THE DOCUMENT COMPANY
FUJI XEROX

セキュリティーターゲット

富士ゼロックス
ApeosPort C7550 I/C6550 I/C5540 I,
DocuCentre C7550 I/C6550 I/C5540 I シリーズ
データセキュリティーキット

26 July 2006

Version: V1.03

富士ゼロックス株式会社

更新履歴

NO	更新日	バージョン	更新内容
1	2006 年 6 月 9 日	V1.00	初版
2	2006 年 6 月 21 日	V1.01	ASE-001-01 対応など
3	2006 年 7 月 3 日	V1.02	資料名変更など
4	2006 年 7 月 26 日	V1.03	資料名変更など
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

－ 目次 －

1. ST 概説

1.1. ST 識別情報

（1） ST 識別

ST 識別	ApeosPort C7550 I/C6550 I/C5540 I, DocuCentre C7550 I/C6550 I/C5540 I シリーズ データセキュリティーキット セキュリティーターゲット
バージョン	V1.03
作成者名	富士ゼロックス株式会社
作成日	2006 年 7 月 26 日
CC 識別	Common Criteria for Information Technology Security Evaluation, Version2.1, 1999/8 CCIMB Interpretations-0407
PP 識別	なし
キーワード	デジタル複合機、コピー、プリンター、スキャナー、ハードディスク装置、上書き消去、暗号

（2） TOE 識別

TOE 識別	Fuji Xerox ApeosPort C7550 I/C6550 I/C5540 I, DocuCentre C7550 I/C6550 I/C5540 ISeries Security Kit for Asia Pacific
バージョン	Controller ROM Ver1.102.2
製造者	富士ゼロックス株式会社

本セキュリティーターゲットは、日本工業規格 JIS X5070 および ISO/IEC 15408(1999)に準拠する。
JIS X5070 は、ISO/IEC15408(1999)の日本語訳である。

1.2. ST 概要

本セキュリティーターゲットは、コピー機能、プリンター機能、およびスキャナー機能を有するデジタル複合機「ApeosPort C7550 I」、「ApeosPort C6550 I」、「ApeosPort C5540 I」、「DocuCentre C7550 I」、「DocuCentre C6550 I」および「DocuCentre C5540 I」のオプション製品であるデータセキュリティーキットのセキュリティー仕様について記述したものである。

データセキュリティーキットは、「ApeosPort C7550 I」、「ApeosPort C6550 I」、「ApeosPort C5540 I」、「DocuCentre C7550 I」、「DocuCentre C6550 I」および「DocuCentre C5540 I」によって処理された後、ハードディスク装置内に蓄積された文書データ(以降、これを「利用済み文書データ」と記す)を不正な暴露から保護するための製品である。

本製品は以下のセキュリティー機能を提供する。

- ハードディスク蓄積データ上書き消去機能
- ハードディスク蓄積データ暗号化機能
- 機械管理者認証機能
- カストマーエンジニアの操作制限機能

1.3. 評価保証レベル

TOE の評価保証レベルは **EAL2** である。

[理由] TOE は、SOHO、企業/官公庁、大学などの組織の施設内で利用することを目的としており、利用者は組織関係者に限定される。このため、本 TOE の評価保証レベルを **EAL2** とする。

1.4. 適合する PP

適合するプロテクションプロファイルはない。

1.5. 関連する ST

関連するセキュリティーターゲットはない。

1.6. CC 適合

本 TOE は、以下の情報セキュリティー評価基準に適合する。

JIS X5070 第 2 部(CC Version2.1 パート 2)	適合
JIS X5070 第 3 部(CC Version2.1 パート 3)	適合
JIS X5070	EAL2適合

1.7. 略語

本 ST で使用する略語を以下に示す。

略語	定義
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)
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)
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)
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	セキュリティー機能(Security Function)
SFP	セキュリティー機能方針(Security Function Policy)
SOF	機能強度(Strength of Function)
ST	セキュリティーターゲット(Security Target)
TOE	評価対象(Target of Evaluation)
TSC	TSF 制御範囲(TSF Scope of Control)
TSF	TOE セキュリティー機能
TSFI	TSF インタフェース(TSF Interface)
TSP	TOE セキュリティー方針(TOE Security Policy)
UI	ユーザーインタフェース(User Interface)

1.8. 用語

本 ST で使用する用語について説明する。

ApeosPort/DocuCentre

本 ST では「ApeosPort C7550 I」、「ApeosPort C6550 I」、「ApeosPort C5540 I」、「DocuCentre C7550 I」、

「DocuCentre C6550 I」および「DocuCentre C5540 I」を総称して ApeosPort/DocuCentre と表記する。

一般利用者

ApeosPort/DocuCentre のコピー機能およびプリンター機能を利用する者。

機械管理者

ApeosPort/DocuCentre の機械管理を行う者。

カストマーエンジニア

ApeosPort/DocuCentre の保守/修理を行う富士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

ApeosPort/DocuCentre 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。

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。一般利用者は、利用者クライアントにインストールされたプリンタードライバーを使用して ApeosPort/DocuCentre のプリンター機能を利用する。

機械管理者クライアント

機械管理者が利用するクライアント。機械管理者は WEB ブラウザを使って、ApeosPort/DocuCentre に対して、TOE 設定データの確認や書き換えを行う。

センターウェアインターネットサービス

機械管理者が WEB ブラウザを使って、ApeosPort/DocuCentre 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。

プリンタードライバー

利用者クライアント上のデータを ApeosPort/DocuCentre 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。利用者クライアントで利用する。

印刷データ

ApeosPort/DocuCentre 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。

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富士ゼロックス独自方式で画像圧縮して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。

ネットワークスキャナーユーティリティ

ApeosPort/DocuCentre の内部ハードディスク装置に蓄積された文書データにアクセスするためのソフトウエア。利用者クライアントで利用する。

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 ApeosPort/DocuCentre の内部ハードディスク装置に一旦蓄積し、一般利用者の操作パネルより指示もしくは、指定時刻になる事により印刷を開始するプリント方法。

以下の 5 種類がある。

- セキュリティープリント
- サンプルプリント
- 認証プリント
- 時刻指定プリント
- 親展ボックスを使った印刷

セキュリティープリント

利用者クライアント上のプリンタードライバーより暗証番号を設定し、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。

認証プリント

認証機能を利用している場合に、認証に失敗したプリントジョブを蓄積し、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方法。

時刻指定プリント

利用者クライアント上のプリンタードライバーより印刷開始時刻を指定し、指定時刻になると印刷が実行される蓄積プリント方法。

親展ボックスを使った印刷

拡張親展ボックスに、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方法。セキュリティープリントやサンプルプリントに比べ、印刷時にホチキス、パンチ、用紙サイズの設定を行う機能が追加される。

スプール

プリンター機能において、利用者クライアントから送信される印刷データ全てを内部の記憶装置に受信し、受信が終了した後に、デコンポーズを開始する方式。

本機能を使用することにより、複数の利用者クライアントからの印刷データの同時受信が可能となる。

ハードディスクスプール

スプール用内部記憶装置として、ハードディスク装置を使用するもの。

メモリスプール

スプール用内部記憶装置として、揮発性メモリを使用するもの。

ノンスプール

プリンター機能において、利用者クライアントから送信される印刷データを受信しながら、デコンポーズを行

う方式。この場合、複数の利用者クライアントからの印刷データを同時に受信する事はできない。

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。

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 ApeosPort/DocuCentre 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、ApeosPort/DocuCentre の内部ハードディスク装置に作られた拡張親展ボックスに蓄積する。蓄積された文書データは利用者クライアント上のネットワークスキャナーユーティリティにより取り出す。

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

拡張親展ボックス

ApeosPort/DocuCentre の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拡張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できる。

文書データ

本 ST では、一般利用者が ApeosPort/DocuCentre のコピー機能、プリンター機能、スキャナー機能を利用する際に、ApeosPort/DocuCentre 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。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、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。

利用済み文書データ

ApeosPort/DocuCentre の内部ハードディスク装置に蓄積され、利用が終了した文書データ。

制御データ

ApeosPort/DocuCentre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。

ハードディスク装置からの削除

本 ST では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できなくなる。しかし、文書データ自体はクリアされていない状態となる。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ハードディスク装置上に残る。

上書き消去

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。これをもとに暗号鍵を生成する。

暗号鍵

暗号化キーを元に自動生成される 128bit のデータ。これを使って暗号化を行う。

1.9. 参考資料

本 ST の参考資料を以下に示す。

[JIS X5070-1]	JIS X5070 セキュリティー技術-情報技術セキュリティーの評価基準-第1部:総則及び一般モデル
[JIS X5070-2]	JIS X5070 セキュリティー技術-情報技術セキュリティーの評価基準-第2部:セキュリティー機能要件
[JIS X5070-3]	JIS X5070 セキュリティー技術-情報技術セキュリティーの評価基準-第3部:セキュリティー保証要件
[CC パート1]	Common Criteria for Information Technology Security Evaluation Part1:Introduction and general model Version2.1, August 1999 CCIMB-99-031
[CC パート2]	Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version2.1, August 1999 CCIMB-99-032
[CC パート 3]	Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version2.1, August 1999 CCIMB-99-033
[CEM パート 1]	Common Evaluation Methodology for Information Technology Security Part1: Introduction and General Model Version0.6, Novmber 1997
[CEM パート 2]	Common Evaluation Methodology for Information Technology Security Part2: Evaluation and Methodology Version1.0, August 1999
[PDTR15446]	Information Technology Security techniques Guide for the production of protection profiles and security targets Propsed Draft, April 2000
[I-0407]	CCIMB Interpretations-0407

2. TOE 記述

2.1. TOE の種別

TOE は、デジタル複合機に内蔵されるデータセキュリティーキットであり、デジタル複合機によって処理された後、ハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するためのファームウエア製品である。

TOE は、富士ゼロックス社製デジタル複合機「ApeosPort C7550 I」、「ApeosPort C6550 I」、「ApeosPort C5540 I」、「DocuCentre C7550 I」、「DocuCentre C6550 I」および「DocuCentre C5540 I」のオプション製品として提供される。

2.2. TOE の利用環境

TOE は内部ネットワーク、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 に示す。

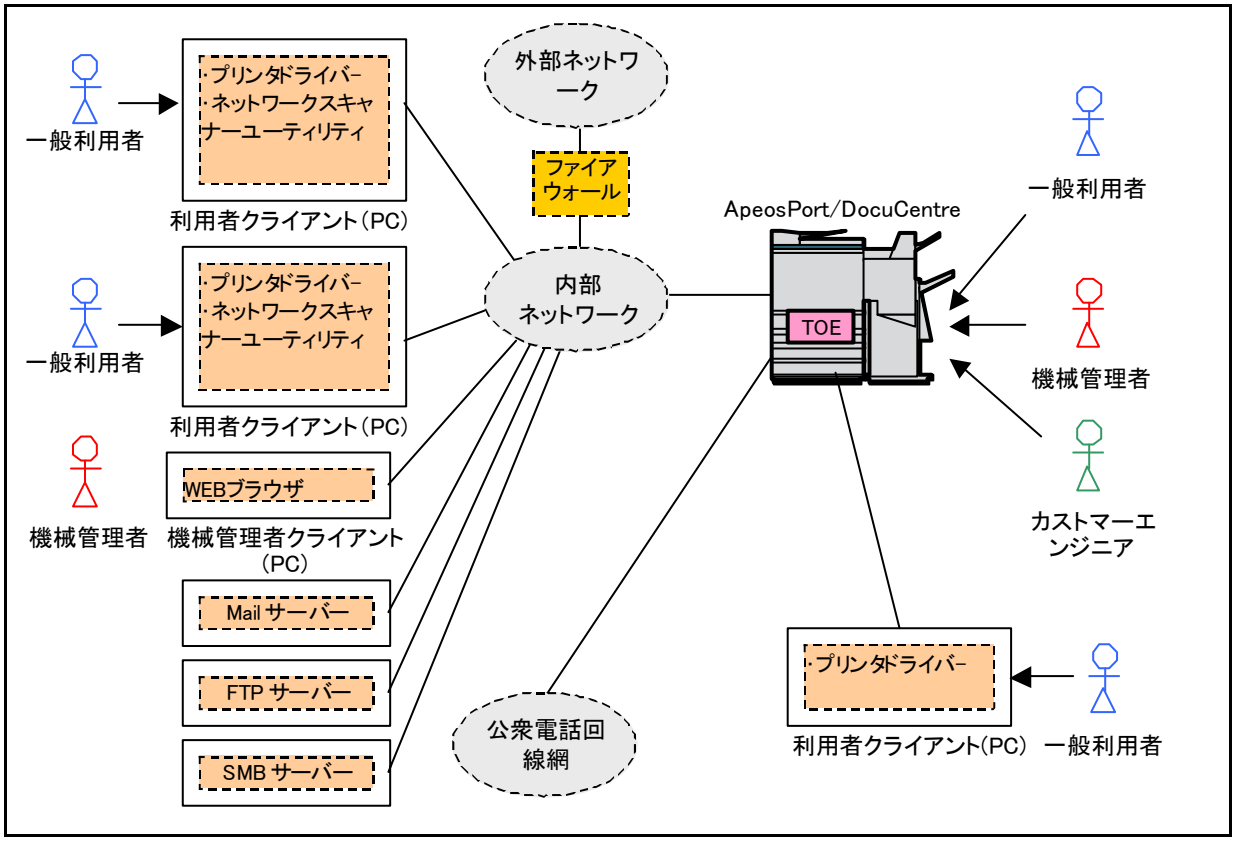

図 1 TOE の想定する利用環境

内部ネットワークには、以下のものが接続される。

・ 利用者クライアント:

プリンタードライバーおよびネットワークッスキャナユーティリティがインストールされており、

ApeosPort/DocuCentre に対して、文書データのプリント要求、文書データの取り出し要求を行う。

・ 機械管理者クライアント

WEB ブラウザを使って、ApeosPort/DocuCentre に対して、TOE 設定データの確認や書き換えを行う。

・ Mail サーバー:

ApeosPort/DocuCentre 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。

・ FTP サーバー:

ApeosPort/DocuCentre 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。

・ SMB サーバー:

ApeosPort/DocuCentre 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。

また、内部ネットワークの各機器を保護するため、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接続を行う。

2.3. TOE の利用目的

TOE の利用目的は、ApeosPort/DocuCentre の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、不正な暴露から保護することである。

2.4. TOE の構成

2.4.1. 物理的構成

図 2 に ApeosPort/DocuCentre 内の各ユニットと、TOE の物理的境界を示す。

ApeosPort/DocuCentre は、コントローラボード、操作パネルの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 IIT の間、コントローラボードと IOT の間は、文書データおよび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。

コントローラボードは、ApeosPort/DocuCentre のコピー機能、プリンター機能およびスキャナー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(IEEE1284、USB)を有し、IIT、IOT が接続される。

操作パネルは、ApeosPort/DocuCentre のコピー機能、プリンター機能およびスキャナー機能の操作および設定を行うパネルである。

TOE は、コントローラボードに装着されているシステム ROM の中に記録されているプログラムである。

TOE の物理的構成要素である ROM に記録されているプログラムを表 1に示す。

表1 TOE の物理的構成要素

構成要素	格納プログラム
システム ROM	ApeosPort/DocuCentre を制御するプログラムを記録しており、以下の機能を提供する。 ・ コピー制御機能 ・ プリンター制御機能 ・ スキャナー制御機能 ・ 操作パネル制御機能 ・ 機械管理者認証機能 ・ 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

	・ CWIS

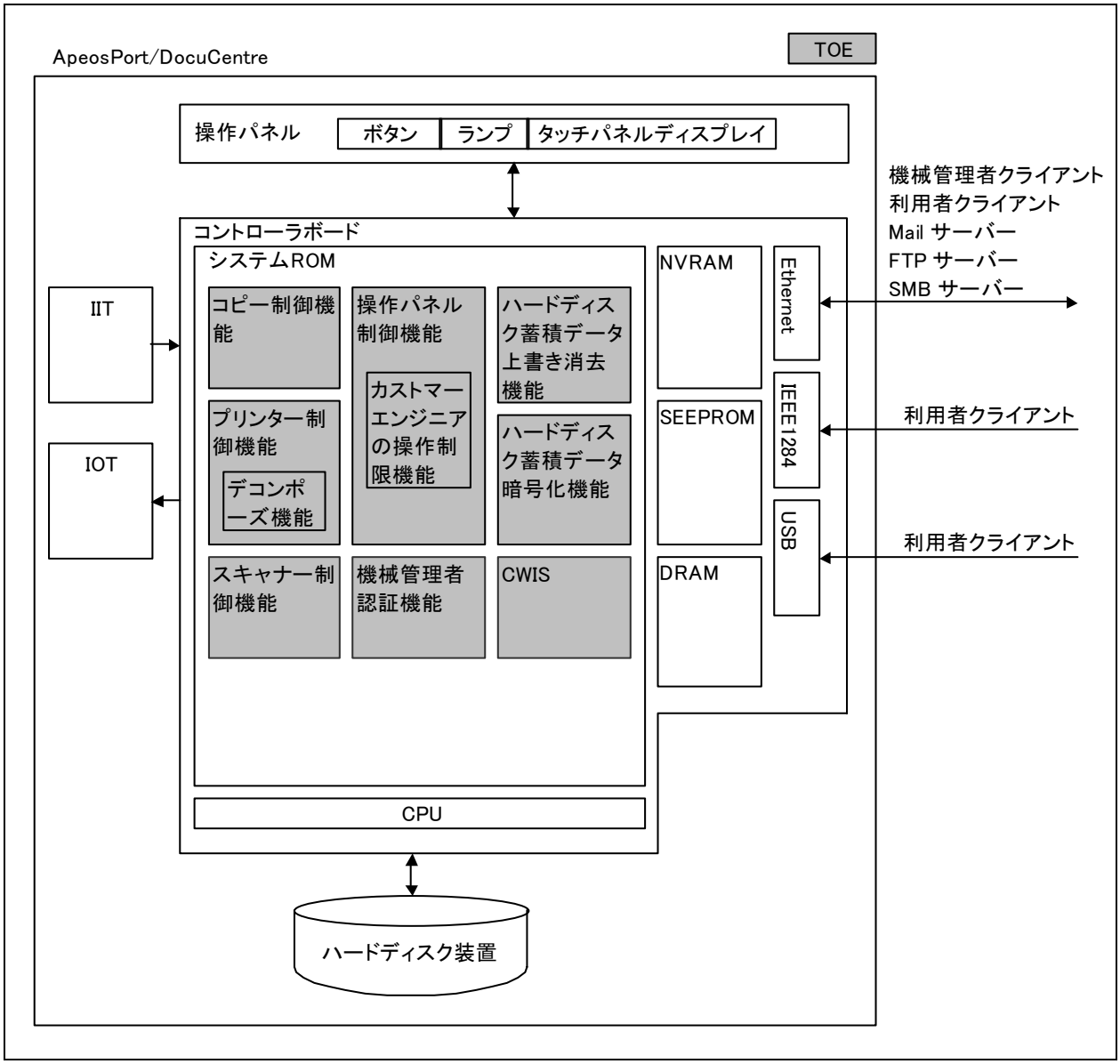

図 2 ApeosPort/DocuCentre 内の各ユニットと、TOE の物理的境界

2.4.2. 論理的構成

ApeosPort/DocuCentre の論理的構成を図 3 に示す。

ApeosPort/DocuCentre は一般利用者に対し、コピー機能、プリンター機能およびスキャナー機能を提供する。

●コピー機能

コピー機能は、一般利用者の操作パネルからの指示により、IIT で原稿を読み取り、IOT から印刷を行う機能である。

●プリンター機能

プリンター機能は、利用者クライアントから送信された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旦 ApeosPort/DocuCentre の内部ハードディスク装置に蓄積して、一般利用者の操作パネルからの指示により IOT から印刷を行う蓄積プリントがある。また、プリンター機能では、利用者クライアントから送信された印刷データを一時的に記録装置(ApeosPort/DocuCentre の内部メモリ、または内部ハードディスク装置)に受信し、受信終了後デコンポーズを開始するスプール方式と、利用者クライアントから送信された印刷データを ApeosPort/DocuCentre の内部メモリに受信しながらデコンポーズを行うノンスプール方式がある。

●スキャナー機能

スキャナー機能は、一般利用者の操作パネルからの指示により、IIT で原稿を読み取り、ApeosPort/DocuCentre の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利用者クライアント上のネットワークスキャナーユーティリティを使用して取り出したり、ApeosPort/DocuCentre に設定された情報に従い外部サーバーに転送したりすることができる。

●操作パネル制御機能

操作パネル制御機能は、機械管理者及びカストマーエンジニアの操作パネルからの入力をカストマーエンジニアの操作制限機能あるいは機械管理者認証機能に伝える。カストマーエンジニアあるいは機械管理者と認証された場合は、TOE 設定データにアクセスすることができる。

●CWIS

CWIS は、Web ブラウザを使った機械管理者クライアントの入力を機械管理者認証機能に伝える。機械管理者と認証された場合は、TOE 設定データにアクセスすることができる。

ApeosPort/DocuCentre は内部ハードディスク装置を一つ持つ。ハードディスク装置に蓄積された文書データは利用が終了して削除される際には、管理情報だけが削除され、蓄積されたデータ自体はクリアされない。このため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。

TOE は、これらのハードディスク装置に格納される利用済み文書データに対し、以下に示すセキュリティー機能を提供する。

● ハードディスク蓄積データ上書き消去機能

コピー、プリンターおよびスキャナーの各機能の動作後、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。

● ハードディスク蓄積データ暗号化機能

コピー、プリンターおよびスキャナー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。

また、上記セキュリティー機能の動作を保証するために、TOE は以下に示すセキュリティー機能を提供する。

● 機械管理者認証機能

操作パネル、または、機械管理者クライアントからの機械管理者の識別および認証を行い、TOE のセキュリティー機能に関する設定を機械管理者のみが行えるようにする。

● カストマーエンジニアの操作制限機能

カストマーエンジニアが TOE のセキュリティー機能に関する設定の参照および変更をできなくする機械管理者の設定機能である。

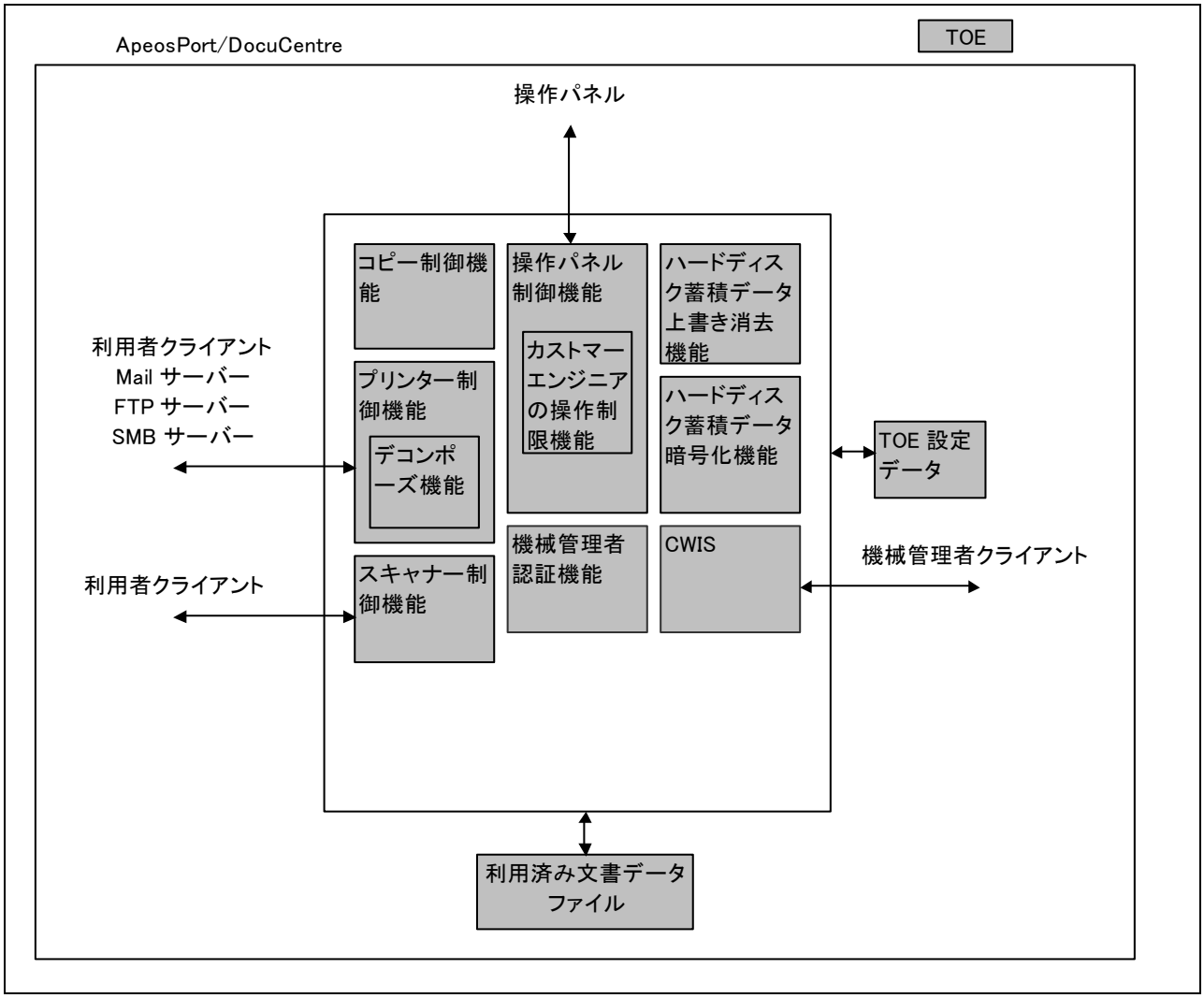

図3 TOE の論理的構成

表 2に ApeosPort/DocuCentre のコントローラボードの NVRAM および SEEPROM に記憶される TOE 設定データを示す。

表2 ApeosPort/DocuCentre の TOE 設定データと記録場所

設定データ	記憶場所
ハードディスク蓄積データ上書き消去機能設定	NVRAM
パスワードの使用設定	
機械管理者パスワード	

カストマーエンジニアの操作制限機能設定	
機械管理者 ID の認証失敗によるアクセス拒否	
ハードディスク蓄積データ暗号化機能設定	SEEPROM
ハードディスク蓄積データ暗号化キー	

ハードディスク蓄積データ上書き消去機能設定は、ハードディスク装置に記録されている利用済み文書データに対して上書き消去を実行する回数を、次の範囲で設定できる。

・「しない」: 上書き消去を行わない。
TOE のセキュリティー機能を利用しない場合に設定し、上書き消去によって発生する、コピー機能、プリンター機能の処理速度低下を回避する事ができる。

・「する(1 回)」: 全て 0 のデータで 1 回の上書き消去が行われる。
上書き消去により、利用済み文書データの再生を困難とする。3 回の上書き消去よりも、コピーやプリントの処理速度低下の影響が少ない。ハードディスク蓄積データ暗号化機能設定と組合せて設定することにより、利用済み文書データを保護する。

・「する(3 回)」: 「乱数」、「乱数」、「全て 0」の 3 回の上書き消去が行われる。
推奨設定値である。1 回の上書き消去でも利用済み文書データの再生は困難であるが、3 回の上書き消去を行う事で、再生をより困難とする。ハードディスク蓄積データ暗号化機能設定と組合せて設定することにより、利用済み文書データを保護する。

パスワードの使用設定は、次の範囲で設定できる。

・「しない」: パスワードを使用しない。
機械管理者の認証を行う場合に、機械管理者の User ID の入力だけを要求し、入力されたものが ApeosPort/DocuCentre の NVRAM に記録された情報と一致した場合に、機械管理者として認証する。セキュリティーのレベルとしては低いが、より利便性を求める場合に使用する。

・「する」: パスワードを使用する。
機械管理者の認証を行う場合に、機械管理者の User ID と機械管理者パスワードの入力を要求し、入力されたものが ApeosPort/DocuCentre の NVRAM に記録された情報と一致した場合に、機械管理者として認証する。

ハードディスク蓄積データ暗号化機能設定は、ハードディスク装置に記録される文書データについての暗号操作を次の範囲で設定できる。

・「しない」: 暗号化を行わない。
TOE のセキュリティー機能を利用しない場合に設定し、暗号化による処理速度低下を回避する事ができる。

・「する」: 暗号化を行う。

暗号化により、文書データの解析を困難とする。ハードディスク蓄積データ上書き消去機能設定と組合せて設定することにより、利用済み文書データを保護する。

ハードディスク蓄積データ暗号化キーは、ハードディスク蓄積データ暗号化機能設定が「する」の時に有効となり、ハードディスク装置に記録される文書データを暗号化するための暗号鍵を生成する際に使用する 12 桁の英数字を設定できる。

カストマーエンジニアの操作制限機能設定は、次の範囲で設定できる。

・「しない」: カストマーエンジニアの操作制限を使用しない。
TOE のセキュリティー機能を利用しない場合に設定し、カストマーエンジニアが TOE セキュリティー機能に関する設定の参照および変更を実施できる。

・「する」: カストマーエンジニアの操作制限使用する。
カストマーエンジニアが、TOE セキュリティー機能に関する設定の参照および変更をできないように制限する。

機械管理者 ID の認証失敗によるアクセス拒否は、次の範囲で設定できる。

・「しない」: 機械管理者認証エラー回数を制限しない。

・「する」: 機械管理者認証に失敗した時の許容回数。1～10の範囲で設定できる。1が設定されていた場合、1 回認証に失敗したら 2 回目以降は受け付けない。

2.5. TOE の関連者

本 ST では、以下の関連者を想定する。

関連者	説明
組織の責任者	ApeosPort/DocuCentre を利用運用する組織の責任者
一般利用者	ApeosPort/DocuCentre が提供するコピー機能およびプリンター機能の利用者。
機械管理者	ApeosPort/DocuCentre の機械管理を行う者。ApeosPort/DocuCentre の機器動作設定などを行う特別な権限を持つ。 機械管理者は、ApeosPort/DocuCentre の操作パネル及び、機械管理者クライアントの WEB ブラウザを使用して機械の管理を行う。
カストマーエンジニア	カストマーエンジニアは、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、ApeosPort/DocuCentre の機器動作設定を行う。このカストマーエンジニア専用のインターフェイスは ApeosPort/DocuCentre の保守のためのものである。

2.6. TOE が保護する資産

TOE が保護する資産は、ApeosPort/DocuCentre のハードディスク装置に蓄積された利用済み文書データと、NVRAM 、および SEEPROM に格納されている TOE 設定データである。

文書データには、コピー機能により格納されたビットマップデータと、利用者クライアントから送信されて格納された印刷データがある。印刷データは TOE のデコンポーズ機能によりビットマップデータに変換して蓄積、印刷される。利用済み文書データには、利用済みになったビットマップデータと、利用済みになった印刷データの2種類がある。

TOE が保護する資産の内容、格納媒体、および発生パターンを表 3に示す。

表3 保護資産の内容、格納媒体、および発生パターン

保護資産	内容
R.DOCDATA **（ハードディスク装置に蓄積された利用済み文書データ）**	[資産内容] コピー機能もしくはプリンター機能利用時、ハードディスク装置に蓄積される、利用済み文書データ。 [格納媒体] ApeosPort/DocuCentre のハードディスク装置内に格納される。 [発生パターン] コピー機能利用時 ・ 一般利用者により操作パネルから指示されたコピーが全て終了した時に利用済みとなるビットマップデータ。 ・ コピー中に一般利用者により操作パネルから中止が指示された時に利用済みとなるビットマップデータ。 プリンター機能利用時 ・ ハードディスクスプール方式の通常プリントで、利用者クライアントから送信された印刷データの印刷が全て終了した時に利用済みとなるスプール中の印刷データ。 ・ ハードディスクスプール方式の通常プリントで印刷中に、一般利用者により操作パネルから中止が指示された時に利用済みとなるスプール中の印刷データ。 ・ ハードディスクスプール方式の通常プリントまたは蓄積プリントで、利用者クライアントからの印刷データ送信中に、利用者クライアントから中止が指示された時に利用済みとなるスプール中の印刷データ。 ・ ハードディスクスプール方式の蓄積プリントで、デコンポーズが終了してビットマップデータがハードディスク装置に蓄積された時に利用済みとなるスプール中の印刷データ。 ・ 蓄積プリントで、一般利用者により操作パネルから蓄積されている文書データの印刷が指示され、印刷が全て終了した時に利用済みとなるビットマップデータ。 ・ 蓄積プリントで、指定時刻となり、印刷が全て終了した時に利用済みとなるビットマップデータ。 ・ 蓄積プリントの文書データを印刷中に、一般利用者により操作パネルから中止が指示された時に利用済みとなるビットマップデータ。 ・ 蓄積プリントで、一般利用者により操作パネルから蓄積されている文書データの削除が指示された時に利用済みとなるビットマップデータ。 ・ 利用者クライアントから送信された印刷データの印刷が全て終了した時に利用済みとなるビットマップデータ。 ・ 印刷中に一般利用者により操作パネルから中止が指示された時に利用済みとなるビットマップデータ。 スキャナー機能利用時 ・ 利用者クライアント上のネットワークスキャナーユーティリティにより、蓄積されている文書データの取り出しが終了した時に利用済みとなるビットマップデータ。 ・ 蓄積されている文書データを FTP サーバー、Mail サーバーもしくは SMB サーバーへ転送する事が終了した時に利用済みとなるビットマップデータ。 ・ 一般利用者により操作パネルから蓄積されている文書データの削除が指示された時に利用済みとなるビットマップデータ。 ・ スキャン中に一般利用者により操作パネルから中止が指示された時に利用済みとなるビットマップデータ。
R.CONFDATA **（TOE 設定データ）**	[資産内容] ・ 「ハードディスク蓄積データ上書き消去機能設定」 ・ 「パスワードの使用設定」 ・ 「機械管理者パスワード」 ・ 「カストマーエンジニアの操作制限機能設定」 ・ 「ハードディスク蓄積データ暗号化機能設定」 ・ 「ハードディスク蓄積データ暗号化キー」 ・ 「機械管理者 ID の認証失敗によるアクセス拒否」 [格納媒体] NVRAM に格納されているもの。（注意）

	・ 「ハードディスク蓄積データ上書き消去機能設定」 ・ 「パスワードの使用設定」 ・ 「機械管理者パスワード」 ・ 「カストマーエンジニアの操作制限機能設定」 ・ 「機械管理者 ID の認証失敗によるアクセス拒否」 SEEPROM に格納されているもの。(注意) ・ 「ハードディスク蓄積データ暗号化機能設定」 ・ 「ハードディスク蓄積データ暗号化キー」

(注意)

・ ApeosPort/DocuCentre の NVRAM と SEEPROM には、「ハードディスク蓄積データ上書き消去機能設定」、「パスワードの使用設定」、「機械管理者パスワード」、「ハードディスク蓄積データ暗号化機能設定」、「ハードディスク蓄積データ暗号化キー」、「カストマーエンジニアの操作制限機能設定」「機械管理者 ID の認証失敗によるアクセス拒否」

以外のデータ(節電時間の設定データなど)も格納されているが、それらのデータは、TOE のセキュリティー機能に関係しないため保護対象の資産ではない。

2.7. TOE の機能

2.7.1. TOE のセキュリティー機能

TOE は以下のセキュリティー機能を提供する。

機能分類	説明
ハードディスク蓄積データ上書き消去機能	ApeosPort/DocuCentre の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、特定パターンで上書き消去する機能。 電源断などで利用済み文書データが上書き未終了となってしまった場合、次回の電源投入時に自動的にその利用済み文書データ領域を「ハードディスク蓄積データ上書き消去機能設定」に従い上書き消去する。
ハードディスク蓄積データ暗号化機能	ApeosPort/DocuCentre のハードディスク装置に蓄積された文書データを暗号化する機能。
機械管理者認証機能	機械管理者の識別および認証を行い、TOE 設定データに関する設定を機械管理者のみが行えるようにする機能。設定回数、認証に失敗すると認証を拒否する。
カストマーエンジニアの操作制限機能	カストマーエンジニアがTOE設定データを参照及び変更する際に利用する。カストマーエンジニア専用のインタフェースを使用できなくする機能で、機械管理者が設定することができる。 本機能を有効にすることによって、カストマーエンジニアになりすました攻撃者が、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 設定データの参照及び変更ができなくなる。

2.7.2. TOE の非セキュリティー機能

TOE は以下の非セキュリティー機能を提供する。

機能分類	説明
コピー制御機能	ApeosPort/DocuCentre のコピー動作を制御する機能。IIT から読み取った文書データを、デジタルフィルタなどにより画像変換して IOT により印刷する。
プリンター制御機能	ApeosPort/DocuCentre のプリンター動作を制御する機能。利用者クライアントから送信されるページ記述言語(PDL)で構成されている印刷データをデコンポーズ機能により、印刷が可能なビットマップデータに変換して IOT により印刷する。
デコンポーズ機能	プリンター機能において、利用者クライアントから送信されるページ記述言語(PDL)で構成されている印刷データを解析して、印刷が可能なビットマップデー

	タに変換する機能。
スキャナー制御機能	ApeosPort/DocuCentre のスキャナー動作を制御する機能。IIT から読み取った文書データを、デジタルフィルタなどにより画像変換してハードディスク装置に蓄積する。
CWIS	Web ブラウザを使って、ApeosPort/DocuCentre の消耗品などの状態を確認したり各種設定データを読み出したり書き込んだりする機能。

2.8. TOE 利用方法

TOE 設定データは、機械管理者によって設定される。機械管理者は、操作パネルより工場出荷時に設定されたデフォルトの機械管理者の User ID を入力し認証された後、以下設定項目の設定を行う。尚、下記の機械管理者パスワードの変更のみ、機械管理者クライアントより設定が可能である。

- **パスワードの使用設定**

  「する」に設定する。

- **機械管理者パスワードの変更**

  デフォルト値以外の 7 文字～12 文字の値を設定する。

- **機械管理者 ID の認証失敗によるアクセス拒否の設定**

  「5」に設定する。

- **カストマーエンジニアの操作制限機能の設定**

  「する」に設定する。

- **ハードディスク蓄積データ上書き消去機能の設定**

  「する(1 回)」か「する(3 回)」に設定する。

- **ハードディスク蓄積データ暗号化機能の設定**

  「する」に設定する。

- **ハードディスク蓄積データ暗号化キーの設定**

  12 文字の値を設定する。(12 文字以下が設定された場合、不足分は自動的に「0」が設定される。)

一般利用者が ApeosPort/DocuCentre のコピー機能およびプリンター機能を利用する際、利用済み文書データは、「表 4 ApeosPort/DocuCentre の各機能におけるデータの流れ」 に示す様に、ApeosPort/DocuCentre の内蔵ハードディスク装置に蓄積される。

この、蓄積された利用済み文書データに対して、一般利用者は意識する事無く、機械管理者の設定に従い TOE のセキュリティー機能が動作する。

表 4に、ApeosPort/DocuCentre の各機能における各ユニット間の制御データおよび文書データの流れを示す。

表4 ApeosPort/DocuCentre の各機能におけるデータの流れ

機能		データ種別	データの流れ
IIT、IOT	通常コピー	制御データ	操作パネル→コントローラボード→IOT
		文書データ	IIT→コントローラボード→ハードディスク装置→コントローラボード→IOT

プリンター	通常プリント(ノンスプール)	制御データ	利用者クライアント→コントローラボード→IOT
		文書データ (印刷データ)	利用者クライアント→コントローラボード ↓(コントローラボードでデコンポーズしてビットマップデータを作成)
		文書データ (ビットマップデータ)	コントローラボード→IOT
	通常プリント(ハードディスク装置スプール)	制御データ	利用者クライアント→コントローラボード→ハードディスク装置→コントローラボード→IOT
		文書データ (印刷データ)	利用者クライアント→コントローラボード→ハードディスク装置→コントローラボード ↓(コントローラボードでデコンポーズしてビットマップデータを作成)
		文書データ (ビットマップデータ)	コントローラボード→IOT
	蓄積プリント(ノンスプール)	制御データ	①文書データのディスク蓄積 利用者クライアント→コントローラボード→ハードディスク装置 ②文書データのプリント出力 (操作パネルでの操作により起動される) ハードディスク装置→コントローラボード→IOT
		文書データ (印刷データ)	①文書データのディスク蓄積 利用者クライアント→コントローラボード ↓(コントローラボードでデコンポーズしてビットマップデータを作成)
		文書データ (ビットマップデータ)	コントローラボード→ハードディスク装置 ②文書データのプリント出力 (操作パネルでの操作により起動される) ハードディスク装置→コントローラボード→IOT
	蓄積プリント(ハードディスク装置スプール)	制御データ	①文書データのディスク蓄積 利用者クライアント→コントローラボード→ハードディスク装置→コントローラボード→ハードディスク装置 ②文書データのプリント出力 (操作パネルでの操作により起動される) ハードディスク装置→コントローラボード→IOT
		文書データ (印刷データ)	①文書データのディスク蓄積 利用者クライアント→コントローラボード→ハードディスク装置→コントローラボード ↓(コントローラボードでデコンポーズしてビットマップデータを作成)
		文書データ (ビットマップデータ)	コントローラボード→ハードディスク装置 ②文書データのプリント出力 (操作パネルでの操作により起動される) ハードディスク装置→コントローラボード→IOT
スキャナー	スキャン蓄積	制御データ	操作パネル→コントローラボード→IIT
		文書データ	IIT→コントローラボード→ハードディスク装置
	スキャン取り出し	制御データ	利用者クライアント→コントローラボード
		文書データ	ハードディスク装置→コントローラボード→利用者クライアント

操作パネルでの操作	制御データ（操作）	操作パネル→コントローラボード
機械管理者クライアントの操作	制御データ（操作）	機械管理者クライアント(Web ブラウザ)→内部ネットワーク→コントローラボード

3. TOE セキュリティー環境

3.1. 前提条件

本 TOE の動作/運用/利用に関わる前提条件を表 5に示す。

表5 前提条件

前提条件	内容
A.SECMODE	<保護モード> 機械管理者は、TOE を運用するにあたって、以下の通り設定するものとする。 機械管理者パスワード:7 文字～12 文字 カストマーエンジニアの操作制限機能設定:する パスワードの使用設定:する 機械管理者 ID の認証失敗によるアクセス拒否:するで 5 回 さらに、機械管理者パスワードは推測や暴露を防ぐように管理される。
A.ADMIN	<機械管理者の信頼> 機械管理者は、課せられた役割を遂行するために必要な知識を有し、悪意をもった不正を行わないものとする。
A.NET	<ネットワークの接続条件> TOE が搭載された ApeosPort/DocuCentre 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 ApeosPort/DocuCentre 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 ApeosPort/DocuCentre へアクセスできない。

3.2. 脅威

TOE に対する特別なアクセス権限を与えられている機械管理者は信頼できるため、攻撃者には該当しない。本 TOE に対するセキュリティー脅威および攻撃者を表 6に示す。

攻撃者は低レベルの攻撃力を持つものとする。

表6 セキュリティー脅威

脅威	内容	攻撃者	保護資産
T.RECOVER	**<利用済み文書データの不正再生>** 一般利用者および TOE の非関連者がハードディスク装置を取り外し、直接ツールに接続するなどして、利用済み文書データを、再生するかもしれない。	・一般利用者 ・非関連者	R.DOCDATA
T.CONFDATA	**<TOE 設定データの不正アクセス>** 一般利用者および TOE の非関連者が、操作パネル及び機械管理者クライアントから、機械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を変更するかもしれない。	・一般利用者 ・非関連者	R.CONFDATA

3.3. 組織のセキュリティー方針

組織のセキュリティー方針はない。

4. セキュリティー対策方針

4.1. TOE のセキュリティー対策方針.

TOE のセキュリティー対策方針を表 7に示す。

表7 TOE のセキュリティー対策方針

対策方針	説明
O.RESIDUAL	TOE は、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再生を上書き消去により不可能にしなければならない。
O.DECIPHER	TOE は、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解析を暗号化により困難にしなければならない。
O.MANAGE	TOE は、認証された機械管理者だけが、TOE 設定データの変更を可能としなければならない。

4.2. 環境のセキュリティー対策方針

4.2.1. IT 環境のセキュリティー対策方針

IT 環境のセキュリティー対策方針はない。

4.2.2. 運用/管理のセキュリティー対策方針

運用/管理のセキュリティー対策方針を表 8に示す。

表8 運用/管理のセキュリティー対策方針

対策方針	説明
OE.AUTH	機械管理者は「機械管理者パスワード」の推測や暴露を防ぐ様に管理しなくてはならない。具体的には、機械管理者パスワードを容易に推測できる値に設定したり、攻撃者の目に触れる場所に格納したりなどしてはならない。 また、「機械管理者パスワード」は 7 文字～12 文字の値に設定し、「カストマーエンジニアの操作制限機能」、および「パスワードの使用」が機能する様に設定された状態で「機械管理者 ID の認証失敗によるアクセス拒否」を 5 回に設定し、TOE を運用しなければならない。
OE.FUNCON	機械管理者は「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」が機能する様に設定された状態で、TOE を運用しなければならない。
OE.ADMIN	組織の責任者は、機械管理者が課せられた役割を遂行するために必要な知識を有し、悪意をもった行為を行わないことを保証するために、適切な人選を行うと共に管理や教育を実施しなければならない。
OE.NET	組織の責任者は、TOE が搭載された ApeosPort/DocuCentre 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 ApeosPort/DocuCentre 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。

5. IT セキュリティー要件

5.1. TOE セキュリティー機能要件

TOE が提供するセキュリティー機能要件を規定する。

5.1.1. クラス FCS： 暗号サポート

FCS_CKM.1 暗号鍵生成

下位階層: なし

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]

なし

[割付: 暗号鍵生成アルゴリズム]

富士ゼロックスオリジナルの FXOSENC 方式

[割付: 暗号鍵長]

128 bits

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ー属性

FCS_COP.1 暗号操作

下位階層: なし

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]

AES (Advanced Encryption Standerd)

[割付: 暗号アルゴリズム]

ラインダールアルゴリズム (Rijndael Algorithm)

[割付: 暗号鍵長]

128 bits

[割付: 暗号操作のリスト]

ハードディスク装置に蓄積される文書データの暗号化

ハードディスク装置に蓄積された文書データの復号

依存性: [FDP_ITC.1 セキュリティー属性なし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
FMT_MSA.2 セキュアなセキュリティー属性

5.1.2. クラス FDP : 利用者データ保護

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: への資源割当て、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事を保証しなければならない:[割付: オブジェクトのリスト]。

[選択: への資源割当て、からの資源の割当て解除]

からの資源の割当て解除

[割付: オブジェクトのリスト]

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

依存性: なし

5.1.3. クラス FIA : 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 TSF は、[割付:認証事象リスト]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]

機械管理者認証機能

[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」]

1～10 回内における管理者設定可能な正の整数値

FIA_AFL.1.2 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: アクションのリスト]をしなければならない。

[割付: アクションのリスト]

認証を拒否する認証拒否状態への遷移

認証拒否状態を解除する機能は存在しない

依存性: FIA_UAU.1 認証のタイミング

FIA_UID.2　　アクション前の利用者識別

下位階層:　FIA_UID.1

FIA_UID.2.1　TSF は、その[詳細化: 機械管理者]を代行する他の TSF 調停アクションを許可する前に、[詳細化: 機械管理者]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

FIA_UAU.2　　アクション前の利用者認証

下位階層:　FIA_UAU.1

FIA_UAU.2.1　TSF は、その[詳細化: 機械管理者]を代行する他の TSF 調停アクションを許可する前に、[詳細化: 機械管理者]に[詳細化: 機械管理者パスワードによる]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

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、[詳細化: 機械管理者認証のための機械管理者パスワード]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]

機械管理者パスワードとして入力された文字数と同数の '*' 文字

依存性:　FIA_UAU.1 認証のタイミング

5.1.4. クラス FMT : セキュリティー管理

FMT_MOF.1 (1)　セキュリティー機能のふるまいの管理(1)

下位階層:　なし

FMT_MOF.1.1　TSF は、機能[割付: 機能のリスト][選択: のふるまいを決定する、を停止する、を動作させる、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]

ハードディスク蓄積データ上書き消去機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

のふるまいを決定する

を停止する

を動作させる

[割付: 許可された識別された役割]

機械管理者

依存性:　FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

FMT_MOF.1 (2)　セキュリティー機能のふるまいの管理（2）

下位階層:　なし

FMT_MOF.1.1　TSF は、機能[割付: 機能のリスト][選択: のふるまいを決定する、を停止する、を動作させる、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]

ハードディスク蓄積データ暗号化機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

を停止する

を動作させる

[割付: 許可された識別された役割]

機械管理者

依存性:　FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

FMT_MOF.1 (3)　セキュリティー機能のふるまいの管理（3）

下位階層:　なし

FMT_MOF.1.1　TSF は、機能[割付: 機能のリスト][選択: のふるまいを決定する、を停止する、を動作させる、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]

機械管理者認証機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

のふるまいを決定する

[割付: 許可された識別された役割]

機械管理者

依存性:　FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

FMT_MTD.1(1)　TSF データの管理(1)

下位階層:　なし

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]

パスワードの使用設定

機械管理者 ID の認証失敗によるアクセス拒否

[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]

機械管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

FMT_MTD.1(2) TSF データの管理(2)

下位階層: なし

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]

ハードディスク蓄積データ暗号化キー

[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]]

改変

[割付: 許可された識別された役割]

機械管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

FMT_MTD.1(3) TSF データの管理(3)

下位階層: なし

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]

カストマーエンジニアの操作制限機能設定

[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]]

改変

[割付: 許可された識別された役割]

機械管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティー役割

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ー管理機能を行う能力を持たねばならない:[割付:TSF によって提供されるセキュリティー管理機能のリスト]。

[割付: TSF によって提供されるセキュリティー管理機能のリスト]

表 9に示す管理項目を管理する機能

表9 管理項目を管理する機能

機能要件	管理要件	管理項目
FCS_CKM.1	暗号鍵属性の変更の管理	無し（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	予見される管理アクティビティはない	無し
FDP_RIP.1	いつ残存情報保護を実施するのかの選択（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。	文書データ削除時固定
FIA_AFL.1	不成功の認証試行に対する閾値の管理 認証失敗の事象においてとられるアクションの管理	機械管理者認証エラー回数 認証拒否状態
FIA_UID.2	利用者識別情報の管理	機械管理者の User ID
FIA_UAU.2	機械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	機械管理者パスワード
FMT_MOF.1 (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	機械管理者固定
FMT_MOF.1 (2)	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	機械管理者固定
FMT_MOF.1 (3)	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	機械管理者固定
FMT_MTD.1(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	機械管理者固定
FMT_MTD.1(2)	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	機械管理者固定
FMT_MTD.1(3)	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	機械管理者固定
FMT_SMR.1	役割の一部をなす利用者のグループの管理	機械管理者固定 （機械管理者パスワードを知るものだけが、機械管理者となれる。）

FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMR.1 に関し、唯一、機械管理者パスワードにより認証された機械管理者だけが管理されており、グループの管理は行っていない。

依存性: なし

FMT_SMR.1 セキュリティー管理役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割 [割付: 許可された識別された役割]を維持しなければならない。

[割付： 許可された識別された役割]

機械管理者

FMT_SMR.1.2 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

5.1.5. クラス FPT： TSF の保護

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

5.2. TOE セキュリティー保証要件

TOE の評価保証レベルは、EAL2 である。[CC パート 3]に規定されている EAL2 保証パッケージのコンポーネントを以下に示す。

表10 EAL2 保証要件

保証クラス	保証コンポーネント ID	保証コンポーネント	依存性
構成管理	ACM_CAP.2	構成要素	なし
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
開発	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	非形式的対応の実証	なし
ガイダンス文書	AGD_ADM.1	機械管理者ガイダンス	ADV_FSP.1
	AGD_USR.1	利用者ガイダンス	ADV_FSP.1
テスト	ATE_COV.1	カバレージの分析	ADV_FSP.1 ATE_FUN.1
	ATE_FUN.1	機能テスト	なし
	ATE_IND.2	独立試験・サンプル	ADV_FSP.1 ADV_ADM.1 AGD_USR.1 ATE_FUN.1
脆弱性評定	AVA_SOF.1	TOE セキュリティー機能強度評価	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 環境セキュリティー機能要件

TOE の IT 環境が提供するセキュリティー機能要件はない。

5.4. TOE セキュリティー機能強度主張

TOE のセキュリティー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 セキュリティー機能要件は、FIA_AFL.1、FIA_UAU.2 である。

6. TOE 要約仕様

6.1. TOE セキュリティー機能

本 TOE は、TOE セキュリティー機能要件を満足するために以下のセキュリティー機能を有する。

- ハードディスク蓄積データ上書き消去機能（SF.OVERWRITE）
- ハードディスク蓄積データ暗号化機能（SF.ENCRYPTION）
- 機械管理者認証機能(SF.MANAGE)
- カストマーエンジニアの操作制限機能(SF.CEREST)

表 11に、各 TOE セキュリティー機能とセキュリティー機能要件の関係を示す。

表11 TOE セキュリティー機能とセキュリティー機能要件との関係

TOE セキュリティー機能 / セキュリティー機能要件	SF.OVERWRITE	SF.ENCRYPTION	SF.MANAGE	SF.CEREST
FCS_CKM.1		○		
FCS_COP.1		○		
FDP_RIP.1	○			
FIA_AFL.1			○	
FIA_UID.2			○	
FIA_UAU.2			○	
FIA_UAU.7			○	
FMT_MOF.1 (1)			○	
FMT_MOF.1 (2)			○	
FMT_MOF.1 (3)			○	
FMT_MTD.1(1)			○	
FMT_MTD.1(2)			○	
FMT_MTD.1(3)				○
FMT_SMF.1			○	
FMT_SMR.1			○	
FPT_RVM.1	○	○	○	

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

この機能は、機械管理者により設定された「ハードディスク蓄積データ上書き消去機能設定」に従い、ハードディスク装置上の利用済み文書データ領域を表 12に示す方法により上書き消去する。

ハードディスク装置上には、上書き消去予定の利用済み文書データの一覧を持ち、システム起動時に、この一覧に利用済み文書データが存在する事を示している場合、本機能は、利用済み文書データの上書き消去を実施する。

本機能は、バイパス手段を有し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。

表12 上書きの制御

上書き回数	上書きデータ
1 回	0
3 回	1 回目: 乱数 2 回目: 乱数 3 回目: 0

6.1.2. ハードディスク蓄積データ暗号化機能 (SF.ENCRYPTION)

この機能は、機械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機能設定」に従い、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。暗号鍵は機械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オリジナルの 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、起動時に生成され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、蓄積された文書データを読み出す際に起動時に生成された暗号鍵を使用して復号を行う。

起動時に生成された暗号鍵は、ApeosPort/DocuCentre 内のコントローラボードの DRAM(揮発性メモリ)に記憶する。なお、暗号鍵は ApeosPort/DocuCentre 本体の電源を切断すると消滅する。

本機能は、バイパス手段を有し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。

また、本機能は、セキュリティメカニズムとして、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)を利用している。

6.1.3. 機械管理者認証機能 (SF.MANAGE)

この機能は、TOE 設定データの操作を認証された機械管理者が行えるよう制御する。TOE 設定データの操作を許可する前に、操作パネル及び機械管理者クライアントの WEB ブラウザ画面から入力された「機械管理者の User ID」と「機械管理者パスワード」により機械管理者を識別・認証する。

操作パネル及び機械管理者クライアントの WEB ブラウザから「機械管理者パスワード」を入力中は、入力したパスワードの文字数と同数の"*"文字を操作パネル及び機械管理者クライアントの WEB ブラウザの「パスワード」入力フィールドに表示する。

操作パネル及び機械管理者クライアントの WEB ブラウザから入力された「機械管理者の User ID」および「機械管理者パスワード」が正しく、機械管理者の識別・認証に成功した場合には、TOE 設定データの操作を許可する。また、操作パネル及び機械管理者クライアントの WEB ブラウザから入力された「機械管理者の User ID」あるいは「機械管理者パスワード」の何れかが不正であり、機械管理者の識別・認証に失敗した場合には、識別・認証エラーを表示する。「機械管理者 ID の認証失敗によるアクセス拒否」で設定される回数、認証に失敗すると認証を拒否する。こうして認証された機械管理者だけが、

「ハードディスク蓄積データ上書き消去機能」を、「しない」、「する(1 回)」、「する(3 回)」

「パスワードの使用設定」を、「しない」、「する」

「ハードディスク蓄積データ暗号化機能」を、「しない」、「する」
「機械管理者パスワード」を、7文字～12文字の英数字
「機械管理者 ID の認証失敗によるアクセス拒否」を、「しない」、「する（1～10回）」
「ハードディスク蓄積データ暗号化キー」を、12文字の英数字
に設定することができる。

本機能は、バイパス手段を有し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. カストマーエンジニアの操作制限機能（SF.CEREST）

この機能は、TOE 設定データである「カストマーエンジニアの操作制限機能設定」の操作を認証された機械管理者が行えるよう制御する。

「カストマーエンジニアの操作制限機能設定」は、「しない」、または「する」に設定することができるが、TOE を使用するときには「する」を設定しなければならない。「する」に設定することによって、カストマーエンジニアの操作を制限し、カストマーエンジニアが TOE セキュリティー機能に関する設定の参照および変更をできないようにすることができる。本機能は、バイパス手段を有し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. 確率的または順列的メカニズムにより実現される機能

TOE セキュリティー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機械管理者認証機能(SF.MANAGE)である。本機能の機能強度レベルは SOF-基本である。

6.2. 保証手段

6.2.1. C7550 I シリーズ 構成管理説明書 (AS.CONFIGURATION)

「C7550 I 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ー保証要件

- ACM_CAP.2

6.2.2. C7550 I シリーズ TOE 構成リスト (AS.CONFIGURATIONLIST)

「C7550 I シリーズ TOE 構成リスト」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ー保証要件

- ACM_CAP.2

6.2.3. 海外機 配布、導入、運用手続き説明書 (AS.DELIVERY)

「海外機 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 のセキュリティーを維持するための、作成環境から利用者への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/起動に関するセキュリティー上の注意事項と正しい導入/設置/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/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ー保証要件

- ADO_DEL.1
- ADO_IGS.1

6.2.4. C7550 I シリーズ 機能仕様書 (AS.FUNCSPEC)

「C7550 I 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ー機能と、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、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 のセキュリティー機能の完全なる記述

対応するセキュリティー保証要件

- ADV_FSP.1

6.2.5. C7550 I シリーズ 上位レベル設様書 (AS.HIGHLDESIGN)

「C7550 I 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 のセキュリティー機能の構造
- 全サブシステム間のインタフェースについて、目的と利用方法(例外事項、エラーメッセージを含む)
- セキュリティー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ー保証要件

- ADV_HLD.1

6.2.6. C7550 I シリーズ 対応分析書 (AS.REPRESENT)

「C7550 I シリーズ 対応分析書」には、以下の内容が記述されている。

・ セキュリティー機能に関して、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ー保証要件

・ ADV_RCR.1

6.2.7. ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide (AS. GUIDANCE)

富士ゼロックスは、TOE の開発において、マニュアル(「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit 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。

<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、セキュリティーへの影響、セキュリティーを維持するための方策、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、非矛盾性の確認
・ TOE の C7550 I シリーズ 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

「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」は、機械管理者および一般利用者共通である。
「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」には、以下の内容が記述されている。

<機械管理者向け記載内容>

・ 機械管理者が利用する管理機能とそのインタフェース
・ セキュリティーを確保して、TOE を管理するための方法
・ セキュリティー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
・ 機械管理者の管理下にある全てのセキュリティー関連のパラメータとパラメータ値の注意事項
・ 管理機能に対する全てのセキュリティー事象の種別
・ 機械管理者の責任や行為についての前提条件
・ 機械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
・

<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ー機能の使用法

- 一般利用者が利用する機能とそのインタフェース
- セキュリティー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ー保証要件

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

6.2.8. C7550 I シリーズテスト計画書 兼 報告書 (AS.TEST)

「C7550 I 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、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「C7550 I シリーズ 機能仕様書」に記載された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ー保証要件

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

6.2.9. C7550 I シリーズ 脆弱性分析書 (AS.VULNERABILITY)

TOE のセキュリティー強度および脆弱性の確認評価を行うため、「C7550 I シリーズ 脆弱性分析書」を作成する。

「C7550 I シリーズ 脆弱性分析書」には、以下の内容を記載し、想定される環境で、TOE のセキュリティー強度、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。

〈セキュリティー強度〉

・TOE のセキュリティー機能に対して、そのセキュリティー強度が本 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。
・セキュリティー強度分析の仮説の妥当性検証結果。
〈脆弱性〉
・一般的なセキュリティー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ー保証要件
・AVA_SOF.1
・AVA_VLA.1

7. PP 主張

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

PP への修整はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

8.1. セキュリティー対策方針根拠

まず、セキュリティー対策方針と脅威および前提条件の対応を表 13に示す。

(1) 必要性

セキュリティー対策方針の必要性の根拠を示す。

表 13に示すように、全てのセキュリティー対策方針は、1つ以上の脅威または前提条件に対応している。

表13 セキュリティー対策方針と脅威および前提条件の対応

脅威・前提条件 / セキュリティー対策方針	T.RECOVER	T.CONFDATA	A.SEGMODE	A.NET	A.ADMIN
O.RESIDUAL	○				
O.DECIPHER	○				
O.MANAGE		○			
OE.ADMIN					○
OE.AUTH			○		
OE.FUNCON	○				
OE.NET				○	

○: 対象のセキュリティー対策方針が対応している脅威または前提条件である事を示す。

(2) 十分性

TOE に対する全ての脅威および前提条件に対し、十分な対策がなされている根拠を述べる。

全ての脅威は表 13に示すように、いずれかのセキュリティー対策方針が対応している。対応するセキュリティー対策方針が満たされることにより、脅威に対抗できる。

全ての前提条件は表 13に示すように、いずれかのセキュリティー対策方針が対応している。対応するセキュリティー対策方針が満たされることにより、前提条件は保証される。

TOE に対する脅威および前提条件がセキュリティー対策方針によって、対策されている根拠を、表 14に示す。

表14 セキュリティー対策方針の十分性

脅威・ 前提条件	セキュリティー対策方針
T.RECOVER	この脅威に対抗するには、TOE のセキュリティー機能を有効にし、かつ、その機能が完全に実行されるように運用すること、および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再生を不可能にする事が必要であり、以下の対策方針によって対抗する。 **O.RESIDUAL**、および **O.DECIPHER** により、TOE は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再生を不可能にする。 プリンター機能を利用する場合に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には印刷データが含まれている。この印刷データは、テキストで構成されている場合があり、比較的解析が容易である。このため、**O.DECIPHER** によってハードディスク装置に蓄積される文書データを暗号化した上で、更に **O.RESIDUAL** により上書き消去することによって、TOE はハードディスク装置に蓄積する利用済み文書データの再生を不可能にする。 これらの対策方針により、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再生を不可

	能にする。 **OE.FUNCON** により、機械管理者は TOE セキュリティー機能(ハードディスク蓄積データ上書き消去機能、およびハードディスク蓄積データ暗号化機能)を有効な状態で運用する。 この対策方針により、TOE のセキュリティー機能は有効にされ、かつ、その機能が完全に実行されるように運用できる。 以上により、**T.RECOVER** に対抗することができる
T.CONFDATA	この脅威に対抗するためには、TOE 設定データの変更を認証された機械管理者に限定する事が必要であり、以下の対策方針によって対抗する。 **O.MANAGE** により、認証された機械管理者だけが、TOE 設定データの変更が可能となる。 この対策方針により、TOE 設定データを変更できる者は、認証された機械管理者だけに限定されるため、**T.CONFDATA** に対抗することができる。
A.SECMODE	**OE.AUTH** により、機械管理者は「機械管理者パスワード」の推測や暴露を防ぐ様に管理し、「機械管理者パスワード」を 7 文字～12 文字の値に設定し、「カストマーエンジニアの操作制限機能」および「パスワードの使用」が機能する様に設定された状態で、「機械管理者 ID の認証失敗によるアクセス拒否」を 5 回に設定し TOE の運用を行う。。 これらの対策方針により、**A.SECMODE** を実現できる。
A.ADMIN	**OE.ADMIN** により、組織の責任者は、機械管理者の適切な人選を行うと共に、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.NET	本条件は、ApeosPort/DocuCentre 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。 ApeosPort/DocuCentre 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 ApeosPort/DocuCentre 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。 この対策方針により、**A.NET** を実現できる。

8.2. セキュリティー要件根拠

8.2.1. セキュリティー機能要件根拠

(1) 必要性

セキュリティー機能要件とセキュリティー対策方針の関係を表 15に示す。

TOE セキュリティー機能要件で、セキュリティー対策方針を実現するために対応しないものはない。

全てのセキュリティー機能要件は、少なくとも1つのセキュリティー対策方針に対応している。

TOE に不正なサブジェクトは存在しない。

表15 セキュリティー機能要件とセキュリティー対策方針の対応

セキュリティー対策方針 / セキュリティー機能要件	O.RESIDUAL	O.MANAGE	O.DECIPHER
FCS_CKM.1			○
FCS_COP.1			○
FDP_RIP.1	○		
FIA_AFL.1		○	
FIA_UID.2		○	
FIA_UAU.2		○	
FIA_UAU.7		○	
FMT_MOF.1 (1)		○	
FMT_MOF.1 (2)		○	
FMT_MOF.1 (3)		○	
FMT_MTD.1(1)		○	
FMT_MTD.1(2)		○	
FMT_MTD.1(3)		○	
FMT_SMF.1		○	
FMT_SMR.1		○	
FPT_RVM.1	○	○	○

○: TOE に対する機能要件

(2) 十分性

TOE に対する全てのセキュリティー対策方針が、機能要件によりその対策が保証されていることを表 16示す。

表16 対策方針の十分性

セキュリティー対策方針	機能要件	十分性
O.RESIDUAL	**FDP_RIP.1** **FPT_RVM.1**	**FDP_RIP.1** により、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の以前の情報の内容を利用できなくする。 **FPT_RVM.1** により、TOE セキュリティー機能が確実に呼び出され、バイパスされることはない。 これらのセキュリティー機能要件によって、TOE は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再生を上書き消去により不可能にするというセキュリティー対策方針 **O.RESIDUAL** を実現できる。

O.DECIPHER	FCS_CKM.1 FCS_COP.1 FPT_RVM.1	FCS_CKM.1 により、指定された暗号鍵長に従う暗号鍵が生成される。また、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ハードディスク装置に蓄積される文書データが暗号化され、読み出し時に復号される。 FPT_RVM.1 により、TOE セキュリティー機能が確実に呼び出され、バイパスされることはない。 これらのセキュリティー機能要件によって、TOE は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解析を暗号化により困難にするというセキュリティー対策方針 O.DECIPHER を実現できる。
O.MANAGE	FIA_AFL.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FMT_MOF.1 (1) FMT_MOF.1 (2) FMT_MOF.1 (3) FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_SMF.1 FMT_SMR.1 FPT_RVM.1	FIA_AFL.1 により、機械管理者が設定回数認証に失敗した場合、電源の OFF/ON が必要になり連続した攻撃が防止される。 FIA_UID.2 および FIA_UAU.2 により、機械管理者が識別･認証されていることが必要な操作パネル及び機械管理者クライアントの WEB ブラウザによる操作の前には識別･認証が行われる。 なお、FIA_UAU.7 により、認証フィードバックは保護されるので、認証情報の不正漏洩は防止される。 FMT_MTD.1(1)、 FMT_MTD.1(2) および FMT_MTD.1(3)により、TOE 設定データである「パスワードの使用設定」、「機械管理者 ID の認証失敗によるアクセス拒否」、「ハードディスク蓄積データ暗号化キー」、「カストマーエンジニアの操作制限機能設定」、の設定値の問い合わせ、および改変を機械管理者だけに制限し、FMT_MOF.1 (1) により、TOE セキュリティー機能である「ハードディスク蓄積データ上書き消去機能」の上書き消去回数の設定、機能の停止、および機能の動作を機械管理者に限定しているので、「ハードディスク蓄積データ上書き消去機能」は機械管理者しか設定できない。さらに、FMT_MOF.1 (2) により、TOE セキュリティー機能である「ハードディスク蓄積データ暗号化機能」および機能の動作を機械管理者に限定しているので、「ハードディスク蓄積データ暗号化機能」は機械管理者しか設定できない。 FMT_MOF.1 (3) により、TOE セキュリティー機能である「機械管理者認証機能」のパスワードの使用の設定を機械管理者に限定しているので、「機械管理者認証機能」のパスワードの使用は機械管理者しか設定できない。 なお、FMT_SMR.1 により、特権を持つ利用者として機械管理者の役割を維持する事により、セキュリティーに関する役割を機械管理者に特定する。 また、FMT_SMF.1 により、機械管理者パスワードを管理するためのセキュリティー管理機能を提供する。 FPT_RVM.1 により、TOE セキュリティー機能が確実に呼び出され、バイパスされることはない。 これら、セキュリティー機能要件によって、O.MANAGE を実現できる。

(3) セキュリティー機能強度レベルの妥当性

本 TOE が想定する攻撃者の攻撃力は低レベルである。したがって、最小機能強度レベルが"SOF-基本"であることは妥当である。FIA_AFL.1、FIA_UAU.2 の全ての確率的・順列的メカニズムが SOF 基本であるので、TOE の必要とするセキュリティー機能強度を満たしている。

(4) セキュリティー機能要件の依存性

セキュリティー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を表 17に示す。

表17 機能要件の依存性

コンポーネント	依存先	依存しないコンポーネント
FCS_CKM.1	FCS_COP.1	FCS_CKM.4 暗号鍵は、ApeosPort/DocuCentre 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、

		ApeosPort/DocuCentre 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がない。 よって FCS_CKM.4 への依存性を満たす必要はない。 FMT_MSA.2 暗号鍵は、機械管理者により設定された TOE 設定データである「ハードディスク蓄積データ暗号化キー」を元に、TOE が自動的に 128 ビット固定の鍵長の暗号鍵を生成する。 この TOE により自動生成される暗号鍵の鍵長は、128 ビット固定であり、セキュアな値だけを受け入れることを保証する必要はない。TOE は自動生成した暗号鍵を常に使用し、鍵長以外のセキュリティー属性は存在しない。 よって FMT_MSA.2 への依存性は満たす必要はない。
FCS_COP.1	FCS_CKM.1	FCS_CKM.4 暗号鍵は、ApeosPort/DocuCentre 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、ApeosPort/DocuCentre 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がない。 よって FCS_CKM.4 への依存性を満たす必要はない。 FMT_MSA.2 暗号鍵は、機械管理者により設定された TOE 設定データである「ハードディスク蓄積データ暗号化キー」を元に TOE が自動的に 128 ビット固定の鍵長の暗号鍵を生成する。 この TOE により自動生成される暗号鍵の鍵長は、128 ビット固定であり、セキュアな値だけを受け入れることを保証する必要はない。TOE は自動生成した暗号鍵を常に使用し、鍵長以外のセキュリティー属性は存在しない。 よって、FMT_MSA.2 への依存性は満たす必要はない。
FDP_RIP.1	なし	なし
FIA_AFL.1	FIA_UAU.2	FIA_UAU.1 FIA_UAU.2 は、FIA_ UAU.1 の上位階層のセキュリティー機能要件であるため、FIA_ UAU.1 への依存性は満たされる。
FIA_UID2	なし	なし
FIA_UAU.2	FIA_UID.2	FIA_UID.1 FIA_UID.2 は、FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満たされる。
FIA_UAU.7	FIA_UID.2	FIA_UID.1 FIA_UID.2 は、FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満たされる。
FMT_MOF.1 (1)	FMT_SMF.1 FMT_SMR.1	なし
FMT_MOF.1 (2)	FMT_SMF.1 FMT_SMR.1	なし
FMT_MOF.1 (3)	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	なし
FMT_SMF.1	なし	なし
FMT_SMR.1	FIA_UID.2	FIA_UID.1 FIA_UID.2 は、FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満たされる。
FPT_RVM.1	なし	なし

(5) セキュリティー機能要件の相互作用

表 18に、セキュリティー機能要件の相互作用について検証する。

表18 セキュリティー機能要件の相互作用

セキュリティー機能要件	迂回	非活性化
FCS_CKM.1	FPT_RVM.1	FMT_MOF.1 (2)
FCS_COP.1	FPT_RVM.1	FMT_MOF.1 (2)
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1 (1)
FIA_AFL.1	FPT_RVM.1	N/A
FIA_UID.2	FPT_RVM.1	N/A
FIA_UAU.2	FPT_RVM.1	FMT_MOF.1 (3)
FIA_UAU.7	FPT_RVM.1	N/A
FMT_MOF.1 (1)	N/A	N/A
FMT_MOF.1 (2)	N/A	N/A
FMT_MOF.1 (3)	N/A	N/A
FMT_MTD.1(1)	N/A	N/A
FMT_MTD.1(2)	N/A	N/A
FMT_MTD.1(3)	N/A	N/A
FMT_SMF.1	N/A	N/A
FMT_SMR.1	N/A	N/A
FPT_RVM.1	N/A	N/A

N/A: 相互サポートを実施するセキュリティー機能要件はない。

〇迂回

FPT_RVM.1

TOE セキュリティー機能（FCS_CKM.1, FCS_COP.1）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別のモジュールへの置換は不可能であり、また常に実行される構造を築いているため、暗号鍵生成、及び暗号操作を迂回することはできず、非バイパス性を確保している。

TOE セキュリティー機能（FDP_RIP.1）は、独自のソフトウエアで構成されており別のモジュールへの置換は不可能である。また、電源断などにより上書き消去が中断した場合には、起動時に上書き消去を再実行する仕組みを築いており、非バイパス性を確保している。

TOE セキュリティー機能（FIA_AFL.1）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別のモジュールへの置換は不可能である。また、一旦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しないので、非バイパス性を確保している。

TOE セキュリティー機能（FIA_UID.2,FIA_UAU.2,FIA_UAU.7）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別のモジュールへの置換は不可能であり、また TOE 設定データをアクセスするときはには、必ず識別認証の機能が実行されるため、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できず、非バイパス性を確保している。

〇非活性化

FMT_MOF.1 (1)

ハードディスク蓄積データ上書き消去機能 (FDP_RIP.1)は、FMT_MOF.1 (1)により、機械管理者以外の利用者の非活性化行為から保護されることを保証する。

FMT_MOF.1 (2)

ハードディスク蓄積データ暗号化機能(FCS_CKM.1, FCS_COP.1)は、FMT_MOF.1 (2) により、機械管理者以外の利用者の非活性化行為から保護されることを保証する。

FMT_MOF.1 (3)

機械管理者認証機能(FIA_UAU.2)は、FMT_MOF.1 (3) により、機械管理者以外の利用者の非活性化行為から保護されることを保証する。

8.2.2. セキュリティー保証要件根拠

攻撃者は、低レベルの攻撃力を持ち、操作パネル及び機械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を行う。このため、TOE は、不特定者からの低レベルの攻撃に対抗する必要があり、評価保証レベル EAL2 が妥当といえる。

8.3. TOE 要約仕様根拠

8.3.1. 機能要約仕様根拠

(1) 必要性

セキュリティー機能要件と TOE セキュリティー機能との対応を表 19に示す。

TOE セキュリティー機能で、セキュリティー機能要件を実現するために対応しないものはない。

全ての TOE セキュリティー機能は、セキュリティー機能要件を実現するために必要である。

表19 セキュリティー機能要件と TOE セキュリティー機能の対応

TOE セキュリティー機能 / セキュリティー機能要件	SF.OVERWRITE	SF.ENCRYPTION	SF. MANAGE	SF. CEREST
FCS_CKM.1		○		
FCS_COP.1		○		
FDP_RIP.1	○			
FIA_AFL.1			○	
FIA_UID.2			○	
FIA_UAU.2			○	
FIA_UAU.7			○	
FMT_MOF.1 (1)			○	
FMT_MOF.1 (2)			○	
FMT_MOF.1 (3)			○	
FMT_MTD.1(1)			○	
FMT_MTD.1(2)			○	
FMT_MTD.1(3)				○
FMT_SMF.1			○	
FMT_SMR.1			○	
FPT_RVM.1	○	○	○	

○: 対象のセキュリティー機能要件を満たすセキュリティー機能である事を示す。

(2) 十分性

TOE のセキュリティー機能要件が、TOE のセキュリティー機能により十分に実現されていることを表 20に示す。

表20 セキュリティー機能要件の十分性

機能要件	セキュリティー機能
FCS_CKM.1	SF.ENCRYPTION により、TOE は機械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オリジナルの 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、富士ゼロックスオリジナルの 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。 このセキュリティー機能により、暗号鍵生成 FCS_CKM.1 は保証できる。
FCS_COP.1	SF.ENCRYPTION により、TOE は自動生成された暗号鍵を使用して、ハードディスク装置に蓄積される文書データを暗号化する。 このセキュリティー機能により、暗号操作 FCS_COP.1 は保証できる。
FDP_RIP.1	SF.OVERWRITE により、TOE は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。 SF.OVERWRITE は上書きの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)の選択ができる。 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、セキュリティー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回とする。1回の上書き消去回数は、処理速度低下の影響が少なく、かつデータを再生しようとする低レベルの攻撃に対抗できるため、妥当な回数である。 セキュリティー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。 このセキュリティー機能により、サブセット残存情報保護 FDP_RIP.1 は保証できる。
FIA_AFL.1	SF. MANAGE により、TOE は、機械管理者が設定された回数、認証に失敗すると認証を拒否する。 このセキュリティー機能により、認証失敗時の取り扱い FIA_AFL.1 は保証できる。
FIA_UID.2	SF. MANAGE により、TOE は、機械管理者の操作パネル及び機械管理者クライアントの WEB ブラウザからの操作を許可する前に機械管理者に User ID を入力させ、入力された機械管理者名が TOE に登録されている機械管理者の User ID 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。 このセキュリティー機能により、アクション前の利用者識別 FIA_UID.2 は保証できる。
FIA_UAU.2	SF. MANAGE により、TOE は、機械管理者の操作パネル及び機械管理者クライアントの WEB ブラウザからの操作を許可する前に、機器管理者にパスワードを入力させ、入力されたパスワードが TOE に登録されている「機械管理者パスワード」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。このセキュリティー機能により、アクション前の利用者認証 FIA_UAU.2 は保証できる。
FIA_UAU.7	SF. MANAGE により、TOE は、機械管理者の認証時に、機械管理者パスワードとして入力された文字数と同数の`*`文字を操作パネル及び機械管理者クライアントの WEB ブラウザに表示する。 このセキュリティー機能により、保護された認証フィードバック FIA_UAU.7 は保証できる。
FMT_MOF.1 (1)	SF. MANAGE により、TOE は、認証された機械管理者に、TOE 設定データ「ハードディスク蓄積データ上書き消去機能」の変更を許可する。このセキュリティー機能により、TOE 設定データ「ハードディスク蓄積データ上書き消去機能」の変更は機械管理者に限定されるので、セキュリティー機能のふるまいの管理(1) FMT_MOF.1 (1) は保証できる。
FMT_MOF.1 (2)	SF. MANAGE により、TOE は、認証された機械管理者に、TOE 設定データ「ハードディスク蓄積データ暗号化機能」の変更を許可する。このセキュリティー機能により、TOE 設定データ「ハードディスク蓄積データ暗号化機能」の変更は機械管理者に限定されるので、セキュリティー機能のふるまいの管理(2) FMT_MOF.1 (2) は保証できる。
FMT_MOF.1 (3)	SF. MANAGE により、TOE は、認証された機械管理者に、TOE セキュリティ機能「機械管理者認証機能」のふるまいの決定に関係する機械管理者パスワードの定義と変更を許可する。このセキュリティー機能により、セキュリティー機能「機械管理者認証機能」の変更は機械管理者に限定されるので、セキュリティー機能のふるまいの管理(3) FMT_MOF.1 (3) は保証できる。
FMT_MTD.1(1)	SF. MANAGE により、TOE は、認証された機械管理者に、TOE 設定データ「パスワードの使用設定」、「機械管理者 ID の認証失敗によるアクセス拒否」の変更を許可する。このセキュリティー機能により、TOE 設定データ「パスワードの使用設定」、「機械管理者 ID の認証失敗によるアクセス拒否」の変更は機械管理者に限定されるので、TSF データの管理 FMT_MTD.1(1)は保証できる。

FMT_MTD.1(2)	SF. MANAGE により、TOE は、認証された機械管理者に、TOE 設定データ「ハードディスク蓄積データ暗号化キー」の変更を許可する。このセキュリティー機能により、TOE 設定データ、「ハードディスク蓄積データ暗号化キー」の変更は機械管理者に限定されるので、TSF データの管理 FMT_MTD.1(2)は保証できる。
FMT_MTD.1(3)	SF. CEREST により、TOE は、カストマーエンジニアが TOE 設定データ「カストマーエンジニアの操作制限機能設定」の変更をすることができないようにする。このセキュリティー機能により、TOE 設定データ「カストマーエンジニアの操作制限機能設定」の変更は機械管理者に限定されるので、TSF データの管理 FMT_MTD.1(3)は保証できる。
FMT_SMF.1	SF. MANAGE により、TOE は、認証された機械管理者に、TOE 設定データの変更を許可する。
FMT_SMR.1	SF.MANAGE により、機械管理者の役割を維持し、利用者をその役割に関連付けている。 このセキュリティー機能により、セキュリティー管理役割 FMT_SMR.1 は保証できる。
FPT_RVM.1	SF.ENCRYPTION, SF.OVERWRITE, SF.MANAGE, SF.CEREST 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。 これらのセキュリティー機能により、TSP の非バイパス性 FPT_RVM.1 は保証できる。

(3) セキュリティー機能強度

TOE セキュリティー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機械管理者認証機能(SF.MANAGE)である。本機能の機能強度は SOF-基本であり、「5.4TOE セキュリティー機能強度主張」で主張した最小機能強度レベル SOF-基本を満足している。

8.3.2. 保証手段根拠

保証手段が必要かつ十分であることの根拠を記述する。

(1) 必要性

6.2に記述した全ての保証手段は、セキュリティー保証要件を実現するために必要であることを以下に示す。

全ての保証手段は、EAL2 のセキュリティー保証要件を実現するために必要である。

表21 保証手段とセキュリティー保証要件の対応

	AS.CONFIGURATION	AS.CONFIGURATIONLIST	AS.DELIVERY	AS.FUNCSPEC	AS.HIGHLDESIGN	AS.REPRESENT	AS.GUIDANCE	AS.TEST	AS.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									○

○: 対象のセキュリティー保証要件を満たす保証手段である事を示す。

(2) 十分性

各セキュリティー保証要件に対応する保証手段を示し、その実現には十分であることを示す。

①ACM_CAP.2 認可の管理

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のバージョンが識別できる命名規約、構成要素の一覧表、各構成要素の一意の識別子といった要件を満足することができる。

- 「C7550 I シリーズ 構成管理説明書」(AS. CONFIGURATION)
- 「C7550 I シリーズ TOE 構成リスト」(AS. CONFIGURATIONLIST)

② ADO_DEL.1 配付手続き

【対応する保証手段】

以下の文書が準備されている。これにより、TOE の識別と輸送中の完全性の維持、配布手続きの詳細、機械管理者の TOE の確認方法といった要件を満足することができる。

- 「海外機 配布、導入、運用手続き説明書」(AS. DELIVERY)
- 「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」(AS. GUIDANCE)

③ ADO_IGS.1 設置、生成、及び立ち上げ手順

【対応する保証手段】

以下の文書が準備されている。これにより、TOE の設置/起動の手順と確認方法、例外事象への対処といった要件を満足することができる。

- 「海外機 配布、導入、運用手続き説明書」(AS. DELIVERY)
- 「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」(AS. GUIDANCE)

④ ADV_FSP.1 非形式的機能仕様

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のセキュリティー機能と外部インタフェースの一貫した完全なる記述、外部インタフェースの詳細記述といった要件を満足することができる。

- 「C7550 I シリーズ 機能仕様書」(AS.FUNCSPEC)

⑤ ADV_HLD.1 セキュリティー実施上位レベル設計

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のセキュリティー機能の構造に関する一貫した記述、サブシステム間のインタフェースの識別と記述、セキュリティー機能を提供するサブシステムの識別といった要件を満足することができる。

・ 「C7550 I シリーズ 上位レベル設計書」(AS.HIGHLDESIGN)

⑥ ADV_RCR.1 非形式的対応の実証

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のセキュリティー機能の各レベル(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った要件を満足することができる。

・ 「C7550 I シリーズ 対応分析書」(AS.REPRESENT)

⑦ AGD_ADM.1 機械管理者ガイダンス

【対応する保証手段】

以下の文書が準備されている。これにより、機械管理者が利用可能な管理機能とインタフェースの記述、機械管理者の責任や行為について前提条件、警告メッセージに対する対策方法といった要件を満足することができる。

・ 「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」(AS. GUIDANCE)

⑧ AGD_USR.1 利用者ガイダンス

【対応する保証手段】

以下の文書が準備されている。これにより、一般利用者が利用可能なセキュリティー機能とインタフェースの記述、一般利用者の責任や行為について前提条件、警告メッセージに対する対策方法といった要件を満足することができる。

・ 「ApeosPort C7550 I/C6550 I/C5540 I, ApeosPort 750 I/650 I, ApeosPort 550 I/450 I/350 I, DocuCentre C7550 I/C6550 I/C5540 I/, DocuCentre 750 I/650 I, DocuCentre 550 I/450 I Security Kit Supplementary Guide」(AS. GUIDANCE)

⑨ ATE_COV.1 カバレージの分析

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のセキュリティー機能のテストの十分性/完全性の要件を満足することができる。

・ 「C7550 I シリーズテスト計画書 兼 報告書」(AS.TEST)

⑩ ATE_FUN.1 機能テスト

【対応する保証手段】

以下の文書が準備されている。これにより、TOE のセキュリティー機能が確実にテストされているという要件を満足することができる。

・ 「C7550 I シリーズテスト計画書 兼 報告書」（AS.TEST）

⑪ ATE_IND.2 独立テスト・サンプル

【対応する保証手段】

以下の文書が準備されている。これにより、TOE セキュリティー機能のテスト環境の再現およびテスト資材の提供という要件を満足することができる。

・ 「C7550 I シリーズテスト計画書 兼 報告書」（AS.TEST）

⑫ AVA_SOF.1 セキュリティー機能強度評価

以下の文書が準備されている。これにより、TOE のセキュリティー強度の十分性という要件を満足することができる。

・「C7550 I シリーズ 脆弱性分析書」（AS.VULNERABILITY）

⑬ AVA_VLA.1 開発者脆弱性分析

【対応する保証手段】

以下の文書が準備されている。これにより、TOE の識別された脆弱性が想定環境で悪用されないことの確認という要件を満足することができる。

・ 「C7550 I シリーズ 脆弱性分析書」（AS.VULNERABILITY）

8.4. PP 主張根拠

適合を主張する PP はない。