Fuji Xerox
ApeosPort-Ⅱ 7000/6000 Series
Controller Software for Asia Pacific
セキュリティターゲット

Version 1.0.9

FUJI Xerox

― 更新履歴 ―

No.	更新日	バージョン	更新内容
1	2008 年 4 月 4 日	V 1.0.0	初版
2	2008 年 4 月 22 日	V 1.0.1	誤記修正
3	2008 年 5 月 30 日	V 1.0.2	指摘事項修正
4	2008 年 6 月 11 日	V 1.0.3	指摘事項修正
5	2008 年 6 月 18 日	V 1.0.4	指摘事項修正
6	2008 年 6 月 25 日	V 1.0.5	指摘事項修正
7	2008 年 7 月 1 日	V 1.0.6	指摘事項修正、ROM バージョン更新
8	2008 年 7 月 10 日	V 1.0.7	指摘事項修正
9	2008 年 7 月 22 日	V 1.0.8	指摘事項修正
10	2008 年 9 月 26 日	V 1.0.9	指摘事項修正
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

－ 目次 －

－ 図表目次 －

1. ST 概説

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

本節では ST の識別情報を記述する。

タイトル:	Fuji Xerox ApeosPort-Ⅱ7000/6000 Series Controller Software for Asia Pacific セキュリティターゲット
バージョン:	V 1.0.9
発行日:	2008 年 9 月 26 日
作成者:	富士ゼロックス株式会社

1.2. TOE 参照

本節では TOE の識別情報を記述する。

Fuji Xerox ApeosPort-Ⅱ7000、Fuji Xerox ApeosPort-Ⅱ6000 の 2 機種とも同じ TOE が動作し、下記 TOE 名とバージョンで識別する。

TOE 名:	Fuji Xerox ApeosPort-Ⅱ7000/6000 Series Controller Software for Asia Pacific
TOE のバージョン:	Controller ROM Ver. 1.180.7
開発者:	富士ゼロックス株式会社

1.3. TOE 概要

1.3.1. TOE 種別および主要セキュリティ機能

1.3.1.1. 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、スキャナー機能を有する MFP のコントローラソフトウェアである。 TOE は、コントローラボード上のコントローラ ROM に格納されており、MFP 全体の制御および利用済み文書データと TOE 設定データを脅威から保護するファームウエア製品である。

1.3.1.2. 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

機能種別（標準/オプション）	左記種別により TOE が提供可能となる機能
標準機能	・ CWIS 機能 ・ システム管理者セキュリティ管理機能 ・ 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
オプション （データセキュリティキット）	・ 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 ・ カストマーエンジニア操作制限機能
オプション （TOE 対象外のファクスボード）	・ ファクス機能 ・ D-FAX 機能、iFAX 機能 ・ ファクスフローセキュリティ機能

- プリンター機能、スキャナー機能、D-FAX 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ー、スキャナードライバー、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いることが必要である。
- オプションのデータセキュリティキットはセキュリティ機能実現のために必須である。

1.3.1.3. TOE の使用法と主要セキュリティ機能

TOE の主な使用法を以下に示す。

- コピー機能により、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 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。
- プリンター機能により、一般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、MFP 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一般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 MFP 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、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
- ネットワークスキャン機能により、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。
- ファクス機能により、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。

- iFAX 機能により、公衆電話回線網を使用することなく、インターネットを経由してファクスの送受信を行う。
- D-FAX 機能により、データをプリントジョブとして MFP に送り、紙に印刷すること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。

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）
  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。
- ハードディスク蓄積データ暗号化機能（TSF_CIPHER）
  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に、ハードディスク装置に文書データを蓄積する際に、文書データの暗号化を行う機能である。
- システム管理者セキュリティ管理機能（TSF_FMT）
  操作パネルまたはシステム管理者クライアントから、システム管理者の識別および認証を行い、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。
- 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が TOE のセキュリティ機能に関する設定の変更をできなくするシステム管理者の設定機能である。
- ファクスフローセキュリティ機能（TSF_FAX_FLOW）
  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を防ぐ機能である。

1.3.2. TOE 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。

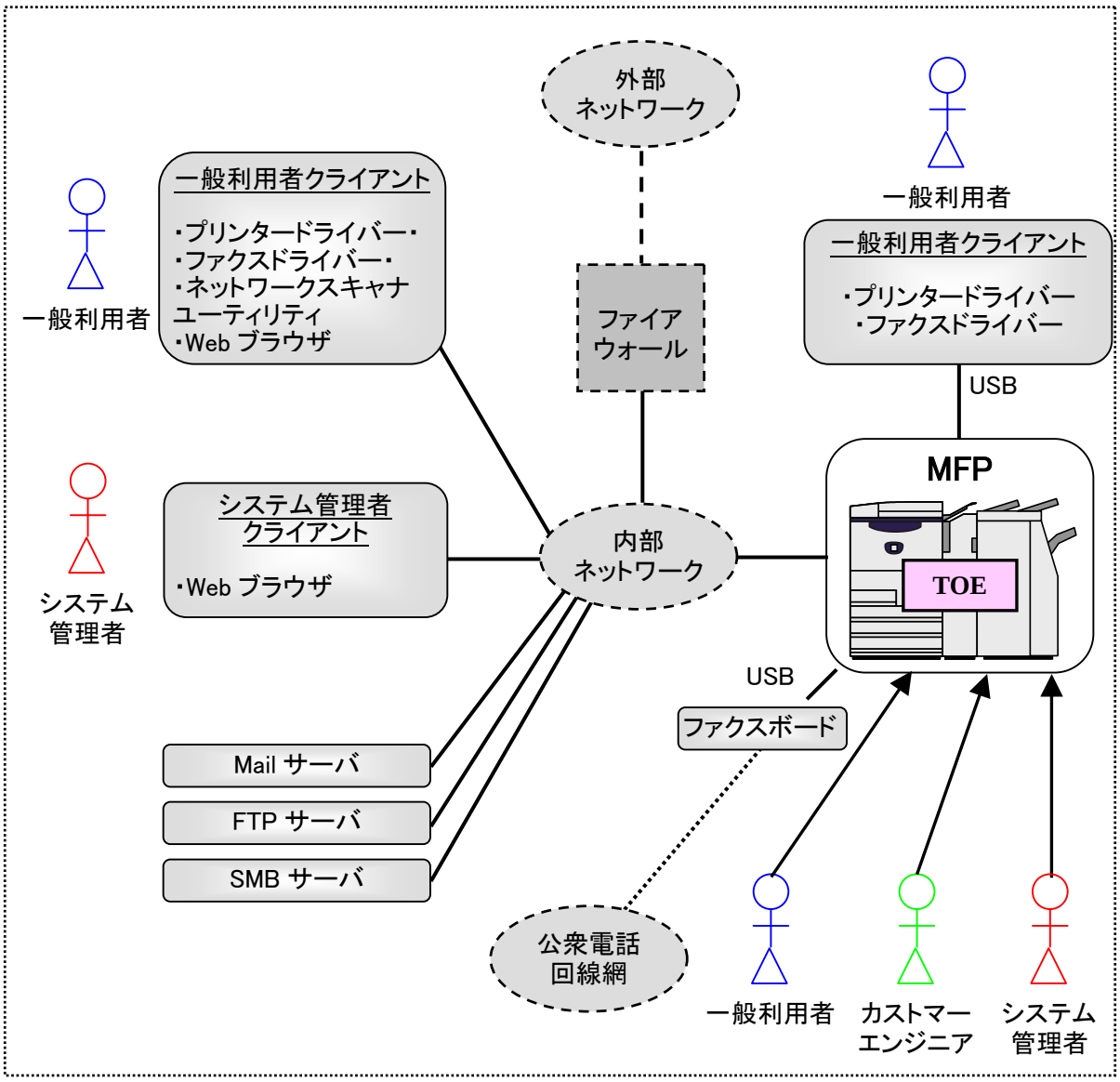

図 1 TOE の想定する利用環境

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成

図-1 に示す利用環境の中で TOE はコントローラソフトウェアであり、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 MFP 本体

MFP(ApeosPort-Ⅱ7000/6000 Series)は操作パネル、ADF、IIT、IOT、コントローラボード、ファクスボード(オプション)から構成され、MFP 機能を提供するためのユーザーインターフェイス、スキャナー機能、プリンター機能、コピー機能のためのハードウェアを有する。

② 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 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 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 でローカル接続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。

③ 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。

④ Mail サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFP はメールプロトコルを用いて、Mail サーバと文書データの送受信を行う。

⑤ FTP サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFP は FTP プロトコルを用いて、FTP サーバに文書データの送信を行う。

⑥ SMB サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFP は SMB プロトコルを用いて、SMB サーバに文書データの送信を行う。

⑦ 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。

また不正なアクセスから、内部ネットワークの各機器を保護するために、外部ネットワークと接続する場合は、ファイアウォールを介して各機器を接続しなければならない。

1.4. TOE 記述

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ついて記述する。

1.4.1. TOE 関連の利用者役割

本 ST で、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 が提供するコピー機能、プリンター機能、ファクス機能等の TOE 機能の利用者。

関連者	内容説明
システム管理者	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/更新を行う。
カストマーエンジニア	カストマーエンジニアは、操作パネルからカストマーエンジニア専用のインタフェースを使用して TOE の機器動作設定を行う。

1.4.2. 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。

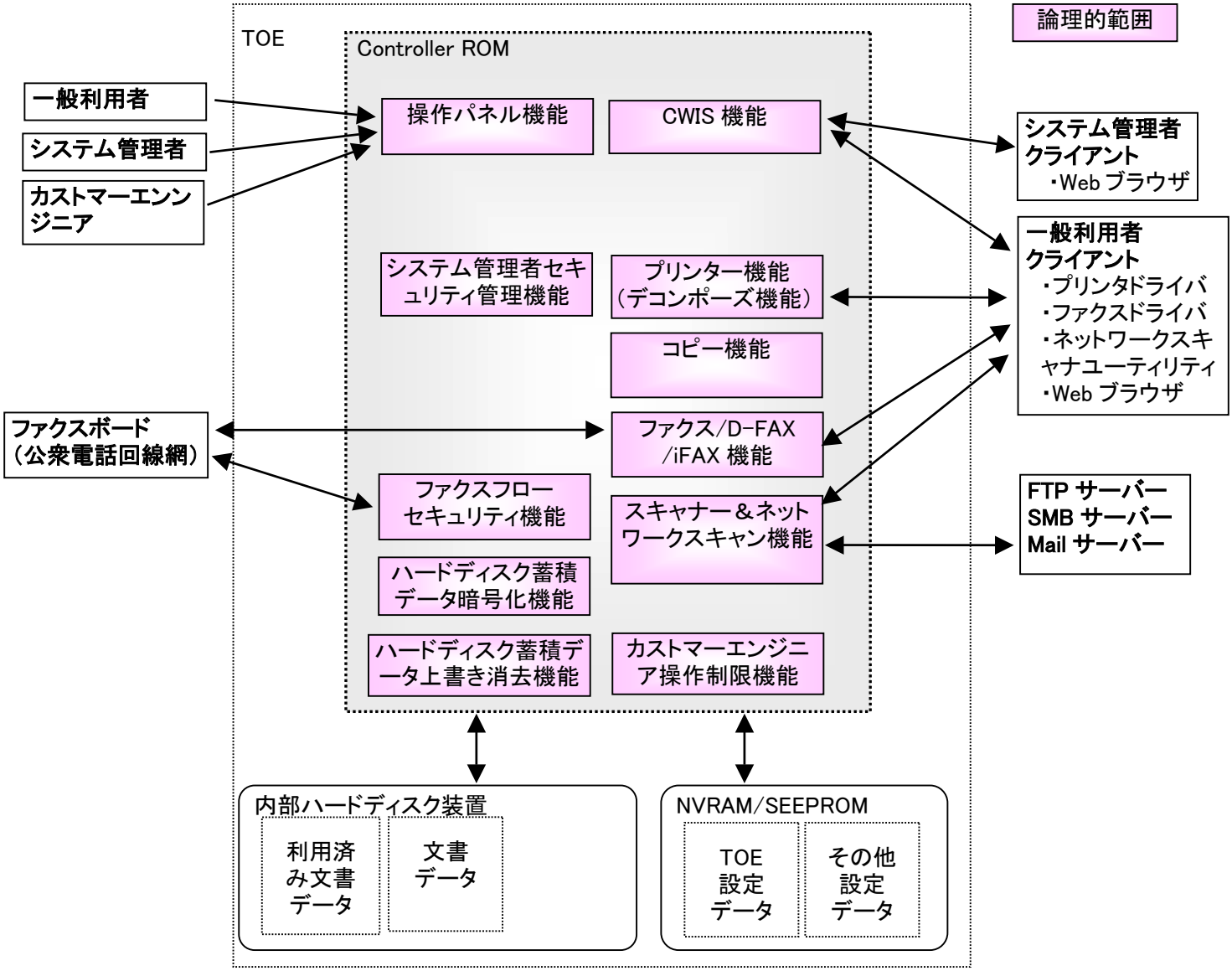

図 2 MFP 内の各ユニットと TOE の論理的範囲

1.4.2.1. TOE が提供する基本機能

TOE は一般利用者に対して、下記 表 3 のように操作パネル機能、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、ファクス機能、i FAX 機能、D-FAX 機能および CWIS 機能を提供する。

表 3 TOE の基本機能

機能	概要
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 MFP 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イス機能である。
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。 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。
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。
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、Mail サーバ、SMB サーバへ転送する機能である。
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。
D-FAX 機能、i FAX 機能	D-FAX 機能は、一般利用者が一般利用者クライアントから出力先としてファクス送信指示をすると、ファッ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。 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。
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、スキャナー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。

1.4.2.2. TOE が提供するセキュリティ機能

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（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、ファクス機能、i FAX 機能および D-FAX 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。

（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蓄積される文書データは、利用が終了するまでは内部ハードディスク装置内に保存され、利用が終了すると削除される。ただし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、ファクス機能、i FAX 機能および D-FAX 機能動作時の内部ハードディスク装置に文書データを蓄積する際に、文書データの暗号化を行う。

（3）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、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の有効/無効
・ハードディスク蓄積データ暗号化の有効/無効
・本体パネルからの認証時のパスワード使用の有効/無効
・システム管理者の ID とパスワード変更
・システム管理者 ID 認証失敗によるアクセス拒否の有効/無効と失敗回数
・カストマーエンジニア操作機能制限の有効/無効

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。

・システム管理者の ID とパスワード変更

・システム管理者 ID 認証失敗によるアクセス拒否の有効/無効と認証失敗回数

(4)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(3)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から、カストマーエンジニア操作機能制限の有効/無効の参照と設定を行う権限を許可する。

(5)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。

1.4.3. TOE の物理的範囲

本 TOE の物理的範囲はコントローラボードであり、図 3 に MFP 内の各ユニット構成と TOE の物理的範囲を記述する。

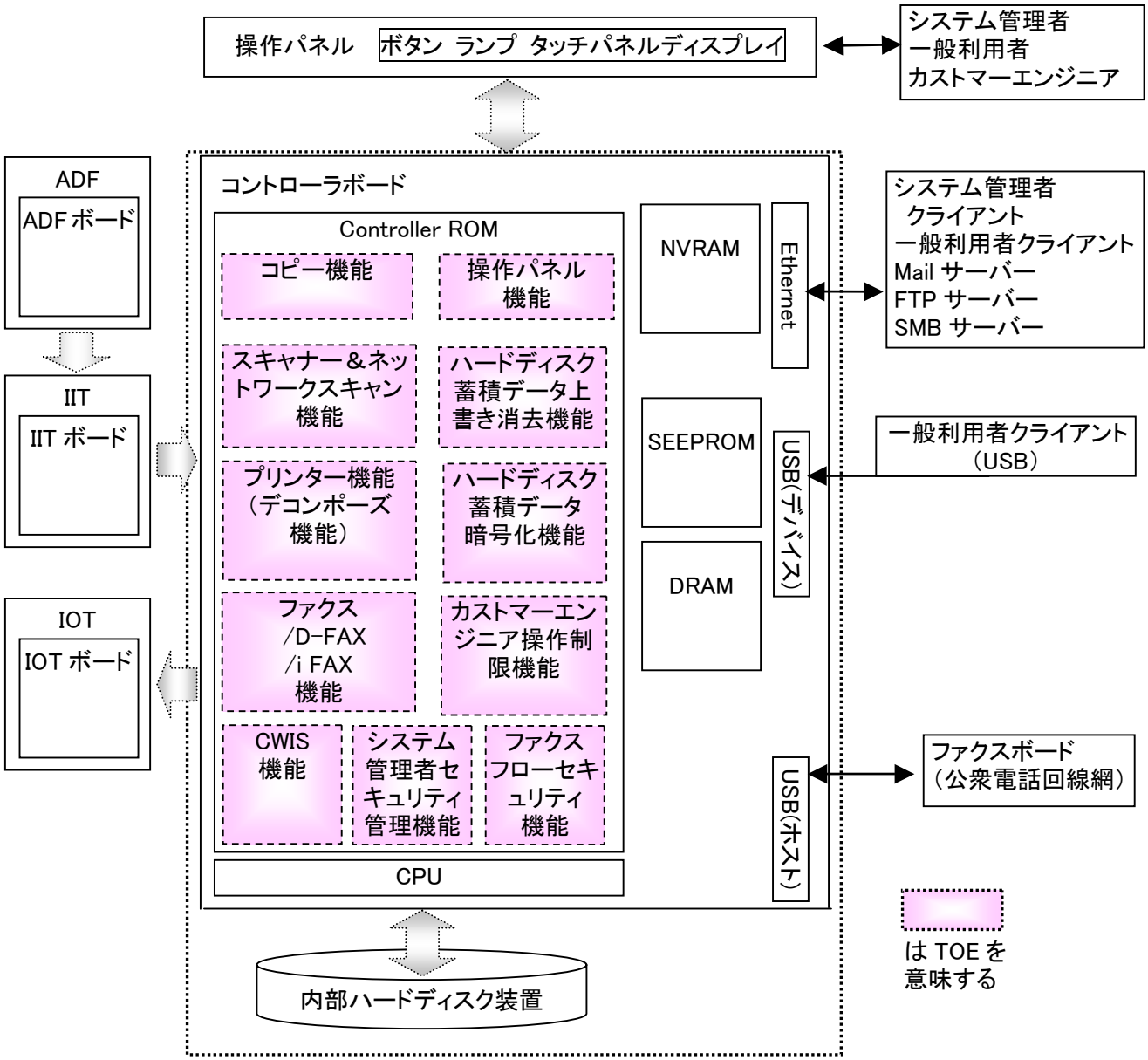

図 3 MFP 内の各ユニットと TOE の物理的範囲

MFP は、コントローラボード、操作パネルの回路基板ユニットおよび IIT、IOT 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、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）、ローカルインタフェース（USB）を持ち、IIT ボードや IOT ボードが接続されている。
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。
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。

1.4.4. ガイダンス

本 TOE を構成するガイダンス文書は以下のとおりである。
ApeosPort-Ⅱ 7000/6000 DocuCentre-Ⅱ7000/6000 Administrator Guide
ApeosPort-Ⅱ 7000/6000 Security Function Supplementary Guide

2. 適合主張

2.1. CC 適合主張

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

パート 1: 概説と一般モデル 2007 年 3 月 バージョン 3.1 翻訳第 1.2 版
パート 2: セキュリティ機能コンポーネント 2008 年 3 月 バージョン 3.1 翻訳第 2.0 版
パート 3: セキュリティ保証コンポーネント 2008 年 3 月 バージョン 3.1 翻訳第 2.0 版

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

2.2. PP 主張、パッケージ主張

2.2.1. PP 主張

本 ST が適合している PP はない。

2.2.2. パッケージ主張

EAL3 適合

2.2.3. 適合根拠

本 ST は PP 適合を主張していないので、PP 適合根拠はない。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威

3.1.1. TOE 資産

本 TOE が保護する資産は以下のとおりである(図 4)。

（1） 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。

（2） 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 4）。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。

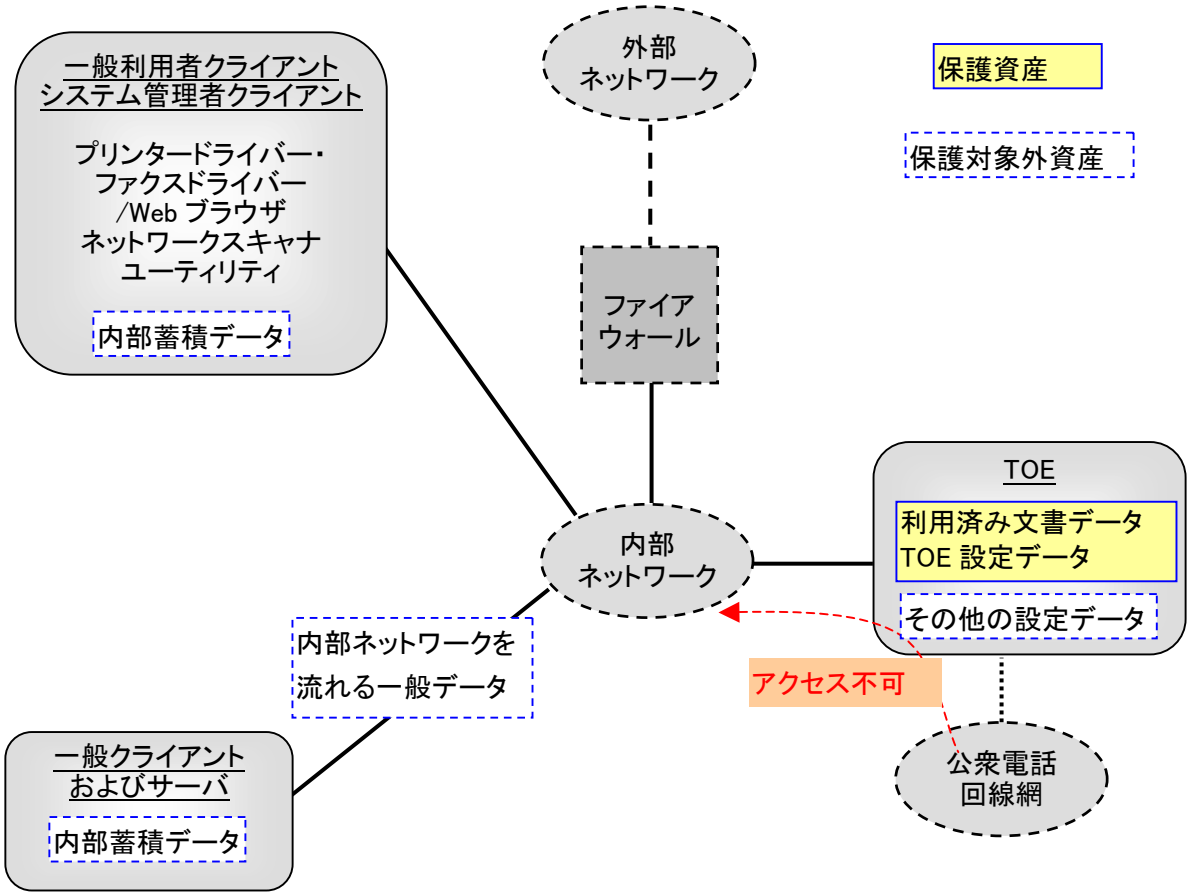

図 4 保護資産と保護対象外資産

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。

表 4 にコントローラボードの NVRAM および SEEPROM に記憶される TOE 設定データを記述する。

表 4 TOE 設定データ項目分類

TOE 設定データ項目分類（注）
本体パネルからの認証時のパスワード使用情報
システム管理者 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
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
カストマーエンジニア操作制限情報

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。

3.1.2. 脅威

本 TOE に対する脅威を表 5 に記述する。攻撃者は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。

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を読み出して漏洩させるかもしれない。
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設定の変更、または不正な読み出しを行うかもしれない。

3.2. 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
P.FAX_OPT	オーストラリア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。

3.3. 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 7 に記述する。

表 7 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:7 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 • 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
ネットワークの接続条件	
A.NET	• TOE が搭載された MFP を設置する内部ネットワークは盗聴されない環境を構成する。 • TOE が搭載された MFP を設置する内部ネットワークが外部ネットワークと接続される場合は、外部ネットワークから MFP へアクセスできない。

4. セキュリティ対策方針

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

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 8 に記述する。

表 8 TOE セキュリティ対策方針

セキュリティ対策方針（識別子）	詳細内容
O.CIPHER	本 TOE は、内部ハードディスク装置に蓄積されている利用済み文書データを取り出しても解析が出来ないように、ハードディスク上に蓄積されるデータを暗号化する。
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システム管理者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。

4.2. 運用環境の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を表 9 に記述する。

表 9 運用環境のセキュリティ対策方針

セキュリティ対策方針（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。 • 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：7 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
OE.FUNCTION	本 TOE を管理するシステム管理者は、下記の通りに TOE のセキュリティ機

セキュリティ対策方針（識別子）	詳細内容
	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
OE.NET	組織の責任者は、TOE が搭載された MFP を設置する内部ネットワークに盗聴されない環境を実現する機器を設置し、盗聴されないための適切な管理運用を行う。 組織の責任者は、外部ネットワークから TOE が搭載された MFP を設置する内部ネットワークへのアクセスを遮断するための機器を設置し、アクセスを遮断するよう適切に設定する。

4.3. セキュリティ対策方針根拠

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表 10 に示す。また各 TOE 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表 11 に記述する。

表 10 セキュリティ対策方針と対抗する脅威、組織セキュリティ方針及び前提条件

セキュリティ課題定義 / セキュリティ対策方針	A.ADMIN	A.SECMODE	A.NET	T.RECOVER	T.CONFDATA	P.FAX_OPT
O.CIPHER				○		
O.FAX_SEC						○
O.MANAGE					○	
O.RESIDUAL				○		
OE.ADMIN	○					
OE.AUTH		○			○	
OE.FUNCTION		○		○		
OE.NET			○			

表 11 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

セキュリティ課題定義	セキュリティ対策方針根拠
A.ADMIN	運用環境の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	運用環境の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、またカストマーエンジニア操作制限機能を有効にして運用する。 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」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利用済み文書データの復元を、不可能にする。 この対策方針により、A.SECMODE を実現できる。
A.NET	本条件は、MFP を設置する内部ネットワークでの盗聴行為、外部ネットワークから不特定多数の者による攻撃などが行われないことを想定している。 OE.NET は、内部ネットワークが盗聴されない環境を実現するための機器を設置する。MFP をクライアント PC 間の暗号化を行う等の措置を実施し、盗聴されないための適切な環境設定を行うことが想定されており、外部ネットワークから MFP へのアクセスを遮断するための機器を設置し、外部アクセスを遮断するよう適切に実施することが規定されている。 これらの対策方針により、A.NET を実現できる。
T.RECOVER	この脅威に対抗するには、運用環境の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」 利用済み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を 暗号化し、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、運用環境の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。

セキュリティ課題定義	セキュリティ対策方針根拠
	• 「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。 これらの対策方針により、T.CONFDATA 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

5. 拡張コンポーネント定義

5.1. 拡張コンポーネント

本 ST は CC パート 2 及び CC パート 3 に適合しており、拡張コンポーネントは定義しない。

6. セキュリティ要件

本章では、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
公衆電話回線受信	ファクス受信として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する。
公衆電話回線送信	ファクス送信として操作パネルやクライアント PC からの一般利用者の指示に従い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。
内部ネットワーク送信	内部ネットワーク内でネットワークスキャンや iFAX 受信のデータを宛先のクライアント PC へ送信する。
内部ネットワーク受信	内部ネットワーク内でクライアント PC からのプリントデータや D-FAX、iFAX 送信されて来たデータを受信する。

・ オブジェクト

名称	定義
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	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。

・ 操作

名称	定義
受け渡す	ファクスの公衆回線網から受信したデータをMFPが受け取る。
改変	本体パネルからの認証時のパスワード使用情報、システム管理者 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、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およびカストマーエンジニア操作制限情報の設定変更。

・ 情報

名称	定義
公衆回線データ	ファクスの公衆回線網を流れる送受信のデータ

・ セキュリティ属性

なし

・ 外部のエンティティ

名称	定義
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。

・ その他の用語

名称	定義
富士ゼロックス標準の FXOSENC 方式	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。
認証失敗によるアクセス拒否	システム管理者 ID 認証失敗が所定回数に達した時に、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、また Web ブラウザでは本体の電源の切断/投入まで認証操作を受け付けなくなる動作。
本体パネルからの認証時のパスワード使用情報	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。
システム管理者 ID 情報	TOE 設定データであり、システム管理者認証のための ID 情報。
システム管理者パスワード情報	TOE 設定データであり、システム管理者認証のためのパスワード情報
システム管理者認証失敗によるアクセス拒否情報	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
カストマーエンジニア操作制限情報	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。
ハードディスク蓄積データ暗号化情報	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。
ハードディスク蓄積データ上書き情報	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。
公衆電話回線、 公衆電話回線網	ファクス送信、受信のデータが流れる回線と構成される網。
システム管理者モード	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 セキュリティ機能の参照/更新といった設定の変更を行う動作モード。

6.1. 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。

6.1.1. クラス FCS: 暗号サポート

①FCS_CKM.1	暗号鍵生成
下位階層:	なし
依存性:	[FCS_CKM.2 暗号鍵配付、または FCS_COP.1 暗号操作] FCS_CKM.4 暗号鍵破棄
FCS_CKM.1.1	TSF は、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵を生成しなければならない。 [割付: 標準のリスト] *指定なし* [割付: 暗号鍵生成アルゴリズム] *富士ゼロックス標準の FXOSENC 方式* [割付: 暗号鍵長] *・128 ビット*
②FCS_COP.1	暗号操作
下位階層:	なし
依存性:	[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、 または FCS_CKM.1 暗号鍵生成] FCS_CKM.4 暗号鍵破棄
FCS_COP.1.1	TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。 [割付: 標準のリスト] *FIPS PUB 197* [割付: 暗号アルゴリズム] *・AES*

[割付: 暗号鍵長]
・*128 ビット*
[割付: 暗号操作のリスト]
・*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、内部ハードディスク装置から取り出される文書データの復号化*

6.1.2. クラス FDP: 利用者データ保護

①FDP_IFC.1　サブセット情報フロー制御
下位階層:　なし
依存性:　FDP_IFF.1 単純セキュリティ属性

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

[割付: SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト]
・*表 12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*

表 12 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*

[割付: 情報フロー制御 SFP]
・*ファクス情報フローSFP*

②FDP_IFF.1　単純セキュリティ属性
下位階層:　なし
依存性:　FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

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

[割付: 情報フロー制御 SFP]

・ファクス情報フローSFP
[割付：示されたSFP下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性]
・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、及び各々に対応する、セキュリティ属性はない

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

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

[割付：追加の情報フロー制御SFP規則]
・追加の情報フロー制御SFP規則はない

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

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

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

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

③FDP_RIP.1	サブセット情報保護
下位階層:	なし
依存性:	なし
FDP_RIP.1.1	TSF は、[割付: オブジェクトのリスト]のオブジェクト[選択: への資源の割当て、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: オブジェクトのリスト] ・*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* [選択: への資源の割当て、からの資源の割当て解除] ・*からの資源の割当て解除*

6.1.3. クラス FIA: 識別と認証

①FIA_AFL.1	認証失敗時の取り扱い
下位階層:	なし
依存性:	FIA_UAU.1 認証のタイミング
FIA_AFL.1.1	TSF は、[割付: 認証事象のリスト]に関して、[選択: [割付: 正の整数値]、[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]回の不成功認証試行が生じたときを検出しなければならない。 [割付: 認証事象のリスト] ・*システム管理者の認証* [選択: [割付: 正の整数値]、 [割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値] ・*[割付: 正の整数値]* [割付: 正の整数値] ・*5*
FIA_AFL.1.2	不成功の認証試行が定義した回数[選択:に達する、を上回った]とき、TSF は、[割付: アクションのリスト]をしなければならない。 [選択:に達する、を上回った]

・*に達する*

[割付: アクションのリスト]
・*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*

②FIA_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
依存性:	FIA_UID.1 識別のタイミング
FIA_UAU.2.1	TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。
③FIA_UAU.7	保護された認証フィードバック
下位階層:	なし
依存性:	FIA_UAU.1 認証のタイミング
FIA_UAU.7.1	TSF は、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。 [割付: フィードバックのリスト] ・*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*
④FIA_UID.2	アクション前の利用者識別
下位階層:	FIA_UID.1 識別のタイミング
依存性:	なし
FIA_UID.2.1	TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.4. クラス FMT:セキュリティ管理

①FMT_MOF.1	セキュリティ機能のふるまいの管理
下位階層:	なし
依存性:	FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定
FMT_MOF.1.1	TSF は、機能［割付: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：許可された識別された役割］に制限しなければならない。

［割付：機能のリスト］
・*表 13 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］
・*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*
［割付：許可された識別された役割］
・*システム管理者*

表 13 セキュリティ機能のリスト

TSF データ	ふるまい
本体パネルからの認証時のパスワード使用	*動作、停止*
システム管理者認証失敗によるアクセス拒否	*動作、停止、改変*
カストマーエンジニア操作制限機能	*動作、停止*
ハードディスク蓄積データ暗号化機能	*動作、停止*
ハードディスク蓄積データ上書き消去機能	*動作、停止、改変*

②FMT_MTD.1　TSF データの管理
下位階層：　なし
依存性：　FMT_SMR.1 セキュリティの役割
FMT_SMF.1　管理機能の特定

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

[割付：TSF データのリスト]
・*表 14 の TSF データのリスト*

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

[割付: 許可された識別された役割]
・*システム管理者*

表 14 TSF データのリスト

TSF データ	操作
本体パネルからの認証時のパスワード使用情報	*問い合わせ、改変*
システム管理者 ID 情報	*問い合わせ、改変*
システム管理者パスワード情報	*改変*
システム管理者認証失敗によるアクセス拒否情報	*問い合わせ、改変*
カストマーエンジニア操作制限情報	*問い合わせ、改変*
ハードディスク蓄積データ暗号化情報	*問い合わせ、改変*
ハードディスク蓄積データ上書き情報	*問い合わせ、改変*

③FMT_SMF.1　　管理機能の特定
下位階層:　　なし
依存性:　　なし

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

[割付: TSF によって提供される管理機能のリスト]
・*表 15 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 15 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
FCS_CKM.1	なし	-
FCS_COP.1	なし	*・ハードディスク蓄積データ暗号化情報の管理*
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て)が、TOEにおいて設定可能にされる。	*・ハードディスク蓄積データ上書き情報の管理*
FIA_AFL.1	・ 不成功の認証試行に対する閾値の管理	*・認証失敗によるアクセス拒否と認証失敗回数の管理*

	・ 認証失敗の事象においてとられるアクションの管理	
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。	*・本体パネルからの認証時のパスワード使用情報* *・システム管理者 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。	*・システム管理者 ID とパスワードの管理*
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	*・カストマーエンジニア操作制限情報の管理*
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。	*・カストマーエンジニア操作制限情報の管理*
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*

⑥FMT_SMR.1　　セキュリティの役割
下位階層:　　なし
依存性:　　FIA_UID.1 識別のタイミング

FMT_SMR.1.1　　TSF は、役割[割付: 許可された識別された役割]を維持しなければならない。
FMT_SMR.1.2　　TSF は、利用者を役割に関連付けなければならない。

[割付: 許可された識別された役割]
・システム管理者

6.2. セキュリティ保証要件

表 16 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 EAL3 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、EAL3 のコンポーネントを直接引用している。

表 16 EAL3 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 ADV:	開発	
ADV_ARC.1	セキュリティアーキテクチャ記述	ADV_FSP.1, ADV_TDS.1
ADV_FSP.3	完全な要約を伴う機能仕様	ADV_TDS.1
ADV_TDS.2	アーキテクチャ設計	ADV_FSP.3
クラス AGD:	ガイダンス文書	
AGD_OPE.1	利用者操作ガイダンス	ADV_FSP.1,
AGD_PRE.1	準備手続き	なし
クラス ALC:	ライフサイクルサポート	
ALC_CMC.3	許可の管理	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	実装表現の CM カバレージ	なし
ALC_DEL.1	配布手続き	なし
ALC_DVS.1	セキュリティ手段の識別	なし
ALC_LCD.1	開発者によるライフサイクルモデルの定義	なし
クラス ASE:	セキュリティターゲット評価	
ASE_CCL.1	適合主張	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
ASE_ECD.1	拡張コンポーネント定義	なし
ASE_INT.1	ST 概説	なし
ASE_OBJ.2	セキュリティ対策方針	ASE__SPD.1
ASE_REQ.2	導き出されたセキュリティ要件	ASE_OBJ.2, ASE_ECD.1
ASE_SPD.1	セキュリティ課題定義	なし
ASE_TSS.1	TOE 要約仕様	ASE_INT.1, ASE_REQ.1, ADV_FSP.1
クラス ATE:	テスト	
ATE_COV.2	カバレージの分析	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	テスト:基本設計	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
ATE_FUN.1	機能テスト	ATE_COV.1
ATE_IND.2	独立テスト – サンプル	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

保証要件	セキュリティ保証要件名称	依存性
クラス AVA:	脆弱性評定	
AVA_VAN.2	脆弱性分析	ADV_ARC.1,ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応を表 17 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表 18 に記述する。

表 17 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

セキュリティ対策方針 / セキュリティ機能要件	O.CIPHER	O.FAX_SEC	O.MANAGE	O.RESIDUAL
FCS_CKM.1	○			
FCS_COP.1	○			
FDP_IFC.1		○		
FDP_IFF.1		○		
FDP_RIP.1				○
FIA_AFL.1			○	
FIA_UAU.2			○	
FIA_UAU.7			○	
FIA_UID.2			○	
FMT_MOF.1			○	
FMT_MTD.1			○	
FMT_SMF.1			○	
FMT_SMR.1			○	

表 18 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.CIPHER	O.CIPHER は内部ハードディスク装置に蓄積されている利用済み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。

セキュリティ対策方針	セキュリティ機能要件根拠
	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 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、利用済み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、読み出し時に複合化される。 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.FAX_SEC	O.FAX_SEC は、公衆電話回線網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。 以上のセキュリティ機能要件により O.FAX_SEC を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システム管理者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、 FIA_AFL.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を識別するために、認証が行われる。 FIA_UAU.7 によりシステム管理者を識別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を識別するために、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 により 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、改変は、システム管理者だけに制限される。 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。 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。

セキュリティ対策方針	セキュリティ機能要件根拠
	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。 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。

6.3.2. 依存性の検証

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 19 に記述する。

表 19 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
FCS_CKM.1 暗号鍵生成 （HDD 蓄積データ）	FCS_COP.1	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	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_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: ファクス情報フローはセキュリティ属性が無いため、静的属性初期化が不要である。
FDP_RIP.1 サブセット残存情報保護	なし	
FIA_AFL.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_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。
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

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
		要件のため、FIA_UAU.1への依存性は満たされる。
FIA_UID.2 アクション前の利用者識別	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	—
FMT_MTD.1 TSF データの管理	FMT_SMF.1 FMT_SMR.1	—
FMT_SMF.1 管理機能の特定	なし	
FMT_SMR.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。

6.3.3. セキュリティ保証要件根拠

本 TOE はデジタル複合機である、商用の製品である。 低レベルの攻撃力を持つ攻撃者は、操作パネルおよびシステム管理者クライアントの Web ブラウザから TOE の外部インタフェースを使用した攻撃、または内部ハードディスク装置を取り出して、市販のツール等に接続して、物理的な手段として情報を読み出そうとすることである。
これらに対して本 TOE は安全性を確保するためのセキュリティ機能を提供する必要がある。

EAL3 は TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、及び開発環境や開発生産物の管理状況の評価)を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれるので妥当な選択であるといえる。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。

7.1. TOE セキュリティ機能

表 20 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。

表 20 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_FMT	TSF_CE_LIMIT	TSF_FAX_FLOW
FCS_CKM.1		○			
FCS_COP.1		○			
FDP_IFC.1					○
FDP_IFF.1					○
FDP_RIP.1	○				
FIA_AFL.1			○		
FIA_UAU.2			○		
FIA_UAU.7			○		
FIA_UID.2			○		
FMT_MOF.1			○	○	
FMT_MTD.1			○	○	
FMT_SMF.1			○	○	
FMT_SMR.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、ファクス機能、i FAX 機能および D-FAX 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。

（1） FDP_RIP.1 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、ファクス機能、i FAX 機能および D-FAX 機能動作時の内部ハードディスク装置に文書データを蓄積する際に、文書データの暗号化を行う。

(1) FCS_CKM.1 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 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）。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 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 128 ビット長の暗号鍵と FIPS PUBS 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 128 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. 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） FIA_AFL.1 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。システム管理者 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 MFP 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_UAU.2 アクション前の利用者認証
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クライアントの Web ブラウザを通じて CWIS 機能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。

（3） FIA_UAU.7 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。

（4） FIA_UID.2 アクション前の利用者識別
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クライアントの Web ブラウザを通じて CWIS 機能の操作を許可する前に、システム管理者 ID を入力させて、入力されたシステム管理者 ID が、TOE 設定に登録されているシステム管理者 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。

（5） FMT_MOF.1 セキュリティ機能のふるまいの管理
FMT_MTD.1 TSF データの管理
FMT_SMF.1 管理機能の特定
TOE は認証されたシステム管理者のみに、下記の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 ID の設定を参照し、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
・ システム管理者 ID の設定を参照し、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、認証失敗回数の設定を行う

（6） FMT_SMR.1 セキュリティ役割
TOE は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。

7.1.4. 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のなりすましによる設定変更が出来なくなる。

（1）FMT_MOF.1 セキュリティ機能のふるまいの管理
FMT_MTD.1 TSF データの管理
FMT_SMF.1 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フェースを提供する。
またこ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。

7.1.5. ファクスフローセキュリティ機能（TSF_FAX_FLOW）

ファクスフローセキュリティ機能は、いかなる場合においても USB インターフェイスでコントローラボードと接続されているファクスボードを通じて TOE に不正にアクセスすることはできず、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機能である。

（1）FDP_IFC.1 サブセット情報フロー制御
FDP_IFF.1 単純セキュリティ属性

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。

8. ST 略語・用語

8.1. 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 Copire)
D-FAX	ダイレクトファクス(Direct FAX)
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)
iFAX	インターネットファクス(Internet FAX)
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)
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)
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)
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)

8.2. 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、システム管理者、およびカストマーエンジニア。
カストマーエンジニア	MFP の保守/修理を行うエンジニア。
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 MFP に対して、TOE 設定データの確認や書き換えを行う。
システム管理者モード	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。
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。
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、利用者クライアントで使用する。
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。
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 3 種類がある。

用語	定義内容
	• セキュリティプリント: 一般利用者クライアント上のプリンタードライバーよりパスワードを設定し、操作パネルよりその暗証番号を入力することにより印刷が可能となる蓄積プリント。 • 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。
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。
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。 • 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。
内部蓄積データ	一般クライアントおよびサーバ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、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、システム管理者 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

用語	定義内容
	情報。
一般クライアントおよびサーバ	TOE の動作に関与しないクライアントやサーバを示す。
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。
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やクライアント PC 間のチャネルを指す。

9. 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 3.1 パート 1: 概説と一般モデル 2006 年 9 月 CCMB-2006-09-001 (平成 19 年 3 月翻訳第 1.2 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 3.1 パート 2: セキュリティ機能要件 2007 年 9 月 CCMB-2007-09-002 (平成 20 年 3 月翻訳第 2.0 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 3.1 パート 3: セキュリティ保証要件 2007 年 9 月 CCMB-2007-09-003 (平成 20 年 3 月翻訳第 2.0 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 評価方法 2007 年 9 月 CCMB-2007-09-004 (平成 20 年 3 月翻訳第 2.0 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)