Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model

Security Target

Version 1.04
2016/06/07

キヤノン株式会社

目 次

1 ST introduction

1.1 ST reference

本節では Security Target（以下、ST と略す）の識別情報を記述する。

ST 名称: Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model Security Target

バージョン: 1.04
発行者: キヤノン株式会社
発行日: 2016/06/07
キーワード: IEEE 2600、Canon、キヤノン、imageRUNNER、iR、Advance、デジタル複合機、複合機、コピー、プリント、ファクス、送信、ファクシミリ、識別、認証、アクセス制御、ログ、暗号化、セキュアプリント、ボックス、セキュリティキット、セキュリティーキット

1.2 TOE reference

本節では TOE の識別情報を記述する。

TOE 名称: Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model
バージョン: 1.1

尚、本 TOE は以下に示すソフトウェア、ハードウェア、及びライセンスから構成される。

iR-ADV セキュリティーキット・L1 for IEEE 2600.1 Ver 1.01
HDD データ暗号化キット C
（Canon MFP Security Chip 2.01）
スーパーG3FAX ボード・AR1（F モデルは本体標準）
Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series
Access Management System（本体標準装備）

※英文名称
iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Ver 1.01
HDD Data Encryption Kit-C
（Canon MFP Security Chip 2.01）
Super G3 FAX Board-AR1
Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series
Access Management System（ライセンスオプション：北米地区では本体標準装備）

※ Canon imageRUNNER ADVANCE C33900KG/C3300KG Series は Canon imageRUNNER ADVANCE C3300 Series の韓国官需専用モデルです。

1.3 TOE overview

TOE は、< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model >というデジタル複合機である。通常モデルの< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series >に以下の 4 つの製品(一部標準装備)をインストール・設置し、各種設定を行うことで TOE である< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300

Series 2600.1 model >が完成する。

- iR-ADV セキュリティーキット・L1 for IEEE 2600.1
- HDD データ暗号化キット
- ファクスボード(F モデルは本体標準)
- (Access Management System) :ライセンスオプション [1]

  日本・北米地区では、デジタル複合機本体に標準装備。

  アジアオセアニア地区では、ACCESS MANAGEMENT SYSTEM KIT-B1 が必要。

iR-ADV セキュリティーキット・L1 for IEEE 2600.1 には、< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series >の制御ソフトウェア及びセキュリティーキットライセンスが含まれる。
HDD データ暗号化ボードは、HDD に格納されるデータ全体(ソフトウェアを含む)を暗号化するためのハードウェアである。本 TOE の HDD はリムーバブルディスクとして扱うことが可能である。
ファクスボードはファクス機能を使用するためのハードウェアである。
< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model >は、以下の複合機用の Protection Profile(以下、PP と略す)、およびその PP で定義されている 7 個の SFR Packages で要求されているセキュリティ機能を、完全に装備することができる。

Protection Profile

- 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A

SFR Packages

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
- 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

1.4 略語・用語

本 ST では以下の略語・用語を使用する。

Table 1 —略語・用語

略語・用語	説明
デジタル複合機	コピー機能、ファクス機能、プリント機能、送信(Universal Send)機能などを併せ持つ複合機のこと。これらの機能を使用するため、大容量の HDD を持つ。
制御ソフトウェア	本体ハードウェア上動作しセキュリティ機能の制御を司るソフトウェアである。

[1] Access Management System はライセンスオプションであり、実際の構成要素は、iR-ADV セキュリティーキット・L1 for IEEE 2600.1 として提供される制御ソフトウェアに含まれる。

略語・用語	説明
操作パネル	デジタル複合機を構成するハードウェアのひとつであり、操作キーとタッチパネルから構成され、デジタル複合機を操作するときに使用されるインターフェースである。
リモート UI	Web ブラウザから LAN を経由してデジタル複合機にアクセスし、デジタル複合機の動作状況の確認やジョブの操作、ボックスに対する操作、各種設定などができるインターフェースである。
HDD	デジタル複合機に搭載されるハードディスクのこと。制御ソフトウェアおよび、保護資産が保存される。
I ファクス	ファクス文書の送受信を行うためのインフラとして、電話回線ではなく、インターネットを使用するインターネットファクスのこと。
イメージファイル	読み込み、プリント、受信などによってデジタル複合機内に生成された画像データ。
テンポラリイメージファイル	コピー・プリント等のジョブの途中に生成され、ジョブが完了すると不要になるイメージファイル。
ロール	アクセス制御機能で利用するユーザーの権限であり、各ユーザーにはひとつのロールが関連付けられる。 あらかじめ定義されているデフォルトロールに加え、カスタムロールとしてデフォルトロールで決められたアクセス制限値を変更した新規のロールを作成することが可能である。デフォルトロールには以下のロールがある Administrator/Power User/General User/Limited User/Guest User Administrator ロールとは管理機能を利用する権限(管理権限)を示す
管理者	Administrator ロールが割り当てられた管理権限を有するユーザー。 PP で定義されている U.ADMINISTRATOR。
ジョブ	ユーザーが TOE の機能を利用して文書を操作する際のユーザーの作業指示と対象となる文書のデータ(電子文書)を組み合わせたもの。 文書の操作には、読み込み、プリント、コピー、ファクス送信、保存、削除があり、ユーザーの操作によりジョブの生成、実行、完了までの一連の処理が行われる。
電子文書	デジタル複合機内で取り扱われるユーザーデータであり、イメージファイルと属性情報から構成される。
メモリー受信	受信したファクス/I ファクスを、プリントしないでシステムボックスに保存しておく機能のこと。
ボックス	デジタル複合機において読み込みやプリント、ファクス受信した電子文書を保存する領域。 ユーザーボックス、ファクスボックス、システムボックスの 3 種類が存在する。 ※本 TOE では、ファクスボックスを利用しない。
ユーザーボックス	デジタル複合機で一般ユーザーが読み込んだ電子文書や、PC からプリント指示した電子文書などが保存されるボックスであり、電子文書のプリントが可能である。

略語・用語	説明
システムボックス	ファクスメモリー受信/I ファクスメモリー受信した電子文書が保存されるボックスであり、電子文書のプリントや送信などが可能である。
メールサーバー	デジタル複合機で読み込んだ電子文書を I ファクス送信や電子メール送信する場合に必要なサーバー。
ユーザー認証サーバー	ユーザーID やパスワード等のユーザー情報を保持し、ネットワークを介してユーザー認証を行うサーバー。
Firewall	Internet から内部 LAN への攻撃を防ぐための装置やシステム。
タイムサーバー	時刻を正確に合わせており、Internet を介して、Network Time Protocol を使った時刻の問い合わせに答えることができるサーバー。
「セキュアプリント」	セキュアプリント(暗証番号が付与されたプリント)を操作する機能を起動する操作パネル上のボタン。
「コピー」	コピー機能を起動する操作パネル上のボタン。
「ファクス」	ファクス機能を起動する操作パネル上のボタン。
「スキャン」	紙文書を読み込んでボックスへ保存する機能や読み込んだ電子文書を電子メールアドレスや PC の共有フォルダー等へ送信する機能を起動する操作パネル上のボタンである「スキャンして送信」「スキャンして保存」ボタン。
「受信トレイ」	「受信トレイ」とは受信トレイへの操作パネル上のボタン。 受信トレイとは、ファクス／I ファクス受信されたファイルを一時的に保存するトレイであり、システムボックスとファクスボックスの 2 種類があります。
「保存ファイルの利用」	ボックスへ保存された電子文書を操作する機能を起動する操作パネル上のボタン。
リモートUI 上の「受信/保存ファイルの利用」	ボックスへ保存された電子文書を操作する機能を起動するリモート UI 上のボタン。

1.5 TOE description

TOE は、コピー機能・プリント機能・送信（Universal Send）機能・ファクス機能・I ファクス受信機能・ユーザーボックス機能、などを併せ持つ複合機である。TOE が適合する 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A では以下のような利用環境を想定している。（" 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A" clause "1.1 Scope" からの引用）

This standard is for a Protection Profile for Hardcopy Devices in a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance are required. The typical information processed in this environment is trade secret, mission critical, or subject to legal and regulatory considerations, such as for privacy or governance. This environment is not intended to support life-critical or national security applications. This environment will be known as "Operational Environment A."

Figure 1 は、TOE であるデジタル複合機＜ Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model ＞のオプションを含む機能を使用する場合の想定設置環境であり、使用しない機能がある場合には、設置環境は異なる場合がある。

Figure 1 デジタル複合機＜ Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series **＞の想定設置使用環境**

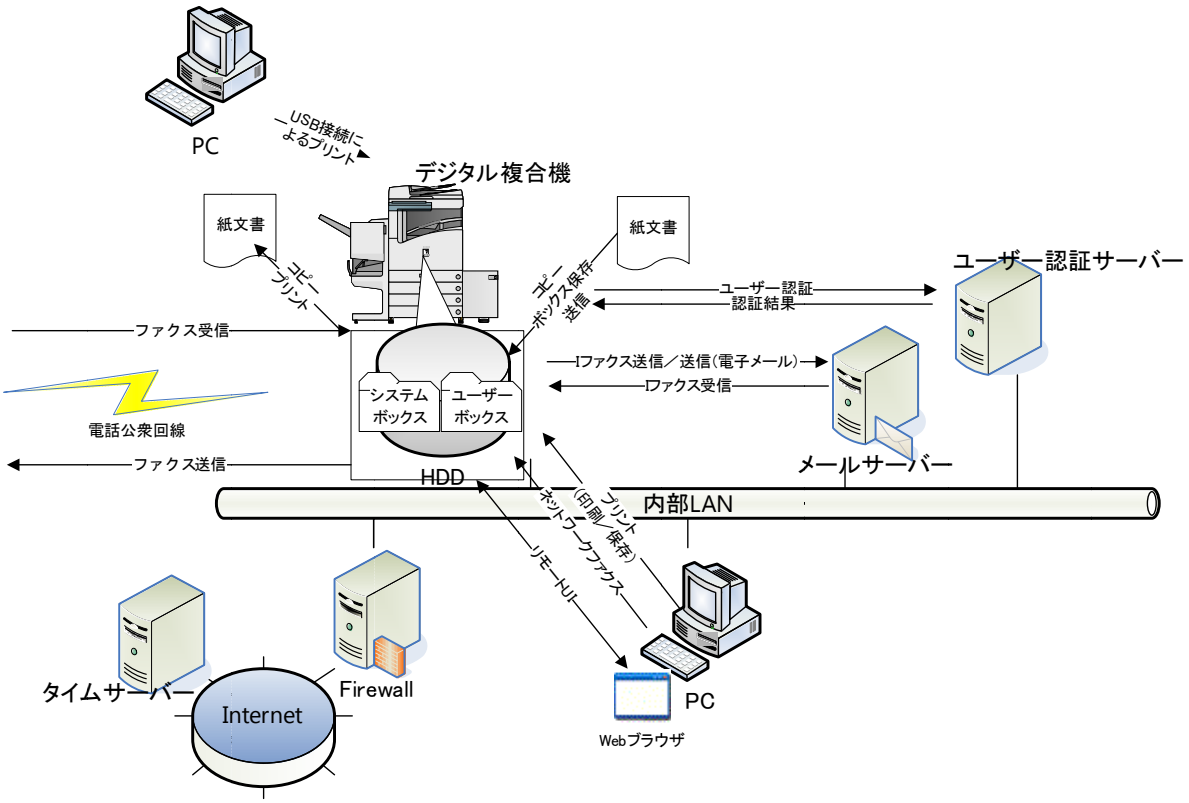


Figure1 に示すような想定設置使用環境では、デジタル複合機は内部 LAN によってメールサーバー、ユーザー認証サーバー、PC、Firewall に接続されており、Firewall によって Internet から内部 LAN への攻撃を防いでいる。デジタル複合機は、自身で読み込んだ電子文書を I ファクス送信や電子メール送信したり、I ファクスを受信したりするためにメールサーバーに接続する。また、PC を用いて電子文書をプリント、保存、I ファクスを利用することができ、Web ブラウザ[2]を PC 上にインストールすることでデジタル複合機をリ

[2] CC 評価におけるテスト環境では、Web ブラウザは Microsoft Internet Explorer 11 を利用した。

モート操作することも可能である。ただし、PC からプリントを行う場合は、適切なプリンタードライバーを PC にインストールして使用する必要がある。USB ケーブルで PC を直接接続することで PC から電子文書をプリント、保存することも可能である。ただし、USB 接続でデジタル複合機から PC や USB デバイスにデータを保存することはできないように設置時に設定する。

更に、TOE はタイムサーバーから正確な日時を取得して時刻同期を行ったり、外部のユーザー認証サーバーと連携することで利用者の識別認証機能を提供したりすることを可能としている。このような想定設置使用環境において、デジタル複合機は以下の機能を利用することができる。

- コピー機能

紙文書をスキャナで読み込み、プリントすることにより、紙文書を複写する機能である。

- プリント機能

デジタル複合機内の電子文書や PC から送信される電子文書を紙文書にプリントする機能である。

- I ファクス受信機能

インターネットを介して、I ファクスとして電子文書を受信する機能である。I ファクス受信されたファイルは、受信時にプリントされずにシステムボックスに保存される。保存されたファイルは、必要なときにプリント、送信、削除ができる。

- ファクス受信機能

ファクス回線を介して、電子文書を受信する機能である。ファクス受信されたファイルは、受信時にプリントされずにシステムボックスに保存される。保存されたファイルは、必要なときにプリント、送信、削除ができる。

- ファクス送信機能

紙文書をスキャンして生成された電子文書やシステムボックスに保存されている電子文書をファクス送信する機能である。

- 送信（Universal Send）機能

紙文書をスキャンして生成された電子文書やシステムボックスに保存されている電子文書を TIFF や PDF ファイル形式で電子メールアドレスや PC の共有フォルダー、I ファクスなどに送信する機能である。

- ユーザーボックス機能

この機能は、ユーザーボックスへイメージファイルを保存する機能とユーザーボックスの保存ボックスを利用する機能に大別できる。

- ユーザーボックスへイメージファイルを保存する機能

  スキャナから読み込んだ電子文書や、PC にてボックス保存を指定した電子文書をユーザーボックスに保存する機能である。

- ユーザーボックスの保存ボックスを利用する機能

  ユーザーボックスに保存された電子文書に対して以下の操作ができる。

  - 電子文書のプリント
  - 電子文書の削除

1.6 TOE の範囲

TOE が適合する 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A の要求仕様を実現するために以下のような TOE を構成する。

TOE の物理的範囲と論理的範囲は以下の通りである。

1.6.1 TOE の物理的範囲

TOE はハードウェアとソフトウェアから構成されたデジタル複合機である。物理的範囲は以下の Figure 2 に示す部分である。

Figure 2 TOE のハードウェア/ソフトウェア

<table>
<tr><td colspan="3">制御ソフトウェア
（TOE:ソフトウェア）</td></tr>
<tr><td>ファクスボード
（F モデルは本体ハードウェアに標準装備）
（TOE：ハードウェア）</td><td>Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series
本体ハードウェア
（TOE：ハードウェア）</td><td>HDD データ暗号化ボード
（TOE：ハードウェア）</td></tr>
</table>

制御ソフトウェアは iR-ADV セキュリティーキット・L1 for IEEE 2600.1 として提供される。
本体ハードウェアと iR-ADV セキュリティーキット・L1 for IEEE 2600.1 を合わせてデジタル複合機本体とする。

TOE である< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series 2600.1 model > はデジタル複合機本体に HDD データ暗号化ボードおよび、ファクスボードを組み合わせたものである。

TOE を構成する本体ハードウェアである< Canon imageRUNNER ADVANCE C33900KG/C3300KG/C3300 Series >には以下のラインアップがある。

Table 2 —製品ラインアップ一覧

製品ラインアップ
iR-ADV C33930KG/ iR-ADV C33925KG/ iR-ADV C33920KG/ iR-ADV C3330KG/ iR-ADV C3325KG/ iR-ADV C3320KG/ iR-ADV C3330/ iR-ADV C3330i/ iR-ADV C3330F/ iR-ADV C3325/ iR-ADV C3325i/ iR-ADV C3320/ iR-ADV C3320i/ iR-ADV C3320F

TOE に含まれるガイダンスは以下の通りである。

（和文名称）
- imageRUNNER ADVANCE C3300 Series 2600.1 model eマニュアル CD
- iR-ADV セキュリティーキット・L1 for IEEE 2600.1 アドミニストレーターガイド
- iR-ADV セキュリティーキット・L1 for IEEE 2600.1 をお使いになる前にお読みください
- HDD データ暗号化キット ユーザーズガイド

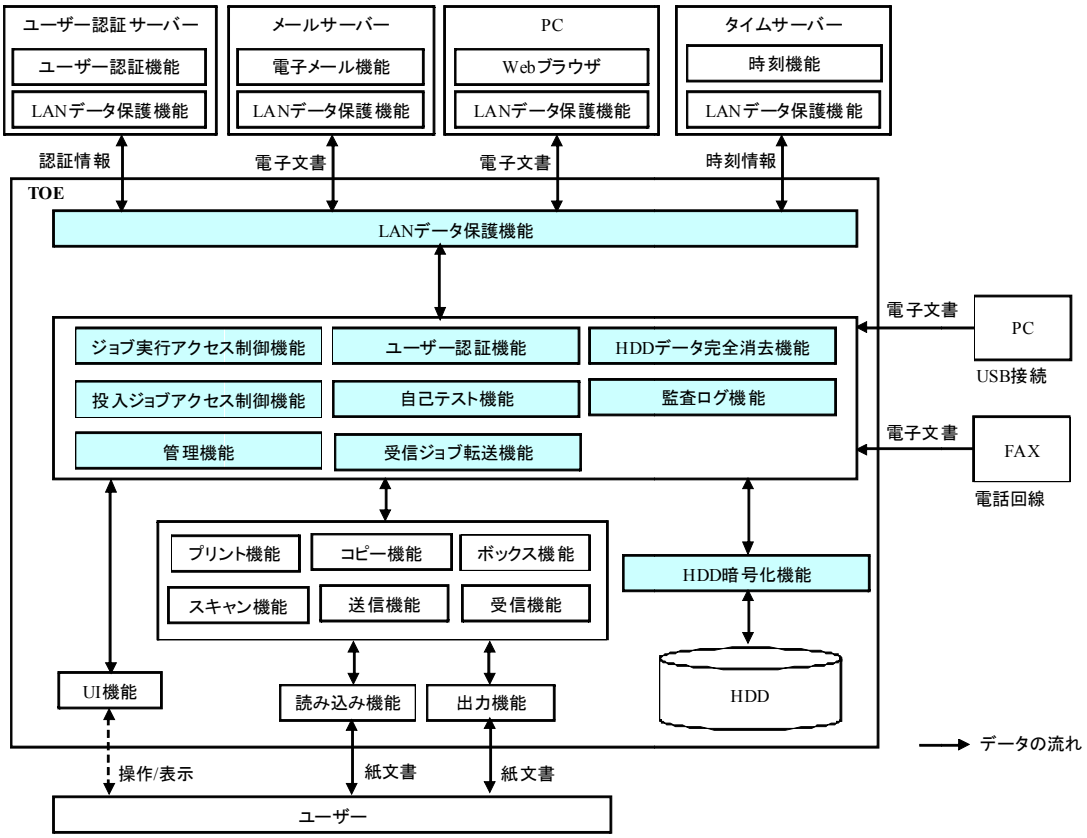
（英文名称）
- imageRUNNER ADVANCE C3300 Series 2600.1 model e-Manual CD（USE Version）

- imageRUNNER ADVANCE C3300 Series 2600.1 model e-Manual CD（APE Version）
- iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Certification Administrator Guide
- Before Using the iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Certification HDD Data Encryption Kit Reference Guide

1.6.2 TOE の論理的範囲

TOE の論理的範囲を以下の Figure 3 で図示する(ユーザー、ユーザー認証サーバー、メールサーバー、PC、タイムサーバーを除く)。TOE のセキュリティ機能は色つきで示す部分である。

Figure 3 TOE の機能構成



TOE は 1.5 章で説明した機能に加え以下の一般機能を有する。

- UI 機能

  ユーザーが操作パネルを用いて TOE を操作したり、TOE が操作パネルに表示したりする。

- 出力機能

  TOE が紙文書を出力する。

- 読み込み機能

TOE が紙文書を入力する。

TOE は、以下のセキュリティ機能を有する。

- ユーザー認証機能

  登録外の人によって勝手に TOE が利用されないように、正当なユーザーを認証する。

  ユーザー認証は、TOE 内で認証する内部認証と外部のユーザー認証サーバーを用いて認証する外部認証をサポートする。外部認証における認証方式は Kerberos 認証[3]もしくは LDAP 認証[4]を用いる。

- ジョブ実行アクセス制御機能

  認証されたユーザーが権限外のデジタル複合機の機能を実行できないように、ユーザーのロールに応じて各種機能の実行を許可する。

- 投入ジョブアクセス制御機能

  投入したジョブに対して、プリントやジョブキャンセル等の操作をジョブ投入したユーザーに制限する。

- 受信ジョブ転送機能

  受信したジョブの LAN への転送を制御する。ファクスラインを悪用した攻撃に対抗するために、ファクス受信ジョブの転送を制限する。

- HDD データ完全消去機能

  ジョブ実行時に作成されたイメージデータが再利用されることを防ぐために、HDD の残存イメージデータ領域を上書きして完全消去する

- HDD 暗号化機能

  HDD 単体の持ち去り、もしくは、HDD と HDD データ暗号化ボードを併せて持ち去り HDD データへのアクセスする脅威に対抗するために、HDD データ暗号化ボードは、毎回起動時にデジタル複合機本体を識別し、正しいデジタル複合機本体だった場合のみ HDD アクセスを許可する。さらに、HDD データの機密性を保護するために、HDD に格納されるすべてのデータを暗号化する

- LAN データ保護機能

  LAN データの IP パケットへのスニッファリング対策として、IP パケットを IPSec にて暗号化する

- 自己テスト機能

  主要のセキュリティ機能が正常であることを、スタートアップ時に検証する

- 監査ログ機能

  ユーザーの操作を監査できるようにログを生成し、HDD 内に保存する機能であり、更に保存された監査記録を保護、閲覧できるようにする

  ログに記録される日時情報は、TOE から提供される。TOE の日時情報は、管理機能の利用、もしくはタイムサーバーから正確な日時を取得して時刻同期することで設定される。

- 管理機能

  ユーザーやロールを登録・削除するためのユーザー管理機能と各種セキュリティ機能が適切に動作するためのデバイス管理機能であり、ともに管理者のみに操作が限定されている

[3] CC 評価におけるテスト環境では、Kerberos 認証として Active Directory Domain Services を利用した。
[4] CC 評価におけるテスト環境では、LDAP 認証として eDirectory 8.8 SP8 を利用した。

1.7 TOE のユーザー

TOE のユーザー（U.USER）は、以下の 2 種類のユーザーに分類できる。

Table 3 —Users

Designation		Definition
U.USER		Any authorized User.
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE.
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

1.8 Assets

資産は、User Data, TSF Data, Functions の 3 種類である。

1.8.1 User Data

User Data は、ユーザーによって作成される TOE のセキュリティ機能には影響を与えないデータであり、以下の 2 種類に分類できる。

Table 4 — 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.

1.8.2 TSF Data

TSF Data は、TOE のセキュリティ機能に影響を与えるデータであり、以下の 2 種類に分類できる。

Table 5 — 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 で扱う TSF Data を以下の Table 6 に示す。

Table 6 — TSF Data の具体化

タイプ	TSF データ	内容	保存先
D.PROT	ユーザー名	ユーザー識別認証機能で利用するユーザーの識別情報	HDD
	ロール	アクセス制御機能で利用するユーザーの権限情報	HDD
	ロックアウトポリシー設定	ロックアウト機能の設定情報であり、ロックアウトの許容回数とロックアウト時間の設定情報	HDD
	パスワードポリシー設定	ユーザー認証機能で利用するパスワードの設定情報であり、最小パスワード長、使用可能文字、組み合わせに関する制約の設定情報	HDD
	オートクリア設定	操作パネルのセッションタイムアウトの時間設定情報	HDD
	日付/時刻設定	日付と時刻の設定情報	RTC
	HDD 完全消去設定	HDD データ完全消去機能設定情報であり、機能の有効/無効化に関する設定情報	HDD
	IPSec 設定	LAN データ保護機能に関する設定情報であり、機能の有効/無効化に関する設定情報	HDD
D.CONF	パスワード	ユーザー識別認証機能で利用するユーザーの認証情報	HDD
	監査ログ	監査ログ機能で生成されるログ	HDD
	ボックス暗証番号	投入ジョブアクセス制御機能で利用する、ユーザーボックス、システムボックスへのアクセス制御で利用するボックス毎の暗証番号	HDD

1.8.3 Functions

Table 7 に示す機能

2 Conformance claims

2.1 CC Conformance claim

この ST は、以下の Common Criteria（以下、CC と略す）に適合する。

- Common Criteria version: Version 3.1 Release 4
- Common Criteria conformance: Part 2 extended and Part 3 conformant
- Assurance level: EAL3 augmented by ALC_FLR.2

2.2 PP claim, Package claim

この ST は、以下の PP に適合する。

- Title ：2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  - Version：1.0, dated June 2009

この ST は、以下の SFR Packages 適合、追加である。

- 2600.1-PRT 適合
- 2600.1-SCN 適合
- 2600.1-CPY 適合
- 2600.1-FAX 適合
- 2600.1-DSR 適合
- 2600.1-NVS 追加
- 2600.1-SMI 追加

2.3 SFR Packages

2.3.1 SFR Packages reference

Title: 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as printers, paper-based fax machines, and MFPs) that perform a printing function in which electronic document input is converted to physical document output.

Title: 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as scanners, paper-based fax machines, and

MFPs) that perform a scanning function in which physical document input is converted to electronic document output.

Title: 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This Protection Profile shall be used for HCD products (such as copiers and MFPs) that perform a copy function in which physical document input is duplicated to physical document output.

Title: 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as fax machines and MFPs) that perform a scanning function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a printing function in which a telephone-based document facsimile (fax) reception is converted to physical document output.

Title: 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as MFPs) that perform a document storage and retrieval feature in which a document is stored during one job and retrieved during one or more subsequent jobs.

Title: 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for products that provide storage of User Data or TSF Data in a nonvolatile storage device (NVS) that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel. This package applies for TOEs that provide the ability to protect data stored on Removable Nonvolatile Storage devices from unauthorized disclosure and modification. If such protection is supplied only by the TOE environment, then this package cannot be claimed.

Title: 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products that transmit or receive 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. This package applies for TOEs that provide a trusted channel function allowing for secure and authenticated communication with other IT systems. If such protection is supplied by only the TOE environment, then this package cannot be claimed.

2.3.2 SFR Package 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 7:

Table 7 —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.NVS	Nonvolatile storage: a function that stores User Data or TSF Data on a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel
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

2.3.3 SFR Package 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 8:

Table 8 —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.
+NVS	Indicates data that are stored on a nonvolatile storage device.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.4 PP Conformance rationale

TOE は、デジタル複合機の主要な機能であるコピー、プリント、スキャナ、ファクスの機能に加え、文書保存機能、HDD 暗号化機能、LAN データの暗号化機能を装備することから、2.2 章の PP claim, Package claim における PP に定義されているすべての SFR Packages に適合することは適切である。

以下に、7 個すべての SFR Packages を包含した PP とこの ST を比較していく。

まず、Security Problem Definition に関して、PP と ST を比較すると、以下の OSP をひとつ追加している以外は同じである。

P.HDD.ACCESS.AUTHORIZATION

これは、運用環境を制約しているのではなく、TOE を制約している OSP である。

従って、以下が成立する。

- STのセキュリティ課題定義を満たすすべてのTOEは、PPのセキュリティ課題定義も満たしている
- PPのセキュリティ課題定義を満たすすべての運用環境は、STのセキュリティ課題定義も満たしている

次に、Objective に関して、PP と ST を比較すると、以下の Objective をひとつ追加しているほかは同じである。

O.HDD.ACCESS.AUTHORISED

これは、TOE を制約している Objective である。

従って、以下が成立する。

- STのTOEのセキュリティ対策方針を満たすすべてのTOEは、PPのTOEのセキュリティ対策方針も満たしている
- PPの運用環境のセキュリティ対策方針を満たすすべての運用環境は、STの運用環境のセキュリティ対策方針も満たしている

さらに、機能要件に関して、PP と ST を比較すると、Table 9 のように 7 個の SFR Packages 含めすべての機能要件に対応して、さらに ST では機能要件が追加されている。

Table 9 —PP、ST での機能要件対応表

PP_Package	PP の機能要件	ST の機能要件
Common	FAU_GEN.1	FAU_GEN.1
Common	FAU_GEN.2	FAU_GEN.2
Common	FAU_SAR.1	FAU_SAR.1
Common	FAU_SAR.2	FAU_SAR.2
Common	FAU_STG.1	FAU_STG.1
Common	FAU_STG.4	FAU_STG.4
Common	FDP_ACC.1(a)	FDP_ACC.1(delete-job)
Common	FDP_ACC.1(b)	FDP_ACC.1(exec-job)
Common	FDP_ACF.1(a)	FDP_ACF.1(delete-job)
Common	FDP_ACF.1(b)	FDP_ACF.1(exec-job)
Common	FDP_RIP.1	FDP_RIP.1
Common	FIA_ATD.1	FIA_ATD.1
Common	FIA_UAU.1	FIA_UAU.1
Common	FIA_UID.1	FIA_UID.1
Common	FIA_USB.1	FIA_USB.1
Common	FMT_MSA.1(a)	FMT_MSA.1(delete-job)
Common	FMT_MSA.3(a)	FMT_MSA.3(delete-job)
Common	FMT_MSA.1(b)	FMT_MSA.1(exec-job)
Common	FMT_MSA.3(b)	FMT_MSA.3(exec-job)
Common	FMT_MTD.1(FMT_MTD.1.1(a))	FMT_MTD.1(device-mgt)
Common	FMT_MTD.1(FMT_MTD.1.1(b))	FMT_MTD.1(user-mgt)
Common	FMT_SMF.1	FMT_SMF.1
Common	FMT_SMR.1	FMT_SMR.1
Common	FPT_STM.1	FPT_STM.1
Common	FPT_TST.1	FPT_TST.1
Common	FTA_SSL.3	FTA_SSL.3(lui), FTA_SSL.3(rui)
PRT	FDP_ACC.1	FDP_ACC.1(in-job)
PRT	FDP_ACF.1	FDP_ACF.1(in-job)
SCN	FDP_ACC.1	FDP_ACC.1(in-job)

PP_Package	PP の機能要件	ST の機能要件
SCN	FDP_ACF.1	FDP_ACF.1(in-job)
CPY	FDP_ACC.1	FDP_ACC.1(in-job)
CPY	FDP_ACF.1	FDP_ACF.1(in-job)
FAX	FDP_ACC.1	FDP_ACC.1(in-job)
FAX	FDP_ACF.1	FDP_ACF.1(in-job)
DSR	FDP_ACC.1	FDP_ACC.1(in-job)
DSR	FDP_ACF.1	FDP_ACF.1(in-job)
NVS	FPT_CIP_EXP.1	FPT_CIP_EXP.1
SMI	FAU_GEN.1	FAU_GEN.1
SMI	FPT_FDI_EXP.1	FPT_FDI_EXP.1
SMI	FTP_ITC.1	FTP_ITC.1
Common	-	FIA_AFL.1
Common	-	FIA_SOS.1
Common	-	FIA_UAU.7
NVS	-	FCS_COP.1(h)
NVS･SMI	-	FCS_CKM.1
SMI	-	FCS_COP.1(n)
SMI	-	FCS_CKM.2
NVS	-	FPT_PHP.1

PP では、FDP_ACF.1(a)において、+FAXIN の D.DOC の Delete、+FAXIN の D.FUNC の Delete に対する Subject を U.NORMAL としているが、ST では FDP_ACF.1(delete-job)において、Subject を U.ADMINISTRATOR とし、U.NORMAL の Access Control rule を「Denied」としている。また、PP では、FDP_ACC.1 において、+FAXIN の D.DOC の Read に対する Subject を U.NORMAL としているが、ST では FDP_ACC.1(in-job)において、Read に対する Subject を U.ADMINISTRATOR とし、U.NORMAL の Access Control rule を「Denied」としている。

上述した ST の機能要件の割り付けは Delete や Read 可能な Subject の範囲を狭め、U.NORMAL のアクセス可能な Object をなくす割り付けであり、PP の機能要件よりも制限的なアクセス制御を行っていると言える。

PP では、FDP_ACF.1(a)において、+FAXIN の D.FUNC の Modify に対する Subject を U.NORMAL としているが、ST では FDP_ACF.1(delete-job)において、Subject を U.User とし、Access Control rule を「Denied」としている。

ST の機能要件の割り付けは、機能の利用をどの Subject にも許さないようにする割り付けであり、PP の機能要件よりも制限的なアクセス制御を行っていると言える。

以上の説明より、ST で記述されている SFR は、PP で記述されている SFR より「同等またはより制限的」であるといえる。

従って、以下が成立する。

- STのSFRを満たすすべてのTOEは、PPのSFRも満たしている

また、ST の保証要件は PP の保証要件と同じである。

以上により、この ST は PP に比較して、TOE に同等以上の制限を課し、TOE の運用環境に同等以下の制限を課している。

従って、この ST は PP を論証適合している。

3 Security Problem Definition

3.1 Notational conventions

- Defined terms in full form are set in title case (for example, “Document Storage and Retrieval”).
- Defined terms in abbreviated form are set in all caps (for example, “DSR”).
- In tables that describe Security Objectives rationale, a checkmark (“✓”) place at the intersection of a row and column indicates that the threat identified in that row is wholly or partially mitigated by the objective in that column.
- In tables that describe completeness of security requirements, a **bold** typeface letter “P” placed at the intersection of a row and column indicates that the requirement identified in that row performs a principal fulfillment of the objective indicated in that column. A letter “S” in such an intersection indicates that it performs a supporting fulfillment.
- In tables that describe the sufficiency of security requirements, a **bold** typeface requirement name and purpose indicates that the requirement performs a principal fulfillment of the objective in the same row. Requirement names and purposes set in normal typeface indicate that those requirements perform supporting fulfillments.In specifications of Security Functional Requirements (SFRs):

  - **Bold typef**ace indicates the portion of an SFR that has been completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition.
  - *Italic* typeface indicates the portion of an SFR that must be completed by the ST Author in a conforming Security Target.
  - ***Bold italic*** typeface indicates the portion of an SFR that has been partially completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition, but which also must be completed by the ST Author in a conforming Security Target.

- The following prefixes are used to indicate different entity types:

Table 10— Notational prefix conventions

Prefix	Type of entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security attribute

3.2 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.

3.3 Threats to TOE Assets

This section describes threats to assets described in clause 1.8.

Table 11—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

Table 12—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

3.4 Organizational Security Policies

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.

Table 13—Organizational Security Policies

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.ACCESS.AUTHORIZATION	To prevent access TOE assets in the HDD with connecting the other HCDs, TOE will have authorized access the HDD data.

3.5 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.

Table 14—Assumptions

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.

Assumption	Definition
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 Security Objectives

4.1 Security Objectives for the TOE

この章では、TOE の満たすべきセキュリティ対策方針に関して記述する。

Table 15— 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.HDD.ACCESS.AUTHORISED	The TOE shall protect TOE assets in the HDD from accessing without the TOE authorization.

4.2 Security Objectives for the IT environment

この章では、IT 環境のセキュリティ対策方針に関して記述する。

Table 16— Security Objectives for the IT environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3 Security Objectives for the non-IT environment

この章では、非 IT 環境のセキュリティ対策方針に関して記述する。

Table 17— Security Objectives for the non-IT 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.

4.4 Security Objectives rationale

この章では、セキュリティ対策方針（Security Objectives）の根拠に関して記述する。

Table 18—Completeness of Security Objectives

	Objectives																		
Threats. Policies, and Assumptions	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.HDD.ACCESS.AUTHORISED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
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															✓		✓			
P.HDD.ACCESS.AUTHORIZATION											✓									

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.HDD.ACCESS.AUTHORISED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
A.ACCESS.MANAGED																✓				
A.ADMIN.TRAINING																		✓		
A.ADMIN.TRUST																			✓	
A.USER.TRAINING																				✓

Table 19—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 unauthorized persons	O.CONF.NO_DIS protects D.CONF 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.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.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modifications
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed
P.HDD.ACCESS.AUTHORIZATION	To prevent access TOE assets in the HDD with connecting the other HCDs, TOE will have authorized access the HDD data.	O.HDD.ACCESS.AUTHORISED protects TOE assets in the HDD from accessing without the TOE authorization.
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
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.TRUST 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 Extended components definition (APE_ECD)

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

5.1 FPT_CIP_EXP Confidentiality and integrity of stored data

Family behaviour:

This family defines requirements for the TSF to protect the confidentiality and integrity of both TSF and user data.

Confidentiality and integrity of stored data is important security functionality in the case where the storage container is not, or not always, in a protected environment. Confidentiality and integrity of stored data is often provided by functionality that the TSF uses for both TSF and user data in the same way. Examples are full disk encryption functions, where the TSF stores its own data as well as user data on the same disk. Especially when a disk is intended to be removable and therefore may be transported into an unprotected environment, this becomes a very important functionality to achieve the Security Objectives of protection against unauthorized access to information.

Component leveling:

FPT_CIP_EXP.1 Confidentiality and integrity of stored data	1

FPT_CIP_EXP.1 Confidentiality and integrity of stored data, provides for the protection of user and TSF data stored on a storage container that cannot be assumed to be protected by the TOE environment.

Management: FPT_CIP_EXP.1

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

a) Management of the conditions under which the protection function is activated or used;

b) Management of potential restrictions on the allowance to use this function.

Audit: FPT_CIP_EXP.1

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

a) Basic: failure condition that prohibits the function to work properly, detected attempts to bypass this functionality (e. g. detected modifications).

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: *media used to store the data*].

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs

[assignment: *list of actions*] when it detects alteration of user and TSF data when either is written to [assignment: *media used to store the data*].

Rationale:

The Common Criteria defines the protection of user data in its FDP class and the protection of TSF data in its FPT class. Although both classes contain components that define confidentiality protection and integrity protection, those components are defined differently for user data and TSF data and therefore are difficult to use in cases where a TOE provides functionality for the confidentiality and integrity for both types of data in an identical way.

This Protection Profile defines an extended component that combines the confidentiality and integrity protection for both types of data in a single component. The authors of this Protection Profile view this as an approach that simplifies the statement of security functional requirements significantly and therefore enhances the readability and applicability of this Protection Profile. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or FPT class. Since it is intended to protect data that are exported to storage media, and in particular, storage media that might be removable from the TOE, 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 led the authors to define a new family with just one member.

5.2 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	1

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 these data are 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 are 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 it 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 led 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 Security requirements

この章では、TOE のセキュリティ要件（security requirements）に関して記述する。

6.1 Security functional requirements

この章では、TOE のセキュリティ機能要件（security functional requirements）に関して記述する。
尚、コンポーネント識別情報や機能エレメント名の後ろの（）書きは、繰り返しの操作を示す識別子を示している。

6.1.1 ユーザー認証機能

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 1 to 10

[assignment: *list of authentication events*]
- 操作パネルもしくはリモート UI を使ったログイン試行

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*]
- ロックアウト

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*]
- ユーザー名、ロール

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***]
- プリントジョブ、ファクスジョブ、I ファクスジョブの投入

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*]
- *

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***]
- プリントジョブ、ファクスジョブ、I ファクスジョブの投入

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*]
- ユーザー名、ロール

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

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

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

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

FTA_SSL.3(lui) TSF-initiated termination

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

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

[assignment: *time interval of user inactivity*]
- 操作パネルを操作しない状態が、設定時間経過

FTA_SSL.3(rui) TSF-initiated termination

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

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

[assignment: *time interval of user inactivity*]
- リモート UI を操作しない状態が、15 分間経過

6.1.2 ジョブ実行アクセス制御機能

FMT_MSA.1(exec-job) 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(exec-job) 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]*]
- query, modify, delete, create

[assignment: *list of security attributes*]
- ロール

[assignment: *the authorised identified roles*]
- U.ADMINISTRATOR

FMT_MSA.3(exec-job) 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(exec-job) 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]*]
- Restrictive

[refinement]
- TOE Function Access Control Policy → TOE Function Access Control SFP

FMT_MSA.3.2(exec-job) 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

FDP_ACC.1(exec-job) Subset access control

Hierarchical to: **No other components.**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(exec-job) The TSF shall enforce the **TOE Function Access Control SFP** on **users as subjects, TOE functions as objects, and the right to use the functions as**

operations.

FDP_ACF.1(exec-job) 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(exec-job) 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*]

- objects controlled under the TOE Function Access Control SFP in Table 20, and for each, the indicated security attributes in Table 20.

FDP_ACF.1.2(exec-job) 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]

- rules specified in the TOE Function Access Control SFP in Table 20 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects

FDP_ACF.1.3(exec-job) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **the user acts in the role U.ADMINISTRATOR,** [assignment: ***other*** *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

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

- なし

FDP_ACF.1.4(exec-job) 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

Table 20—TOE Function Access Control SFP

Object	Attribute	Operation(s)	Subject	Attribute	Access control rule

Object	Attribute	Operation(s)	Subject	Attribute	Access control rule
「セキュアプリント」	+PRT	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
「コピー」	+CPY +DSR	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
「スキャン」	+SCN +DSR	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
「ファクス」	+FAXOUT	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
「受信トレイ」	+FAXIN	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
「保存ファイルの利用」	+DSR	Object の Pointer を利用したジョブ実行	U.USER	ロール	Object の属性に対して Subject のロールが Operation を許可されたロールである
リモート UI 上の「受信/保存ファイルの利用」	+DSR +FAXIN	Object の Pointer を利用したジョブ実行	U.USER	ロール	Subject のロールが Administrator であれば Operation が可能

6.1.3 投入ジョブアクセス制御機能

6.1.3.1 ジョブ削除機能

FMT_MSA.1(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22,** [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)*]

- **In The JOB Access Control SFP in Table 23**

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

- Table 21 の「**操作**」の項

[assignment: *list of security attributes*]
- Table 21 の「**security attributes**」の項

[assignment: *the authorised identified roles*]
- Table 21 の「**ロール**」の項

Table 21—Management of security attributes

security attributes	操作	ロール
ユーザー名	delete, create, query	U.ADMINISTRATOR
ボックス暗証番号	modify, create	U.ADMINISTRATOR
自身のボックス暗証番号	modify	U.NORMAL

APPLICATION NOTE 1. This Protection Profile does not define any mandatory security attributes, but some may be defined by SFR packages or by the ST Author. The ST Author should define how security attributes are managed. Note that this Protection Profile allows the ST Author to instantiate "Nobody" as an authorized identified role, which makes it possible for the ST Author to state that some management actions (e.g., deleting a security attribute) may not be performed by any User.

FMT_MSA.3(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22,** [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*]
- **Common Access Control SFP in Table 22**
- **In The JOB Access Control SFP in Table 23**

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

FMT_MSA.3.2(delete-job) 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

FDP_ACC.1(delete-job)Subset access control

Hierarchical to: **No other components.**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22** on

the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 22.

FDP_ACF.1(delete-job) 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(delete-job) The TSF shall enforce the **Common Access Control SFP in Table 22** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 22, and for each, the indicated security attributes in Table 22.**

FDP_ACF.1.2(delete-job) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 22 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects.**

FDP_ACF.1.3(delete-job) 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*]
- U.ADMINISTRATOR は、すべての D.DOC・D.FUNC の削除が可能
- U.ADMINISTRATOR は、+CPY, +SCN, +DSR, +FAXOUT の D.FUNC の Modify が可能

FDP_ACF.1.4(delete-job) 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

Table 22—Common Access Control SFP

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	+PRT,+SCN,+CPY, +FAXOUT, +DSR	Delete	U.NORMAL	Denied, except for his/her own documents
D.DOC	+FAXIN	Delete	U.NORMAL	Denied
D.FUNC	+PRT,+SCN,+CPY, ＋FAXOUT, +DSR	Modify; Delete	U.NORMAL	Denied, except for his/her own function data
D.FUNC	+FAXIN	Modify	U.USER	Denied
D.FUNC	+FAXIN	Delete	U.NORMAL	Denied

6.1.3.2　ジョブ中アクセス制御機能

FDP_ACC.1(in-job)　　Subset access control

Hierarchical to:　No other components.

Dependencies:　FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(in-job)　The TSF shall enforce the **In The JOB Access Control SFP in Table 23** on **the list of subjects, objects, and operations among subjects and objects covered by the In The JOB Access Control SFP in Table 23**.

FDP_ACF.1(in-job)　　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(in-job)　The TSF shall enforce the **In The JOB Access Control SFP in Table 23** to objects based on the following: **the list of subjects and objects controlled under the In The JOB Access Control SFP in Table 23, and for each, the indicated security attributes in Table 23**.

FDP_ACF.1.2(in-job)　The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the In The JOB Access Control SFP in Table 23 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3(in-job)　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*]
- U.ADMINISTRATOR は、+FAXIN/+DSR の D.DOC の read が可能

FDP_ACF.1.4(in-job)　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

Table 23—In The JOB Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+PRT	Read	U.USER	Denied, except for his/her own documents
D.DOC	+SCN	Read	U.USER	Denied, except for his/her own documents
D.DOC	+CPY	Read	U.USER	Denied
D.DOC	+FAXIN	Read	U.NORMAL	Denied
D.DOC	+FAXOUT	Read	U.USER	Denied, except for his/her own documents

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+DSR	Read	U.NORMAL	Denied, except for his/her own documents

6.1.4 受信ジョブ転送機能

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**.

6.1.5 HDD データ完全消去機能

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

6.1.6 HDD 暗号化機能

6.1.6.1 暗号化/復号機能

FCS_COP.1(h) 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(h) 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 へ書き込まれるデータの暗号化操作
- HDD から読み出されるデータの復号操作

[assignment: *cryptographic algorithm*]
- AES

[assignment: *cryptographic key sizes*]
- 256 bit

[assignment: *list of standards*]
- FIPS PUB 197

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: **No other components.**

Dependencies: **No dependencies**

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

[assignment: ***a Removable Nonvolatile Storage device***]
- HDD

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs [assignment: *list of actions*] when it detects alteration of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

[assignment: *list of actions*]
- no action

[assignment: ***a Removable Nonvolatile Storage device***]
- HDD

APPLICATION NOTE 2. Today many manufacturers are looking at hardware solutions such as fully encrypting disks to meet disk encryption requirements. Some of these drives will not allow data to be written to the drive unless the correct credentials (either the key itself or credentials required to unlock the key stored in a secure area of the drive) are presented. Assuming that this functionality cannot be bypassed, detection of modifications is not a useful function within the TOE and therefore it should be possible to instantiate "no action" in the assignment for the "list of actions" in FPT_CIP_EXP.1.2, arguing that unauthorized modification is prevented by the design of the system.
Quote from [PP Guide]

6.1.6.2 本体識別認証機能

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: **No other components.**

Dependencies: **No dependencies.**

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might

compromise the TSF.

[refinement] physical tampering → HDD 及び HDD データ暗号化ボードのすり替え

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[refinement] physical tampering → HDD 及び HDD データ暗号化ボードのすり替え

6.1.7 LAN データ保護機能

6.1.7.1 IP パケット暗号化機能

FCS_COP.1(n) 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(n) 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*]
- LAN へ送信する IP パケットの暗号化操作
- LAN から受信する IP パケットの復号操作

[assignment: *cryptographic algorithm*]
- Table 24 の「cryptographic algorithm」の項

[assignment: *cryptographic key sizes*]
- Table 24 の「cryptographic key sizes」の項

[assignment: *list of standards*]
- Table 24 の「list of standards」の項

Table 24— IPSec cryptographic algorithm, key sizes and standards

cryptographic algorithm	cryptographic key sizes	list of standards
3DES-CBC	168 bit	FIPS PUB 46-3
AES-CBC	128 bit, 192bit, 256 bit	FIPS PUB 197
AES-GCM	128 bit, 192bit, 256 bit	SP800-38D

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**.

6.1.8 自己テスト機能

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*]
- LAN データ保護機能で利用する暗号アルゴリズム(AES、3DES)

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

[selection: [assignment: *parts of TSF*], *TSF data*]
- 暗号鍵

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.9 監査ログ機能

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 25;** [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 25: (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

Table 25—Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Changes to the time	FPT_STM.1	Minimum	None required
Termination of an interactive session by the session locking mechanism[5]	FTA_SSL.3	Minimum	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

[5] PP Guide の「14.1 IEEE Std 2600.1 Errata」を参照
IEEE Std 2600.1には“Locking of an interactive session by the session locking mechanism”とあるが、転記ミスである旨が記載

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.

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]
- Table 25 に示す監査ログのリスト

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 unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, *choose one of: prevent, detect*] unauthorised 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

6.1.10 管理機能

6.1.10.1 ユーザー管理機能

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*]

- 4 文字以上 32 文字以下のパスワード長
- 3 文字以上連続する文字列を含めない
- 英大文字(A～Z)を 1 文字以上含める
- 英小文字(a～z)を 1 文字以上含める
- 数字(0～9)を 1 文字以上含める
- アルファベット以外の文字(^-@[]:;,./¥!"#$%&'()=~|{`+*}_?><)を 1 文字以上含める
- 使用可能文字
  - 制御文字以外の全ての文字

FMT_MTD.1(user-mgt) 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 (user-mgt) 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 are associated***]].

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
- Table 26 の「操作」の項

[assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***]
- Table 26 の「TSF data」の項

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated*]]
- Table 26 の「ロール」の項

Table 26—ユーザー情報管理

TSF data	ロール	操作
ユーザー名	U.ADMINISTRATOR	delete, create, query
ロール	U.ADMINISTRATOR	modify, delete, create, query
パスワード	U.ADMINISTRATOR	modify, delete, create
自身のパスワード	U.NORMAL	modify

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**.

6.1.10.2 暗号鍵管理機能

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 186-2 に基づく暗号鍵生成アルゴリズム

[assignment: *cryptographic key sizes*]
- 128bit, 168bit, 192bit, 256 bit

[assignment: *list of standards*]
- FIPS PUB 186-2

FCS_CKM.2 Cryptographic key distribution

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

[assignment: *cryptographic key distribution method*]
- DH（Diffie Hellman）および ECDH（Elliptic Curve Diffie Hellman）

[assignment: *list of standards*]
- SP800-56A

6.1.10.3 デバイス管理機能

FMT_MTD.1(device-mgt) 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(device-mgt) 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]*]
- Table 27 の「操作」の項

[assignment: *list of TSF data*]
- Table 27 の「TSF Data」の項

[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*, [assignment: *the authorized identified roles* ***except U.NORMAL***]]]
- Table 27 の「ロール」の項

Table 27—デバイス管理機能

TSF Data	ロール	操作
日付/時刻設定	U.ADMINISTRATOR	modify
HDD完全消去設定	U.ADMINISTRATOR	query, modify

TSF Data	ロール	操作
IPSec 設定	U.ADMINISTRATOR	query, modify
オートクリア設定	U.ADMINISTRATOR	query, modify
ロックアウトポリシー設定	U.ADMINISTRATOR	query, modify
パスワードポリシー設定	U.ADMINISTRATOR	query, modify
監査ログ	U.ADMINISTRATOR	query, delete

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*]

- 以下の Table 28 に示す管理機能

Table 28—The management of security requirements

管理機能	操作
日付/時刻設定	modify
HDD完全消去設定	query, modify
IPSec 設定	query, modify
オートクリア設定	query, modify
ロックアウトポリシー設定	query, modify
パスワードポリシー設定	query, modify
監査ログ	query, delete
ユーザー名	delete, create, query
ロール	modify, delete, create, query
パスワード	modify, delete, create
ボックス暗証番号	modify, create

管理機能	操作
自身のパスワード	modify
自身のボックス暗証番号	modify

6.2 Security assurance requirements

This section defines the security assurance requirements for the TOE.

Table 29 lists the security assurance requirements for 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, and related SFR packages, EAL 3 augmented by ALC_FLR.2.

Table 29— 2600.1 Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL3)
	ALC_LCD.1 Developer defined life-cycle model
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.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3 Security functional requirements rationale

6.3.1 The completeness of security requirements

Table 30 は TOE セキュリティ対策方針とセキュリティ機能要件をマッピングしたものである。これにより、各セキュリティ機能要件が少なくとも 1 つの TOE セキュリティ対策方針に対応していることを示している。主要な対応関係を **Bold** 体の（P）で表し、サポートしている対応関係を（S）で示した。

Table 30—The 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.HDD.ACCESS.AUTHORISED
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	
FIA_USB.1							**P**				
FTA_SSL.3(lui)							**P**	**P**			
FTA_SSL.3(rui)							**P**	**P**			
FMT_MSA.1(exec-job)							S				
FMT_MSA.3(exec-job)							S				
FDP_ACC.1(exec-job)							**P**				
FDP_ACF.1(exec-job)							S				
FMT_MSA.1(delete-job)	S	S	S								
FMT_MSA.3(delete-job)	S	S	S								
FDP_ACC.1(delete-job)	**P**	**P**	**P**								
FDP_ACF.1(delete-job)	S	S	S								
FDP_ACC.1(in-job)	**P**										
FDP_ACF.1(in-job)	S										
FPT_FDI_EXP.1								**P**			
FDP_RIP.1	**P**										
FPT_CIP_EXP.1	**P**	**P**	**P**	**P**	**P**	**P**					
FCS_COP.1(h)	S	S	S	S	S	S					
FPT_PHP.1											**P**
FCS_COP.1(n)	S	S	S	S	S	S					
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					
FCS_CKM.1	S	S	S	S	S	S					
FCS_CKM.2	S	S	S	S	S	S					
FPT_TST.1									**P**		
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_SAR.1										**P**	
FAU_SAR.2										**P**	
FAU_STG.1										**P**	
FAU_STG.4										**P**	
FPT_STM.1										S	
FIA_SOS.1							S				
FMT_MTD.1(user-mgt)				**P**	**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.HDD.ACCESS.AUTHORISED
FMT_SMR.1	S	S	S	S	S	S	S				
FMT_MTD.1(device-mgt)				**P**	**P**	**P**					
FMT_SMF.1	S	S	S	S	S	S					

6.3.2 The sufficiency of security requirements

本章では、セキュリティ機能要件が TOE セキュリティ対策方針を満たすのに十分である根拠を記述する。

O.DOC.NO_DIS は、user document data が暴露されないように、
FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job)、FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job)によりジョブキャンセル操作を本人のみにアクセス制限するうえに、
FDP_ACC.1(in-job)/FDP_ACF.1(in-job)、
による印刷ジョブ中のユーザーデータへのアクセスを本人のみに制限したり、それ以外のジョブ中のユーザーデータへのアクセスは誰もできなくしたりすることにより実現される。
また、ジョブ処理に生成された user document data の残存情報は、FDP_RIP.1 により完全消去される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1, FCS_COP.1(h), FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。
これらに関連する管理機能は FMT_SMF.1 によって提供されている。

O.DOC.NO_ALT は、user document data が改ざんされないように、
FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job)、FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job)により操作を本人のみにアクセス制限することにより実現される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1, FCS_COP.1(h), FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。
これらに関連する管理機能は FMT_SMF.1 によって提供されている。

O.FUNC.NO_ALT は、user function data が改ざんされないように、
FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_MSA.1(delete-job)/FMT_MSA.3(delete-job)、FDP_ACC.1(delete-job)/FDP_ACF.1(delete-job)により操作を本人のみにアクセス制限することにより実現される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1, FCS_COP.1(h), FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。
これらに関連する管理機能は FMT_SMF.1 によって提供されている。

O.PROT.NO_ALT は、TSF protected data が改ざんされないように、
FMT_MTD.1(user-mgt)で管理された FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_SMR.1, FMT_MTD.1(device-mgt) , FMT_SMF.1 によるデバイス管理機能により実現される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1, FCS_COP.1(h), FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。

O.CONF.NO_DIS は、TSF confidential data が暴露されないように、
FMT_MTD.1(user-mgt)で管理された FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_SMR.1, FMT_MTD.1(device-mgt) , FMT_SMF.1 によるデバイス管理機能により実現される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1, FCS_COP.1(h), FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。

O.CONF.NO_ALT は、TSF confidential data が改ざんされないように、
FMT_MTD.1(user-mgt)で管理された FIA_UID.1 でのユーザー識別情報に応じて、FMT_SMR.1 で管理されたロールが割り当てられ、そのロールに基づき、
FMT_SMR.1, FMT_MTD.1(device-mgt) , FMT_SMF.1 によるデバイス管理機能により実現される。
さらに、HDD 内のユーザーデータ・TSF データへの改ざん・暴露に対して
FPT_CIP_EXP.1(h), FCS_COP.1, FCS_CKM.1 により保護され、
LAN を送受信するユーザーデータ・TSF データへの改ざん・暴露に対して
FCS_COP.1(n), FTP_ITC.1, FCS_CKM.1, FCS_CKM.2 により保護される。

O.USER.AUTHORIZED は、FIA_UAU.1、 FIA_UID.1、FIA_UAU.7、FIA_AFL.1 での識別認証メカニズムにより認証されたユーザーが、
FIA_ATD.1、FIA_USB.1、FTA_SSL.3(lui)/FTA_SSL.3(rui)によりユーザーのセッション管理され、FDP_ACC.1(exec-job)/FDP_ACF.1(exec-job) によるアクセス制御により、権限を付与された機能を利用できることにより実現される。
さらに、FIA_SOS.1, FMT_MSA.1(exec-job), FMT_MSA.3(exec-job), FMT_SMR.1 により正当なユーザーを管理する。

O.INTERFACE.MANAGED は、入出力インターフェースを管理する対策方針であり、FIA_UAU.1, FIA_UID.1, FTA_SSL.3(lui)/FTA_SSL.3(rui)によるユーザーインターフェースの管理と FPT_FDI_EXP.1

による LAN への転送を保護する機能によって実現される。

O.SOFTWARE.VERIFIED は、FPT_TST.1 の自己テスト機能によって実現される。

O.AUDIT.LOGGED は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4 による監査ログ機能によって実現される。さらに、監査フォーマットに必要なユーザー情報と時刻情報を提供するために FIA_UID.1 と FPT_STM.1 によってサポートされる。

O.HDD.ACCESS.AUTHORISED は、HDD アクセス前に FPT_PHP.1 による本体識別認証機能によって実現される。

6.3.3 The dependencies of security requirements

本章では、ST で機能要件の依存性を満たしていなくとも問題のない理由を記述する。

Table 31—The dependencies of security requirements

機能要件	CC で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A（依存性を満たしている）
FIA_ATD.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A（依存性を満たしている）
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A（依存性を満たしている）
FIA_UID.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A（依存性を満たしている）
FTA_SSL.3(lui)	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FTA_SSL.3(rui)	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FMT_MSA.1(exec-job)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(exec-job) FMT_SMR.1 FMT_SMF.1	N/A（依存性を満たしている）
FMT_MSA.3(exec-job)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(exec-job) FMT_SMR.1	N/A（依存性を満たしている）
FDP_ACC.1(exec-job)	FDP_ACF.1	FDP_ACF.1(exec-job)	N/A（依存性を満たしている）
FDP_ACF.1(exec-job)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(exec-job) FMT_MSA.3(exec-job)	N/A（依存性を満たしている）
FMT_MSA.1(delete-job)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(delete-job) FMT_SMR.1 FMT_SMF.1	N/A（依存性を満たしている）
FMT_MSA.3(delete-job)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(delete-job) FMT_SMR.1	N/A（依存性を満たしている）
FDP_ACC.1(delete-job)	FDP_ACF.1	FDP_ACF.1(delete-job)	N/A（依存性を満たしている）
FDP_ACF.1(delete-job)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(delete-job) FMT_MSA.3(delete-job)	N/A（依存性を満たしている）
FDP_ACC.1(in-job)	FDP_ACF.1	FDP_ACF.1(in-job)	N/A（依存性を満たしている）
FDP_ACF.1(in-job)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(in-job) FMT_MSA.3(delete-job)	N/A（依存性を満たしている）
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	N/A（依存性を満たしている）

機能要件	CC で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
FDP_RIP.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FPT_CIP_EXP.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FCS_COP.1(h)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 を主張していない理由： 暗号鍵は RAM 上に生成され電源を切ると消える。また暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FPT_PHP.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FTP_ITC.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FCS_COP.1(n)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 を主張していない理由： 暗号鍵は RAM 上に生成され電源を切ると消える。また暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1(n) FCS_COP.1(h)	FCS_CKM.4 を主張していない理由： 暗号鍵は RAM 上に生成され電源を切ると消える。また暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 を主張していない理由： 暗号鍵は RAM 上に生成され電源を切ると消える。また暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FPT_TST.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A（依存性を満たしている）
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A（依存性を満たしている）
FPT_STM.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A（依存性を満たしている）
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A（依存性を満たしている）
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A（依存性を満たしている）
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A（依存性を満たしている）
FIA_SOS.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）
FMT_MTD.1(user-mgt)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A（依存性を満たしている）
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A（依存性を満たしている）
FMT_MTD.1(device-mgt)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A（依存性を満たしている）
FMT_SMF.1	No dependencies.	No dependencies.	N/A（依存性の要求なし）

6.4 Security assurance requirements rationale

This Protection Profile has been developed for 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 are 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 Summary specification

この章では、TOE 要約仕様を記述する。

7.1 ユーザー認証機能

- **対応する機能要件： FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1, FIA_USB.1, FIA_AFL.1, FTA_SSL.3(lui), FTA_SSL.3(rui)**

TOE は、正規のユーザーを識別認証するために、ユーザーが操作パネルやリモート UI においてデジタル複合機を操作する前にユーザーの識別認証を要求する。但し、プリントジョブ、ファクスジョブ、Iファクスジョブの投入は許可している。[**FIA_UAU.1, FIA_UID.1**]

ユーザー認証は、以下の2種類の認証方式をサポートする。

- 外部認証方式

ユーザー認証サーバーに登録されているユーザー情報を利用する認証方式。例えば、ユーザー認証サーバーには、Kerberos 認証方式の Active Directory サーバーや LDAP 認証方式の LDAP サーバーが該当する。

- 内部認証方式

デバイスに登録されているユーザー情報を利用する認証方式。

TOE はユーザー認証として、ユーザー名・パスワード・認証先であるログイン先の入力を要求して、指定したログイン先にてユーザー名・パスワードが合致した場合のみユーザーを識別認証する。なおパスワード入力の際のパスワードテキストエリアは、*で表示する。[**FIA_UAU.7**]

TOE は、ユーザーの識別認証に成功すると、ユーザーごとに Access Control Token(以後 ACT)を発行する。

ACT とは、ユーザー名やロールに加えて、ユーザーのロールごとに設定されたアプリケーション機能へのアクセス権が含まれたオブジェクトである。[**FIA_ATD.1, FIA_USB.1**]

TOE は、不正なログイン試行を減らすために以下のロックアウト機能を提供する。[**FIA_AFL.1**]

- 設定したロックアウトの許容回数に達した場合は該当ユーザーに対してロックアウトさせる。ロックアウトの許容回数は、1～10 回から選択できる。(初期値は 3 回)
- 設定したロックアウト時間中は、該当ユーザーのログインを認めない。ロックアウト時間は 1-60 分から選択できる。(初期値は 3 分)

TOE は、操作パネルやリモート UI を一定時間操作しない状態が経過するとログアウトさせる。[**FTA_SSL.3(lui), FTA_SSL.3(rui)**]

- 操作パネルを操作しない状態が、オートクリア機能にて設定されたタイムアウト時間の経過。

10 秒-9 分から選択できる。(初期値は 2 分)

- リモート UI を操作しない状態が、15 分間経過。

7.2 ジョブ実行アクセス制御機能

- **対応する機能要件： FDP_ACC.1(exec-job), FDP_ACF.1(exec-job), FMT_MSA.1(exec-job), FMT_MSA.3(exec-job), FMT_SMF.1**

TOE は、識別認証されたユーザーに発行された ACT の内容に応じて、UI 毎にジョブ実行アクセス制御機能を提供する。ユーザーに発行される ACT のロールの問い合わせ、改変、削除、追加は U.ADMINISTRATOR のみに限定される。このジョブ実行アクセス制御に対する、制御対象の属性は各機能そのものであり、常に固定である。

操作パネルの場合のジョブ実行アクセス制御は、ACT のロールに基づく「アプリケーション制限」の属性値に応じてジョブ実行を許可して、それ以外はアクセスを拒否する。

リモートUIの場合のジョブ実行アクセス制御は、ACTのロールの属性値に応じてジョブの実行を拒否して、それ以外はアクセスを許可する。

また、U.ADMINISTRATOR は、すべてのジョブ実行が可能である。

Table 32—ジョブ実行のアクセス制御ポリシー

UI 種別	制御対象	条件	操作
操作パネル	「セキュアプリント」の Pointer	U.USER のロールが「セキュアプリント」を許可されたロールである	制御対象を活性化することで実行可能
	「コピー」の Pointer	U.USER のロールが「コピー」を許可されたロールである	制御対象を活性化することで実行可能
	「スキャンして送信」の Pointer	U.USER のロールが「スキャンして送信」を許可されたロールである	制御対象を活性化することで実行可能
	「ファクス」の Pointer	U.USER のロールが「スキャンして送信」を許可されたロールである	制御対象を活性化することで実行可能
	「受信トレイ」の Pointer	U.USER のロールが「保存ファイルの利用」を許可されたロールである	制御対象を活性化することで実行可能
	「保存ファイルの利用」の Pointer	U.USER のロールが「保存ファイルの利用」を許可されたロールである	制御対象を活性化することで実行可能
	「スキャンして保存」の Pointer	U.USER のロールが「スキャンして保存」を許可されたロールである	制御対象を活性化することで実行可能
リモートUI	「受信/保存ファイルの利用」の Pointer	U.USERのロールがAdministratorロール以外	実行不可

7.3 投入ジョブアクセス制御機能

TOE は、ユーザーが投入したプリント/コピー/スキャン/FAX 等の投入ジョブに対して以下のアクセス制御

のセキュリティ機能を提供する。

7.3.1 ジョブのキャンセル機能

- **対応する機能要件:FDP_ACC.1(delete-job), FDP_ACF.1(delete-job), FMT_MSA.1(delete-job) , FMT_MSA.3(delete-job), FMT_SMF.1**

TOE は、コピー/プリント/スキャン/ファクス送信のジョブを以下の方法でキャンセルできる。これらのジョブのユーザー名は投入ジョブ生成時にそのジョブを生成したユーザー名で初期化されている。

- U.NORMAL は、自分のジョブの削除が可能
- U.ADMINISTRATOR は、すべてのジョブのリストを表示し、任意のジョブの削除が可能

ジョブのキャンセルに伴い、ジョブに付属する属性値も削除される。

7.3.2 ジョブ中の電子文書へのアクセス制御機能

- **対応する機能要件:FDP_ACC.1(in-job), FDP_ACF.1(in-job), FMT_MSA.1(delete-job), FMT_MSA.3(delete-job), FMT_SMF.1**

TOE は、それぞれのジョブ中の電子文書に対して以下のアクセス制御を提供する。これらのジョブのユーザー名は投入ジョブ生成時にそのジョブを生成したユーザー名で初期化されている。

「コピー/スキャン/ファクス送信のジョブ中の電子文書へのアクセス制御機能」

- TOE は、コピーのジョブ中の電子文書に対して誰も参照することができない。
  ただし、所有者および U.ADMINISTRATOR は、割込/優先プリントを行うことができる。
- TOE は、スキャン/ファクス送信のジョブ中の電子文書に対して、7.3.3「送信ジョブ一時保存機能」の場合を除き、誰も参照することができない。

「プリントジョブ中の電子文書へのアクセス制御機能」

TOE は、暗証番号を付与されたプリントジョブが投入されると、そのままプリントせずに一時保存する。更に、プリントジョブに付与されたユーザー名でそのプリントジョブの所有者を判断し、以下のアクセス制御を実現している。

U.USER は、一時保存したプリントジョブの電子文書に対して、自身のユーザー名とプリントジョブのユーザー名が一致した場合に、以下の操作が可能、

- プリントする。
- プリントの優先度を変更する。
- 削除する。

但し、プリントする場合は、プリントジョブの電子文書に付与された暗証番号と、操作パネルにて入力された暗証番号が一致する必要がある。

U.ADMINISTRATOR は、すべての一時保存したプリントジョブの電子文書のリストを表示し、それに対して、以下の操作が可能、

- ジョブの削除する。

「ファクス受信ジョブの電子文書へのアクセス制御機能」

TOE は、受信したファクス/ I ファクス受信ジョブの電子文書をそのままプリントせず、一旦ファイル保存する機能を有する。これらの電子文書が保存される際には、必ずシステムボックスに保存されるため、システムボックスへのアクセス制御がそのまま電子文書のアクセス制御に適用される。システムボックスの電子文書を他人に操作されないように、システムボックスに対して事前に 7 桁の暗証番号を設定することができる。システムボックスの暗証番号の初期化、登録、変更は U.ADMINISTRATOR に限定されるため、電子文書にアクセス可能なユーザーは U.ADMINISTRATOR のみである。したがって、TOE は U.ADMINISTRATOR を保存された電子文書の所有者と判断し、U.NORMAL が電子文書のプリントや送信、削除をできないようにアクセス制御を実現している。

U.ADMINISTRATOR は、操作パネルからアクセスする場合、暗証番号を入力しなくとも、電子文書に対して以下の操作が可能、

- プリントする。
- 送信する。
- 削除する。

U.ADMINISTRATOR は、リモート UI からアクセスする場合、システムボックスに対して事前に設定された暗証番号と、システムボックス操作時に入力された暗証番号が一致した場合のみ、以下の操作が可能、

- プリントする。
- 送信する。
- 削除する。

「ユーザーボックスの電子文書へのアクセス制御機能」

TOE は、コピー/スキャン/送信ジョブの電子文書を、ユーザーボックスに保存する機能を提供する。これらの電子文書を操作する際には、ユーザーボックスへのアクセス制御が適用される。

それぞれのユーザーボックスに対して事前に 7 桁の暗証番号を設定することができる。

ボックスに電子文書を保存する際は暗証番号の入力は不要であり、TOE は正しい暗証番号を入力した U.USER を保存された電子文書の所有者と判断し、アクセス制御を実現している。

U.NORMAL は、ユーザーボックスに事前に設定された暗証番号と、ユーザーボックス操作時に入力された暗証番号が一致した場合のみ、ユーザーボックス内の電子文書に対して以下の操作が可能、

- プリントする。
- プリント設定を変更する。
- 削除する。

U.ADMINISTRATOR は、操作パネルからアクセスする場合、暗証番号を入力しなくとも、電子文書に対して以下の操作が可能、

- プリントする。
- プリント設定を変更する。
- 削除する。

U.ADMINISTRATOR は、リモート UI からアクセスする場合、電子文書に対して、事前に設定された暗証番号と、ボックス操作時に入力された暗証番号が一致した場合のみ、以下の操作が可能、

- プリントする。
- プリント設定を変更する。
- 削除する。

【ボックス暗証番号】
ボックスにアクセスするための暗証番号の登録、変更ができる権限を Administrator ロールが割り当てられた U.ADMINISTRATOR にのみ与える。ただし、自身が利用するボックスの暗証番号に関しては、U.NORMAL でも変更できる。

7.3.3 送信ジョブ一時保存機能

- **対応する機能要件： FDP_ACC.1(in-job), FDP_ACF.1(in-job), FDP_ACC.1(delete-job), FDP_ACF.1(delete-job)**

送信ジョブには、FAX 送信とスキャンの 2 種類があり、それぞれの送信ジョブには一時保存するための送信ジョブ一時保存機能として、「タイマー送信」と「プレビュー」がある。

「タイマー送信」

TOE は、タイマー送信の設定がされた送信ジョブが投入されると、そのまま送信せずに設定された時刻まで一時保存する。

U.NORMAL は、一時保存した送信ジョブに対して、自身のユーザー名と送信ジョブのユーザー名が一致した場合に、以下の操作が可能、

- 宛先を変更する

U.ADMINISTRATOR は、すべての一時保存した送信ジョブに対して、以下の操作が可能、

- 宛先を変更する

「プレビュー」

TOE は、プレビューの設定がされた送信ジョブが投入されると、すぐに送信せずにジョブ内容をプレビューして確認した後に送信できる。

U.USER は、一時保存した送信ジョブに対して、自身のユーザー名と送信ジョブのユーザー名が一致した場合に、以下の操作が可能、

- 電子文書内容のプレビュー
- 電子文書内容のページ削除
- ジョブの中止

7.4 受信ジョブ転送機能

- **対応する機能要件：FPT_FDI_EXP.1**

TOE は物理的に受信したデータを直接他の PC・サーバーに転送できる構造となっておらず、受信したジョブの LAN への転送ができないように制御されている。

7.5 HDD データ完全消去機能

- **対応する機能要件：FDP_RIP.1**

TOE が電子文書やテンポラリイメージファイルを HDD から削除する際は、その HDD 領域を無意味なデータで上書きすることにより電子文書やテンポラリイメージファイルの残存情報の完全消去を実施する。

完全消去には以下の方法から1種類選択できる。

- DoD 方式で上書き
- 3 回ランダムデータで上書き
- 1 回ランダムデータで上書き
- 1 回 NULL データで上書き

またこの機能は、以下のタイミングに動作する。

- ジョブ処理中に HDD 内に一時的に保存されるテンポラリイメージファイルを、ジョブ処理中もしくはジョブ処理後に HDD から完全消去する。
- ボックスに保存された電子文書の削除後に HDD から完全消去する。
- 突然の電源遮断により完全消去できなかった残存情報を、TOE の起動時に HDD から完全消去する。

7.6 HDD 暗号化機能

- **対応する機能要件：FPT_CIP_EXP.1**

TOE の「HDD データ暗号化ボード」は、以下のセキュリティ機能を提供する。

暗号化/復号機能と本体識別認証機能によって、HDD に格納されるユーザーデータおよび TSF データの機密性と完全性を確保する。

7.6.1 暗号化/復号機能

- **対応する機能要件：FCS_COP.1(h)**

TOE は、HDD に格納されるユーザーデータおよび TSF データの機密性を確保するために、次の暗号操作を行い HDD に格納されるデータ全体を暗号化する。

- HDD へ書き込まれるデータを暗号化する。
- HDD から読み出されるデータを復号する。

暗号操作に用いる暗号アルゴリズム、暗号鍵は以下のとおりである。

- FIPS PUB 197 に従った「AES アルゴリズム」
- 鍵長が「256 ビット」の暗号鍵

7.6.2 暗号鍵管理機能

- **対応する機能要件：FCS_CKM.1**

TOE は、次の仕様に基づき、HDD データ暗号化機能で使用する暗号鍵を生成する。

- 暗号鍵を生成するアルゴリズムは、「FIPS PUB 186-2 に基づく暗号鍵生成アルゴリズム」
- 生成される暗号鍵の鍵長は「256 ビット」

暗号鍵の管理は以下のように行う。

- 起動時に、TOE は FlashROM に格納された Seed 情報を読み出して暗号鍵を生成する
- TOE は暗号鍵を生成した後、RAM 上に格納する

なお、Seed を暗号ボードから取得する手段は存在しない。また、暗号鍵は揮発性メモリーである RAM 上に保持されるため、電源 OFF により消失する。

7.6.3 本体識別認証機能

- **対応する機能要件：FPT_PHP.1**

HDD データ暗号化ボードは、毎回起動時にデジタル複合機本体を識別し、正しいデジタル複合機本体だった場合のみ HDD アクセスを許可する。この機能により、HDD データ暗号化ボードと HDD をセットで他のデジタル複合機本体に接続しても、HDD データにアクセスすることができない。

【認証 ID の登録】

HDD データ暗号化ボードは、ボード取り付け時に、デジタル複合機本体から本体認証 ID を受取り、FlashROM に保存する。

【識別認証の手順】

HDD データ暗号化ボードは起動時に擬似乱数を生成し、チャレンジ用の乱数としてデジタル複合機本体へ渡す。デジタル複合機本体は、本体認証 ID とチャレンジ用の乱数から演算し、そのハッシュ値（SHA-1）をレスポンスとして暗号ボードへ渡す。HDD データ暗号化ボードは、同様の計算を行い、レスポンスの検証を行う。

HDD データ暗号化ボードが正しいデジタル複合機本体に取り付けられていることが確認できない場合、HDD へのアクセスを禁止する。

7.7 LAN データ保護機能

LAN データ保護機能は、送受信先の IT 機器との通信に利用するすべての IP パケットを暗号化/復号する。

7.7.1 IP パケット暗号化機能

- **対応する機能要件：FCS_COP.1(n), FTP_ITC.1**

TOE は、送受信先の IT 機器との通信するユーザーデータおよび TSF データの機密性、完全性の確保のために、すべての IP パケットを IPSec にて暗号化/復号する。

- LAN へ送信する IP パケットの暗号化操作

- LAN から受信する IP パケットの復号操作

暗号操作に用いる暗号アルゴリズム、暗号鍵は以下のとおりである。

- Table 24 に同じ

7.7.2 暗号鍵管理機能

- **対応する機能要件: FCS_CKM.1, FCS_CKM.2**

TOE は、次の仕様に基づき、IP パケット暗号化機能で使用する暗号鍵を生成する。

- 暗号鍵を生成するアルゴリズムは、「FIPS PUB 186-2 に基づく暗号鍵生成アルゴリズム」
- 生成される暗号鍵の鍵長は「128、168、192、256 ビット」

また TOE は、以下の方法にて、IP パケット暗号化機能の暗号鍵を送受信先の IT 機器に転送する。

- SP800-56A の標準に基づいた DH(Diffie Hellman)および ECDH(Elliptic Curve Diffie Hellman)

7.8 自己テスト機能

- **対応する機能要件: FPT_TST.1**

TOE は、起動時に以下の自己テストを実施する。

- 暗号アルゴリズム(AES、3DES)の機能チェック
- 暗号鍵の完全性チェック
- 暗号アルゴリズムの実行コードの完全性チェック

7.9 監査ログ機能

- **対応する機能要件: FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4**

TOE は、以下のイベントが生じた際にログを生成する。

- スタートアップ
- シャットダウン
- ジョブ完了
- ユーザー認証の成功/失敗
- ログアウト
- デバイス管理機能の利用
- ユーザー管理機能の利用
- 時刻の変更

- IPSec のコネクション確立失敗

ログの項目は以下である。日時情報は TOE から提供される。ログに記録される日時情報は、TOE から提供される。TOE の日時情報は、管理機能の利用、もしくはタイムサーバーから正確な日時を取得して時刻同期することで設定される。

- 日時、ユーザー名、イベント種別、結果(成功/失敗)

但し、以下のイベントの際には以下の項目も追加する。

- ジョブ完了のログには、ジョブ種
- 認証失敗のログには、認証試行したユーザー名

また、リモート UI から監査ログのエクスポートを実施し、監査記録を読み出す機能を提供する。機能を利用できるのは U.ADMINISTRATOR のみである。

U.ADMINISTRATOR 以外のユーザーはリモート UI から TOE にログインしても監査ログのエクスポート機能を利用することはできない

リモート UI で TOE にアクセスし、「監査ログのクリア」メニューから監査記録を削除する機能を提供する。機能を利用できるのは U.ADMINISTRATOR のみである。

U.ADMINISTRATOR 以外のユーザーはリモート UI から TOE にログインしても「監査ログのクリア機能」を利用することはできず、不正な改変を防止している

監査記録は最大2万件が保持されており、満杯になった場合は最も古くに格納された監査記録を上書きする。

7.10 管理機能

7.10.1 ユーザー管理機能

- **対応する機能要件: FIA_SOS.1 , FMT_MTD.1(user-mgt) , FMT_MSA.1(exec-job) FMT_MSA.1(delete-job), FMT_MSA.3(delete-job) ,FMT_SMR.1, FMT_SMF.1**

TOE は、Administrator ロールが割り当てられた U.ADMINISTRATOR のみにユーザー、ロール、アクセス制御情報、ボックス暗証番号の登録、変更、削除のできるユーザー管理機能を制限する。但し、自分のパスワード、自分の利用するボックスの暗証番号に関しては、U.NORMAL でも変更できる。

【ユーザー、ロール、アクセス制御情報の登録、変更、削除】

ユーザーの新規登録は、ユーザー名・パスワードを設定して、ロールを割り当てることで登録する。また既存ユーザーのパスワード・ロールの変更や、既存ユーザーを削除することもできる。ユーザーが設定したパスワードはパスワードポリシーに合致しているかどうかチェックされる。

ロールには、あらかじめ「ベースロール」と呼ばれる、”Administrator”, ”Power User”, ”General User”, ”Limited User”, ”Guest User”の 5 種類のロールが存在している。「ベースロール」以外の新規の「カスタムロール」を作成する場合には、”Guest User”ロールを除く 4 種類の「ベースロール」を複製編集して、登録することができる。

Administrator ロールとは、「ベースロール」が”Administrator”であるロールで、管理権限を有する。

「ベースロール」の初期値は、”Guest User”を除く 4 種類の「ベースロール」から初期値を変更できる。

各ジョブ実行の許可/禁止を設定するアクセス制御情報は、ロールに基づく「アプリケーション制限」の属性値にて設定されている。「ベースロール」の「アプリケーション制限」の初期値は変更できないが、「カス

タムロール」の「アプリケーション制限」の初期値を変更できる。

【ロール種別】

ロール種別は、U.ADMINISTRATOR と U.NORMAL の 2 種類に大別され、維持している。

- U.ADMINISTRATOR

Administrator ロールが割り当てられた管理権限を有するユーザー。

- U.NORMAL

Guest User ロール、Administrator ロール以外のロールが割り当てられた一般ユーザー。

7.10.2 デバイス管理機能

- **対応する機能要件: FMT_MTD.1(device-mgt), FMT_SMF.1**

TOE は、セキュリティ機能を有効に機能させるべく、Table 27 のような各種デバイス管理機能の設定を U.ADMINISTRATOR のみに限定する。

更に、以下の設定機能を提供する。

【パスワードポリシーの設定】

堅牢なパスワードの設定をユーザーに求めるために、以下のようなパスワードの品質を提供する。

- 4 文字以上 32 文字以下のパスワード長
- 3 文字以上連続する文字列を含めない
- 英大文字(A～Z)を 1 文字以上含める
- 英小文字(a～z)を 1 文字以上含める
- 数字(0～9)を 1 文字以上含める
- アルファベット以外の文字(^-@[]:;,./¥!”#$%&’()=~|{`+*}_?><)を 1 文字以上含める
- 使用可能文字

  制御文字以外の全ての文字

【ロックアウトポリシーの設定】

ロックアウト許容回数とロックアウト時間の設定ができる。

- ロックアウト許容回数

1～10 回から選択できる。(初期値は 3 回)

- ロックアウト時間

1-60 分から選択できる。(初期値は 3 分)

以上