Xerox WorkCentre 7328/7335/7345

セキュリティターゲット

Version 1.2.7

ー 更新履歴 ー

№	更新日	バージョン	更新内容
1	2007 年 6 月 25 日	V 1.0.9	初版
2	2007 年 7 月 18 日	V 1.1.0	所見報告書に対する修正等
3	2007 年 7 月 19 日	V 1.1.1	誤記修正
4	2007 年 7 月 24 日	V 1.1.2	機能要件見直し等
5	2007 年 7 月 27 日	V 1.1.3	指摘事項修正
6	2007 年 7 月 31 日	V 1.1.4	指摘事項修正
7	2007 年 8 月 2 日	V 1.1.5	指摘事項修正
8	2007 年 8 月 8 日	V 1.1.6	指摘事項修正
9	2007 年 8 月 9 日	V 1.1.7	指摘事項修正
10	2007 年 8 月 31日	V 1.1.8	指摘事項修正、誤記修正
11	2007 年 9 月 13 日	V 1.1.9	指摘事項修正、誤記修正
12	2007 年 9 月 21 日	V 1.2.0	指摘事項修正
13	2007 年 10 月 11 日	V 1.2.1	ROM バージョン変更
14	2007 年 10 月 17 日	V 1.2.3	指摘事項修正
15	2007 年 10 月 18 日	V 1.2.4	誤記修正
16	2007 年 11 月 02 日	V 1.2.5	誤記修正
17	2007 年 11 月 22 日	V 1.2.6	誤記修正
18	2007 年 11 月 27 日	V 1.2.7	誤記修正

－ 目次 －

－ 図表目次 －

1. ST 概説

本章では、ST 識別情報、ST 概要、TOE の評価保証レベル、CC 適合、参考資料、および略語と用語について記述する。

1.1. ST 識別

本 ST と TOE を識別するための情報を記述する。 本 ST は ISO/IEC 15408 (2005) に準拠する。

① ST 識別

ST 名称:	Xerox WorkCentre 7328/7335/7345 セキュリティターゲット
ST バージョン:	V 1.2.7
作成者:	富士ゼロックス株式会社
作成日:	2007 年 11 月 27 日
CC 識別:	Common Criteria for Information Technology Security Evaluation, Version 2.3 ISO/IEC 15408 (2005) 補足-0512 (Interpretation-0512)
キーワード:	マルチファンクションシステム、デジタル複合機、コピー、プリンター、スキャナー、ファクス、内部ハードディスク装置、文書データ上書き消去、文書データ暗号化、内部ネットワークデータ保護、SSL/TLS、IPSec、SNMPv3、S/MIME

② TOE 識別

Xerox WorkCentre 7328、Xerox WorkCentre 7335、Xerox WorkCentre 7345 の 3 機種ともすべて同じ TOE 識別、バージョンで識別する。

TOE 識別:	Xerox WorkCentre 7328/7335/7345	
バージョン:	・Controller+PS ROM	Ver. 1.221.100
	・IOT ROM	Ver. 3.0.4
	・IIT ROM	Ver. 20.4.1
	・ADF ROM	Ver. 11.6.5
製造者:	富士ゼロックス株式会社	

1.2. ST 概要

本 ST は、コピー機能、プリンター機能、スキャナー機能およびファクス機能を有するデジタル複合機 (Multi Function Peripheral 略称 MFP) である Xerox WorkCentre 7328/7335/7345 (以降、単に「MFP」と記す) の、セキュリティ仕様について記述したものである。

MFP 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た文書データ、および利用済み文書データを、不正な暴露から保護するためのセキュリティ機能や、MFP と MFP 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 (以降、これを「TOE とリモート間」と記す) の、内部ネットワーク上に存在する文書データや、利用者によるユーザー認証時の認証識別データ等を脅威から保護する一般的な暗号化通信プロトコルによる通信データの保護にも対応する。 但し、暗号化通信プロトコルに対応出来ないリモートとデータ通信をする場合は、内部ネットワークデータ保護機能を利

用することが出来ない。

また、米国政府機関の要請による公衆電話回線網からファクス機能を踏み台に、内部ネットワーク上に存在する利用者データおよび TOE 設定データにアクセスする脅威から保護する。

本 TOE は以下のセキュリティ機能を提供する。

- 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暗号化機能（TSF_CIPHER）
- ユーザー認証機能（TSF_USER_AUTH）
- システム管理者セキュリティ管理機能（TSF_FMT）
- カストマーエンジニア操作制限機能（TSF_CE_LIMIT）
- セキュリティ監査ログ機能（TSF_FAU）
- 内部ネットワークデータ保護機能（TSF_NET_PROT）
- ファクスフローセキュリティ機能（TSF_FAX_FLOW）

1.3. CC 適合の主張

本 ST は下記の情報セキュリティ評価基準に適合している。 なお本 ST が適合している PP はない。

CC パート 2： 適合
CC パート 3： 適合
評価保証レベル： EAL2 適合

1.4. 参考資料

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]	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 2.3 パート 1：概説と一般モデル 2005 年 8 月 CCMB-2005-08-001 （平成 17 年 12 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]	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 2.3 パート 2：セキュリティ機能要件 2005 年 8 月 CCMB-2005-08-002 （平成 17 年 12 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]	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 2.3 パート 3：セキュリティ保証要件 2005 年 8 月 CCMB-2005-08-003 （平成 17 年 12 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 2.3 評価方法 2005 年 8 月 CCMB-2005-08-004 （平成 17 年 12 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）

略称	ドキュメント名
[ISO/IEC TR15446]	WD N3374　PP/ST 作成のためのガイド バージョン 0.93 (平成 16 年 1 月仮訳 独立行政法人 情報処理推進機構 セキュリティセンター)
[I-0512]	補足-0512 (平成 17 年 12 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)

1.5. ST 略語･用語

1.5.1. 略語

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(Centre Ware Internet Service)
DC	デジタルコピー (Digital Copier)
DRAM	ダイナミックランダムアクセスメモリ(Dynamic Random Access Memory)
EAL	評価保証レベル (Evaluation Assurance Level)
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)
IPSec	IP パケット暗号化プロトコル(Security Architecture for Internet Protocol)
Kerberos	ネットワーク上で暗号を用いて個人認証を行う方式の一つ
LDAP	ディレクトリサービス通信プロトコル(Lightweight Directory Access Protocol)
MFP	デジタル複合機(Multi Function Peripheral)
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)
SF	セキュリティ機能 (Security Function)
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)
SNMPv3	ネットワーク制御/監視プロトコル(Simple network Management

略語	定義内容
	protocol Ver. 3)
SOF	機能強度 (Strength of Function)
SSLv3/TLSv1 (SSL/TLS と記す)	セキュアソケットレイヤ(Secure Socket Layer Ver. 3) / トランスポートレイヤーセキュリティ(Transport Layer Security Ver. 1)
ST	セキュリティターゲット (Security Target)
S/MIME	エスマイム (Secure/Multipurpose Internet Mail Extensions)
TOE	評価対象 (Target of Evaluation)
TSC	TSF 制御範囲 (TSF Scope of Control)
TSF	TOE セキュリティ機能 (TOE Security Function)
TSFI	TSF インタフェース (TSF Interface)
TSP	TOE セキュリティ方針 (TOE Security Policy)

1.5.2. 用語

本 ST における用語を以下に説明する。

用語	定義内容
利用者	TOE の外部にあって TOE と対話する任意のエンティティ。具体的には一般利用者、機械管理者、および SA(System Administrator)。
一般利用者	MFP のコピー機能、スキャナー機能、ファクス機能およびプリンター機能を利用する者。
機械管理者	MFP 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)	機械管理者から、MFP の機械管理や TOE セキュリティ機能の設定を許可された者。
システム管理者	MFP の機械管理や TOE セキュリティ機能の設定を行う管理者。 機械管理者と、SA の総称
カストマーエンジニア	MFP の保守/修理を行うゼロックスのエンジニア。
攻撃者	悪意を持って TOE を利用する者。
操作パネル	MFP 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	一般利用者および SA が MFP を利用するためのクライアント。
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 MFP に対して、TOE 設定データの確認や書き換えを行う。
利用者クライアント	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を示す。
センターウェアインターネットサービス (CWIS)	MFP に対してスキャナ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取り出す機能を提供する。 さらにシステム管理者に、Web ブラウザを使い MFP に対して、TOE 設定データの確認や書き換えを行う機能を提供する。
ツールモード	一般利用者が MFP 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。

用語	定義内容
プリンタードライバー	一般利用者クライアント上のデータを、MFP 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、一般利用者クライアントで使用する。
ファクスドライバ	一般利用者クライアント上のデータを印刷と同じ操作で、MFP へデータを送信し、直接ファクス送信する (ダイレクトファクス機能) ためのソフトウェアであり一般利用者クライアントで使用する。
ネットワークスキャナユーティリティ	MFP 内の親展ボックスに保存されている文書データを一般利用者クライアントから取り出すためのソフトウェア。
印刷データ	MFP 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	MFP 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。
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。
プリンター機能	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機能。
プリンター制御機能	プリンター機能を実現するために装置を制御する機能。
蓄積プリント	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、MFP の内部ハードディスク装置に一旦蓄積し、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で、以下の方法がある。 • プライベートプリント: 一般利用者クライアント上のプリンタードライバーでユーザーID とパスワードを設定し、MFP で認証が成功したジョブのみ保存し、操作パネルよりユーザー認証することにより印刷が可能となる蓄積プリント方法。 • サンプルプリント: 1 部目は通常に印刷を行い、印刷結果を確認後、操作パネルより指示することにより残り部数の印刷を行う蓄積プリント方法。 • 親展ボックスを使った印刷: 親展ボックスに、デコンポーズされたビットマップデータを蓄積し、操作パネルより指示することにより印刷を行う蓄積プリント。
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。

用語	定義内容
コピー機能	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 より印刷を行う機能。 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 MFP 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。
コピー制御機能	コピー機能を実現するために装置を制御する機能。
スキャナー機能	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、MFP 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 やネットワークスキャナユーティリティの機能により取り出す。
スキャナー制御機能	スキャナー機能を実現するために装置を制御する機能。
ネットワークスキャン機能	操作パネルからの一般利用者の指示に従い IIT で原稿を読み込み後に MFP に設定されている情報に従って、FTP サーバ、SMB サーバ、Mail サーバへ文書データの送信を行う。
ネットワークスキャン制御機能	ネットワークスキャン機能を実現するために装置を制御する機能。
ファクス機能	ファクス送受信を行う。 ファクス送信は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、公衆電話回線網により接続された相手機に文書データを送信する。 ファクス受信は公衆電話回線網により接続相手機から送られた文書データを受信し、IOT から印刷を行う。
ファクス制御機能	ファクス機能を実現するために装置を制御する機能。
ダイレクトファクス (D-FAX) 機能	データをプリントジョブとして MFP に送り、紙に印刷するのではなく、ファクス機能により公衆電話回線網を使用して送信する機能。
インターネットファクス (i FAX) 機能	公衆電話回線網を使用するのではなく、インターネットを経由してファクスの送受信を行う機能。
D-FAX、i FAX 制御機能	D-FAX、i FAX 機能を実現するために装置を制御する機能
親展ボックス	MFP の内部ハードディスク装置に作成される論理的なボックス。 スキャナー機能により読み込まれた文書データや親展ボックスを使った印刷のための文書データを蓄積することが出来る。。個別親展ボックスと共用親展ボックスがある。
個別親展ボックス	一般利用者が個別に使用できる親展ボックス。各一般利用者が作成する。
共用親展ボックス	すべての一般利用者が共有して使える親展ボックス。機械管理者が作成できる。
文書データ	一般利用者が MFP のコピー機能、プリンター機能、スキャナー機能、ファクス機能を利用する際に、MFP 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 で印刷されるビットマップデータ。

用語	定義内容
	• 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。 • ファクス機能を利用する際に、IIT から読み込まれ接続相手機に送信するビットマップデータ、および、接続相手機から受信し IOT で印刷されるビットマップデータ。
利用済み文書データ	MFP 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及び TOE に関して作成されたデータであり、TOE の動作に影響を与える可能性のあるもの。具体的には、内部ハードディスク蓄積データ上書き情報、ハードディスク暗号化情報、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、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情報、親展ボックス情報、ユーザー認証情報など。
一般クライアントおよびサーバー	TOE の動作に直接関与しないクライアントやサーバーを示す。
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ー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。
上書き消去	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。
暗号化キー	ユーザーが入力する 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 128 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。

用語	定義内容
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に対して保護されているネットワーク内の、MFP と MFP 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。
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。
ユーザー認証	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。
ローカル認証	TOE のユーザー認証を MFP で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。

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 構成、TOE の物理的範囲や論理的範囲、TOE の保護対象となる資産、および TOE の利用方法について記述する。

2.1. TOE 概要

2.1.1. TOE の種別

本 TOE は IT 製品であり、コピー機能、プリンター機能、スキャナー機能および TOE 外のファクスボードと連携しファクス通信を実現するためのファクス制御機能および不正なアクセスを防ぐファクスフローセキュリティ機能を有する MFP である。 TOE は MFP 全体の制御、および 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および TOE 設定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MFP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および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。

2.1.2. TOE の機能種別

表 1 に TOE が提供する製品の機能種別を記述する。

表 1 TOE の製品機能種別

MFP 機能	機能種別 (標準/オプション)	提供機能
・基本機能	標準機能	・CWIS 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 ・システム管理者セキュリティ機能 ・内部ネットワークデータ保護機能 ・ユーザー認証機能 ・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
・コピー ・プリント		・コピー機能 ・プリンタ機能
・スキャン ・ネットワークスキャン	オプション (スキャンキット)	・スキャナ機能 ・ネットワークスキャン機能
・ファクス ・i-FAX、D-FAX	オプション (TOE 対象外のファクスボード)	・ファクス機能 ・i-FAX、D-FAX 機能 ・ファクスフローセキュリティ機能

2.1.3. TOE のサービス概要

2.1.3.1. TOE の利用環境

本 TOE は、IT 製品として一般的な業務オフィスに、内部ネットワーク、公衆電話回線網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。

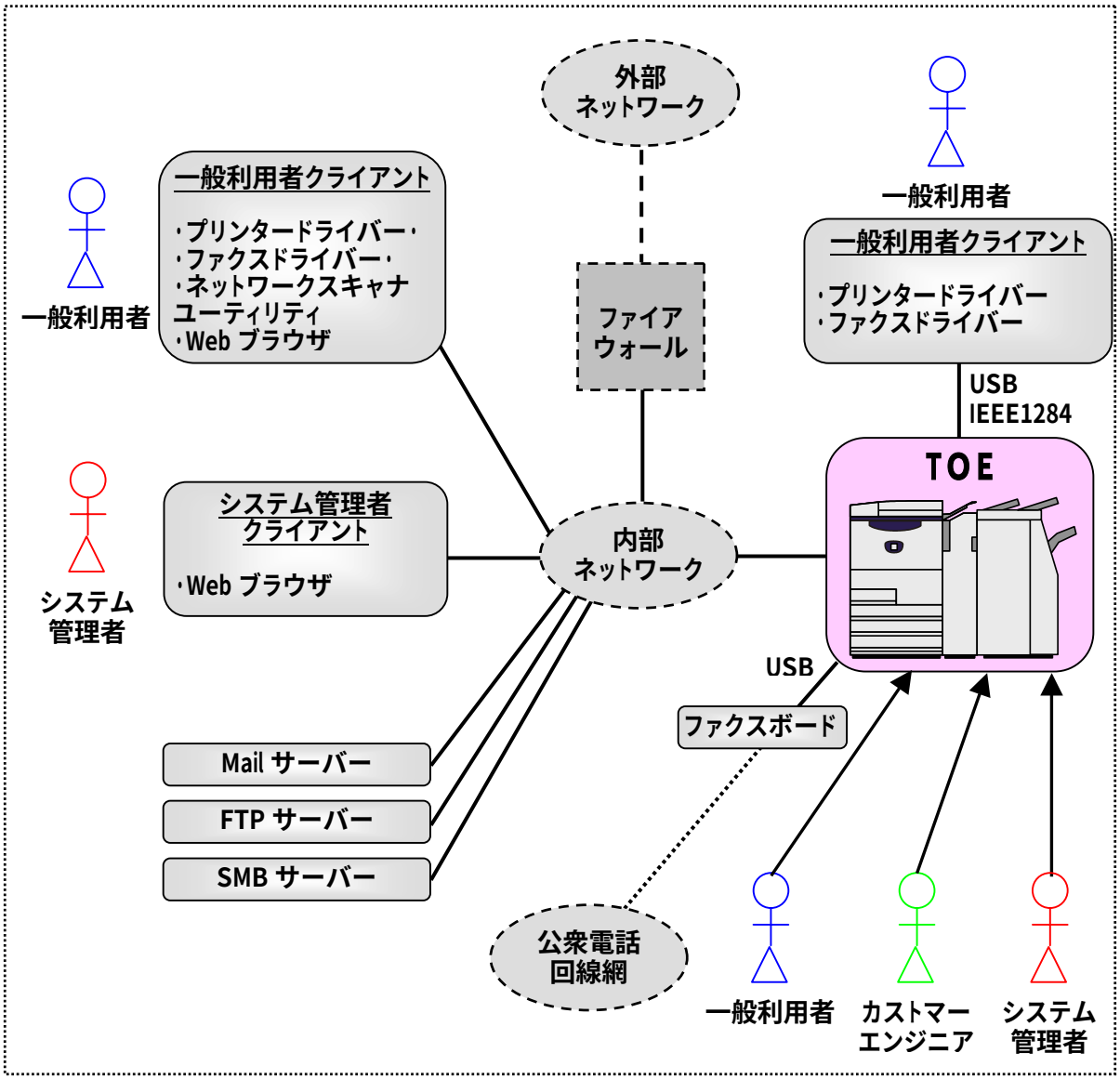

図 1 TOE の想定する利用環境

MFP と接続される内部ネットワーク環境として、以下のものを想定する。

① 一般利用者クライアント:
ネットワーク接続されている場合、プリンタードライバー、ネットワークスキャナユーティリティおよびファクスドライバーがインストールされており、MFP に対して文書データのプリント要求、および文書データのファクス要求、文書データの取り出し要求を行うことができる。
また、Web ブラウザを使用して、MFP に対してスキャナ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 MFP 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 または IEEE1284 でローカル接続されている場合、プリンタードライバー、およびファクスドライバーがインストールされており、MFP に対して文書データのプリント要求、および文書データのファクス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：
Web ブラウザを使用して TOE に対して TOE 設定データの確認や変更、およびセキュリティ監査ログデータのダウンロードを行うことが出来る。

③ Mail サーバー：
MFP 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：
MFP 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 SMB サーバー：
MFP は SMB プロトコルを用いて、SMB サーバーに文書データの送信を行う。

⑥ ファクスボード
外部公衆回線に接続されており G3/G4 プロトコルに対応するファクスボードである。MFP とは USB のインターフェイスで接続されファクスデータの送受信を行う。

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 Windows2000、WindowsXP、WindowsVISTA とする。

2.1.3.2. TOE のセキュリティ機能概要

本 TOE が提供するセキュリティ機能概要を、以下に記述する。

- TOE は、各ジョブの処理中に作成される文書データを、一時的に内部ハードディスク装置に蓄積するが、各ジョブ終了時の利用済み文書データを、不正な暴露から保護するために、文書データの上書き消去機能を提供する。
  またTOEは、各ジョブの処理中に作成される文書データを、不正な暴露から保護するために、内部ハードディスク装置に書き込む前に、文書データを暗号化する機能を提供する。
- TOE は、文書データ、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目的で、SSL/TLS・IPSec・SNMPv3・S/MIME といった、暗号化通信プロトコルによる通信データの保護に対応している。 これらの一般的なネットワークプロトコルを利用することで、TOE とリモート間でセキュアなデータ通信が可能になる。
- TOEは、いつ、誰が、どのような作業をMFPで行ったかという、TOEの重要なイベント（例えば障害や構成変更、ユーザ操作など）を追跡して記録するセキュリティ監査ログ機能を提供する。 この機能を利用することにより、TOE の不正使用や不正使用の試みを監視することが出来る。
- TOE は、操作パネルおよび Web ブラウザを通して、TOE 機器の動作設定の参照/更新を行う前に、システム管理者 ID とパスワードを入力するといった、システム管理者を識別するためのシステム管理者セキュリティ管理機能を提供する。 この機能を利用することで、認証されたシステム管理者のみに、TOE セキュリティ機能の設定を行う権限を許可することが出来る。
- TOE は、操作パネル、Web ブラウザおよびネットワークスキャナユーティリティを通して TOE 機器を使用する前に、ユーザーID とパスワードを入力するといった一般利用者を識別するための

ユーザー認証機能を提供する。 この機能を利用することで、認証された一般利用者のみに TOE 機能の使用を許可することが出来る。

- TOE は、システム管理者が、カストマーエンジニアによるセキュリティ機能の設定を行う権限を、制限させる機能を提供する。 この機能を利用することで、カストマーエンジニアのなりすましによる設定変更が出来ないようにすることが出来る。
- TOE は、ファクスの電話回線やモデムの通信路を通じて内部ネットワークに不正にアクセスする可能性を阻止するため、電話回線から、ファクスデータ以外のデータが内部ネットワークに流れないようにすることで電話回線から内部ネットワークへの不正アクセスを不可能にしている。

2.2. TOE 関連の利用者役割

本 ST では、TOE に対して想定する利用者役割を表 2 に記述する。

表 2 TOE が想定する利用者役割

関連者	内容説明
組織の管理者	TOE を使用して運用する組織の責任者または管理者。
一般利用者	TOE が提供するコピー、プリント、ファクス等の TOE 機能の利用者。
システム管理者 (機械管理者＋SA)	TOE のツール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/更新を行う。

2.3. TOE の論理的範囲

TOE の論理的範囲は Controller ROM の中に記録されている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。

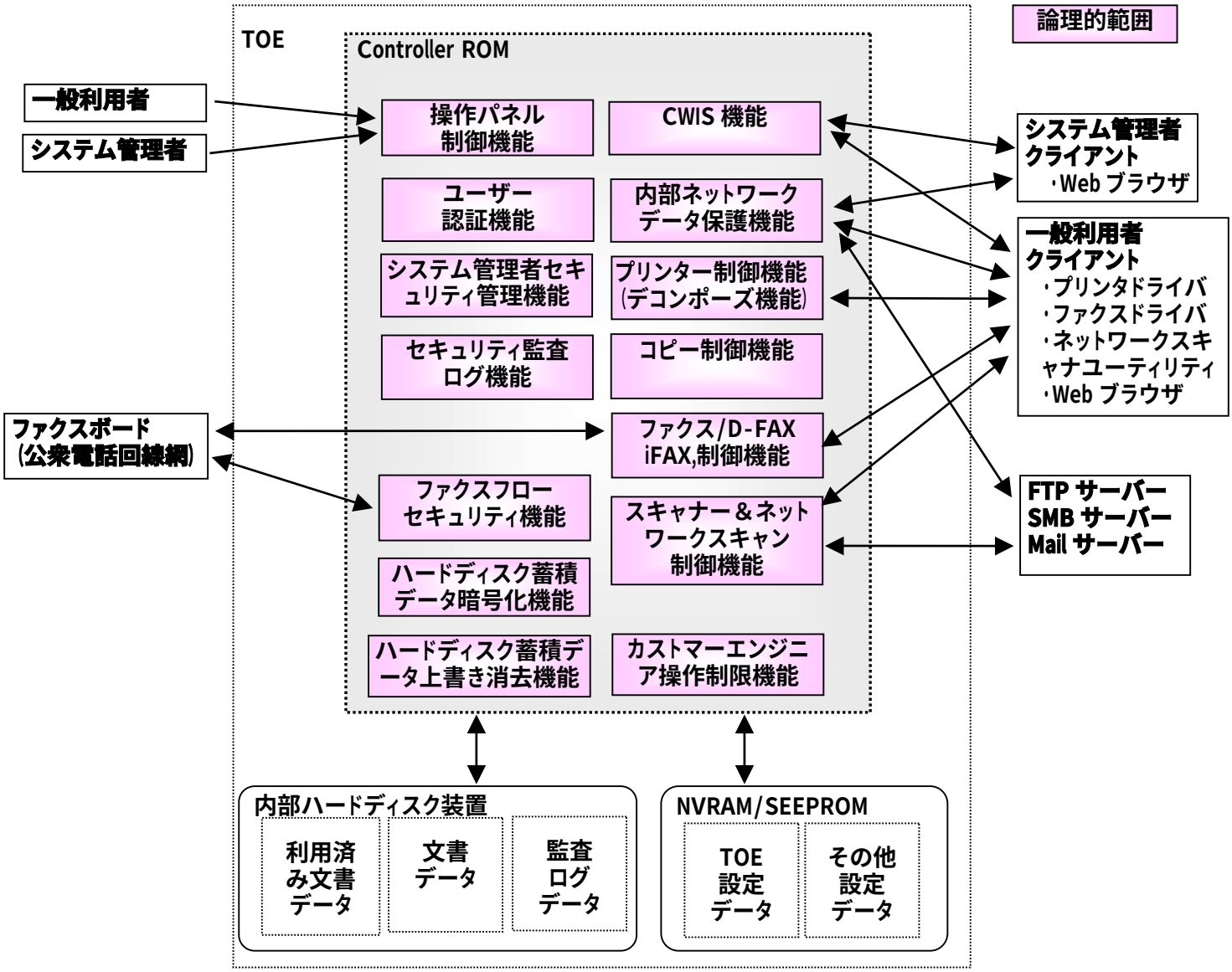

図 2 MFP 内の各ユニットと TOE の論理的範囲

2.3.1. TOE が提供する基本機能

TOE は一般利用者に対して、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、ファクス機能、i-FAX と D-FAX、および CWIS 機能を提供する。

2.3.1.1. 操作パネル機能

操作パネル機能は一般利用者、システム管理者が MFP の機能を利用するための操作に必要な機能であり、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から構成される。

2.3.1.2. コピー機能

コピー機能は、一般利用者が MFP 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。

2.3.1.3. 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して、プリンタドライバを介して作成された印刷データが MFP へ送信され、MFP 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。
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。

2.3.1.4. 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 MFP 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 機能やネットワークスキャナユーティリティ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 MFP に設定されている情報に従って、一般利用者が MFP 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、SMB サーバーへ転送する機能である。

2.3.1.5. ファクス機能

ファクス機能は、ファクス送信とファクス受信があり、 ファクス送信は一般利用者が MFP 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、公衆電話回線網により接続された相手機に文書データを送信する。 ファクス受信は公衆電話回線網を介して接続相手機から送られて来た文書データを、IOT から印刷を行う機能である。

2.3.1.6. i FAX・D-FAX 機能

i FAX 機能は、通常のファクス機能と同様にファクス送信とファクス受信がある。 i FAX 送信は一般利用者が MFP 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、インターネットを介して接続された相手機に文書データを送信する。 i FAX 受信はインターネットを介して接続相手機から送られて来た文書データを、IOT から印刷を行う機能である。
D-FAX 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タ先としてファクス送信指示をすると、ファクスドライバを介して作成された印刷データが MFP へ送信され、MFP 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、ファクス送信データに変換後に公衆電話回線網を使用して、文書データを送信する機能である。

2.3.1.7. CWIS 機能

CWIS は、一般利用者が一般利用者クライアントの Web ブラウザからの指示により、内部ハードディスク装置に蓄積されている、スキャナから読み取られた文書データやファクス受信データの取り出しを行う。
またシステム管理者は、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 MFP 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。

2.3.2. TOE が提供するセキュリティ機能

TOE は MFP であり、汎用的なコンピュータやソフトウエアではないため、構造的にセキュリティ機能をバイパス、破壊、盗聴、改ざん、その他の点で危うくなることはない。 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。

2.3.2.1. ハードディスク蓄積データ上書き消去機能 (TSF_IOW)

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。 このため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、上書き消去機能を提供する。

上記に加えて、システム管理者が設定した時刻に蓄積文書を削除して上書き消去する (時刻指定文書削除機能) 機能も提供する。

2.3.2.2. ハードディスク蓄積データ暗号化機能 (TSF_CIPHER)

内部ハードディスク装置に文書データやセキュリティ監査ログデータを蓄積する際に、データの暗号化機能を提供する。

2.3.2.3. ユーザー認証機能 (TSF_USER_AUTH)

TOE は、許可された特定の利用者だけに MFP 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プリンタドライバ、ネットワークスキャナユーティリティ、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する機能を有する。

認証が成功した一般利用者のみが下記の機能を使用可能となる。

① 本体操作パネルで制御される機能

コピー機能、ファクス機能 (送信) 、iFAX 機能 (送信) 、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 (プリンタドライバでのユーザーID とユーザーパスワードの設定が条件であり印刷時に操作パネルで認証する)

②一般利用者クライアントのネットワークスキャナユティリティで制御される機能

親展ボックスからの文書データ取出し機能

③CWIS 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

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プリンター機能(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、ネットワークスキャナユティリティ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。

これらの機能の認証フローを図 3 に示す。

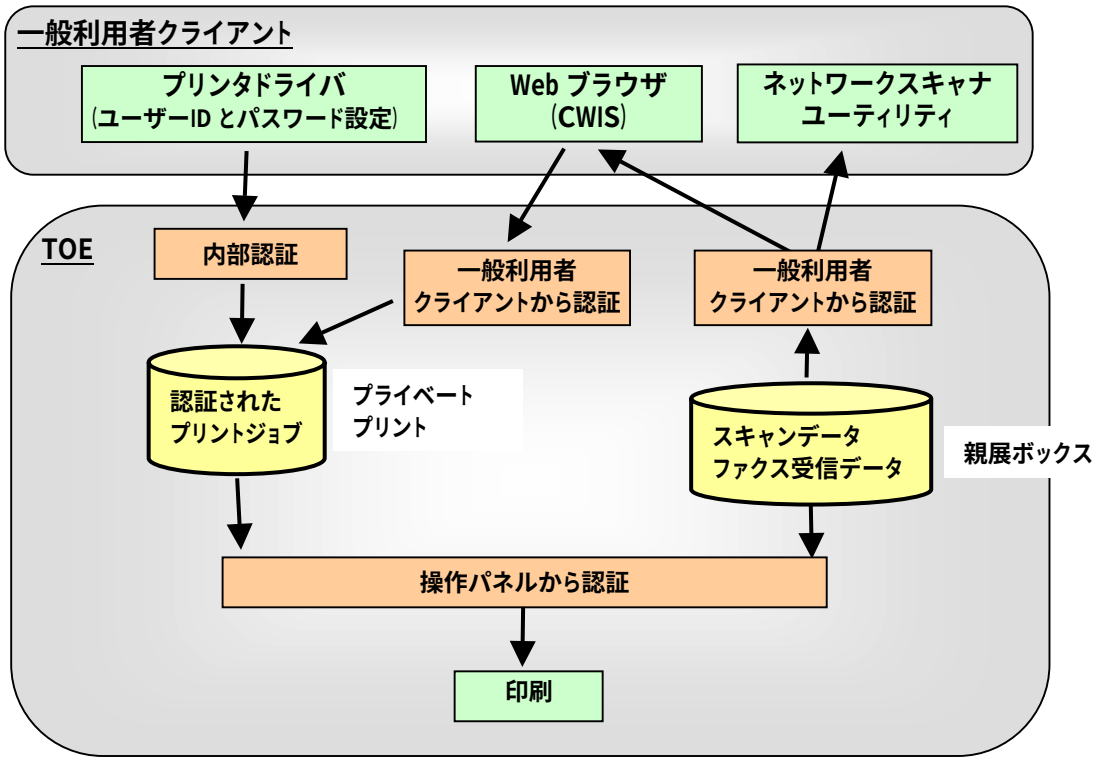

図 3 プライベートプリントと親展ボックスの認証フロー

- **プライベートプリント機能**

MFP で「認証成功のジョブをプライベートプリントに保存」の設定を行うと、一般利用者が一般利用者クライアントのプリンタドライバーからユーザーID とパスワードを設定した状態でプリント指示をする場合、MFP 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) してプライベートプリントとしてユーザーID ごとに区分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、認証後に一般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。

一般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、MFP 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。一般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 とファクスボードから親展ボックスにスキャンデータとファクス受信データを格納することが可能である。

スキャンデータを親展ボックスに格納するには、一般利用者が MFP 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、認証されるとスキャン機能の利用が可能になり、操作パネルから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。

ファクス受信データを親展ボックスに格納する場合にはユーザー認証は行わず、公衆電話回線網を介して接続相手機から送られて来たファクス受信データのうち、送信時に親展ボックスを指定した

親展ファクス受信データ、特定相手の電話番号ごとのファクス受信データ、送信元不定のファクス受信データがそれぞれ指定された親展ボックスに自動的に格納されることで可能となる。

登録されたユーザーID ごとの個別親展ボックスは、一般利用者が操作パネル、CWIS またはネットワークスキャナーユーティリティからユーザーID とパスワードを入力すると MFP 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、削除の操作が可能となる。

個別親展ボックスのほかに機械管理者のみが登録可能な共用親展ボックスがあり、認証が成功した一般利用者のみが共有して利用できる。

2.3.2.4. システム管理者セキュリティ管理機能 (TSF_FMT)

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、ツール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　有効/無効にする
- ハードディスク蓄積データ暗号化　する/しない
- ハードディスク蓄積データ暗号化キーを設定する
- 本体パネルからの認証時のパスワードの使用　有効/無効にする
- 機械管理者 ID とパスワード変更をする (機械管理者のみ可能)
- SA、一般利用者の ID とパスワード変更をする
- システム管理者の認証失敗によるアクセス拒否回数を設定する
- ユーザーパスワード(一般利用者と SA)の最小文字数を設定する
- カストマーエンジニア操作機能制限　する/しない
- SSL/TLS 通信を有効/無効にする、および詳細情報を設定する
- IPSec 通信を有効/無効にする、および詳細情報を設定する
- S/MIME プロトコルを有効/無効にする、および詳細情報を設定する
- 時刻指定文書削除機能：有効/無効にする、および削除時刻を設定する
- ユーザー認証機能を設定する
- 日付、時刻を設定する

また本 TOE は、Web ブラウザを通して、認証されたシステム管理者のみに、CWIS により下記のセキュリティ機能の設定を行う権限を許可する。

- 機械管理者 ID とパスワード変更をする (機械管理者のみ可能)
- SA、一般利用者の ID とパスワード変更をする
- システム管理者の認証失敗によるアクセス拒否回数を設定する
- 監査ログ機能を有効/無効にする
- SSL/TLS 通信を有効/無効にする、および詳細情報を設定する
- IPSec 通信を有効/無効にする、および詳細情報を設定する
- SNMPv3 通信を有効/無効にする、および詳細情報を設定する

- SNMPv3 認証パスワードを設定する
- S/MIME プロトコルを有効/無効にする、および詳細情報を設定する
- X.509 証明書作成/アップロード/ダウンロードする
- 時刻指定文書削除機能を有効/無効にする、および削除時刻を設定する
- ユーザー認証機能を設定する

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

本 TOE は、カストマーエンジニアが、TOE セキュリティ機能に関する設定の参照および変更が出来ないように、システム管理者がカストマーエンジニアのツールモードでの操作を、制限する機能を提供する。 この機能により、カストマーエンジニアのなりすましによる設定変更が出来ないようにする。

2.3.2.6. セキュリティ監査ログ機能 (TSF_FAU)

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 ブラウザを通して、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、SSL/TLS 通信が有効に設定されていなければならない。

2.3.2.7. 内部ネットワークデータ保護機能 (TSF_NET_PROT)

本 TOE は、内部ネットワーク上に存在する文書データ、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。

- SSL/TLS プロトコル
- IPSec プロトコル
- SNMPv3 プロトコル
- S/MIME プロトコル

2.3.2.8. ファクスフローセキュリティ機能 (TSF_FAX_FLOW)

TOE 本体オプションのファクスボードは、コントローラボードと USB インタフェースで接続されるが、公衆電話回線網からファクスボードを通じて TOE の内部や内部ネットワークへ、不正にアクセスすることは出来ない。

2.4. TOE の物理的範囲

図 4 に MFP 内の各ユニット構成と、TOE の物理的範囲を記述する。

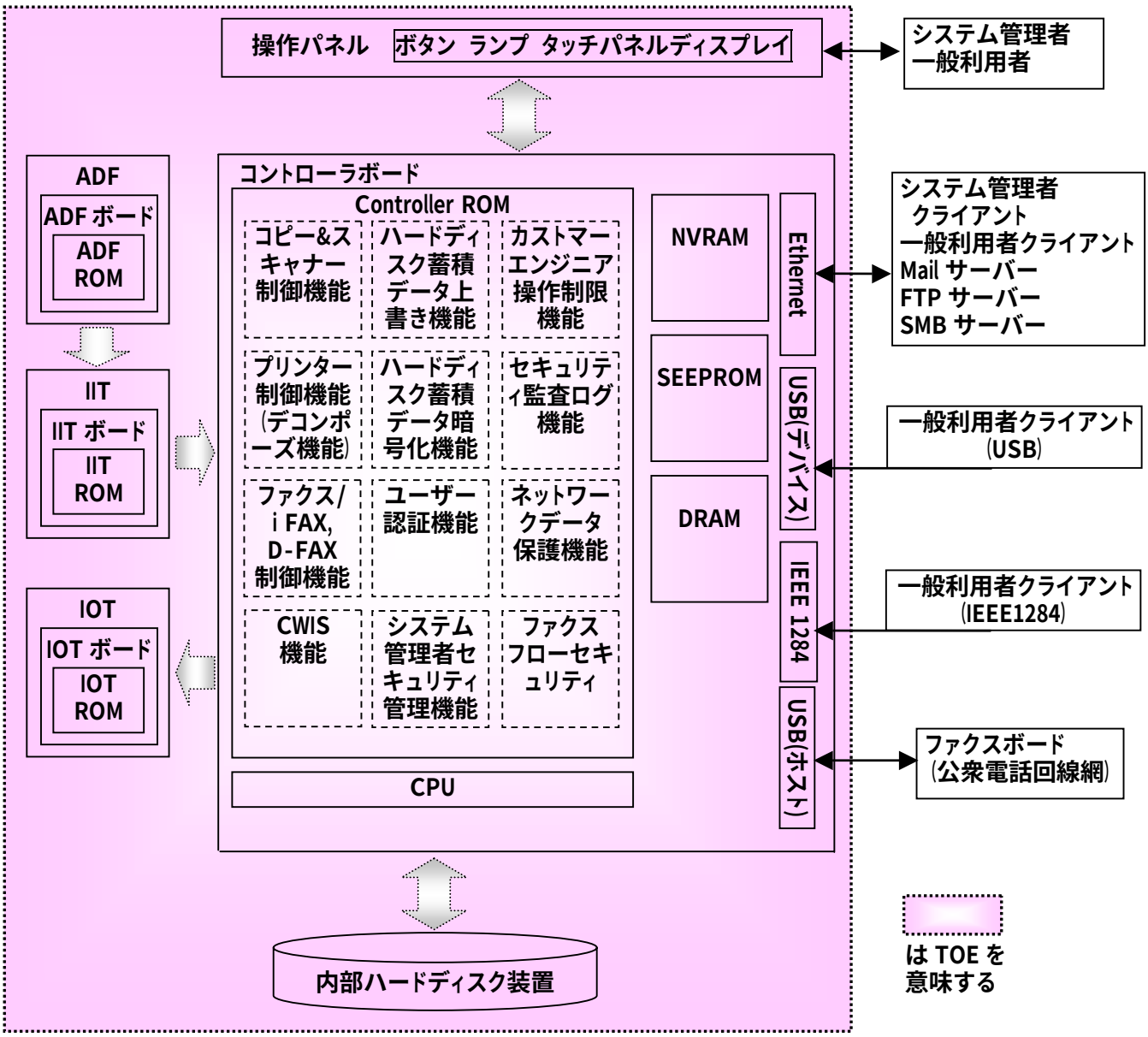

図 4 MFP の各ユニットと TOE の物理的範囲

本 TOE の物理的範囲はファクスボードを除く MFP 全体であり、MFP は、コントローラボード、操作パネル、ADF ボード、IIT ボード、IOT ボードの回路基板ユニットから構成される。

コントローラボードと操作パネル、および ADF ボードの間は、制御データの通信を行う内部インタフェースで接続されている。 またコントローラボードとファクスボードの間は USB インタフェース、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、専用の内部インタフェースで接続されている。

コントローラボードは、MFP のコピー機能、プリンター機能、スキャナー機能、およびファクス機能の制御を行うための回路基板であり、ネットワークインタフェース (Ethernet) 、ローカルプリントインタフェース (IEEE1284 や USB デバイス) を持ち、IIT ボードや IOT ボードが接続されている。

操作パネルは、MFP のコピー機能、プリンター機能、スキャナー機能、およびファクス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。

ADF は、複数枚の原稿を自動的に搬送するためのデバイスである。

画像入力ターミナル (IIT) は、コピー、スキャナー、ファクス機能の利用時に、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。

2.5. TOE の保護資産

本 TOE が保護する資産は以下のとおりである。

- MFP
  一般利用者が、TOE の各機能を使用する権利を資産とする。
- ジョブ処理のために蓄積する文書データ
  一般利用者が MFP をコピー、プリント、ファクス、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 機能やネットワークスキャナーユーティリティにより一般利用者クライアントから MFP 内に蓄積された文書データの取り出しが可能である。これらは一般利用者の機密情報であり、保護資産とする。
- ジョブ処理後の利用済み文書データ
  一般利用者が MFP をコピー、ファクス、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。これらは一般利用者の機密情報であり、保護資産とする。
- セキュリティ監査ログデータ
  MFP に対し、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、ユーザ操作など) を追跡記録するためにセキュリティ監査ログ機能により、内部ハードディスク装置内にログデータが発生した都度、記録保存される。 また CWIS 機能によりシステム管理者クライアントから MFP 内に蓄積されたセキュリティ監査ログデータの取り出しが可能である。この機能はトラブルの予防保全や対応、不正使用の検出に使用され、セキュリティ監査ログデータはシステム管理者のみアクセス可能なデータであり保護資産とする。
- TOE 設定データ
  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、MFP 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 (表 3)。これらは他の保護資産の脅威につながるものであり保護資産とする。

  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が、公衆電話回線網から TOE を介して内部ネットワークへ侵入することは TOE の機能により阻止されるため外部から上記保護対象外の資産へアクセスすることは脅威とはならない。

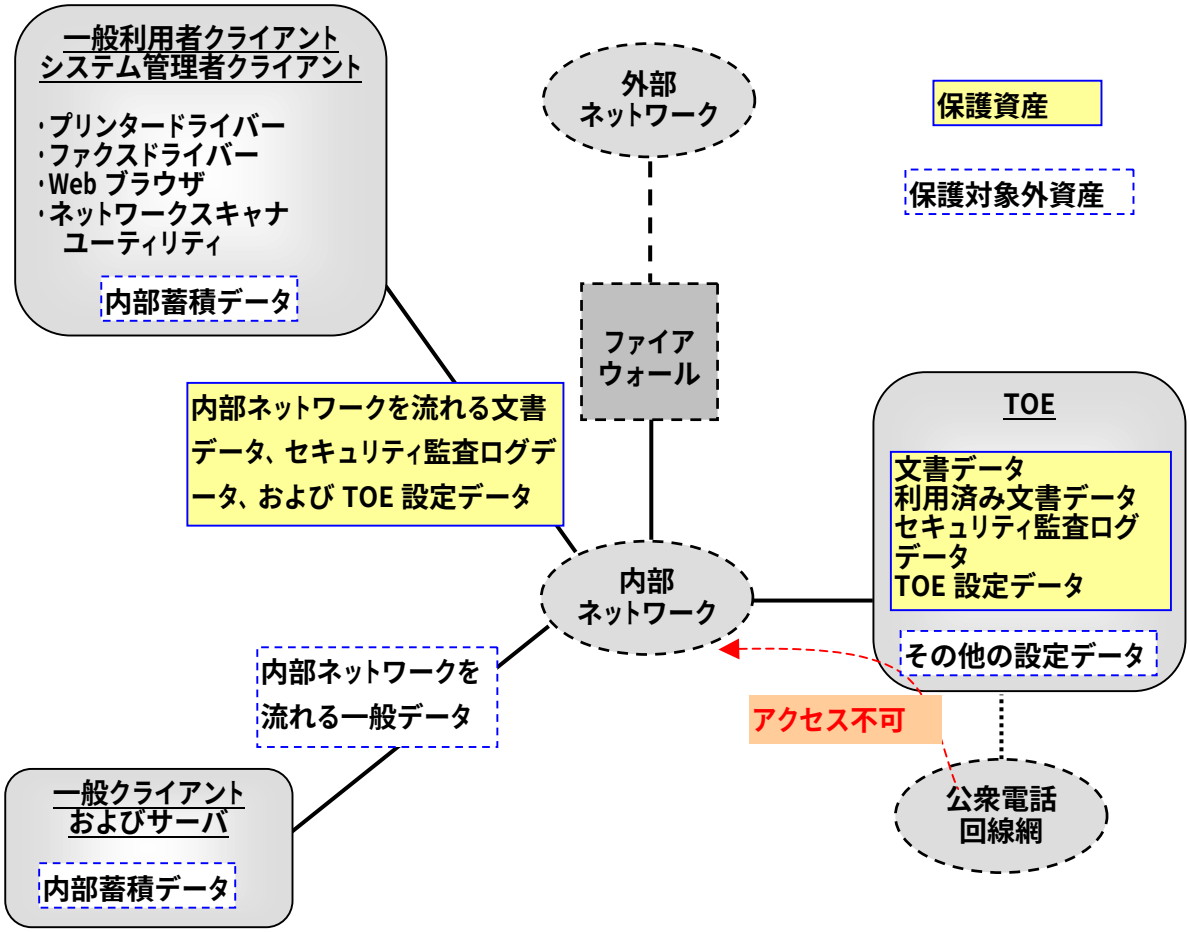

図 5 保護資産と保護対象外資産

表 3 にコントローラボードの NVRAM および SEEPROM に記憶される TOE 設定データ分類を記述する。

表 3 TOE 設定データ項目分類

TOE 設定データ項目分類 (注)
ハードディスク蓄積データ上書き情報
ハードディスク暗号化情報
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
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データ
親展ボックス情報
ユーザー認証情報
日付、時刻情報

注) 記憶場所の NVRAM と SEEPROM には、TOE 設定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。

3. TOE セキュリティ環境

本章では、TOE への前提条件、TOE に対する脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

本 TOE の動作、運用、および利用に関する前提条件を、表 4 に記述する。

表 4 前提条件

前提条件 (識別子)	内容説明
人的な信頼	
A.ADMIN	システム管理者は、TOE の機器管理に課せられた役割を遂行するために、TOE セキュリティ機能に関する必要な知識を持ち、悪意をもった不正を行わないものとする。
保護モード	
A.SECMODE	システム管理者は、TOE を運用するにあたり下記の通りに設定するものとする。 • 本体パネルからの認証時のパスワード使用設定:有効にする • システム管理者パスワード長:9 文字以上 • システム管理者 ID 認証失敗によるアクセス拒否:有効にする • システム管理者 ID 認証失敗によるアクセス拒否回数:5 • カストマーエンジニア操作制限機能設定:有効にする • 認証の種類:ユーザー認証を有効にする • ユーザーパスワード(一般利用者と SA)文字数制限:9 文字以上 • プライベートプリント設定:認証成功のジョブを蓄積にする • 監査ログ機能設定:有効にする • SNMPv3 通信設定:有効にする • SNMPv3 認証パスワード:8 文字以上 • SSL/TLS 通信設定:有効にする • IPSec 通信設定:有効にする • S/MIME プロトコル設定:有効にする • SMB 通信設定:無効にする • ハードディスク蓄積データ上書き消去設定:有効にする • ハードディスク蓄積データ暗号化設定:有効にする • ハードディスク蓄積データ暗号化キー設定:12 文字 • 時刻指定文書削除設定:有効にする

3.2. 脅威

本 TOE に対するする脅威を、表 5 に記述する。 これらの脅威は TOE の動作について公開されている情報の知識を持っている利用者であると想定する。 また攻撃者は低レベルの攻撃能力を持つ者とする。

表 5 脅威

脅威 (識別子)	内容説明
内部ハードディスク装置に蓄積される文書データ、、セキュリティ監査ログデータの不正再生	
T.RECOVER	攻撃者が、内部ハードディスク装置を取り出して、その内容を読み取るために市販のツール等に接続して、内部ハードディスク装置上の利用済み文書データや文書データ、およびセキュリティ監査ログデータを読み出して漏洩させるかもしれない。
文書データおよび TOE 設定データの不正アクセス	
T.CONFDATA	攻撃者が、操作パネルや Web ブラウザから、システム管理者のみアクセスが許可されている TOE 設定データにアクセスして、データの改ざんまたは不正に読み出すかもしれない。
T.DATA_SEC	攻撃者が、操作パネルや Web ブラウザから、文書データやセキュリティ監査ログデータを、不正に読み出すかもしれない。
文書データおよび TOE 設定データの盗聴	
T.COMM_TAP	攻撃者が、内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴や改ざんをするかもしれない。
T.CONSUME	攻撃者が、TOE にアクセスし TOE の機能を不正に使用するかもしれない。

3.3. 組織のセキュリティ方針

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、表 6 に記述する。

表 6 組織のセキュリティ方針

組織の方針 (識別子)	内容説明
アメリカの政府機関要請	
P.FAX_OPT	米国政府機関の要請により、公衆電話回線網から内部ネットワークへのアクセスができないことを保証しなければならない。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針および環境セキュリティ対策方針について記述する。

4.1. TOE セキュリティ対策方針

本 TOE が果たすセキュリティ対策方針を、表 7 に記述する。

表 7 TOE セキュリティ対策方針

TOE 対策方針 (識別子)	詳細内容
O.AUDITS	本 TOE は、不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供しなければならない。
O.CIPHER	本 TOE 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やセキュリティ監査ログ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。
O.COMM_SEC	本 TOE は、TOE とリモート間の内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを、盗聴や改ざんから保護する機能を提供する。
O.FAX_SEC	本 TOE は、TOE のファクスモデムの通信路を通じて、公衆電話回線網から TOE が接続されている内部ネットワークへのアクセスを、防がなければならない。
O.MANAGE	本 TOE は、セキュリティ機能の設定を行うツールモードのアクセスを、認証されたシステム管理者のみ許可して、一般利用者による TOE 設定データやセキュリティ監査ログデータへのアクセスを、不可能にしなければならない。
O.RESIDUAL	本 TOE は、内部ハードディスク装置に蓄積される利用済み文書データの再生および復元を、不可能にしなければならない。
O.USER	本 TOE は、正当な TOE の利用者を識別し、正当な利用者に文書データの読み出しする機能を、一般利用者へ提供しなければならない。
O.RESTRICT	本 TOE は、許可されていない者への TOE の利用を制限する機能を持たなければならない。

4.2. 環境のセキュリティ対策方針

TOE 環境に対するセキュリティ対策方針を、表 8 に記述する。

表 8 環境のセキュリティ対策方針

環境対策方針 (識別子)	詳細内容
OE.ADMIN	組織の管理者は、本 TOE を管理するために信頼できる組織内の適任者をシステム管理者として任命し、TOE を管理するための必要な教育を実施する。
OE.AUTH	本 TOE を管理するシステム管理者は、下記の通りに TOE のセキュリティ機能を設定して、TOE を運用しなければならない。

環境対策方針(識別子)	詳細内容
	• 本体パネルからの認証時のパスワードの使用設定:有効にする • システム管理者パスワード長:9 文字以上 • システム管理者 ID 認証失敗によるアクセス拒否:有効にする • システム管理者 ID 認証失敗によるアクセス拒否回数:5 • カストマーエンジニア操作制限機能設定:有効にする • 認証の種類:ユーザー認証を有効にする(ローカル認証を選択) • ユーザーパスワード(一般利用者と SA)文字数制限:9 文字以上 • プライベートプリント設定:認証成功のジョブを蓄積にする
OE.COMMS_SEC	本 TOE を管理するシステム管理者は、下記の通りに内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定して、TOE を運用しなければならない。 • SNMPv3 通信設定:有効にする • SNMPv3 認証パスワード:8 文字以上 • SSL/TLS 通信設定:有効にする • IPSec 通信設定:有効にする • S/MIME プロトコル設定:有効にする • SMB 通信設定:無効にする
OE.FUNCTION	本 TOE を管理するシステム管理者は、下記の通りに TOE の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、セキュリティ監査ログ機能を設定して、TOE を運用しなければならない。 • ハードディスク蓄積データ上書き消去設定:有効にする • ハードディスク蓄積データ暗号化設定:有効にする • ハードディスク蓄積データ暗号化キー設定:12 文字 • 時刻指定文書削除設定:有効にする • 監査ログ機能設定:有効にする

5. IT セキュリティ要件

本章では、TOE セキュリティ機能要件、および IT 環境に対するセキュリティ機能要件について記述する。

5.1. TOE セキュリティ機能要件

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。 セキュリティ機能要件は [CC パート 2] で規定されているクラスおよびコンポーネントに準拠している。

5.1.1. クラス FAU：セキュリティ監査

① FAU_GEN.1 監査データ生成

下位階層： なし

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない：

a) 監査ログ機能の起動と終了；

b) [選択：*指定なし*] レベルのすべての監査対象事象； 及び

c) [割付：*上記以外の個別に定義した監査対象事象*]

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）； 及び各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、 [割付：*その他の監査関連情報はない*] 。

依存性： FPT_STM.1 高信頼タイムスタンプ

各機能要件を選択した場合に監査対象とすべき基本レベル以下のアクション(規約)と、それに関連する TOE の監査対象事象（実行ログとして記録を残す事象）を表 9 に示す。

表 9 TOE の監査対象事象と個別に定義した監査対象事象

機能要件	CCで定義された監査対象とすべきアクション	TOEの監査対象事象
FAU_GEN.1	なし	－
FAU_SAR.1	基本：監査記録からの情報の読み出し。	*基本：監査ログデータのダウンロード成功を監査する。*
FAU_SAR.2	基本：監査記録からの成功しなかった情報読み出し。	*基本：監査ログデータのダウンロード失敗を監査する。*
FAU_STG.1	なし	－
FAU_STG.4	基本：監査格納失敗によってとられるアクション。	*監査事象は採取しない*

FCS_CKM.1	**最小**: **動作の成功と失敗。** **基本**: **オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。**	***監査事象は採取しない***
FCS_COP.1	**最小**: **成功と失敗及び暗号操作の種別。** **基本**: **すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。**	***監査事象は採取しない***
FDP_ACC.1	**なし**	**ー**
FDP_ACF.1	**最小**: SFP**で扱われるオブジェクトに対する操作の実行における成功した要求。** **基本**: SFP**で扱われるオブジェクトに対する操作の実行におけるすべての要求。** **詳細**: **アクセスチェック時に用いられる特定のセキュリティ属性。**	***基本:*** ***親展ボックスの作成、削除が監査される。*** ***親展ボックスアクセス、蓄積プリントの実行に関しユーザー名、ジョブ情報、成功可否が監査される。***
FDP_IFC.1	**なし**	**ー**
FDP_IFF.1	**最小:要求された情報フローを許可する決定。** **基本:情報フローに対する要求に関するすべての決定。** **詳細:情報フローの実施を決定する上で用いられる特定のセキュリティ属性。** **詳細:方針目的**(policy goal)**に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。**	***監査事象は採取しない***
FDP_RIP.1	**なし**	**ー**
FIA_AFL.1	**最小**: **不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。**	***＜最小＞*** ***連続認証エラーを監査する。***
FIA_UAU.2	**最小**: **認証メカニズムの不成功になった使用**; **基本**: **認証メカニズムのすべての使用。**	***＜最小＞*** ***連続認証エラーを監査する。***
FIA_UAU.7	**なし**	**ー**

FIA_UID.2	**最小**: **提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用**; **基本**: **提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。**	***＜最小＞*** ***連続認証エラーを監査する***
FMT_MOF.1	**基本**: TSF**の機能のふるまいにおけるすべての改変。**	***＜基本＞*** ***セキュリティ機能の設定変更を監査する。***
FMT_MSA.1	**基本**:**セキュリティ属性の値の改変すべて。**	***＜基本＞*** ***親展ボックスの作成、削除が監査される。*** ***親展ボックスアクセス、蓄積プリントの実行に関しユーザー名、ジョブ情報、成功可否が監査される。***
FMT_MSA.3	**基本**:**許可的あるいは制限的規則のデフォルト設定の改変。** **基本**:**セキュリティ属性の初期値の改変すべて。**	***＜個別に定義した監査対象事象＞*** ***システム管理者の認証成功／認証失敗を監査する。***
FMT_MTD.1.	**基本**:TSF **データの値のすべての改変。**	***＜個別に定義した監査対象事象＞*** ***セキュリティ機能の設定変更を監査する。***
FMT_SMF.1	**最小**:**管理機能の使用。**	***＜個別に定義した監査対象事象＞*** ***システム管理者の認証成功／認証失敗を監査する。***
FMT_SMR.1	**最小**:**役割の一部をなす利用者のグループに対する改変**; **詳細**:**役割の権限の使用すべて。**	***＜個別に定義した監査対象事象＞*** ***システム管理者の認証成功／認証失敗を監査する。***
FPT_RVM.1	**なし**	**－**
FPT_STM.1	**最小**:**時間の変更**; **詳細**:**タイムスタンプの提供。**	***＜最小＞*** ***時刻設定の変更を監査する***
FTP_TRP.1	**最小**: **高信頼パス機能の失敗。** **最小**: **もし得られれば、すべての高信頼パス失敗に関係する利用者の識別情報。** **基本**: **高信頼パス機能の使用についてのすべての試み。** **基本**: **もし得られれば、すべての高信頼パス呼出に関係する利用者の識別情報。**	***＜個別に定義した監査対象事象＞*** ***証明書の登録と抹消を監査する。***

② FAU_SAR.1 **監査レビュー**
下位階層: **なし**
FAU_SAR.1.1 TSF **は、**［**割付:***システム管理者*］ **が、**［**割付:***すべてのログ情報*］ **を監査記録から読み出せるようにしなければならない。**
FAU_SAR.1.2 TSF **は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。**
依存性: FAU_GEN.1 **監査データ生成**

③ FAU_SAR.2 **限定監査レビュー**
下位階層: **なし**
FAU_SAR.2.1 TSF **は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。**
依存性: FAU_SAR.1 **監査レビュー**

④ FAU_STG.1 **保護された監査証跡格納**
下位階層: **なし**
FAU_STG.1.1 TSF **は、格納された監査記録を不正な削除から保護しなければならない。**
FAU_STG.1.2 TSF **は、監査証跡内の格納された監査記録への不正な改変を**［**選択:***防止*］ **できねばならない。**
依存性: FAU_GEN.1 **監査データ生成**

⑤ FAU_STG.4 **監査データ損失の防止**
下位階層: FAU_STG.3
FAU_STG.4.1 TSF **は、監査証跡が満杯になった場合、**［**選択:***最も古いタイムスタンプで格納された監査データへの上書き*］ **及び**［**割付:***実施するその他のアクションは無い*］ **を行わねばならない。**
依存性: FAU_STG.1 **保護された監査証跡格納**

5.1.2. クラス FCS: 暗号サポート

① FCS_CKM.1 **暗号鍵生成**
下位階層: **なし**
FCS_CKM.1.1 TSF **は、以下の**［**割付:***指定なし*］ **に合致する、指定された暗号鍵生成アルゴリズム**［**割付:***富士ゼロックス標準の FXOSENC 方式*］ **と指定された暗号鍵長**［**割付:***128 ビット*］ **に従って、暗号鍵を生成しなければならない。**
依存性: ［FCS_CKM.2 **暗号鍵配付**
または
FCS_COP.1 **暗号操作**］
FCS_CKM.4 **暗号鍵破棄**
FMT_MSA.2 **セキュアなセキュリティ属性**

② FCS_COP.1 **暗号操作**
下位階層: **なし**
FCS_COP.1.1 TSF **は、**［**割付:***FIPS PUB 197*］ **に合致する、特定された暗号アル**

ゴリズム［割付：*AES*］と暗号鍵長［割付：*128 ビット*］に従って、［割付：*内部ハードディスク装置に蓄積される文書データおよびセキュリティ監査ログデータの暗号化、内部ハードディスク装置から取り出される文書データ、およびセキュリティ監査ログデータの復号化*］を実行しなければならない

依存性：　FCS_CKM.1　**暗号鍵生成**
FCS_CKM.4　**暗号鍵破棄**
FMT_MSA.2　**セキュアなセキュリティ属性**

5.1.3. クラス FDP：利用者データ保護

① FDP_ACC.1　**サブセットアクセス制御**
下位階層：　**なし**
FDP_ACC.1.1　TSF **は、**［**割付**：*表 10.に示すサブジェクトとオブジェクトのリストおよびオブジェクトの操作のリスト*］**に対して**［**割付**：*MFP アクセス制御 SFP*］**を実施しなければならない。**

表 10 サブジェクトとオブジェクトのリストおよびオブジェクトの操作のリスト

サブジェクト	オブジェクト	操作
機械管理者プロセス	*親展ボックス*	*個別親展ボックスの削除* *共用親展ボックスの作成* *共用親展ボックスの削除* *文書データの登録* *文書データの削除* *文書データの取り出し*
	蓄積プリント	*文書データの登録* *文書データの削除* *文書データの取り出し*
一般利用者プロセス	*親展ボックス*	*個別親展ボックスの作成* *個別親展ボックスの削除* *文書データの登録* *文書データの取り出し* *文書データの削除*
	蓄積プリント	*文書データの登録* *文書データの削除* *文書データの取り出し*

依存性：　FDP_ACF.1　**セキュリティ属性によるアクセス制御**

② FDP_ACF.1　**セキュリティ属性によるアクセス制御**
下位階層：　**なし**
FDP_ACF.1.1　TSF **は、以下の**［**割付**：*・一般利用者プロセスと対応する一般利用者識別情報、・親展ボックスと対応する所有者識別情報、・蓄積プリントと対応する所有者識別情報*］**に基づいて、オブジェクトに対して、**［**割付**：

MFP アクセス制御 SFP] を実施しなければならない。

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：

[割付：*表 11 に示す、制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]

表 11 アクセスを管理する規則

一般利用者プロセスの
親展ボックスの操作の規則
・個別親展ボックスの作成 *一般利用者プロセスが、個別親展ボックスの作成操作を行うと、個別親展ボックスの所有者識別情報に、個別親展ボックスを作成した一般利用者プロセスの一般利用者識別情報が設定された個別親展ボックスが作成される。* *・個別親展ボックスの削除* *個別親展ボックスの所有者識別情報と、一般利用者プロセスの一般利用者識別情報が一致した場合、その個別親展ボックスに関する、個別親展ボックスの削除の操作が許可される。* *・個別親展ボックスの文書データの登録、文書データの取り出し、文書データの削除* *個別親展ボックスの所有者識別情報と、一般利用者プロセスの一般利用者識別情報が一致した場合、その個別親展ボックスに関する、文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。* *・共用親展ボックスの文書データの登録、文書データの取り出し、文書データの削除* *親展ボックスが、共用親展ボックスの場合、その共用親展ボックスに関する、文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。*
蓄積プリントの操作の規則
・文書データの登録 *一般利用者プロセスが、文書データの登録の操作を行うと、一般利用者プロセスが持つ一般利用者識別情報を、その蓄積プリントの所有者識別情報に設定した蓄積プリントが作成され、その蓄積プリントに文書データが登録される。* *・文書データの削除、文書データの取り出し* *蓄積プリントの所有者識別情報と、一般利用者プロセスの一般利用者識別情報が一致した場合、一般利用者プロセスに対して、その蓄積プリントに関する、文書データの取り出し、文書データの削除の操作が許可される。文書データの削除の操作が行われると、その蓄積プリントも削除される。*
機械管理者プロセスの
・共用親展ボックスの作成、共用親展ボックスの削除 *機械管理プロセスの場合、共用親展ボックスの作成操作、共用親展ボックスの削除操作が許可される。*

FDP_ACF.1.3 TSF **は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない**:
[**割付**:*表 12 に示すセキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]

表 12 アクセスを明示的に管理する規則

機械管理者プロセスの
親展ボックスの操作の規則
・機械管理者プロセスの場合、すべての親展ボックスに対し親展ボックスの削除、文書データの登録、文書データの削除、文書データの取り出しの操作を許可する。
蓄積プリントの操作の規則
・機械管理者プロセスの場合、すべての蓄積プリントに対しすべての操作(文書データの登録、文書データの削除、文書データの取り出し)を許可する。

FDP_ACF.1.4 TSF**は、** [**割付**:*アクセスを明示的に拒否する規則は無い*] **に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。**

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

③ FDP_IFC.1 **サブセット情報フロー制御**
下位階層: **なし**
FDP_IFC.1.1 TSF **は、**[**割付**: *表 13 に示すサブジェクトと情報のリストおよび情報の流れを引き起こす操作のリスト*]**に対して**[**割付**: *ファクス情報フローSFP*]**を実施しなければならない。**

表 13 サブジェクトと情報のリストおよび情報の流れを引き起こす操作のリスト

サブジェクト	**情報**	**操作**
公衆電話回線受信 *内部ネットワーク送信*	*公衆回線データ*	*受け渡す*

依存性: FDP_IFF.1 **単純セキュリティ属性**

④ FDP_IFF.1 **単純セキュリティ属性**
下位階層:**なし**
FDP_IFF.1.1 TSF **は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、**[**割付**: *ファクス情報フローSFP*]**を実施しなければならない。**
[**割付**:
・示された SFP 下において制御される公衆電話回線送信、内部ネットワーク受信と公衆回線データのリスト、
・セキュリティ属性はない]
FDP_IFF.1.2 TSF **は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなけ**

		ればならない:
		[**割付**: ***公衆電話回線受信が受信した公衆回線データを、いかなる場合においても内部ネットワーク送信に渡さない***]
	FDP_IFF.1.3	TSF **は、** [**割付**:***追加の情報フロー制御 SFP 規則はない***] **を実施しなければならない。**
	FDP_IFF.1.4	TSF **は、以下の** [**割付**:***追加の SFP 能力のリストはない***] **を提供しなければならない。**
	FDP_IFF.1.5	TSF **は、以下の規則に基づいて、情報フローを明示的に承認しなければならない**: [**割付**:***セキュリティ属性に基づいて明示的に情報フローを承認する規則はない***] 。
	FDP_IFF.1.6	TSF **は、次の規則に基づいて、情報フローを明示的に拒否しなければならない**: [**割付**:***セキュリティ属性に基づいて明示的に情報フローを拒否する規則はない***] 。
	依存性:	FDP_IFC.1 **サブセット情報フロー制御** FMT_MSA.3 **静的属性初期化**
⑤	FDP_RIP.1	**サブセット残存情報保護**
	下位階層:	**なし**
	FDP_RIP.1.1	TSF **は、以下のオブジェクト** [**選択**:***からの資源の割当て解除***] **において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。**: [**割付**:***内部ハードディスク装置に蓄積される利用済み文書データ***]
	依存性:	**なし**

5.1.4. クラス FIA: 識別と認証

①	FIA_AFL.1 (1)	**認証失敗時の取り扱い**
	下位階層:	**なし**
	FIA_AFL.1.1 (1)	TSF **は、** [**割付**:***システム管理者の認証***] **に関して、** [**選択**: [**割付**: *5*]] **回の不成功認証試行が生じたときを検出しなければならない。**
	FIA_AFL.1.2 (1)	**不成功の認証試行が定義した回数に達するか上回ったとき、**TSF **は、** [**割付**:***操作パネルでは電源切断/投入以外の操作は受け付けない。またWeb ブラウザでも"本体の電源の切断/投入まで認証操作は受け付けない***] **をしなければならない。**
	依存性:	FIA_UAU.1 **認証のタイミング**
①	FIA_AFL.1 (2)	**認証失敗時の取り扱い**
	下位階層:	**なし**
	FIA_AFL.1.1 (2)	TSF **は、** [**割付**:***一般利用者の認証***] **に関して、** [**選択**: [**割付**:*1*]] **回の不成功認証試行が生じたときを検出しなければならない。**
	FIA_AFL.1.2 (2)	**不成功の認証試行が定義した回数に達するか上回ったとき、**TSF **は** [**割付**:***操作パネルでは"認証が不成功の"旨のメッセージを表示してユーザー情報の再入力を要求する。 Web ブラウザやネットワークスキャ***

ナーユーティリティではユーザー情報の再入力を要求する] をしなければならない。

依存性: FIA_UAU.1 **認証のタイミング**

② FIA_UAU.2 **アクション前の利用者認証**

下位階層: FIA_UAU.1 **認証のタイミング**

FIA_UAU.2.1 TSF **は、その利用者を代行する他の** TSF **調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。**

依存性: FIA_UID.1 **識別のタイミング**

③ FIA_UAU.7 **保護された認証フィードバック**

下位階層: **なし**

FIA_UAU.7.1 TSF **は、認証を行っている間、** [**割付**: *パスワードとして入力した文字を隠すための'**'*文字の表示*] **だけを利用者に提供しなければならない。**

依存性: FIA_UAU.1 **認証のタイミング**

④ FIA_UID.2 **アクション前の利用者識別**

下位階層: FIA_UID.1 **認証のタイミング**

FIA_UID.2.1 TSF **は、その利用者を代行する他の** TSF **調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。**

依存性: **なし**

5.1.5. クラス FMT:セキュリティ管理

① FMT_MOF.1 **セキュリティ機能のふるまいの管理**

下位階層: **なし**

FMT_MOF.1.1 TSF **は、機能** [**割付**: *表 14 のセキュリティ機能のリスト*] [**選択**: *のふるまいを動作させる、のふるまいを停止する、のふるまいを改変する*] **能力を** [**割付**: *表 14 の役割*] **に制限しなければならない。**

表 14 セキュリティ機能のリスト

TSF データ	ふるまい	役割
カストマーエンジニア操作制限機能	*動作、停止*	*機械管理者、SA*
ハードディスク暗号化機能	*動作、停止*	*機械管理者、SA*
システム管理者セキュリティ機能	*動作、停止、改変*	*機械管理者、SA*
セキュリティ監査ログ機能	*動作、停止*	*機械管理者、SA*
ユーザ認証機能	*動作、停止、改変*	*機械管理者、SA*
内部ネットワークデータ保護機能	*動作、停止、改変*	*機械管理者、SA*
ハードディスク蓄積データ上書き機能	*動作、停止、改変*	*機械管理者、SA*

依存性: FMT_SMF.1 **管理機能の特定**

FMT_SMR.1 **セキュリティ役割**

② FMT_MSA.1 **セキュリティ属性の管理**

下位階層: **なし**

FMT_MSA.1.1 TSF **は、セキュリティ属性**[**割付**: *一般利用者識別子、親展ボックスに*

対応する所有者識別子、*蓄積プリントに対応する識別子*]に対し[選択: *問い合わせ*、*削除*、[割付: *作成*]]をする能力を[割付: *表 15 の操作*、*役割*]に制限するために[割付: *MFP アクセス制御 SFP*]を実施しなければならない。

表 15 セキュリティ属性の管理役割

セキュリティ属性	操作	役割
一般利用者識別子	*問い合わせ*、*削除*、*作成*	*機械管理者*、*SA*
親展ボックスに対応する所有者識別子（個別親展ボックス）	*問い合わせ*、*削除*、*作成*	*一般利用者*
	問い合わせ、*削除*、	*機械管理者*
親展ボックスに対応する所有者識別子（共用親展ボックス）	*問い合わせ*、*削除*、*作成*	*機械管理者*
蓄積プリントに対応する識別子	*問い合わせ*、*削除*	*機械管理者*、*SA*、*一般利用者*

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

③ FMT_MSA.3 **静的属性初期化**
下位階層: **なし**
FMT_MSA.3.1 TSF **は、その** SFP **を実施するために使われるセキュリティ属性として、**[選択: *許可的*、[割付: *なし*]]**デフォルト値を与える**[割付: *MFP アクセス制御 SFP*]**を実施しなければならない。**
FMT_MSA.3.2 TSF **は、オブジェクトや情報が生成されるとき、**[割付: *なし*]**が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。**
依存性: FMT_MSA.1 **セキュリティ属性の管理**
FMT_SMR.1 **セキュリティの役割**

④ FMT_MTD.1 TSF **データの管理**
下位階層: **なし**
FMT_MTD.1.1 TSF **は、**[割付: *表 16 の TSF データの操作リスト*] **を** [選択: *問い合わせ*、*改変*、*削除*[割付: *なし*]] **する能力を** [割付: *表 16 の役割*] **に制限しなければならない。**

表 16 TSF データの操作リスト

TSF データ	操作	役割
機械管理者情報	*問い合わせ*、*改変*	*機械管理者*
SA の管理者権限情報	*問い合わせ*、*改変*	*機械管理者*、*SA*
カストマーエンジニア操作制限情報	*問い合わせ*、*改変*	*機械管理者*、*SA*
ハードディスク暗号化情報	*問い合わせ*、*改変*	*機械管理者*、*SA*
システム管理者情報	*問い合わせ*、*改変*	*機械管理者*、*SA*

セキュリティ監査ログ情報	*問い合わせ、改変*	*機械管理者、SA*
ユーザ認証情報（機械管理者、SA、一般利用者の認証情報）	*問い合わせ、改変、削除*	*機械管理者、SA*
ユーザ認証情報（自分自身の認証情報）	*問い合わせ、改変*	*一般利用者*
内部ネットワークデータ保護情報	*問い合わせ、改変、削除*	*機械管理者、SA*
ハードディスク蓄積データ上書き情報	*問い合わせ、改変*	*機械管理者、SA*
日付、時刻情報	*問い合わせ、改変*	*機械管理者、SA*

依存性： FMT_SMF.1 **管理機能の特定**
FMT_SMR.1 **セキュリティ役割**

⑤ FMT_SMF.1 **管理機能の特定**

下位階層： **なし**

FMT_SMF.1.1 **TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：**
[割付：*表 17 に示す TSF によって提供されるセキュリティ管理機能のリスト*]

表 17 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	CC で定義された管理対象	TOE の管理機能
FAU_GEN.1	なし	-
FAU_SAR.1	監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)	*システム管理者セキュリティ機能：（機械管理者、SA のシステム管理者権限の管理）*
FAU_SAR.2	なし	-
FAU_STG.1	なし	-
FAU_STG.4	監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	*なし* *理由：監査記録の制御パラメータは固定であり管理対象にならない*
FCS_CKM.1	暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある	*なし* *理由：暗号鍵の鍵長は固定であり、鍵長以外の属性はないので暗号鍵属性の変更の管理は必要ない。*
FCS_COP.1	なし	-
FDP_ACC.1	なし	-
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	*なし* *理由：アクセスはユーザ認証情報（ID とパスワード）により管理される*
FDP_IFC.1	なし	-
FDP_IFF.1	明示的なアクセスに基づく決定に使われる属性の管理。	*なし* *理由：アクセスは制限されており管理は必要ない*
FDP_RIP.1	いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除におい	*なし* *理由：文書データの削除時*

	て)が、TOE において設定可能にされる。	***に固定***
FIA_AFL.1	a) **不成功の認証試行に対する閾値の管理** b) **認証失敗の事象においてとられるアクションの管理**	***システム管理者セキュリティ機能:*** ***a) システム管理者情報 (認証失敗回数) の管理*** ***b) 機械動作のロック***
FIA_UAU.2	**管理者による認証データの管理**; **このデータに関係する利用者による認証データの管理。**	***システム管理者セキュリティ機能:*** ***機械管理者情報 (ID とパスワード) および SA 認証情報 (ID とパスワード) の管理***
FIA_UAU.7	**なし**	-
FIA_UID.2	**利用者識別情報の管理。**	***なし*** ***理由: アクセスはユーザ認証情報 (ID とパスワード) により管理される***
FMT_MOF.1	TSF **の機能と相互に影響を及ぼし得る役割のグループを管理すること**	***なし*** ***理由: 役割グループはシステム管理者だけであり管理対象にならない***
FMT_MSA.1	**セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること**	***なし*** ***理由: 役割グループは固定であり管理対象にならない***
FMT_MSA.3	a) **初期値を特定できる役割のグループを管理すること**; b) **所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。**	***なし*** ***理由: 役割グループはシステム管理者だけであり管理対象にならない***
FMT_MTD.1.	TSF **データと相互に影響を及ぼし得る役割のグループを管理すること。**	***なし*** ***理由: 役割グループはシステム管理者だけであり管理対象にならない***
FMT_SMF.1	**なし**	-
FMT_SMR.1	**役割の一部をなす利用者のグループの管理。**	***なし*** ***理由: 役割グループは固定であり管理対象にならない***
FPT_RVM.1	**なし**	-
FPT_STM.1	**時間の管理。**	***なし*** ***理由: システム管理者による管理***
FTP_TRP.1	**もしサポートされていれば、高信頼パスを要求するアクションの設定。**	***内部ネットワークデータ保護機能*** ***(暗号化の設定と証明書情報の管理)***

依存性: **なし**

⑥ FMT_SMR.1 (1) **セキュリティ役割**

下位階層: **なし**

FMT_SMR.1.1 (1) TSF **は、役割** [**割付:** ***機械管理者、SA***] **を維持しなければならない。**

FMT_SMR.1.2 (1) TSF **は、利用者を役割に関連づけなければならない。**
依存性: FIA_UID.1 **識別のタイミング**

⑥ FMT_SMR.1 (2) **セキュリティ役割**
下位階層: **なし**
FMT_SMR.1.1 (2) TSF **は、役割** [**割付**: ***一般利用者***] **を維持しなければならない。**
FMT_SMR.1.2 (2) TSF **は、利用者を役割に関連づけなければならない。**
依存性: FIA_UID.1 **識別のタイミング**

5.1.6. クラス FPT: TSF の保護

① FPT_RVM.1 **TSP の非バイパス性**
下位階層: **なし**
FPT_RVM.1.1 TSF **は、**TSC **内の各機能の動作進行が許可される前に、**TSP **実施機能が呼び出され成功することを保証しなければならない。**
依存性: **なし**

② FPT_STM.1 **高信頼タイムスタンプ**
下位階層: **なし**
FPT_STM.1.1 TSF **は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。**
依存性: **なし**

5.1.7. クラス FTP: 高信頼パス/チャネル

① FTP_TRP.1 **高信頼パス**
下位階層: **なし**
FTP_TRP.1.1 TSF **は、それ自身と** [**選択**: ***リモート***] **利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。**
FTP_TRP.1.2 TSF **は、** [**選択**: ***リモートの利用者***] **が、高信頼パスを介して通信を開始することを許可しなければならない。**
FTP_TRP.1.3 TSF **は、** [**選択**: [**割付**: *TOE の Web による通信サービス、プリンタドライバ用通信サービス、ファクスドライバ用通信サービス、ネットワークユーティティ用通信サービス、高信頼性パスが要求される他のサービス*]] **に対して、高信頼パスの使用を要求しなければならない。**
依存性: **なし**

5.1.8. 最小機能強度レベル

TOE **のセキュリティ機能強度の最小機能強度レベルは、**"SOF - **基本**"**である。 確率的・順列的メカニズムを利用する** TOE **セキュリティ機能要件は、**FIA_AFL.1 (1)、FIA_AFL.1 (2)、FIA_UAU.2、FIA_UAU.7 **である。**

5.2. TOE セキュリティ保証要件

表 18 に TOE 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。 すべての保証要件コンポーネントは、[CC パート 3] で規定されている、EAL2 のコンポーネントを直接引用している。

表 18 EAL2 保証要件

保証要件	セキュリティ保証要件名称	依存性
クラス ACM:	構成管理	
ACM_CAP.2	構成要素	なし
クラス ADO:	配布と運用	
ADO_DEL.1	配布手続き	なし
ADO_IGS.1	設置、生成、及び立ち上げ手順	AGD_ADM.1
クラス ADV:	開発と実装	
ADV_FSP.1	非形式的機能仕様	ADV_RCR.1
ADV_HLD.1	記述的上位レベル設計	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	非形式対応の実証	なし
クラス AGD:	ガイダンス文書	
AGD_ADM.1	管理者ガイダンス	ADV_FSP.1,
AGD_USR.1	利用者ガイダンス	ADV_FSP.1
クラス ATE:	テスト	
ATE_COV.1	カバレージの証拠	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	機能	なし
ATE_IND.2	独立試験 – サンプル	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
クラス AVA:	脆弱性評価	
AVA_SOF.1	TOE セキュリティ機能強度評価	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	開発者脆弱性分析	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

5.3. IT 環境セキュリティ機能要件

TOE の IT 環境が提供するセキュリティ機能要件はない。

6. TOE 要約仕様

本章では、TOE の要約仕様について記述する。

6.1. TOE セキュリティ機能

本 TOE は、5.1 章で記述した TOE セキュリティ機能要件を満足するために、以下のセキュリティ機能を提供する。

セキュリティ機能要件と TOE のセキュリティ機能の関係を、表 19 TOE セキュリティ機能要件とセキュリティ機能の関係に記述する。

① **ハードディスク蓄積データ上書き消去機能** (TSF_IOW)

② **ハードディスク蓄積データ暗号化機能** (TSF_CIPHER)

③ **ユーザー認証機能** (TSF_USER_AUTH)

④ **システム管理者セキュリティ管理機能** (TSF_FMT)

⑤ **カストマーエンジニア操作制限機能** (TSF_CE_LIMIT)

⑥ **セキュリティ監査ログ機能** (TSF_FAU)

⑦ **内部ネットワークデータ保護機能** (TSF_NET_PROT)

⑧ **ファクスフローセキュリティ機能** (TSF_FAX_FLOW)

本 TOE は MFP であり、汎用的なコンピュータやソフトウエアではないため、構造的にセキュリティ機能をバイパス、破壊、盗聴、改ざん、その他の点で危うくなることはない。 TOE の処理の論理的な枠組みは、MFP における各“セション”が独自であり、それぞれの TOE セキュリティ機能がバイパス出来ないことである。 さらに利用者と TOE との相互作用は、以下が満たされるように、TOE とその環境間におけるオブジェクト転送が、TOE セキュリティ機能要件によって、以下のように制御されている。

- 利用者によってドメイン間のデータ転送は出来ない。
- 利用者によって実行可能コードやオブジェクト、または構成ファイル等を、TOE へアップロードすることは出来ない。
- 利用者によってドメインのデータを、参照または更新することは出来ない。

また本 TOE が提供するセキュリティ機能は、バイパス手段を持たないコントローラ ROM 内の独自ソフトウエアで実現されており、確実に動作する構成となっている。

表 19 TOE セキュリティ機能要件とセキュリティ機能の関係

セキュリティ機能 / TOE 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_FAX_FLOW
FAU_GEN.1						○		
FAU_SAR.1						○		
FAU_SAR.2						○		
FAU_STG.1						○		
FAU_STG.4						○		
FCS_CKM.1		○						
FCS_COP.1		○						
FDP_ACC.1			○	○				
FDP_ACF.1			○	○				
FDP_IFC.1								○
FDP_IFF.1								○
FDP_RIP.1	○							
FIA_AFL.1 (1)			○					
FIA_AFL.1 (2)			○					
FIA_UAU.2			○					
FIA_UAU.7			○					
FIA_UID.2			○					
FMT_MOF.1				○	○			
FMT_MSA.1			○	○				
FMT_MSA.3				○				
FMT_MTD.1				○	○			
FMT_SMF.1				○				
FMT_SMR.1 (1)				○				
FMT_SMR.1 (2)			○					
FPT_RVM.1	○	○	○	○	○	○	○	○
FPT_STM.1						○		
FTP_TRP.1							○	

6.1.1. ハードディスク蓄積データ上書き消去機能 (TSF_IOW)

本 TSF_IOW 機能は、システム管理者によりツール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、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。

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、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。

さらに、システム管理者が設定した時刻に蓄積文書を削除して上書き消去する（時刻指定文書削除機能）。

本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

6.1.2. ハードディスク蓄積データ暗号化機能 （TSF_CIPHER）

本 TSF_CIPHER 機能は、システム管理者によりツール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、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。

暗号鍵はシステム管理者によりツールモードで設定された「ハードディスク蓄積データ暗号化キー」を使用し、TOE 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 128 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。）

TOE は内部ハードディスク装置に文書データを蓄積する場合、起動時に生成した暗号鍵を使用して、文書データの暗号化を行った後に蓄積する。 また蓄積した文書データを読み出す場合は、起動時に生成した暗号鍵を使用して復号化を行う。

セキュリティメカニズムとして、暗号鍵は暗号化メカニズム（ラインダールアルゴリズムによる暗号化）を利用して、MFP 本体の電源投入後に生成され、コントローラボード上の DRAM に記憶される。なお暗号鍵は MFP 本体の電源を切断すると消滅する。

本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

6.1.3. ユーザー認証機能 （TSF_USER_AUTH）

本 TSF_USER_AUTH 機能は、許可された特定の利用者だけに MFP の機能を使用する権限を持たせるために、操作パネルまたは利用者クライアントのプリンタドライバ、ネットワークスキャナユーティリティ、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する機能を有する。

認証が成功した一般利用者のみが下記の機能を使用可能となる。

① 本体操作パネルで制御される機能

コピー機能、ファクス機能（送信）、iFAX 機能（送信）、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（プリンタドライバでのユーザーID とユーザーパスワードの設定が条件であり印刷時に操作パネルで認証する）

②一般利用者クライアントのネットワークスキャナユティリティで制御される機能

親展ボックスからの文書データ取出し機能

③CWIS 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

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、

･本体操作パネルから認証する場合のプリンター機能（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、ネットワークスキャナユティリティ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

MFP で「認証成功のジョブをプライベートプリントに保存」の設定を行うと、一般利用者が一般利用者クライアントのプリンタドライバーからユーザーID とパスワードを設定した状態でプリント指示をする場合、MFP 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）してプライベートプリントとしてユーザーID ごとに区分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、認証後に一般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。

一般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、MFP 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。一般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 とファクスボードから親展ボックスにスキャンデータとファクス受信データを格納することが可能である。

スキャンデータを親展ボックスに格納するには、一般利用者が MFP 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、認証されるとスキャン機能の利用が可能になり、操作パネルから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。

ファクス受信データを親展ボックスに格納する場合にはユーザー認証は行わず、公衆電話回線網を介して接続相手機から送られて来たファクス受信データのうち、送信時に親展ボックスを指定した親展ファクス受信データ、特定相手の電話番号ごとのファクス受信データ、送信元不定のファクス受信データがそれぞれ指定された親展ボックスに自動的に格納されることで可能となる。

登録されたユーザーID ごとの個別親展ボックスは、一般利用者が操作パネル、CWIS またはネットワークスキャナーユーティリティからユーザーID とパスワードを入力すると MFP 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、削除の操作が可能となる。

＊ 親展ボックスには、共用親展ボックスと個別親展ボックスがあり下記の通り機能する。

	個別親展ボックス	共用親展ボックス
ボックスの作成	一般利用者が可能	機械管理者が可能
ボックスの削除	登録した一般利用者と機械管理者が可能	機械管理者が可能
文書の登録	登録した一般利用者と機械管理者が可能	一般利用者と機械管理者が可能
文書の取り出し	登録した一般利用者と機械管理者が可能	一般利用者と機械管理者が可能
文書の削除	登録した一般利用者と機械管理者が可能	一般利用者と機械管理者が可能

- システム管理者（機械管理者とSA）は識別認証のために操作パネルまたはシステム管理者クライアントのブラウザー（CWIS）からユーザーIDとパスワードを入力し、MFPは内部に登録されたシステム管理者のIDとパスワードが一致するかをチェックし、一致した場合のみシステム管理者セキュリティ管理機能へのアクセスが可能となる。
- 一般利用者のユーザーIDとパスワードが一致せず、認証が不成功の場合は、操作パネルでは”認証が不成功の”旨のメッセージを表示してユーザー情報の再入力を要求する。
  またWebブラウザやネットワークスキャナーユーティリティではユーザー情報の再入力を要求する。
- システム管理者のユーザーIDとパスワードが一致せず、認証が不成功の場合は一般利用者の認証不成功時と同じく再入力が要求されるが、5回の不成功認証が生じたときは、操作パネルでは電源切断/投入以外の操作は受け付けず、またWebブラウザでも“本体の電源の切断/投入まで認証操作は受け付けない。
- 一般利用者のユーザーIDはシステム管理者のみ作成、変更、削除が可能であるが、一般利用者のパスワードは一般利用者自身が操作パネルから変更可能である。

パスワードの入力は、入力した値を隠すために、すべて'*'文字に置き換えて表示する。
本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

6.1.4. システム管理者セキュリティ管理機能 （TSF_FMT）

本TSF_FMT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、ツール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、許可されたシステム管理者のみに、操作パネルから下記のTOEセキュリティ機能の設定を参照し、設定変更を行う権限を許可する。

- TSF_IOW機能の設定を参照し、有効/無効の設定を行う
- TSF_CIPHER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の使用の設定を参照し、有効/無効の設定を行う
- 機械管理者IDの設定を参照し、IDとパスワード変更をする（機械管理者のみ可能）
- SA、一般利用者のID設定を参照しIDとパスワード変更をする
- 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、拒否回数の設定をする
- ユーザーパスワード（一般利用者とSA）の最小文字数を参照し設定する
- TSF_CE_LIMIT機能の設定を参照し、有効/無効の設定を行う
- TSF_NET_PROTのSSL/TLS通信の設定を参照し、有効/無効および詳細情報を設定する
- TSF_NET_PROTのIPSec通信の設定を参照し、有効/無効および詳細情報を設定する
- TSF_NET_PROTのS/MIME通信の設定を参照し、有効/無効および詳細情報を設定する
- 時刻指定文書削除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
- TSF_USER_AUTH機能の設定を参照し、ローカル認証/無効の設定を行う
- 日付、時刻を参照し設定を行う

さらに本TSF_FMT機能は、セキュアな接続（HTTPS）が可能なWebブラウザを通して、許可されたシステム管理者のみに、CWISから下記のTOEセキュリティ機能の設定を行う権限を許可する。

- 機械管理者IDの設定を参照し、IDとパスワード変更をする（機械管理者のみ可能）

- SA、一般利用者の ID 設定を参照し、ID とパスワード変更をする
- 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、拒否回数の設定をする
- TSF_FAU 機能の設定を参照し有効/無効にする
  （有効時は、監査ログ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。）
- TSF_NET_PROT の SSL/TLS 通信の設定を参照し、有効/無効および詳細情報を設定する
- TSF_NET_PROT の IPSec 通信の設定を参照し、有効/無効および詳細情報を設定する
- TSF_NET_PROT の SNMPv3 通信の設定を参照し、有効/無効および詳細情報を設定する
- SNMPv3 認証パスワード設定を行う
- TSF_NET_PROT の S/MIME 通信の設定を参照し、有効/無効および詳細情報を設定する
- X.509 証明書を作成/アップロード/ダウンロードする
- 時刻指定文書削除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
- TSF_USER_AUTH 機能の設定を参照し、ローカル認証/無効の設定を行う

本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

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

本 TSF_CE_LIMIT 機能は、システム管理者によりツールモードで設定された「カストマーエンジニア操作制限機能設定」に従い、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が出来ないように、システム管理者がカストマーエンジニアのツールモードへの操作を制限する機能である。

本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

6.1.6. セキュリティ監査ログ機能 (TSF_FAU)

本 TSF_FAU 機能は、システム管理者によりツール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。

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。

監査ログへのアクセスは、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。 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、SSL/TLS 通信を有効に設定されていなければならない。

表 20 に監査ログデータの詳細を示す

表 20 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。:

- **Log ID:監査ログ識別子としての通し番号 (1～60000)**
- **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)**
- **Optionally Logged Items:共通保存項目以外に監査ログへ保存される追加情報**

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	
	User operation(Local)	Start/End
	Scheduled Image Overwriting started	Successful/Failed
	Scheduled Image Overwriting finished	Successful/Failed
ユーザー認証		
Login/Logout	Login(Local Access)	Successful, Failed(Invalid UserID), Failed(Invalid Password), Failed
	Logout	
	Locked System Administrator Authentication	- (**失敗回数も保存**)
	Detected continuous Auhtentication Fail	
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	
	Fax	
	Mailbox	
	Print Reports	
	Job Flow Service	

デバイス設定変更		
Device Settings	Adjust Time	Successful/Failed
	Create Mailbox	
	Delete Mailbox	
	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	Import Certificate	Successful/Failed
	Delete Certificate	
	Add Address Entry	
	Delete Address Entry	
	Edit Address Entry	
	Export Audit Log	

本機能は、バイパス手段を持たない独自のソフトウエアで実現されており、確実に動作する構成となっている。

6.1.7. 内部ネットワークデータ保護機能 (TSF_NET_PROT)

本 TSF_NET_PROT **機能は、システム管理者によりツールモードで設定された下記** 5 **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 SSL/TLS **プロトコル**

システム管理者によりツールモードで設定された「SSL/TLS **通信」に従い、内部ネットワーク上を流れる文書データ、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、**SSL/TLS **プロトコルに対応している。**

TOE **が対応する機能により、**SSL/TLS **サーバーまたは** SSL/TLS **クライアントとして動作することが出来る。 また** SSL/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、**MFP **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。**

・ SSLv3/TLSv1 **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。

SSL/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**
SSL_RSA_WITH_RC4_128_SHA	RC4/128 **ビット**	SHA1
SSL_RSA_WITH_3DES_EDE_CBC_SHA	3Key Triple-DES/168 **ビット**	SHA1
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

また改ざんからの保護は、SSL/TLS **記録転送プロトコルの** 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** SSL/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。 SSL/TLS通信は、IPsec、SNMPv3 、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。

② IPSec プロトコル

システム管理者によりツール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、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、MFP 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

③ SNMPv3 プロトコル

システム管理者によりツールモードで設定された「SNMPv3 通信」に従い、ネットワーク管理プロトコルの SNMP を利用する時の、セキュリティソリューションの一つとして、SNMPv3 プロトコルに対応している。 SNMPv3 プロトコルは IETF RFC3414 で規定されているように、データの暗号化のみならず、各 SNMP メッセージを認証するために使用される。

この機能を使用する時は、認証パスワードとプライバシー（暗号化）パスワードの両方を、TOE とリモートサーバーの両方にセットアップしなければならない。 またパスワードは共に 8 文字以上で運用しなければならない。

SNMPv3 の認証は SHA-1 ハッシュ関数を使用し、また暗号化は CBC -DES を使用する。 なお暗号鍵はセションの開始時に生成され、MFP 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。

・SNMPv3E プロトコルとして生成される接続毎の暗号鍵

共通鍵暗号方式/鍵サイズ	ハッシュ方式
DES/56 ビット	SHA1

④ S/MIME プロトコル

システム管理者によりツール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竄を防止する。
なお暗号鍵はメールの暗号化開始時に生成され、MFP 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を選択する。

共通鍵暗号方式/鍵サイズ	ハッシュ方式
RC2/128 ビット	SHA1
3Key Triple-DES/168 ビット	SHA1

6.1.8. ファクスフローセキュリティ機能 (TSF_FAX_FLOW)

本 TSF_FAX_FLOW 機能は、いかなる場合においても公衆電話回線網から内部ネットワークに公衆電話回線データを受け渡さない。

6.2. セキュリティ機能強度

TOE セキュリティ機能の中で、確率的または順列的メカニズムによって実現されている機能は、ユーザー認証機能 (TSF_USER_AUTH) である。 本機能の機能強度レベルは SOF – 基本である。

6.3. 保証手段

本 TOE は、EAL2 の評価保証レベルを満たしており、表 21 に TOE のセキュリティ保証手段を記述する。 以下のセキュリティ保証手段は、5.2 章の TOE セキュリティ保証要件を満たすものである。

表 21 保証コンポーネントと保証手段の対応関係

保証要件	セキュリティ保証要件名称	保証手段 (識別子)
クラス ACM:	構成管理	
ACM_CAP.2	構成要素	構成管理説明書 TOE 構成要素リスト
クラス ADO:	運用と配布	
ADO_DEL.1	配布手続き	配布、導入運用手続き説明書
ADO_IGS.1	設置、生成、及び立ち上げ手順	ユーザーズガイド
クラス ADV:	開発と実装	
ADV_FSP.1	非形式的機能仕様	機能仕様書 Disclosure Paper
ADV_HLD.1	記述的上位レベル設計	上位レベル仕様書
ADV_RCR.1	非形式対応の実証	対応分析書
クラス AGD:	ガイダンス文書	
AGD_ADM.1	管理者ガイダンス	ユーザーズガイド
AGD_USR.1	利用者ガイダンス	

保証要件	セキュリティ保証要件名称	保証手段（識別子）
クラス ATE：	テスト	
ATE_COV.1	カバレージの証拠	テスト計画書兼報告書
ATE_FUN.1	機能テスト	
ATE_IND.2	独立試験 – サンプル	
クラス AVA：	脆弱性評価	
AVA1_SOF.1	セキュリティ機能強度評価	脆弱性分析書
AVA1_VLA.1	開発者脆弱性分析	

6.3.1. 構成管理説明書（TAS_CONFIG）

「WorkCentre 7328 シリーズ構成管理説明書」には、以下の内容が記述されている。

- 構成管理システムについてその機能と利用方法。
- TOE を一意に識別するための命名規則。
- TOE に含まれる構成要素。
- 各構成要素の一意の識別子。
- TOE 構成要素の変更履歴の追跡方法。

対応するセキュリティ保証要件

- ACM_CAP.2

6.3.2. TOE 構成要素リスト（TAS_CONFIG_LIST）

「WorkCentre 7328 シリーズ TOE 構成要素リスト」には、以下の内容が記述されている。

- 証拠資料と対応する TOE 構成要素。
- TOE 構成要素を一意に識別するためのバージョン。

対応するセキュリティ保証要件

- ACM_CAP.2

6.3.3. 配布・導入・運用手続き説明書（TAS_DELIVERY）

「WorkCentre 7328 シリーズ配布、導入、運用手続き説明書」には、以下の内容が記述されている。

- TOE の識別、輸送中の完全性を維持するための手順。
- TOE のセキュリティを維持するための、運用環境から利用者へ配布までに適用する全ての手続き。
- 利用者が TOE を受け取った場合に、TOE が正しいことを確認する方法。
- 導入、設置、および起動に関するセキュリティ上の注意事項と、正しい導入、設置、および起動の確認方法。
- 例外事象の内容とその対処方法。
- 安全な導入、および設置に必要となる最小限のシステム要件。

対応するセキュリティ保証要件

- ADO_DEL.1
- ADO_IGS.1

6.3.4. 機能仕様書 (TAS_FUNC_SPEC)

「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 機能仕様書」には、以下の内容が記述されている。

- TOE の全てのセキュリティ機能と、その外部インタフェース(ある場合のみ)。
- 前記外部インタフェースの目的、機能、および使用方法(パラメータ、例外事項、エラーメッセージを含む)。
- TOE のセキュリティ機能の完全なる記述。

対応するセキュリティ保証要件

- ADV_FSP.1

6.3.5. Disclosure Paper (TAS_DISC_PAPER)

「WorkCentre 7328/7335/7345 Information Assurance Disclosure Paper」には、以下の内容が記述されている。

- TOE の全ての文書データの蓄積・送信方法、ネットワーク環境における MFP の動作、ローカル及びリモート両方からの MFP トへのアクセス方法

対応するセキュリティ保証要件

- ADV_FSP.1

6.3.6. 上位レベル設計書 (TAS_HIGHLDESIGN)

「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 上位レベル設計書」には、以下の内容が記述されている。

- サブシステムから見た TOE のセキュリティ機能の構造。
- 全サブシステム間のインタフェースについて、その目的と利用方法(例外事項、エラーメッセージを含む)。
- セキュリティ機能を提供するサブシステムとそれ以外のサブシステムの識別。

対応するセキュリティ保証要件

- ADV_HLD.1

6.3.7. 対応分析書 (TAS_REPRESENT)

「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 対応分析書」には、以下の内容が記述されている。

- セキュリティ機能に関して、全設計段階で正確かつ完全に反映されている事の分析。

対応するセキュリティ保証要件

- ADV_RCR.1

6.3.8. ユーザーズガイド (TAS_GUIDANCE)

TOE の開発において、マニュアル(Xerox WorkCentre 7328/7335/7345 System Administrator's Guide、 Xerox WorkCentre 7328/7335/7345 Security Function Supplementary Guide)を作成し、以下のレビューを開発部門、製品評価部門、テクニカルサポート部門で行う。

① レビュー内容

- TOE に関する全てのハードウェアおよびソフトウエアの障害発生後の処理、全ての操作ミス発生後の処理、初期設定時の処理、障害復旧時の処理について、その内容とセキュリティへの影響、セキュリティを維持するための対策、運用モードについてのマニュアルへの記載確認。
- 全てのマニュアルにおける用語統一の確認。
- マニュアルの記述内容の明白性、合理性、および非矛盾性の確認。
- TOE の機能仕様書、テスト仕様書とマニュアルに記載された内容の一貫性の確認。

「Xerox WorkCentre 7328/7335/7345 System Administrator's Guide、 Xerox WorkCentre 7328/7335/7345 Security Function Supplementary Guide」には、以下の内容が記述されており、システム管理者、および一般利用者共通である。

② システム管理者向け記載内容

- システム管理者が利用する管理機能とそのインタフェース。
- セキュリティを確保して、TOE を管理するための方法。
- セキュリティが確保された環境で、管理すべき機能や権限に関する注意事項。
- システム管理者の管理下にある、全てのセキュリティ関連のパラメータと、パラメータ値の注意事項。
- システム機能に対する全てのセキュリティ事象の種別。
- システム管理者の責任や行為についての前提条件。
- システム管理者への警告メッセージの内容と具体的な対策方法の明示。

③ 一般利用者向け記載内容

- 一般利用者が利用可能なセキュリティ機能の使用法。
- 一般利用者が利用する機能とそのインタフェース。
- セキュリティが確保された環境で、利用すべき機能や権限に関する注意事項。
- 一般利用者の責任や行為についての前提条件。
- 一般利用者への警告メッセージの内容と具体的な対策方法の明示。

対応するセキュリティ保証要件

- ADO_DEL.1
- ADO_IGS.1
- AGD_ADM.1
- AGD_USR.1

6.3.9. テスト計画書 兼 報告書 (TAS_TEST)

「WorkCentre 7328 シリーズテスト計画書 兼 報告書」には、以下の内容が記述されている。

- テストに使用するシステムの構成やスケジュール、およびテスターに必要なスキルを記載した全体計画。
- テスト項目。
- テスト項目が「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 機能仕様書」に記載されている機能を、全てテストしているかを検証するテストカバレージ分析。
- 各テスト項目の目的。

- 各テスト項目の実施方法。
- 各テスト項目における期待結果。
- 各テスト項目の実施日およびテスト実施者名。
- 各テスト項目の結果。

対応するセキュリティ保証要件

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.3.10. 脆弱性分析書 (TAS_VULNERABILITY)

TOE のセキュリティ強度、および脆弱性の確認評価を行うため、「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 脆弱性分析書」を作成する。脆弱性分析書には、以下の内容が記述されており、想定される環境で TOE のセキュリティ強度、および TOE の識別された脆弱性が問題とならないことを検証する。

① セキュリティ強度

- TOE のセキュリティ機能に対して、そのセキュリティ強度が本 ST で規定された最小強度以上、および各規定強度以上であることの分析結果。
- 確率論、順列、組み合わせなどの技法を利用する全ての機能に対して、強度分析が行われていることの確認結果。
- セキュリティ強度分析の仮説の妥当性検証結果。

② 脆弱性

- 一般的なセキュリティ問題に関する情報や、評価のために提供される全資材を利用して、脆弱性分析を行っていることの確認。
- 識別される全ての脆弱性に対して、それらが想定する運用環境で問題とならないことの検査結果。
- TOE の構成、機能の動作条件設定に関する脆弱性に関して、注意事項がマニュアルに記載されていることの確認結果。

対応するセキュリティ保証要件

- AVA1_SOF.1
- AVA1_VLA.1

7. PP 主張

本章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修正

修正した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、および TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

TOE セキュリティ対策方針および環境セキュリティ対策方針と、TOE セキュリティ環境として記述した前提条件、脅威、組織のセキュリティ方針の対応を、表 22 に記述する。 また各 TOE セキュリティ環境が TOE/環境セキュリティ対策方針により保証されていることを、表 23 に記述する。

表 22 TOE/環境セキュリティ対策方針と TOE セキュリティ環境の対応

TOE セキュリティ環境 / TOE/環境 セキュリティ対策方針	A.ADMIN	A.SECMODE	T.RECOVER	T.CONFDATA	T.COMM_TAP	T.DATA_SEC	T.CONSUME	P.FAX_OPT
O.AUDITS				○		○		
O.CIPHER			○					
O.COMM_SEC					○			
O.FAX_SEC								○
O.MANAGE				○		○		
O.RESIDUAL			○					
O.USER						○	○	
O.RESTRICT							○	
OE.ADMIN	○							
OE.AUTH		○		○		○		
OE.COMMS_SEC		○			○			
OE.FUNCTION		○	○			○		

表 23 TOE セキュリティ環境による TOE セキュリティ対策方針

TOE セキュリティ環境	TOE セキュリティ対策方針根拠
A.ADMIN	環境セキュリティ対策方針である OE.ADMIN により、TOE を運用する組織の責任者は、システム管理者の適切な人選を行うと共に、TOE に関する管理や教育を実施する。 この対策方針により、A.ADMIN を実現できる。
A.SECMODE	環境セキュリティ対策方針である OE.AUTH によりシステム管理者は ID とパスワードを適切に設定し、またユーザー認証を有効にして運用する。

TOE セキュリティ環境	TOE セキュリティ対策方針根拠
	また OE.COMMS_SEC により、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定して運用する。 また OE.FUNCTION により、「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」、「セキュリティ監査ログ機能」を有効に設定して運用する。 この対策方針により、A.SECMODE を実現できる。
T.RECOVER	この脅威に対抗するには、環境セキュリティ対策方針である OE.FUNCTION により、下記の TOE セキュリティ機能を有効に設定して、内部ハードディスク装置に蓄積されている文書データやセキュリティ監査ログデータの読み出しや、利用済み文書データの復元を、不可能にする事が必要であり、具体的にはセキュリティ対策方針である O.RESIDUAL、および O.CIPHER よって対抗する。 「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」 文書データを保護するため、O.CIPHER により、内部ハードディスク装置上に蓄積される文書データやセキュリティ監査ログデータを暗号化することによって、文書データやセキュリティ監査ログデータの閲覧や読み出しを不可能にする。 また利用済み文書データを保護するため、O.RESIDUAL により、利用が終了した文書データを上書き消去することによって、内部ハードディスク装置上に蓄積された利用済み文書データの再生や復元を不可能にする。 これらの対策方針により、T.RECOVER に対抗できる。
T.CONFDATA	この脅威に対抗するには、環境セキュリティ対策方針である OE.AUTH により、下記の TOE セキュリティ機能を有効に設定して、認証されたシステム管理者のみに、TOE 設定データの変更を許可する事が必要であり、具体的にはセキュリティ対策方針である O.MANAGE によって対抗する。 • 「パスワード使用設定」、「システム管理者パスワード」、「システム管理者 ID 認証失敗によるアクセス拒否回数」、「カストマーエンジニア操作制限機能設定」 O.MANAGE により、TOE セキュリティ機能の有効/無効化や、TOE 設定データの参照/更新は、認証されたシステム管理者のみに限定される。 また O.AUDITS により不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供する。 これらの対策方針により、T.CONFDATA に対抗できる。
T.CONSUME	この脅威に対抗するには、環境セキュリティ対策方針である O.RESTRICT と O.USER によって対抗する。 O.USER により、MFP の利用は認証された正当な利用者のみに限定される。 また O.RESTRICT により TOE の利用を制限することができる。

TOE セキュリティ環境	TOE セキュリティ対策方針根拠
	これらの対策方針により、T.CONSUME に対抗できる。
T.COMM_TAP	この脅威に対抗するには、セキュリティ対策方針である O.COMM_SEC により、暗号化通信プロトコルが持つネットワーク認証により、正規の利用者のみ許可される。 また暗号機能により通信データを暗号化することによって、内部ネットワーク上の文書データ、、セキュリティ監査ログデータおよび TOE 設定データの盗聴や改ざんを不可能にする。 さらに環境セキュリティ対策方針である OE.COMMS_SEC により、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定することで、これらのデータが保護対象となる。 これらの対策方針により、T.COMM_TAP に対抗できる。
T.DATA_SEC	この脅威に対抗するには、環境セキュリティ対策方針である OE.AUTH と OE.FUNCTION より、下記のパスワードとユーザー認証機能、セキュリティ監査ログ機能を設定して、認証された正当な利用者のみに、セキュリティ監査ログデータと文書データへのアクセスを許可する必要があり、具体的にはセキュリティ対策方針である O.USER と O.MANAGE によって対抗する。 • 「ユーザーパスワード」、「システム管理者パスワード」「ローカル認証」、「セキュリティ監査ログ機能」 O.USER により、内部ハードディスク装置上に蓄積された文書データやセキュリティ監査ログデータの読み出しは、認証された正当な利用者のみに限定される。 また O.MANAGE によりセキュリティ機能の設定を認証されたシステム管理者のみに限定する。 また O.AUDITS により不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供する。 これらの対策方針により、T.DATA_SEC に対抗できる。
P.FAX_OPT	公衆電話回線網経由で内部ネットワークへアクセス出来ないようにする事が必要であり、セキュリティ対策方針である O.FAX_SEC によって対抗する。 公衆電話回線網から内部ネットワークに公衆電話回線データを受け渡さないので、公衆電話回線受信が受信した公衆回線データは内部ネットワーク送信に渡らない。 この対策方針により、P.FAX_OPT を順守できる

8.2. セキュリティ要件根拠

8.2.1. TOE セキュリティ機能要件根拠

TOE 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、表 24 に記述する。 また各セキュリティ対策方針が TOE セキュリティ機能要件により保証されている根拠を、表 25 に記述する。

表 24 TOE セキュリティ機能要件とセキュリティ対策方針の対応

セキュリティ対策方針 / TOE セキュリティ機能要件	O.AUDITS	O.CIPHER	O.COMM_SEC	O.FAX_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FAU_GEN.1	○							
FAU_SAR.1	○							
FAU_SAR.2	○				○			
FAU_STG.1	○							
FAU_STG.4	○							
FCS_CKM.1		○				○		
FCS_COP.1		○				○		
FDP_ACC.1								○
FDP_ACF.1								○
FDP_IFC.1				○				
FDP_IFF.1				○				
FDP_RIP.1						○		
FIA_AFL.1 (1)					○			
FIA_AFL.1 (2)							○	○
FIA_UAU.2					○		○	○
FIA_UAU.7					○		○	○
FIA_UID.2					○		○	○
FMT_MOF.1					○			
FMT_MSA.1								○
FMT_MSA.3								○
FMT_MTD.1					○			
FMT_SMF.1					○			
FMT_SMR.1 (1)					○			
FMT_SMR.1 (2)								○
FPT_RVM.1	○	○	○	○	○	○	○	○
FPT_STM.1	○							
FTP_TRP.1			○					

表 25 セキュリティ対策方針による TOE セキュリティ機能要件根拠

対策方針	TOE セキュリティ機能要件根拠
O.AUDITS	O.AUDITS は監査イベントの記録機能とセキュリティ監査ログデータ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、 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：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,FSC_COP.1：暗号化の失敗はジョブステータスとして監査される ・FDP_IFF.1：フローは固定であり監査すべき事象はない) 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。 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。 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監査ログに記録される。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.AUDITS 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やセキュリティ監査ログ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 FCS_CKM.1 により指定された 128 ビットの暗号鍵長に従って、暗号鍵が生成される。 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、文書データやセキュリティ監査ログ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、読み出し時に複合化される。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.CIPHER を満たすことができる。
O.COMM_SEC	O.COMM_SEC は内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを、盗聴や改ざんから保護する機能

対策方針	TOE セキュリティ機能要件根拠
	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、 FTP_TRP.1 により 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、セキュリティ監査ログデータおよび 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ことで、高信頼パスを提供することが出来る。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.COMM_SEC を満たすことができる。
O.FAX_SEC	O.FAX_SEC は、公衆電話回線から内部ネットワークへのアクセス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、 FDP_IFC.1、FDP_IFF.1 により、TOE のファクスモデムの通信路を通じて、公衆電話回線網から TOE が接続されている内部ネットワークへのアクセスを防ぐ。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.FAX_SEC は満たすことができる。
O.MANAGE	O.MANAGE はセキュリティ機能の設定を行うツールモードのアクセスを、認証されたシステム管理者のみ許可して、一般利用者による TOE 設定データやセキュリティ監査ログデータへのアクセスを、不可能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.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。 FIA_AFL.1 (1) によりシステム管理者認証の認証失敗時に、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 が必要になり、連続した攻撃を防ぐ。 FIA_UAU.2 により正当なシステム管理者か個人を識別するために、ユーザー認証が行われる。 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。 FIA_UID.2 により正当なシステム管理者か個人を識別するために、ユーザー認証が行われる。 FMT_MOF.1 により TOE 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 TOE 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、TSF データの問い合わせ、改変、削除は、システム管理者だけに制限される。

対策方針	TOE セキュリティ機能要件根拠
	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 (1) により特権を持つ利用者として、システム管理者の役割を維持することで、セキュリティに関する役割をシステム管理者に特定する。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.MANAGE を満たすことができる。
O.RESIDUAL	O.RESIDUAL は内部ハードディスク装置に蓄積される利用済み文書データの再生および復元を、不可能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、 FCS_CKM.1 FCS_COP.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を暗号化することで内容を利用できなくする。 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。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.RESIDUAL を満たすことができる。
O.RESTRICT	O.RESTRICT は許可されていない者への TOE の利用を制限する機能を持つ対策方針である。 本セキュリティ対策方針を実現するためには、 FIA_AFL.1 (2)によりユーザー認証時の認証失敗時に、“パスワードが正しくない”旨のメッセージを表示して、パスワードの再入力を要求する。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者を識別するために、ユーザー認証が行われる。 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。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.RESTRICT を満たすことができる。
O.USER	O.USER は正当な TOE の利用者を識別し、正当な利用者に文書データの読み出しする機能を、一般利用者へ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、 FDP_ACC.1 FDP_ACF.1 によりユーザー認証を実施することで、許可された一般利用者のみに、オブジェクトの操作を許可する。 FIA_AFL.1 (2)によりユーザー認証時の認証失敗時に、“パスワードが正しくない”旨のメッセージを表示して、パスワードの再入力を要求する。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者を識別するために、ユーザー認証が行われる。 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。

対策方針	TOE セキュリティ機能要件根拠
	FMT_MSA.1 によりセキュリティ属性の問い合わせ、削除、作成を管理する。 FMT_SMR.1 (2) により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。 また、FPT_RVM.1 により、確実に呼び出され、バイパスされることはないため、本対策方針に関わる機能要件の確実な実施を保証される。 以上のセキュリティ機能要件により O.USER を満たすことができる。

8.2.2. IT 環境セキュリティ機能要件根拠

TOE の IT 環境が提供するセキュリティ機能要件はない。

8.2.3. 最小機能強度レベル根拠

本 ST は、MFP を対象としており、一般オフィスなどの組織の施設内で、内部ネットワークと公衆電話回線網に接続して利用され、TOE が想定する脅威に対するリスクのレベルは低い。

したがって、最小機能強度レベルが“SOF – 基本”であり、公開情報を利用した低レベルの攻撃者からの不正行為に、十分に対抗できる。

また、FIA_AFL.1 (1), FIA_AFL.1 (2), FIA_UAU.2, FIA_UAU.7 の機能強度レベルは、それぞれ“SOF – 基本”なので、TOE の必要とするセキュリティ機能強度を満たしている。

8.2.4. セキュリティ機能要件依存性

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、表 26 に記述する。

表 26 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 監査データ生成	FPT_STM.1	—
FAU_SAR.1 監査レビュー	FAU_GEN.1	—
FAU_SAR.2 限定監査レビュー	FAU_SAR.1	—
FAU_STG.1 保護された監査証跡格納	FAU_GEN.1	—
FAU_STG.4 監査データ損失の防止	FAU_STG.1	—
FCS_CKM.1 暗号鍵生成 (HDD 蓄積データ)	FCS_COP.1	FMT_MSA.2: 暗号鍵はシステム管理者により設定された TOE 設定データをもとに、TOE が自動的に 128 ビット固定鍵長の暗号鍵を生成するので、常にセキュアな値を保障する必要性がない。

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
		FCS_CKM.4: 暗号鍵は MFP の起動時に生成され、DRAM (揮発性メモリ) に格納される。 この暗号鍵は MFP 本体の電源を切断すると消滅するので、暗号鍵を破棄する必要性がない。
FCS_COP.1 暗号操作 (HDD 蓄積データ)	FCS_CKM.1	FMT_MSA.2: 暗号鍵はシステム管理者により設定された TOE 設定データをもとに、TOE が自動的に 128 ビット固定鍵長の暗号鍵を生成するので、常にセキュアな値を保障する必要性がない。
		FCS_CKM.4: 暗号鍵は MFP の起動時に生成され、DRAM (揮発性メモリ) に格納される。 この暗号鍵は MFP 本体の電源を切断すると消滅するので、暗号鍵を破棄する必要性がない。
FDP_ACC.1 サブセットアクセス制御	FDP_ACF.1	—
FDP_ACF.1 セキュリティ属性によるアクセス制御	FDP_ACC.1	—
FDP_IFC.1 サブセット情報フロー制御 (ファクス情報フロー)	FDP_IFF.1	—
FDP_IFF.1 単純セキュリティ属性 (ファクス情報フロー)	FDP_IFC.1 FMT_MSA.3	—
FDP_RIP.1 サブセット残存情報保護	なし	
FIA_AFL.1 (1) 認証失敗時の取り扱い (システム管理者)	FIA_UAU.2	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_AFL.1 (2) 認証失敗時の取り扱い (一般利用者)	FIA_UAU.2	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_UAU.2 アクション前の利用者認証	—	FIA_UID.1: FIA_UID.2 は FIA_UID.1 の上位階層の機能要件のため、FIA_UID.1 への依存性は満たされる。

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_UAU.7 保護されたフィードバック	—	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 識別のタイミング	なし	
FMT_MOF.1 セキュリティ機能のふるまいの管理	FMT_SMF.1 FMT_SMR.1 (1)	—
FMT_MSA.1 セキュリティ属性の管理	FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.3 静的属性初期化	FMT_MSA.1 FMT_SMR.1	—
FMT_MTD.1 TSF データの管理	FMT_SMF.1 FMT_SMR.1 (1)	—
FMT_SMF.1 管理機能の特定	なし	
FMT_SMR.1 (1) セキュリティ役割 (システム管理者)	FIA_UID.2	FIA_UID.1: FIA_UID.2 は FIA_UID.1 の上位階層の機能要件のため、FIA_UID.1 への依存性は満たされる。
FMT_SMR.1 (2) セキュリティ役割 (一般利用者)	FIA_UID.2	FIA_UID.1: FIA_UID.2 は FIA_UID.1 の上位階層の機能要件のため、FIA_UID.1 への依存性は満たされる。
FPT_RVM.1 TSP の非バイパス性	なし	
FPT_STM.1 高信頼タイムスタンプ	なし	
FTP_TRP.1 高信頼パス	なし	

8.2.5. セキュリティ機能要件相互補完性

TOE セキュリティ機能要件の相互作用の関係を表 27 に記述する。

表 27 セキュリティ機能要件の相互作用

機能要件コンポーネント		バイパス防止	非活性化防止
機能要件	要件名称		
FAU_GEN.1	監査データ生成	FPT_RVM.1	FMT_MOF.1
FAU_SAR.1	監査レビュー	FPT_RVM.1	FMT_MOF.1
FAU_SAR.2	限定監査レビュー	FPT_RVM.1	FMT_MOF.1

機能要件コンポーネント		バイパス防止	非活性化防止
機能要件	要件名称		
FAU_STG.1	保護された監査証跡格納	FPT_RVM.1	FMT_MOF.1
FAU_STG.4	監査データ損失の防止	FPT_RVM.1	FMT_MOF.1
FCS_CKM.1	暗号鍵生成 (HDD 蓄積データ)	FPT_RVM.1	FMT_MOF.1
FCS_COP.1	暗号操作 (HDD 蓄積データ)	FPT_RVM.1	FMT_MOF.1
FDP_ACC.1	サブセットアクセス制御	FPT_RVM.1	FMT_MOF.1
FDP_ACF.1	セキュリティ属性による アクセス制御	FPT_RVM.1	FMT_MOF.1
FDP_IFC.1	サブセット情報フロー制御 (ファクス情報フロー)	FPT_RVM.1	FMT_MOF.1
FDP_IFF.1	単純セキュリティ属性 (ファクス情報フロー)	FPT_RVM.1	FMT_MOF.1
FDP_RIP.1	サブセット残存情報保護	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1 (1)	認証失敗時の取り扱い (システム管理者認証)	FPT_RVM.1	—
FIA_AFL.1 (2)	認証失敗時の取り扱い (ユーザー認証)	FPT_RVM.1	—
FIA_UAU.2	アクション前の利用者認証	FPT_RVM.1	—
FIA_UAU.7	保護された 認証フィードバック	FPT_RVM.1	—
FIA_UID.2	識別のタイミング	FPT_RVM.1	—
FMT_MOF.1	セキュリティ機能の ふるまいの管理	—	—
FMT_MSA.1	セキュリティ属性の管理	FPT_RVM.1	—
FMT_MSA.3	静的属性初期化	FPT_RVM.1	—
FMT_MTD.1	TSF データの管理	FPT_RVM.1	—
FMT_SMF.1	管理機能の特定	—	—
FMT_SMR.1 (1)	セキュリティ役割	—	—
FMT_SMR.1 (2)	セキュリティ役割	—	—
FPT_RVM.1	TSP の非バイパス性	—	—
FPT_STM.1	高信頼タイムスタンプ	FPT_RVM.1	FMT_MOF.1
FTP_TRP.1	高信頼パス	FPT_RVM.1	FMT_MOF.1

8.2.5.1. バイパス防止

表 27 セキュリティ機能要件の相互作用で定義した、各セキュリティ機能要件に対するバイパス防止根拠を、表 28 に記述する。

表 28 セキュリティ機能要件のバイパス防止根拠

機能要件	機能要件コンポーネントのバイパス防止根拠
FPT_RVM.1	
FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FAU_STG.1 FAU_STG.4 FPT_STM.1	これらのセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、またシステム管理者の設定により、監査対象イベントが発生した時は、常にタイムスタンプと共に監査ログファイルへ記録される構造を築いているため、監査ログ機能を迂回することは出来ず、非バイパス性を保証する。
FCS_CKM.1 FCS_COP.1	これらのセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、またシステム管理者の設定により、常に実行される構造を築いているため、暗号鍵生成、および暗号操作を迂回することは出来ず、非バイパス性を保証する。
FDP_ACC.1 FDP_ACF.1 FIA_AFL.1 (1) FIA_AFL.1 (2) FIA_UAU.2 FIA_UAU.7 FIA_UID.2	これらのセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、ユーザー認証が必要な機能へアクセスする時は、必ずシステム管理者 ID 認証が実行されるため、アクション前の利用者識別、アクション前の利用者認証、保護された認証フィードバックを迂回することは出来ず、非バイパス性を保証する。 システム管理者の認証時は、認証失敗時のアクセス拒否回数に達して、認証拒否状態になると、この認証拒否状態を解除する機能は存在せず、電源切断/投入以外の他の操作は受け付けない。 一般利用者の認証時は、エラーメッセージを表示してユーザー認証を迂回することは出来ない。 さらにユーザー認証失敗時の失敗状態を解除する機能は存在しないため、ユーザー認証を迂回することは出来ず、非バイパス性を保証する。
FDP_IFC.1 FDP_IFF.1	これらのセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能である。 公衆電話回線網から内部ネットワークに、いかなる時も公衆電話回線データを受け渡さない構造を築いているために迂回することは出来ず、非バイパス性を保証する。
FTP_TRP.1	このセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、またシステム管理者の設定により、常に実行される構造を築いている。 また TOE とリモート間のデータ通信において、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータや TOE 設定データを盗聴より保護するように設定されているために迂回することは出来ず、非バイパス性を保証する。
FDP_RIP.1	このセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、またシステム管理者の設定により、常に実行される構造を築いている。 また電源 OFF などにより上書き消去処理が中断した場合は、電源 ON 時に上書き消去処理を再実行する仕組みを築いているため、迂回することは出来ず、

機能要件	機能要件コンポーネントのバイパス防止根拠
	非バイパス性を保証する。
FMT_MTD.1	これらのセキュリティ機能要件は、バイパス手段を有しないソフトウエアで構成されており、別のソフトウエアやモジュールへの置換は不可能であり、TSF データへアクセスする時は、必ずシステム管理者認証を経る必要があり、迂回することは出来ず、非バイパス性を保証する。

8.2.5.2. 非活性化防止

表 27 セキュリティ機能要件の相互作用で定義した、各セキュリティ機能要件に対する非活性化防止根拠を、表 29 に記述する。

表 29 セキュリティ機能要件の非活性化防止根拠

機能要件	機能要件コンポーネントの非活性化防止根拠
FMT_MOF.1	
FAU_GEN.1, FAU_SAR.1 FAU_SAR.2, FAU_STG.1 FAU_STG.4, FCS_CKM.1 FCS_COP.1, FDP_ACC.1 FDP_ACF.1 FDP_RIP.1 FPT_STM.1	下記の TOE セキュリティ機能のふるまいは、FMT_MOF.1 により許可されたシステム管理者のみに制限されており、システム管理者以外の一般利用者による非活性化行為から保護されていることを保証する。 • 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暗号化機能 (TSF_CIPHER) • システム管理者セキュリティ管理機能 (TSF_FMT) • カストマーエンジニア操作制限機能 (TSF_CE_LIMIT) • セキュリティ監査ログ機能 (TSF_FAU) • 内部ネットワークデータ保護機能 (TSF_NET_PROTECT) • ユーザー認証機能 (TSF_USER_AUTH)

8.2.5.3. 干渉

本 TOE は、公衆電話回線網と接続されているが、ファクスフローセキュリティ機能により、いかなる場合においても外部からのアクセスを拒否しているため不正なオブジェクトは存在しえないことと、ファクス以外のインタフェースからもシステム管理者のみに、セキュリティ機能のふるまいの管理を許可しており、不正なプログラムおよびオブジェクトは存在しないため、アクセス制御の必要はなく、TOE セキュリティ機能が破壊されることは無い。

8.2.5.4. 無効化の検出

各セキュリティ機能に対し、表 9 に示す監査対象事象に対し監査ログが生成される。これによりセキュリティ機能の動作に対する事後分析を可能とするとともに重要度に応じたセキュリティ侵害の可能性を検知し通知することができる。

8.2.6. セキュリティ機能要件間一貫性根拠

TOE セキュリティ機能要件のいくつかは、セキュリティ管理機能を必要とする。 [CC パート 2] では、各機能要件コンポーネントに予見される管理アクティビティを、各コンポーネントの管理要件として割り当てている。 すべての機能要件コンポーネントについて、そのコンポーネントが必要とする管理機能を表 30 に記述する。

“管理機能の特定”コンポーネントの FMT_SMF.1 で定義したセキュリティ管理機能と、表 30 で定義した管理機能と合致しているため、TOE セキュリティ機能要件は、セキュリティ管理機能に関して、内部的に一貫している。

表 30 TOE セキュリティ機能の管理項目

機能要件コンポーネント		コンポーネントで必要な管理機能
機能要件	要件名称	
FAU_GEN.1	監査データ生成	監査ログデータの管理
FAU_SAR.1	監査レビュー	—
FAU_SAR.2	限定監査レビュー	—
FAU_STG.1	保護された監査証跡格納	—
FAU_STG.4	監査データ損失の防止	—
FCS_CKM.1	暗号鍵生成 (HDD 蓄積データ)	暗号化キーデータの管理
FCS_COP.1	暗号操作 (HDD 蓄積データ)	—
FDP_ACC.1	サブセットアクセス制御	許可されたシステム管理者 ID の管理
FDP_ACF.1	セキュリティ属性による アクセス制御	許可されたシステム管理者 ID の管理
FDP_IFC.1	サブセット情報フロー制御 (ファクス情報フロー)	—
FDP_IFF.1	単純セキュリティ属性 (ファクス情報フロー)	—
FDP_RIP.1	サブセット残存情報保護	内部ハードディスク装置に蓄積される利用済み文書データの管理
FIA_AFL.1 (1)	認証失敗時の取り扱い (システム管理者認証)	認証失敗回数データの管理
FIA_AFL.1 (2)	認証失敗時の取り扱い (ユーザー認証)	—
FIA_UAU.2	アクション前の利用者認証	• システム管理者 ID の管理 • システム管理者パスワードデータの管理
FIA_UAU.7	保護された 認証フィードバック	—
FIA_UID.2	識別のタイミング	—

機能要件コンポーネント		コンポーネントで必要な管理機能
機能要件	要件名称	
FMT_MOF.1	セキュリティ機能の ふるまいの管理	下記の機能設定の管理 • 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暗号化機能 (TSF_CIPHER) • システム管理者セキュリティ管理機能 (TSF_FMT) • カストマーエンジニア操作制限機能 (TSF_CE_LIMIT) • セキュリティ監査ログ機能 (TSF_FAU) • 内部ネットワークデータ保護機能 (TSF_NET_PROTECT) • ユーザー認証機能 (TSF_USER_AUTH)
FMT_MSA.1	セキュリティ属性の管理	• 識別子の管理
FMT_MSA.3	静的属性初期化	• 適切なデフォルト値の管理
FMT_MTD.1	TSF データの管理	• TSF データの設定の管理
FMT_SMF.1	管理機能の特定	—
FMT_SMR.1 (1)	セキュリティ役割 (システム管理者)	—
FMT_SMR.1 (2)	セキュリティ役割 (一般利用者)	—
FPT_RVM.1	TSP の非バイパス性	—
FPT_STM.1	高信頼タイムスタンプ	日付と時刻データの管理
FTP_TRP.1	高信頼パス	—

8.2.7. セキュリティ保証要件根拠

本 TOE は MFP である、商用の製品である。 脅威は低レベルの攻撃力を持つ攻撃者による、操作パネルおよび Web ブラウザ、ネットワークスキャナーユーティリティから TOE の外部インタフェースを使用した攻撃、内部ネットワーク上に存在するデータの盗聴や改ざん、市販ツール等の接続による内部ハードディスク装置の情報読み出しである。

このため TOE は商用として十分である EAL2 を保証レベルとしている。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能要件根拠

6.1 章の表 19 TOE セキュリティ機能要件とセキュリティ機能の関係で定義した、各 TOE セキュリティ機能要件が、セキュリティ機能により実現されている根拠を、表 31 に記述する。

表 31 TOE セキュリティ機能要件とセキュリティ機能の対応根拠

機能要件	セキュリティ機能の対応根拠
FAU_GEN.1	TSF_FAU は、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。
FAU_SAR.1	TSF_FAU は、監査ログ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。
FAU_SAR.2	TSF_FAU は、監査ログの読み出しを、認証されたシステム管理者のみに限定する。
FAU_STG.1	TSF_FAU は、監査ログの不正な改ざんや改変から保護されている。
FAU_STG.4	TSF_FAU は、監査ログが満杯になった時、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。
FCS_CKM.1	TSF_CIPHER により、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 128 ビットの暗号鍵生成を行う。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。
FCS_COP.1	TSF_CIPHER により、TOE は自動生成された暗号鍵を使用して、内部ハードディスク装置に蓄積される文書データやセキュリティ監査ログデータを暗号化、および複合化する能力を持っている。
FDP_ACC.1 FDP_ACF.1	TSF_USER_AUTH により、ツールモードへアクセスする前に、システム管理者のユーザー認証を実施する。 TSF_USER_AUTH により、親展ボックスや蓄積プリントへアクセスする前に、一般利用者のユーザー認証を実施する。 TSF_FMT により、ツールモードへのアクセスを、認証されたシステム管理者のみに限定する。
FDP_IFC.1 FDP_IFF.1	TSF_FAX_FLOW の、公衆電話回線網から内部ネットワークに公衆電話回線データを受け渡さないので、公衆電話回線受信が受信した公衆回線データは内部ネットワーク送信に渡らない。
FDP_RIP.1	TSF_IOW により、TOE は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ファイルを上書き消去する。 上書き消去の制御として、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。 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) であり、データを再生しようとする低レベルの攻撃力に対して十分に対抗できるため、妥当な回数である。
FIA_AFL.1 (1)	TSF_USER_AUTH により、ツールモードへアクセスする前に、システム管理者のユーザー認証を行うが、認証時の認証失敗対応機能を提供している。 シス

機能要件	セキュリティ機能の対応根拠
	テム管理者 ID 認証失敗によるアクセス拒否回数で設定されている回数分の連続失敗で、電源切断/投入以外の他の操作は受け付けなくなる。
FIA_AFL.1 (2)	TSF_USER_AUTH により、MFP の機能を使用する前に、一般利用者のユーザー認証を行うが、正当な一般利用者が設定したパスワードと一致しない場合、"パスワードが正しくない"旨のメッセージを表示してパスワードの再入力を要求する。
FIA_UAU.2	TSF_USER_AUTH により、TOE はシステム管理者の操作パネル、およびシステム管理者や一般利用者の Web ブラウザからの操作を許可する前に、パスワードを入力させて、入力されたパスワードが、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。 本認証と識別 (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。
FIA_UAU.7	TSF_USER_AUTH により、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。
FIA_UID.2	TSF_USER_AUTH により、TOE はシステム管理者の操作パネル、およびシステム管理者や一般利用者の Web ブラウザからの操作を許可する前に、ユーザーID を入力させて、入力されたユーザーID が、TOE 設定に登録されているユーザーID 情報と一致することを検証する。 本識別と認証 (FIA_UAU.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。
FMT_MOF.1	TSF_FMT、TSF_CE_LIMIT により、認証されたシステム管理者に、TOE 設定データ設定インタフェースを許可する。 この機能により TOE 設定データの変更は、システム管理者のみに限定される。
FMT_MSA.1	TSF_FMT により、TOE はシステム管理者のみに一般利用者識別子、共用親展ボックスに対応する識別子の操作を限定する。 TSF_USER_AUTH により個別親展ボックス、蓄積プリントに対応する識別子の操作を認証された利用者に許可する。
FMT_MSA.3	TSF_FMT により、TOE は適切なデフォルト値を提供する。
FMT_MTD.1	TSF_FMT、TSF_CE_LIMIT により、TOE は認証されたシステム管理者のみに TOE 設定データの変更を限定する。
FMT_SMF.1	TSF_FMT により、TOE は認証されたシステム管理者のみに、TOE 設定データの変更を限定する。
FMT_SMR.1 (1)	TSF_FMT により、システム管理者の役割を維持し、その役割をシステム管理者に関連付けている。
FMT_SMR.1 (2)	TSF_USER_AUTH により、一般利用者の役割を維持し、その役割を正当な一般利用者に関連付けている。
FPT_RVM.1	全ての TOE セキュリティ機能は、バイパス手段を有しない独自のソフトウエアで構成されており、確実に動作する構成になっている。
FPT_STM.1	TSF_FAU により、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。

機能要件	セキュリティ機能の対応根拠
FTP_TRP.1	TSF_NET_PROT により、TOE とリモート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る、文書データ、、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。 この高信頼パスは、他の通信パス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。

8.3.2. セキュリティ機能強度根拠

本 TOE において、確率的または順列メカニズムに基づくセキュリティ機能は、ユーザー認証機能（TSF_USER_AUTH）の ID パスワード方式である。 これらのセキュリティ機能強度は、6.2 章において“SOF – 基本”を指定している。 またこの TOE の最小機能強度レベルは、5.1.8 章においても“SOF – 基本”を指定している。 したがって両レベルは一貫している。

8.3.3. セキュリティ保証手段根拠

セキュリティ保証要件と保証手段の対応を、表 32 に記述する。 また各保証手段がセキュリティ保証要件により保証されていることを、表 33 に記述する。 全ての保証手段は、EAL2 のセキュリティ保証要件を実現するために必要である。

表 32 セキュリティ保証要件と保証手段の対応

保証手段（識別子） / セキュリティ保証要件	TAS_CONFIG	TAS_CONFIG_LIST	TAS_DELIVERY	TAS_FUNC_SPEC	TAS_DISC_PAPER	TAS_HIGHLDESIGN	TAS_REPRESENT	TAS_GUIDANCE	TAS_TEST	TAS_VULNERABILITY
ACM_CAP.2	○	○								
ADO_DEL.1			○					○		
ADO_IGS.1			○					○		
ADV_FSP.1				○	○					
ADV_HLD.1						○				
ADV_RCR.1							○			
AGD_ADM.1								○		
AGD_USR.1								○		
ATE_COV.1									○	
ATE_FUN.1									○	
ATE_IND.2									○	
AVA_SOF.1										○
AVA_VLA.1										○

表 33 保証手段によるセキュリティ保証要件の十分性

保証手段 (識別子)	保証要件	セキュリティ保証要件の十分性
TAS_CONFIG TAS_CONFIG_LIST	「構成管理説明書」 「WorkCentre 7328 シリーズ TOE 構成要素リスト」	
	ACM_CAP.2	このドキュメントにより、TOE のバージョンが識別出来る命名規約や構成要素の一覧表、および各構成要素の一意の識別子という要件を満足することが出来る。
TAS_DELIVERY	「WorkCentre 7328 シリーズ配布・導入・運用手続き説明書」	
	ADO_DEL.1	このドキュメントにより、TOE の識別と輸送中の完全性や配布手続きの詳細、およびシステム管理者の TOE の確認方法という要件を満足することが出来る。
	ADO_IGS.1	このドキュメントにより、TOE の設置や起動手順と確認方法、および例外事象への対処という要件を満足することが出来る。
TAS_FUNC_SPEC TAS_DISC_PAPER	「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 機能仕様書」 「WorkCentre 7328/7335/7345Information Assurance Disclosure Paper」	
	ADV_FSP.1	このドキュメントにより、TOE セキュリティ機能と外部インタフェースの一貫した完全なる記述、および外部インタフェースの詳細記述という要件を満足することが出来る。
TAS_HIGHLDESIGN	「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 上位レベル設計書」	
	ADV_HLD.1	このドキュメントにより、TOE セキュリティ機能の構造に関する一貫した記述、およびサブシステム間のインタフェースの識別と記述や、セキュリティ機能を提供するサブシステム機能を提供するサブシステムの識別という要件を満足することが出来る。
TAS_REPRESENT	「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 対応分析書」	
	ADV_RCR.1	このドキュメントにより、TOE のセキュリティ機能の各レベル (ST の TOE 要約仕様 – 機能仕様 – 構造設計仕様) での、完全なる対応という要件を満足することが出来る。
TAS_GUIDANCE	「Xerox WorkCentre 7328/7335/7345 System Administrator's Guide、 Xerox WorkCentre 7328/7335/7345 Security Function Supplementary Guide」	
	ADO_DEL.1	このドキュメントにより、、TOE の識別と輸送中の完全性や配布手続きの詳細、およびシステム管理者の TOE の確認方法という要件を満足することが出来る。

保証手段（識別子）	保証要件	セキュリティ保証要件の十分性
	ADO_IGS.1	このドキュメントにより、TOE の設置や起動手順と確認方法、および例外事象への対処という要件を満足することが出来る。
	AGD_ADM.1	このドキュメントにより、システム管理者が利用可能な管理機能とインタフェースの記述やシステム管理者の責任や行為についての前提条件、および警告メッセージに対する対策方法という要件を満足することが出来る。
	AGD_USR.1	このドキュメントにより、一般利用者が利用可能なセキュリティ機能とインタフェースの記述や一般利用者の責任や行為についての前提条件、および警告メッセージに対する対策方法という要件を満足することが出来る。
TAS_TEST	「WorkCentre 7328 シリーズテスト計画書兼報告書」	
	ATE_COV.1	このドキュメントにより、すべての TOE セキュリティ機能が、機能仕様通りに動作することを確認するという要件を満足することが出来る。
	ATE_FUN.1	このドキュメントにより、すべての TOE セキュリティ機能の実行が、仕様通りであることを確認するという要件を満足することが出来る。
	ATE_IND.2	このドキュメントにより、TOE セキュリティ機能のテスト環境の再現やテスト資材の提供という要件を満足することが出来る。
TAS_VULNERABILITY	「WorkCentre 7328 シリーズ、DocuCentre-II 3005 シリーズ、DocuCentre-II C3000 シリーズ 脆弱性分析書」	
	AVA_SOF.1	このドキュメントにより、TOE のセキュリティ強度の十分性を満足することが出来る。
	AVA_VLA.1	このドキュメントにより、TOE の識別された脆弱性が想定する環境で悪用されないことの確認要件を満足することが出来る。

5.2 章の表 18 EAL2 保証要件で定義したように、EAL2 で必要なすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。 また保証手段によって、本 ST で規定した TOE セキュリティ保証要件が要求する証拠を網羅している。 したがって EAL2 における TOE セキュリティ保証要件が要求している証拠に合致している。

8.4. PP 主張根拠

適合を主張する PP はない。