TASKalfa 4012i, TASKalfa 3212i
ハードディスク、データセキュリティキット、ファクス付きモデル
セキュリティターゲット
第 1.21 版

2018 年 9 月 5 日

京セラドキュメントソリューションズ株式会社

- 更新履歴 -

日付	Version	更新内容
2017/12/01	0.80	・初版作成
2018/02/02	0.85	・指摘事項修正
2018/02/22	0.90	・指摘事項修正
2018/04/02	0.95	・指摘事項修正
2018/07/02	1.00	・指摘事項修正
2018/08/20	1.10	・指摘事項修正
2018/09/03	1.20	・指摘事項修正
2018/09/05	1.21	・指摘事項修正

～ 目次 ～

～ 図目次 ～

～ 表目次 ～

1. ST 概説

1.1. ST 参照

ST 名称： TASKalfa 4012i, TASKalfa 3212i ハードディスク、データセキュリティキット、ファクス付きモデル セキュリティターゲット

ST バージョン： 第 1.21 版

作成日： 2018/09/05

作成者： 京セラドキュメントソリューションズ株式会社

1.2. TOE 参照

TOE 名称： TASKalfa 4012i, TASKalfa 3212i, TASKalfa 4012iG, TASKalfa 3212iG(KYOCERA), CS 4012i, CS 3212i(Copystar), 4062i, 3262i(TA Triumph-Adler/UTAX) ハードディスク、データセキュリティキット、ファクス付きモデル

【注釈】
ハードディスク、データセキュリティキット、ファクス付きモデルとは、TASKalfa 4012i, TASKalfa 3212i, TASKalfa 4012iG, TASKalfa 3212iG, CS 4012i, CS 3212i, 4062i, 3262i に、次の追加オプションを付加した製品構成である

- ハードディスク : HD-12
- データセキュリティキット : Data Security Kit (E)
- ファクス : FAX System 12

TOE バージョン： システム : 2V6_20IS.C01.010
パネル : 2V6_70IS.C01.010
ファクス : 3R2_5100.003.012

開発者： 京セラドキュメントソリューションズ株式会社

対象 MFP： KYOCERA TASKalfa 4012i, KYOCERA TASKalfa 3212i,
KYOCERA TASKalfa 4012iG, KYOCERA TASKalfa 3212iG,
Copystar CS 4012i, Copystar CS 3212i,
TA Triumph-Adler 4062i, TA Triumph-Adler 3262i,
UTAX 4062i, UTAX 3262i

本TOEは、TOE名称で併記されているそれぞれのMFPの名称と、上記TOEに搭載される３種類のファームウェアの各バージョンの組み合わせで識別される。またMFPの製品名称は複数存在するが、それらは印刷速度や販売する仕向け地の違いだけであり、MFPの構成要素は全て同一である。

1.3. TOE 概要

1.3.1. TOE の種別

本STが定義するTOEは、主としてコピー機能、スキャン送信機能、プリンター機能、FAX機能、ボックス機能を有する複合機（Multi Function Printer：以下MFPと略称）である京セラドキュメントソリューションズ株式会社製MFP「TASKalfa 4012i, TASKalfa 3212i, TASKalfa 4012iG, TASKalfa 3212iG, CS 4012i, CS 3212i, 4062i, 3262i」である。このうち、HDDについては、オプションであるHD-12を装着し、FAX機能については、オプションであるFAX System 12 を装着することで利用可能となる。また、TOEのセキュリティ機能の一部は、MFP「TASKalfa 4012i, TASKalfa 3212i, TASKalfa 4012iG, TASKalfa 3212iG, CS 4012i, CS 3212i, 4062i, 3262i」の使用におけるオプション「Data Security Kit (E)」を購入し、MFPに対してライセンス情報を入力することで活性化され、これにより全てのセキュリティ機能が利用可能となる。

1.3.2. TOE の使用法

本TOEは、利用者が扱う様々な文書をコピー（複製）、プリント（紙出力）、送信（電子化）、保存（蓄積）することが可能である。TOEは、一般的なオフィスに設置され、単独で使用するだけでなく、LANに接続されて、ネットワーク環境でも使用される。ネットワーク環境では、ファイアウォールなどで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事を想定している。また、ローカルポート（USBポート）に接続されて使用される事も想定している。

この利用環境において、操作パネル上のボタン操作やネットワーク上及びローカル接続のクライアントPCからの操作により、上記機能を実施することが出来る。

図1.1 に一般的な利用環境を示す。

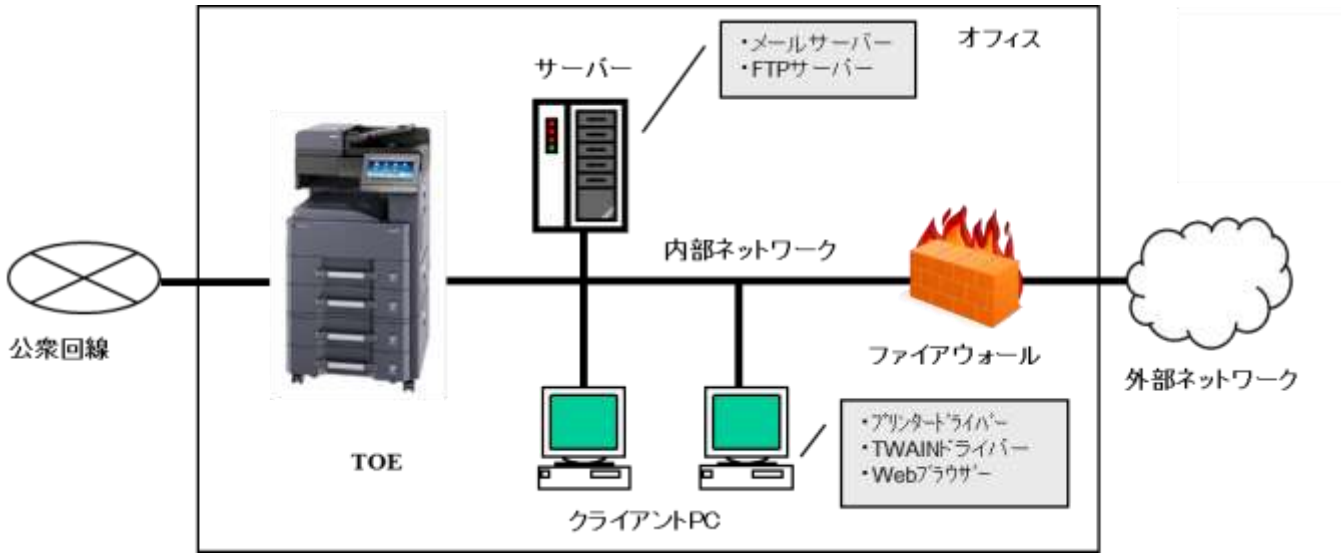


図 1.1 一般的な利用環境

TOEの一般機能を使用するための環境を以下に示す。

- 内部ネットワーク：
  ファイアウォールなどで外部ネットワークの不正アクセスから保護されたオフィス内のネットワーク環境。

- クライアント PC：
  内部ネットワークまたはローカルポート（USB ポート）経由で MFP と接続され、利用者からの指示で MFP の一般機能を利用することが出来る。
  クライアント PC には以下が必要となる
  - プリンタードライバー
  - TWAIN ドライバー
  - Web ブラウザー

- サーバー：
  MFP の文書を送信する際に利用される。以下の種類のサーバーが必要となる。
  - メールサーバー
  - FTP サーバー

- 公衆回線
  MFP の文書を FAX 送受信する際に、必要となる公衆回線網。

1.3.3. TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOEに必要なTOE以外のハードウェア/ソフトウェア・ファームウェアの名称を以下に示す。

- クライアント PC
  - プリンタードライバー：KX ドライバー
  - TWAIN ドライバー：Kyocera TWAIN ドライバー
  - Web ブラウザー：Microsoft Internet Explorer 11.0
- メールサーバー：IPsec(IKEv1)が使用できること
- FTP サーバー：IPsec(IKEv1)が使用できること

1.3.4. TOE の主要なセキュリティ機能の特徴

TOEは、利用者が扱う文書をコピー、プリント、スキャン送信、FAX送受信、ボックスに保存することが可能である。これらの文書の改ざん、漏洩を防止するために、TOEは利用者を識別認証する機能、画像データや機能へのアクセスを制御する機能、画像データを暗号化する機能、残存する画像データを上書き消去する機能、監査ログを生成し、参照させる機能、TOE自身をテストする機能、及びネットワークを保護する機能を備える。

1.4. TOE 記述

1.4.1. TOE の利用者

TOEの利用に関連する人物の役割を以下に定義する。

表 1.1 TOE の利用者

Designation		Explanation
U.USER 利用者		TOE の利用を許可された人。
	U.NORMAL 一般利用者	TOE を利用する人。一般利用者は、コピー、プリント、スキャン送信、FAX 送信、ボックスの各機能を利用することが出来る。
	U.ADMINISTRATOR 機器管理者	TOE を管理する人。機器管理者は、TOE に対する特権を有し、TOE を構成する機器の管理、及び TOE を正しく動作させるための導入と運用管理を行う。本 ST では、工場出荷時に予め登録されている管理者権限を持つ利用者（機器管理者）と、運用中に随時追加登録出来る管理者権限を持つ利用者（管理者）の両方を含む。

1.4.2. TOE の物理的構成

TOEの物理的構造の概念図を 図1.2 で示す。

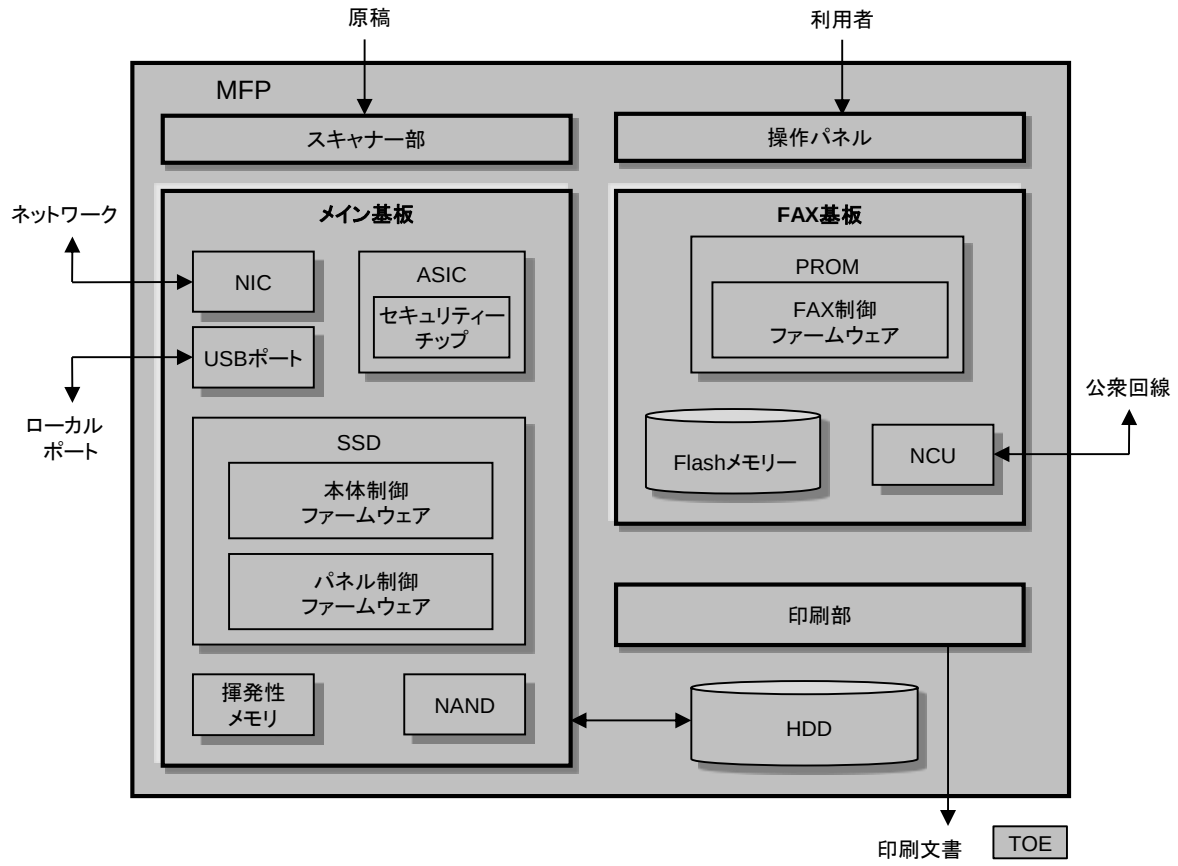


図 1.2 TOE の物理的構成図

TOE は、操作パネル、スキャナー部、印刷部、メイン基板、FAX 基板、HDD、SSD のハードウェアおよびそのファームウェアで構成される。
操作パネルは、TOE の利用者からの入力を受け付け、状態や結果を表示するハードウェアであり、スキャナー部、印刷部は、それぞれ MFP に対して原稿を入力し、また印刷物として出力するハードウェアである。
メイン基板は、TOE 全体の制御を行うための回路基板であり、メイン基板上の SSD に格納される形で本体制御ファームウェア、パネル制御ファームウェアが搭載されている。インターフェイスとして、ネットワークインターフェイス（NIC）とローカルインターフェイス（USB ポート）を持つ。
またメイン基板上の ASIC には、セキュリティ機能の一部の実装を分担するセキュリティチップが搭載されている。セキュリティチップでは、HDD 暗号化機能、HDD 上書き消去機能（後述）におけるセキュリティ演算処理を実現している。
FAX 基板には、FAX 通信を制御するための FAX ファームウェアが、FAX 基板上の PROM に格納される形で搭載されている。また、インターフェイスとして NCU を持つ。

また、記憶媒体として、メイン基板上に機器設定を保存する NAND、作業領域として使用する揮発性

メモリー、およびファームウェア格納用の SSD、FAX 基板上に FAX 送受信画像を保存する Flash メモリーとファームウェア格納用の PROM、メイン基板に接続され画像データやジョブデータを保存する HDD を持つが、いずれも取り外し可能な記憶媒体ではない。ここで、Flash メモリーには FAX 送受信画像のみが保存され、その他の基本機能が扱う画像データは HDD に保存される。また、SSD には画像データは保存されない。

HDDについては、販売地域により、HDDオプション搭載済みで販売される製品が存在する。

表 1.2 MFP 製品と HDD 構成

MFP 製品名称	販売地域	HDD 構成
TASKalfa 4012i, TASKalfa 4012iG, CS 4012i, CS 3212i, 4062i	-	HDD オプション搭載済み
TASKalfa 3212i	北米地域	HDD オプション搭載済み
	その他地域	HDD オプション未搭載
TASKalfa 3212iG, 3262i	-	HDD オプション未搭載

TOE の構成品の配布方法は以下の通りである。また、ガイダンスも TOE の一部である。

表 1.3 TOE 構成品の配布方法

TOE 構成	形態	配付方法	識別情報
MFP 本体（HDD オプション搭載済みの製品）	MFP 装置	クーリエ配送	表 1.2 で示す MFP 製品名称および TOE 参照で示すファームウェアバージョン情報＋大容量記憶装置:HDD320GB
MFP 本体（HDD オプション未搭載の製品）	MFP 装置	クーリエ配送	表 1.2 で示す MFP 製品名称および TOE 参照で示すファームウェアバージョン情報＋大容量記憶装置:なし
ハードディスク ※オプションとして装着が必要な場合	HDD ハードウェア	クーリエ配送	HD-12
ファクス	ファクスボード	クーリエ配送	FAX System 12
データセキュリティキット	紙媒体	クーリエ配送	Data Security Kit (E)
ガイダンス	紙媒体、DVD 内 PDF 形式ファイル	MFP 本体に同梱	表 1.4 に示す名称およびバージョン

※ファームウェアは MFP 本体にプレインストール

1.4.3. TOE の論理的構成

TOEの論理的構造の概念図を 図1.3 で示す。

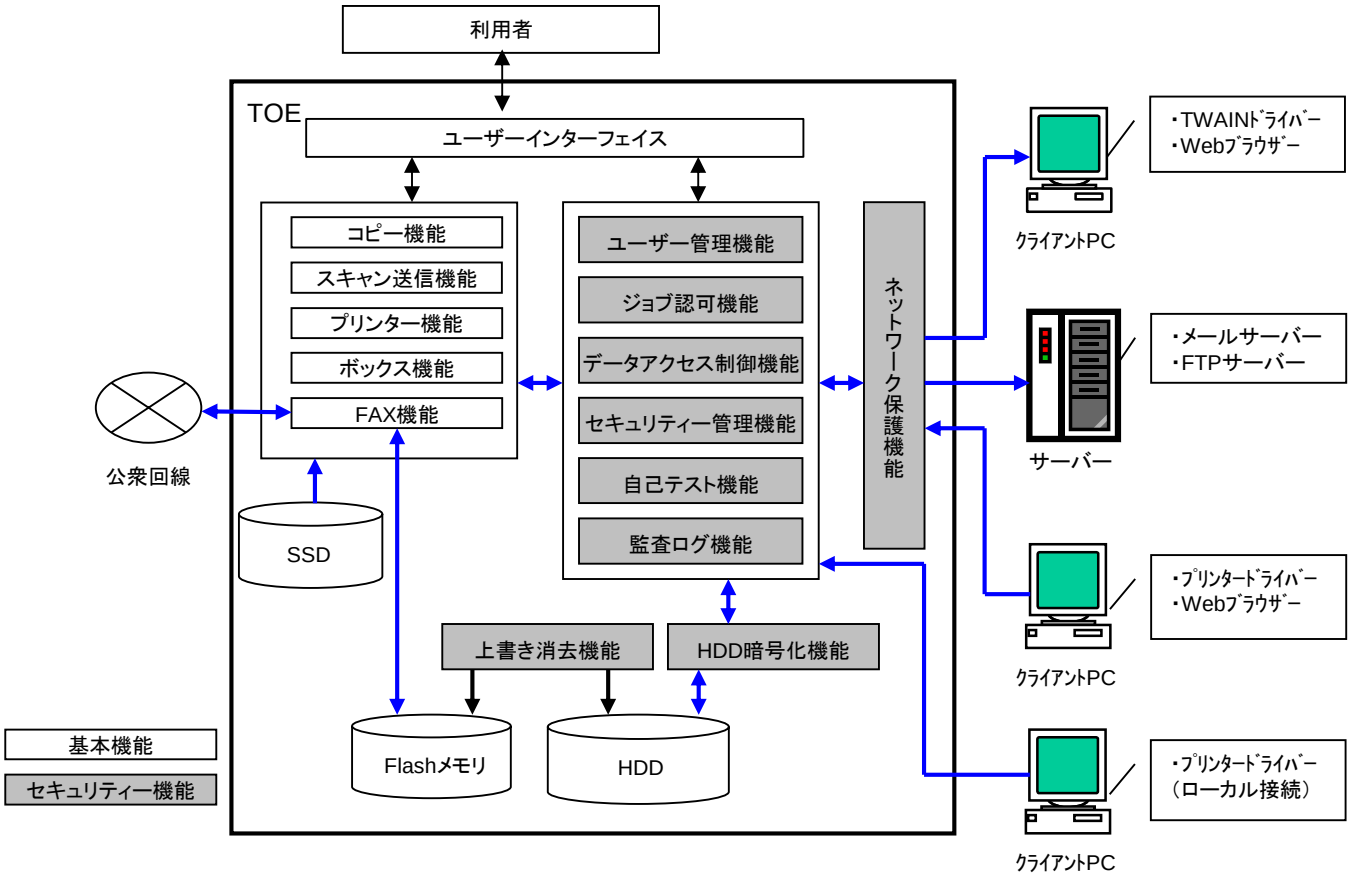


図 1.3 TOE の論理的構造図

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の機能を提供する。

- コピー機能
  一般利用者が、操作パネルから入力/操作を行うことにより、画像データを TOE のスキャナーから読込み、TOE の印刷部から出力する機能。(コピージョブの実行)

- スキャン送信機能
  一般利用者が、操作パネル、又はクライアント PC 上の TWAIN ドライバーから入力/操作を行うことにより、画像データを LAN 経由で接続されたクライアント PC、サーバー、及びローカル接続された USB メモリーに送信する機能。
  送信種別として、以下の種類の送信機能を持つ。(スキャン送信ジョブの実行)

- ✓ FTP 送信 （FTP サーバー）
- ✓ E-mail 送信（メールサーバー）
- ✓ TWAIN 送信 （TWAIN ドライバー）
- ✓ USB メモリー送信（USB メモリー）

- プリンター機能
  一般利用者が、LAN 経由、又はローカル接続されたクライアント PC から印刷指示することにより、受信した画像データを TOE の印刷部から出力する機能。ローカル接続された USB メモリーから印刷することも可能。
  印刷指示は、クライアント PC 上のプリンタードライバーから印刷指示する。また、USB メモリーからの印刷では、操作パネルから印刷指示する。（プリンター印刷ジョブの実行）

- FAX 機能
  公衆回線を通して、FAX 送受信を行う機能。FAX 送信ではスキャンした画像データを外部に送信し、FAX 受信では、受信した画像データを TOE の印刷部から出力、及び外部に転送することが出来る。（FAX 送信ジョブの実行）

- ボックス機能
  一般利用者が、画像データを HDD 上に保存、及び読み出して送信、印刷する機能。ボックス内で画像データを移動、結合することも出来る。ただし、FAX 機能で送受信する画像データは Flash メモリーに保存される。（ボックス保存ジョブ、ボックス送信ジョブ、ボックス印刷ジョブの実行）

  一般利用者が、操作パネルから入力/操作を行うか、もしくは、LAN 上、又はローカル接続されたクライアント PC から入力/操作を行うことにより、入力された画像データを HDD 上に保存する。また、FAX 機能で送受信する画像データを Flash メモリーに保存する。保存された画像データは、TOE の印刷部から出力、もしくは、クライアント PC、メールサーバーなどのサーバー、公衆回線上の他 FAX へ送信することが出来る。保存された画像データを削除することも可能である。ここで、クライアント PC からの入力にはプリンタードライバーを使用し、クライアント PC からの操作には、Web ブラウザーを使用する。
  送信種別として、以下の種類の送信機能を持つ。
  - ✓ FTP 送信 （FTP サーバー）
  - ✓ E-mail 送信（メールサーバー）
  - ✓ TWAIN 送信 （TWAIN ドライバー）
  - ✓ FAX 送信 （他 FAX）
  - ✓ USB メモリー送信（USB メモリー）

- ユーザーインターフェイス
  機器管理者、一般利用者が TOE の機能を利用するために、操作パネルからの入力/操作を受け付ける機能。状態や処理結果などの操作パネルへの表示も行う。

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の機能を提供する。

- ユーザー管理機能

  TOE の利用を、許可された利用者だけが行えるように、利用者を識別認証する機能。
  操作パネル及び､クライアント PC からの利用時にログインユーザー名とログインユーザーパスワードを入力させて識別認証を行う。ユーザー管理機能の中には、識別認証を連続して失敗した利用者に対してアクセスを一定時間禁止するユーザーアカウントロックアウト機能、識別認証を行う際のログインユーザーパスワードの入力に対してフィードバックを保護する機能、一定時間無操作状態が継続した場合に自動でログアウトする機能が含まれる。

- データアクセス制御機能

  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。
  アクセス制御機能の種別として以下がある。
  - ✓ 画像データへのアクセス制御機能
  - ✓ ジョブデータへのアクセス制御機能

- ジョブ認可機能

  TOE の基本機能を、許可された利用者のみが利用出来るように、機能の利用を制限する機能。
  ジョブ認可の種別として以下がある。
  - ✓ コピージョブ（コピー機能）
  - ✓ 印刷ジョブ（プリンター機能）
  - ✓ 送信ジョブ（スキャン送信機能）
  - ✓ FAX 送信ジョブ（FAX 機能）
  - ✓ FAX 受信ジョブ（FAX 機能）
  - ✓ 保存ジョブ（ボックス機能）
  - ✓ ネットワークジョブ（ネットワーク保護機能）

- HDD 暗号化機能

  TOE 内の HDD に保存されたデータを漏洩から保護するために､HDD に保存される保護資産を暗号化する機能。

- 上書き消去機能

  TOE の基本機能を使用する際に HDD 上､Flash メモリー上に作成された画像データに対し､データの再利用を不可能な状態にするために、論理的に画像データの管理情報だけを削除するのではなく、実データ領域も全て上書き消去する機能。

- 監査ログ機能
  TOE の利用とセキュリティ関連事象の監査証跡を提供できるように、利用者の操作とセキュリティ関連事象に対する監査ログを記録し、HDD 内に保持する機能。
  保持した監査ログには、機器管理者のみがアクセスすることが出来る。また、保持した監査ログは、機器管理者が設定した宛先に E-mail として送信される。

- セキュリティ管理機能
  TOE のセキュリティ機能に関する諸設定を行う機能。
  セキュリティ管理機能は、許可された利用者のみが利用することが出来る。
  操作パネル及び、クライアント PC から利用することが出来る。クライアント PC からの操作には、Web ブラウザーを使用する。

- 自己テスト機能
  TOE のセキュリティ機能の実行コードの不正改ざんを検出するために、TSF 実行コードおよび TSF データの完全性を検証する機能。

- ネットワーク保護機能
  TOE が接続される内部ネットワーク上を流れるデータが盗聴などにより、漏洩、改ざんされないように、通信経路上を保護する機能。
  スキャン送信機能、プリンター機能、ボックス機能、ボックス機能におけるクライアント PC（Web ブラウザー）からの操作、セキュリティ管理機能におけるクライアント PC（Web ブラウザー）からの操作を利用する際に、接続先の正当性を検証し、ネットワーク上を流れる対象資産を暗号化することで保護する。ただし、プリンター機能におけるローカル接続での利用は対象外である。
  また、外部インターフェイスからの情報を、TOE を介して内部ネットワークに無断転送することを防止する機能も提供する。

1.4.4. ガイダンス

本TOEを構成するガイダンスを以下に示す。

表 1.4 TOE を構成するガイダンス

名称	バージョン	仕向地
TASKalfa 3212i / TASKalfa 4012i クイックガイド	初版 2017.11 302V65603001	日本
TASKalfa 3212i / TASKalfa 4012i セーフティーガイド / Safety Guide	2017.11 302V65622001	日本/海外
TASKalfa 3212i / TASKalfa 4012i 使用説明書	初版 2017.11 2V6KDJA000	日本

FAX System 12 使用説明書	Rev.5 2017.11 3RKKDJA005	日本
TASKalfa 4012i / TASKalfa 3212i Data Security Kit (E) 使用説明書	2018.7 3MS2V6KDJA0	日本
Command Center RX 操作手順書	Rev.15 2017.10 CCRXKDJA15	日本
TASKalfa 3212i / TASKalfa 4012i プリンタードライバー 操作手順書	2V6BWKTJA710.2017.08	日本
KYOCERA Net Direct Print 操作手順書	DirectPrintKDJA1.2016.02	日本
お知らせ / Notice	2018.9 303MS5639001	日本/海外
Data Security Kit (E) 設置手順書 / Installation Guide	2013.1 303MS56710-02	日本/海外
FAX System 12 設置手順書 / Installation Guide	2016.6 303RK56710-03	日本/海外
HD-12 設置手順書 / Installation Guide *1	2016.4 303S15631001	日本/海外
TASKalfa 3212i / TASKalfa 4012i FIRST STEPS QUICK GUIDE	2017.11 302V65602001	海外
TASKalfa 3212i / TASKalfa 4012i OPERATION GUIDE	First edition 2017.11 2V6KDEN000	海外
FAX System 12 FAX OPERATION GUIDE	Rev.5 2017.11 3RKKDEN105	海外
TASKalfa 4012i / TASKalfa 3212i Data Security Kit (E) OPERATION GUIDE	2018.7 3MS2V6KDEN0	海外
Command Center RX User Guide	Rev.14 2017.10 CCRXKDEN14	海外
TASKalfa 3212i / TASKalfa 4012i Printer Driver User Guide	2V6BWKTEN710.2017.09	海外
KYOCERA Net Direct Print User Guide	DirectPrintKDEN1.2016.02	海外

*1 HD-12 設置手順書 / Installation Guide は、HDDオプション搭載済みで販売される製品では同梱されない。

1.4.5. TOE の保護資産

TOE の保護資産は、User Data、TSF Data、Functions である。

1.4.5.1. User Data

User Data は、利用者によって作成され、TOE のセキュリティ機能（TSF）には影響を及ぼさないデータである。User Data には以下の２種類が存在する。

表 1.5 User Data

Designation	Definition
D.DOC	User Document Data consist of the information contained in a user’s document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user’s document or job to be processed by the TOE.

本TOEが対象とするUser Dataを表 1.6に示す。

表 1.6 本 TOE が対象とする User Data

Designation	User Data	Explanation
D.DOC	画像データ	表 2.2 で示された、+PRT、+SCN、+CPY、+FAXIN、+FAXOUT、+DSR、+SMI の属性を持つ画像データ
	残存データ	上記画像データの処理後、不要になった画像データは削除されるが、管理情報だけが削除されるため、残存してしまう実データ
D.FUNC	ジョブデータ	基本機能を実行した際に生成されるジョブデータ

1.4.5.2. TSF Data

TSF Data は、TOE によって作成され、TOE に影響を与えるかもしれないデータである。TSF Data には以下の２種類が存在する。

表 1.7 TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

本TOEが対象とするTSF Dataを表 1.8に示す。

表 1.8 本 TOE が対象とする TSF Data

Designation	TSF Data	Explanation
D.PROT	ログインユーザー名	ユーザー管理機能で使用する利用者の識別情報
	ユーザー権限	ユーザー管理機能で使用する利用者の権限情報のこと。本 TOE では、U. ADMINISTRATOR と U.NORMAL の権限が存在する。
	ジョブ認可設定	TOE が持つ実行属性毎に、実行を許可されているかどうかを示す設定のこと。ユーザー管理機能で使用する利用者毎にジョブ認可設定が割り振られる。
	実行属性	TOE が持つコピー機能、プリンター機能、スキャン送信機能、FAX 機能、ボックス機能を実行可能であることを示す属性。
	所有者情報	対象の資産が持つ所有者の情報。所有者情報にはログインユーザー名が割り当てられる。
	ロックまでの回数（ユーザーアカウントロックアウトポリシー設定）	ユーザー管理機能で使用する、ユーザーアカウントロックアウトへの移行回数情報
	ロックアウト期間（ユーザーアカウントロックアウトポリシー設定）	ユーザー管理機能で使用する、ユーザーアカウントロックアウト中の受付拒否時間情報
	ロックアウトリスト	ユーザー管理機能で使用する、ユーザーアカウントロックアウト中のユーザーリスト 機器管理者は、このリストの中からユーザーアカウント毎にロックアウトの解除を指示することができる
	自動ログアウト時間設定	ログインのセッションを自動で終了する時間情報
	パスワードポリシー設定	パスワードのポリシー情報で、パスワードの長さ、パスワードの複雑さ、及びパスワードの有効期間を設定するための情報
	ボックスの所有者	該当ボックスの所有者を示すための設定。所有者の情報にはログインユーザー名が割り当てられる。

	ボックスの共有設定	ボックス内の文書を、利用者全員で共有するための設定。共有設定が有効になっているボックスには、利用者全員がアクセス可能となる。
	日時設定	日付と時刻の設定情報
	ネットワーク暗号設定	ネットワーク保護機能に使用する TLS、IPsec 暗号化通信のための設定情報
	FAX 転送設定	FAX 受信したデータを、転送するための設定。
	監査ログレポート送信先情報	監査ログレポートを外部に送信する際の送信先情報
D.CONF	ログインユーザーパスワード	ユーザー管理機能で使用する利用者の認証情報
	監査ログ	監査ログ機能で生成されるログデータ
	暗号鍵	HDD 暗号化機能で使用する暗号鍵

1.4.5.3. Functions

Functions は、表 2.1 SFR Package functions で示される機能である。

2. 適合主張

2.1. CC 適合主張

本ST およびTOE のCC 適合主張は、以下のとおりである。

ST とTOE が適合を主張するCC のバージョン：

Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 3.1 Revision 5
Part2: Security functional components Version 3.1 Revision 5
Part3: Security assurance components Version 3.1 Revision 5

Common Criteria conformance: CC Part2 extended and CC Part3 conformant

2.2. PP 主張

本ST およびTOE が適合するPPは、以下の通りである。

PP名称　　: U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009)
バージョン : 1.0

注釈: 本 PP は Common Criteria Portal に掲載されている「IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B」に適合し、かつ「CCEVS Policy Letter #20」も満たしている。

2.3. パッケージ主張

本ST およびTOE は、パッケージ：EAL2 追加を主張する。追加のコンポーネントはALC_FLR.2である。

本ST は、次のSFR Packages に適合する。

2600.2-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment B 適合
2600.2-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment B 適合
2600.2-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment B 適合
2600.2-FAX SFR Package for Hardcopy Device Fax Functions, Operational Environment B 適合
2600.2-DSR SFR Package for Hardcopy Device Document Storage and Retrieval(DSR) Functions, Operational Environment B 適合
2600.2-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational

Environment B 適合

2.4. SFR Packages

2.4.1. SFR Packages functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 表 2.1.

表 2.1 SFR Package functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.4.2. SFR Packages attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional

Requirements that depend on the function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 表 2.2 SFR Package attributes

表 2.2 SFR Package attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.5. 適合根拠

本ST がPPに適合していることの根拠を以下に示す。

本 TOE の種別は、主としてコピー機能、スキャン送信機能、プリンター機能、FAX 機能、ボックス機能を有する複合機であり、PP である 2600.2, Protection Profile for Hardcopy Devices, Operational Environment A に記載の Hardcopy Devices という TOE 種別と一貫していると言える。また、内部ネットワークに接続するためのネットワーク機能も有しているが、記憶媒体として有している NAND、揮発性メモリー、Flash メモリー、HDD 、SSD、また、ファームウェアを格納するための PROM は、いずれも取り外し可能な記憶媒体ではないため、PP で定義された 7 個の SFR Package のうち、2600.2-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B を除く 6 個の SFR Package に適合していることは適切であると言える。

次に、セキュリティ課題定義、セキュリティ対策方針、セキュリティ要件において、PP に適合していることを示していく。

セキュリティ課題定義では、PP の内容を全て網羅した上で、P.HDD.ENCRYPTION を追加している。P.HDD.ENCRYPTION は、運用環境に新たな制約をかける OSP ではない。よって、PP のセキュリティ課題定義を満たす運用環境は、本 ST のセキュリティ課題定義も満たす。このため、本 ST は、PP の全

てのセキュリティ課題定義よりも制限的であると言える。

セキュリティ対策方針では、OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED を除き

PP の内容を全て含んだ上で、O.HDD.ENCRYPTION を追加している。O.HDD.ENCRYPTION は、運用環境に新たな制約をかける Objective ではない。よって、PP のセキュリティ対策方針を満たす運用環境は、本 ST のセキュリティ対策方針も満たす。このため、本 ST は、PP の全てのセキュリティ対策方針よりも制限的であると言える。
なお、PP で規定しているセキュリティ対策方針のうち、P.AUDIT.LOGGING に対する対策方針 OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED をそれぞれ O.AUDIT_STORAGE.PROTECTED と O.AUDIT_ACCESS.AUTHORIZED に置き換えている。O.AUDIT_STORAGE.PROTECTED と O.AUDIT_ACCESS.AUTHORIZED を実施する内部機能は、OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED で要求される運用環境のセキュリティ対策方針と同等のことが出来ると言える。

セキュリティ要件では、本 ST で規定している SFR と PP で規定している SFR の関係を表 2.3 に示す。

表 2.3 本 ST の SFR と PP の SFR の関係

本 ST の SFR	PP の要求	
FAU_GEN.1	✓	
FAU_GEN.2	✓	
FAU_SAR.1		
FAU_SAR.2		
FAU_STG.1		
FAU_STG.4		
FCS_CKM.1		
FCS_COP.1		
FDP_ACC.1(a)	✓	
FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	✓	
FDP_ACF.1(b)	✓	
FDP_RIP.1	✓	
FIA_AFL.1		
FIA_ATD.1	✓	
FIA_SOS.1		
FIA_UAU.1	✓	
FIA_UAU.7		

本 ST の SFR	PP の要求	
FIA_UID.1	✓	
FIA_USB.1	✓	
FMT_MSA.1(a)	✓	
FMT_MSA.3(a)	✓	
FMT_MSA.1(b)	✓	
FMT_MSA.3(b)	✓	
FMT_MTD.1(a)	✓	
FMT_MTD.1(b)	✓	
FMT_SMF.1	✓	
FMT_SMR.1	✓	
FPT_STM.1	✓	
FPT_TST.1	✓	
FPT_FDI_EXP.1	✓	
FTA_SSL.3	✓	
FTP_ITC.1	✓	

本 ST では、PP で要求されている全ての SFR を適用した上で、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4、FCS_CKM.1、FCS_COP.1、FIA_AFL.1、FIA_SOS.1、FIA_UAU.7 を追加している。また、FTA_SSL.3 の割付操作において、操作パネルと Web ブラウザーの無操作時間間隔を指定しているが、本 TOE には操作パネルと Web ブラウザー以外のインターフェイスには対話セッションは存在しない。FDP_ACF.1.3(b)において、U.ADMINISTRATOR への明示的に許可する規則の割付操作を削除しているが、追加の許可の規則を持たないことは修正前の PP の要件に比べてより厳格である。このため、本 ST を満たす全ての TOE は、PP のセキュリティ要件も満たしつつ、より制限的であると言える。

最後に、PP で規定している SAR と、本 ST で規定している SAR は全く同等である。

従って、本 ST は、PP に対して、同等またはより制限的な方法で PP における一般的なセキュリティ課題定義に対する解決策を提供しているため、PP に対して論証適合していると言える。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. Threats agents

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE
b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized.
d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Protection Profile address the threats posed by these threat agents.

3.2. Threats to TOE Assets

This section describes threats to assets described in clause 1.4.5.

表 3.1 Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

表 3.2 Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.3. Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

表 3.3 Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.ENCRYPTION	To improve the confidentiality of the documents, User Data and TSF Data stored in HDD will be encrypted by the TOE.

3.4. Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Protection Profile are based on the condition that all of the assumptions described in this section are satisfied.

表 3.4 Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer’s guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1. Security Objectives for the TOE

This section describes the security objectives that the TOE shall fulfill.

表 4.1 Security objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.

Objective	Definition
O.HDD.ENCRYPTION	The TOE shall encrypt User Data and TSF Data, when the TOE stores them in HDD.

4.2. Security Objectives for the operational environment

This section describes the security objectives that must be fulfilled by operational environment of the TOE.

表 4.2 Security objectives for the operational environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization, have the training, competence, and time to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3. Security Objectives rationale

This section demonstrates that each threat, organizational security policy, and assumption, are mitigated by at least one Security Objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

表 4.3 Completeness of security objectives

Threats, Policies, and Assumptions	Objectives																			
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	O.HDD.ENCRYPTION
T.DOC.DIS	✓						✓	✓												
T.DOC.ALT		✓					✓	✓												
T.FUNC.ALT			✓				✓	✓												
T.PROT.ALT				✓			✓	✓												
T.CONF.DIS					✓		✓	✓												
T.CONF.ALT						✓	✓	✓												
P.USER.AUTHORIZATION							✓	✓												
P.SOFTWARE.VERIFICATION									✓											
P.AUDIT.LOGGING										✓	✓	✓	✓							
P.INTERFACE.MANAGEMENT														✓		✓				
A.ACCESS.MANAGED															✓					
A.ADMIN.TRAINING																	✓			
A.ADMIN.TRUST																		✓		
A.USER.TRAINING																			✓	
P.HDD.ENCRYPTION																				✓

表 4.4 Sufficiency of security objectives

Threats. Policies, and Assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.DOC.ALT	User Document Data may be altered by unauthorized persons	O.DOC.NO_ALT protects D.DOC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.FUNC.ALT	User Function Data may be altered by unauthorized persons	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons	O.PROT.NO_ALT protects D.PROT from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.DIS	TSF Confidential Data may be disclosed to	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure

	unauthorized persons	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons	O.CONF.NO_ALT protects D.CONF from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed by the TOE and its IT environment.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		O.AUDIT_STORAGE.PROTECTED protects audit records from unauthorized access, deletion and modifications
		O.AUDIT_ACCESS.AUTHORIZED provides appropriate access to audit records only by authorized persons.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed

P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces
P.HDD.ENCRYPTION	User Data and TSF Data stored in HDD will be encrypted by the TOE.	O.HDD.ENCRYPTION encrypts User Data and TSF Data stored in HDD by TOE
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5. 拡張コンポーネント定義

This ST defines components that are extensions to Common Criteria 3.1 Release 4, Part 2. These extended components are defined in the ST but are used in SFR Packages, and therefore, are employed only in TOEs whose STs conform to those SFR Packages.

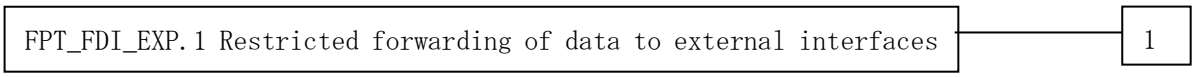
5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:



FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces, provides for the functionality to require TSF controlled processing of data received over defined external interfaces before this data is sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

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

a) definition of the role(s) that are allowed to perform the management activities;
b) management of the conditions under which direct forwarding can be allowed by an administrative role;

c) revocation of such an allowance.

Audit: FPT_FDI_EXP.1

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

There are no auditable events foreseen.

Rationale:

Quite often a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data is allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i. e. without processing the data first) between different external interfaces is therefore a function that - if allowed at all - can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and could therefore be placed in either the FDP or FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this lead the authors to define a new family with just one member.

FPT_FDI_EXP.1　Restricted forwarding of data to external interfaces

Hierarchical to:　No other components.

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

FPT_FDI_EXP.1.1　The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

6. セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

6.1. TOE セキュリティ機能要件

6.1.1. クラス FAU:セキュリティ監査

FAU_GEN.1　　Audit data generation

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

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

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 6.1;** [assignment: *other specifically defined auditable events*].

[selection, choose one of: *minimum, basic, detailed, not specified*]

- not specified

[assignment: *other specifically defined auditable events*]

- なし

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 6.1: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- なし

表 6.1 Audit data requirements

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
FAU_GEN.1	-	-	There are no auditable events foreseen.
FAU_GEN.2	-	-	There are no auditable events foreseen.
FAU_SAR.1	[Not specified] -	-	a) Basic: Reading of information from the audit records.
FAU_SAR.2	[Not specified] -	-	a) Basic: Unsuccessful attempts to read information from the audit records.
FAU_STG.1	-	-	There are no auditable events foreseen.
FAU_STG.4	[Not specified] -	-	a) Basic: Actions taken due to the audit storage failure.
FCS_CKM.1	[Not specified] -	-	a) Minimum: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_COP.1	[Not specified] -	-	a) Minimum: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACC.1(a)	-	-	There are no auditable events foreseen.
FDP_ACF.1(a)	[Not specified] 以下に示すオブジェクトに対する操	Type of job	a) Minimum: Successful requests to perform an operation on

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
	作の実行における成功した要求 ・D.DOC の参照 ・D.DOC の削除 ・D.FUNC の参照 ・D.FUNC の改変 ・D.FUNC の削除		an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.
FDP_ACC.1(b)	-	-	There are no auditable events foreseen.
FDP_ACF.1(b)	[Not specified] -	-	a) Minimum: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.
FDP_RIP.1	-	-	There are no auditable events foreseen.
FIA_AFL.1	[Minimum] 最後の成功した認証以降の連続した不成功認証試行が閾値に到達した時にとられる以下のアクション ・ ユーザーアカウントロックアウトの実行 及び、正常状態に復元する以下のアクション ・ 機器管理者によるロックアウト状態の解除	-	a) Minimum: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	-	-	There are no auditable events foreseen.
FIA_SOS.1	[Minimum]		a) Minimum: Rejection by the TSF

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
	以下に示すテストされた秘密の拒否 ・ 利用者情報の新規作成時に入力されたログインユーザーパスワードの品質検査による拒否 ・ 利用者情報の編集時に変更されたログインユーザーパスワードの品質検査による拒否		of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.
FIA_UAU.1	[Basic] Both successful and unsuccessful use of the authentication mechanism	None required	Defined by PP: Both successful and unsuccessful use of the authentication mechanism
FIA_UAU.7	-	-	There are no auditable events foreseen.
FIA_UID.1	[Basic] Both successful and unsuccessful use of the identification mechanism	Attempted user identity	Defined by PP: Both successful and unsuccessful use of the identification mechanism
FIA_USB.1	[Not specified] -	-	a) Minimum: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).
FMT_MSA.1(a)	[Not specified] -	-	a) Basic: All modifications of the values of security attributes.
FMT_MSA.3(a)	[Not specified] -	-	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
			security attributes.
FMT_MSA.1(b)	[Not specified] -	-	a) Basic: All modifications of the values of security attributes.
FMT_MSA.3(b)	[Not specified] -	-	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MTD.1(a)	[Not specified] -	-	a) Basic: All modifications to the values of TSF data.
FMT_MTD.1(b)	[Not specified] -	-	a) Basic: All modifications to the values of TSF data.
FMT_SMF.1	[Minimum] Use of the management functions	None required	Defined by PP: Use of the management functions
FMT_SMR.1	[Minimum] Modifications to the group of users that are part of a role	None required	Defined by PP: Modifications to the group of users that are part of a role
FPT_STM.1	[Minimum] Changes to the time	None required	Defined by PP: Changes to the time
FPT_TST.1	[Not specified] -	-	a) Basic: Execution of the TSF self tests and the results of the tests.
FPT_FDI_EXP.1	-	-	There are no auditable events foreseen.
FTA_SSL.3	[Minimum] Termination of an interactive session by the session locking mechanism	None required	a) Minimal: Termination of an interactive session by the session locking mechanism.
FTP_ITC.1	[Minimum] Failure of the trusted channel functions	失敗した高信頼チャネル機能の通信先 IP アドレス (通信元の IP アドレスは TOE 自身のアドレス	Defined by PP: Failure of the trusted channel functions b) Identification of the initiator and target of

Relevant SFR	Auditable event	Additional information	Actions to be audited (defined by CC or PP)
		固定であるため取得不要)	failed trusted channel functions.

FAU_GEN.2 User identify association

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

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

FAU_SAR.1 Audit review

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

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

[assignment: *authorised users*]
- U.ADMINISTRATOR

[assignment: *list of audit information*]
- 表 6.1 に示す Audit data requirements の「Auditable event」欄、及び「Additional information」欄に示す情報

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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

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

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.1.2 The TSF shall be able to [selection, *choose one of: prevent, detect*] unauthorized modifications to the stored audit records in the audit trail.

[selection: *choose one of: prevent, detect*]

- Prevent

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

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

[selection: *choose one of: "ignore audited events", "prevent audited events,*

except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”]

- “overwrite the oldest stored audit records”

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

- なし

6.1.2. クラス FCS:暗号サポート

FCS_CKM.1	Cryptographic key generation
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

- FIPS PUB 180-4 に基づく暗号鍵生成アルゴリズム

[assignment: cryptographic key sizes]

- 256bit

[assignment: list of standards]

- FIPS PUB 180-4

FCS_COP.1	Cryptographic operation
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.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of cryptographic operations]
- HDD へ書き込み時の D.DOC、D.FUNC、D.PROT、D.CONF の暗号化
- HDD から読み出し時の D.DOC、D.FUNC、D.PROT、D.CONF の復号

[assignment: cryptographic algorithm]
- AES

[assignment: cryptographic key sizes]
- 256bit

[assignment: list of standards]
- FIPS PUB 197

6.1.3. クラス FDP:利用者データ保護

FDP_ACC.1(a)	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the **User Data Access Control SFP in Table 6.2** on **the list of users as subjects, objects, and operations among subjects and objects covered by the User Data Access Control SFP in Table 6.2.**

FDP_ACF.1(a)	**Security attribute based access control**
Hierarchical to:	No other components.

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

FDP_ACF.1.1(a) The TSF shall enforce the **User Data Access Control SFP in Table 6.2** to objects based on the following: **the list of users as subjects and objects controlled under the User Data Access Control SFP in Table 6.2, and for each, the indicated security attribute in Table 6.2.**

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the User Data Access Control SFP in Table 6.2 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects.**

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- 表 6.3 で示された Explicitly authorize access control rule

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- なし

表 6.2 User Data Access Control SFP

Object (Security attribute)	Attribute	Operation(s)	Subject (Security attribute)	Access control rule
D.DOC (所有者情報)	+PRT,+SCN,+CPY,+FAXOUT	Read, Delete	U.NORMAL (ログインユーザー名)	Denied, except for his/her own documents U.NORMAL の「ログインユーザー名」と、D.DOC の「所有者情報」が一致する場合に、Operation を許可する。
D.DOC (ボックスの所有者、ボックスの共有設定)	+DSR	Read, Delete	U.NORMAL (ログインユーザー名)	Denied, except (1) for his/her own documents, or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE (1) U.NORMAL の「ログインユーザー名」と、D.DOC が格納された「ボックスの所有者」が一致する場合に、Operation を許可する。 (2) D.DOC が格納された「ボックスの共有設定」が有効である場合に、U.NORMAL に Operation を許可する。
D.DOC (所有者情報)	+FAXIN	[assignment: other operations] Any Operations	U.NORMAL (ログインユーザー名)	Denied U.NORMAL からの全ての Operation を禁止する。
D.FUNC (所有者情報)	N/A	Read, Modify, Delete	U.NORMAL (ログインユーザー名)	Denied, except for his/her own function data. U.NORMAL の「ログインユーザー名」と、D.FUNC の「所有者情報」が一致する場合に、Operation を許可する。

表 6.3 User Data Access Control SFP for U.ADMINISTRATOR

Object (Security attribute)	Attribute	Operation(s)	Subject (Security attribute)	Explicitly authorize access control rule
D.DOC (所有者情報)	+PRT	Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する
D.DOC (所有者情報)	+SCN	Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する
D.DOC (所有者情報)	+CPY	Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する
D.DOC (所有者情報)	+FAXOUT	Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する
D.DOC (ボックスの所有者)	+DSR	Read, Delete	U.ADMINISTRATOR (ユーザー権限)	「ボックスの所有者」の値に関わらず、Operation を許可する
D.DOC (所有者情報)	+FAXIN	Read, Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する
D.FUNC (所有者情報)	N/A	Read, Modify, Delete	U.ADMINISTRATOR (ユーザー権限)	「所有者情報」の値に関わらず、Operation を許可する

FDP_ACC.1(b)　Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP in Table 6.4** on **users as subjects, TOE functions as objects, and the right to use the functions as operations.**

FDP_ACF.1(b)　Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** to objects based on the following: **users and [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]**.

[assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]

- 表 6.4 の「Object」欄に示された機能と「security attribute」欄に示されたセキュリティ属性

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]**.

[selection: *the user is explicitly authorized by U.ADMINISTATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]

- [assignment: other conditions]

[assignment: *other conditions*]

- 表 6.4 で示された規則

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- なし

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

- なし

表 6.4 TOE Function Access Control SFP

Object (Security attribute)	Operation	Subject (Security attribute)	Access control rule
F.CPY (実行属性)	ジョブの実行	U.ADMINISTRATOR U.NORMAL (ジョブ認可設定)	Subject が有するジョブ認可設定の中に Object の実行属性が含まれる場合に Operation を許可する
F.PRT (実行属性)	ジョブの実行	U.ADMINISTRATOR U.NORMAL (ジョブ認可設定)	Subject が有するジョブ認可設定の中に Object の実行属性が含まれる場合に Operation を許可する
F.SCN (実行属性)	ジョブの実行	U.ADMINISTRATOR U.NORMAL (ジョブ認可設定)	Subject が有するジョブ認可設定の中に Object の実行属性が含まれる場合に Operation を許可する
F.FAX (実行属性)	ジョブの実行	U.ADMINISTRATOR U.NORMAL (ジョブ認可設定)	Subject が有するジョブ認可設定の中に Object の実行属性が含まれる場合に Operation を許可する
F.DSR (実行属性)	ジョブの実行	U.ADMINISTRATOR U.NORMAL (ジョブ認可設定)	Subject が有するジョブ認可設定の中に Object の実行属性が含まれる場合に Operation を許可する

FDP_RIP.1　　Subset residual information protection

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

FDP_RIP.1.1　The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC,** [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]
- deallocation of the resource from

[assignment: *list of objects*]
- なし

6.1.4. クラス FIA:識別と認証

FIA_AFL.1　　Authentication failure handling

Hierarchical to:　　No other components.
Dependencies:　　FIA_UAU.1 Timing of authentication

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

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

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

[assignment: range of acceptable values]

- *1 to 10*

[assignment: *list of authentication events*]

- 操作パネルからのログインで指定されたログインユーザー名に対して、最後の成功した認証以降の連続した不成功認証試行
- クライアント PC からのログインで指定されたログインユーザー名に対して、最後の成功した認証以降の連続した不成功認証試行

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

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

- 1～60 分の間で機器管理者が指定した時間が経過するまで、もしくは機器管理者がロック状態を解除するまで、該当アカウントからのログインの受付をロックする。

FIA_ATD.1　　User attribute definition

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

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

[assignment: *list of security attributes*]
- ログインユーザー名、ユーザー権限、ジョブ認可設定

FIA_SOS.1　　Verification of secrets

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

FIA_SOS.1.1　The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]
- パスワード長　　：8文字以上
- 文字種別　　：英数字記号

FIA_UAU.1　　Timing of authentication

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

FIA_UAU.1.1　The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]
- 機器状態の取得

- ジョブ情報一覧の表示
- カウンター情報の表示
- FAXデータの受信

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

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

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

[assignment: *list of feedback*]

- ダミー文字（*：asterisk）

FIA_UID.1 Timing of identification

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

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

- 機器状態の取得
- ジョブ情報一覧の表示
- カウンター情報の表示
- FAXデータの受信

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

FIA_USB.1	User-subject binding

Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

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

[assignment: *list of user security attributes*]

- ログインユーザー名、ユーザー権限、ジョブ認可設定

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

[assignment: *rules for the initial association of attributes*]

- 無し

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

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

- 無し

6.1.5. クラス FMT:セキュリティ管理

FMT_MSA.1(a)	Management of security attributes

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(a) The TSF shall enforce the **User Data Access Control SFP in Table 6.2**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

- なし

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

- 表 6.5 で示された Operation(s)

[assignment: *list of security attributes*]

- 表 6.5 で示された Security Attributes

[assignment: *the authorised identified roles*]

- 表 6.5 で示された Role

表 6.5 Management of security attributes

Security Attributes	Operation(s)	Role
ボックスの所有者	modify	U.ADMINISTRATOR
ボックスの共有設定	modify	U.ADMINISTRATOR
		ボックスの所有者と一致する U.NORMAL
所有者情報	modify	U.ADMINISTRATOR

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(a) The TSF shall enforce the **User Data Access Control SFP in Table 6.2,** [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one

of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]
- なし

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

FMT_MSA.3.2(a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]
- Nobody

FMT_MSA.1(b) Management of security attributes

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(b) The TSF shall enforce the **TOE Function Access Control SFP,** [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]
- なし

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

[assignment: *other operations*]

- Any Operations

[assignment: *list of security attributes*]
- 実行属性

[assignment: *the authorised identified roles*]
- Nobody

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1(b) The TSF shall enforce the **TOE Function Access Control Policy**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]
- なし

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

FMT_MSA.3.2(b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]
- Nobody

FMT_MTD.1(a) Management of TSF data

Hierarchical to:	No other components.

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

FMT_MTD.1.1(a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*,** [assignment: *the authorized identified roles* ***except U.NORMAL***]]].

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

- 表 6.6 で示された Operation

[assignment: *list of TSF data*]

- 表 6.6 で示された TSF data

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*, [assignment: *the authorized identified roles* ***except U.NORMAL***]]]

- 表 6.6 で示された Roles

表 6.6 Operation of TSF data

TSF data	Roles	Operation
ログインユーザー名	U.ADMINISTRATOR	modify, delete, create
ログインユーザーパスワード	U.ADMINISTRATOR	modify, delete, create
ユーザー権限	U.ADMINISTRATOR	modify, delete, create
ジョブ認可設定	U.ADMINISTRATOR	modify, delete, create
ロックまでの回数（ユーザーアカウントロックアウトポリシー設定）	U.ADMINISTRATOR	modify
ロックアウト期間（ユーザーアカウントロックアウトポリシー設定）	U.ADMINISTRATOR	modify
ロックアウトリスト	U.ADMINISTRATOR	modify
自動ログアウト時間設定	U.ADMINISTRATOR	modify
パスワードポリシー設定	U.ADMINISTRATOR	modify
日時設定	U.ADMINISTRATOR	modify
ネットワーク暗号設定	U.ADMINISTRATOR	modify
FAX 転送設定	U.ADMINISTRATOR	modify
監査ログレポート送信先情報	U.ADMINISTRATOR	modify
暗号鍵	Nobody	*[assignment: other operations]* ・Any Operations

FMT_MTD.1(b)　Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles.
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1(b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data **associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***] to [selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated*]].

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

- 表 6.7 で示された Operation

[assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***]

- 表 6.7 で示された TSF data

[selection, choose one of: *Nobody*, [selection: ***U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated***]]

- 表 6.7 で示された Roles

表 6.7 Operation of TSF data

TSF data	Roles	Operation
U.NORMAL に関連付いたログインユーザーパスワード	U.NORMAL	modify

FMT_SMF.1　　Specification of Management Functions

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

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

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

- ボックス機能におけるセキュリティ属性(ボックスの所有者､ボックスの共有設定、所有者情報）を管理する機能
- TSF データ（ログインユーザー名、ログインユーザーパスワード、ユーザー権限、ジョブ認可設定、ロックまでの回数、ロックアウト期間、ロックアウトリスト、自動ログアウト時間設定、パスワードポリシー設定、日時設定、ネットワーク暗号設定、FAX 転送設定、監査ログレポート送信先情報）を管理する機能

表 6.8 Management functions

Relevant SFR	Management Functions	Management item (defined by CC or PP)
FAU_GEN.1	-	There are no management activities foreseen.
FAU_GEN.2	-	There are no management activities foreseen.
FAU_SAR.1	U.ADMINISTRATOR 権限の管理	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	-	There are no management activities foreseen.
FAU_STG.1	-	There are no management activities foreseen.
FAU_STG.4	なし （アクションは固定であり、管理する必要はない）	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FCS_CKM.1	-	There are no management activities foreseen.
FCS_COP.1	-	There are no management activities foreseen.
FDP_ACC.1(a)	-	There are no management activities foreseen.
FDP_ACF.1(a)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_ACC.1(b)	-	There are no management activities foreseen.
FDP_ACF.1(b)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_RIP.1	なし （割当て解除時にのみ残存情報保護を実施するため、残存情報保護のタイミングを管理する必要はない）	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.
FIA_AFL.1	認証失敗回数の管理	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	なし （追加のセキュリティ属性は存在しないため、管理する必要はない）	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.

Relevant SFR	Management Functions	Management item (defined by CC or PP)
FIA_SOS.1	ログインユーザーパスワードのパスワードポリシーの管理	a) the management of the metric used to verify the secrets.
FIA_UAU.1	U.ADMINISTRATOR によるログインユーザーパスワードの管理 U.NORMAL による自身のログインユーザーパスワードの管理	a) management of the authentication data by an administrator; b) management of the authentication data by the associated user; c) managing the list of actions that can be taken before the user is authenticated.
FIA_UAU.7	-	There are no management activities foreseen.
FIA_UID.1	Management of the user identities	Defined by PP: Management of the user identities
FIA_USB.1	なし （サブジェクトのセキュリティ属性は固定のため、管理する必要はない）	a) an authorised administrator can define default subject security attributes. b) an authorised administrator can change subject security attributes.
FMT_MSA.1(a)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3(a)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MSA.1(b)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3(b)	なし （役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない）	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.

Relevant SFR	Management Functions	Management item (defined by CC or PP)
FMT_MTD.1(a)	なし（役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない)	a) managing the group of roles that can interact with the TSF data.
FMT_MTD.1(b)	なし（役割のグループは U.ADMINISTRATOR 固定であるため、管理する必要はない)	a) managing the group of roles that can interact with the TSF data.
FMT_SMF.1	-	There are no management activities foreseen.
FMT_SMR.1	利用者のユーザー権限のグループの管理	a) managing the group of users that are part of a role.
FPT_STM.1	Management of system time	Defined by PP: Management of system time
FPT_TST.1	なし（自己テストの実行条件は固定であるため、管理する必要はない)	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate.
FPT_FDI_EXP.1	FAX の転送条件の管理	a) definition of the role(s) that are allowed to perform the management activities; b) management of the conditions under which direct forwarding can be allowed by an administrative role; c) revocation of such an allowance.
FTA_SSL.3	自動ログアウト時間の管理	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) specification of the default time of user inactivity after which termination of the interactive session occurs.
FTP_ITC.1	ネットワーク暗号設定の管理	a) Configuring the actions that require trusted channel, if supported.

	FMT_SMR.1	Security roles
	Hierarchical to:	No other components.
	Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].	
	[selection: *Nobody*, [assignment: *the authorised identified roles*]]	
	● Nobody	
FMT_SMR.1.2	The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated.**	

6.1.6. クラス FPT:TSF の保護

	FPT_STM.1	Reliable time stamps
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.	

	FPT_TST.1	TSF testing
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].	

[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

- during initial start-up

[selection: [assignment: *parts of TSF*], *the TSF*]

- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]

- HDD 暗号化機能

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*].

[selection: [assignment: *parts of TSF data*], *TSF data*]

- [assignment: *parts of TSF data*]

[assignment: *parts of TSF data*]

- 暗号鍵

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*].

[selection: [assignment: *parts of TSF*], *TSF*]

- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]

- TSF 実行モジュール

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles.

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any**

Shared-medium Interface.

6.1.7. クラス FTA:TOE アクセス

FTA_SSL.3	**TSF-initiated termination**

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

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

[assignment: *time interval of user inactivity*]

- 操作パネル : 無操作状態が、機器管理者による設定時間経過後(5 秒～495 秒)
- Web ブラウザー : 無操作状態が、10 分間経過後

※ 操作パネルと Web ブラウザー以外に対話セッションは存在しない

6.1.8. クラス FTP:高信頼パス/チャネル

FTP_ITC.1	**Inter-TSF trusted channel**

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

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface.**

6.2. TOE セキュリティ保証要件

表 6.9 2600.2 Security Assurance Requirements にセキュリティ保証要件を示す
本 TOE の評価保証レベルは EAL3 であり、セキュリティ保証コンポーネント ALC_FLR.2 を追加している。

表 6.9 2600.2 Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ対策方針に対する TOE セキュリティ機能要件の対応を示す。
太字で記載した項目は対策方針の主要(P)な実現を提供し、標準書体で記載した項目はその実現を支援(S)する。

表 6.10 Completeness of security requirements

SFRs	Objectives												
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.HDD.ENCRYPTION
FAU_GEN.1										P			
FAU_GEN.2										P			
FAU_SAR.1					P							P	
FAU_SAR.2					P							P	
FAU_STG.1						P					P		
FAU_STG.4						P					P		
FCS_CKM.1													P
FCS_COP.1													P
FDP_ACC.1(a)	P	P	P										
FDP_ACF.1(a)	S	S	S										
FDP_ACC.1(b)							P						
FDP_ACF.1(b)							S						
FDP_RIP.1	P												
FIA_AFL.1							S	S					
FIA_ATD.1							S						
FIA_SOS.1							S	S					
FIA_UAU.1							P	P					
FIA_UAU.7							S	S					
FIA_UID.1	S	S	S	S	S	S	P	P		S			
FIA_USB.1							P						
FMT_MSA.1(a)	S	S	S	P									
FMT_MSA.3(a)	S	S	S										
FMT_MSA.1(b)				P			S						
FMT_MSA.3(b)							S						
FMT_MTD.1(a)				P	P	P							
FMT_MTD.1(b)					P	P							

SFRs	Objectives												
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.HDD.ENCRYPTION
FMT_SMF.1	S	S	S	S	S	S							
FMT_SMR.1	S	S	S	S	S	S	S						
FPT_STM.1										S			
FPT_TST.1									P				
FPT_FDI_EXP.1								P					
FTA_SSL.3							P	P					
FTP_ITC.1	P	P	P	P	P	P							

以下に、『表 6.10 Completeness of security requirements』の根拠を示す。

O.DOC.NO_DIS

O.DOC.NO_DIS は、不正な開示から D.DOC を保護する対策方針である。

FIA_UID.1 により、利用者が識別され、FDP_ACC.1(a)、FDP_ACF.1(a)により、許可された利用者のみに D.DOC への操作を許可する。

FDP_RIP.1により､残存データとしてのD.DOCにおいて､以前のどの情報の内容も利用できなくする。

FMT_MSA.1(a)により、セキュリティ属性への操作を管理する。

FMT_MSA.3(a)により、D.DOC が生成された際に、D.DOC の所有者情報、もしくは D.DOC が格納されるボックスの所有者、ボックスの共有設定が適切なデフォルト値を有していることを保証する。

FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられ維持される。

FMT_SMF.1 により、セキュリティ管理機能を U.ADMINISTRATOR と D.DOC の所有者である U.NORMAL へ提供する。

FTP_ITC.1 により、TOE と他の高信頼 IT 製品間のネットワーク上を流れる D.DOC に対する改変や暴露から保護される。

従って、O.DOC.NO_DIS は、不正な開示から D.DOC を保護することを保証することが出来る。

O.DOC.NO_ALT

O.DOC.NO_ALT は、不正な改変から D.DOC を保護する対策方針である。

FIA_UID.1 により、利用者が識別され、FDP_ACC.1(a)、FDP_ACF.1(a)により、許可された利用者のみ

に D.DOC への操作を許可する。
FMT_MSA.1(a)により、セキュリティ属性への操作を管理する。
FMT_MSA.3(a)により、D.DOC が生成された際に、D.DOC の所有者情報、もしくは D.DOC が格納されるボックスの所有者、ボックスの共有設定が適切なデフォルト値を有していることを保証する。。
FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられ維持される。
FMT_SMF.1 により、セキュリティ管理機能を U.ADMINISTRATOR と D.DOC の所有者である U.NORMAL へ提供する。
FTP_ITC.1 により、TOE と他の高信頼 IT 製品間のネットワーク上を流れる D.DOC に対する改変や暴露から保護される。
従って、O.DOC.NO_ALT は、不正な改変から D.DOC を保護することを保証することが出来る。

O.FUNC.NO_ALT
O.FUNC.NO_ALT は、不正な改変から D.FUNC を保護する対策方針である。
FIA_UID.1 により、利用者が識別され、FDP_ACC.1(a)、FDP_ACF.1(a)により、許可された利用者のみに D.FUNC への操作を許可する。
FMT_MSA.1(a)により、セキュリティ属性への操作を管理する。
FMT_MSA.3(a)により、D.FUNC が生成された際に、D.FUNC の所有者情報が適切なデフォルト値を有していることを保証する。
FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられ維持される。
FMT_SMF.1 により、セキュリティ管理機能を U.ADMINISTRATOR と D.FUNC の所有者である U.NORMAL へ提供する。
FTP_ITC.1 により、TOE と他の高信頼 IT 製品間のネットワーク上を流れる D.FUNC に対する改変や暴露から保護される。
従って、O.FUNC.NO_ALT は、不正な改変から D.FUNC を保護することを保証することが出来る。

O.PROT.NO_ALT
O.PROT.NO_ALT は、不正な改変から D.PROT を保護する対策方針である。
FIA_UID.1 により、利用者が識別され、許可された利用者のみに D.PROT への操作を許可する。
FMT_MTD.1(a)、FMT_MSA.1(a)、FMT_MSA.1(b)により、TSF data への操作は、U.ADMINISTRATOR に制限される。
FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられ維持される。
FMT_SMF.1 により、セキュリティ管理機能を U.ADMINISTRATOR と D.PROT の所有者である U.NORMAL へ提供する。
FTP_ITC.1 により、TOE と他の高信頼 IT 製品間のネットワーク上を流れる D.PROT に対する改変や暴露から保護される。
従って、O.PROT.NO_ALT は、不正な改変から D.PROT を保護することを保証することが出来る。

O.CONF.NO_DIS、O.CONF.NO_ALT
O.CONF.NO.DIS、O.CONF.NO_ALT は、不正な開示、改変から D.CONF を保護する対策方針である。
FAU_SAR.1、FAU_SAR.2 により、TSF Data（監査ログ）の読み出し操作は、U.ADMINISTRATOR に制限

される。
FAU_STG.1 により、TSF Data（監査ログ）は、不正な削除、改変から保護される。
FAU_STG.4 により、TSF Data（監査ログ）は、満杯時の消失のおそれから保護される。
FIA_UID.1 により、利用者が識別され、許可された利用者のみに D.CONF への操作を許可する。
FMT_MTD.1(a)により、TSF data への操作は、U.ADMINISTRATOR と Nobody に制限される。
FMT_MTD.1(b)により、U.NORMAL の TSF data への操作は、D.CONF の所有者である U.NORMAL に制限される。
FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL、Nobody のユーザー権限が維持され、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられる。
FMT_SMF.1 により、セキュリティ管理機能を U.ADMINISTRATOR と D.CONF の所有者である U.NORMAL へ提供する。
FTP_ITC.1 により、TOE と他の高信頼 IT 製品間のネットワーク上を流れる D.CONF に対する改変や暴露から保護される。
従って、O.CONF.NO.DIS、O.CONF.NO_ALT は、不正な開示、改変から D.CONF を保護することを保証することが出来る。

O.USER.AUTHORIZED
O.USER.AUTHORIZED は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証する対策方針である。
FIA_UID.1、FIA_UAU.1 により、利用者の識別と認証が実施される。
FIA_UAU.7 により、利用者認証時の認証フィードバックが保護される。
FIA_AFL.1 により、利用者認証の連続した認証失敗時に、ログインの受付がロックされる。
FIA_ATD.1 により、ログインユーザー名、ユーザー権限、ジョブ認可設定の利用者属性が維持される。
FIA_SOS.1 により、利用者認証の秘密が定義された品質尺度に合致することが検証される。
FIA_USB.1 により、ログインユーザー名、ユーザー権限、ジョブ認可設定の利用者属性をサブジェクトのセキュリティ属性に結びつけられる。
FTA_SSL.3 により、利用者のセッションが管理され、休止中のセッションは終了される。
FDP_ACC.1(b)、FDP_ACF.1(b)により、許可された利用者のみに基本機能の操作を許可する。
FMT_MSA.1(b)により、セキュリティ属性への操作を管理する。
FMT_MSA.3(b)により、セキュリティ属性である実行属性が適切なデフォルト値を有していることを保証する。
FMT_SMR.1 により、U.ADMINISTRATOR と U.NORMAL のユーザー権限が割り当てられ維持される。
従って、O.USER.AUTHORIZED は、利用者の識別と認証を要求し、セキュリティ方針に従って利用者にアクセス権を付与した後、TOE 使用を許可することを保証することが出来る。

O.INTERFACE.MANAGED
O.INTERFACE.MANAGED は、セキュリティ方針に従い、外部インターフェイスの操作を管理する対策方針である。
FIA_UID.1、FIA_UAU.1 により、利用者の識別と認証が実施される。
FIA_UAU.7 により、利用者認証時の認証フィードバックが保護される。

FIA_AFL.1により、利用者認証の連続した認証失敗時に、ログインの受付がロックされる。
FIA_SOS.1により、利用者認証の秘密が定義された品質尺度に合致することが検証される。
FTA_SSL.3により、利用者のセッションが管理され、休止中のセッションは終了される。
FPT_FDI_EXP.1により、内部ネットワークへの転送が保護される。
従って、O.INTERFACE.MANAGEDは、外部インターフェイスの操作を管理することが出来る。

O.SOFTWARE.VERIFIED
O.SOFRWARE.VERIFIEDは、TSFの実行コードを自己検証する手続きを提供する対策方針である。
FPT_TST.1により、TOEの起動時に自己テストのスイートの実行、TSFデータの一部の完全性検証が実施され、起動後の任意のタイミングにおける操作により TSF の一部の実行コード完全性検証が実施される。
従って､O.SOFRWARE.VERIFIEDは､TSFの実行コードを自己検証する手続きを提供することが出来る。

O.AUDIT.LOGGED
O.AUDIT.LOGGED は、TOE の使用とセキュリティに関連する事象を記録して管理し、不正な開示や改変を阻止する対策方針である。
FAU_GEN.1により、監査対象イベントに対して監査ログが生成される。
FAU_GEN.2、FIA_UID.1により、監査事象に対して利用者の識別情報と関連付けられる。
FPT_STM.1により、TOE内の高信頼タイムスタンプ機能を用い、監査事象に対して発生時刻が記録される。
従って、O.AUDIT.LOGGED は、TOE の使用とセキュリティに関連する監査事象を記録して管理し、不正な開示や改変を阻止することを保証することが出来る。

O.AUDIT_STORAGE.PROTECTED
O.AUDIT_STORAGE.PROTECTEDは、不正なアクセス、削除、改変から監査ログを保護することを保証する対策方針である。
FAU_STG.1により、格納された監査ログに対して、不当な削除及び改変から保護される。
FAU_STG.4により、監査ログが満杯になったとき、最も古くに格納された監査ログへの上書きを実施し、新しい監査ログを格納する。
従って、O.AUDIT_STORAGE.PROTECTEDは、不正なアクセス、削除、改変から監査ログを保護することを保証することが出来る。

O.AUDIT_ACCESS.AUTHORIZED
O.AUDIT_ACCESS.AUTHORIZEDは、潜在的なセキュリティ違反を検出するために、権限のある者だけが監査ログにアクセスすることを保証する対策方針である。
FAU_SAR.1により、U.ADMINISTRATORに監査ログからの情報の読み出し能力を提供する。
FAU_SAR.2により、U.ADMINISTRATOR以外の監査ログへのアクセスを制限する。
従って、O.AUDIT_ACCESS.AUTHORIZEDは、潜在的なセキュリティ違反を検出するために、権限のある者だけが監査ログにアクセスすることを保証することが出来る。

O.HDD.ENCRYPTION

O.HDD.ENCRYPTION は、TOE 内部の HDD に保存された User Data、TSF Data を暗号化する対策方針である。

FCS_CKM.1 により、指定されたアルゴリズムに従って、暗号鍵が生成される。

FCS_COP.1 により、指定された暗号アルゴリズムと暗号鍵長を使用して、HDD に保存する D.DOC、D.FUNC、D.PROT、D.CONF を暗号化し、読み出す D.DOC、D.FUNC、D.PROT、D.CONF を復号する。

従って、O.HDD.ENCRYPTION は、HDD に保存する User Data、TSF Data を暗号化することを保証することが出来る。

6.3.2. TOE セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間の依存関係を以下に示す。

表 6.11 TOE セキュリティ機能要件間の依存関係

機能要件	依存関係	依存性を満足していない要件
FAU_GEN.1	FPT_STM.1	－
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	－
FAU_SAR.1	FAU_GEN.1	－
FAU_SAR.2	FAU_SAR.1	－
FAU_STG.1	FAU_GEN.1	－
FAU_STG.4	FAU_STG.1	－
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	FCS_CKM.4 6.3.2.1 節参照
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	FCS_CKM.4 6.3.2.1 節参照
FDP_ACC.1(a)	FDP_ACF.1(a)	－
FDP_ACF.1(a)	FDP_ACC.1(a) FMT_MSA.3(a)	－
FDP_ACC.1(b)	FDP_ACF.1(b)	－
FDP_ACF.1(b)	FDP_ACC.1(b) FMT_MSA.3(b)	－
FDP_RIP.1	No dependencies.	－
FIA_AFL.1	FIA_UAU.1	－
FIA_ATD.1	No dependencies.	－
FIA_SOS.1	No dependencies.	－
FIA_UAU.1	FIA_UID.1	－

FIA_UAU.7	FIA_UAU.1	－
FIA_UID.1	No dependencies.	－
FIA_USB.1	FIA_ATD.1	－
FMT_MSA.1(a)	FDP_ACC.1(a) FMT_SMF.1 FMT_SMR.1	－
FMT_MSA.3(a)	FMT_MSA.1(a) FMT_SMR.1	－
FMT_MSA.1(b)	FDP_ACC.1(b) FMT_SMF.1 FMT_SMR.1	－
FMT_MSA.3(b)	FMT_MSA.1(b) FMT_SMR.1	－
FMT_MTD.1(a)	FMT_SMF.1 FMT_SMR.1	－
FMT_MTD.1(b)	FMT_SMF.1 FMT_SMR.1	－
FMT_SMF.1	No dependencies.	－
FMT_SMR.1	FIA_UID.1	－
FPT_STM.1	No dependencies.	－
FPT_TST.1	No dependencies.	－
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	－
FTA_SSL.3	No dependencies.	－
FTP_ITC.1	No dependencies.	－

6.3.2.1. FCS_CKM.4 の依存性を必要としない根拠

暗号鍵は主電源 ON 時に機器ごとに一意な値で毎回生成され揮発性メモリーに格納されるが、主電源を OFF にした後も、TOE は運用環境のセキュリティー対策方針 OE.PHYSICAL.MANAGED により物理的に保護されている。このため暗号鍵を破棄する要件は必要としない。

6.3.3. セキュリティ保証要件根拠

This TOE is Hardcopy Devices used in restrictive commercial information processing environments that require a relatively high level of document security, operational

accountability and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of user and TSF data is provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 3 is appropriate.

EAL 3 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。
表 7.1 は、TOE セキュリティ機能とセキュリティ機能要件の関係を示す。

表 7.1 TOE セキュリティ機能とセキュリティ機能要件

セキュリティ機能 / 機能要件	TSF.USER_AUTHENTICATION	TSF.DATA_ACCESS	TSF.JOB_AUTHORIZED	TSF.HDD_ENCRYPTION	TSF.DOC_OVERWRITE	TSF.AUDIT_LOGGED	TSF.SECURITY_MANAGEMENT	TSF.SELF_TEST	TSF.NETWORK_PROTECTION
FAU_GEN.1						✓			
FAU_GEN.2						✓			
FAU_SAR.1						✓			
FAU_SAR.2						✓			
FAU_STG.1						✓			
FAU_STG.4						✓			
FCS_CKM.1				✓					
FCS_COP.1				✓					
FDP_ACC.1(a)		✓							
FDP_ACF.1(a)		✓							
FDP_ACC.1(b)			✓						
FDP_ACF.1(b)			✓						
FDP_RIP.1					✓				
FIA_AFL.1	✓								
FIA_ATD.1	✓								
FIA_SOS.1	✓								
FIA_UAU.1	✓								
FIA_UAU.7	✓								
FIA_UID.1	✓								
FIA_USB.1	✓								
FMT_MSA.1(a)							✓		
FMT_MSA.3(a)		✓							
FMT_MSA.1(b)							✓		

FMT_MSA.3(b)			✓						
FMT_MTD.1(a)							✓		
FMT_MTD.1(b)							✓		
FMT_SMF.1							✓		
FMT_SMR.1							✓		
FPT_STM.1						✓			
FPT_TST.1								✓	
FPT_FDI_EXP.1									✓
FTA_SSL.3	✓								
FTP_ITC.1									✓

7.1. ユーザー管理機能

TSF.USER_AUTHENTICATION

ユーザー管理機能は、利用者が操作パネルもしくはクライアントPCからTOEを操作しようとした際に、許可された利用者かどうかを識別認証する機能である。

TOEは、操作パネルもしくはWebブラウザーからTOEの操作を行おうとした際に、ログイン画面を表示し、ログインユーザー名とログインユーザーパスワードの入力を要求する。

また、プリンタードライバー、TWAINドライバーからTOEにアクセスする際には、ジョブに付与されたログインユーザー名とログインユーザーパスワードにより、許可された利用者かどうかを識別認証する。

(1) FIA_UID.1　識別のタイミング

TOEは、利用者がログインを実施しようとした際に、入力されたログインユーザー名がTOE内部に登録されている利用者情報に存在することを検証する。

機器状態の取得については、TOEは、利用者の識別を行う前に、情報を提供する。ジョブ情報一覧とカウンター情報については、TOEは、利用者の識別を行う前に、情報を表示する。FAXデータの受信については、TOEは、利用者の識別を行う前に、FAXデータを受信する。

(2) FIA_UAU.1　認証のタイミング

TOEは、FIA_UID.1で識別が成功した場合に、同時に入力されたログインユーザーパスワードがTOE内部に登録されているパスワード情報と一致することを検証する。

機器状態の取得については、TOEは、利用者の認証を行う前に、情報を提供する。ジョブ情報一覧とカウンター情報については、TOEは、利用者の認証を行う前に、情報を表示する。FAXデータの受信については、TOEは、利用者の認証を行う前に、FAXデータを受信する。

(3) FIA_UAU.7　保護された認証フィードバック

TOEは、操作パネルもしくはクライアントPCから入力されたログインユーザーパスワードに対して、ダミー文字（*：asterisk）をログイン画面に表示する

(4) FIA_ATD.1　利用者属性定義
TOE は、ログインユーザー名、ユーザー権限、ジョブ認可設定の利用者属性を定義し、維持する。

(5) FIA_SOS.1　秘密の検証
TOE は、ログインユーザーパスワードが、定義された品質尺度に合致することを検証する。
定義された品質尺度は、パスワード長：8 文字以上、文字種別：英数字記号 である。

(6) FIA_USB.1　利用者 - サブジェクト結合
TOE は、ログインユーザー名、ユーザー権限、ジョブ認可設定の利用者属性をサブジェクトに割り当てる。

(7) FIA_AFL.1　認証失敗時の取り扱い
TOE は、操作パネル、もしくはクライアント PC からのログインに対し、最後の成功した認証以降の連続したログインの失敗回数が機器管理者の設定した値に達した場合に、該当アカウントのログインを許可しない（ロック状態）状態に移行する。
機器管理者による失敗回数の設定は 1 回～10 回の範囲で設定可能である。
ロック状態に移行した後は、1～60 分の間で機器管理者が指定した時間が経過するか、もしくは機器管理者がロック状態を解除すると通常状態に移行する。

(8) FTA_SSL.3　TSF 起動による終了
TOE は、操作パネル、もしくは Web ブラウザーからの操作が、一定時間無操作状態が継続した場合に、自動ログアウトを実施する。
※操作パネルと Web ブラウザー以外に対話セッションは存在しない。

- 操作パネル
  利用者がログイン後、無操作状態が機器管理者の設定した時間継続した場合に自動ログアウトを実施する。
  機器管理者による設定は 5 秒～495 秒の範囲で設定可能である。
- Web ブラウザー
  利用者がログイン後、無操作状態が 10 分間継続した場合に自動ログアウトを実施する。

7.2. データアクセス制御機能

TSF.DATA_ACCESS

データアクセス制御機能は、TOE の基本機能であるコピー、スキャン送信、プリンター、FAX、ボックスの各機能を用いて、TOE 内に保存されている画像データ、ジョブデータへのアクセスを、許可された利用者のみに制限する機能である。

(1) FDP_ACC.1(a)　サブセットアクセス制御
FDP_ACF.1(a)　セキュリティ属性によるアクセス制御

TOE は、表 7.2 に示す通り、各基本機能が扱う画像データ、ジョブデータに対し、利用者に対するアクセス制御規則に則って、許可された利用者のみにアクセスを許可する。
ここで、表 7.2 のアクセス制御規則において、「自身が実行したジョブ」の判別は、利用者のログインユーザー名と、対象資産が持つ所有者情報の一致により行われる。

表 7.2 データアクセス制御機能のアクセス制御規則

対象資産	操作内容	利用者	アクセス制御規則
画像データ（プリンター機能）	ボックス印刷（プリンタードライバーからの印刷指示後のジョブ）、USB メモリーからの印刷、削除	一般利用者	自身が実行したジョブの画像データへのアクセスを許可する
	削除	機器管理者	全てのジョブの画像データへのアクセスを許可する
画像データ（スキャン送信機能）	FTP 送信、E-mail 送信、TWAIN 送信、USB メモリー送信、送信画像プレビュー、削除	一般利用者	自身が実行したジョブの画像データへのアクセスを許可する
	削除	機器管理者	全てのジョブの画像データへのアクセスを許可する
画像データ（コピー機能）	コピー印刷、コピー画像プレビュー、削除	一般利用者	自身が実行したジョブの画像データへのアクセスを許可する
	削除	機器管理者	全てのジョブの画像データへのアクセスを許可する
画像データ（FAX 送信機能）	FAX 送信、送信画像プレビュー、削除	一般利用者	自身が実行したジョブの画像データへのアクセスを許可する
	削除	機器管理者	全てのジョブの画像データへのアクセスを許可する
画像データ（ボックス機能）	ボックス印刷、ボックスプレビュー、ボックス送信、ボックス内文書の移動/結合、削除	一般利用者	自身が所有者と設定されているボックス、もしくは、共有設定が有効に設定されているボックスの画像データへのアクセスを許可する
		機器管理者	全てのジョブの画像データへのアクセスを許可する
画像データ（FAX 受信機能）	FAX 受信印刷、FAX 転送、削除	機器管理者	FAX ボックスに保存されている画像データへのアクセスを許可する
ジョブデータ	ジョブ状況確認、変更、削除	一般利用者	自身が実行したジョブのジョブデータへのアクセスを許可する
		機器管理者	全てのジョブのジョブデータへのア

対象資産	操作内容	利用者	アクセス制御規則
			クセスを許可する

(2) FMT_MSA.3(a)　静的属性初期化

TOE は、新規に作成される画像データ、及びボックスのデフォルト値を設定する。画像データを新規に作成した場合の所有者情報は、作成した利用者のログインユーザー名として作成される。ボックスを新規に作成した場合のボックス所有者は、作成した機器管理者、共有設定は無効として作成される。

7.3. ジョブ認可機能

TSF.JOB_AUTHORIZED

ジョブ認可機能は、TOE の基本機能であるコピー、スキャン送信、プリンター、FAX、ボックスの各機能の利用を、許可された利用者のみに制限する機能である。

(1) FDP_ACC.1(b)　サブセットアクセス制御

FDP_ACF.1(b)　セキュリティ属性によるアクセス制御

TOE は、表 7.3 に示す通り、ユーザー管理機能にて識別認証された利用者の利用者情報に含まれるジョブ認可設定を確認し、利用を許可された基本機能のみ、ジョブの実行を許可する。

表 7.3 ジョブ認可機能のアクセス制御規則

対象機能	利用者	アクセス制御規則
コピー機能	一般利用者 機器管理者	利用者のジョブ認可設定に対象機能の実行属性が含まれる場合、ジョブの実行を許可する
プリンター機能	一般利用者 機器管理者	利用者のジョブ認可設定に対象機能の実行属性が含まれる場合、ジョブの実行を許可する
スキャン送信機能	一般利用者 機器管理者	利用者のジョブ認可設定に対象機能の実行属性が含まれる場合、ジョブの実行を許可する
FAX 機能	一般利用者 機器管理者	利用者のジョブ認可設定に対象機能の実行属性が含まれる場合、ジョブの実行を許可する
ボックス機能	一般利用者 機器管理者	利用者のジョブ認可設定に対象機能の実行属性が含まれる場合、ジョブの実行を許可する

(2) FMT_MSA.3(b)　静的属性初期化

TOE は、表 7.3 に示す利用者毎のジョブ認可設定の対象機能となるジョブの実行属性のデフォルト値を設定する。利用者を新規に追加した場合のジョブ認可設定に含まれる実行属性のデフォルト値は、全てのジョブが設定されている。

7.4. HDD 暗号化機能

TSF.HDD_ENCRYPTION

TOE は、基本機能を実行すると、画像データやジョブデータ、TSF データを HDD に保存する。HDD 暗号化機能は、これらのデータを HDD に保存する際に、データを暗号化して保存する機能である。

(1) FCS_CKM.1 暗号鍵生成

TOE は、AES アルゴリズムに使用する 256bit 暗号鍵を FIPS PUB 180-4 に基づく暗号鍵生成アルゴリズムを用いて生成する。この鍵は、複数の情報を元に、TOE の電源 ON 時に機器ごとに一意な値で毎回生成され、揮発性メモリーに保持される。尚、暗号鍵の元となる情報は運用開始時にのみ設定され、運用中に変更されることは無い。

(2) FCS_COP.1 暗号操作

TOE は、HDD にデータを保存する際、起動時に生成した暗号鍵生成(FCS_CKM.1)により作成した 256bit 暗号鍵を用い、FIPS PUBS 197 に基づく AES 暗号アルゴリズムに従ってデータの暗号化を行い、HDD に書込む。また、HDD に保存されたデータを読み出す際、同様に起動時に作成した暗号鍵を用い、AES 暗号アルゴリズムに従ってデータを復号する。

7.5. 上書き消去機能

TSF.DOC_OVERWRITE

TOE は、基本機能の各ジョブ完了後に、HDD と Flash メモリーに保存された画像データの削除を指示する。上書き消去機能は、この HDD と Flash メモリーに保存された画像データの削除が指示された際に、画像データの実データ領域に対して無意味な文字列を上書きし、実データ領域を再利用できなくする機能である。

(1) FDP_RIP.1 サブセット残存情報保護

TOE は、上書き消去の対象となる資源割り当て解除後の利用済み画像データを HDD、Flash メモリー上の特定の領域に置き、この特定の領域を監視するプロセスにより上書き消去を実行する。別の基本機能が指示され、上書き消去が待機状態になった場合や、上書き消去中の電源断により未了となった利用済み画像データがある場合も、待機状態が解除された時点や、電源が起動された時点で、監視プロセスにより上書き消去を実行する。

7.6. 監査ログ機能

TSF.AUDIT_LOGGED

監査ログ機能は、監査対象イベントが発生した際、監査ログを生成し記録・管理する機能である。

(1) FAU_GEN.1 監査データ生成

TOE は、表 7.4 で示す監査対象イベントが発生した際に、表 7.4 で示した監査データを記録し、監査ログを生成する。

表 7.4 監査対象イベントと記録する監査データ

監査対象イベント	監査データ	追加の監査データ
電源投入*1	イベントの日時 イベントの種別 利用者の識別情報（ログインを試みた利用者の識別情報を含む） イベントの結果(成功/失敗)	－
電源断*1		－
ジョブの完了		イベントの識別情報
ジョブデータの操作（参照、改変、削除）		イベントの識別情報
利用者識別認証の成功と失敗		－
最後の成功した認証以降の連続した不成功認証試行が閾値に到達した時のユーザーアカウントロックアウトの実行と、機器管理者によるロックアウト状態の解除		－
自動ログアウトによるセッション終了		－
画像データの操作（参照、削除）		イベントの識別情報
ユーザー管理情報の編集(利用者に対するユーザー権限の変更)		－
ログインユーザーパスワード登録時（新規作成、編集）の品質検査による拒否		
セキュリティ管理機能の使用		－
時刻の変更		－
TLS、IPsec 通信の通信失敗		通信先 IP アドレス

*1 監査機能の開始と終了は、TOE の開始と終了と同期するため、TOE の電源投入、電源断のイベントで代用する

(2) FAU_GEN.2　利用者識別情報の関連付け

TOE は、各監査対象イベントに対し、その原因となった利用者の識別情報を監査ログに関連付ける。

(3) FAU_SAR.1　監査レビュー

FAU_SAR.2　限定監査レビュー

TOE は、監査ログからの情報読み出し能力を、機器管理者のみに提供する。さらに機器管理者に対し、その情報を解釈するのに適した形式で監査記録を提供する。監査ログの読み出しは、機器管理者が設定した宛先に E-mail として送信される。

(4) FAU_STG.1　保護された監査証跡格納

TOE は、監査ログからの情報読み出し、削除を行う能力を、機器管理者のみに提供する。機器管理者以外の一般利用者が監査ログにアクセスするための機能は提供しない。

(5) FAU_STG.4　監査データ損失の防止
TOE は、監査ログが満杯になった場合、最も古い日時で格納された監査ログへの上書きを行い、新しい監査対象イベントを記録する。

(6) FPT_STM.1　高信頼タイムスタンプ
TOE は、TOE 内部にシステム時計を有する。監査対象イベントが発生した際、このシステム時計を基にイベントの発生日時を記録する。TOE 内部のシステム時計が刻む時刻を遅延なく即時に監査記録に刻印することで高信頼なタイムスタンプを提供する。

7.7. セキュリティ管理機能

TSF.SECURITY_MANAGEMENT

セキュリティ管理機能は、利用者情報の編集や、TOE のセキュリティ機能の設定を、許可された利用者のみに制限し、管理する機能である。操作パネル及び、クライアント PC から利用することが出来る。クライアント PC からの操作には、Web ブラウザーを使用する。

(1) FMT_MSA.1(a)　セキュリティ属性の管理
TOE は、ボックス機能における、全てのボックスに対する以下の操作を、機器管理者のみに許可する。

- ボックスの所有者の参照と変更
- ボックスの共有設定の参照と変更

また、ボックス機能における、文書に対する以下の操作を、機器管理者のみに許可する。

- 文書の所有者情報の参照と変更

一般利用者に対しては、自身が所有者になっているボックスに対して、以下の操作を許可する。

- ボックスの共有設定の参照と変更

(2) FMT_MSA.1(b)　セキュリティ属性の管理
TOE には、表 7.3 に示す実行属性を操作できる役割は無い。

(3) FMT_MTD.1(a)　TSF データ管理
TOE は表 7.5 に示す TSF データに対する、表 7.5 で示される操作を機器管理者のみに提供する。

表 7.5 機器管理者による TSF データの操作

TSF データ	許可された操作
利用者情報の登録 （ログインユーザー名、ログインユーザーパスワード、ユーザー権限、ジョブ認可設定）	編集、削除、新規作成
ユーザーアカウントロックアウトポリシー設定 （ロックまでの回数、ロックアウト期間）	変更
ロックアウトリスト	変更
自動ログアウト時間設定	変更
パスワードポリシー設定	変更
日時設定	変更
ネットワーク暗号設定	変更
FAX 転送設定	変更
監査ログレポート送信先情報	変更

(4) FMT_MTD.1(b)　TSF データ管理

TOE は表 7.6 に示す TSF データに対する、表 7.6 で示される操作を一般利用者に提供する。

表 7.6 一般利用者による TSF データの操作

TSF データ	許可された操作
利用者情報の編集 （利用者に関連付いたログインユーザーパスワード）	編集

(5) FMT_SMR.1　セキュリティの役割

TOE は、機器管理者 及び 一般利用者のユーザー権限を維持し、利用者をそのユーザー権限に関連付ける。

(6) FMT_SMF.1　管理機能の特定

TOE は、(1)に示したボックス機能に対するセキュリティ属性の管理機能、及び、表 7.5、表 7.6 に示した TSF データに対する表 7.5、表 7.6 で示した操作を行うセキュリティ管理機能を提供する。

7.8. 自己テスト機能

TSF.SELF_TEST

自己テスト機能は、以下の自己テストを実施する機能である。

(1) FPT_TST.1 TSF テスト

TOE は以下の自己テストを実施する。

- HDD 暗号化機能の正常動作チェック
- 暗号鍵の完全性チェック
- セキュリティ機能の実行モジュールの完全性チェック

起動時に、暗号鍵を用いて暗号化/復号の動作確認を実施することで、HDD 暗号化機能の正常動作チェックと暗号鍵の完全性チェックを同時に実施する。また、セキュリティ機能の実行モジュールの完全性チェックは機器管理者の指示で実施する。
起動時のチェックにて、異常が認められた場合は、TOE の操作パネルに異常を表示し、利用者に異常状態であることを示す。利用者は、異常表示が無ければ、正常に動作出来ているものとして TOE を利用することが出来る。

7.9. ネットワーク保護機能

TSF.NETWORK_PROTECT

ネットワーク保護機能は、TOE と他の高信頼 IT 製品間のネットワーク上を流れる全てのデータを暗号化し、不正な改変や暴露から保護する機能である。
また、外部インターフェイスから TOE にアクセスする情報を、TOE を介して内部ネットワークに無断転送することを防止する機能も提供する。

(1) FTP_ITC.1 TSF 間高信頼チャネル

TOE は、高信頼 IT 製品である各種サーバーやクライアント PC と通信を行う際に、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できる。
対象となる機能は以下の通りである。

- スキャン送信機能
- プリンター機能
- ボックス機能（送信機能）
- ボックス機能におけるクライアント PC（Web ブラウザー）からの操作
- セキュリティ管理機能におけるクライアント PC（Web ブラウザー）からの操作

ただし、プリンター機能におけるローカル接続での利用は対象外である。

TOE が提供する高信頼チャネル通信は以下の通りである。

表 7.7 TOE が提供する高信頼チャネル通信

通信先	プロトコル	暗号アルゴリズム
クライアント PC	TLSv1.2	3DES(168 bits)、AES(128bits、256bits)
メールサーバー	IPsec	3DES(168 bits)、AES(128bits、192bits、256bits)
FTP サーバー	IPsec	3DES(168 bits)、AES(128bits、192bits、256bits)

(2) FPT_FDI_EXP.1　外部インターフェイスへの制限された情報転送

TOE は、全ての外部インターフェイスから入力された情報、及び受信したデータを、直接内部ネットワーク上のサーバーやクライアント PC に転送する仕組みは持っておらず、無断転送できないように制御されている。

また、電話回線を通して受信するデータは、FAX 機能だけに制限されており、FAX 通信プロトコルに則ったデータのみを受信する仕組みとなっている。このため、無断で内部ネットワークに転送することはできないように制御されている。

8. 略語・用語

8.1. 用語の定義

本 ST で使用される用語の定義を表 8.1 で示す。

表 8.1 ST で使用される用語の定義

用語	定義
Data Security Kit (E)	TOE のセキュリティ機能の一部である、HDD 暗号化機能/上書き消去機能を活性化させるためのセキュリティ強化ライセンスである。MFP のオプション製品として提供されており、ライセンス情報を MFP に入力することで、活性化される。
FAX System 12	FAX 機能を利用するために、MFP のオプション製品として提供されている。専用の FAX 基盤を MFP に装着することにより、FAX 機能が利用可能となる。
HD-12	ボックス機能を拡張するための HDD ストレージオプションである。ボックス機能に保存する容量やボックス件数を多く登録することが出来る。
TWAIN	TOE のスキャナーから画像を読み込み、クライアント PC に画像を送信するための機能である。TWAIN という用語自身は API 仕様のことを指す。
FAX データの受信	TOE に送られてくる FAX のデータを受け取るまでの動作のことを指す。(データの印刷や転送の処理は含まない。)
ジョブ	TOE が持つコピー機能、プリンター機能、スキャン送信機能、FAX 機能、ボックス機能を実現するための作業プロセスの処理単位のこと。
ジョブデータ	一般利用者が、コピー機能、スキャン送信機能、プリンター機能、FAX 機能及びボックス機能を利用し、ジョブを実行した場合に生成されるデータ。 ジョブデータは、実行待ちのためにジョブキューに入り、ジョブが完了すると消去されるデータである。
ジョブ情報	ジョブが持つ情報を指す。主に稼働中のジョブのことを指すが、実行結果の履歴を含めて指すこともある。
ジョブ情報一覧	ジョブ情報をリスト化したもの。
ジョブ状況確認	ジョブデータの詳細情報を確認すること。
ボックス情報	ボックス機能で使用するボックスと呼ばれる領域（箱）に関する情報。ボックス名称やボックス番号、ボックスサイズなどがある。セキュリティ属性である、ボックスの所有者とボックスの共有設定も含まれる。

編集	利用者情報やボックス情報など、利用者が登録したデータを変更する操作のこと。
移動	ボックス内に保存された文書を、別のボックスに移動すること。
結合	ボックス内に保存された複数の文書同士を結合すること。元の文書は残したまま、新しく結合文書を作成する。
送信画像プレビュー	スキャン送信機能、FAX 機能の操作の１つ。送信するために TOE のスキャナーから読み込んだ画像のプレビューを操作パネルに表示する機能である。
コピー画像プレビュー	コピー機能の操作の１つ。コピーするために TOE のスキャナーから読み込んだ画像のプレビューを操作パネルに表示する機能である。
ボックスプレビュー	ボックス機能の操作の１つ。ボックス内に保存されている文書のプレビューを操作画面に表示することである。
機器状態	TOE の状態を表す情報のこと。用紙残量やトナー残量、機械的なエラーなどが表示される。
カウンター情報	TOE が実行したジョブなどよりカウントされる情報。プリンター機能が実行されれば、印刷カウンターが増加し、スキャン送信機能が実行されれば、送信カウンターが増加する。
画像データ	一般利用者が、コピー機能、スキャン送信機能、プリンター機能、FAX 機能及びボックス機能を利用した際に、TOE 内部で処理される画像情報のことを指す。
クライアント PC	ネットワークに接続された TOE に対して、ネットワークに接続して TOE のサービス(機能)を利用する側のコンピュータのことを指す。
FIPS PUB 180-4	米国の NIST（National Institute of Standards and Technology：国立標準技術研究所）で規格化されたハッシュ関数に関するアルゴリズムである。
FIPS PUB 197	米国の NIST（National Institute of Standards and Technology：国立標準技術研究所）で規格化された共通鍵暗号に関するアルゴリズムである。AES 暗号とも呼ばれる。
管理領域	画像データの中で、そのデータの管理情報が記された領域。画像データを論理的に削除するとは、この領域だけを認識不可能なものにすることを指す。
実データ領域	画像データの中で、実際の画像を構成するデータが記された領域。画像データを論理的に削除した場合には、この領域は残存してしまう。この残存した領域を指して「残存データ」と呼ぶ。

上書き消去	HDD に保存された画像データの削除が指示された際に、画像データの実データ領域に対して無意味な文字列を上書きし、実データ領域を完全に消去した上で画像データの管理情報を削除することを指す。こうすることでデータ再利用を不可能な状態にすることが出来る。
操作パネル	複合機の一番上部に設置され、液晶パネルで構成される。 外部インターフェイスであり、利用者は、操作パネルを通して TOE を利用することが出来る。

8.2. 略語の定義

本 ST で使用される略語の定義を表 8.2 で示す。

表 8.2 ST で使用される略語の定義

用語	定義
A.	assumption (when used in hierarchical naming)
ADMIN.	administrator (when used in hierarchical naming)
AES	Advanced Encryption Standard
ALT	alteration
CC	Common Criteria
CONF.	confidential (when used in hierarchical naming)
CPY	copy
D.	data (when used in hierarchical naming)
DIS	disclosure
DOC.	document (when used in hierarchical naming)
DSR	document storage and retrieval
EAL	Evaluation Assurance Level
F.	Function (when used in hierarchical naming)
FAX	facsimile
FUNC.	function (when used in hierarchical naming)
HCD	Hardcopy Device
HDD	Hard Disk Drive
IT	information technology
MFP	Multifunctional Product / peripheral / printer
NAND	Not AND
NCU	Network Control Unit
NVS	nonvolatile storage

O.	Security Objective (of the TOE) (when used in hierarchical naming)
OE.	Security Objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PP	Protection Profile
PROT.	protected (when used in hierarchical naming)
PRT	print
SAR	Security Assurance Requirement
SCN	scan
SFP	Security Function Policy
SFR	Security Functional Requirement
SMI	Shared-medium Interface
SSD	Solid State Drive
ST	Security target
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
U.	user (when used in hierarchical naming)
USB	Universal Serial Bus

（　最終ページ　）