をセット後、操作パネルで、[シンプルスキャン]、または[FTP/Desktop]からファイルサーバー送信スキャンを実行
  - 操作パネルで、[ドキュメントファイリング]の[送信する]からファイルサーバー送信を実行
- メールサーバーとの通信:
  - MFD のスキャナーユニットに原稿をセット後、操作パネルで、[シンプルスキャン]、または[E-Mail]から E-mail 送信スキャンを実行
  - 操作パネルで、[ドキュメントファイリング]の[送信する]から E-mail 送信を実行

FTP_TRP.1(a) / FTP_TRP.1(b)

TSFは、以下のように、TOEとの通信が既知の終端との間で行われることを保証するため、高信頼の通信パスを確立する。

- クライアントとTOEの Web ページとの間の通信は、通信データを盗聴等から保護する高信頼通信パスを提供するため、HTTPS 通信機能を使用する。HTTPS 通信は、リモート管理者、またはリモート利用者がクライアント上の Web ブラウザーから HTTPS 通信で接続することで、TOE の Web ページとの通信を開始する。クライアントからの識別認証およびすべてのリモート操作は、HTTPS 通信を使用している場合のみ実行される。
- クライアントのプリンタードライバーと TOE との間の通信は、送信される印刷データを盗聴等から保護する高信頼通信パスを提供するため、IPP over TLS 通信機能を使用する。リモート管理者、またはリモート利用者がクライアントのアプリケーションプログラム等における印刷操作を介して、クライアントのプリンタードライバーから IPP over TLS 通信で接続することで、TOE との通信を開始する。クライアントのプリンタードライバーからの識別認証およびすべてのリモート操作は、IPP over TLS 通信を使用している場合のみ実行される。

本要件に関する TSF インタフェースは、以下に示すとおりである。

- Web ページから TOE をリモート操作
- MFD 用のプリンタードライバーがインストールされている PC から印刷を実行

7.9 現地交換可能な不揮発性ストレージデバイス上の秘密のデータ 1

本節では主に、6.2.9 節の条件付き必須要件 B1 に関する要約仕様を記述する。

FPT_KYP_EXT.1

本 TOE で FCS_KYC_EXT.1 における鍵チェインを構成する鍵は鍵暗号鍵とストレージ鍵である。
TSF は、鍵暗号鍵を基板上に半田付けされた不揮発性メモリー1 内に平文で保存するが、内部ストレージには保存しない。
TSF は、不揮発性メモリー2 内に鍵暗号鍵で暗号化したストレージ鍵を保存し、TOE の電源 ON 時に鍵暗号鍵で復号した平文のストレージ鍵を揮発性メモリーに保存するが、内部ストレージには保存しない。

FCS_KYC_EXT.1

本 TOE で鍵チェインにおける BEV はストレージ鍵である。ストレージ鍵は、FCS_RBG_EXT.1 による RBG で生成された乱数を用いて 256 ビット長で生成され、FCS_COP.1(f)による鍵暗号化を用いて、FCS_RBG_EXT.1 による RBG で生成された乱数を用いて生成された 256 ビット長の鍵暗号鍵で暗号化/復号される。よって、TSF は、鍵チェインの各段階において、256 ビット以上のセキュリティ強度を確保している。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- TOE 設置作業後の初回起動
- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行後、TOE を再起動
- MFD の電源 ON (停電からの復旧も同等)

FDP_DSK_EXT.1

TSF は、文書データ、ジョブ情報および各種 TSF データを現地交換可能な不揮発性ストレージである内部ストレージに書き込む際、必ず FCS_COP.1(d)に従い暗号化してから書き込み、内部ストレージから読み出す際に復号する。
ガイダンスに従い、所定の手順で本 TOE を構成することにより、暗号化は自動的に有効化される。
内部ストレージには、暗号化されない領域がある。具体的には、パーティションテーブル等のデバイス管理領域、TOE ファームウェアを格納したブート領域、および、ガイダンスを格納した領域である。暗号化される領域とされない領域はパーティション単位で区別され、暗号化されない領域には利用者文書データおよび秘密の TSF データは含まれない。
本要件に関する TSF インタフェースは、FDP_ACC.1/FDP_ACF.1 および FMT_SMF.1 の TSF インタフェースに準じる。

7.10 画像上書き

本節では主に、6.2.10 節のオプション要件 C2 に関する要約仕様を記述する。

FDP_RIP.1(a)

TSF は、以下のとおり、イメージデータを上書き消去する。

- ジョブ処理のために内部ストレージにスプール保存されたイメージデータを、当該ジョブ完了または中止時に上書き消去する。
- ドキュメントファイリング機能により内部ストレージに保存されたイメージデータを、利用者の操作により削除される際に上書き消去する。

上書きにおいて書き込むデータおよび書き込む回数は、乱数による1回上書きがデフォルトとして設定されているが、組込み管理者が操作パネルの設定モード、または Web ページで、[システム設定]→[セキュリティ設定]→[管理設定]内の[データエリア消去設定]から設定を変更することが可能である。書き込むデータは、乱数か 0x00～0xFF の間から1つの値を選択することができる。また、書き込み回数は、1～10 回の間で設定することが可能で、1回ごとに書き込むデータを指定することができる。
TSF は上記の各機能を所定のタイミングで必ず起動し、非活性化する手段を提供しない。これらの機能は、ガイダンスにおいて[各ジョブ完了後の自動消去 (Auto Clear at Job End)]と呼ばれる。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- FDP_ACC.1/FDP_ACF.1 の D.USER.JOB アクセス制御における、Create/Delete 操作の TSF インタフェースに準じる
- FDP_ACC.1/FDP_ACF.1 の D.USER.DOC アクセス制御における、Storage/retrieval の Delete 操作の TSF インタフェースに準じる

7.11 データの完全削除

本節では主に、6.2.11 節のオプション要件 C3 に関する要約仕様を記述する。

FDP_RIP.1(b)

TSF は、操作パネルにて管理者の要求に応じ、内部ストレージ上にあるすべての利用者データおよび TSF データを上書き消去する。このとき、併せてストレージ鍵に関する鍵暗号鍵を再生成し、以前の鍵暗号鍵を破棄する。本機能は、主に TOE を手放す際に使用する。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を起動

7.12 現地交換可能な不揮発性ストレージデバイス上の秘密のデータ 2

本節では主に、6.2.12 節の選択ベース要件 D1 に関する要約仕様を記述する。

FCS_COP.1(d)

TSF は、FDP_DSK_EXT.1 に従い利用者データおよび TSF データを暗号化および復号する際、次のように行う。

- 暗号鍵:
  FCS_CKM.1(b)で生成された 256 ビット長のサイズを持つ暗号鍵を用いる。
- 暗号アルゴリズム:
  ISO/IEC 18033-3 で規定される AES アルゴリズム、および、ISO/IEC 10116 で規定される CBC モードを用いる。

本要件に関する TSF インタフェースは、FDP_DSK_EXT.1 の TSF インタフェースに準じる。

FCS_COP.1(f)

TSF は、FCS_KYC_EXT.1 に従う鍵暗号化および復号の際、上記 FCS_COP.1(d) と同様に行う。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- TOE 設置作業後の初回起動
- 操作パネルの設定モードで、[システム設定]→[セキュリティ設定]→[個人情報及び本機内データの初期化]から初期化を実行後、TOE を再起動
- MFD の電源 ON (停電からの復旧も同等)

7.13 保護された通信

本節では主に、6.2.13 節の選択ベース要件 D2 に関する要約仕様を記述する。

FCS_TLS_EXT.1

TSF は、TLS 通信として TLS1.2(RFC 5246)をサポートする。
TSF が TLS 通信においてサポートする暗号スイートは TLS_RSA_WITH_AES_128_CBC_SHA, 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 および TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 である。
TSF は、FCS_RBG_EXT.1 および FCS_CKM.1(a)に従い、TLS 通信で用いるサーバー秘密鍵および公開鍵を生成する。
TSF は、FCS_COP.1(a)に従い、TLS 通信における通信データの暗号化および復号を行う。
TSF は、FCS_COP.1(b)に従い、FTP_ITC.1 に示す各種サーバーとの TLS 通信において、サーバー証明書検証を行う。
TSF は、FCS_COP.1(c)および FCS_COP.1(g)に従い、鍵付きハッシングによるメッセージ認証符号(HMAC)を用いた TLS 通信を行う。
本要件に関する TSF インタフェースは、FTP_ITC.1 の TSF インタフェースに準じる。

FCS_HTTPS_EXT.1

TSF は、TOE とリモート管理者との間の通信および TOE とリモート利用者との間の通信において、FTP_TRP.1(a)および FTP_TRP.1(b)に従った高信頼パスを提供するため、RFC2818 に適合し、FCS_TLS_EXT.1 に則った TLS プロトコルを使用した HTTPS 通信を適用する。
TSF は、リモート管理者またはリモート利用者によってクライアント PC 上の Web ブラウザーから TOE の Web ページに対して接続要求が行われた場合に、TOE とクライアント PC との間で TLS 通信のネゴシエーションを確立した後、HTTPS 通信を開始する。
クライアント PC からの TOE の Web ページ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。
本要件に関する TSF インタフェースは、以下に示すとおりである。

- Web ページから TOE をリモート操作

FCS_COP.1(g)

TSF は、FIPS PUB198-1 に規定された The Keyed-Hash Message Authentication Code および FIPS PUB180-3 に規定された Secure Hash Standard を満たす、メッセージダイジェスト長が 160 ビットで鍵長 160 ビットの HMAC-SHA-1、またはメッセージダイジェスト長が 256 ビットで鍵長 256 ビットの HMAC-SHA-256 に従い、鍵付きハッシングによるメッセージ認証符号(HMAC)を用いた通信を行う。
ハッシングには、FCS_COP.1(c)に従うSHA-1、またはSHA-256の暗号ハッシングサービスを使用し、ハッシュ値を計算する。
本要件に関する TSF インタフェースは、FCS_TLS_EXT.1 の TSF インタフェースに準じる。

7.14 高信頼アップデート

本節では主に、6.2.14 節の選択ベース要件 D3 に関する要約仕様を記述する。

FCS_COP.1(c)

TSF は、FPT_TUD_EXT.1 および FCS_TLS_EXT.1 におけるハッシュ値の計算に、ISO/IEC 10118-3:2004 に適合する SHA-1、または SHA-256 に従った暗号ハッシングサービスを使用する。
本要件に関する TSF インタフェースは、FPT_TUD_EXT.1 および FCS_TLS_EXT.1 の TSF インタフェースに準じる。

8 付章

本章では、参照文献および用語定義を示す。

8.1 用語

本 ST で使用される用語の内、2 章で適合主張している CC および PP で定義された用語については、その定義に従う。それ以外の用語の定義を Table 8.1 に示す。

Table 8.1: ST で使用される用語の定義

用語	定義
IPアドレス	IPにおいて通信相手となる各機器を識別するための呼出符号。
TOEのWebページ / Webページ	TOEであるMFDのリモート操作用I/Fとして、MFD内蔵Webサーバーが提供するWebページ。
Rijndael	AESに採用された暗号アルゴリズム。開発者はベルギーのJoan Daemen氏とVincent Rijmen氏。
イメージデータ	本書では特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
エンジンユニット	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。
揮発性メモリー	電源を切れば記憶内容が消失する記憶装置。
基板	プリント基板に部品を半田付け実装したものを指す。
コントローラーユニット	MFD全体を制御する装置。TOEのファームウェアを実行するためのCPU, 揮発性メモリー, HBA, ES, 不揮発性メモリー等を有する。
コントローラーファームウェア	MFDのコントローラーユニットを制御するファームウェア。
再操作	ドキュメントファイリング機能により保存したイメージデータに対し、印刷、送信、プレビュー、または削除を行うこと。
スキャナーユニット	原稿をスキャンしてイメージデータを得る装置。コピー、スキャン送信およびスキャン保存の際に使用する。
スキャン保存	ドキュメントファイリング機能の一つ。原稿を読み取って得たイメージデータを内部ストレージに保存するが、印刷や送信は実行しない。
スプール	入出力効率のため、ジョブのイメージデータを一時的に内部ストレージに保持すること。
操作パネル	MFDの正面にあるユーザーインタフェース用ユニット。機能キーおよびタッチ操作式の液晶ディスプレイを含む。
ドキュメントファイリング	MFDが取り扱うイメージデータを利用者が後で再操作できるようにするため、内部ストレージに保存する機能。
内部認証利用者	内部認証時に参照されるTOE本体内に登録された利用者
ファームウェア	機器のハードウェアを制御するために、機器に組み込まれたソフトウェア。
不揮発性メモリー	電源を切っても記憶内容を保持することができる記憶装置。
メモリー	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。
ロック	誤ったパスワードが連続して入力された等で、パスワードの受付を停止した状態。

8.2 略語

本 ST で使用される略語の定義を Table 8.2 に示す。

Table 8.2: ST で使用される略語の定義

略語	定義
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CC	Common Criteria
CM	Configuration Management
CPU	Central Processing Unit

略語	定義
DRBG	Deterministic Random Bit Generator
ES	Entropy Source
FIPS PUB 197	Federal Information Processing Standards Publication 197
HBA	Host Bus Adapter
HCD	Hardcopy Device
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL/TLS
I/F	Interface
IP	Internet Protocol
IPP	Internet Printing Protocol
IPP-SSL	IPP over SSL/TLS
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MFD	Multifunction Device
MFP	Multifunction Printer, Multifunction Peripheral
NIC	Network Interface Card, Network Interface Controller
OS	Operating System
PC	Personal Computer
PP	Protection Profile
RBG	Random Bit Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality