# ECOSYS M6635cidn, ECOSYS M6630cidn, TASKalfa 351ci データセキュリティキット、SSD 付きモデル セキュリティターゲット 第 1.11 版

2019 年 5 月 17 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 |
|---|---|---|
| 2018/01/10 | 0.80 | ・初版作成 |
| 2018/02/05 | 0.85 | ・指摘事項修正 |
| 2018/02/22 | 0.90 | ・指摘事項修正 |
| 2018/08/31 | 1.00 | ・指摘事項修正 |
| 2018/10/25 | 1.01 | ・指摘事項修正 |
| 2018/11/02 | 1.02 | ・指摘事項修正 |
| 2018/11/21 | 1.03 | ・指摘事項修正 |
| 2018/12/05 | 1.04 | ・指摘事項修正 |
| 2018/12/14 | 1.05 | ・指摘事項修正 |
| 2019/02/26 | 1.06 | ・指摘事項修正 |
| 2019/03/13 | 1.07 | ・指摘事項修正 |
| 2019/04/02 | 1.08 | ・指摘事項修正 |
| 2019/04/10 | 1.09 | ・指摘事項修正 |
| 2019/04/22 | 1.10 | ・指摘事項修正 |
| 2019/05/17 | 1.11 | ・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： ECOSYS M6635cidn, ECOSYS M6630cidn, TASKalfa 351ci データセキュリティキット、SSD 付きモデル
セキュリティターゲット

ST バージョン： 第 1.11 版

作成日： 2019/05/17

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： ECOSYS M6635cidn, ECOSYS M6630cidn, ECOSYS M6635cidnG, ECOSYS M6630cidnG, TASKalfa 351ci(KYOCERA), P-C3566i MFP, P-C3066i MFP, 356ci(TA Triumph-Adler/UTAX) データセキュリティキット、SSD 付きモデル

【注釈】
データセキュリティキット、SSD 付きモデルとは、ECOSYS M6635cidn, ECOSYS M6630cidn, ECOSYS M6635cidnG, ECOSYS M6630cidnG, TASKalfa 351ci, P-C3566i MFP, P-C3066i MFP, 356ci に、次の追加オプションを付加した製品構成である

- データセキュリティキット : Data Security Kit (E)
- オプション SSD : HD-7

TOE バージョン： システム : 2V1_S0IS.C01.010

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 ECOSYS M6635cidn, KYOCERA ECOSYS M6630cidn,
KYOCERA ECOSYS M6635cidnG, KYOCERA ECOSYS M6630cidnG,
KYOCERA TASKalfa 351ci,
TA Triumph-Adler P-C3566i MFP, TA Triumph-Adler P-C3066i MFP,
UTAX P-C3566i MFP, UTAX P-C3066i MFP
TA Triumph-Adler 356ci, UTAX 356ci

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に搭載されるファームウェアの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「ECOSYS M6635cidn, ECOSYS M6630cidn, ECOSYS M6635cidnG, ECOSYS M6630cidnG, TASKalfa 351ci, P-C3566i MFP, P-C3066i MFP, 356ci」である。このうち、SSD については、オプションである「HD-7」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「ECOSYS M6635cidn, ECOSYS M6630cidn, ECOSYS M6635cidnG, ECOSYS M6630cidnG, TASKalfa 351ci, P-C3566i MFP, P-C3066i MFP, 356ci」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。

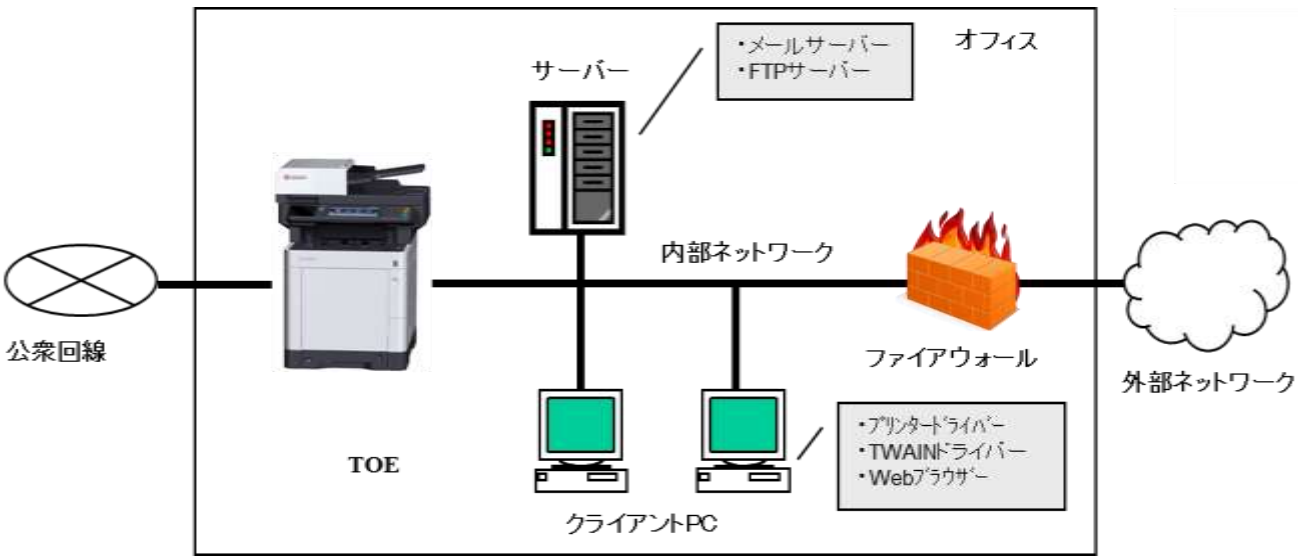


**図 1.1 一般的な利用環境**

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、ボックスに保存された文書データへのアクセスを制御する機能、SSDに格納される文書データを暗号化する機能、

公衆回線から受信したデータを内部ネットワークへ転送することを制御する機能、及びネットワークを保護する機能を備える。なお、本TOEは監査機能と自己テスト機能は備えていない。

## 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。

利用者には、一般利用者と機器管理者がある。

- 一般利用者

  TOE が提供するコピー機能、プリンター機能、スキャン送信機能、FAX 機能、ボックス機能などの TOE の機能を利用する人。

- 機器管理者

  TOE の運用管理を行い、TOE の管理者として登録されている人。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および TOE を正しく動作させるための導入と運用管理を行う。

### 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。

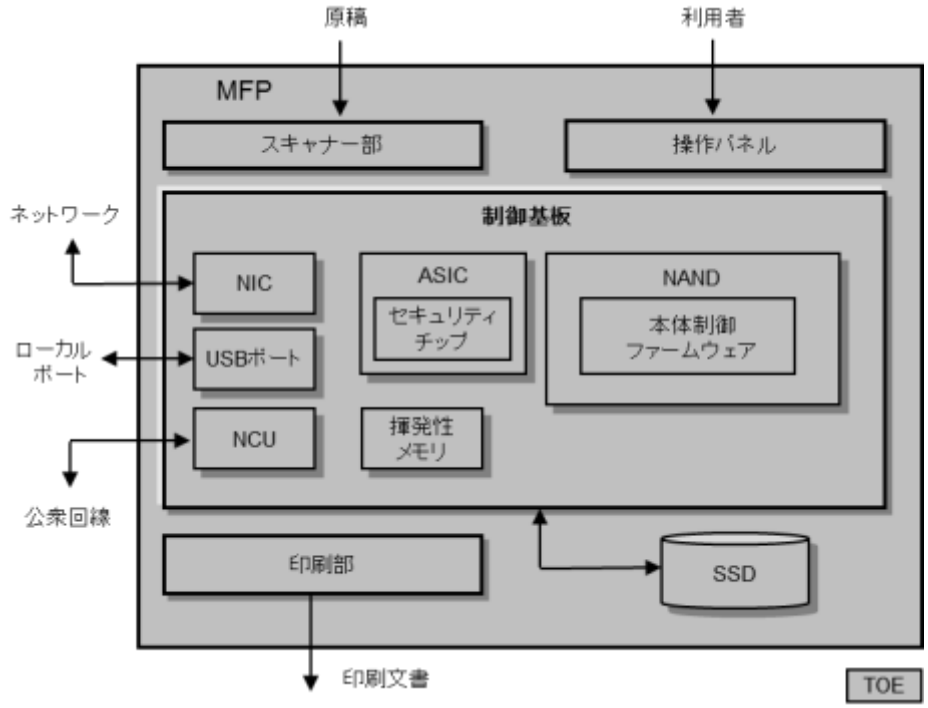


図 1.2 TOE の物理的構成図

TOE は、操作パネル、スキャナー部、印刷部、制御基板、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。
制御基板は、TOE 全体の制御を行うための回路基板であり、制御基板上の NAND メモリーに格納される形で本体制御ファームウェアが搭載されている。インタフェースとして、ネットワークインタフェース（NIC)、ローカルインタフェース（USB ポート）と公衆回線インタフェース（NCU）を持つ。
また制御基板上の 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、SSD 暗号化機能（後述）におけるセキュリティ演算処理を実現している。

また、記憶媒体として、制御基板上にファームウェアと機器設定を保存する NAND と作業領域として使用する揮発性メモリーと文書データを保存する SSD 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、機器設定のうち、ボックス機能に関する情報は SSD に保存される。

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 1.1 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 | MFP 装置 | クーリエ配送 | TOE 参照で示す MFP 製品名称およびファームウェアバージョン情報 |
| SSD | SSD ハードウェア | クーリエ配送 | HD-7 |
| 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 1.2 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。

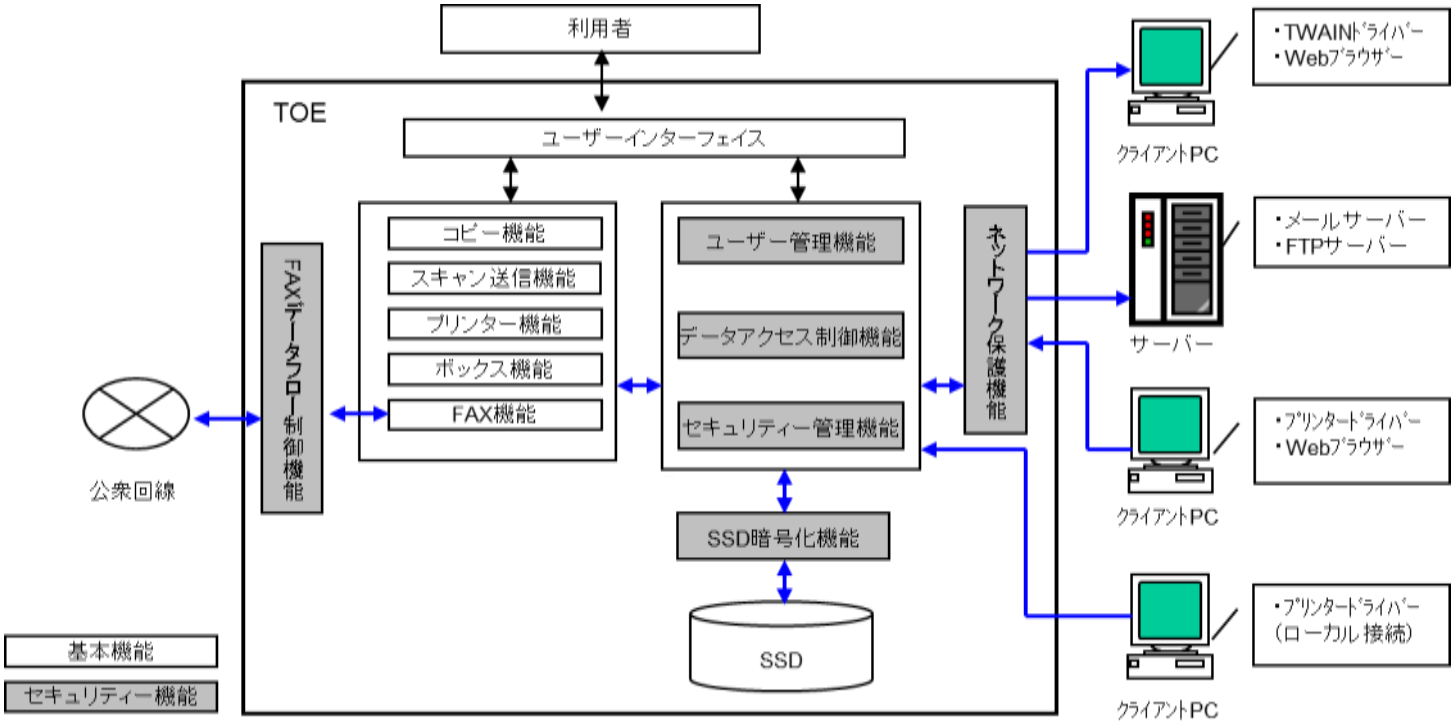


**図 1.3 TOE の論理的構造図**

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、文書データを 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。

- 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、文書データを 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。
  - ✓ 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、

受信した文書データを 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。

- 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文書データを外部に送信し、FAX 受信では、受信した文書データを TOE の印刷部から出力、または TOE 内に保存することが出来る。

- ボックス機能
  一般利用者が、文書データをボックスに保存、及び読み出して送信、印刷する機能。ボックス内で文書データを移動、結合することも出来る。

  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、入力された文書データを SSD 上に保存する。また、FAX 機能で受信する文書データを SSD 上に保存することも出来る（FAX ボックス）。保存された文書データは、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。保存された文書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）

- ユーザーインタフェース
  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 内のボックス文書データに対し、許可された利用者のみがアクセス可能となるように、アクセスを制限する機能。

- FAX データフロー制御機能
  公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送されないように制御する機能。

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

- 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。

- 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。
  TOE のスキャン送信機能、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。

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 1.2 TOE を構成するガイダンス**

| 名称 | バージョン | 仕向地 |
|---|---|---|
| ECOSYS M6635cidn クイックガイド | 初版 2017.10<br>302V15603001 | 日本 |
| ECOSYS M6635cidn セーフティーガイド<br>ECOSYS M6635cidn / ECOSYS M6630cidn Safety Guide | 2017.10<br>302V15621001 | 日本/海外 |
| ECOSYS M6635cidn 使用説明書 | Rev.1 2017.12<br>2V1KDJA001 | 日本 |
| ECOSYS M6635cidn ファクス使用説明書 | Rev.1 2017.12<br>2V1KDJA501 | 日本 |
| ECOSYS M6635cidn Data Security Kit (E) 使用説明書 | 2019.5<br>3MS2V1KDJA2 | 日本 |
| Command Center RX 操作手順書 | Rev.14 2017.10<br>CCRXKDJA14 | 日本 |
| ECOSYS M6635cidn プリンタードライバー 操作手順書 | 2TXCLKTJA720.2<br>017.10 | 日本 |
| KYOCERA Net Direct Print 操作手順書 | DirectPrintKDJ<br>A1.2016.02 | 日本 |
| お知らせ / Notice | 2019.3<br>303MS5640002 | 日本/海外 |
| Data Security Kit (E) 設置手順書 / Installation Guide | 2013.1<br>303MS56710-02 | 日本/海外 |
| ECOSYS M6630cidn / ECOSYS M6635cidn FIRST STEPS QUICK GUIDE | 2017.10<br>302V15602001 | 海外 |
| ECOSYS M6630cidn / ECOSYS M6635cidn OPERATION GUIDE *1 | Rev.1 2018.1<br>2V1KDEN001 | 海外 |
| ECOSYS M6630cidn / ECOSYS M6635cidn FAX OPERATION GUIDE *1 | Rev.1 2017.12<br>2V1KDEN501 | 海外 |
| ECOSYS M6630cidn / ECOSYS M6635cidn Data Security Kit (E) OPERATION GUIDE | 2019.5<br>3MS2V1KDEN3 | 海外 |
| Command Center RX User Guide | Rev.13 2017.10<br>CCRXKDEN13 | 海外 |
| ECOSYS M6635cidn / ECOSYS M6630cidn / TASKalfa 351ci Printer Driver User Guide | 2V1CLKTEN720.2<br>017.10 | 海外 |

| | | |
|---|---|---|
| KYOCERA Net Direct Print User Guide | DirectPrintKDE N1.2016.02 | 海外 |
| TASKalfa 351ci OPERATION GUIDE *2 | First edition 2018.1 2VWKDEN000 | 海外 |
| TASKalfa 351ci FAX OPERATION GUIDE *2 | First edition 2017.12 2VWKDEN500 | 海外 |

*1 は ECOSYS M6635cidn, M6630cidn, M6635cidnG, M6630cidnG, P-C3566i MFP, P-C3066i MFP 用のガイダンスであり、*2 は TASKalfa 351ci, 356ci 用のガイダンスである。また、これら以外は全製品に共通のガイダンスである。

### 1.4.5. TOE の保護資産

TOE が保護する資産は、以下のとおりである。

(1) スプール文書データ
一般利用者が TOE のスキャン送信機能およびプリンター機能を利用した際に、ジョブ処理時に TOE 内部の SSD に一時的に保存する文書データ。

(2) ボックス文書データ
一般利用者が TOE の基本機能であるボックス機能を利用した際に、TOE 内部の SSD に保存する文書データ。ただし、ボックス機能のうち、ローカル接続された USB メモリーが指定された際は、USB メモリーに保存される。この文書データは、操作パネルや Web インタフェースからの操作で送信、印刷、移動、削除をすることが出来る。

(3) TOE 設定データ
機器管理者、一般利用者が TOE のセキュリティ機能を適切に管理、使用するために設定、登録する表 1.3 で記載するデータ。表 1.3 のうち、ボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）は SSD に保存される。

(4) 内部ネットワーク上の通信データ
一般利用者が基本機能を利用した際、または機器管理者が Web インタフェース経由で TOE のセキュリティ設定を変更、管理する際に、内部ネットワーク上を流れるデータ。文書データと TOE 設定データの両方を含む。

表 1.3 本 TOE が対象とする TOE 設定データ

| TOE 設定データ | 概要 |
|---|---|
| ログインユーザー名 | TOE を利用する際に使用される利用者の識別情報。<br>機器管理者により登録され 64 文字以内の半角文字で構成される。 |
| ログインユーザーパスワード | ログインユーザー名に対する利用者の認証情報。<br>利用者により登録され 64 文字以内の半角文字で構成される。 |
| 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<br>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。所有者の情報には登録されているログインユーザー名の１つが割り当てられる。 |
| 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であり、有効か無効が設定される。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。 |
| ネットワーク暗号設定（TLS、IPsec 設定） | ネットワーク保護機能に使用する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。<br>転送先として F コード値に対応する FAX ボックスの設定が出来る。 |

# 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：

情報技術セキュリティ評価のためのコモンクライテリア
パート1: 概説と一般モデル　バージョン3.1　改訂第5版
パート2: セキュリティ機能コンポーネント　バージョン3.1　改訂第5版
パート3: セキュリティ保証コンポーネントバージョン3.1　改訂第5版

CCパート2に対するSTの適合：CCパート2適合
CCパート3に対するSTの適合：CCパート3適合

## 2.2. PP 主張

本ST およびTOE が適合するPPはない。

## 2.3. パッケージ主張

本ST およびTOE は、パッケージ：EAL2適合 を主張する。追加する保証コンポーネントはない。

## 2.4. 適合根拠

本STおよびTOEは、PP適合を主張していないので、PP適合根拠はない。

# 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. 脅威

本TOEに対する脅威を表3.1のとおり識別する。また、攻撃者は基本的な攻撃能力を持つ者であることを想定している。

**表 3.1 脅威**

| 脅威 | 内容 |
|---|---|
| T.SETTING_DATA | 悪意のある者が、操作パネルおよびクライアントPCからTOE設定データへ不正にアクセスして、設定値を変更する、もしくは、漏洩するかもしれない。 |
| T.IMAGE_DATA | 悪意のある者が、操作パネルおよびクライアントPCからアクセス権限のないボックス文書データへ不正にアクセスし、ボックス文書データを漏洩もしくは改ざんするかもしれない。 |
| T.NETWORK | 悪意のある者が、内部ネットワーク上の文書データおよびTOE設定データに対して不正に盗聴もしくは改ざんするかもしれない。 |

## 3.2. 組織のセキュリティ方針

本TOEが遵守しなければならない組織のセキュリティ方針を表3.2に記載する。

**表 3.2 組織のセキュリティ方針**

| 組織のセキュリティ方針 | 内容 |
|---|---|
| P.SSD_ENCRYPTION | TOEは､SSD上に保存される文書データおよびTOE設定データを暗号化しなければならない。 |
| P.FAX_CONTROL | TOEは、公衆回線から受信したデータをTOEが接続された内部ネットワークへ転送しないように制御しなければならない。 |

### 3.3. 前提条件

本TOEの前提条件を表3.3に記載する。

**表 3.3 前提条件**

| 前提条件 | 内容 |
|---|---|
| A.ACCESS | TOE を構成するハードウェアおよびソフトウェアは、不正な解析や改ざんなどのセキュリティ侵害から保護された環境に設置される。 |
| A.NETWORK | TOE は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に接続されて使用される。 |
| A.USER_EDUCATION | TOE の利用者は、組織のセキュリティ方針やその手順を認識し、その方針や手順に従うよう教育を受ける。 |
| A.DADMIN_TRUST | TOE の機器管理者は、機器管理者として機器を適切に管理する能力を有し、悪意のある目的のために、機器管理者としての権限を悪用しない信頼性がある。 |

# 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. TOE のセキュリティ対策方針

TOEのセキュリティ対策方針を表4.1に記載する。

**表 4.1 TOE のセキュリティ対策方針**

| セキュリティ対策方針 | 内容 |
|---|---|
| O.SSD_ENCRYPTION | TOE は、SSD に保存する文書データおよび TOE 設定データを暗号化する機能を提供しなければならない。 |
| O.NETWORK_ENCRYPTION | TOE は、内部ネットワーク上の文書データおよび TOE 設定データを盗聴や改ざんから保護するために、ネットワーク保護に必要な暗号化通信機能を提供しなければならない。 |
| O.FAX_CONTROL | TOE は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する FAX データフロー制御機能を提供しなければならない。 |
| O.SETTING_DATA | TOE は、操作パネルおよびクライアント PC からの TOE 設定データへのアクセスを認証された正当な利用者のみに許可し、許可されない者からの TOE 設定データへのアクセスを不可能にし、TOE 設定データの設定変更、および漏洩を不可能にしなければならない。 |
| O.ACCESS_CONTROL | TOE は、操作パネルおよびクライアント PC からアクセスする利用者を識別認証し、正当な利用者のみに、ボックス文書データへのアクセスが可能となるように、ボックス文書データへのアクセスを制御する機能を提供しなければならない。 |

4.2. 運用環境のセキュリティ対策方針

TOE の運用環境のセキュリティ対策方針を表 4.2 に記載する。

**表 4.2 運用環境のセキュリティ対策方針**

| セキュリティ対策方針 | 内容 |
|---|---|
| OE.ACCESS | TOE は機器管理者による監視が可能な管理された環境で運用し、機器管理者による監視により、TOE を構成するハードウェアおよびソフトウェアに対する解析、改ざんを行う攻撃を防止しなければならない。 |
| OE.NETWORK_PROTECTION | TOE が接続される内部ネットワークは、ファイアーウォールなどの機器を設置して、外部ネットワークから TOE への攻撃を防止しなければならない。 |
| OE.USER_EDUCATION | 組織は、組織のセキュリティ方針や手順を認識し、当該の方針や手順に従うように、TOE の利用者に教育し、それらを習得させなければならない。 |
| OE.DADMIN_TRUST | 機器管理者は、信頼のできる人物を選出し、所属する組織のセキュリティ方針や運用ルールを遵守するよう、また製品ガイダンスの記載に従って適切な操作ができるように、十分な指導を受けなければならない。 |

4.3. セキュリティ対策方針根拠

前提条件、脅威、および組織のセキュリティ方針とセキュリティ対策方針の対応関係を下表に示す。セキュリティ対策方針が少なくとも１つ以上の前提条件、脅威、組織のセキュリティ方針に対応していることを示している。

**表 4.3 前提条件、脅威、組織のセキュリティ方針とセキュリティ対策方針の対応関係**

| | 前提条件、脅威、組織のセキュリティ方針 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| セキュリティ対策方針 | A.ACCESS | A.NETWORK | A.USER_EDUCATION | A.DADMIN_TRUST | T.SETTING_DATA | T.IMAGE_DATA | T.NETWORK | P.SSD_ENCRYPTION | P.FAX_CONTROL |
| O.SSD_ENCRYPTION | | | | | | | | ✓ | |
| O.NETWORK_ENCRYPTION | | | | | | | ✓ | | |
| O.FAX_CONTROL | | | | | | | | | ✓ |
| O.SETTING_DATA | | | | | ✓ | | | | |
| O.ACCESS_CONTROL | | | | | | ✓ | | | |
| OE.ACCESS | ✓ | | | | | | | | |
| OE.NETWORK_PROTECTION | | ✓ | | | | | | | |
| OE.USER_EDUCATION | | | ✓ | | | | | | |
| OE.DADMIN_TRUST | | | | ✓ | | | | | |

また、前提条件、脅威、組織のセキュリティ方針に対するセキュリティ対策方針根拠を表 4.4 に記載する。

**表 4.4 セキュリティ課題定義に対するセキュリティ対策方針根拠**

| 前提条件、<br>脅威、<br>組織のセキュリティ方針 | セキュリティ対策方針根拠 |
|---|---|
| A.ACCESS | A.ACCESS の前提条件は、TOE を構成するハードウェアおよびソフトウェアが不正な解析や改ざんなどのセキュリティ侵害から |

| | |
|---|---|
| | 保護された環境に設置されることを必要する。<br>OE.ACCESS の対策により、TOE は機器管理者による監視が可能な管理された環境で運用し、機器管理者による監視により TOE を構成するハードウェアおよびソフトウェアに対する解析、改ざん等を行う攻撃を制限することを行うので、攻撃方法、攻撃機会が制限され、A.ACCESS を実現することができる。 |
| A.NETWROK | A.NETWORK の前提条件は、TOE が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に接続されて使用されることを必要とする。<br>OE.NETWORK_PROTECTION の対策により、TOE が設置される内部ネットワークは、ファイアーウォールなどの機器を設置して、外部ネットワークからの TOE への攻撃を制限することを行うので、外部ネットワークからの不特定多数の脅威エージェントによる攻撃方法、攻撃機会が制限され、A.NETWORK を実現することができる。 |
| A.USER_EDUCATION | A.USER_EDUCATION の前提条件は、TOE の利用者が、組織のセキュリティ方針や手順を認識し、その方針や手順に従うよう教育を受けることを必要とする。<br>OE.USER_EDUCATION の対策により、TOE の利用者は、組織のセキュリティ方針や手順を認識し、該当の方針や手順に従うように、TOE の利用者に教育し、それらを習得させることを行うので、A.USER_EDUCATION を実現することができる。 |
| A.DADMIN_TRUST | A.DADMIN_TRUST の前提条件は、TOE の機器管理者が、機器管理者として機器を適切に管理する能力を有し、悪意のある目的のために、機器管理者としての権限を悪用しない信頼性が必要である。<br>OE.DADMIN_TRUST の対策により、機器管理者は、信頼のできる人物を選出し、所属する組織のセキュリティ方針や運用ルールを遵守するよう、また製品ガイダンスの記載に従って適切な操作ができるように、十分な指導を受けることで、A.DADMIN_TRUST を実現することができる。 |

| | |
|---|---|
| T.SETTING_DATA | T.SETTING_DATA に対抗するためには、操作パネルおよびクライアント PC から TOE 設定データに不正にアクセスして、設定値を変更させない、もしくは、漏洩させないようにする必要がある。<br>この脅威に対して、O.SETTING_DATA の対策方針により、対抗することができる。すなわち、O.SETTING_DATA により、操作パネルおよびクライアント PC からの TOE 設定データへのアクセスを認証された正当な利用者のみに許可し、許可されない者からの設定データへのアクセスを不可能にし、TOE 設定データの設定変更、および漏洩を不可能にすることができるので、TOE 設定データに対し不正にアクセスして、設定値を変更させたり、漏洩させたりすることから防止することができる。 |
| T.IMAGE_DATA | T.IMAGE_DATA に対抗するためには、操作パネルおよびクライアント PC からアクセス権限のないボックス文書データへ不正にアクセスし、ボックス文書データを漏洩もしくは改ざんさせないようにする必要がある。<br>この脅威に対し、O.ACCESS_CONTROL の対策方針により、対抗することができる。すなわち、O.ACCESS_CONTROL により、操作パネルおよびクライアント PC からアクセスする利用者を識別認証し、正当な利用者のみに、ボックス文書データへのアクセスが可能となるように制御するので、ボックス文書データへ不正にアクセスしたり、ボックス文書データを漏洩もしくは改ざんさせたりすることから防止することができる。 |
| T.NETWORK | T.NETWORK に対抗するためには、内部ネットワーク上の文書データおよび TOE 設定データに対して不正に盗聴もしくは改ざんされないようにする必要がある。<br>この脅威に対し、O.NETWORK_ENCRYPTION の対策方針により、対抗することができる。すなわち、<br>O.NETWORK_ENCRYPTION により、ネットワーク保護に必要な暗号化通信機能を使用することで、内部ネットワーク上の文書データおよび TOE 設定データを盗聴や改ざんから防止することができる。 |

| | |
|---|---|
| P.SSD_ENCRYPTION | P.SSD_ENCRYPTION の組織のセキュリティ方針は、SSD 上に保存される文書データおよび TOE 設定データを暗号化することを想定している。<br>O.SSD_ENCRYPTION により、SSD に保存されている文書データおよび TOE 設定データを暗号化することができるので、このセキュリティ方針を達成することができる。 |
| P.FAX_CONTROL | P.FAX_CONTROL の組織のセキュリティ方針は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないことを想定している。<br>O.FAX_CONTROL により、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する FAX データフロー制御を提供することができるので、このセキュリティ方針を達成することができる。 |

# 5. 拡張コンポーネント定義

拡張コンポーネントは定義しない。

# 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 FCS:暗号サポート

| | FCS_CKM.1 | 暗号鍵生成 |
|---|---|---|

下位階層: なし
依存性: [FCS_CKM.2 暗号鍵配付、または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

**FCS_CKM.1.1** TSF は、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付: 標準のリスト]
- *FIPS PUB 180-4*

[割付: 暗号鍵生成アルゴリズム]
- *FIPS PUB 180-4 に基づく暗号鍵生成アルゴリズム*

[割付: 暗号鍵長]
- *256 ビット*

| | FCS_COP.1 | 暗号操作 |
|---|---|---|

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、
またはFCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト]
- *FIPS PUB 197*

[割付: 暗号アルゴリズム]
- *AES*

[割付: 暗号鍵長]
- *256 ビット*

[割付: 暗号操作のリスト]
- *SSD へ書き込む文書データの暗号化*
- *SSD へ書き込むボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）の暗号化*
- *SSD から読み出した文書データの復号*
- *SSD から読み出したボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）の復号*

### 6.1.2. クラス FDP:利用者データ保護

**FDP_ACC.1 サブセットアクセス制御**

下位階層: なし
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 TSFは、[割付: サブジェクト、オブジェクト、及び*SFP*で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御*SFP*]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及び*SFP*で扱われるサブジェクトとオブジェクト間の操作のリスト]
- *表 6.1 に示すサブジェクト、オブジェクト、及びサブジェクトとオブジェクト間の操作のリスト*

[割付: アクセス制御 *SFP*]
- *ボックス文書データアクセス制御 SFP*

**表 6.1 サブジェクト、オブジェクト、及びサブジェクトとオブジェクト間の操作のリスト**

| サブジェクト | オブジェクト | 操作 |
|---|---|---|
| 利用者を代行するタスク | ボックス文書データ | ボックス文書データの読み出し、削除 |

**FDP_ACF.1　　セキュリティ属性によるアクセス制御**

下位階層:　　なし
依存性:　　FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

**FDP_ ACF.1.1**　TSF は、以下の[割付: 示された*SFP* 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、*SFP* 関連セキュリティ属性、または*SFP* 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 *SFP*]を実施しなければならない。

[割付: 示された*SFP* 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、*SFP* 関連セキュリティ属性、または*SFP* 関連セキュリティ属性の名前付けされたグループ]

- *表 6.2 に示すボックス文書データアクセス制御 SFP のリスト*

[割付: アクセス制御 *SFP*]

- *ボックス文書データアクセス制御 SFP*

**FDP_ ACF.1.2**　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

- *表 6.2 に示すログインユーザー名に基づくボックス文書データアクセス制御 SFP のアクセス制御規則*

表 6.2 ログインユーザー名に基づくボックス文書データアクセス制御 SFP

| オブジェクト<br>（セキュリティ属性） | 操作 | サブジェクト<br>（セキュリティ属性） | アクセス制御規則 |
|---|---|---|---|
| ボックス文書データ<br>（ボックスの所有者、<br>ボックスの共有設定） | 読み出し、<br>削除 | 利用者を代行するタスク<br>（ログインユーザー名） | (1)「ログインユーザー名」と、ボックス文書データが格納された「ボックスの所有者」が一致する場合に、操作を許可する。<br>(2) ボックス文書データが格納された「ボックスの共有設定」が有効である場合に、一般利用者に操作を許可する。 |

FDP_ ACF.1.3 TSF は、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]

- *表 6.3 に示すユーザー権限に基づくボックス文書データアクセス制御 SFP のアクセス制御規則*

表 6.3 ユーザー権限に基づくボックス文書データアクセス制御 SFP

| オブジェクト<br>（セキュリティ属性） | 操作 | サブジェクト<br>（セキュリティ属性） | アクセス制御規則 |
|---|---|---|---|
| ボックス文書データ<br>（ボックスの所有者、<br>ボックスの共有設定） | 読み出し、<br>削除 | 利用者を代行するタスク<br>（ユーザー権限） | 機器管理者のユーザー権限の場合、「ボックスの所有者」、「ボックスの共有設定」の値に関わらず、操作を許可する |

FDP_ ACF.1.4 TSF は、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

- *なし*

**FDP_ IFC.1　　サブセット情報フロー制御**

下位階層：　　なし
依存性：　　FDP_IFF.1　単純セキュリティ属性

FDP_IFC.1.1　TSF は、[割付: *SFP* によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト]に対して[割付:情報フロー制御*SFP*]を実施しなければならない。

[割付: *SFP* によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト

- *表6.4で示すサブジェクト、情報、および操作のリスト*

**表 6.4 サブジェクト、情報、および、情報の流れを引き起こす操作のリスト**

| サブジェクト（セキュリティ属性） | 情報（セキュリティ属性） | 操作 | 情報制御フロー規制 |
|---|---|---|---|
| 公衆回線からの受信タスク（FAX 転送設定- FAX ボックス：F コード値に対応する FAX ボックス） | 公衆回線から受信したデータ（F コード指定） | 転送 | 公衆回線からの受信タスク（サブジェクト）が受信した公衆回線から受信したデータ（情報）を、FAX 転送設定（セキュリティ属性）に従い転送する（操作）。 |

[割付:情報フロー制御 *SFP*]

- *FAX情報フロー制御SFP*

**FDP_IFF.1　　単純セキュリティ属性**

下位階層：　　なし
依存性：　　FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

FDP_IFF.1.1　TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付: 情報フロー制御*SFP*]を実施しなければならない。: [割付: 示された*SFP* 下において制御さ

れるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性]

[割付: 情報フロー制御 *SFP*]
- *FAX情報フロー制御SFP*

[割付: 示された*SFP* 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性]
- *表6.4 に示すサブジェクトと情報、及び各々に対応するセキュリティ属性*

FDP_IFF.1.2 TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: 各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]。

[割付: 各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]

- *表6.4 で示すサブジェクトと情報間で操作を制御する情報フロー制御規則として、情報のFコード指定があるときには、サブジェクトのFAX転送設定でのFコード転送先と一致する場合にFAXボックスに保存される。Fコード転送先と一致しない場合、および情報のFコード指定が無い場合は、印刷部からの出力を許可する。*

FDP_IFF.1.3 TSF は、[割付: 追加の情報フロー制御 *SFP* 規則]を実施しなければならない。

[割付: 追加の情報フロー制御 *SFP* 規則]
- *なし*

FDP_IFF.1.4 TSF は、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に許可する規則]に基づいて、情報フローを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいて情報フローを明示的に許可する規則]
- *なし*

FDP_IFF.1.5 TSF は、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に拒否する規則]に基づいて、情報フローを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいて情報フローを明示的に拒否する規則]
- *なし*

6.1.3. クラス FIA:識別と認証

**FIA_AFL.1　　認証失敗時の取り扱い**

下位階層:　　なし
依存性:　　FIA_UAU.1 認証のタイミング

FIA_AFL.1.1　TSF は、[割付: 認証事象のリスト]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]*内における管理者設定可能な正の整数値]回の不成功認証試行が生じたときを検出しなければならない。

[割付: 認証事象のリスト]
- *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*

[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]* 内における管理者設定可能な正の整数値]
- *〔割付：許可可能な値の範囲〕内における管理者設定可能な正の整数値*

〔割付：許可可能な値の範囲〕
- *1 から 10*

FIA_AFL.1.2　不成功の認証試行が定義した回数[選択：に達する、を上回った]とき、TSF は、[割付: アクションのリスト]をしなければならない。

[選択：に達する、を上回った]
- *に達する*

[割付: アクションのリスト]
- *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　　利用者属性定義**

下位階層:　　なし
依存性:　　なし

FIA_ATD.1.1　TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付: セキュリティ属性のリスト]

[割付: セキュリティ属性のリスト]
- *ログインユーザー名、ユーザー権限*

**FIA_SOS.1　　秘密の検証**

下位階層:　　なし
依存性:　　なし

FIA_SOS.1.1　TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付: 定義された品質尺度]
- *パスワード長： 8 文字以上*
- *文字種別： 英数字記号*

**FIA_UAU.1　　認証のタイミング**

下位階層:　　なし
依存性:　　FIA_UID.1 識別のタイミング

FIA_UAU.1.1　TSF は、利用者が認証される前に利用者を代行して行われる[割付: *TSF* 仲介アクションのリスト]を許可しなければならない。

[割付: *TSF* 仲介アクションのリスト]
- *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 TSF は、その利用者を代行する他のすべてのTSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

### FIA_UAU.7 保護された認証フィードバック

下位階層: なし
依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.7.1 TSF は、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。

[割付: フィードバックのリスト]
- *ダミー文字（*：アスタリスク）*

### FIA_UID.1 識別のタイミング

下位階層: なし
依存性: なし

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付: *TSF* 仲介アクションのリスト]を許可しなければならない。

[割付: *TSF* 仲介アクションのリスト]
- *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 TSF は、その利用者を代行する他のTSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

**FIA_USB.1　利用者-サブジェクト結合**

下位階層:　なし
依存性:　FIA_ATD.1 利用者属性定義

FIA_USB.1.1　TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]
- *ログインユーザー名、ユーザー権限*

FIA_USB.1.2　TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の最初の関連付けの規則]

[割付: 属性の最初の関連付けの規則]
- *なし*

FIA_USB.1.3　TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の変更の規則]

[割付: 属性の変更の規則]
- *なし*

### 6.1.4. クラス FMT:セキュリティ管理

**FMT_MSA.1(a)　セキュリティ属性の管理**

下位階層:　なし
依存性:　[FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1(a)　TSF は、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、*[割付：その他の操作]*]をする能力を[割付: 許可された識別された役割]に制限する[割付: アクセス制御*SFP*、情報フロー制御*SFP*]を実施しなければ

ならない。

[割付: セキュリティ属性のリスト]
- *表 6.5 で示すセキュリティ属性*

[選択: デフォルト値変更、問い合わせ、改変、削除、*[割付：その他の操作]*]
- *〔割付：その他の操作〕*

[割付: その他の操作]
- *表 6.5 で示す操作*

[割付: 許可された識別された役割]
- *表 6.5 で示す役割*

[割付: アクセス制御 *SFP*、情報フロー制御 *SFP*]
- *ボックス文書データアクセス制御 SFP*

**表 6.5 セキュリティ属性の管理(ボックス文書データアクセス制御)**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| ボックスの所有者 | 改変 | 機器管理者 |
| ボックスの共有設定 | 改変 | 機器管理者 |
| | | ボックスの所有者と一致する一般利用者 |

**FMT_MSA.1(b)　セキュリティ属性の管理**

下位階層:　なし
依存性:　[FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

**FMT_MSA.1.1(b)** TSF は、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、*[割付：その他の操作]*]をする能力を[割付: 許可された識別された役割]に制限する[割付: アクセス制御*SFP*、情報フロー制御*SFP*]を実施しなければならない。

[割付: セキュリティ属性のリスト]

- *表 6.6 で示すセキュリティ属性*

[選択: デフォルト値変更、問い合わせ、改変、削除、*[割付：その他の操作]*]

- *〔割付：その他の操作〕*

[割付: その他の操作]

- *表 6.6 で示す操作*

[割付: 許可された識別された役割]

- *表 6.6 で示す役割*

[割付: アクセス制御 *SFP*、情報フロー制御 *SFP*]

- *FAX データフロー制御 SFP*

**表 6.6 セキュリティ属性の管理(FAX データフロー制御)**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| FAX 転送設定<br>（FAX ボックス:F コード値に対応する FAX ボックス） | 改変 | 機器管理者 |

## FMT_MSA.3(a)　静的属性初期化

下位階層:　なし
依存性:　FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

**FMT_MSA.3.1(a)** TSF は、そのSFP を実施するために使われるセキュリティ属性に対して[選択: 制限的、許可的、*[割付：その他の特性]*: から1 つのみ選択]デフォルト値を与える[割付: アクセス制御*SFP*、情報フロー制御*SFP*]を実施しなければならない。

[選択: 制限的、許可的、*[割付：その他の特性]*: から1 つのみ選択]

- *制限的*

[割付: アクセス制御*SFP*、情報フロー制御*SFP*]

- *ボックス文書データアクセス制御 SFP*

FMT_MSA.3.2(a) TSF は、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]
- *なし*

### FMT_MSA.3(b) 静的属性初期化

下位階層: なし
依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1(b) TSF は、そのSFP を実施するために使われるセキュリティ属性に対して[選択: 制限的、許可的、*[割付：その他の特性]*: から1 つのみ選択]デフォルト値を与える[割付: アクセス制御*SFP*、情報フロー制御*SFP*]を実施しなければならない。

[選択: 制限的、許可的、*[割付：その他の特性]*: から1 つのみ選択]
- *許可的*

[割付: アクセス制御*SFP*、情報フロー制御*SFP*]
- *FAX データフロー制御 SFP*

FMT_MSA.3.2(b) TSF は、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]
- *なし*

### FMT_MTD.1(a) TSF データの管理

下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(a) TSF は、[割付: *TSF* データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、*[*割付*:* その他の操作*]*]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: *TSF* データのリスト]

- *表 6.7 で示された TSF データ*

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、*[*割付*:* その他の操作*]*]

- *〔割付：その他の操作〕*

[割付: その他の操作]

- *表 6.7 で示された 操作*

[割付: 許可された識別された役割]

- *表 6.7 で示された 役割*

**表 6.7 TSF データの操作**

| TSF データ | 役割 | 操作 |
|---|---|---|
| ログインユーザー名 | 機器管理者 | 改変、削除、〔割付：その他の操作〕<br>〔割付：その他の操作〕<br>・*作成* |
| ログインユーザーパスワード | 機器管理者 | 改変、削除、〔割付：その他の操作〕<br>〔割付：その他の操作〕<br>・*作成* |
| ユーザー権限 | 機器管理者 | 改変、削除、〔割付：その他の操作〕<br>〔割付：その他の操作〕<br>・*作成* |
| 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） | 機器管理者 | 改変 |
| 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） | 機器管理者 | 改変 |
| ロックアウトリスト | 機器管理者 | 改変 |
| 自動ログアウト時間設定 | 機器管理者 | 改変 |
| パスワードポリシー設定 | 機器管理者 | 改変 |
| ネットワーク暗号設定（TLS、IPsec 設定） | 機器管理者 | 改変 |

**FMT_MTD.1(b)　TSF データの管理**

下位階層:　なし
依存性:　FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(b)　TSF は、[割付: *TSF* データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、*[*割付：その他の操作*]*]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: *TSF* データのリスト]
- *表 6.8 で示された TSF データ*

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、*[*割付：その他の操作*]*]
- *〔割付：その他の操作〕*

[割付: その他の操作]
- *表 6.8 で示された 操作*

[割付: 許可された識別された役割]
- *表 6.8 で示された 役割*

**表 6.8 TSF データの操作**

| TSF データ | 役割 | 操作 |
|---|---|---|
| 一般利用者に関連付いたログインユーザーパスワード | 一般利用者 | 改変 |

**FMT_SMF.1　管理機能の特定**

下位階層:　なし
依存性:　なし

FMT_SMF.1.1　TSF は、以下の管理機能を実行することができなければならない。 :[割付: *TSF* によって提供される管理機能のリスト]

[割付: *TSF* によって提供される管理機能のリスト]

- *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）、FAX データフロー制御機能におけるセキュリティ属性（FAX 転送設定）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、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、ネットワーク暗号設定（TLS、IPsec 設定））を管理する機能*

**表 6.9 管理機能**

| 機能要件 | 管理機能 | CC で定義されている管理項目 |
|---|---|---|
| FCS_CKM.1 | - | 予見される管理アクティビティはない。 |
| FCS_COP.1 | - | 予見される管理アクティビティはない。 |
| FDP_ACC.1 | - | 予見される管理アクティビティはない。 |
| FDP_ACF.1 | なし<br>（明示的なアクセスまたは拒否に基づく決定に使用される属性値は機器管理者固定であるため、管理する必要はない） | a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。 |
| FDP_IFC.1 | - | なし |
| FDP_IFF.1 | なし<br>（明示的なアクセスに基づく決定に使われる属性は無いので管理する必要はない） | a) 明示的なアクセスに基づく決定に使われる属性の管理 |
| FIA_AFL.1 | 認証失敗回数の管理 | a) 不成功の認証試行に対する閾値の管理；<br>b) 認証失敗の事象においてとられるアクション管理。 |
| FIA_ATD.1 | なし<br>（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) もし割付にしめされていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。 |
| 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) 秘密の検証に使用される尺度の管理。 |
| FIA_UAU.1 | 機器管理者によるログインユーザーパスワードの管理<br>一般利用者による自身のログインユーザーパスワードの管理 | a) 管理者による認証データの管理;<br>b) 関係する利用者による認証データの管理;<br>c) 利用者が認証される前にとられるアクションのリストを管理すること。 |

| 機能要件 | 管理機能 | CC で定義されている管理項目 |
|---|---|---|
| FIA_UAU.7 | - | 予見さえる管理アクティビティはない。 |
| FIA_UID.1 | 利用者識別の管理 | 利用者識別情報の管理 |
| FIA_USB.1 | なし<br>（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) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。<br>b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる。 |
| FMT_MSA.1(a) | なし<br>（役割のグループは 機器管理者 固定であるため、管理する必要はない） | a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること；<br>b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。 |
| FMT_MSA.3(a) | なし<br>（役割のグループは 機器管理者 固定であるため、管理する必要はない） | a) 初期値を特定し得る役割のグループを管理すること；<br>b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること；<br>c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。 |
| FMT_MSA.1(b) | なし<br>（役割のグループは 機器管理者 固定であるため、管理する必要はない） | a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること；<br>b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。 |
| FMT_MSA.3(b) | なし<br>（役割のグループは 機器管理者 固定であるため、管理する必要はない） | a) 初期値を特定し得る役割のグループを管理すること；<br>b) 所定のアクセス制御SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること；<br>c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。 |
| FMT_MTD.1(a) | なし<br>（役割のグループは機器管理者固定であるため、管理する必要はない） | a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。 |
| FMT_MTD.1(b) | なし<br>（役割のグループはは機器管理者固定であるため、管理する必要はない） | a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。 |
| FMT_SMF.1 | - | 予見される管理アクティビティはない。 |

| 機能要件 | 管理機能 | CC で定義されている管理項目 |
|---|---|---|
| FMT_SMR.1 | 利用者のユーザー権限のグループの管理 | a) 役割の一部をなす利用者のグループの管理。 |
| FTA_SSL.3 | 自動ログアウト時間の管理 | a) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定；<br>b) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。 |
| FTP_ITC.1 | 内部ネットワークデータ保護の管理<br>（ネットワーク暗号（TLS、IPsec 設定）） | a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。 |

**FMT_SMR.1　　セキュリティの役割**

下位階層:　　なし
依存性:　　FIA_UID.1 識別のタイミング

**FMT_SMR.1.1**　TSF は、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]
- *機器管理者*
- *一般利用者*

**FMT_SMR.1.2**　TSF は、利用者を役割に関連付けなければならない。

6.1.5. クラス FTA:TOE アクセス

**FTA_SSL.3　　TSF 起動による終了**

下位階層:　　なし
依存性:　　なし

FTA_SSL.3.1 TSF は、[割付: 利用者が非アクティブである時間間隔]後に対話セションを終了しなければならない。

[割付: 利用者が非アクティブである時間間隔]

- *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

### 6.1.6. クラス FTP:高信頼パス/チャネル

**FTP_ITC.1 TSF 間高信頼チャネル**

下位階層: なし
依存性: なし

FTP_ITC.1.1 TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSFは、[選択: *TSF*、他の高信頼*IT*製品]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択: *TSF*、他の高信頼 *IT* 製品]

- *TSF*
- *他の高信頼 IT 製品*

FTP_ITC.1.3 TSF は、[割付: 高信頼チャネルが要求される機能のリスト]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付: 高信頼チャネルが要求される機能のリスト]

- *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）からの機能*

*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。*

## 6.2. TOE セキュリティ保証要件

表 6.10 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 EAL2 である。

**表 6.10 セキュリティ保証要件**

| 保証クラス | 保証コンポーネント |
|---|---|
| ADV: 開発 | ADV_ARC.1 セキュリティアーキテクチャ記述 |
| | ADV_FSP.2 セキュリティ実施機能仕様 |
| | ADV_TDS.1 基本設計 |
| AGD: ガイダンス文書 | AGD_OPE.1 利用者操作ガイダンス |
| | AGD_PRE.1 準備手続き |
| ALC: ライフサイクルサポート | ALC_CMC.2 CM システムの使用 |
| | ALC_CMS.2 TOE の一部の CM 範囲 |
| | ALC_DEL.1 配付手続き |
| ASE: セキュリティターゲット評価 | ASE_CCL.1 適合主張 |
| | ASE_ECD.1 拡張コンポーネント定義 |
| | ASE_INT.1 ST 概説 |
| | ASE_OBJ.2 セキュリティ対策方針 |
| | ASE_REQ.2 派生したセキュリティ要件 |
| | ASE_SPD.1 セキュリティ課題定義 |
| | ASE_TSS.1 TOE 要約仕様 |
| ATE: テスト | ATE_COV.1 カバレージの証拠 |
| | ATE_FUN.1 機能テスト |
| | ATE_IND.2 独立テスト - サンプル |
| AVA: 脆弱性評定 | AVA_VAN.2 脆弱性分析 |

## 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と TOE セキュリティ機能要件の対応を表 6.11 で示す。

表 6.11 セキュリティ対策方針とセキュリティ機能要件の対応

| セキュリティ機能要件 | セキュリティ対策方針 | | | | |
|---|---|---|---|---|---|
| | O.SSD_ENCRYPTION | O.NETWORK_ENCRYPTION | O.FAX_CONTROL | O.SETTING_DATA | O.ACCESS_CONTROL |
| FCS_CKM.1 | ● | | | | |
| FCS_COP.1 | ● | | | | |
| FDP_ACC.1 | | | | | ● |
| FDP_ACF.1 | | | | | ● |
| FDP_IFC.1 | | | ● | | |
| FDP_IFF.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 | | | ● | ● | ● |
| FTA_SSL.3 | | | | ● | ● |
| FTP_ITC.1 | | ● | | | |

以下に、『表 6.10 セキュリティ対策方針とセキュリティ機能要件の対応』の根拠を示す。

O.SSD_ENCRYPTION

O.SSD.ENCRYPTION は、SSD に保存する文書データと TOE 設定データ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、SSD に保存する文書データと TOE 設定データを暗号化し、読み出す文書データと TOE 設定データを復号する。
従って、O.SSD_ENCRYPTION は、SSD に保存する文書データと TOE 設定データを暗号化することを保証することができる。

O.NETWORK_ENCRYPTION

O.NETWORK ENCRYPTION は、内部ネットワーク上の文書データおよび TOE 設定データを盗聴や改ざんから保護するために、ネットワーク保護に必要な暗号化通信機能を提供する対策方針がある。
FTP_ITC.1 により、TOE が内部ネットワーク上で文書データおよび TOE 設定データを盗聴や改ざんから保護するために、通信暗号化をすることで、高信頼チャネルを提供することができる。
従って、O.NETWORK_ENCRYPTION は、内部ネットワーク上の文書データおよび TOE 設定データを盗聴や改ざんから保護するために、ネットワーク保護に必要な暗号化通信機能を提供することを保証することができる。

O.FAX_CONTROL

O.FAX_CONTROL は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する FAX データフロー制御機能を提供する対策方針である。
FDP_IFC.1、FDP_IFF.1 により、TOE の FAX 情報フロー制御機能を使用することで、公衆回線から受信したデータは許可された役割が設定した FAX 転送設定に従って転送処理が行われる。ここで、公衆回線から受信したデータに F コードが指定されている際に F コード値に対応する FAX ボックスに保存される場合があるが、この処理は TOE が接続された内部ネットワークへの転送ではないため、対策方針を満足している。また、F コード値が一致しない場合、および受信したデータに F コードが指定されていない場合は印刷部から出力されるが、この場合も TOE が接続された内部ネットワークへの転送ではないため、対策方針を満足している。
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、FAX 転送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、機器管理者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機器管理者へ提供する。
従って、O.FAX_CONTROL は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する FAX データフロー制御機能を提供することを保証することができる。

O.ACCESS_CONTROL

O.ACCESS_CONTROL は、利用者を識別認証し、正当な利用者のみに、ボックス文書データへのアクセスが可能となるように、ボックス文書データへのアクセスを制御する機能を提供する対策方針である。
FIA_UID.1、FIA_UAU.1 により、操作パネルおよびクライアント PC から TOE にアクセスしようとする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_ATD.1、FIA_USB.1 により、ログインユーザー名、ユーザー権限のセキュリティ属性を維持し、許可された利用者にサブジェクトのセキュリティ属性を関連づける。
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。
FDP_ACC.1、FDP_ACF.1 により、許可された利用者のみにボックス文書データ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、ボックス文書データが生成された際に、ボックス文書データ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、機器管理者と 一般利用者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機器管理者とボックス文書データの所有者である 一般利用者へ提供する。
従って、O.ACCESS_CONTROL は、ボックス文書データへのアクセスを制御することを保証することができる。

O.SETTING_DATA
O.SETTING_DATA は、TOE 設定データへのアクセスを認証された正当な利用者のみに許可し、許可されない者からの TOE 設定データへのアクセスを不可能にし、TOE 設定データの設定変更、および漏洩を不可能にする対策方針である。
FIA_UID.1、FIA_UAU.1 により、操作パネルおよびクライアント PC から TOE にアクセスしようとする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。
FMT_MTD.1(a)により、TOE 設定データへの操作は、機器管理者に制限される。
FMT_MTD.1(b)により、一般利用者の TOE 設定データへの操作は、TOE 設定データの所有者である一般利用者に制限される。
FMT_SMR.1 により、機器管理者 と 一般利用者の利用者権限が維持され、機器管理者と 一般利用者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機器管理者と TOE 設定データの所有者である 一般利用者へ提供する。
従って、O.SETTING_DATA は、許可されない者からの TOE 設定データへのアクセスを不可能にし、TOE 設定データの設定変更、および漏洩を不可能にすることを保証することができる。

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 6.12 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 |
|---|---|---|
| FCS_CKM.1 | FCS_COP.1<br>FCS_CKM.4 | FCS_CKM.4<br>6.3.2.1 節参照 |
| FCS_COP.1 | FCS_CKM.1<br>FCS_CKM.4 | FCS_CKM.4<br>6.3.2.1 節参照 |
| FDP_ACC.1 | FDP_ACF.1 | － |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | － |
| FDP_IFC.1 | FDP_IFF.1 | － |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | － |
| FIA_AFL.1 | FIA_UAU.1 | － |
| FIA_ATD.1 | なし | － |
| FIA_SOS.1 | なし | － |
| FIA_UAU.1 | FIA_UID.1 | － |
| FIA_UAU.7 | FIA_UAU.1 | － |
| FIA_UID.1 | なし | － |
| FIA_USB.1 | FIA_ATD.1 | － |
| FMT_MSA.1(a) | FDP_ACC.1<br>FMT_SMF.1<br>FMT_SMR.1 | － |
| FMT_MSA.3(a) | FMT_MSA.1<br>FMT_SMR.1 | － |
| FMT_MSA.1(b) | FDP_ACC.1<br>FMT_SMF.1<br>FMT_SMR.1 | － |
| FMT_MSA.3(b) | FMT_MSA.1<br>FMT_SMR.1 | － |
| FMT_MTD.1(a) | FMT_SMF.1<br>FMT_SMR.1 | － |
| FMT_MTD.1(b) | FMT_SMF.1<br>FMT_SMR.1 | － |
| FMT_SMF.1 | なし | － |
| FMT_SMR.1 | FIA_UID.1 | － |

| | | |
|---|---|---|
| FTA_SSL.3 | なし | － |
| FTP_ITC.1 | なし | |

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.ACCESS 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

本 TOE は、基本的な攻撃能力を持つ攻撃者による文書データの露顕の脅威に対抗することを目的としているため、基本レベルの攻撃への対抗性の保証が必要となる。

EAL2 は TOE における開発段階のセキュリティ対策の分析（機能仕様に基づくテストの実施と分析、及び成果物の管理状況と配付手続きの評価）を含む、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれる。保証要件は、EAL2 適合であるため、EAL2 の選択は妥当である。

# 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.FAXDATAFLOW | TSF.SSD_ENCRYPTION | TSF.SECURITY_MANAGEMENT | TSF.NETWORK_PROTECTION |
|---|---|---|---|---|---|---|
| FCS_CKM.1 | | | | ● | | |
| FCS_COP.1 | | | | ● | | |
| FDP_ACC.1 | | ● | | | | |
| FDP_ACF.1 | | ● | | | | |
| FDP_IFC.1 | | | ● | | | |
| FDP_IFF.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 | | | | | ● | |
| 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（*：アスタリスク）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
  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 の基本機能であるボックス機能を用いて TOE 内に保存されている文書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　サブセットアクセス制御
FDP_ACF.1　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、ボックス機能が扱う文書データに対し、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。

**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 |
|---|---|---|---|
| ボックス文書データ（ボックス機能） | 文書の読み出し、文書の移動、文書の削除 | 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文書データへのアクセスを許可する |
| | | 機器管理者 | 全ての文書データへのアクセスを許可する |

(2) FMT_MSA.3(a)　静的属性初期化

TOE は、新規に作成されるボックスのデフォルト値を設定する。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. FAX データフロー制御機能

**TSF.FAXDATA_FLOW**

FAX データフロー制御機能は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する機能である。

(1) FDP_IFC.1　サブセット情報フロー制御

FDP_IFF.1　単純セキュリティ属性

TOE は、公衆回線から受信したデータを TOE が接続された内部ネットワークへ転送しないように制御する情報フロー制御を実施する。受信したデータに F コードが指定されているときには、FAX 転送設定での F コード転送先と一致する場合に FAX ボックスに保存され、F コード転送先と一致しない場合、および受信したデータに F コードが指定されていない場合は印刷部からの出力を許可する。これにより、公衆回線からの受信タスクは、公衆回線から受信したデータ（情報）を TOE が接続された内部ネットワークへ転送されないように制御することができる。

(2) FMT_MSA.3(b) 静的属性初期化

TOE は、新規に作成される FAX 転送設定のデフォルト値を設定する。新規に作成される FAX 転送設定のデフォルト値は、印刷部から出力する転送設定なしとして作成される。

## 7.4. SSD 暗号化機能

**TSF.SSD_ENCRYPTION**

TOE は、基本機能を実行すると、文書データや一部の TOE 設定データを SSD に保存する。SSD 暗号化機能は、SSD へ書き込む文書データ、ボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）を暗号化して保存し、これらのデータを読み出す際に復号する機能である。

(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、SSD に文書データ、ボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）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、SSD に書込む。ま

た、SSD に保存された文書データ、ボックス機能に関する情報（ボックスの所有者、ボックスの共有設定）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. 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変更
- ボックスの共有設定の変更

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 は、FAX データフロー制御機能における、FAX 転送設定に対する以下の操作を、機器管理者のみに許可する。

- FAX 転送設定の変更

(3) FMT_MTD.1(a) TSF データ管理

TOE は表 7.3 に示す TSF データに対する、表 7.3 で示される操作を機器管理者のみに提供する。

表 7.3 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<br>（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） | 変更、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<br>(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 |
| ネットワーク暗号設定（TLS、IPsec 設定） | 変更 |

(4) FMT_MTD.1(b)　TSF データ管理

TOE は、表 7.4 に示す TSF データに対する、表 7.4 で示される操作を一般利用者に提供する。

表 7.4 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<br>（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 7.3、表 7.4 に示した TSF データに対する表 7.3、表 7.4 で示した操作を行うセキュリティ管理機能を提供する。

## 7.6. 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 が接続された内部ネットワーク上を流れるデータを暗号化し、改変、暴露から保護する機能である。TOE のスキャン送信による機能、プリンタードライバーによる機能、Web ブラウザーによる機能を利用する際に、接続先の正当性を検証し、内部ネットワーク上を流れるデータを暗号化することで保護する。

(1) FTP_ITC.1　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
- FAX 機能における受信したデータを TOE が接続された内部ネットワークへ転送する機能
- 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 7.5** 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) |

# 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、SSD 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。 |
| HD-7 | SSD ストレージオプション。キャッシュ付 SSD 採用により、HDD より高速で安定した性能を実現する。 |
| 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。) |
| F コード | F コードとは、ITU-T で標準化された通信規格の 1 つである。F コード機能を持つ機種間の通信では、他社機の場合も F コードを使用したさまざまな機能を使用することが出来る。<br>F コードは、0～9 の数字とスペース、「#」、「*」の文字を使用して最大 20 桁まで指定することが出来る。 |
| 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。 |
| ユーザー権限 | 利用者に付与される権限。一般利用者と機器管理者の権限がある。 |
| 編集 | 利用者情報やボックス機能に関する情報など、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。 |
| 機器設定 | TOE を使用するうえでのシステム設定。これには TOE 設定データも含まれる。 |

| | |
|---|---|
| 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。 |
| 文書データ | TOE の利用者が取り扱う原稿に記載された画像情報からなるデータ。スプール文書データとボックス文書データを含む。 |
| 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。 |
| 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。<br>外部インタフェースであり、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。 |
| 利用者を代行するタスク | 利用者（一般利用者、機器管理者）に成り代わって実行するプロセス |
| 公衆回線からの受信タスク | 公衆回線から受信するプロセス |

## 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) |
| DADMIN. | Device administrator |
| AES | Advanced Encryption Standard |
| CC | Common Criteria |
| EAL | Evaluation Assurance Level |
| FAX | facsimile |
| IT | information technology |
| MFP | Multifunctional Product / peripheral / printer |

| | |
|---|---|
| NCU | Network Control Unit |
| NAND | Not AND |
| 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) |
| SAR | Security Assurance Requirement |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| ST | Security target |
| T. | threat (when used in hierarchical naming) |
| TOE | Target of Evaluation |
| TSF | TOE security functionality |
| USB | Universal Serial Bus |

（　最終ページ　）