Xerox D95/D110/D125 Copier/Printer
セキュリティターゲット

Version 1.1.4

September 2018

― 更新履歴 ―

№	更新日	バージョン	更新内容
1	2017 年 8 月 18 日	1.0.0	初版
2	2017 年 10 月 12 日	1.0.1	誤記修正
3	2018 年 1 月 26 日	1.0.2	誤記修正
4	2018 年 2 月 15 日	1.0.3	誤記修正
5	2018 年 6 月 14 日	1.0.4	誤記修正
6	2018 年 7 月 3 日	1.0.5	誤記修正
7	2018 年 7 月 10 日	1.0.6	誤記修正
8	2018 年 8 月 7 日	1.0.7	誤記修正
9	2018 年 8 月 28 日	1.0.8	誤記修正
10	2018 年 8 月 31 日	1.0.9	誤記修正
11	2018 年 9 月 4 日	1.1.0	誤記修正
12	2018 年 9 月 5 日	1.1.1	誤記修正
13	2018 年 9 月 14 日	1.1.2	誤記修正
14	2018 年 9 月 19 日	1.1.3	誤記修正
15	2018 年 9 月 20 日	1.1.4	誤記修正

－ 目次 －

1. ST 概説 (ST Introduction) 1

1.1. ST 参照 (ST Reference) 1

1.2. TOE 参照 (TOE Reference) 1

1.3. TOE 概要 (TOE Overview) 1

1.3.1. TOE 種別および主要セキュリティ機能 (TOE Type and Major Security Features) ... 1

1.3.2. TOE 利用環境 (Environment Assumptions) 4

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成 (Required Non-TOE Hardware and Software) 5

1.4. TOE 記述 (TOE Description) 6

1.4.1. TOE 関連の利用者役割 (User Assumptions) 6

1.4.2. TOE の論理的範囲 (Logical Scope and Boundary) 6

1.4.3. TOE の物理的範囲 (Physical Scope and Boundary) 14

1.4.4. ガイダンス (Guidance) 15

2. 適合主張 (Conformance Claim) 16

2.1. CC 適合主張 (CC Conformance Claim) 16

2.2. PP 主張、パッケージ主張 (PP claim, Package Claim) 16

2.2.1. PP 主張 (PP Claim) 16

2.2.2. パッケージ主張 (Package Claim) 16

2.2.3. 適合根拠 (Conformance Rational) 17

3. セキュリティ課題定義 (Security Problem Definition) 19

3.1. 脅威 (Threats) 19

3.1.1. TOE 資産 (Assets Protected by TOE) 19

3.1.2. 脅威エージェント (Threats agents) 21

3.1.3. 脅威 (Threats) 22

3.2. 組織のセキュリティ方針 (Organizational Security Policies) 22

3.3. 前提条件 (Assumptions) 23

4. セキュリティ対策方針 (Security Objectives) 24

4.1. TOE のセキュリティ対策方針 (Security Objectives for the TOE) 24

4.2. 運用環境のセキュリティ対策方針 (Security Objectives for the Environment) 25

4.3. セキュリティ対策方針根拠 (Security Objectives Rationale) 25

5. 拡張コンポーネント定義 (Extended Components Definition) 30

5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces 30

6. セキュリティ要件 (Security Requirements) 32

6.1. セキュリティ機能要件 (Security Functional Requirements)..... 35
6.1.1. Class FAU: Security Audit..... 38
6.1.2. Class FCS: Cryptographic Support..... 45
6.1.3. Class FDP: User Data Protection..... 46
6.1.4. Class FIA: Identification and Authentication..... 60
6.1.5. Class FMT: Security Management..... 63
6.1.6. Class FPT: Protection of the TSF..... 80
6.1.7. Class FTA: TOE Access..... 81
6.1.8. Class FTP: Trusted Path/Channels..... 82

6.2. セキュリティ保証要件 (Security Assurance Requirements)..... 83

6.3. セキュリティ要件根拠 (Security Requirement Rationale) 84
6.3.1. セキュリティ機能要件根拠 (Security Functional Requirements Rationale) 84
6.3.2. 依存性の検証 (Dependencies of Security Functional Requirements) 91
6.3.3. セキュリティ保証要件根拠 (Security Assurance Requirements Rationale) 95

7. TOE 要約仕様 (TOE Summary Specification).....96

7.1. セキュリティ機能 (Security Functions) 96
7.1.1. ハードディスク蓄積データ上書き消去機能(TSF_IOW)..... 97
7.1.2. ハードディスク蓄積データ暗号化機能(TSF_CIPHER) 98
7.1.3. ユーザー認証機能(TSF_USER_AUTH)..... 98
7.1.4. システム管理者セキュリティ管理機能 (TSF_FMT) 103
7.1.5. カストマーエンジニア操作制限機能 (TSF_CE_LIMIT)..... 104
7.1.6. セキュリティ監査ログ機能(TSF_FAU)..... 105
7.1.7. 内部ネットワークデータ保護機能(TSF_NET_PROT) 107
7.1.8. インフォメーションフローセキュリティ機能(TSF_INF_FLOW)..... 109
7.1.9. 自己テスト機能(TSF_S_TEST)..... 110

8. ST 略語・用語 (Acronyms And Terminology) 111

8.1. 略語 (Acronyms) 111

8.2. 用語 (Terminology) 112

9. 参考資料 (References) 116

― 図表目次 ―

図 1 TOE の想定する利用環境 5
図 2 MFD 内の各ユニットと TOE の論理的範囲 7
図 3 プライベートプリントと親展ボックスの認証フロー 10
図 4 MFD 内の各ユニットと TOE の物理的範囲 14
図 5 保護資産と保護対象外資産 21

Table 1 TOE が提供する機能と機能種別 2
Table 2 TOE が想定する利用者役割 6
Table 3 TOE の基本機能 8
Table 4 利用者データに関する保護資産 19
Table 5 TSF データに関する保護資産 20
Table 6 その他の保護資産 20
Table 7 利用者データ と TSF データに対する脅威 22
Table 8 組織のセキュリティ方針 22
Table 9 前提条件 23
Table 10 TOE セキュリティ対策方針 24
Table 11 運用環境のセキュリティ対策方針 25
Table 12 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針及び前提条件 26
Table 13 セキュリティ課題定義に対応するセキュリティ対策方針根拠 26
Table 14 機能要件一覧 35
Table 15 Auditable Events of TOE and Individually Defined Auditable Events 38
Table 16 Common Access Control SFP 46
Table 17 SFR Package attributes 47
Table 18 Function Access Control SFP 48
Table 19 PRT Access Control SFP 50
Table 20 SCN Access Control SFP 50
Table 21 CPY Access Control SFP 51
Table 22 DSR Access Control SFP 52
Table 23 List of Security Functions 64
Table 24 Security Attributes and Authorized Roles 65
Table 25 Security Attributes and Authorized Roles(Function Access) 66
Table 26 Security Attributes and Authorized Roles(PRT) 67
Table 27 Security Attributes and Authorized Roles(SCN) 68
Table 28 Security Attributes and Authorized Roles(DSR) 69
Table 29 Initialization property 70
Table 30 Initialization property 72
Table 31 Operation of TSF Data 74
Table 32 Operation of TSF Data 76
Table 33 Security Management Functions Provided by TSF 76
Table 34 セキュリティ保証要件 83

Table 35 セキュリティ機能要件とセキュリティ対策方針の対応関係 84
Table 36 セキュリティ対策方針によるセキュリティ機能要件根拠 86
Table 37 セキュリティ機能要件コンポーネントの依存性 91
Table 38 TOE セキュリティ機能とセキュリティ機能要件の対応関係 96
Table 39 セキュリティ属性の管理 100
Table 40 基本機能へのアクセス制御 101
Table 41 利用者データへのアクセス制御 101
Table 42 監査ログのデータ詳細 105

1. ST 概説 (ST Introduction)

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1. ST 参照 (ST Reference)

本節では ST の識別情報を記述する。

タイトル:	Xerox D95/D110/D125 Copier/Printer セキュリティターゲット
バージョン:	V 1.1.4
発行日:	2018 年 9 月 20 日
作成者:	富士ゼロックス株式会社

1.2. TOE 参照 (TOE Reference)

本節では TOE の識別情報を記述する。
TOE は Xerox D95 Copier/Printer、 Xerox D110 Copier/Printer、Xerox D125 Copier/Printer として動作する。TOE 名は、まとめて下記に統合する。

TOE 名:	Xerox D95/D110/D125 Copier/Printer
TOE のバージョン:	Controller+PS ROM Ver. 1.204.17
開発者:	富士ゼロックス株式会社

対象の機種は下記である。
Xerox D95:
Controller+PS ROM Ver. 1.204.17

Xerox D110:
Controller+PS ROM Ver. 1.204.17

Xerox D125:
Controller+PS ROM Ver. 1.204.17

1.3. TOE 概要 (TOE Overview)

1.3.1. TOE 種別および主要セキュリティ機能 (TOE Type and Major Security Features)

1.3.1.1. TOE の種別 (TOE Type)

本 TOE は IT 製品であり、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能を有するデジタル複合機(Multi-Function Device 略称 MFD)である Xerox D95/D110/D125 Copier/Printer (以降、単に「MFD」と記す)である。 TOE は、MFD 全体の制御、TOE とリモート間の内部ネットワーク上を流れる文書データ、ジョブ情報、TOE 設定データおよびセキュリティ監査ログデータを脅威から保護するための暗号化通信プロトコルによる通信データの保護に対応する製品である。 また MFD によ

り処理された後、内部ハードディスク装置に蓄積される文書データ、利用済み文書データを不正な暴露から保護するための機能も TOE に含まれる。

1.3.1.2. TOE の機能種別（Function Types）

Table1 に TOE が提供する製品の機能種別を記述する。

Table 1 TOE が提供する機能と機能種別

機能種別	TOE が提供する機能
基本機能	・操作パネル機能 ・コピー機能 ・プリンター機能 ・スキャナー機能 ・ネットワークスキャン機能 ・CWIS 機能
セキュリティ機能	・ハードディスク蓄積データ上書き消去機能 ・ハードディスク蓄積データ暗号化機能 ・ユーザー認証機能 ・システム管理者セキュリティ管理機能 ・カストマーエンジニア操作制限機能 ・セキュリティ監査ログ機能 ・内部ネットワークデータ保護機能 ・自己テスト機能 ・インフォメーションフローセキュリティ機能

- プリンター機能を使用するためには、TOE 外の一般利用者クライアントおよびシステム管理者クライアントにプリンタードライバがインストールされていることが必要である。
- ユーザー認証機能には本体認証と外部認証の 2 種類の認証方式があり、設定により TOE はどちらかの認証方式で動作する。
  本 ST 内では、この 2 種類の認証方式で動作が異なる場合は明記される。また、特に明記してない場合は、どちらの認証方式でも同じ動作をすることを意味する。
  外部認証方式には LDAP 認証と Kerberos 認証がある。

注）
- 本 TOE の USB プリント/保存オプションは初期設定で「無効」にしているため評価の構成に含まれていない。従って[Store to USB]と[Media Print]のボタンは操作パネルに現れない。
- 本 TOE では、ガイダンスで PostScript ドライバの利用を禁止しており、プリント機能において、PostScript は評価対象にしていない。
- 親展ボックスには SA，一般利用者が作成する個人親展ボックスと、機械管理者が作成する共有親展ボックスがあるが、本 TOE ではガイダンスで共有親展ボックスの利用を禁止している。

1.3.1.3. TOE の使用法と主要セキュリティ機能 (Usage and Major Security Features of TOE)

TOE の主な使用法を以下に示す。

- コピー機能と操作パネル機能により、操作パネルからの一般利用者の指示に従い、IIT で原稿を読み込み IOT より印刷を行う。 同一原稿の複数部のコピーが指示された場合、IIT で読み込んだ文書データは、一旦 MFD の内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。またコピー蓄積機能として再出力用データの IOT への印刷と同時保存、および再出力用保存が可能である。
- 同一原稿の複数部のコピーが指示された場合、IIT で読み込んだ文書データは、一旦 MFD の内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
- プリンター機能により、利用者クライアントから送信された印刷データをデコンポーズして印刷する。
- CWIS 機能により、MFD に対してスキャナー機能によりスキャンして、親展ボックスに格納された文書データを利用者クライアントから取り出す。
  さらにシステム管理者は、Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う。
- スキャナー機能と操作パネル機能により、操作パネルからの利用者の指示に従い、IIT で原稿を読み込み、MFD の内部ハードディスク装置に作られた親展ボックスに蓄積する。
  蓄積された文書データは、一般的な Web ブラウザを使用して CWIS から取り出すことも可能である。
- ネットワークスキャン機能と操作パネル機能により、操作パネルからの利用者の指示に従い IIT で原稿を読み込み後に MFD に設定されている情報に従って、FTP サーバー、Mail サーバーへ文書データの送信を行う。

TOE は以下のセキュリティ機能を提供する。

(1) ハードディスク蓄積データ上書き消去機能
コピー、プリンターおよびスキャナー等の各機能の動作後、ハードディスク装置に蓄積された利用済みの文書データの上書き消去を行う機能である。

(2) ハードディスク蓄積データ暗号化機能
コピー、プリンターおよびスキャナー等の各機能の動作時や各種機能設定時にハードディスク装置に蓄積される文書データの暗号化を行う機能である。

(3) ユーザー認証機能
許可された特定の利用者だけに TOE の機能を使用する権限を持たせるために、操作パネルまたは一般利用者クライアントの CWIS からユーザーID とユーザーパスワードを入力させて識別認証し、TOE使用のアクセス制御を実施する機能である。

(4) システム管理者セキュリティ管理機能
操作パネルまたはシステム管理者クライアントから、識別および認証されたシステム管理者が、TOE のセキュリティ機能に関する設定の参照および変更をシステム管理者のみが行えるようにする機能である。

(5) カストマーエンジニア操作制限機能
カストマーエンジニアが TOE のセキュリティ機能に関する設定の参照および変更をできなくするシステム管理者の設定機能である。

(6) セキュリティ監査ログ機能
いつ、誰が、どのような作業を行ったかという事象や重要なイベント(例えば障害や構成変更、ユーザー操

作など)を、追跡記録するための機能である。

(7) 内部ネットワークデータ保護機能

内部ネットワーク上に存在する文書データ、ジョブ情報、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護する機能である。

一般的な暗号化通信プロトコル(TLS, IPSec, S/MIME)に対応する。

(8) インフォメーションフローセキュリティ機能

外部インターフェースと内部ネットワーク間における許可されない通信を制限する機能である。

(9) 自己テスト機能

TOE の TSF 実行コードおよび TSF データの完全性を検証するための機能である。

1.3.2. TOE 利用環境 (Environment Assumptions)

本 TOE は、IT 製品として一般的な業務オフィスに、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワークおよび利用者クライアントと接続されて利用される事を想定している。

TOE の想定する利用環境を図 1 に記述する。

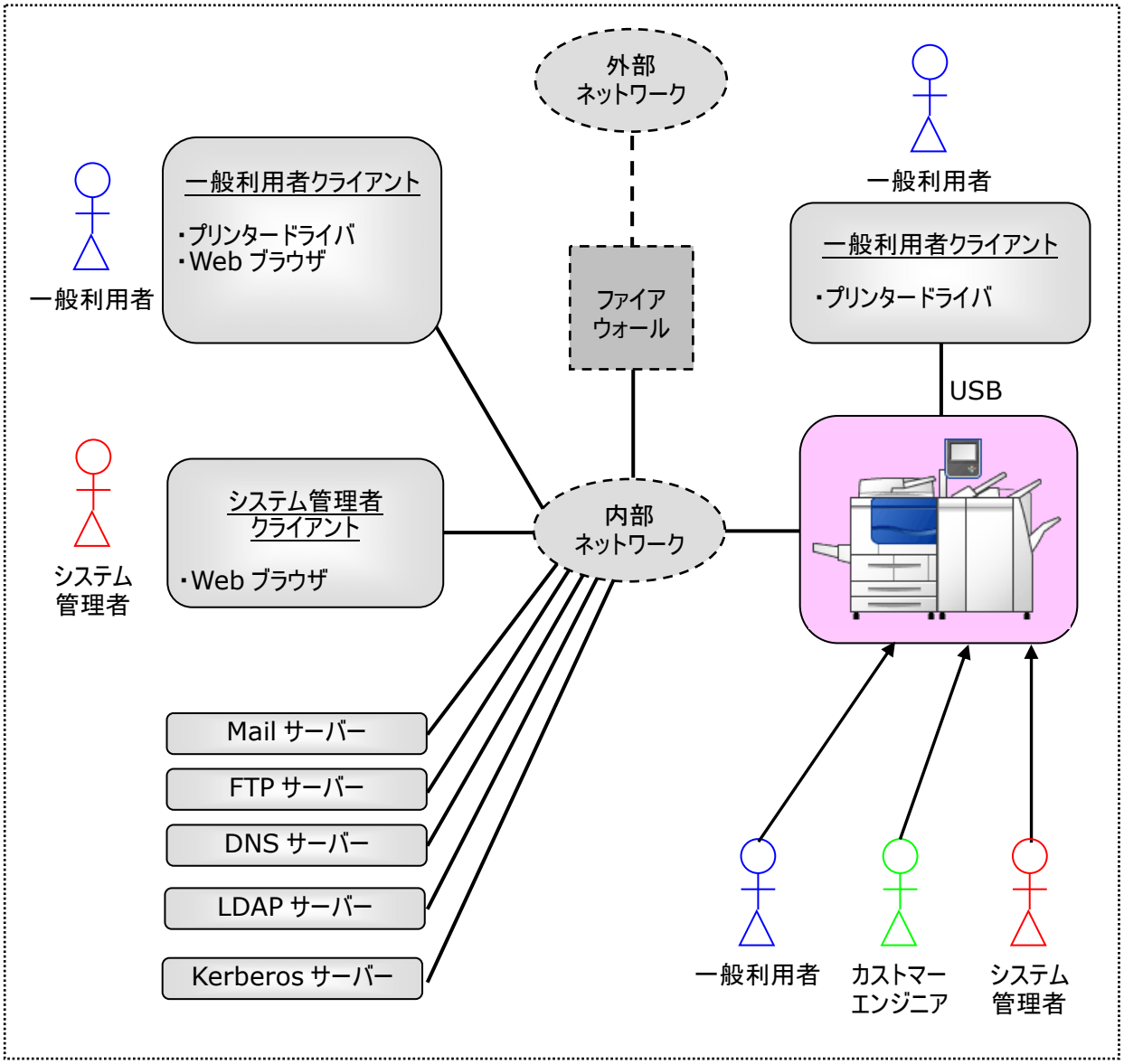

図 1 TOE の想定する利用環境

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成 (Required Non-TOE Hardware and Software)

図-1 に示す利用環境の中で TOE は MFD であり、下記の TOE 以外のハードウェアおよびソフトウェアが存在する。

(1) 一般利用者クライアント
ハードウェアは汎用の PC であり、プリンタードライバがインストールされており、MFD に対して文書データのプリント要求を行うことができる。
また、Web ブラウザを使用して MFD のスキャナー機能によりスキャンした文書データの取り出し要求を行う。
また一般利用者が MFD に登録した親展ボックスのボックス名称、パスワード、アクセス制限、および文書の自動削除指定の設定変更が出来る。
USB でローカル接続されている場合、プリンタードライバがインストールされており、MFD に対して文書データのプリント要求を行うことができる。

(2) システム管理者クライアント
ハードウェアは汎用の PC であり、Web ブラウザを使用して TOE に対して TOE 設定データの参照や変更を行うことができる。

(3) Mail サーバー
ハードウェア/OS は汎用の PC またはサーバーであり、MFD はメールプロトコルを用いて、Mail サーバーと文書データの送受信を行う。

(4) FTP サーバー
ハードウェア/OS は汎用の PC またはサーバーであり、MFD は FTP プロトコルを用いて、FTP サーバーに文書データの送信を行う。

(5) DNS サーバー
ハードウェア/OS は汎用の PC またはサーバーであり、MFD は DNS プロトコルを用いて、DNS サーバーから IP アドレス情報を取得する。

(6) LDAP サーバー
ハードウェア/OS は汎用の PC またはサーバーであり、MFD は LDAP プロトコルを用いて、LDAP サーバーから識別認証情報の取得を行う。また利用者役割としての SA 情報を取得する。

(7) Kerberos サーバー
ハードウェア/OS は汎用の PC またはサーバーであり、MFD は Kerberos プロトコルを用いて、Kerberos サーバーから識別認証情報の取得を行う。

(1)、(2)の一般利用者クライアントとシステム管理者クライアントの OS は Windows 7、Windows 8.1 とする。
(1)において、”PCL6 Driver – 64bit, Xerox User Interface – Microsoft Certified”をプリンタードライバとして使用する。
(6)、(7)の LDAP サーバーと Kerberos サーバーは Windows Active Directory とする。

1.4. TOE 記述 (TOE Description)

本章では、TOE の利用者役割、TOE の論理的範囲、および物理的範囲について記述する。

1.4.1. TOE 関連の利用者役割 (User Assumptions)

本 ST で、TOE に対して想定する利用者役割を Table 2 に記述する。

Table 2 TOE が想定する利用者役割

Designation		PP Definition	補足説明
U.USER		Any authorized User.	利用者に該当する。
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE.	一般利用者に該当する。 TOE が提供するコピー機能、プリンター機能等の TOE 機能の利用者。
	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.	システム管理者(機械管理者と SA)に該当する。 TOE のシステム管理者モードで機器管理を行うための特別な権限を持つ利用者で、TOE の操作パネル、および Web ブラウザを使用して、TOE 機器の動作設定の参照/更新、および TOE セキュリティ機能設定の参照/更新のみを行う利用者。
TOE Owner		A person or organizational entity responsible for protecting TOE assets and establishing related security policies.	組織の管理者に該当する。 TOE を使用して運用する組織の責任者または管理者。
カストマーエンジニア		-	カストマーエンジニア専用のインターフェースを使用して、TOE の機器動作設定を行う者。

1.4.2. TOE の論理的範囲 (Logical Scope and Boundary)

TOE の論理的範囲はプログラムの各機能である。
図 2 に TOE の論理的構成を記述する。

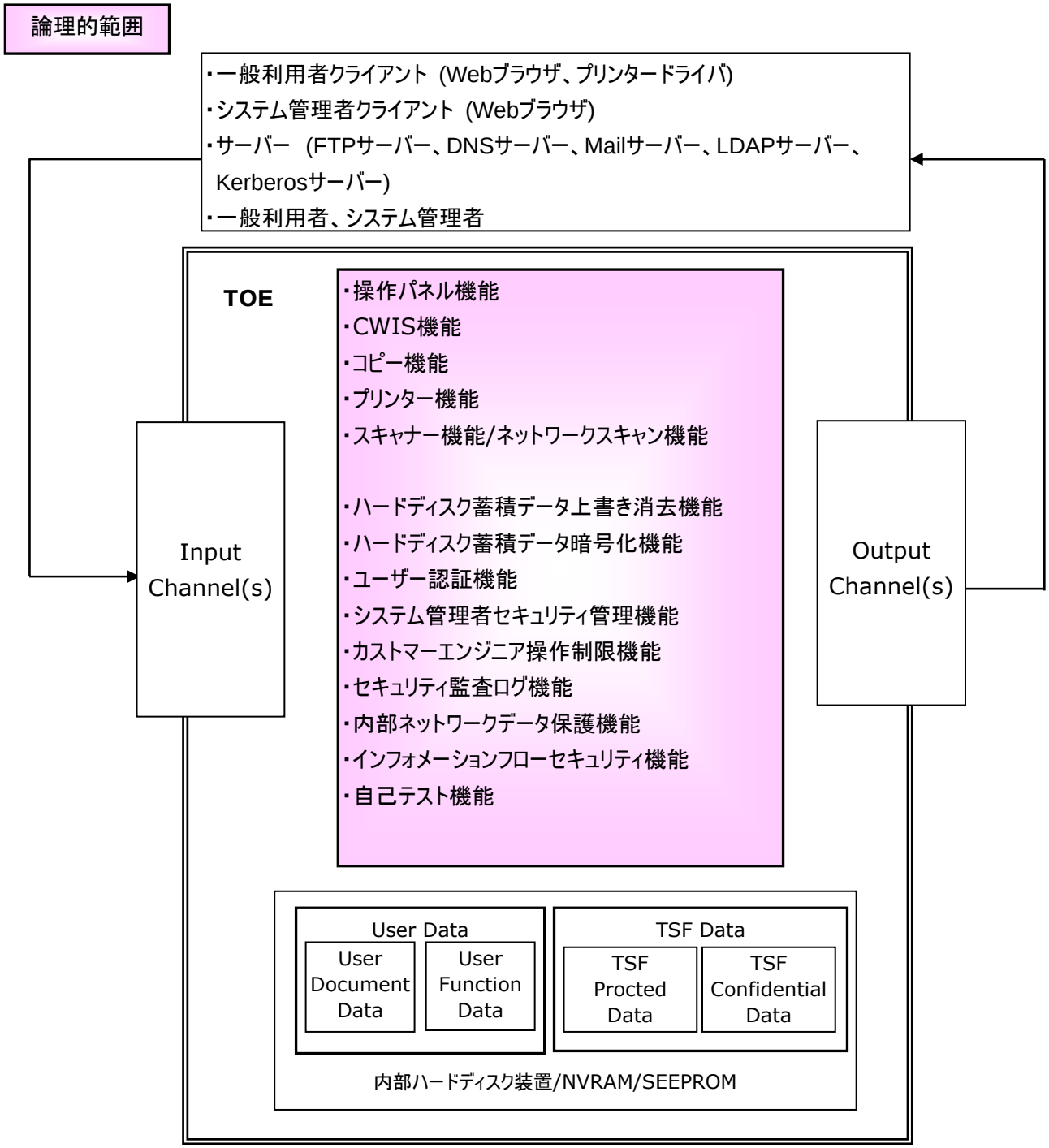

図 2 MFD 内の各ユニットと TOE の論理的範囲

Channel には以下の 4 つのタイプがある。

a) Private Medium Interface

複数の利用者が同時にアクセスすることのできない操作パネルやローカルインターフェース。

b) Shared Medium Interface

複数の利用者が同時にアクセスすることのできるネットワーク等のインターフェース。

c) Original Document Handler

ハードコピーの User Document Data を TOE に転送するメカニズム

d) HardCopy Output Handler

User Document Data をハードコピーで TOE の外に転送するメカニズム

1.4.2.1. TOE が提供する基本機能 (Basic Functions)

TOE は一般利用者に対して、下記 Table 3 のようにコピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能、操作パネル機能および CWIS 機能を提供する。

Table 3 TOE の基本機能

機能	概要
コピー機能	コピー機能は、一般利用者が MFD の操作パネルから指示をすることにより、IIT で原稿を読み取り IOT から印刷を行う機能である。またコピー蓄積機能として再出力用データの IOT への印刷と同時保存、および再出力用保存が可能である。また保存された親展ボックス内のコピー文書データは、ページ削除/合紙挿入/文書合成の編集が可能である。 同一原稿の複数部のコピーが指示された場合、IIT で読み込んだ文書データは、一旦 MFD の内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
プリンター機能	プリンター機能は、一般利用者が一般利用者クライアントからプリント指示をすると印刷データが MFD へ送信され、MFD は印刷データを解析しビットマップデータに変換(デコンポーズ)して、IOT から印刷を行う機能である。 印刷データはプリンタードライバを介して PDL に変換して送る方法と CWIS から文書ファイルを直接指定して送る方法がある。 またプリンター機能には、直接 IOT から印刷を行う通常プリントと、ビットマップデータを一時的に内部ハードディスク装置に蓄積して、一般利用者が操作パネルから印刷指示をした時点で IOT から印刷を行う蓄積プリントがある。
スキャナー機能、 ネットワークスキャン機能	スキャナー機能は、一般利用者が MFD の操作パネルから指示をすることにより、IIT で原稿を読み取り、文書データとして内部ハードディスク装置に蓄積する機能である。 蓄積された文書データは、一般利用者が一般利用者クライアントを使って CWIS 機能により取り出すことができる。 またネットワークスキャン機能は MFD に設定されている情報に従って、一般利用者が MFD の操作パネルから原稿を読み取り後に自動的に一般利用者クライアント、FTP サーバー、Mail サーバーへ転送する機能である。
操作パネル機能	操作パネル機能は一般利用者、システム管理者、カストマーエンジニアが MFD の機能を利用するための操作に必要なユーザーインターフェース機能である。
CWIS 機能	CWIS 機能は、一般利用者が一般利用者クライアントの Web ブラウザを介して操作する機能である。システム管理者は、システム管理者クライアントの Web ブラウザからシステム管理者の ID とパスワードを入力して MFD に認証されると、システム管理者セキュリティ管理機能により TOE 設定データにアクセスしてデータを更新することが出来る。

1.4.2.2. TOE が提供するセキュリティ機能 (Security Functions)

本 TOE は利用者に対して、以下のセキュリティ機能を提供する。

(1) ハードディスク蓄積データ上書き消去機能

内部ハードディスク装置に蓄積される文書データは、利用が終了して削除される際に管理情報だけが削除され、蓄積された文書データ自体は削除されない。 このため内部ハードディスク装置上に利用済み文書データとして残存した状態になる。 この問題を解決するために、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能のジョブ完了後に、内部ハードディスク装置に蓄積された利用済み文書データに対して、上書き消去を行う。

上記に加えて、システム管理者が設定した時刻またはマニュアル指示で蓄積文書を削除して上書き消去する機能(On Demand Overwrite)も提供する。

(2) ハードディスク蓄積データ暗号化機能

内部ハードディスク装置には親展ボックス内の文書データのように電源がオフされても残り続けるデータがある。この問題を解決するために、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能動作時や各種機能設定時に内部ハードディスク装置に蓄積される文書データの暗号化を行う。

(3) ユーザー認証機能

TOE は、許可された特定の利用者だけに MFD の機能を使用する権限を持たせるために、操作パネル、利用者クライアントの CWIS、プリンタードライバからユーザーID とユーザーパスワードを入力させて識別認証する機能を有する。

認証が成功した利用者のみが下記の機能を使用可能となる。

a) 本体操作パネルで制御される機能
   コピー機能、スキャン機能、ネットワークスキャン機能、親展ボックス操作機能、プリンター機能(プリンタードライバでの認証管理の設定が条件であり印刷時に操作パネルで認証する)
b) CWIS で制御される機能
   機械状態の表示、ジョブ状態・履歴の表示、親展ボックスからの文書データ取出し機能、ファイル指定によるプリント機能
c) 利用者クライアントのプリンタードライバを使用する機能
   利用者クライアント上のデータを、MFD が解釈可能なページ記述言語(PDL)で構成された印刷データに変換し TOE にプリントデータを蓄積する(プライベートプリント)。
   利用者が利用者クライアントのプリンタードライバで認証管理を設定した状態でプリント指示をすると、MFD は受信データをビットマップデータに変換(デコンポーズ)してユーザーID ごとに内部ハードディスクに蓄積する。

セキュリティ機能としてのユーザー認証機能は、攻撃者が正規の利用者になりすまして内部ハードディスク装置内の文書データを不正に読み出すことを防ぐ機能であり、上記の認証により制御される機能中の
・本体操作パネルから認証する場合の蓄積プリント機能(プライベートプリント機能)および親展ボックス操作機能
・CWIS から認証する場合の親展ボックスからの文書データ取出し機能(親展ボックス操作機能)、

CWIS からのファイル指定による蓄積プリント機能(プライベートプリント機能)がセキュリティ機能に該当する。

プライベートプリント機能、親展ボックス機能の認証フローを図 3 に示す。

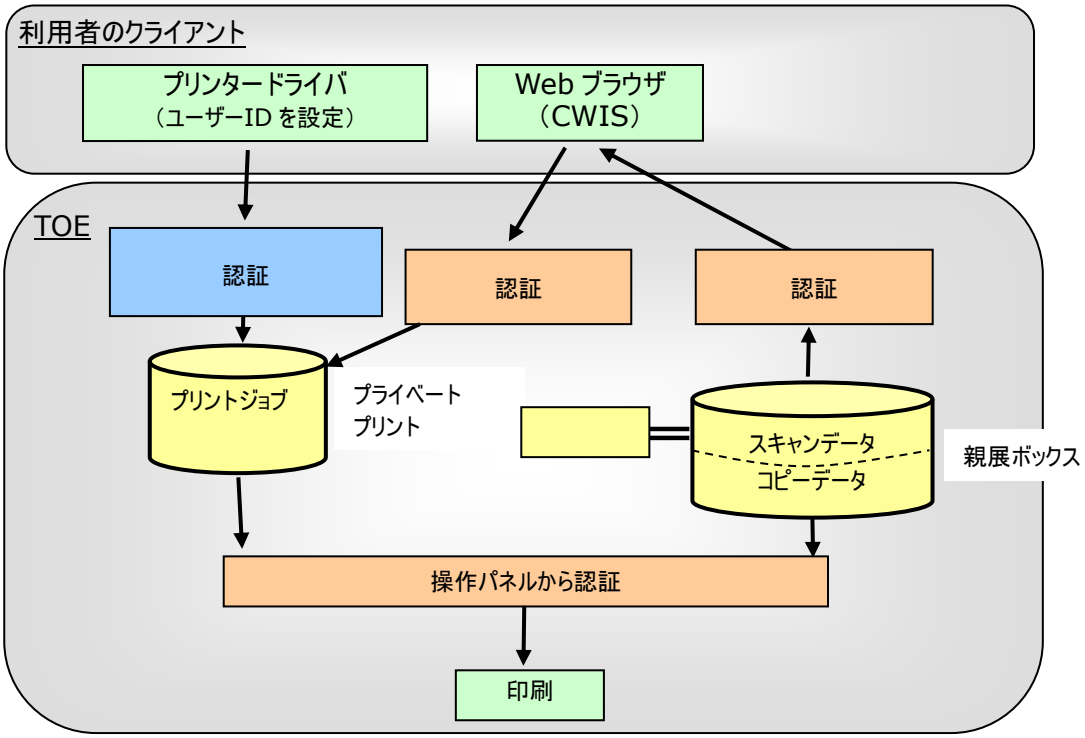

図 3 プライベートプリントと親展ボックスの認証フロー

- 蓄積プリント機能(プライベートプリント機能)
  MFD で「プライベートプリントに保存」の設定をした場合、利用者が利用者クライアントのプリンタードライバで認証管理を設定しプリント指示をすると、MFD は識別認証後に印刷データをビットマップデータに変換(デコンポーズ)してユーザーID ごとにプライベートプリントとして内部ハードディスク装置に一時蓄積する。
  また CWIS からユーザーID とパスワードを入力し、認証後に利用者クライアント内のファイル指定によりプリント指示をする場合も同様にユーザーID ごとのプライベートプリントとして内部ハードディスク装置に一時蓄積される。
  利用者は一時蓄積されたプリントデータを確認するために、MFD の操作パネルからユーザーID とパスワードを入力し、認証されるとユーザーID に対応したプリント待ちのリストだけが表示される。利用者はこのリストから印刷指示、または削除の指示が可能となる。

- 親展ボックス操作機能
  図 3 には図示されていない IIT から親展ボックスにスキャンデータおよびコピーデータを格納することが可能である。
  スキャンデータまたはコピーデータを親展ボックスに格納するには、利用者が MFD の操作パネルからユーザーID とユーザーパスワードを入力させて、認証されるとコピー機能およびスキャン機能の利用が可能になり、操作パネルからコピー蓄積またはスキャン指示をすることにより IIT が原稿を読み取り、内部ハードディスク

装置に蓄積する。
登録されたユーザーID ごとの個人親展ボックスは、利用者が操作パネルまたは CWIS からユーザーIDとパスワードを入力すると MFD は内部に登録されたユーザーIDとパスワードが一致するかをチェックし、一致した場合のみ認証が成功しボックス内のデータを確認することが可能となり、取出しや印刷、削除、編集の操作が可能となる。

(4) システム管理者セキュリティ管理機能
本 TOE は、ある特定の利用者へ特別な権限を持たせるために、システム管理者モードへのアクセスをシステム管理者にのみに制限して、認証されたシステム管理者のみに、操作パネルから下記のセキュリティ機能の参照と設定を行う権限を許可する。

- ハードディスク蓄積データ上書き消去機能の参照と設定
- ハードディスク蓄積データ暗号化機能の参照と設定
- ハードディスク蓄積データ暗号化キーの設定
- 本体パネルからの認証時のパスワード使用機能の参照と設定
- 機械管理者 ID とパスワードの設定 ;機械管理者のみ可能
- SA、一般利用者 ID の参照と設定およびとパスワード設定 ;本体認証時のみ
- システム管理者認証失敗によるアクセス拒否機能の参照と設定
- ユーザーパスワード(一般利用者と SA)の文字数制限機能の参照と設定 ;本体認証時のみ
- TLS 通信機能の参照と設定
- IPSec 通信機能の参照と設定
- S/MIME 通信機能の参照と設定
- On Demand Overwrite 機能の参照と設定
- ユーザー認証機能の参照と設定
- 蓄積プリント機能の参照と設定
- 日付、時刻の参照と設定
- 操作パネルオートクリア機能の参照と設定
- 自己テスト機能の参照と設定
- レポート出力機能の参照と設定

また本 TOE はシステム管理者クライアントから Web ブラウザを通じて CWIS 機能により、認証されたシステム管理者のみに、CWIS 機能により下記のセキュリティ機能の参照と設定を行う権限を許可する。
- 機械管理者 ID とパスワードの設定 ;機械管理者のみ可能
- SA、一般利用者 ID の参照と設定およびパスワード設定 ;本体認証時のみ
- システム管理者認証失敗によるアクセス拒否機能の参照と設定
- ユーザーパスワード(一般利用者と SA)の文字数制限機能の参照と設定 ;本体認証時のみ
- セキュリティ監査ログ機能の参照と設定
- TLS 通信機能の参照と設定
- IPSec 通信機能の参照と設定
- S/MIME 通信機能の参照と設定
- X.509 証明書の作成/アップロード/ダウンロード
- On Demand Overwrite 機能の参照と設定

・ ユーザー認証機能の参照と設定
・ CWIS オートクリア機能の参照と設定

(5) カストマーエンジニア操作制限機能
本 TOE は、カストマーエンジニアが(4)のシステム管理者セキュリティ管理機能に関する設定の参照および変更が出来ないように、認証されたシステム管理者のみに操作パネルと CWIS から、カストマーエンジニア操作制限機能の有効/無効の参照と設定を行う権限を許可する。

(6) セキュリティ監査ログ機能
本 TOE は、いつ、誰が、どのような作業を行ったかという事象や重要なイベント(例えば障害や構成変更、ユーザー操作など)を、追跡記録するためのセキュリティ監査ログ機能を提供する。 この機能はシステム管理者のみ利用可能であり、閲覧や解析のために Web ブラウザを通じて CWIS によりタブ区切りのテキストファイルでダウンロードすることが可能である。 システム管理者がセキュリティ監査ログデータをダウンロードするためには、TLS 通信が有効に設定されていなければならない。

(7) 内部ネットワークデータ保護機能
本 TOE は、内部ネットワーク上に存在する文書データ、ジョブ情報、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護するための以下の一般的な暗号化通信プロトコルに対応する。
・ TLS プロトコル
・ IPSec プロトコル
・ S/MIME プロトコル

(8) インフォメーションフローセキュリティ機能
本 TOE は、外部インターフェースと内部ネットワーク間における許可されない通信を制限する機能を有する。

(9) 自己テスト機能
本 TOE は、TSF 実行コードおよび TSF データの完全性を検証するための自己テスト機能を実行することが可能である。

1.4.2.3. セキュリティ機能を有効にするための設定 (Settings for the Secure Operation)

1.4.2.2 のセキュリティ機能を有効にするためにシステム管理者は TOE に以下の設定をすることが必要である。

- ハードディスク蓄積データ上書き消去機能
  [1 回]あるいは[3 回]に設定
- ハードディスク蓄積データ暗号化機能
  [有効]に設定
- 本体パネルからの認証時のパスワード使用機能
  [有効]に設定

- システム管理者認証失敗によるアクセス拒否機能
  [5]回に設定
- TLS 通信機能
  [有効]に設定
- IPSec 通信機能
  [有効]に設定
- S/MIME 通信機能
  [有効]に設定
- On Demand Overwrite 機能
  [有効]に設定
- ユーザー認証機能
  [本体認証]または[外部認証]に設定
- 蓄積プリント機能
  「プライベートプリントに保存」に設定
- オートクリア機能
  [有効]に設定
- セキュリティ監査ログ機能
  [有効]に設定
- カストマーエンジニア操作制限機能
  [有効]に設定
- 自己テスト機能
  [有効]に設定

1.4.3. TOE の物理的範囲 (Physical Scope and Boundary)

本 TOE の物理的範囲は複合機全体である。図 4 に MFD 内の各ユニット構成と、TOE の物理的範囲を記述する。

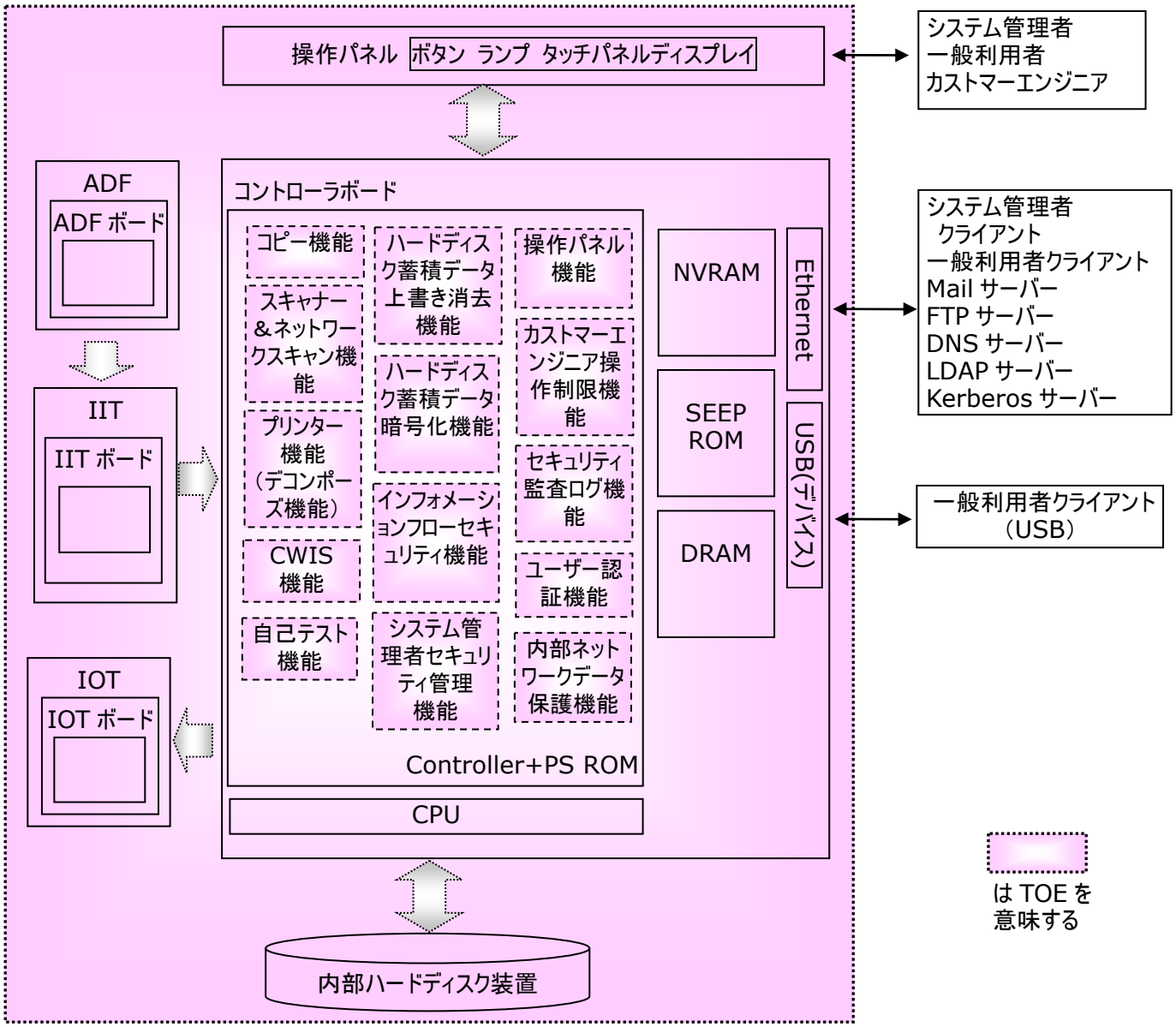

図 4 MFD 内の各ユニットと TOE の物理的範囲

MFD はコントローラボード、IIT、IOT、ADF および操作パネルから構成される。
コントローラボードと操作パネルの間は、制御データの通信を行う内部インターフェースで接続されている。 まコントローラボードと IIT ボードの間、およびコントローラボードと IOT ボードの間は、文書データおよび制御データの通信を行うための、専用の内部インターフェースで接続されている。
コントローラボードは、MFD のコピー機能、プリンター機能、スキャナー機能の制御およびセキュリティ機能のための回路基板であり、ネットワークインターフェース(Ethernet)、ローカルインターフェース(USB)を持ち、IIT

ボードや IOT ボードが接続されている。プログラムは Controller+PS ROM に搭載されている。
画像入力ターミナル(IIT)は、コピー、スキャナー機能の利用時に、原稿を読み込み、画像情報をコントローラボードへ転送する入力デバイスである。
画像出力ターミナル(IOT)は、コントローラボードから転送される画像情報を出力するデバイスである。
自動原稿送り装置(ADF)は、原稿を自動的に IIT に搬送するデバイスである。
操作パネルは、MFD のコピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能の操作および設定に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネルである。
TOE 中の NVRAM と内部ハードディスク装置は取り外し可能ではない記憶媒体である。

4 タイプの Channel は TOE 中で下記が相当する。

- Private Medium Interface
  操作パネル、USB
- Shared Medium Interface
  Ethernet
- Original Document Handler
  IIT
- HardCopy Output Handler
  IOT

1.4.4. ガイダンス (Guidance)

本 TOE を構成するガイダンス文書は以下のとおりである。

- Xerox D95/D110/D125/D136 Copier/Printer User Guide; Version 3.0 September 2013
  (SHA256 ハッシュ値:
  4524d4c91d5002b543dd1ebe4bc0310c7704db8146b86198d5fefbc8b73ada6c)
- Xerox D95/D110/D125/D136 Copier/Printer System Administration Guide; Version 3.1 January 2014
  (SHA256 ハッシュ値:
  16e971b5953d5fa38676016260cf0aed61a14f291fdbf2543056bad01c0a42b1)
- Xerox D95/D110/D125/D136 Copier/Printer Security Function Supplementary Guide; Version 1.0 September 2018
  (SHA256 ハッシュ値:
  0a4b5a995a9b414b354bfde243842f80fff4f89be79b3ebed2734cdea0decce2)

2. 適合主張 (Conformance Claim)

2.1. CC 適合主張 (CC Conformance Claim)

本 ST および TOE の CC 適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン:

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model (September 2012 Version 3.1 Revision 4)
Part 2: Security functional components (September 2012 Version 3.1 Revision 4)
Part 3: Security assurance components (September 2012 Version 3.1 Revision 4)

CC Part2 extended [FPT_FDI_EXP.1]
CC Part3 conformant

2.2. PP 主張、パッケージ主張 (PP claim, Package Claim)

2.2.1. PP 主張 (PP Claim)

本 ST は、
U.S. Government Approved Protection Profile - U.S. Government, Protection Profile for Hardcopy Device Version 1.0 (IEEE Std. 2600.2™ -2009)
への論証適合を主張する。

2.2.2. パッケージ主張 (Package Claim)

EAL2 に ALC_FLR.2 の追加(EAL2 augmented by ALC_FLR.2)を主張する。

また PP 記述の選択可能な SFR Package の内、下記のパッケージをパッケージ適合(package conformant)として主張する。

Title: 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
Package Version: 1.0

Title: 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
Package Version: 1.0

2.2.3. 適合根拠 (Conformance Rational)

本 ST は、PP に記述されている Common HCD Functions と Print Functions、Scan Functions、Copy Functions、Document Storage and Retrieval Functions、Shared-medium Interfaces Functions を網羅した上で一部機能を追加して記述されている。

本 ST にある TOE の種別は、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能を有するデジタル複合機(Multi Function Device 略称 MFD)であり、PP の 4.1 Typical Products に記述されている Hardcopy Device と同義であり要求機能を包含している。

また下記に示すようにセキュリティ課題定義、セキュリティ対策方針、セキュリティ要件は PP を網羅して記述されている。

- PP で規定している脅威/OSP/前提条件に、P.CIPHER を追加の OSP としている。P.CIPHER は内部ハードディスク装置のデータの暗号化であり、他の課題定義とは独立しており影響を与えない。前提条件は変更なく、これらのことから脅威/OSP/前提条件は PP のセキュリティ課題定義のステートメントより制限的である。

- PP で規定している運用環境の対策方針の内、OE.AUDIT_STORAGE.PROTECTED と OE.AUDIT_ACCESS.AUTHORIZED を削除し、TOE の対策方針としている。その他は内容を変更せずに引用されており、追加の運用環境の対策方針はないことから運用環境の対策方針は、PP のセキュリティ対策方針のステートメントと同等以下の制限である。

- PP で規定している TOE の対策方針、O.AUDIT_STORAGE.PROTECTED、O.AUDIT_ACCESS.AUTHORIZED を追加の対策方針としている。TOE のセキュリティ対策方針は、PP のセキュリティ対策方針のステートメントより制限的である。

- PP で規定している SFR と ST で使用している SFR の関係を Table 14 に示している。
  ここで各々の SFR 記述の詳細化、SFR の追加内容を記述している。
  Common Access Control SFP の文書データの登録操作の追加は、アクセスを許可された利用者に制限しており、FDP_ACC.1/FDP_ACF.1 は PP より制限的である。
  ＋SMI のセキュリティ属性は定義していないが、FPT_FDI_EXP.1 の転送を制限するための操作は存在しないため PP の要求と同等である。

D.DOC のアクセス制御 SFP で一部の削除の処理を U.USER に対しても許さない定義があるが、FDP_ACC.1 は PP より制限的である。
PP で規定している他の SFR は要求と同等であり、追加の SFR により、TOE をより制限的にしている。
このことにより、本 ST の SFR は PP の SFR より制限的である。

尚、本 ST では PP の SFR に対して、選択部分を抜き出し、その選択内容をイタリックで記述しているが、その選択内容は PP の要求している内容を記述している。
また同様に割付部分を抜き出し、その割付内容を PP で確定している部分も含めてイタリックで記述している。

- PP で規定しているセキュリティ対策方針根拠の内、P.AUDIT.LOGGING の対策方針は OE.AUDIT_STORAGE.PROTECTED、OE.AUDIT_ACCESS.AUTHORIZED を O.AUDIT_STORAGE.PROTECTED、O.AUDIT_ACCESS.AUTHORIZED に置き換えている。
また P.CIPHER の対策方針に O.CIPHER を追加している。その他は内容を変更せずに PP の要求している内容を記述しており保証されていることを記述している。

- セキュリティ機能要件根拠は、説明を日本語で記述している。
追加された TOE 対策方針と SFR に関しては追加の説明をしている。
セキュリティ対策方針と FMT_MSA.1 の対応関係が PP と異なるが、これはユーザーデータの保護のためにセキュリティ属性の漏えいや改ざんに対する保護への要件を、TSF データ保護の対策方針にも対応させるのであり、PP が指定するセキュリティ機能要件の内容を変更するものではない。
その他は PP の要求している内容を記述しており保証されていることを記述している。

- PP で規定している SAR は内容を変更せずに PP の要求している内容を記述している。

故に本 ST は PP に論証適合している。

3. セキュリティ課題定義 (Security Problem Definition)

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威 (Threats)

3.1.1. TOE 資産 (Assets Protected by TOE)

本 TOE が保護する資産は以下のとおりである。

Table 4 利用者データに関する保護資産

Designation	PP Definition	具体的な保護資産	補足説明
D.DOC	User Document Data consists 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.	ジョブ処理のために蓄積する文書データ	利用者が MFD をコピー、プリント、スキャン、ネットワークスキャン等の目的で利用すると画像処理や通信、蓄積プリントのために内部ハードディスク装置に一時的に文書データが蓄積される。また CWIS 機能により利用者クライアントから MFD 内の親展ボックスに蓄積された文書データの取り出しが可能である。
		ジョブ処理後の利用済み文書データ	利用者が MFD をコピー、スキャン、ネットワークスキャン等の目的で利用すると画像処理や通信、蓄積プリントのために内部ハードディスク装置に一時的に文書データが蓄積され、ジョブの完了やキャンセル時は管理情報を削除するがデータは残存する。
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.	ユーザージョブ情報	利用者または外部エンティティにより指示されたジョブ。

Table 5 TSF データに関する保護資産

Designation	PP Definition	具体的な保護資産	補足説明
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.	Table 24、Table 25、Table 26、Table 27、Table 28、Table 31 と Table 32 の下記 D.CONF 以外の情報	左記の TOE 設定データ、セキュリティ属性に関しての内容については開示されてもセキュリティ上の脅威とならない情報。
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.	・利用者のパスワード情報 ・監査ログ（Table 15） ・ハードディスク蓄積データ暗号化情報 ・内部ネットワークデータ保護情報	システム管理者はシステム管理者セキュリティ管理機能により TOE のセキュリティ機能の設定が、MFD の操作パネルやシステム管理者クライアントから可能であり、設定データは TOE 内に保存される。 一般利用者はユーザー認証機能により、自身の ID とパスワードの設定が、MFD の操作パネルから可能であり、設定データは TOE 内に保存される。 システム管理者はセキュリティ監査ログデータをシステム管理者クライアントから取り出し可能であり、セキュリティ監査ログデータは TOE 内に保存される。

Table 6 その他の保護資産

Designation	PP Definition	具体的な保護資産	補足説明
Functions	Functions perform processing, storage, and transmission of data that may be present in HCD products. These functions are used by SFR packages.	MFD の機能	許可された特定の利用者だけが TOE のコピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能等を使用することが可能。

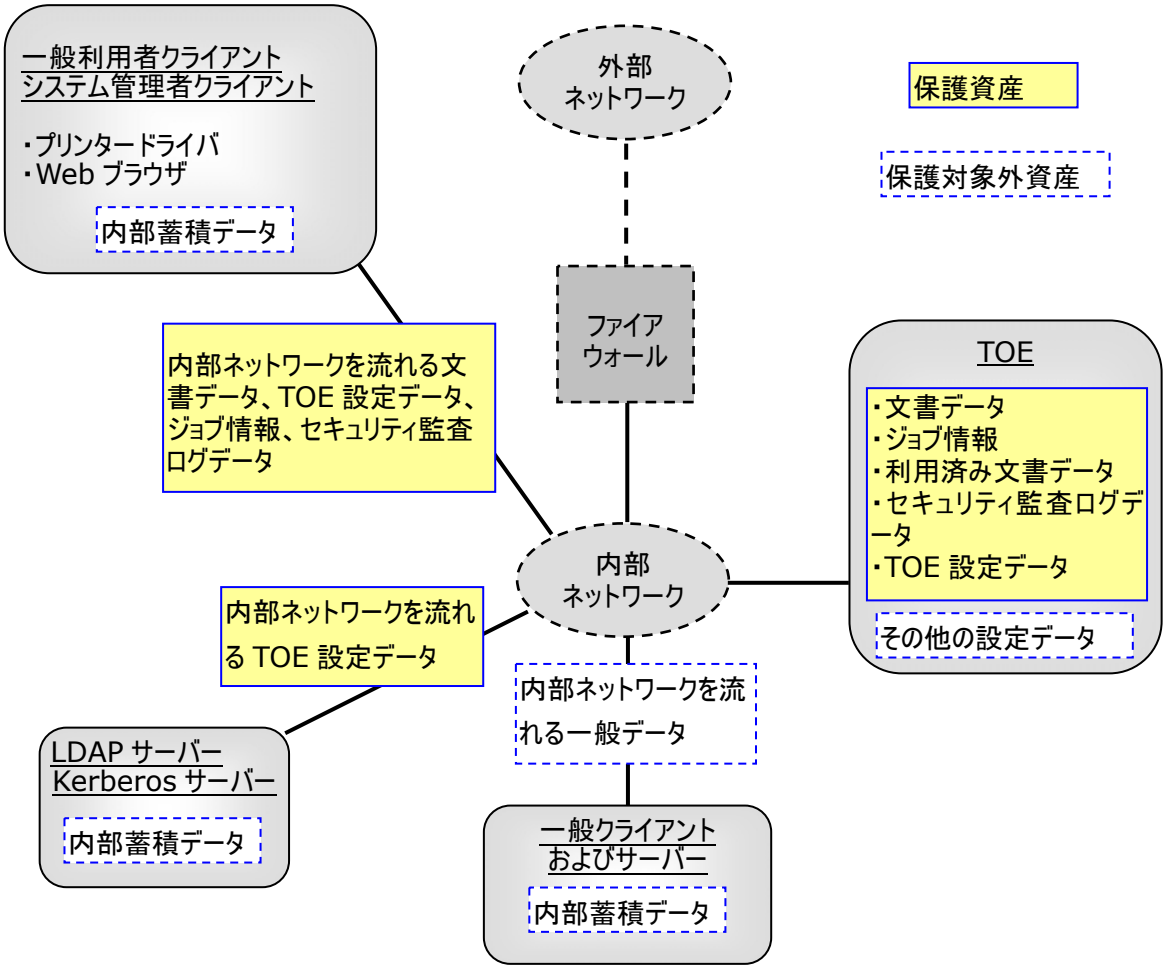

図 5 保護資産と保護対象外資産

注）内部ネットワーク内に存在する一般クライアントおよびサーバー内部の蓄積データや内部ネットワークを流れる一般データは保護対象外の資産である。

Table 5 の TSF データは、内部ハードディスク装置、コントローラボードの NVRAM、SEEPROM に保存されている。
ただし時計の日時データはこれらには含まれない。

記憶場所の NVRAM と SEEPROM には、TSF データ以外のデータも格納されているが、それらの設定データは TOE のセキュリティ機能に関係しないため保護対象の資産ではない。
セキュリティ監査ログデータは、一時的に NVRAM に記憶されるが、ファイルとしては内部ハードディスク装置に保存される。

3.1.2. 脅威エージェント (Threats agents)

本 ST では下記４種類の脅威エージェントを攻撃者と想定する。いずれも低レベルの攻撃能力を持つ者であり TOE の動作について公開されている情報知識を持っていると想定する。

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 are not authorized.
d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

3.1.3. 脅威 (Threats)

本 TOE に対する脅威を、Table 7 に記述する。unauthorized persons は 3.1.2 の脅威エージェントであると想定する。

Table 7 利用者データ とTSF データに対する脅威

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
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

3.2. 組織のセキュリティ方針 (Organizational Security Policies)

本 TOE が順守しなければならない組織のセキュリティ方針を Table 8 に記述する。

Table 8 組織のセキュリティ方針

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 the interfaces will be controlled by the TOE and its IT environment.
P.CIPHER	To prevent unauthorized reading-out, the document data in the internal HDD will be encrypted by the TOE.

3.3. 前提条件 (Assumptions)

本 TOE の動作、運用、および利用に関する前提条件を、Table 9 に記述する。

Table 9 前提条件

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

4. セキュリティ対策方針 (Security Objectives)

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

4.1. TOE のセキュリティ対策方針 (Security Objectives for the TOE)

TOE のセキュリティ対策方針を Table 10 に記述する。

Table 10 TOE セキュリティ対策方針

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.
O.CIPHER	The TOE shall provide the function to encrypt the document data in the internal HDD so that they cannot be read out.

4.2. 運用環境のセキュリティ対策方針 (Security Objectives for the Environment)

運用環境のセキュリティ対策方針を Table 11 に記述する。

Table 11 運用環境のセキュリティ対策方針

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

4.3. セキュリティ対策方針根拠 (Security Objectives Rationale)

セキュリティ対策は、セキュリティ課題定義で規定した前提条件に対応するためのもの、あるいは脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対応する前提条件、対抗する脅威、実現する組織のセキュリティ方針の対応関係を Table 12 に示す。また各セキュリティ課題定義がセキュリティ対策方針により保証されていることを Table 13 に記述する。

Table 12 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針及び前提条件

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

Table 13 セキュリティ課題定義に対応するセキュリティ対策方針根拠

Threats, policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the

Threats, policies, and assumptions	Summary	Objectives and rationale
	persons.	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	O.CONF.NO_ALT protects D.CONF from unauthorized alteration. O.USER.AUTHORIZED establishes user

Threats, policies, and assumptions	Summary	Objectives and rationale
	persons.	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 authorization to use the TOE.identification and authentication as the basis for OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to selfverify 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.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed. O.AUDIT_STORAGE.PROTECTED protects audit logs from unauthorized access, deletion, and alteration for the TOE. O.AUDIT_ACCESS.AUTHORIZED enables the analysis of audit logs only by authorized users to detect potential security violations for the TOE.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies. OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
P.CIPHER	User Data stored in the HDD will be encrypted by the TOE.	O.CIPHER encrypts the document data in the internal HDD to disable unauthorized reading-out of them.

Threats, policies, and assumptions	Summary	Objectives and rationale
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. 拡張コンポーネント定義 (Extended Components Definition)

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_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	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 this data is sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1
The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities.
b) Management of the conditions under which direct forwarding can be allowed by an administrative role.
c) Revocation of such an allowance.

Audit: FPT_FDI_EXP.1
The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:
There are no auditable events foreseen.

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

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

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

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

FPT_FDI_EXP.1	**Restricted forwarding of data to external interfaces**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles.
FPT_FDI_EXP.1.1	The TSF shall provide the capability to restrict data receivedon [assignment: list of external interfaces] from being forwarded without further processing by the TSF to [assignment: list of external interfaces].

6. セキュリティ要件 (Security Requirements)

本章では、セキュリティ機能要件、セキュリティ保証要件およびセキュリティ要件根拠について記述する。
なお、本章で使用する用語の定義は以下のとおりである。

・ サブジェクト

名称	定義
Key Operator	機械管理者のユーザー認証が成功した状態での基本機能、親展ボックス内の文書データ、蓄積プリントに対する操作
SA	SA のユーザー認証が成功した状態での基本機能、親展ボックス内の文書データ、蓄積プリントに対する操作
U.ADMINISTRATOR	Key Operator, SA のユーザー認証が成功した状態での基本機能、親展ボックス内の文書データ、蓄積プリントに対する操作
U.NORMAL	一般利用者(U.NORMAL)のユーザー認証が成功した状態での基本機能、親展ボックス内の文書データ、蓄積プリントに対する操作
U.USER	U.ADMINISTRATOR, U.NORMAL のユーザー認証が成功した状態での基本機能、親展ボックス内の文書データ、蓄積プリントに対する操作

・ オブジェクト

名称	定義
Used document data stored in the internal HDD	MFD の内部ハードディスク装置に蓄積された後、利用が終了しファイルは削除されるが、内部ハードディスク装置内にはデータ部は残存している状態の文書データ。
Document data	一般利用者(U.NORMAL)、SA が MFD のコピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能を利用する際に、MFD 内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。
Security Audit Log	いつ、誰が、どのような作業を行ったかという事象や重要なイベント(例えば障害や構成変更、ユーザー操作など)を、追跡記録されたデータ。

・ 操作

名称	定義
send the scanned data	スキャンした文書データを自動的に利用者クライアント、FTP サーバー、メールサーバーへ配信すること。

retrieve the document data	親展ボックスから文書データを下記へ出力すること ・印刷（スキャン文書データ、コピー文書データ） ・操作パネルでのプレビュー（スキャン文書データ、コピー文書データ） ・CWIS から利用者クライアントへのエクスポート（スキャン文書データ）
edit	親展ボックス内のコピー文書データを編集すること ・ページ削除 ・合紙挿入 ・文書合成
modify the behavior	ユーザー認証機能(本体、外部)、蓄積プリント機能(認証失敗時の蓄積、削除)、内部ネットワークデータ保護機能(認証方式、暗号化方式)、ハードディスク蓄積データ上書き消去機能(上書き回数、上書き情報、On Demand Overwrite 情報)、レポート出力機能(システム管理者のみ、利用者)のふるまいの変更
modify	TOE 設定データの設定変更およびセキュリティ属性(利用者識別情報、機能に対応する利用者識別情報)の変更
Mailbox operation	親展ボックス内に保存された文書データに対する操作 印刷、プレビュー、利用者クライアントへのエクスポートなど

・ セキュリティ属性

名称	定義
General User role	一般利用者(U.NORMAL)が TOE を利用する際に必要な権限を表す
SA role	SA が TOE を利用する際に必要な権限を表す
Key Operator role	機械管理者が TOE を利用する際に必要な権限を表す
User identifier	General User identifier、SA identifier、Key Operator identifier の総称である
General User identifier	一般利用者(U.NORMAL)を識別認証するためのユーザーID
SA identifier	SA を識別認証識別するためのユーザーID
Key Operator identifier	機械管理者を識別認証するためのユーザーID
User identifier for each function	コピー機能、プリンター機能、スキャナー機能に対応したアクセス可能なユーザー情報、使用制限の情報
Owner identifier of D.DOC	親展ボックス、プライベートプリント内の文書データに対応したアクセス可能なユーザー情報
Owner identifier of D.FUNC	ジョブに対応したアクセス可能なユーザー情報

・ 外部のエンティティ

名称	定義
Key Operator	MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。

SA(System Administrator Privilege)	機械管理者あるいは既に作成された SA がアカウントを作成することができ、MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。
U.ADMINISTRATOR (System Administrator)	Key Operator と SA の総称。
U.NORMAL (General User)	MFD のコピー機能、スキャナー機能、ネットワークスキャン機能およびプリンター機能を利用する者。

・ その他の用語

名称	定義
The Fuji Xerox's standard method, FXOSENC	富士ゼロックス標準の暗号鍵生成アルゴリズムで、起動時に使用される。
AES	FIPS 標準規格の暗号化アルゴリズムで、ハードディスクデータの暗号化と復号化に使用される。
Access denial due to authentication failure of system administrator ID	システム管理者 ID 認証失敗が所定回数に達した時に、当該利用者の識別認証に関しては、TOE の電源切断/再投入まで受け付けなくなる動作。
Data on use of password entered from MFD control panel in user authentication	TOE 設定データであり、本体パネルからの認証時のパスワード使用機能の有効/無効の情報。
Data on minimum user password length	TOE 設定データであり、SA/一般利用者のパスワード設定時の最小文字数の情報
Data on key operator ID	TOE 設定データであり、機械管理者識別のための ID 情報。
Data on key operator Password	TOE 設定データであり、機械管理者認証のためのパスワード情報
Data on SA ID	TOE 設定データであり、SA 識別のための ID 情報。
Data on SA Password	TOE 設定データであり、SA 認証のためのパスワード情報
Data on General user ID	TOE 設定データであり、一般利用者(U.NORMAL)識別のための ID 情報。
Data on General user Password	TOE 設定データであり、一般利用者(U.NORMAL)認証のためのパスワード情報
Data on access denial due to authentication failures of system administrator	TOE 設定データであり、システム管理者 ID 認証失敗に関係する機能の有効/無効の情報と失敗回数情報
Data on Security Audit Log	TOE 設定データであり、いつ、誰が、どのような作業を行ったかという事象や重要なイベント(例えば障害や構成変更、ユーザー操作など)を、追跡記録する機能の有効/無効の情報。

Data on User Authentication	TOE 設定データであり、MFD のコピー機能、スキャナー機能、ネットワークスキャン機能およびプリンター機能を利用する際に、ユーザー認証情報にて認証する機能の有効/無効および設定の情報。
Data on Store Print	TOE 設定データであり、プリントデータ受信時にプライベートプリントに蓄積させるか印刷させるかの設定情報。
Data on Internal Network Data Protection	TOE 設定データであり、内部ネットワーク上に存在する文書データ、ジョブ情報、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護するために対応する一般的な暗号化通信プロトコルの有効/無効および設定の情報および証明書、認証用/暗号化パスワード、共通鍵パスワード情報。
Data on Customer Engineer Operation Restriction-	TOE 設定データであり、カストマーエンジニア操作制限機能の有効/無効の情報及び保守パスワードの情報。
Data on Hard Disk Data Encryption	TOE 設定データであり、ハードディスク蓄積データ暗号化機能に関係する機能の有効/無効の情報と暗号化キー情報。
Data on Hard Disk Data Overwrite	TOE 設定データであり、ハードディスク蓄積データ上書き消去機能に関係する機能の有効/無効の情報と上書き回数情報、および On Demand Overwrite 機能の有効/無効の情報と日時指定情報。
Data on date and time	TOE 設定データであり、タイムゾーン/サマータイム設定情報と現在時刻データである。
Data on Auto Clear	TOE 設定データであり、操作パネルオートクリア機能の有効/無効およびクリア時間の情報、および CWIS のオートクリア機能の有効/無効の情報。
Data on Self Test	TOE 設定データであり、自己テスト機能の有効/無効の情報。
Data on Report Print	TOE 設定データであり、レポート出力機能の設定情報。
Store Print/Private Print	プリンター機能において、印刷データをデコンポーズして作成したビットマップデータを、MFD の内部ハードディスク装置に一旦蓄積し、認証された一般利用者が操作パネルより指示する事で印刷を開始するプリント方法。

6.1. セキュリティ機能要件 (Security Functional Requirements)

本 TOE が提供するセキュリティ機能要件を以下に記述する。
本 ST で、使用する機能要件の一覧を、Table 14 に示す。

Table 14 機能要件一覧

機能要件コンポーネント		PP 要求	記述内容と PP との差
FAU_GEN.1	Audit data generation	Yes	TOE にあわせて Auditable Event を具体的に記述、追加している。
FAU_GEN.2	User identity association	Yes	PP から変更なし

機能要件コンポーネント		PP 要求	記述内容と PP との差
FAU_SAR.1	Audit review	No	この SFR の追加によりシステム管理者のみに監査ログデータの読み出し機能を提供する。
FAU_SAR.2	Restricted audit review	No	
FAU_STG.1	Protected audit trail storage	No	この SFR の追加により監査ログデータを、不正な削除や改変から保護する。
FAU_STG.4	Prevention of audit data loss	No	この SFR の追加により監査ログが満杯になった時に、最も古い監査ログに新しい監査イベントを上書きする。
FCS_CKM.1	Cryptographic key generation	No	このSFRの追加により内部ハードディスク装置のデータを暗号化する。
FCS_COP.1	Cryptographic operation	No	
FDP_ACC.1(a)	Subset access control	Yes	Attributes、Operations、Access Control rule は PP の記述を引用し、さらにTOEにあわせてDelete、Modifyの操作の詳細化と操作の追加をしている。
FDP_ACC.1(b)	Subset access control	Yes	Access Control SFP を TOE にあわせて記述している。
FDP_ACC.1(c) (PRT SFR Package) FDP_ACC.1(d) (SCN SFR Package) FDP_ACC.1(e) (CPY SFR Package) FDP_ACC.1(f) (DSR SFR Package)	Subset access control	Yes	Attributes、Operations、Access Control rule は PP の記述を引用し、さらに TOE にあわせて Read の操作の詳細化をしている。
FDP_ACF.1(a)	Security attribute based access control	Yes	Attributes、Operations、Access Control rule は PP の記述を引用し、さらにTOEにあわせてDelete、Modifyの操作を詳細化と操作の追加をしている。
FDP_ACF.1(b) FDP_ACF.1(c) (PRT SFR Package) FDP_ACF.1(d) (SCN SFR Package) FDP_ACF.1(e) (CPY SFR Package) FDP_ACF.1(f) (DSR SFR Package)	Security attribute based access control	Yes	Attributes、Operations、Access Control rule は PP の記述を引用し、さらに TOE にあわせて Read の操作を詳細化している。

機能要件コンポーネント		PP 要求	記述内容と PP との差
FDP_RIP.1	Subset residual information protection	Yes	TOE にあわせて割付している。
FIA_AFL.1 (a) FIA_AFL.1 (b)	Authentication failure handling	No	この SFR の追加により機械管理者認証、SA 認証の認証失敗によるアクセス拒否機能を提供する。
FIA_ATD.1	User attribute definition	Yes	TOE にあわせて割付している。
FIA_SOS.1	Verification of secrets	No	TOE にあわせて割付している。
FIA_UAU.2	User authentication before any action	Yes	FIA_UAU.1 から上位階層である FIA_UAU.2 に変更している
FIA_UAU.7	Protected authentication feedback	No	この SFR の追加により認証フィードバックを保護する。
FIA_UID.2	User identification before any action	Yes	FIA_UID.1 から上位階層である FIA_UID.2 に変更している
FIA_USB.1	User-subject binding	Yes	TOE にあわせて割付している。
FMT_MOF.1	Management of security functions behaviour	No	この SFR の追加によりセキュリティ機能の設定を、システム管理者だけに限定する。
FMT_MSA.1(a) FMT_MSA.1(b)	Management of security attributes	Yes	セキュリティ属性の管理役割を TOE にあわせて割付している。
FMT_MSA.1(c) FMT_MSA.1(d) FMT_MSA.1(e) FMT_MSA.1(f)	Management of security attributes	No	セキュリティ属性の管理を TOE にあわせて記述している。
FMT_MSA.3(a) FMT_MSA.3(b)	Static attribute initialisation	Yes	TOE にあわせて割付している。
FMT_MSA.3(c) FMT_MSA.3(d) FMT_MSA.3(e) FMT_MSA.3(f)	Static attribute initialisation	No	TOE にあわせて記述している。
FMT_MTD.1(a) FMT_MTD.1(b)	Management of TSF data	Yes	TSF データの操作リストを TOE にあわせて記述している。 ただし FMT_MTD.1(b)は D.Conf のみ
FMT_SMF.1	Specification of Management Functions	Yes	セキュリティ管理機能のリストを TOE にあわせて記述している。
FMT_SMR.1	Security roles	Yes	TOE にあわせて割付している。
FPT_FDI_EXP.1 (SMI SFR Package)	Restricted forwarding of data to external interfaces	Yes	PP から変更なし

機能要件コンポーネント		PP 要求	記述内容と PP との差
FPT_STM.1	Reliable time stamps	Yes	PP から変更なし
FPT_TST.1	TSF testing	Yes	TOE にあわせて割付している。
FTA_SSL.3	TSF-initiated termination	Yes	TOE にあわせて割付している。
FTP_ITC.1 (SMI SFR Package)	Inter-TSF trusted channel	Yes	PP から変更なし

6.1.1. Class FAU: Security Audit

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
- [assignment: other specifically defined auditable events].

[selection, choose one of: minimum, basic, detailed, not specified]
- not specified
[assignment: other specifically defined auditable events]
- all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table15;

Table 15 Auditable Events of TOE and Individually Defined Auditable Events

Relevant SFR	Auditable event	Audit level	Additional information	Actions to be audited (defined by CC)
FAU_GEN.1	－	－	－	There are no auditable events foreseen.
FAU_GEN.2	－	－	－	There are no auditable events foreseen.
FAU_SAR.1	*Successful download of audit log data.*	*＜Basic＞*	*None*	a) Basic: Reading of information from the audit records.
FAU_SAR.2	*Unsuccessful download of audit*	*＜Basic＞*	*None*	a) Basic: Unsuccessful attempts to read

	log data.			information from the audit records.
FAU_STG.1	—	—	—	There are no auditable events foreseen.
FAU_STG.4	*None*	—	—	a) Basic: Actions taken due to the audit storage failure.
FCS_CKM.1	*None*	—	—	a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_COP.1	*None*	—	—	a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACC.1	—	—	—	There are no auditable events foreseen.
FDP_ACF.1(a)	*Job completion and cancellation of Print, Copy, Scan.*	*<not specified>*	*Type of job*	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.
FDP_ACF.1(b)	*Job completion and cancellation of Print, Copy, Scan.*			
FDP_ACF.1(c)	*User name, job information, and success/failure regarding execution of Store Print.*			

FDP_ACF.1(d)	*User name, job information, and success/failure regarding access to the document in Mailbox.*			
FDP_ACF.1(f)	*User name, job information, and success/failure regarding access to the document in Mailbox.*			
FDP_RIP.1	－	－	－	There are no auditable events foreseen.
FIA_AFL.1(a) FIA_AFL.1(b)	*Authentication lock of system administrator*	*<Minimal>*	*None required*	a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	－	－	－	There are no auditable events foreseen.
FIA_SOS.1	*Change in quality metrics*	*<not specified>*	－	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics

FIA_UAU.2	*Success/failure of authentication*	*<Basic>*	*None required*	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.
FIA_UAU.7	－	－	－	There are no auditable events foreseen.
FIA_UID.2	*Success/failure of identification and authentication*	*<Basic>*	*Attempted user identity*	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.
FIA_USB.1	*User login failure*	*<not specified>*	*None*	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).
FMT_MOF.1	*Changes in security function configuration*	*<Basic>*	*None*	a) Basic: All modifications in the behavior of the functions in the TSF.
FMT_MSA.1(a) FMT_MSA.1(b) FMT_MSA.1(c) FMT_MSA.1(d) FMT_MSA.1(e) FMT_MSA.1(f)	*Changes in security settings*	*<not specified>*	*None*	a) Basic: All modifications of the values of security attributes.

FMT_MSA.3 (a) FMT_MSA.3 (b) FMT_MSA.3 (c) FMT_MSA.3 (d) FMT_MSA.3 (e) FMT_MSA.3 (f)	*None*	*<Basic>*	*None*	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
FMT_MTD.1(a)	*Changes in registration data (ID, password) of system administrator, and in the setting of security functions*	*<not specified>*	*None*	a) Basic: All modifications to the values of TSF data.
FMT_MTD.1(b)	*Changes in registration data (ID, password) of system administrator*			
FMT_SMF.1	*Access to system administrator mode*	*<Minimal>*	*None required*	a) Minimal: Use of the management functions.
FMT_SMR.1	*Registration of system administrator, changes in user registration data(role), and deletion of system administrator*	*<Minimal>*	*None required*	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.
FPT_STM.1	*Changes in time setting*	*<Minimal>*	*None required*	a) Minimal: changes to the time; b) Detailed: providing a timestamp.
FPT_TST.1	*Execution of Self Test and the test result*	*<Basic>*	*None*	Basic: Execution of the TSF self tests and the results of the tests.
FTA_SSL.3	*Log-in timeout from remote.*	*<Minimal>*	*None required*	a) Minimal: Termination of an interactive session

	Log-in timeout from control panel.			by the session locking mechanism.
FTP_ITC.1	*Failure of the trusted Communication within a specified period of time, and client host data (host name or IP address)*	*<Minimal>*	*None required*	a)Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.
FPT_FDI_EXP.1	—	—	—	There are no auditable events foreseen.

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, [assignment: other audit relevant information].

[assignment: other audit relevant information]
- for each Relevant SFR - listed in Table15: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is 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.
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: authorized users] with the capability to read [assignment: list of audit information] from the audit records. [assignment: authorized users] *- U.ADMINISTRATOR* [assignment: list of audit information] *- all log information*
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	Restricted audit review
Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAU_STG.1	Protected audit trail storage
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail. [selection, choose one of: prevent, detect] *- prevent*
FAU_STG.4	Prevention of audit data loss

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

FAU_STG.4.1 The TSF shall [selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorized 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 authorized 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]
- no other actions to be taken

6.1.2. Class FCS: Cryptographic Support

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 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: list of standards]
- none
[assignment: cryptographic key generation algorithm]
- the Fuji Xerox's standard method, FXOSENC
[assignment: cryptographic key sizes]
- 256bits

FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]. [assignment: list of standards] *- FIPS PUB 197* [assignment: cryptographic algorithm] *- AES* [assignment: cryptographic key sizes] *- 256bits* [assignment: list of cryptographic operations] *- encryption of the document data to be stored in the internal HDD and decryption of the document data retrieved from the internal HDD.*

6.1.3. Class FDP: User Data Protection

The Security Function Policy (SFP) described in Table16 is referenced by the Class FDP SFRs in this clause.

Table 16 Common Access Control SFP

Object	Attribute	Operation(s)	Subject	*Access control rule
D.DOC	*attributes from Table 17*	*Delete* *- Delete the document data in Mailbox and Private Print*	*U.USER*	*Denied, except for his/her own documents* *- R1* *- R2* *- R3* *- R4*

Object	Attribute	Operation(s)	Subject	*Access control rule
		Delete *- Delete the document data except for Mailbox and Private Print.*	*U.USER*	*Denied*
D.FUNC	*attributes from Table 17*	*Modify; Delete* *- Modify and delete the Job data*	*U.NORMAL*	*Denied*
			U.ADMINISTRATOR	*permitted*

*Details of Access control rule

R1: When the owner identifier of D.DOC matches the user identifier, operation to delete the document in Mailbox is permitted.

R2: When the owner identifier of D.DOC matches the user identifier, operation to delete the document in Private Print is permitted.

R3: In the Key Operator process, operation to delete the document in Mailbox is permitted.

R4: In the U.ADMINISTRATOR process, operation to delete the document in Private Print is permitted.

Table 17 SFR Package attributes

Designation	Definition
+PRT	*Indicates data that is associated with a print job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+SCN	*Indicates data that is associated with a scan job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+CPY	*Indicates data that is associated with a copy job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+DSR	*Indicates data that are associated with a document storage and retrieval job.* *- User identifier* *- Owner identifier of D.DOC* *- Owner identifier of D.FUNC*
+SMI	*Indicates data that is transmitted or received over a shared-medium interface.*

	- none

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

FDP_ACC.1.1 (a) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]
- Common Access Control SFP in Table16
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table16

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

FDP_ACC.1.1 (b) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]
- TOE Function Access Control SFP in Table 18
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- users as subjects, TOE functions as objects, and the right to use the functions as operations in Table 18.

Table 18 Function Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
Copy (F.CPY, F.SCN, F.DSR)	*- User identifier* *- User identifier for each function*	*- Copy operation from control panel*	*U.USER*	*When the user identifier for the function*

Object	Attribute(s)	Operation	Subject	Access control rule
Scan / Network Scan (F.SCN, F.DSR, F.SMI)	*- User identifier* *- User identifier for each function*	*- Scan operation to Mailbox from control panel* *- Send the scanned data from control panel to user client, FTP server, and Mail server*	*U.USER*	*matches the user identifier, operation of the function is permitted.*
Print (F.PRT, F.SMI)	*- User identifier* *- User identifier for each function*	*- Print(*) the document data in Private Print from control panel*	*U.USER*	
Mailbox Operation (F.DSR, F.SMI)	*- User identifier* *- User identifier for each function*	*- Mailbox operation*	*U.USER*	

**Job abort for Print function is restricted to the control panel.*

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

FDP_ACC.1.1(c) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]
- PRT Access Control SFP in Table19
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
- the list of subjects, objects, and operations among subjects and objects covered by the PRT Access Control SFP in Table19.

Table 19 PRT Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+PRT*	*Read* *Print the document data in Private Print*	*U.USER*	*Denied, except for his/her own documents* *- When the owner identifier of D.DOC matches the user identifier, print operation is permitted.* *- In the U.ADMINISTRATOR process, operation to read all the documents in Private Print is permitted.*

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

FDP_ACC.1.1 (d) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]
- SCN Access Control SFP in Table20
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the SCN Access Control SFP in Table 20

Table 20 SCN Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+SCN*	*Read* *- Send the document data to server*	*U.USER*	*Denied, except for his/her own documents*

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

FDP_ACC.1.1 (e) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among

subjects and objects covered by the SFP].

[assignment: access control SFP]
- CPY Access Control SFP in Table21
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the CPY Access Control SFP in Table 21

Table 21 CPY Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+CPY*	*Read*	*This package does not specify any access control restriction*	

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

FDP_ACC.1.1 (f) The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]
- DSR Access Control SFP in Table 22
[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].
- the list of subjects, objects, and operations among subjects and objects covered by the DSR Access Control SFP in Table 22

Table 22 DSR Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	*+DSR*	*Read* *- Retrieve and edit the document data in Mailbox*	*U.USER*	*Denied, except (1) for his/her own documents or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE* *- When the owner identifier of D.DOC matches the user identifier, retrieval and editing operations are permitted.*

FDP_ACF.1 (a) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (a) The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- Common Access Control SFP in Table 16
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of users as subjects and objects controlled under the Common Access Control SFP in Table 16, and for each, the indicated security attributes in Table 17

FDP_ACF.1.2 (a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- rules specified in the Common Access Control SFP in Table 16 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- In the U.ADMINISTRATOR process, operation to delete the documents in all Mailbox and all Private Print is permitted by On Demand Overwrite function.

FDP_ACF.1.4 (a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [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].
- none

FDP_ACF.1 (b) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (b) The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- TOE Function Access Control SFP *in Table 18*

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- users and *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP in Table 19*

FDP_ACF.1.2 (b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- [selection: the user is explicitly authorized by U.ADMINISTRATOR 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]
- rules specified in the TOE Function Access Control SFP in Table 18

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- 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]
-none

FDP_ACF.1.4 (b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [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].
-none

FDP_ACF.1(c)	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(c) The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- PRT Access Control SFP in Table 19
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the PRT Access Control SFP in Table 19, and for each, the indicated security attributes in Table 19.

FDP_ACF.1.2(c) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- rules specified in the PRT Access Control SFP in Table 19 governing access among Users and controlled objects using controlled operations on controlled objects.

FDP_ACF.1.3(c)	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]. [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]. *-none*
FDP_ACF.1.4(c)	The TSF shall *explicitly* deny access of subjects to objects based on the following additional rules: [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]. *- none*
FDP_ACF.1 (d) Hierarchical to: Dependencies:	Security attribute based access control No other components. FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1 (d)	The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. [assignment: access control SFP] ***- SCN Access Control SFP in Table 20*** [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. *- the list of subjects and objects controlled under the SCN Access Control SFP in Table 20, and for each, the indicated security attributes in Table 20.*
FDP_ACF.1.2 (d)	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among

controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- rules specified in the SCN Access Control SFP in Table 20 governing access among Users and controlled objects using controlled operations on controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- none

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

FDP_ACF.1 (e) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (e) The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- CPY Access Control SFP in Table 21

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the CPY Access Control SFP in Table 21, and for each, the indicated security attributes in Table 21.

FDP_ACF.1.2 (e) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- rules specified in the CPY Access Control SFP in Table 21 governing access among Users and controlled objects using controlled operations on controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- none

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

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

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (f) The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]
- DSR Access Control SFP in Table 22
[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- the list of subjects and objects controlled under the DSR Access Control SFP in Table 22, and for each, the indicated security attributes in Table 22.

FDP_ACF.1.2 (f) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
- rules specified in the DSR Access Control SFP in Table 22 governing access among Users and controlled objects using controlled operations on controlled objects.

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

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- none

FDP_ACF.1.4 (f) The TSF shall *explicitly* deny access of subjects to objects

based on the following additional rules: [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].
- none

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]
- none

6.1.4. Class FIA: Identification and Authentication

FIA_AFL.1(a) Authentication failure handling
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1(a) 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].

[assignment: list of authentication events]
- key operator authentication
[selection: [assignment: positive integer number] , an administrator configurable positive integer within [assignment: range of acceptable values]
- [assignment: positive integer number]

- 5

FIA_AFL.1.2 (a) 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]
- Identification and authentication of key operator is inhibited until the TOE is cycled.

FIA_AFL.1 (b) Authentication failure handling
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 (b) 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].

[assignment: list of authentication events]
- SA authentication (with local authentication)
[selection: [assignment: positive integer number] , an administrator configurable positive integer within [assignment: range of acceptable values]
- [assignment: positive integer number]
- 5

FIA_AFL.1.2 (b) 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]
- Identification and authentication of relevant user is inhibited until the TOE is cycled.

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]. *- Key Operator role* *- SA role* *- U.NORMAL role*
FIA_SOS.1 Hierarchical to: Dependencies:	Verification of secrets No other components. No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets *(SA password and U.NORMAL password when local authentication is used)* meet [assignment: a defined quality metric]. [assignment: a defined quality metric]. *Password length is restricted to 9 or more characters*
FIA_UAU.2 Hierarchical to: Dependencies:	User authentication before any action FIA_UAU.1 Timing of authentication FIA_UID.1 Timing of identification
FIA_UAU.2.1	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 Hierarchical to: Dependencies:	Protected authentication feedback No other components 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] *- display of asterisks (“*”) to hide the entered password characters*
FIA_UID.2	User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies
FIA_UID.2.1	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]
- Key Operator role
- SA role
- U.NORMAL role

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]
- none

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]
- none

6.1.5. Class FMT: Security Management

FMT_MOF.1	Management of security functions behavior
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [selection: determine the

behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

[selection: determine the behavior of, disable, enable, modify the behavior of]
- disable, enable, modify the behavior of
[assignment: list of functions]
-List of security functions in Table 23
[assignment: the authorized identified roles]
-the roles listed in Table 23

Table 23 List of Security Functions

Security Functions	Operation	Roles
User Authentication	*enable, disable, modify the behavior*	*U.ADMINISTRATOR*
Security Audit Log	*enable, disable*	*U.ADMINISTRATOR*
Internal Network Data Protection	*enable, disable, modify the behavior*	*U.ADMINISTRATOR*
Customer Engineer Operation Restriction	*enable, disable*	*U.ADMINISTRATOR*
Hard Disk Data Encryption	*enable, disable*	*U.ADMINISTRATOR*
Hard Disk Data Overwrite	*enable, disable, modify the behavior*	*U.ADMINISTRATOR*
Self Test	*enable, disable*	*U.ADMINISTRATOR*

FMT_MSA.1 (a) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (a) The TSF shall enforce the [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 authorized identified roles].

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

SFP(s)]
- ***Common Access Control SFP in Table16***
[selection: change default, query, modify, delete,
[assignment: other operations]]
- query, modify, delete, [assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 24

Table 24 Security Attributes and Authorized Roles

Security attributes	Operation	Roles
Key operator identifier	*modify*	*Key Operator*
SA identifier	*query* *modify* *delete, creation*	*U.ADMINISTRATOR*
General user identifier	*query* *modify* *delete, creation*	*U.ADMINISTRATOR*
Owner identifier for D.DOC (own document data in Mailbox)	*query*	*U.USER*
Owner identifier of D.DOC (all document data in Mailbox)	*query, delete*	*Key Operator*
Owner identifier of D.DOC (all document data in Mailbox)	*delete*	*SA*
Owner identifier of D.DOC (own document data in Private Print)	*query, delete, creation*	*U.USER*
Owner identifier of D.DOC (all document data in Private Print)	*query, delete*	*U.ADMINISTRATOR*
Owner identifier of D.FUNC	*query, delete*	*U.ADMINISTRATOR*

FMT_MSA.1 (b) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (b) The TSF shall enforce the [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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- TOE Function Access Control SFP *in Table 18,*
[selection: change default, query, modify, delete, [assignment: other operations]]
- query, modify ,delete ,[assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 18
[assignment: the authorized identified roles].
- the roles listed in Table 25

Table 25 Security Attributes and Authorized Roles(Function Access)

Security Attributes	Operation	Roles
Key operator identifier	*modify*	*Key Operator*
SA identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
General user identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
User identifier for each function	*query, modify*	*U.ADMINISTRATOR*

FMT_MSA.1 (c) 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 (c) The TSF shall enforce the [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

authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- PRT Access Control SFP in Table 19
[selection: change default, query, modify, delete,
[assignment: other operations]]
- query, modify, delete,[assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 26

Table 26 Security Attributes and Authorized Roles(PRT)

Security Attributes	Operation	Roles
Key operator identifier	*modify*	*Key Operator*
SA identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
General user identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (own document data in Private Print)	*query, delete, creation*	*U.USER*
Owner identifier of D.DOC (all document data in Private Print)	*query, delete*	*U.ADMINISTRATOR*

FMT_MSA.1 (d) 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 (d) The TSF shall enforce the [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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- SCN Access Control SFP in Table 20
[selection: change default, query, modify, delete,
[assignment: other operations]]
- query, modify,delete,[assignment: other operations]
[assignment: other operations]
- creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 27

Table 27 Security Attributes and Authorized Roles(SCN)

Security Attributes	Operation	Roles
Key operator identifier	*modify*	*Key Operator*
SA identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
General user identifier	*query, modify delete,creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (own document data in Mailbox)	*query*	*U.USER*
Owner identifier of D.DOC (all document data in Mailbox)	*query, delete*	*Key Operator*

FMT_MSA.1 (e) 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 (e) The TSF shall enforce the [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 authorized identified roles].

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

- CPY Access Control SFP in Table 21
[selection: change default, query, modify, delete,
[assignment: other operations]]
- none
[assignment: other operations]
- none
[assignment: list of security attributes]
- none
[assignment: the authorized identified roles].
- none

FMT_MSA.1 (f) 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 (f) The TSF shall enforce the [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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]
- DSR Access Control SFP in Table 22
[selection: change default, query, modify, delete,
[assignment: other operations]]
- query, modify ,delete,[assignment: other operations]
[assignment: other operations]
- Creation
[assignment: list of security attributes]
- the security attributes listed in Table 17
[assignment: the authorized identified roles].
- the roles listed in Table 28

Table 28 Security Attributes and Authorized Roles(DSR)

Security Attributes	Operation	Roles
Key operator identifier	*modify*	*Key Operator*

SA identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
General user identifier	*query, modify delete, creation*	*U.ADMINISTRATOR*
Owner identifier of D.DOC (own document data in Mailbox)	*query*	*U.USER*
Owner identifier of D.DOC (all document data in Mailbox)	*query, delete*	*Key Operator*

FMT_MSA.3 (a) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (a) The TSF shall enforce the, [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 Table16***
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- *[assignment: other property]*
- *Initialization property in Table 29*

Table 29 Initialization property

Object	Security Attributes	Default
D.DOC	*Owner identifier of D.DOC*	*Creator's user identifier and available user identifier*
D.FUNC	*Owner identifier of D.FUNC*	

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

[assignment: the authorized identified roles]
- *none*

FMT_MSA.3 (b) Static attribute initialization
Hierarchical to: No other components.

Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 (b)	The TSF shall enforce the [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] **-** *TOE Function Access control SFP in Table 18* [selection, choose one of: restrictive, permissive, [assignment: other property]] *- [assignment: other property]* *- permissive initialization property for basic functions such as copy, print, and scan as the default of security attribute.*
FMT_MSA.3.2 (b)	The TSF shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created. [assignment: the authorized identified roles] *- none*
FMT_MSA.3 (c) Hierarchical to: Dependencies:	Static attribute initialization No other components. FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 (c)	The TSF shall enforce the [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] *- PRT Access Control SFP in Table 19* [selection, choose one of: restrictive, permissive, [assignment: other property]] *- [assignment: other property]* *- Initialization property in Table 30*

Table 30 Initialization property

Object	Security Attributes	Default
D.DOC	*Owner identifier of D.DOC*	*Creator's user identifier and available user identifier*

FMT_MSA.3.2 (c) 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]
- none

FMT_MSA.3 (d) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (d) The TSF shall enforce the [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]
- SCN Access Control SFP in Table 20
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- Initialization property in Table 30

FMT_MSA.3.2 (d) 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]
- none

FMT_MSA.3 (e) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (e) The TSF shall enforce the [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]
- CPY Access Control SFP in Table 21
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- permissive

FMT_MSA.3.2 (e) 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]
- none

FMT_MSA.3 (f) Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (f) The TSF shall enforce the [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]
- DSR Access Control SFP in Table 22
[selection, choose one of: restrictive, permissive, [assignment: other property]]
- [assignment: other property]
- Initialization property in Table 30

FMT_MSA.3.2 (f) 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]
- none

FMT_MTD.1 (a) Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (a) The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[selection: change default, query, modify, delete, clear, [assignment: other operations]]
- query, modify, delete
[assignment: other operations]
- creation
[assignment: list of TSF data]
- TSF data listed in Table 31
[assignment: the authorized identified roles].
- selection, choose one of: Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]
- U.ADMINISTRATOR, Key Operator

Table 31 Operation of TSF Data

TSF Data	Operation	Roles
Data on key operator ID	*Modify*	*Key Operator*
Data on key operator Password	*Modify*	*Key Operator*
Data on SA ID	*query, modify, delete, creation*	*U.ADMINISTRATOR*
Data on SA Password	*modify*	*U.ADMINISTRATOR*
Data on User Authentication	*query, modify*	*U.ADMINISTRATOR*
Data on use of password entered from MFD control panel in user authentication	*query, modify*	*U.ADMINISTRATOR*
Data on minimum user password length	*query, modify*	*U.ADMINISTRATOR*
Data on Store Print	*query, modify*	*U.ADMINISTRATOR*

Data on Access denial due to authentication failure of system administrator	*query, modify*	*U.ADMINISTRATOR*
Data on Security Audit Log	*query, modify*	*U.ADMINISTRATOR*
Data on Internal Network Data Protection	*query, modify, delete*	*U.ADMINISTRATOR*
Data on Customer Engineer Operation Restriction	*query, modify*	*U.ADMINISTRATOR*
Data on Hard Disk Data Encryption	*query, modify*	*U.ADMINISTRATOR*
Data on Hard Disk Data Overwrite	*query, modify*	*U.ADMINISTRATOR*
Data on date and time	*query, modify*	*U.ADMINISTRATOR*
Data on Auto Clear	*query, modify*	*U.ADMINISTRATOR*
Data on Self Test	*query, modify*	*U.ADMINISTRATOR*
Data on Report Print	*query, modify*	*U.ADMINISTRATOR*

FMT_MTD.1 (b) Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (b) The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[selection: change default, query, modify, delete, clear, [assignment: other operations]]
- query, modify, delete
[assignment: other operations]
- creation
[assignment: list of TSF data]
- list of TSF data associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL in Table 32
[assignment: the authorized identified roles].
- selection, choose one of: Nobody, [selection: U.ADMINISTRATOR、U.NORMAL to whom such TSF data is associated].
- U.ADMINISTRATOR, U.NORMAL to whom such TSF data is

associated

Table 32 Operation of TSF Data

TSF Data	Operation	Roles
Data on General user ID	*query, modify, delete, creation*	*U.ADMINISTRATOR*
Data on General user Password	*modify*	*U.ADMINISTRATOR , U.NORMAL*

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]
- Security Management Functions listed in Table 33

Table 33 Security Management Functions Provided by TSF

Relevant SFR	Management Function	Management items defined by CC
FAU_GEN.1	*Management of data on Security Audit Log settings*	There are no management activities foreseen.
FAU_GEN.2	-	There are no management activities foreseen.
FAU_SAR.1	*Management of data on key operator and SA (ID and password)*	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	-	There are no management activities foreseen.
FAU_STG.1	-	There are no management activities foreseen.
FAU_STG.4	*none* *Reason: The control parameter of audit log is fixed and is not managed*	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FCS_CKM.1	-	There are no management

		activities foreseen.
FCS_COP.1	*Management of data on Hard Disk Data Encryption*	There are no management activities foreseen.
FDP_ACC.1(a) FDP_ACC.1(b) FDP_ACC.1(c) FDP_ACC.1(d) FDP_ACC.1(e) FDP_ACC.1(f)	-	There are no management activities foreseen.
FDP_ACF.1(a)	*- Management of user identifier* *- Management of owner identifier of D.DOC* *- Management of owner identifier of D.FUNC*	a)Managing the attributes used to make explicit access or denial based decisions.
FDP_ACF.1(b)	*- Management of user identifier* *- Management of owner identifier of function*	
FDP_ACF.1(c)	*- Management of user identifier* *- Management of owner identifier of D.DOC* *- Management of data on Store Print*	
FDP_ACF.1(d) FDP_ACF.1(f)	*- Management of user identifier* *- Management of owner identifier of D.DOC*	
FDP_ACF.1(e)	*None* *Reason: there are no additional security attributes and is not managed.*	
FDP_RIP.1	*Management of data on Hard Disk Data Overwrite*	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.
FIA_AFL.1(a) FIA_AFL.1(b)	*Management of data on access denial due to authentication failure of system administrator*	a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	*none*	a) If so indicated in the

	Reason: there are no additional security attributes and there are no additional security attributes to be managed.	assignment, the authorized administrator might be able to define additional security attributes for users.
FIA_SOS.1	*Management of Data on minimum user password length*	a) the management of the metric used to verify the secrets.
FIA_UAU.2	*- Management of data on use of password entered from MFD control panel in user authentication.* *- Management of data on key operator, SA, and general user (password)* *- Management of data on user authentication.* *- Management of data on minimum user password length*	a) Management of the authentication data by an administrator; b) Management of the authentication data by the user associated with this data;
FIA_UAU.7	-	There are no management activities foreseen.
FIA_UID.2	*- Management of data on key operator, SA, and general user (ID)* *- Management of data on user authentication.*	a) The management of the user identities.
FIA_USB.1	*None* *Reason: action and security attributes are fixed and are not managed.*	a) an authorized administrator can define default subject security attributes. b) an authorized administrator can change subject security attributes.
FMT_MOF.1	*Management of data on Customer Engineer Operation Restriction*	a) Managing the group of roles that can interact with the functions in the TSF;
FMT_MSA.1(a) FMT_MSA.1(b) FMT_MSA.1(c) FMT_MSA.1(d) FMT_MSA.1(e) FMT_MSA.1(f)	*None* *Reason: The role group is fixed and is not managed*	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3(a) FMT_MSA.3(b) FMT_MSA.3(c) FMT_MSA.3(d)	*None* *Reason: The role group is only a system administrator and is not managed.*	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default

FMT_MSA.3(e) FMT_MSA.3(f)		values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MTD.1(a)	*- Management of data on Customer Engineer Operation Restriction* *- Management of data on Report Print*	a) Managing the group of roles that can interact with the TSF data.
FMT_MTD.1(b)	*None* *Reason: The role group is fixed and is not managed*	
FMT_SMF.1	-	There are no management activities foreseen.
FMT_SMR.1	*None* *Reason: The role group is fixed and is not managed*	a) Managing the group of users that are part of a role.
FPT_STM.1	*- Management of time and data.*	a) management of the time.
FPT_TST.1	*- Management of data on Self Test.*	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate.
FTA_SSL.3	*- Management of data on Auto Clear.*	a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user; b) specification of the default time of user inactivity after which termination of the interactive session occurs.
FTP_ITC.1	*- Management of data on Internal Network Data Protection.*	a) Configuring the actions that require trusted channel, if supported.
FPT_FDI_EXP.1	*none* *Reason: The role and transfer conditions are fixed and are not managed.*	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.

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 [assignment: the authorized identified roles].

[assignment: the authorized identified roles]
- U.ADMINISTRATOR, U.NORMAL, key operator, SA

FMT_SMR.1.2 The TSF shall be able to associate users with roles, except for the role "Nobody" to which no user shall be associated.

6.1.6. Class FPT: Protection of the TSF

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].

[assignment: list of external interfaces]
- any external interfaces
[assignment: list of external interfaces]
- any Shared-medium interfaces

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

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].

[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]
- at the conditions [assignment: conditions under which self test should occur]
[assignment: conditions under which self test should occur]
- at initiation under which self test is set
[selection: [assignment: parts of TSF], the TSF].
- [assignment: parts of TSF]
- TSF executable code

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

[selection: [assignment: parts of TSF data], TSF data]
- [assignment: parts of TSF data]
- TSF data (excluding audit log data, and present time data)

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

[selection: [assignment: parts of TSF], TSF]
- [assignment: parts of TSF]
- TSF executable code

6.1.7. Class FTA:TOE Access

FTA_SSL.3	TSF-initiated termination
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

[assignment: time interval of user inactivity]
- Auto clear time can be set to 10 to 900 seconds on the control panel.
- Login timeout from CWIS is fixed to 20 minutes.
- There is no inactive time with printer driver.

6.1.8. Class FTP: Trusted Path/Channels

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 channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

[selection: the TSF, another trusted IT product]
- the TSF, another trusted IT product

FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

[assignment: list of functions for which a trusted channel is required].
- communication of D.DOC, D.FUNC, D.PROT and D.CONF over any Shared-medium Interface

6.2. セキュリティ保証要件（Security Assurance Requirements)

Table 34 にセキュリティ保証要件を記述する。
本 TOE の評価保証レベルは EAL2 である。 追加したセキュリティ保証コンポーネントは、ALC_FLR.2 である。

Table 34 セキュリティ保証要件

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

6.3. セキュリティ要件根拠 (Security Requirement Rationale)

6.3.1. セキュリティ機能要件根拠 (Security Functional Requirements Rationale)

セキュリティ機能要件とセキュリティ対策方針の対応を、Table 35に記述する。 この表で示す通り、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。また各セキュリティ対策方針が、セキュリティ機能要件により保証されている根拠を、Table36 に記述する。

Table 35 セキュリティ機能要件とセキュリティ対策方針の対応関係

Objectives / SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FAU_GEN.1										✓			
FAU_GEN.2										✓			
FAU_SAR.1												✓	
FAU_SAR.2												✓	
FAU_STG.1											✓		
FAU_STG.4											✓		
FCS_CKM.1													✓
FCS_COP.1													✓
FDP_ACC.1 (a)	✓	✓	✓										
FDP_ACC.1 (b)							✓						
FDP_ACC.1 (c)	✓												
FDP_ACC.1 (d)	✓												
FDP_ACC.1 (e)	✓												
FDP_ACC.1 (f)	✓												
FDP_ACF.1 (a)	✓	✓	✓										
FDP_ACF.1 (b)							✓						
FDP_ACF.1 (c)	✓												
FDP_ACF.1 (d)	✓												
FDP_ACF.1 (e)	✓												
FDP_ACF.1 (f)	✓												

Objectives / SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FDP_RIP.1	✓												
FIA_AFL.1 (a)							✓	✓					
FIA_AFL.1 (b)							✓	✓					
FIA_ATD.1							✓						
FIA_SOS.1							✓	✓					
FIA_UAU.2							✓	✓					
FIA_UAU.7							✓	✓					
FIA_UID.2	✓	✓	✓	✓	✓	✓	✓	✓		✓			
FIA_USB.1							✓						
FMT_MOF.1				✓	✓	✓							
FMT_MSA.1 (a)	✓	✓	✓	✓									
FMT_MSA.1 (b)				✓			✓						
FMT_MSA.1 (c)	✓			✓									
FMT_MSA.1 (d)	✓			✓									
FMT_MSA.1 (e)	✓			✓									
FMT_MSA.1 (f)	✓			✓									
FMT_MSA.3 (a)	✓	✓	✓										
FMT_MSA.3 (b)							✓						
FMT_MSA.3 (c)	✓												
FMT_MSA.3 (d)	✓												
FMT_MSA.3 (e)	✓												
FMT_MSA.3 (f)	✓												
FMT_MTD.1 (a)				✓	✓	✓							
FMT_MTD.1 (b)				✓	✓	✓							
FMT_SMF.1	✓	✓	✓	✓	✓	✓							
FMT_SMR.1	✓	✓	✓	✓	✓	✓	✓						
FPT_FDI_EXP.1								✓					
FPT_STM.1										✓			

Objectives / SFRs	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.CIPHER
FPT_TST.1									✓				
FTA_SSL.3							✓	✓					
FTP_ITC.1	✓	✓	✓	✓	✓	✓							

Table 36 セキュリティ対策方針によるセキュリティ機能要件根拠

セキュリティ対策方針	セキュリティ機能要件根拠
O.AUDIT.LOGGED (監査イベントの記録と認可されたアクセス)	O.AUDIT.LOGGED は TOE の使用・セキュリティに係わるイベントのログを作成・維持し、権限のない不正な漏洩・改ざんを防ぐ対策方針である。 本セキュリティ対策方針を実現するためには、 FAU_GEN.1 により監査対象イベントに対してセキュリティ監査ログデータが生成される。 ただし下記の機能要件は示す理由により監査は不要である。 FAU_STG.4：セキュリティ監査ログデータの総件数は固定であり格納、更新は自動的に処理される。 FCS_CKM.1：暗号鍵生成の失敗は起動時にエラーとなる FCS_COP.1：暗号化の失敗はジョブステータスとして取得される FMT_MSA.3：デフォルト値、ルールの変更は無い FAU_GEN.2、FIA_UID.2により各監査対象事象を、その原因となった利用者の識別情報に関連付ける。 FPT_STM.1 により TOE の持つ高信頼なクロックを用いて、監査対象イベントと共にタイムスタンプがセキュリティ監査ログに記録される。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.SOFTWARE.VERIFIED (ソフトウェア完全性の検証)	O.SOFTWARE.VERIFIED は TOE 自身の実行コードの自己検証の手順を提供する対策方針である。 本セキュリティ対策方針を実現するためには、 FPT_TST.1 により TSF 実行コードおよび TSF データの完全性を検証するための自己テスト機能を起動時に設定し実行することができる。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.INTERFACE.MA	O.INTERFACE.MANAGED はセキュリティポリシーに従って、外部インターフェース

セキュリティ対策方針	セキュリティ機能要件根拠
NAGED (外部インターフェースの管理)	である CWIS、操作パネル、プリンタードライバに関する操作を管理する対策方針である。 本セキュリティ対策方針を実現するためには、 攻撃者がシステム管理者が有する特権により保護資産へアクセスする事を防止するために、FIA_AFL.1(a)により機械管理者認証の認証失敗時に、 FIA_AFL.1(b)により SA の認証失敗時(本体認証時)に認証失敗によるアクセス拒否回数分の認証に失敗した場合、電源 OFF/ON が必要になる。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者およびシステム管理者を識別するために、CWIS と操作パネルへのアクセス時にユーザー識別認証が行われる。また、プライベートプリントの格納時にもユーザー識別認証が行われる。 FIA_UAU.7 によりユーザー認証に関して認証フィードバックは保護されるので、パスワードの漏洩は防げる。 FTA_SSL.3 により、CWIS と操作パネルに一定時間のアクセスが無い場合はログインをクリアし再認証を要求する。 プリンタードライバとのセッションを保持せずに要求処理後ただちにセッションを終了する。 FIA_SOS.1 により、SA と一般利用者の最小パスワード長を制限する。 FPT_FDI_EXP.1 により外部インターフェースからの受信データの内部ネットワークへの許可されない転送を制限する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.USER.AUTHORIZED (一般利用者と管理者の TOE 使用の認可)	O.USER.AUTHORIZED は TOE の使用を許可する前に、使用者がセキュリティポリシーに従って権限を付与されており、その認証と識別を求める対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_ACC.1(b)、FDP_ACF.1(b)によりユーザー識別認証を実施することで、許可された利用者のみに基本機能の操作を許可する。 攻撃者がシステム管理者が有する特権により保護資産へアクセスする事を防止するために、FIA_AFL.1(a)により機械管理者認証の認証失敗時に、 FIA_AFL.1(b)により SA の認証失敗時(本体認証時)に認証失敗によるアクセス拒否回数分の認証に失敗した場合、電源 OFF/ON が必要になる。 FIA_ATD.1、 FIA_USB.1 により機械管理者役割、SA 役割、一般利用者役割を維持することにより、許可された利用者のみにサブジェクトを割り当てる。 FIA_SOS.1 により、SA と一般利用者の最小パスワード長を制限する。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者およびシステム管理者を識別するために、CWIS と操作パネルからのアクセス時にユーザー識別認証が行われる。またプライベートプリントの格納時にもユーザー識別認証が行われる。 FIA_UAU.7 によりユーザー認証に関して認証フィードバックは保護されるので、パスワードの漏洩は防げる。 FMT_MSA.1(b)によりセキュリティ属性の問い合わせ、改変、削除、作成を管理する。 FMT_MSA.3 (b)により適切なデフォルト値を管理する。

セキュリティ対策方針	セキュリティ機能要件根拠
	FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FTA_SSL.3 により CWIS と操作パネルに一定時間のアクセスが無い場合は設定をクリアし再認証を要求する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.DOC.NO_DIS (利用者文書データの不正開示保護)	O.DOC.NO_DIS は TOE を権限のない不正な漏洩から User Document Data を守る対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_RIP.1 により内部ハードディスク装置に蓄積された利用済み文書データの、以前の情報の内容を利用できなくする。 FDP_ACC.1(a),FDP_ACC.1(c), FDP_ACC.1(d), FDP_ACC.1(e), FDP_ACC.1(f), FDP_ACF.1(a),FDP_ACF.1(c), FDP_ACF.1(d), FDP_ACF.1(e), FDP_ACF.1(f), FIA_UID.2 によりユーザー識別を実施することで、許可された利用者のみに、User Document Data の操作を許可する。 FMT_MSA.1(a),FMT_MSA.1(c),FMT_MSA.1(d)、FMT_MSA.1(e)、FMT_MSA.1(f)によりセキュリティ属性の問い合わせ、改変、削除、作成を管理する。 FMT_MSA.3 (a),FMT_MSA.3 (c),FMT_MSA.3 (d),FMT_MSA.3 (e),FMT_MSA.3 (f)により適切なデフォルト値を管理する。 FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FMT_SMF.1 により TOE セキュリティ管理機能をシステム管理者へ提供する。 FTP_ITC.1 により TOE と IT プロダクト間の内部ネットワーク上を流れる User Document Data を脅威から保護するために、通信データ暗号化プロトコルに対応する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.DOC.NO_ALT, (利用者文書データの不正改ざん保護)	O.DOC.NO_ALT は、TOE を権限のない不正な改ざんから User Document Data を守る対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_ACC.1(a)、FDP_ACF.1(a), FIA_UID.2 によりユーザー識別を実施することで、許可された利用者のみに、User Document Data の操作を許可する。 FMT_MSA.1(a)によりセキュリティ属性の問い合わせ、改変、削除、作成を管理する。 FMT_MSA.3 (a)により適切なデフォルト値を管理する。 FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FMT_SMF.1 により TOE セキュリティ管理機能をシステム管理者へ提供する。 FTP_ITC.1 により TOE と IT プロダクト間の内部ネットワーク上を流れる User Document Data を脅威から保護するために、通信データ暗号化プロトコルに対応する。

セキュリティ対策方針	セキュリティ機能要件根拠
	以上のセキュリティ機能要件により対策方針を満たすことができる。
O.FUNC.NO_ALT (利用者機能データの不正改ざん保護)	O.FUNC.NO_ALT は、TOE を権限のない不正な改ざんから User Function Data を守る対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_ACC.1(a),FDP_ACF.1(a), FIA_UID.2 によりユーザー識別を実施することで、許可された利用者のみに、User Function Data の操作を許可する。 FMT_MSA.1(a) によりセキュリティ属性の問い合わせ、改変、削除、作成を管理する。 FMT_MSA.3 (a)により適切なデフォルト値を管理する。 FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FMT_SMF.1 により TOE セキュリティ管理機能をシステム管理者へ提供する。 FTP_ITC.1 により TOE と IT プロダクト間の内部ネットワーク上を流れる User Function Data を脅威から保護するために、通信データ暗号化プロトコルに対応する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.PROT.NO_ALT, (TSF データの不正改ざん保護)	O.PROT.NO_ALT は TOE を権限のない不正な改ざんから TSF Data を守る対策方針である。 本セキュリティ対策方針を実現するためには、 FIA_UID.2 によりユーザー識別を実施することで、許可されたシステム管理者だけに、TSF Data の操作を許可する。 FMT_MOF.1 によりセキュリティ機能の動作や停止、および機能の設定は、システム管理者だけに限定しているので、システム管理者だけに制限される。 FMT_MSA.1(a), FMT_MSA.1(b),FMT_MSA.1(c),FMT_MSA.1(d)、FMT_MSA.1(e)、FMT_MSA.1(f)によりセキュリティ属性の改変、削除、作成を管理する。 FMT_MTD.1(a)によりセキュリティ機能の機能設定は、システム管理者だけに限定しているので、TOE 設定データの改変は、システム管理者だけに制限される。 FMT_MTD.1(b)により一般利用者 ID の設定は、システム管理者と所有者に限定している。 FMT_SMF.1 により TOE セキュリティ機能の管理機能の設定を、システム管理者へ提供する。 FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FTP_ITC.1 により TOE と IT プロダクト間の内部ネットワーク上を流れる TOE 設定データを脅威から保護するために、通信データ暗号化プロトコルに対応する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.CONF.NO_DIS, O.CONF.NO_ALT (TSF データの不正改	O.CONF.NO_DIS, O.CONF.NO_ALT は TOE を権限のない不正な漏洩や改ざんから D.CONF を守る対策方針である。 本セキュリティ対策方針を実現するためには、

セキュリティ対策方針	セキュリティ機能要件根拠
ざんおよび不正開示保護)	FIA_UID.2 によりユーザー識別を実施することで、許可された利用者だけに、D.CONF の操作を許可する。 FMT_MOF.1 によりセキュリティ機能の動作や停止、および機能の設定は、システム管理者だけに限定しているので、システム管理者だけに制限される。 FMT_MTD.1(a)によりセキュリティ機能の機能設定は、システム管理者だけに限定しているので、D.CONF の問い合わせ、改変は、システム管理者だけに制限される。 FMT_MTD.1(b)により一般利用者の IDとパスワードの設定は、システム管理者と所有者に限定している。 FMT_SMF.1 により TOE セキュリティ機能の管理機能の設定を、許可された利用者へ提供する。 FMT_SMR.1 により機械管理者、SA、システム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 FTP_ITC.1 により TOEと IT プロダクト間の内部ネットワーク上を流れるセキュリティ監査ログデータおよび D.CONF を脅威から保護するために、通信データ暗号化プロトコルに対応する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.AUDIT_STORAGE.PROTECTED	O.AUDIT_STORAGE.PROTECTED は監査記録を権限のないアクセス・削除・変更から守る対策方針である。 本セキュリティ対策方針を実現するためには、 FAU_STG.1 により監査ログファイルに格納されているセキュリティ監査ログデータを、不正な削除や改変から保護する。 FAU_STG.4 により監査ログが満杯になった時に、最も古いタイムスタンプで格納された監査ログを上書き削除して、新しい監査イベントを、監査ログファイルへ格納する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.AUDIT_ACCESS.AUTHORIZED	O.AUDIT_ACCESS.AUTHORIZED は監査記録が権限のある者によってのみ、潜在的なセキュリティ違反を検知する為に分析されるようにする対策方針である。 本セキュリティ対策方針を実現するためには、 FAU_SAR.1 により許可されているシステム管理者は、監査ログファイルからのセキュリティ監査ログデータの読み出し機能を提供する。 FAU_SAR.2 により許可されているシステム管理者以外の監査ログへのアクセスを禁止する。 以上のセキュリティ機能要件により対策方針を満たすことができる。
O.CIPHER	O.CIPHER は内部ハードディスク装置に蓄積されている文書データを取り出しても解析が出来ないように、内部ハードディスク装置上に蓄積されるデータを暗号化する対策方針である。 本セキュリティ対策方針を実現するためには、 FCS_CKM.1 により指定された 256 ビットの暗号鍵長に従って、暗号鍵が生成さ

セキュリティ対策方針	セキュリティ機能要件根拠
	れる。 FCS_COP.1により決められた暗号アルゴリズムと暗号鍵長で、文書データを内部ハードディスク装置へ蓄積する時に暗号化され、読み出し時に復号化される。 以上のセキュリティ機能要件により対策方針を満たすことができる。

6.3.2. 依存性の検証 (Dependencies of Security Functional Requirements)

セキュリティ機能要件が依存している機能要件、および依存関係を満足しない機能要件と、依存関係が満たされなくても問題がない根拠を、Table 37 に記述する。

Table 37 セキュリティ機能要件コンポーネントの依存性

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FAU_GEN.1 Audit data generation	FPT_STM.1	—
FAU_GEN.2 User identity association	FAU_GEN.1	FIA_UID.1: FIA_UID.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FAU_SAR.1 Audit review	FAU_GEN.1	—
FAU_SAR.2 Restricted audit review	FAU_SAR.1	—
FAU_STG.1 Protected audit trail storage	FAU_GEN.1	—
FAU_STG.4 Prevention of audit data loss	FAU_STG.1	—
FCS_CKM.1 Cryptographic key generation	FCS_COP.1	FCS_CKM.4: 暗号鍵は MFD の起動時に生成され、DRAM(揮発性メモリ)に格納される。 この暗号鍵に外部からアクセスする手段はないので、暗号鍵を破棄する必要性がない。
FCS_COP.1 Cryptographic operation	FCS_CKM.1	FCS_CKM.4: 暗号鍵は MFD の起動時に生成され、DRAM(揮発性メモリ)に格納される。 この暗号鍵に外部からアクセスする手段はないので、暗号鍵を破棄する必要性がない。

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FDP_ACC.1(a) Subset access control	FDP_ACF.1(a)	—
FDP_ACC.1(b) Subset access control	FDP_ACF.1(b)	—
FDP_ACC.1(c) Subset access control	FDP_ACF.1(c)	—
FDP_ACC.1(d) Subset access control	FDP_ACF.1(d)	—
FDP_ACC.1(e) Subset access control	FDP_ACF.1(e)	—
FDP_ACC.1(f) Subset access control	FDP_ACF.1(f)	—
FDP_ACF.1(a) Security attribute based access control	FDP_ACC.1(a) FMT_MSA.3(a)	—
FDP_ACF.1 (b) Security attribute based access control	FDP_ACC.1(b) FMT_MSA.3(b)	—
FDP_ACF.1 (c) Security attribute based access control	FDP_ACC.1(c) FMT_MSA.3(c)	—
FDP_ACF.1 (d) Security attribute based access control	FDP_ACC.1(d) FMT_MSA.3(d)	—
FDP_ACF.1 (e) Security attribute based access control	FDP_ACC.1e) FMT_MSA.3(e)	—
FDP_ACF.1 (f) Security attribute based access control	FDP_ACC.1(f) FMT_MSA.3(f)	—
FDP_RIP.1 Subset residual information protection	なし	
FIA_AFL.1 Authentication failure handling		FIA_UAU.1: FIA_UAU.2はFIA_UAU.1の上位階層の機能要件のため、FIA_UAU.1への依存性は満たされる。
FIA_ATD.1 User attribute definition	なし	

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FIA_SOS.1 Verification of secrets	なし	
FIA_UAU.2 User authentication before any action		FIA_UID.1: FIA_UID.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FIA_UAU.7 Protected authentication feedback		FIA_UAU.1: FIA_UAU.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FIA_UID.2 User identification before any action	なし	
FIA_USB.1 User-subject binding	FIA_ATD.1	—
FMT_MOF.1 Management of security functions behavior	FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(a) Management of security attributes	FDP_ACC.1(a) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(b) Management of security attributes	FDP_ACC.1(b) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(c) Management of security attributes	FDP_ACC.1(c) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(d) Management of security attributes	FDP_ACC.1(d) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(e) Management of security attributes	FDP_ACC.1(e) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.1(f) Management of security attributes	FDP_ACC.1(f) FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.3(a) Static attribute initialization	FMT_MSA.1(a) FMT_SMR.1	—

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FMT_MSA.3(b) Static attribute initialization	FMT_MSA.1(b) FMT_SMR.1	―
FMT_MSA.3(c) Static attribute initialization	FMT_MSA.1(c) FMT_SMR.1	―
FMT_MSA.3(d) Static attribute initialization	FMT_MSA.1(d) FMT_SMR.1	―
FMT_MSA.3(e) Static attribute initialization	FMT_MSA.1(e) FMT_SMR.1	―
FMT_MSA.3(f) Static attribute initialization	FMT_MSA.1(f) FMT_SMR.1	―
FMT_MTD.1 Management of TSF data	FMT_SMF.1 FMT_SMR.1	―
FMT_SMF.1 Specification of management functions	なし	
FMT_SMR.1 Security roles		FIA_UID.1: FIA_UID.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FPT_STM.1 Reliable time stamp	なし	
FPT_TST.1 TSF testing	なし	
FTA_SSL.3 TSF-initiated termination	なし	
FTP_ITC.1 Inter-TSF trusted channel	なし	
FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces	FMT_SMF.1 FMT_SMR.1	―

6.3.3. セキュリティ保証要件根拠 (Security Assurance Requirements Rationale)

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

7. TOE 要約仕様 (TOE Summary Specification)

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。

7.1. セキュリティ機能 (Security Functions)

Table 38 に TOE セキュリティ機能とセキュリティ機能要件の対応を示す。
本節で説明する TOE セキュリティ機能は 6.1 節に記述されるセキュリティ機能要件を満たすものである。

Table 38 TOE セキュリティ機能とセキュリティ機能要件の対応関係

セキュリティ機能 / セキュリティ機能要件	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT	TSF_INF_FLOW	TSF_S_TEST
FAU_GEN.1						✓			
FAU_GEN.2						✓			
FAU_SAR.1						✓			
FAU_SAR.2						✓			
FAU_STG.1						✓			
FAU_STG.4						✓			
FCS_CKM.1		✓							
FCS_COP.1		✓							
FDP_ACC.1(a)			✓						
FDP_ACC.1(b)			✓						
FDP_ACC.1(c)			✓						
FDP_ACC.1d)			✓						
FDP_ACC.1(e)			✓						
FDP_ACC.1(f)			✓						
FDP_ACF.1(a)			✓						
FDP_ACF.1(b)			✓						
FDP_ACF.1(c)			✓						
FDP_ACF.1(d)			✓						
FDP_ACF.1(e)			✓						
FDP_ACF.1(f)			✓						
FDP_RIP.1	✓								
FIA_AFL.1(a)			✓						
FIA_AFL.1(b)			✓						
FIA_ATD.1			✓						
FIA_SOS.1			✓						

セキュリティ機能 / セキュリティ機能要件	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT	TSF_INF_FLOW	TSF_S_TEST
FIA_UAU.2			✓						
FIA_UAU.7			✓						
FIA_UID.2			✓						
FIA_USB.1			✓						
FMT_MOF.1				✓	✓				
FMT_MSA.1(a)			✓						
FMT_MSA.1(b)			✓						
FMT_MSA.1(c)			✓						
FMT_MSA.1(d)			✓						
FMT_MSA.1(e)			✓						
FMT_MSA.1(f)			✓						
FMT_MSA.3(a)				✓					
FMT_MSA.3(b)				✓					
FMT_MSA.3(c)				✓					
FMT_MSA.3(d)				✓					
FMT_MSA.3(e)				✓					
FMT_MSA.3(f)				✓					
FMT_MTD.1(a)				✓	✓				
FMT_MTD.1(b)				✓					
FMT_SMF.1				✓	✓				
FMT_SMR.1				✓					
FTA_SSL.3			✓						
FTP_ITC.1							✓		
FPT_FDI_EXP.1								✓	
FPT_STM.1						✓			
FPT_TST.1									✓

以下では各 TOE セキュリティ機能に関して概要と対応するセキュリティ機能要件について説明する。

7.1.1. ハードディスク蓄積データ上書き消去機能(TSF_IOW)

ハードディスク蓄積データ上書き消去機能は、システム管理者によりシステム管理者モードで設定された「ハードディスク蓄積データ上書き消去機能設定」に従い、コピー機能、プリンター機能、スキャナー機能、ネットワ

ークスキャン機能の各ジョブの完了後に、内部ハードディスク装置に蓄積された利用済み文書データに対して、内部ハードディスク装置の文書データ領域を、1 回または 3 回の上書きにより消去する。これは複合機の使用環境に応じて、処理の効率性を優先する場合と、セキュリティ強度を優先する場合を考慮しているためである。
処理の効率性を優先する場合は、上書き消去の回数を1回とし、セキュリティ強度を優先する場合は、上書き消去の回数を３回とする。 ３回の上書き消去回数は、1回に比べて処理速度は低下するが、より強固な上書き消去回数(推奨値)である。
さらに、システム管理者が設定した時刻またはマニュアル指示で蓄積文書を削除して上書き消去する(On Demand Overwrite 機能)。

(1) FDP_RIP.1 Subset residual information protection (サブセット残存情報保護)
TOE は各ジョブ完了後の上書き消去機能の制御として、上書き回数 1 回(”0(ゼロ)”による上書き)と、3 回(乱数・乱数・”0(ゼロ)”による上書き)の選択が出来る。また内部ハードディスク装置上に、上書き消去予定の利用済み文書データの一覧を持ち、TOE 起動時に一覧をチェックして、消去未了の利用済み文書データが存在する場合は、上書き消去処理を実行する。

7.1.2. ハードディスク蓄積データ暗号化機能(TSF_CIPHER)

ハードディスク蓄積データ暗号化機能は、システム管理者によりシステム管理者モードで設定された「ハードディスク蓄積データ暗号化機能設定」に従い、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能や各種機能設定時に内部ハードディスク装置に蓄積される文書データの暗号化を行う。

(1) FCS_CKM.1 Cryptographic key generation (暗号鍵生成)
TOE はシステム管理者により設定された「ハードディスク蓄積データ暗号化キー」を使用し、起動時に富士ゼロックス標準の FXOSENC 方式アルゴリズムによって 256 ビットの暗号鍵生成を行う(「ハードディスク蓄積データ暗号化キー」が同じであれば、同じ暗号鍵が生成される)。なお FXOSENC 方式アルゴリズムは、十分な複雑性を持ったセキュアなアルゴリズムである。

(2) FCS_COP.1 Cryptographic operation (暗号操作)
TOE は内部ハードディスク装置に文書データを蓄積する際に、起動時に暗号鍵生成(FCS_CKM.1)により生成した 256 ビット長の暗号鍵と FIPS PUB 197 に基づく AES アルゴリズムとにより文書データの暗号化を行う。 また蓄積した文書データを読み出す場合も同様に、起動時に生成した 256 ビット長の暗号鍵と AES アルゴリズムにより復号化を行う。

7.1.3. ユーザー認証機能(TSF_USER_AUTH)

ユーザー認証機能は、許可された特定の利用者だけに MFD の機能を使用する権限を持たせるために、操作パネル、利用者クライアントの CWIS、プリンタードライバからユーザーID とユーザーパスワードを入力させて識別認証する機能である。
MFD または外部のサーバーに登録されているユーザー情報を利用して、認証を行う。

ユーザー情報の登録方法によって、次の 2 種類がある。

a) 本体認証

本体認証は、TOE 内に登録したユーザー情報を使用して認証管理を行う。

b) 外部認証

外部の認証サーバーに対して認証を行う。TOE 内にユーザー情報は登録されていない。
外部認証は、外部の認証サーバー(LDAP サーバー、Kerberos サーバー) で管理されているユーザー情報を使用して、認証する。

認証が成功した利用者のみが下記の機能を使用可能となる。

a) 本体操作パネルで制御される機能

コピー機能、スキャン機能、ネットワークスキャン機能、親展ボックス操作機能、プリンター機能(プリンタードライバでの認証管理の設定が条件であり印刷時に操作パネルで認証する)

b) CWIS で制御される機能

機械状態の表示、ジョブ状態・履歴の表示、親展ボックスからの文書データ取出し機能、ファイル指定によるプリント機能

c) 利用者クライアントのプリンタードライバを使用する機能

利用者クライアント上のデータを、MFD が解釈可能なページ記述言語(PDL)で構成された印刷データに変換し TOE にプリントデータを蓄積する（プライベートプリント）。利用者が利用者クライアントのプリンタードライバで認証管理を設定した状態でプリント指示をすると、MFD は受信データをビットマップデータに変換(デコンポーズ)してユーザーID ごとに内部ハードディスクに蓄積する。

また本機能は操作パネルおよびシステム管理者クライアントから TOE セキュリティ機能の参照と設定変更を行う権限を持たせるためにシステム管理者 ID とパスワードを入力させて識別認証するものでもある。

(1) FIA_AFL.1(a) Authentication failure handling (認証失敗時の取り扱い)

TOE はシステム管理者モードへアクセスする前に、システム管理者の認証を行うが、認証時の認証失敗対応機能を提供している。機械管理者 ID 認証失敗を検出し、アクセス拒否回数で設定されている 5 回の連続失敗に達すると、操作パネルでは電源切断/投入以外の操作は受け付けなくなり、Web ブラウザでも MFD 本体の電源の切断/投入まで認証操作は受け付けなくなる。

(2) FIA_AFL.1(b) Authentication failure handling (認証失敗時の取り扱い)

TOE はシステム管理者モードへアクセスする前に、システム管理者の認証を行うが、認証時の認証失敗対応機能を提供している。
本体認証時に SA の ID 認証失敗を検出しアクセス拒否回数で設定されている 5 回の連続失敗に達すると、操作パネルでは電源切断/投入以外の操作は受け付けなくなり、Web ブラウザでも MFD 本体の電源の切断/投入まで認証操作は受け付けなくなる。

(3) FIA_ATD.1 User attribute definition (利用者属性定義)

TOE は機械管理者、SA および一般利用者の役割を定義し維持する。

(4) FIA_SOS.1 Verification of secrets（秘密の検証）

TOE は SA、一般利用者のパスワード設定時に最小文字数に至らない場合は設定を拒否する。

(5) FIA_UAU.2 User authentication before any action (アクション前の利用者認証)
FIA_UID.2 User identification before any action (アクション前の利用者識別)

TOE は操作パネル、利用者クライアントの Web ブラウザを通じて MFD 機能の操作を許可する前に、ID とパスワードを入力させて、入力された ID とパスワードが、TOE 設定データに登録されているパスワード情報と一致することを検証する。またプライベートプリントの格納時にも ID とパスワード検証によるユーザー識別認証が行われる。認証(FIA_UAU.2)と識別(FIA_UID.2)は、同時に実行され識別・認証の両方が成功した時のみ操作が許可される。

(6) FIA_UAU.7 Protected authentication feedback(保護されたフィードバック)

TOE はユーザー認証時に、パスワードを隠すために、パスワードとして入力された文字数と同数の`*`文字を、操作パネルや Web ブラウザに表示する機能を提供する。

(7) FIA_USB.1 User-subject binding(利用者・サブジェクト結合)

TOE は認証された ID から機械管理者、SA および一般利用者の役割をサブジェクトに割り当てる。

(8) FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MSA.1(c)、FMT_MSA.1(d)、FMT_MSA.1(e)、FMT_MSA.1(f) Management of security attributes(セキュリティ属性の管理)

TOE は Table 39 の通り、セキュリティ属性の操作をユーザー認証機能により識別認証された利用者に制限する。

Table 39 セキュリティ属性の管理

セキュリティ属性	操作	役割
機能に対応する利用者識別情報	問い合わせ、改変	機械管理者、SA
D.DOC(親展ボックス内の所有文書データ)に対応する所有者識別情報	問い合わせ	一般利用者、SA、機械管理者
D.DOC(親展ボックス内のすべての文書データ)に対応する所有者識別情報	問い合わせ、削除	機械管理者
D.DOC(親展ボックス内のすべての文書データ)に対応する所有者識別情報	削除	SA
D.DOC(プライベートプリント内の所有文書データ)に対応する所有者識別情報	問い合わせ、削除、作成	一般利用者、機械管理者、SA
D.DOC(プライベートプリント内のすべての文書データ)に対応する所有者識別情報	問い合わせ、削除	機械管理者、SA
D.FUNC(ジョブ情報)に対応する所有者識別情報	問い合わせ、削除、	機械管理者、SA

(9) FTA_SSL.3 TSF-initiated termination (TSF 起動による終了)

TOE は Web ブラウザから CWIS に一定時間(20 分)のアクセスが無い場合はログイン(認証セッション)をクリアし再認証を要求する。

また操作パネルから一定時間(10～900 秒で設定可能)の操作が無い場合は、操作パネルの設定がクリアされ認証画面へ戻る。

プリンタードライバとのセッションを保持せず、プリントの要求処理後ただちにセッションを終了する。

(10) FDP_ACC.1(a)、FDP_ACC.1(b)、FDP_ACC.1(c)、FDP_ACC.1(d)、FDP_ACC.1(e)、FDP_ACC.1(f) Subset access control (サブセットアクセス制御), FDP_ACF.1(a)、FDP_ACF.1(b)、FDP_ACF.1(c)、FDP_ACF.1(d)、FDP_ACF.1(e)、FDP_ACF.1(f) Security attribute based access control (セキュリティ属性によるアクセス制御)

TOE は Table 40 に示すとおり、ユーザー認証機能により MFD の基本機能であるコピー、スキャン、プリントの操作を識別認証された利用者に制限する。

Table 40 基本機能へのアクセス制御

機能	許可される操作と規則	利用者
コピー機能	機能に対応する利用者識別情報と利用者識別情報が一致した場合、操作パネルからのコピー操作、再出力用データ(コピー文書データ)の同時保存、および再出力用保存が許可される。	機械管理者 SA 一般利用者
スキャナー機能、ネットワークスキャン機能	機能に対応する利用者識別情報と利用者識別情報が一致した場合、操作パネルからの親展ボックスへのスキャン操作および操作パネルからの利用者クライアント、FTP サーバー、Mail サーバーへのスキャンデータ送信が許可される。	
プリンター機能、親展ボックス操作	機能に対応する利用者識別情報と利用者識別情報が一致した場合、利用者クライアントからのプリントデータをプライベートプリントへ保存、プライベートプリントデータ内の文書データの印刷、親展ボックス内文書データの取り出し/編集(*1)が許可される。	

TOE は Table 41 に示すとおり、利用者データへの操作を識別認証された利用者に制限する。

Table 41 利用者データへのアクセス制御

利用者データ	許可される操作と規則	利用者
コピーデータ	基本機能のアクセス制御で許可されたコピージョブが実行される。 D.DOC(コピーデータ)の削除機能は無い。	機械管理者 SA 一般利用者
スキャンデータ	基本機能のアクセス制御で許可されたスキャンジョブが実行されると、スキャンデータの FTP サーバー、Mail サーバーへの送信が許可される。 D.DOC(スキャンデータ)の削除機能は無い。	機械管理者 SA 一般利用者

利用者データ	許可される操作と規則	利用者
親展ボックス内の文書データ	D.DOC(親展ボックス内のすべての文書データ)に対応する所有者識別情報と利用者識別情報が一致した場合、すべての親展ボックス内の文書データの取り出し/編集(*1)、削除が許可される。	機械管理者
	D.DOC(親展ボックス内の所有文書データ)に対応する所有者識別情報と利用者識別情報が一致した場合、親展ボックス内の所有文書データの取り出し/編集(*1)、削除が許可される。	一般利用者、SA
	識別認証されたシステム管理者は、On Demand Overwrite 機能により D.DOC(親展ボックス内のすべての文書データ)の削除が許可される。	機械管理者 SA
プライベートプリント内の文書データ	D.DOC(プライベートプリント内のすべての文書データ)に対応する所有者識別情報と利用者識別情報が一致した場合、プライベートプリント内のすべての文書データの印刷、削除が許可される。	機械管理者 SA
	D.DOC(プライベートプリント内の所有文書データ)に対応する所有者識別情報と利用者識別情報が一致した場合、プライベートプリント内の所有文書データの印刷、削除が許可される。	一般利用者
	識別認証されたシステム管理者は、On Demand Overwrite 機能によりD.DOC(プライベートプリント内のすべての文書データ)の削除が許可される。	機械管理者 SA
実行中のジョブデータ	D.FUNC に対応する所有者識別情報と利用者識別情報が一致した場合、コピー、スキャン、プリントの実行中ジョブの削除,改変の操作が許可される。	機械管理者 SA

TOE は Table 41 に示すとおり、ユーザー認証機能により親展ボックス、プライベートプリント操作を認証された利用者に制限する。

- 蓄積プリント機能(プライベートプリント機能)
  MFD で「プライベートプリントに保存」の設定を行い、利用者が利用者クライアントのプリンタードライバで認証管理を設定した状態でプリント指示をする場合、識別認証後に印刷データをビットマップデータに変換(デコンポーズ)してユーザーID ごとのプライベートプリントとして内部ハードディスク装置に一時蓄積する。また CWIS からユーザーIDとパスワードを入力し、認証後に利用者クライアント内のファイル指定によりプリント指示をする場合も同様にユーザーID ごとのプライベートプリントとして内部ハードディスク装置に一時蓄積される。
  利用者は一時蓄積されたプリントデータを確認するために、MFD の操作パネルからユーザーID とパスワードを入力し、認証されるとユーザーID に対応したプリント待ちのリストだけが表示される。利用者はこのリストから印刷指示、または削除の指示が可能となる。

- 親展ボックス操作機能
  図 3 には図示されていない IIT から親展ボックスにスキャンデータとコピーデータを格納することが可能であ

る。
個人親展ボックスでは、個人親展ボックスを作成したユーザーIDと同じIDで認証された一般利用者、SAおよび機械管理者のみが、ボックス内データの取出し/編集(*1)や印刷、削除が可能である。

*1) ・スキャン文書データに対する操作:印刷、プレビュー、CWISから利用者クライアントへのエクスポート。
・コピー文書データに対する操作:印刷、プレビュー、編集

7.1.4. システム管理者セキュリティ管理機能 (TSF_FMT)

システム管理者セキュリティ管理機能は、ある特定の利用者へ特別な権限を持たせるために、システム管理者モードへのアクセスをシステム管理者のみに制限して、許可されたシステム管理者のみに操作パネルおよびシステム管理者クライアントからTOEセキュリティ機能の参照と設定変更を行う権限を許可する。

(1) FMT_MOF.1 Management of security functions behaviour(セキュリティ機能のふるまいの管理)
FMT_MTD.1(a)、FMT_MTD.1(b) Management of TSF data (TSFデータの管理)
FMT_SMF.1 Specification of Management Functions (管理機能の特定)
FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MSA.1(c)、FMT_MSA.1(d)、
FMT_MSA.1(e)、FMT_MSA.1(f) Management of security attributes(セキュリティ属性の管理)

TOEは識別認証されたシステム管理者のみに、下記のTOEセキュリティ機能に関係するTOE設定データの参照と設定変更、および各機能の有効/無効を設定するユーザーインターフェースを提供する。
またこれらの機能により、要求されるセキュリティ管理機能を提供する。

操作パネルからは下記のTOEセキュリティ機能の設定を参照し、設定変更を行うことが可能である。

- ハードディスク蓄積データ上書き消去機能の設定を参照し、有効/無効、上書き回数の設定を行う
- ハードディスク蓄積データ暗号化機能の設定を参照し、有効/無効の設定を行う
- ハードディスク蓄積データ暗号化キーの設定を行う
- 本体パネルからの認証時のパスワード使用の設定を参照し、有効/無効の設定を行う
- システム管理者認証失敗によるアクセス拒否設定を参照し、有効/無効、拒否回数の設定を行う
- 機械管理者IDとパスワードの設定を行う ;機械管理者のみ可能
- SA、一般利用者IDの設定を参照しIDとパスワードの設定を行う ;本体認証時のみ
- ユーザーパスワード(一般利用者とSA)の最小文字数制限を参照し設定を行う ;本体認証時のみ
- 内部ネットワークデータ保護機能のTLS通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能のIPSec通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能のS/MIME通信の設定を参照し、有効/無効および詳細情報の設定を行う
- On Demand Overwrite機能の設定を参照し、有効/無効および削除時刻の設定を行う
- ユーザー認証機能の設定を参照し、本体認証/外部認証/無効および詳細情報の設定を行う

・ 蓄積プリント機能の設定を参照し、蓄積/印刷の設定を行う
・ 日付、時刻を参照し設定を行う
・ 操作パネルオートクリア機能の設定を参照し、有効/無効およびクリア時間の設定を行う
・ 自己テスト機能の設定を参照し、有効/無効の設定を行う
・ レポート出力の設定を参照し、システム管理者限定/利用者の設定を行う

またシステム管理者クライアントから Web ブラウザを通じて CWIS 機能により、下記の TOE セキュリティ機能の設定を参照し、設定変更を行うことが可能である

・ 機械管理者 ID とパスワードの設定を行う ;機械管理者のみ可能
・ SA、一般利用者の ID 設定を参照し、ID とパスワードの設定を行う
・ システム管理者認証失敗によるアクセス拒否設定を参照し、有効/無効、拒否回数の設定を行う
・ ユーザーパスワード(一般利用者と SA)の最小文字数制限を参照し設定を行う ;本体認証時のみ
・ セキュリティ監査ログ機能の設定を参照し有効/無効の設定を行う
(有効時は、セキュリティ監査ログデータをタブ区切りのテキストファイルで、システム管理者クライアント PC 上にダウンロードすることが可能。)
・ 内部ネットワークデータ保護機能の TLS 通信の設定を参照し、有効/無効および詳細情報の設定を行う
・ 内部ネットワークデータ保護機能の IPSec 通信の設定を参照し、有効/無効および詳細情報の設定を行う
・ 内部ネットワークデータ保護機能の S/MIME 通信の設定を参照し、有効/無効および詳細情報の設定を行う
・ X.509 証明書を作成/アップロード/ダウンロードする
・ On Demand Overwrite 機能の設定を参照し、有効/無効および削除時刻の設定を行う
・ ユーザー認証機能の設定を参照し、本体認証/外部認証/無効および詳細情報の設定を行う
・ CWIS オートクリア機能の設定を参照し、有効/無効の設定を行う

(2) FMT_MSA.3(a)、FMT_MSA.3(b)、FMT_MSA.3(c)、FMT_MSA.3(d)、FMT_MSA.3(e)、FMT_MSA.3(f) Static attribute initialization (静的属性初期化)
TOE は基本機能であるコピー機能、プリンター機能、スキャナー機能、に対しセキュリティ属性のデフォルト値として全機能許可を設定する。
また D.DOC、D.FUNC に関しセキュリティ属性のデフォルト値として、所有者識別情報に作成した利用者識別情報と利用可能な利用者識別情報を設定する。
個人親展ボックスでは、親展ボックスを作成した SA または一般利用者個人と機械管理者の利用者識別情報を所有者識別情報として設定する。

(3) FMT_SMR.1 Security roles(セキュリティ役割)
TOE は機械管理者、SA、システム管理者および一般利用者の役割を維持し、その役割を正当な利用者に関連付けている。

7.1.5. カストマーエンジニア操作制限機能 (TSF_CE_LIMIT)

カストマーエンジニア操作制限機能は、カストマーエンジニアがシステム管理者セキュリティ管理機能

(TSF_FMT)に関する設定の参照および変更が出来ないようにカストマーエンジニアのシステム管理者モードへの操作を制限する機能である。
この機能により、カストマーエンジニアによる設定変更が出来なくなる。

(1) FMT_MOF.1 Management of security functions behaviour(セキュリティ機能のふるまいの管理)
FMT_MTD.1(a) Management of TSF data (TSF データの管理)
FMT_SMF.1 Specification of Management Functions (管理機能の特定)

TOE は認証されたシステム管理者のみに、操作パネルと CWIS からカストマーエンジニア操作制限機能に関する TOE 設定データの参照と設定変更(機能の有効/無効)のためのユーザーインターフェースを提供する。

7.1.6. セキュリティ監査ログ機能(TSF_FAU)

セキュリティ監査ログ機能は、システム管理者によりシステム管理者モードで設定された「監査ログ設定」に従い、すべての TOE 利用者に対して、いつ、誰が、どのような作業を行ったかという事象や重要なイベント(例えば障害や構成変更、ユーザー操作など)を、追跡記録するためのセキュリティ監査ログ機能を提供する。

(1) FAU_GEN.1 Audit data generation(監査データ生成)
監査データの生成は、定義された監査対象イベントが、監査ログに記録されることを保証する。

Table 42 に監査ログの詳細を示す

Table 42 監査ログのデータ詳細

監査ログ対象イベントは、以下の固定長データと共に記録される。: Date:日付データ(yyyy/mm/dd, mm/dd/yyyy, dd/mm/yyyy のいずれか) Time:時刻データ(hh:mm:ss) Logged Events:イベント名称(最大 32 桁の任意文字列) User Name:利用者名(最大 32 桁の任意文字列) Description:イベントに関する内容の説明(最大 32 桁の任意文字列で詳細は下記参照のこと) Status:イベントの処理結果もしくは状態(最大 32 桁の任意文字列で詳細は下記参照のこと)

Logged Events	Description	Status
デバイスの状態変化		
System Status	Started normally (cold boot)	-
	Started normally (warm boot)	
	Shutdown requested	
	Self Test	Successful/Failed

ユーザー認証		
Login/Logout	Login	Successful, Failed (Invalid UserID), Failed (Invalid Password), Failed
	Logout	
	Locked System Administrator Authentication	-
監査ポリシー変更		
Audit Policy	Audit Log	Enable/Disable
ジョブステータス		
Job Status	Print	Completed, Completed with Warnings, Canceled by User, Canceled by Shutdown, Aborted, Unknown
	Copy	
	Scan	
	Mailbox*1	
デバイス設定変更		
Device Settings	Adjust Time	Successful/Failed
	Add User	
	Edit User	
	Delete User	
	Switch Authentication Mode	Successful (設定項目も保存)
	Change Security Setting	
デバイス格納データへのアクセス		
Device Data	Export Audit Log	Successful/Failed
通信結果		
Communication	Trusted Communication	Failed (プロトコルと通信先も保存)

*1)"Mailbox"は親展ボックス内の文書データ操作を表す

(2) FAU_GEN.2 User identity association(利用者識別情報の関連付け)

TOE は定義された監査対象イベントを監査ログファイルへ記録する時に、その原因となった利用者の識別情報に関連付けて記録している。

(3) FAU_SAR.1 Audit review (監査レビュー)

セキュリティ監査ログデータに記録されたすべての情報を、読み出せることを保証する。
また"テキストファイルとして保存する"という名称のボタンがあり、この機能によりセキュリティ監査ログデータを、タブ区切りのテキストファイルとして、ダウンロードすることが出来る。 セキュリティ監査ログデータをダウンロードする時は、Web ブラウザを利用する前に、TLS 通信を有効に設定されていなければならない。

(4) FAU_SAR.2 Restricted audit review(限定監査レビュー)

セキュリティ監査ログデータの読み出しを、認証されたシステム管理者のみに限定する。
セキュリティ監査ログデータへのアクセスは、システム管理者が Web ブラウザのみ使用可能で、操作パネル

からアクセスすることは出来ない。 システム管理者が Web ブラウザを通して TOE へログインしていなければ、システム管理者の認証(ログイン)後に使用可能になる。

(5) FAU_STG.1 Protected audit trail storage(保護された監査証跡格納)
セキュリティ監査ログデータは読み出し機能のみで、削除機能や修正機能は存在しなく、不正な改ざんや改変から保護されている。

(6) FAU_STG.4 Prevention of audit data loss(監査データ損失の防止)
セキュリティ監査ログデータが満杯になった時、最も古いタイムスタンプで記録された監査データに上書きして、新しい監査データが損失することなく記録される。
監査ログ対象のイベントは、タイムスタンプと共に NVRAM に保存され 50 件に達した場合、NVRAM 上のログを 50 件単位で一つのファイル(以下、「監査ログファイル」と呼ぶ)として、内部ハードディスク装置へ保存をして、最大 15,000 件のイベントを保存することが出来る。 15,000 件を超える場合は、一番古いタイムスタンプで記録された監査ログファイルから順次消去して、繰り返してイベントが記録される。

(7) FPT_STM.1 Reliable time stamps(高信頼タイムスタンプ)
定義された監査対象イベントを監査ログファイルへ記録する時に、TOE が持っているクロック機能によるタイムスタンプを発行する機能を提供する。
時計の設定変更は TSF_FMT によりシステム管理者のみが可能である。

7.1.7. 内部ネットワークデータ保護機能(TSF_NET_PROT)

内部ネットワークデータ保護機能は、システム管理者によりシステム管理者モードで設定された下記 3 つのプロトコル設定の定義により、内部ネットワークデータ保護機能が提供される。

(1) FTP_ITC.1 Inter-TSF trusted channel (TSF 間高信頼チャネル)
TOE と TOE または高信頼 IT 製品間でセキュアなデータ通信が保証される暗号化通信プロトコルにより、文書データ、ジョブ情報、セキュリティ監査ログデータおよび TOE 設定データを保護する機能を提供する。
この高信頼チャネルは、他の通信チャネルと論理的に区別され、その端点の保証された識別および改変や暴露から、通信データを保護する能力を持っている。
TOE が提供する暗号化通信は以下の通りである。

プロトコル	通信先	暗号アルゴリズム
TLS	クライアント PC （Web ブラウザー、プリンタードライバー） LDAP サーバー	AES/128 ビット AES/256 ビット
IPSec	クライアント PC （Web ブラウザー、プリンタードライバー） LDAP サーバー Kerberos サーバー SMTP サーバー	AES/128 ビット Triple-DES/168 ビット

	FTP サーバー DNS サーバー	
S/MIME	SMTP サーバー	Triple-DES/168 ビット AES/128 ビット AES/192 ビット AES/256 ビット

a) TLS プロトコル

システム管理者によりシステム管理者モードで設定された「TLS 通信」に従い、内部ネットワーク上を流れる文書データ、ジョブ情報、セキュリティ監査ログデータや TOE 設定データを保護する一つとして、セキュアなデータ通信が保証される、TLS プロトコルに対応している。

TOE が対応する機能により、TLS サーバーまたは TLS クライアントとして動作することが出来る。 また TLS プロトコルに対応することにより、本 TOE とリモート間のデータ通信は、盗聴や改ざんの両方から保護することが出来る。 盗聴からの保護は、下記の機能により通信データを暗号化することによって実現する。 なお暗号鍵はセションの開始時に生成され、MFD 本体の電源を切断するか、またはセションの終了と同時に消滅する。

・ TLSv1.0/TLSv1.1/TLSv1.2 プロトコルとして生成される接続毎の暗号鍵

具体的には、下記の暗号化スイートの何れかが選択される。

TLS の暗号化スイート	共通鍵暗号方式/鍵サイズ	ハッシュ方式
TLS_RSA_WITH_AES_128_CBC_SHA	AES/128 ビット	SHA1
TLS_RSA_WITH_AES_256_CBC_SHA	AES/256 ビット	SHA1
TLS_RSA_WITH_AES_128_CBC_SHA256	AES/128 ビット	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES/256 ビット	SHA256

また改ざんからの保護は、TLS 暗号通信プロトコルの HMAC(Hashed Message Authentication Code – IETF RFC2104)機能を使用する事によって実現する。

Web クライアント上で TLS 通信を有効にすると、クライアントからの要求は HTTPS を通して、受信しなければならない。 TLS 通信は、IPSec、S/MIME をセットアップする前、またはシステム管理者がセキュリティ監査ログデータをダウンロードする前に有効に設定されていなければならない。

b) IPSec プロトコル

システム管理者によりシステム管理者モードで設定された「IPSec 通信」に従い、内部ネットワーク上を流れる文書データ、ジョブ情報、セキュリティ監査ログデータや TOE 設定データを保護する一つとして、セキュアなデータ通信が保証される、IPSec プロトコルに対応している。

IPSec プロトコルは、TOE とリモート間でどのような IPSec 通信を行うかといった、秘密鍵や暗号アルゴリズムなどのパラメータを定義するための、セキュリティアソシエーションの確立をする。 アソシエーションの確立後、指定された特定の IP アドレス間の全ての通信データは、TOE の電源 OFF またはリセットされるまで IPSec のトランスポートモードにより暗号化される。 なお暗号鍵はセションの開始時に生成され、MFD 本体の電源を切断するか、またはセションの終了と同時に消滅する。

・IPSec プロトコル(ESP:Encapsulating Security Payload)として生成される接続毎の暗号鍵

具体的には、下記の共通鍵暗号方式とハッシュ方式の組み合わせの何れかが選択される。

共通鍵暗号方式/鍵サイズ	ハッシュ方式
AES/128 ビット	SHA1
3Key Triple-DES/168 ビット	SHA1

c) S/MIME プロトコル

システム管理者によりシステム管理者モードで設定された「S/MIME 通信」に従い、内部ネットワークおよび外部ネットワーク上を流れる文書データを保護する一つとして、セキュアなメール通信が保証される、S/MIME プロトコルに対応している。

S/MIME 暗号メールの送受信機能により、外部と電子メールで通信する場合のメール転送経路上での文書データの盗聴を、また S/MIME 署名メールの送受信機能により、文書データの盗聴や改ざんを防止する。

なお暗号鍵はメールの暗号化開始時に生成され、MFD 本体の電源を切断するか、またはメールの暗号化完了と同時に消滅する。

S/MIME プロトコルとして生成されるメール暗号化のための共通鍵暗号方式

共通鍵暗号方式/鍵サイズ
3Key Triple-DES/168 ビット
AES/128 ビット
AES/192 ビット
AES/256 ビット

S/MIME プロトコルとして生成されるメール署名のためのハッシュ方式

ハッシュ方式
SHA1
SHA256

7.1.8. インフォメーションフローセキュリティ機能(TSF_INF_FLOW)

インフォメーションフローセキュリティ機能は、external interfaces(外部インターフェース)と Shared-medium interfaces(内部ネットワーク)間における許可されない通信を制限する機能である。

(1) FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

TOE は、外部インターフェースから受け取られるデータを処理なく内部ネットワークへ転送することを制限する下記能力を提供する。

外部インターフェース	SMI(内部ネットワーク)との通信制限機能
USB(デバイス)	プリントデータ受信用インターフェースであり、他のインターフェースへの転送は許可されない。

	(注:プリントジョブはプライベートプリントへ蓄積される)
Ethernet	プリントデータを受信した場合は他のインターフェースへの転送は許可されない。 他のユーザーデータを利用者クライアントやサーバーから受信することは許可されていなく、転送されることはない。 (注:プリントジョブはプライベートプリントへ蓄積される) 利用者クライアントから識別認証情報を受信した場合、ユーザー認証機能が外部認証に設定されていると、TOE は識別認証情報を LDAP サーバーまたは Kerberos サーバーへ送信する。
操作パネル	操作パネルからの機能使用には必ず識別認証が必要である。 また操作パネルからの入力データを指示なしに他のインターフェースへ転送する機能はない。 ユーザー認証機能が外部認証に設定されていると、TOE は識別認証情報を LDAP サーバーまたは Kerberos サーバーへ送信する。

7.1.9. 自己テスト機能(TSF_S_TEST)

TOE は、TSF 実行コードおよび TSF データの完全性を検証するための自己テスト機能を実行することが可能である。

(1) FPT_TST.1 TSF testing (TSF テスト)

TOE は起動時に NVRAM と SEEPROM の TSF データを含む領域を照合し、異常時は操作パネルにエラーを表示する。
ただしセキュリティ監査ログデータ、時計の日時データはこれらには含まれないため異常の検出はしない。
また TOE は起動時に Controller+PS ROM のチェックサムを計算し所定の値と一致するかを確認し異常時は操作パネルにエラーを表示する。

8. ST 略語・用語 (Acronyms And Terminology)

8.1. 略語 (Acronyms)

本 ST における略語を以下に説明する。

略語	定義内容
ADF	自動原稿送り装置(Auto Document Feeder)
CC	コモンクライテリア(Common Criteria)
CE	カストマーエンジニア(Customer Engineer)
CWIS	センターウェアインターネットサービス(CentreWare Internet Services)
DRAM	ダイナミックランダムアクセスメモリ(Dynamic Randam Access Memory)
EAL	評価保証レベル(Evaluation Assurance Level)
FIPS PUB	米国の連邦情報処理標準の出版物(Federal Information Processing Standard publication)
IIT	画像入力ターミナル(Image Input Terminal)
IOT	画像出力ターミナル(Image Output Terminal)
IT	情報技術(Information Technology)
IP	インターネットプロトコル(Internet Protocol)
MFD	デジタル複合機(Multi Function Device)
NVRAM	不揮発性ランダムアクセスメモリ(Non Volatile Random Access Memory)
PDL	ページ記述言語(Page Description Language)
PP	プロテクションプロファイル(Protection Profile)
SAR	セキュリティ保証要件(Security Assurance Requirement)
SEEPROM	シリアルバスに接続された電気的に書き換え可能な ROM (Serial Electronically Erasable and Programmable Read Only Memory)
SFP	セキュリティ機能方針(Security Function Policy)
SFR	セキュリティ機能要件(Security Functional Requirement)
SMTP	電子メール送信プロトコル(Simple Mail Transfer Protocol)
SOF	機能強度(Strength of Function)
ST	セキュリティターゲット(Security Target)
TOE	評価対象(Target of Evaluation)
TSF	TOE セキュリティ機能(TOE Security Function)

8.2. 用語（Terminology）

本 ST における用語を以下に説明する。

本 ST での用語	定義内容
スキャン/ネットワークスキャン (Scan / Network Scan)	TOE の操作パネルから TOE 内の親展ボックスへ、またネットワーク(FTP/SMTP プロトコル)経由で、パソコンの共有フォルダー、FTP サーバー、メールサーバーへ直接転送指示が可能。また同時に PDF、TIFF、JPEG 等への変換指定が可能。
親展ボックス (Mailbox)	親展ボックスとは読み込んだスキャン文書やコピー文書を TOE 内に保存する場所のこと。 また保存するだけでなく親展ボックスに格納された文書をネットワーク上のコンピュータから取り出すことが可能である。MFD の UI 上は”Folder”と表示される。
個人親展ボックス	一般利用者(U.NORMAL)、SA が個人別に使用できる親展ボックス。 機械管理者はすべての個人親展ボックスにアクセスできる。
共有親展ボックス	すべての利用者が共有して使用できる親展ボックス。 このボックス内の文書には、任意の利用者が作成したものとみなし、すべての利用者が所有権をもつ。ただし、ガイダンスで利用を禁止されている。
蓄積プリント	蓄積プリント機能を有効に設定することで通常プリントは無効になり、第三者に見られたくない文書、機密書類などを出力したい場合に出力データを TOE 内に一時蓄積し、識別認証後に出力を開始する機能。ほかのドキュメントと混ざることもなく、機密性の高いドキュメント出力が実現できる。
センターウェア インターネット サービス(CWIS)	TOE 内の Web サーバーであり、利用者クライアントの Web ブラウザを介して、TOE に対する状態確認、設定変更、文書の取り出し/印刷要求ができるサービスである。 CWIS は、Windows の標準 Web ブラウザで使用することができる。
ユーザー認証 (User Authentication)	TOE の各機能を使用する前に、利用者の識別を行って TOE の利用範囲に制限をかけるための機能である。 本体認証と外部認証の2つのモードがあり、どちらかのモードで動作する。
本体認証 (Local Authentication)	TOE のユーザー認証を MFD に登録したユーザー情報を使用して認証管理を行うモード。
外部認証 (Remote Authentication)	TOE のユーザー認証を外部認証サーバーに登録したユーザー情報を使用して認証管理を行うモード。
上書き消去 (Hard Disk Data Overwrite)	内部ハードディスク装置上に蓄積された文書データを削除する際に、そのデータ領域を特定データで上書きする事を示す。
On Demand Overwrite	内部ハードディスク装置上に蓄積された文書データをマニュアル実行、時刻指定実行により削除し、さらに上書き消去する機能。
デコンポーズ機能	ページ記述言語(PDL)で構成された印刷データを解析し、ビットマップデータに変

本 ST での用語	定義内容
	換する機能。
デコンポーズ	デコンポーズ機能により、ページ記述言語(PDL)で構成されたデータを解析し、ビットマップデータに変換する事。
システム管理者モード (system administrator mode)	一般利用者が MFD の機能を利用する動作モードとは別に、システム管理者が TOE の使用環境に合わせて、TOE 機器の動作設定や TOE セキュリティ機能設定の参照/更新といった、設定値の変更を行う動作モード。
オートクリア機能 (Auto Clear)	操作パネルおよび CWIS から何も操作をしない状態で一定の時間が経過したとき、自動的に認証がログアウトされる機能である。操作パネルの場合はオートクリア時間の設定が可能。
カストマーエンジニア (Customer Engineer)	MFD の保守/修理を行うエンジニア。
攻撃者 (attacker)	攻撃者とは、TOE または保護されている資産に不正な手段を講じてアクセスする者である。攻撃者には、承認された利用者ではあるが、その正体を隠してアクセスする者も含まれる。
操作パネル (Control Panel)	MFD の操作に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネル。
一般利用者クライアント	一般利用者が利用するクライアント。
システム管理者クライアント	システム管理者が利用するクライアント。 システム管理者は Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う。
一般クライアントおよびサーバー	TOE の動作に関与しないクライアントやサーバーを示す。
プリンタードライバ (Printer driver)	一般利用者クライアント上のデータを、MFD が解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウエアで、利用者クライアントで使用する。
印刷データ	MFD が解釈可能なページ記述言語(PDL)で構成されたデータ。 印刷データは、TOE のデコンポーズ機能でビットマップデータに変換される。
制御データ	MFD を構成するハードウエアユニット間で行われる通信のうち、コマンドとそのレスポンスとして通信されるデータ。
ビットマップデータ	コピー機能により読み込まれたデータ、およびプリンター機能により利用者クライアントから送信された印刷データをデコンポーズ機能で変換したデータ。 ビットマップデータは独自方式で画像圧縮して内部ハードディスク装置に格納される。
内部ハードディスク装置からの削除	内部ハードディスク装置からの削除と記載した場合、管理情報の削除の事を示す。 すなわち、文書データが内部ハードディスク装置から削除された場合、対応する管理情報が削除されるため、論理的に削除された文書データに対してアクセスする事は出来なくなる。 しかし文書データ自体はクリアされていない状態となり、文書データ自体は、新たなデータが同じ領域に書き込まれるまで利用済み文書データとして内部ハードディスク装置に残る。
原稿	コピー機能で IIT からの読み込みの対象となる文章や絵画、写真などを示す。

本 ST での用語	定義内容
(Original document)	
文書データ	一般利用者が MFD のコピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能を利用する際に、MFD 内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。 文書データには以下の様な物が含まれる。 コピー機能を使用する際に、IIT で読み込まれ、IOT で印刷されるか内部ハードディスク装置に蓄積されるビットマップデータ。 プリンター機能を利用する際に、一般利用者クライアントから送信される印刷データおよび、それをデコンポーズした結果作成されるビットマップデータ。 スキャナー機能を利用する際に、IIT から読み込まれ内部ハードディスク装置に蓄積されるビットマップデータ。
コピー文書データ	コピー機能により、親展ボックスに保存した文書データ。
スキャン文書データ	スキャン機能により、親展ボックスに保存した文書データ。
利用済み文書データ	MFD の内部ハードディスク装置に蓄積された後、利用が終了しファイルは削除したが、内部ハードディスク装置内には、データ部は残存している状態の文書データ。
セキュリティ監査ログデータ	障害や構成変更、ユーザー操作など、デバイス内で発生した重要な事象を、「いつ」「何(誰)が」、「どうした」、「その結果」という形式で時系列に記録したもの。
内部蓄積データ	一般クライアントおよびサーバーまたは一般利用者クライアント内に蓄積されている、TOE の機能に係わる以外のデータ。
一般データ	内部ネットワークを流れる TOE の機能に係わる以外のデータ。
TOE 設定データ	TOE によって作成されたか TOE に関して作成されたデータであり、TOE のセキュリティ機能に影響を与える可能性のある設定データ。これは TSF データの一部であり、具体的には、下記のデータである：ハードディスク蓄積データ上書き情報、ハードディスク蓄積データ暗号化情報、システム管理者情報、カストマーエンジニア操作制限情報、本体パネルからの認証時のパスワード使用情報、ユーザーパスワードの最小文字数情報、利用者 ID とパスワード情報、システム管理者認証失敗によるアクセス拒否情報、内部ネットワークデータ保護情報、セキュリティ監査ログ設定情報、ユーザー認証情報、蓄積プリント情報、オートクリア情報、自己テスト情報、レポート出力情報、日付・時刻情報。
暗号化キー	利用者が入力する 12 桁の英数字。 内部ハードディスク装置へ暗号化有効時に、このデータをもとに暗号鍵を生成する。
暗号鍵	暗号化キーをもとに自動生成される 256 ビットのデータ。 内部ハードディスク装置へ暗号化有効時の文書データの保存時に、この鍵データを使用して暗号化を行う。
ネットワーク	外部ネットワークと内部ネットワークを包含する一般的に使用する場合の表現。
外部ネットワーク	TOE を管理する組織では管理が出来ない、内部ネットワーク以外のネットワークを指す。
内部ネットワーク	TOE が設置される組織の内部にあり、外部ネットワークからのセキュリティの脅威

本 ST での用語	定義内容
	に対して保護されているネットワーク内の、MFD と MFD へアクセスが必要なリモートの高信頼なサーバーやクライアント PC 間のチャネルを指す。
証明書	ITU-T 勧告の X.509 に定義されており、本人情報(所属組織、識別名、名前等)、公開鍵、有効期限、シリアルナンバ、シグネチャ等が含まれている情報。

9. 参考資料 (References)

本 ST 作成時の参考資料を以下に記述する。

略称	ドキュメント名
[CC パート 1]	Part 1: Introduction and general model (September 2012 Version 3.1 Revision 4) 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改訂第 4 版 パート 1: 概説と一般モデル 2012 年 9 月 CCMB-2012-09-001 (平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC パート 2]	Part 2: Security functional components (September 2012 Version 3.1 Revision 4) 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改訂第 4 版 パート 2: セキュリティ機能コンポーネント 2012 年 9 月 CCMB-2012-09-002 (平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CC パート 3]	Part 3: Security assurance components (September 2012 Version 3.1 Revision 4) 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改訂第 4 版 パート 3: セキュリティ保証コンポーネント 2012 年 9 月 CCMB-2012-09-003 (平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[CEM]	情報技術セキュリティ評価のための共通方法 バージョン 3.1 改訂第 4 版 評価方法 2012 年 9 月 CCMB-2012-09-004 (平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室)
[PP]	U.S. Government Approved Protection Profile - U.S. Government, Protection Profile for Hardcopy Device Version 1.0 (IEEE Std. 2600.2™ -2009)