ECOSYS M3540idn, ECOSYS M3550idn, ECOSYS M3560idn Series Data Security Kit (E), HD-7 付きモデル セキュリティターゲット 第 1.04 版

2015 年 11 月 19 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	担当部署	承認者	作成者	更新内容
2015/01/30	0.76	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	高須	初版作成
2015/03/03	0.77	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	高須	誤記修正
2015/03/09	0.78	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	高須	誤記修正
2015/03/13	0.79	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	高須	誤記修正
2015/03/18	0.80	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	高須	誤記訂正
2015/04/02	0.81	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記訂正
2015/04/08	0.82	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/04/09	0.83	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/04/14	0.84	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/04/16	0.85	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/04/20	0.86	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/04/22	0.87	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/05/14	0.88	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/05/21	0.89	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/05/26	0.90	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正
2015/06/25	0.91	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正

2015/07/30	0.92	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	ファームウェアバージョンの更新
2015/08/21	0.93	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	曽根	誤記修正
2015/11/06	1.00	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	曽根	誤記修正
2015/11/09	1.01	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	曽根	誤記修正
2015/11/10	1.02	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	曽根	誤記修正
2015/11/11	1.03	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	曽根	誤記修正
2015/11/19	1.04	ソフト開発本部 ソフトウェア3統括技術部 第32技術部　SD56 課	濱川	髙須	誤記修正

～ 目次 ～

～ 図目次 ～

～ 表目次 ～

1. ST 概説

1.1. ST 参照

ST 名称： ECOSYS M3540idn, ECOSYS M3550idn, ECOSYS M3560idn Series Data Security Kit (E), HD-7 付きモデル セキュリティターゲット

ST バージョン： 第 1.04 版

作成日： 2015/11/19

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 M3540idn, ECOSYS M3550idn, ECOSYS M3560idn Series Data Security Kit (E), HD-7 付きモデル

【注釈】

Data Security Kit (E), HD-7 付きモデルとは、
ECOSYS M3540idn, ECOSYS M3550idn, ECOSYS M3560idn に、次の追加オプションを付加した製品構成である

- セキュリティオプション (Data Security Kit (E))
- SSD オプション (HD-7)

TOE バージョン：

System	:	2NM_207K.C02.011
Panel	:	2NM_707K.C02.010
FAX	:	2NM_5100.004.001

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 M3540idn, ECOSYS M3550idn, ECOSYS M3560idn」である。このうち、ボックス機能については、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 M3540idn, ECOSYS M3550idn, ECOSYS M3560idn」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。

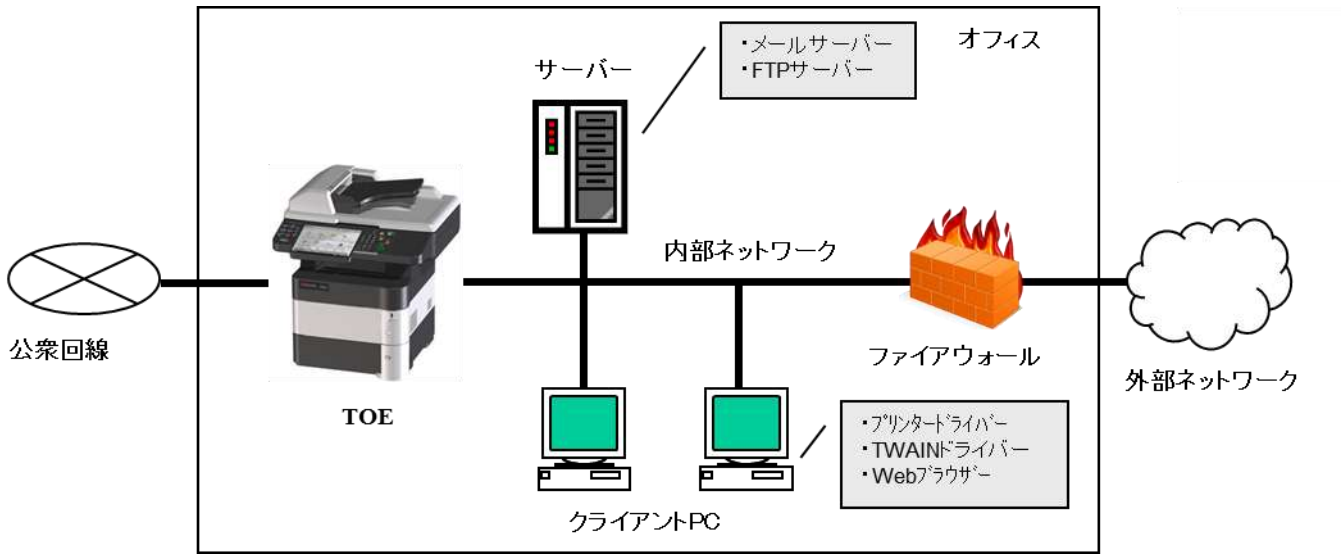

図 1.1 一般的な利用環境

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 Driver
  - TWAINドライバー：Kyocera TWAIN Driver
  - Webブラウザー：Microsoft Internet Explorer 11.0
- メールサーバー：TLS1.2が使用できること
- FTPサーバー：TLS1.2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。TOEが提供する主要なセキュリティ機能は、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、公衆回線から受信されたデータを内部ネットワークへ転送されることを禁じる機能、及びネットワークを保護する機能である。

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。
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。

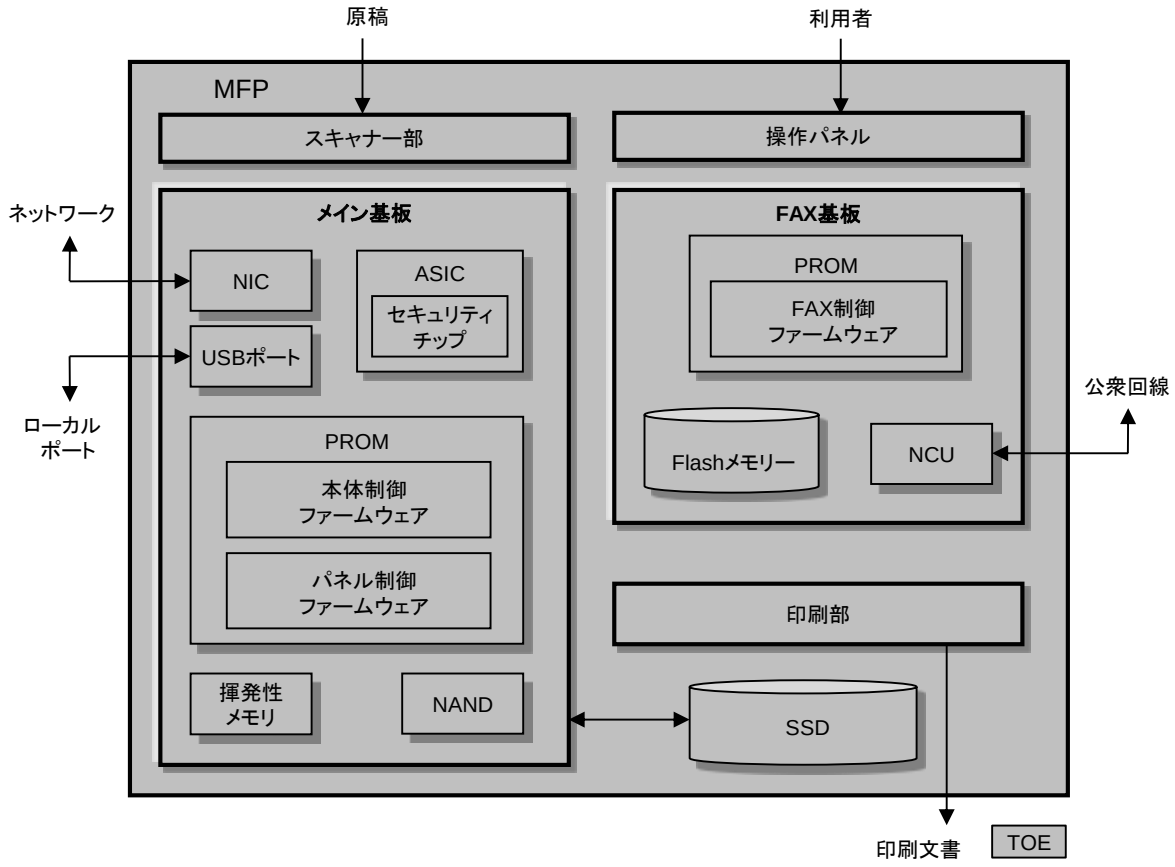

図 1.2 TOE の物理的構成図

TOE は、操作パネル、スキャナー部、印刷部、メイン基板、FAX 基板、SSD のハード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 PROM 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、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。
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 と、作業領域として使用する揮発性メモリーとファームウェア格納用の PROM、FAX 基板上に FAX 送受信した文書データを保存する 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る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、Flash メモリーには FAX 送受信した文書データのみが保存される。また、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。

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。

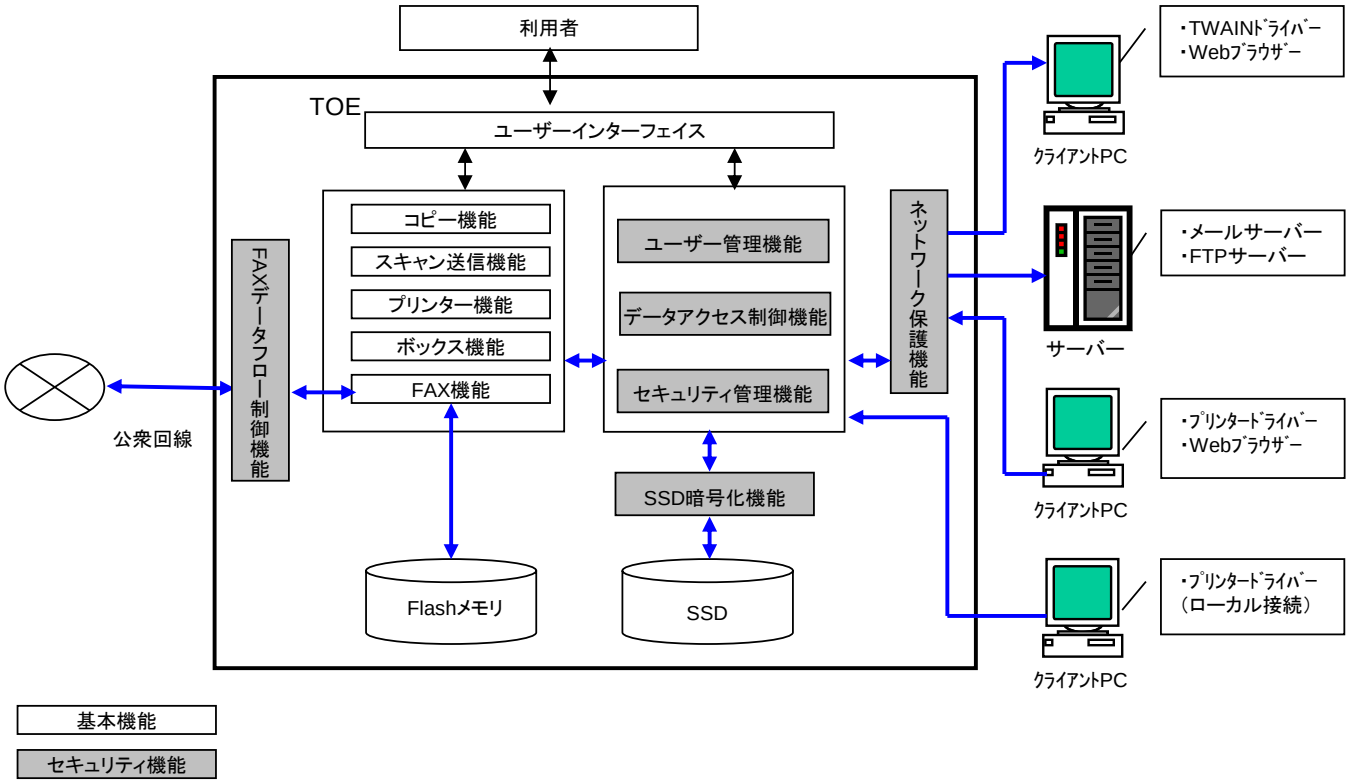

図 1.3 TOE の論理的構造図

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、また FAX 受信では外部から送られてきた文書データを受信し、TOE の印刷部から出力することが出来る。

- 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する機能。
  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 のプリンタードライバーからの印刷指示によりボックス登録する。ボックスに保存した文書データは、TOE の印刷部から出力することが出来る。また、文書データを移動することや削除することも可能である。

- 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
  公衆回線から受信されたデータを TOE が接続された内部ネットワークへ転送されることを禁じる機能。

- 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、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 1.1 TOE を構成するガイダンス

名称	バージョン
ECOSYS M3040dn/ECOSYS M3540dn/ECOSYS M3040idn/ECOSYS M3540idn/ECOSYS M3550idn/ECOSYS M3560idn Safety Guide	Rev.1 2014.10 3V2P65621101
Notice	2015.11 302P65699001
INSTALLATION GUIDE for Data Security Kit (E)	First edition 2015.1 303MS5650001
ECOSYS M3040idn/ECOSYS M3540idn/ECOSYS M3550idn/ECOSYS M3560idn FIRST STEPS QUICK GUIDE	First edition 2014.1 3V2P65601001
ECOSYS M3040idn/ECOSYS M3540idn/ECOSYS M3550idn/ECOSYS M3560idn OPERATION GUIDE	Rev.3 2015.7 2P6KDEN003
ECOSYS M3540idn/ECOSYS M3550idn/ECOSYS M3560idn FAX OPERATION GUIDE	Rev.1 2014.2 2P6KDEN501
Data Security Kit (E) OPERATION GUIDE	Rev.1 3MS2P6KDEN1 2015.11
Command Center RX USER GUIDE	Rev. 6 2015.8 CCRXKDEN06
ECOSYS M3040dn/ECOSYS M3540dn/ECOSYS M3040idn/ECOSYS M3540idn/ECOSYS M3550idn/ECOSYS M3560idn Printer Driver User Guide	Rev.16.25 2014.09
KYOCERA Net Direct Print User Guide	Rev. 3.51 2014.5

1.4.5. TOE の保護資産

TOE が保護する資産は、以下の通りである。

(1) スプール文書データ

一般利用者が TOE のコピー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 インターフェイスからの操作で印刷、移動、削除をすることが出来る。(但し、Web インターフェイスからの印刷は不可。)

(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 1.2 で示すデータ。

(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 インターフェイス経由で 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 1.2 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	ユーザー管理機能で使用する利用者の識別情報
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
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、機器管理者と一般利用者の権限が存在する。
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	ボックス機能に関する情報の 1 つとして、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	ボックス機能に関する情報の 1 つとして、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。
ネットワーク暗号設定（TLS 設定）	ネットワーク保護機能に使用する TLS 暗号化通信のための設定情報

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4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4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4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：EAL1に適合する。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STは、EAL1に適合するため、セキュリティ課題定義はない。

4. セキュリティ対策方針

本章では、運用環境のセキュリティ対策方針について記述する。

4.1. 運用環境のセキュリティ対策方針

TOE の運用環境が実施するセキュリティ対策方針を以下に示す。

OE.LOCATION ：TOE と資産の環境による保護

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 ：TOE の外部ネットワークからの防護

TOE が設置される内部ネットワークは、ファイア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.ADMIN ：機器管理者の信頼性

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。

5. 拡張コンポーネント定義

本 ST では、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 暗号鍵廃棄
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 180-2* [割付: 暗号鍵生成アルゴリズム] ● *FIPS PUB 180-2 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 へ書き込むスプール文書データの暗号化*
- *SSD へ書き込むボックス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 から読み出したスプール文書データの復号*
- *SSD から読み出したボックス文書データの復号*
- *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とオブジェクトのリストおよびオブジェクトの操作のリスト*

[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 サブジェクトとオブジェクトのリストおよびオブジェクトの操作のリスト

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（セキュリティ属性）	操作	サブジェクト（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(ボックスの所有者、ボックスの共有設定)	読み出し、削除	利用者を代行するタスク（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。 (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（セキュリティ属性）	操作	サブジェクト（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(ボックスの所有者、ボックスの共有設定)	読み出し、削除	利用者を代行するタスク（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	情報	サブジェクト	操作
公衆回線からの受信タスク	公衆回線から受信したデータ	内部ネットワークへの送信タスク	転送

〔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〕
- *公衆回線からの受信タスク（サブジェクト）、内部ネットワークへの送信タスク（サブジェクト）、公衆回線から受信したデータ（情報）のいずれも、対応するセキュリティ属性はない。*

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〕
- *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、何時も内部ネットワークへの送信タスク（サブジェクト）へ転送しない（操作）。*

FDP_IFF.1.3　TSF は、〔割付：追加の情報フロー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：許容可能な値の範囲〕
- *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（入力した文字を隠すために*の表示）

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 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 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 で示されたセキュリティ属性*

[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]]
- *表 6.5 で示された操作*

[割付: 許可された識別された役割]
- *表 6.5 で示された役割*

[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

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.3 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 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 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 6.6 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]]

- *表 6.6 で示された操作*

[割付:許可された識別された役割]

- *表 6.6 で示された 役割*

表 6.6 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] [割付：その他の操作] • *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] [割付：その他の操作] • *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] [割付：その他の操作] • *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 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 6.7 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]]

- *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
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）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 設定)）を管理する機能*

表 6.8　管理機能

機能要件	管理機能	CC で定義された管理対象
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 （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 （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； 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 （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）もし割付に示されていれば、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 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； b） 関係する利用者による認証データの管理； 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。
FIA_UAU.7	-	予見される管理アクティビティはない。
FIA_UID.1	機器管理者のログインユーザー名の管理； 一般利用者のログインユーザー名の管理；	a） 利用者識別情報の管理

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) 許可管理者は、デフォルトのサブジェクト属性を定義する。 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	なし （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； 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	なし （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； 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； 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 （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 （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_SMF.1	-	予見される管理アクティビティはない。
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ッ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； b) 対話セッ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 （ネットワーク暗号設定（TLS 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〕後に対話セッ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*

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*

6.2. TOE セキュリティ保証要件

表 6.9 セキュリティ保証要件を示す。
本 TOE の評価保証レベルは EAL1 である。

表 6.9 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_FSP.1 基本機能仕様
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.1 TOE のラベル付け
	ALC_CMS.1 TOE の CM 範囲
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.1 運用環境のセキュリティ対策方針
	ASE_REQ.1 主張されたセキュリティ要件
	ASE_TSS.1 TOE 要約仕様

保証クラス	保証コンポーネント
ATE: テスト	ATE_IND.1 独立テスト - 適合
AVA: 脆弱性評定	AVA_VAN.1 脆弱性調査

6.3. セキュリティ要件根拠

6.3.1. 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 6.10 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 FCS_CKM.4	FCS_CKM.4 6.3.1.1 節参照
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	FCS_CKM.4 6.3.1.1 節参照
FDP_ACC.1	FDP_ACF.1	－
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	－
FDP_IFC.1	FDP_IFF.1	－
FDP_IFF.1	FDP_IFC.1 FDP_MSA.3	FMT_MSA.3 6.3.1.2 節参照
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	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	－
FMT_MSA.3	FMT_MSA.1 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	なし	－
FMT_SMR.1	FIA_UID.1	－
FTA_SSL.3	なし	－
FTP_ITC.1	なし	－

6.3.1.1. 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。このため、暗号鍵は主電源 OFF すると消滅してしまう。また、起動中には SSD にデータを読み書きする暗号処理の目的以外にアクセスするインターフェイスはない。このため暗号鍵を破棄する要件は必要としない。

6.3.1.2. FMT_MSA.3 の依存性を必要としない根拠

FAX 情報フローは、セキュリティ属性がないため、FMT_MSA.3 の依存性を必要としない。

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_FAXDATA_FLOW	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					✓	
FMT_MSA.3		✓	✓			
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（入力した文字を隠すために*の表示）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　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、公衆回線を介して TOE が接続される内部ネットワークへデータが転送されることを TOE が制御することにより禁じる機能である。

(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、公衆回線からの受信データを内部ネットワークへ転送しないフロー制御を実施する。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）をいずれの場合も、内部ネットワークへの送信タスクに転送しない。

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 TSF データを SSD に保存する。SSD 暗号化機能は、これらのデータを SSD 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 180-2 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、SSD に書込む。また、SSD 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. 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　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変更

(2) 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 （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、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
ネットワーク暗号設定 （TLS 設定）	変更

(3) 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 （利用者に関連付いたログインユーザーパスワード）	編集

(4) 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。

(5) 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。
高信頼チャネルには TLS 暗号化通信を提供する。
対象となる機能は以下の通りである。

- 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

以下は対象となるプロトコルである。

- TLS プロトコル

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 のスキャナーから文書を読み込み、クライアント PC に文書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。
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。
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。
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含むボックス機能に関する情報。
文書の移動	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。
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。

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 180-2	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。 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。
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
内部ネットワークへの送信タスク	内部ネットワークへ送信するプロセス

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
AES	Advanced Encryption Standard
CC	Common Criteria
EAL	Evaluation Assurance Level
FAX	Facsimile
SSD	Solid State Drive
IT	Information Technology
MFP	Multifunctional Product / Peripheral / Printer
NCU	Network Control Unit
NAND	Not AND
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
USB	Universal Serial Bus

（　最終ページ　）