THE DOCUMENT COMPANY
FUJI XEROX

# セキュリティーターゲット
# 富士ゼロックス DocuCentre 719/659/559 シリーズ
# データセキュリティーキット

6 August 2004

Version: V1.12

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 | 2003 年 11 月 25 日 | V1.00 | 初版 |
| 2 | 2003 年 12 月 2 日 | V1.01 | 以下の記載を修正<br>1.2 ST 概説<br>5.3 IT 環境セキュリティー機能要件<br>8.2 セキュリティー要件根拠<br>保護資産に関する説明を第 2 章に移動 |
| 3 | 2003 年 12 月 10 日 | V1.02 | 所見報告書 ASE007-01、ASE008-01、ASE009-01、ASE010-01 に対応して修正 |
| 4 | 2004 年 1 月 16 日 | V1.03 | 所見報告書 ASE011-01、ASE012-01、ASE013-01、ASE014-01、ADV004－01 に対応して修正 |
| 5 | 2004 年 2 月 3 日 | V1.04 | 所見報告書 ASE015-01 に対応して修正 |
| 6 | 2004 年 2 月 17 日 | V1.05 | 全体的に見直し実施 |
| 7 | 2004 年 2 月 26 日 | V1.06 | 全体的に見直し実施 |
| 8 | 2004 年 3 月 25 日 | V1.07 | 全体的に見直し実施 |
| 9 | 2004 年 4 月 2 日 | V1.08 | 所見報告書 ASE019-01 に対応して修正 |
| 10 | 2004 年 4 月 15 日 | V1.09 | 所見報告書 ASE020-01 に対応して修正 |
| 11 | 2004 年 4 月 26 日 | V1.10 | 所見報告書 ADV009-01 に対応して修正、8.2 セキュリティー要件根拠修正 |
| 12 | 2004 年 6 月 7 日 | V1.11 | 所見報告書 ASE021-01 に対応して修正 |
| 13 | 2004 年 8 月 6 日 | V1.12 | 指摘に対応して修正 |
| 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** | DocuCentre 719/659/559 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** | V1.12 |
| **作成者名** | 富士ゼロックス株式会社 |
| **作成日** | 2004 年 8 月 6 日 |
| **CC 識別** | Common Criteria for Information Technology Security Evaluation, Version2.1, 1999/8 |
| **PP 識別** | なし |
| **キーワード** | デジタル複写機、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、上書き消去、暗号 |

### (2) TOE 識別

| | |
|---|---|
| **TOE 識別** | DocuCentre719/659/559 シリーズ データセキュリティーキット |
| **バージョン** | DC システム ROM バージョン V512<br>PESS システム ROM バージョン V3.0.4 |
| **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、デジタルコピー機能、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「DocuCentre 719CP」、「DocuCentre 659CP」、「DocuCentre 559CP」およびデジタル複写機「DocuCentre 719」、「DocuCentre 659」、「DocuCentre 559」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、「DocuCentre 719CP」、「DocuCentre 659CP」、「DocuCentre 559CP」、「DocuCentre 719」、「DocuCentre 659」および「DocuCentre 559」によって処理された後、HDD 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。

- DC 用 HDD 蓄積データ上書き消去機能
- PESS 用 HDD 蓄積データ上書き消去機能
- PESS 用 HDD 蓄積データ暗号化機能

## 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) |
| DC | デジタルコピー(Digital Copire) |
| DC-SYS/IPS | デジタルコピー制御システム(DC Control System/Image Processing System) |
| EAL | 評価保証レベル (Evaluation Assurance Level) |
| HDD | ハードディスク装置(Hard Disk Drive) |
| 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) |
| MF-SYS | 複合機能制御システム (Multi Function Control System) |
| 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) |
| PESS | プリンターサブシステム(Printer Electorical Sub System) |
| 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。

**DocuCentre**

本 ST では「DocuCentre 719CP」、「DocuCentre 659CP」、「DocuCentre 559CP」、「DocuCentre 719」、「DocuCentre 659」および「DocuCentre 559」を総称して DocuCentre と表記する。

**一般利用者**

DocuCentre のデジタルコピー機能、プリンター機能およびスキャナー機能を利用する者。

**機械管理者**

DocuCentre の機械管理を行う者。

**サービスエンジニア**

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**

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、ネットワークスキャナーユーティリティを使用して DocuCentre のプリンター機能およびスキャナー機能を利用する。

**保守用クライアント**

サービスエンジニアが利用するクライアント。サービスエンジニアは、保守用クライアントを DocuCentre の保守用ローカルインタフェースに接続し、保守用クライアントにインストールされた、富士ゼロックスオリジナルの保守専用ソフトウエアを使用して、DocuCentre の保守を行う。

**保守用ローカルインタフェース**

DocuCentreと保守用クライアントを接続するための保守専用インタフェース。通常の保守を行うシリアルポートとプログラムダウンロード用のとパラレルポートがある。通信規約は、独自かつ非公開であり、一般のコンピュータを接続して保守を行うことはできない。

**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 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**

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**

デジタルコピー機能、およびスキャナ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 HDD 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**

DocuCentre の内部 HDD 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。

**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 DocuCentre の内部 HDD に一旦蓄積し、一般利用者が操作パネルより指示することにより印刷を開始するプリント方法。

以下の 3 種類がある。

・ セキュリティープリント

・ サンプルプリント

・ 拡張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。

**拡張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。

**HDD スプール**

スプール用内部記憶装置として、HDD 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**

デジタルコピー機能やスキャナー機能で 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。

**デジタルコピー機能**

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 DocuCentre の内部 HDD に蓄積され、指定部数回、内部 HDD から読み出されて印刷される

**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、DocuCentre の内部 HDD 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。

**拡張親展ボックス**

DocuCentre の HDD 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 DocuCentre のデジタルコピー機能、プリンター機能、スキャナー機能を利用する際に、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。

デジタル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 HDD に蓄積されるビットマップデータ。

**利用済み文書データ**

DocuCentre の内部 HDD に蓄積され、利用が終了した文書データ。

**制御データ**

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。

**HDD からの削除**

本 ST では HDD 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 HDD 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 HDD 上に残る。

**上書き消去**

HDD 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。

## 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

[補足-0210] CCIMB Interpretations-0210

# 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、HDD 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「DocuCentre 719CP」、「DocuCentre 659CP」、「DocuCentre 559CP」および、デジタル複写機「DocuCentre 719」、「DocuCentre 659」、「DocuCentre 559」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、デジタル複合機(デジタル複写機)単体でのスタンドアロン利用、またはデジタル複合機からの印刷およびデジタル複合機からの文書データの取り出しを要求する利用者クライアントが接続されたネットワーク環境での利用を想定している。(ただし、デジタル複写機として利用する場合は、スタンドアロン利用のみである。)

## 2.3. TOE の利用目的

TOE の利用目的は、DocuCentre の内部 HDD 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 1に DocuCentre 内の各ユニットと、TOE の物理的境界を示す。

DocuCentre は、デジタルコピー制御システム (DC-SYS/IPS)、プリンターサブシステム (PESS)、複合機能制御システム (MF-SYS) および操作パネルの 4 つの基板ユニットから構成される。

DC-SYS/IPS と MF-SYS の間および、MF-SYS と PESS の間、IIT と DC-SYS/IPS の間、IOT と DC-SYS/IPS 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。また、操作パネルと MF-SYS 間は、制御データの通信を行う内部インタフェースで構成されている。

操作パネルは、DocuCentre のデジタルコピー機能、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。

DC-SYS/IPS は、DocuCentre のデジタルコピー機能の制御を行うための回路基板であり、保守用ローカルインタフェース (RS232C, IEEE1284) を有し、IIT、IOT および MF-SYS が接続される。

MF-SYS は各ユニット間の文書データおよび制御データの通信を制御する回路基板であり、DC-SYS/IPS、PESS および操作パネルと接続される。

PESS は、プリンター機能およびスキャナー機能を制御する回路基板であり、ネットワークインタフェース (Ethernet) およびローカルインタフェース (IEEE1284、USB) を有する。

TOE は、DC-SYS/IPS に装着されている DC システム ROM の中に記録されているデジタルコピー制御機能のプログラムと PESS に装着されている PESS システム ROM の中に記録されているプリンター/スキャナー制御機能のプログラムである。

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

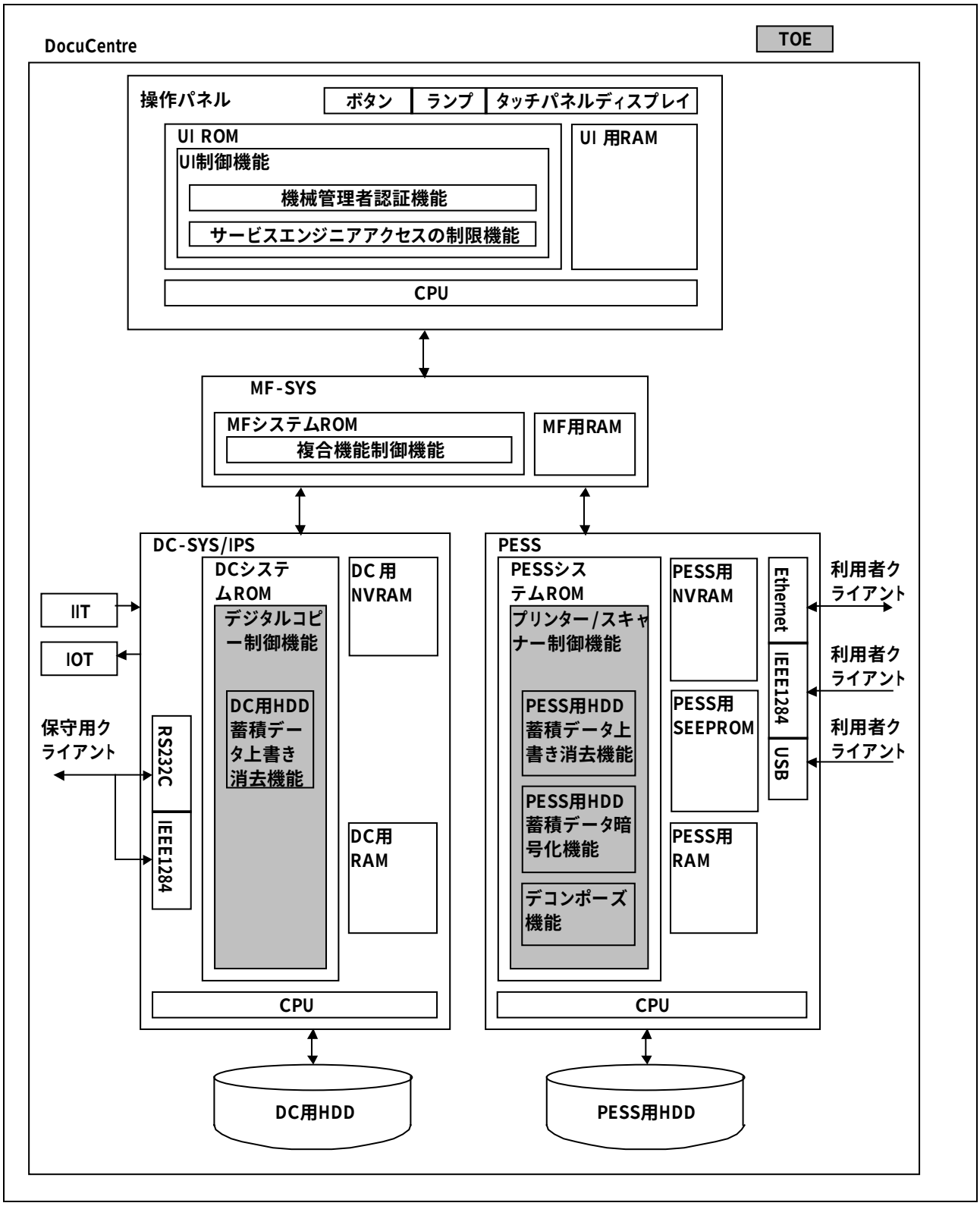


図 1 DocuCentre 内の各ユニットと、TOE の物理的境界

表1　TOE の物理的構成要素

| 構成要素 | 格納プログラム |
|---|---|
| DC システム ROM | デジタルコピー制御機能のプログラムを記録しており、以下の機能を提供する。<br>・ DC 用 HDD 蓄積データ上書き消去機能 |
| PESS システム ROM | プリンター/スキャナー制御機能のプログラムを記録しており、以下の機能を提供する。<br>・ PESS 用 HDD 蓄積データ上書き消去機能<br>・ PESS 用 HDD 蓄積データ暗号化機能<br>・ デコンポーズ機能 |

### 2.4.2.　論理的構成

DocuCentre の論理的構成を図 2 に示す。

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

デジタルコピー機能は、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 DocuCentre の内部 HDD 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(DocuCentre の内部メモリ、または内部 HDD)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 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、DocuCentre の内部 HDD 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すことができる。

DocuCentre は 2 つの内部 HDD を持つ。1つは、デジタルコピー機能によるコピー時、およびプリンター機能によるプリント時に、IOT から印刷するための文書データを蓄積するために使用される。これを DC 用 HDD と呼ぶ。

もう一つは、プリンター機能によるスプール方式によるプリント時、プリンター機能による蓄積プリント時、およびスキャナー機能によるスキャン時に、文書データを蓄積するために使用される。これを PESS 用 HDD と呼ぶ。

これら HDD 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 HDD 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 HDD に格納される利用済み文書データに対し、表 2に示すセキュリティー機能を提供する。

表2 TOE が提供するセキュリティー機能

| セキュリティー機能 | DC 用 HDD | PESS 用 HDD |
|---|---|---|
| DC 用 HDD 蓄積データ上書き消去機能 | ○ | × |
| PESS 用 HDD 蓄積データ上書き消去機能 | × | ○ |
| PESS 用 HDD 蓄積データ暗号化機能 | × | ○ |

○: 機能の実行対象となる HDD
×: 機能の実行対象ではない HDD

TOE の論理的構成要素は、DC-SYS/IPS 上の DC システム ROM によって提供されるデジタルコピー制御機能、PESS 上の PESS システム ROM によって提供されるプリンター/スキャナー制御機能、および、それぞれの TOE 設定データと利用済み文書データファイルである。

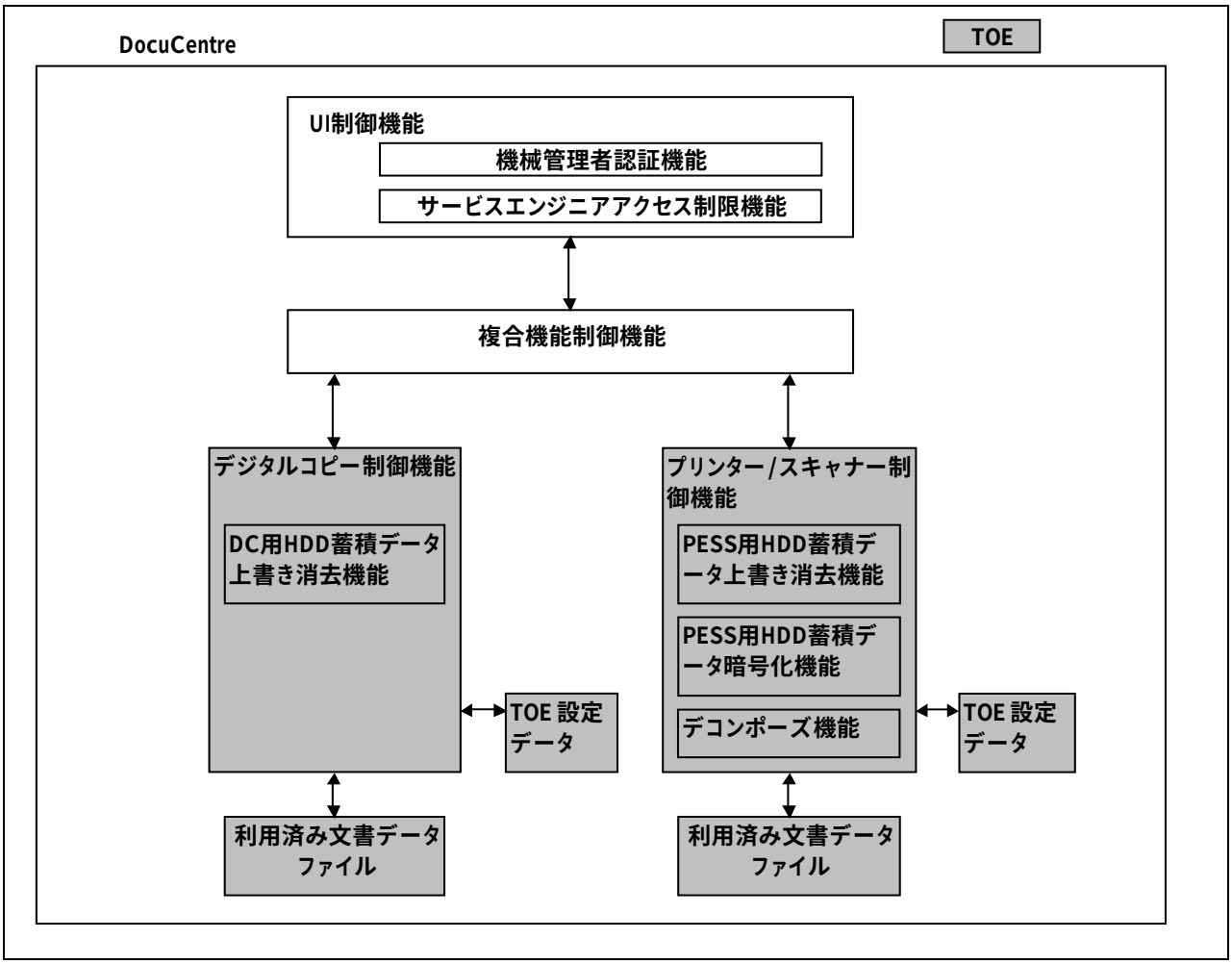


図2 TOE の論理的構成

表 3に DocuCentre の DC 用 NVRAM および PESS 用 SEEPROM に記憶される TOE 設定データを示す。

表3 DocuCentre の TOE 設定データと記録場所

| 機能 | 設定データ | 記憶場所 |
|---|---|---|
| デジタルコピー制御機能 | HDD 蓄積データ上書き消去機能設定 | DC 用 NVRAM |
| プリンター/スキャナー制御機能 | HDD 蓄積データ暗号化機能設定 | PESS 用 SEEPROM |
| | HDD 蓄積データ暗号化パスワード | |

HDD 蓄積データ上書き消去機能設定は、DC 用 HDD および PESS 用 HDD 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、デジタルコピー機能、プリンター機能、スキャナー機能の処理速度低下や、割り込みコピー禁止など制限事項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。HDD 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。HDD 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。

HDD 蓄積データ暗号化機能設定は、PESS 用 HDD 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。HDD 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。

HDD 蓄積データ暗号化パスワードは、HDD 蓄積データ暗号化機能設定が「する」の時に有効となり、PESS 用 HDD 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 桁の数字を設定できる。

また、TOE は以下の IT 環境の機能を利用している。

● 機械管理者認証機能
管理機能を使用するために機械管理者が DocuCentre にアクセスする際に、7～12 桁の数字で構成される機械管理者暗証番号を入力することによって、正しい機械管理者であることを確認する機能。

● サービスエンジニアアクセス制限機能
TOE 設定データの変更を機械管理者に限定する機能。
TOE のセキュリティー機能を利用しない場合に、サービスエンジニアアクセス制限機能の設定を「制限しない」に設定するとサービスエンジニアも TOE 設定データの変更が可能となる。

## 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 | DocuCentre を利用運用する組織の責任者 |
| 一般利用者 | DocuCentre が提供するデジタルコピー機能、プリンター機能およびスキャナー機能の利用者。 |
| 機械管理者 | DocuCentre の機械管理を行う者。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、DocuCentre の操作パネルから、管理機能にアクセスすることができる。 |
| サービスエンジニア | DocuCentre の修理/保守を行う富士ゼロックスのエンジニア。 |

## 2.6. TOE が保護する資産

TOE が保護する資産は、DocuCentre の DC 用 HDD、および PESS 用 HDD に蓄積された利用済み文書データと、DC 用 NVRAM 、および PESS 用 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、デジタルコピー機能、およびスキャナー機能により読み込まれた状態の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た状態の印刷データがある。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 4に示す。

表4 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.D (DC用HDDに蓄積された利用済み文書データ)** | [資産内容]<br>デジタルコピー機能利用時、もしくは、プリンター機能利用時、DC 用 HDD に蓄積される、利用済み文書データ。<br><br>[格納媒体]<br>DC 用 HDD 内に格納される。<br><br>[発生パターン]<br>デジタルコピー機能利用時<br>・ 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。<br>・ 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。<br>プリンター機能利用時<br>・ 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。<br>・ 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。 |
| **R.DOCDATA.P (PESS 用 HDD に蓄積された利用済み文書データ)** | [資産内容]<br>プリンター機能利用時、もしくは、スキャナー機能利用時、PESS 用 HDD に蓄積される、利用済み文書データ。<br><br>[格納媒体]<br>PESS 用 HDD 内に格納される。<br><br>[発生パターン]<br>プリンター機能利用時<br>・ HDD 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。<br>・ HDD 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。<br>・ HDD 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。<br>・ HDD 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 |

| | |
|---|---|
| | PESS 用 HDD 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。<br>・ 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。<br>・ 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。<br>・ 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。<br>スキャナー機能利用時<br>・ 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。<br>・ 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。<br>・ 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**<br>**(TOE 設定データ)** | [資産内容]<br>「HDD 蓄積データ上書き消去機能設定」、「HDD 蓄積データ暗号化機能設定」および「HDD 蓄積データ暗号化パスワード」。<br><br>[格納媒体]<br>「HDD 蓄積データ上書き消去機能設定」は DC-SYS/IPS の DC 用 NVRAM に格納されている。(注意)<br>「HDD 蓄積データ暗号化機能設定」および「HDD 蓄積データ暗号化パスワード」は PESS 用 SEEPROM に格納されている。(注意) |

(注意)

DocuCentre の DC 用 NVRAM と PESS 用 SEEPROM には、「HDD 蓄積データ上書き消去機能設定」、「HDD 蓄積データ暗号化機能設定」および「HDD 蓄積データ暗号化パスワード」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 |
|---|---|
| DC 用 HDD 蓄積データ上書き消去機能 | DocuCentre の DC 用 HDD 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。<br>電源断などで利用済み文書データが上書き未終了で HDD 内に残ってしまった場合、次回の電源投入時に自動的に HDD 全体を「HDD 蓄積データ上書き消去機能設定」に従い上書き消去する。 |
| PESS 用 HDD 蓄積データ上書き消去機能 | DocuCentre の PESS 用 HDD 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。<br>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「HDD 蓄積データ上書き消去機能設定」に従い上書き消去する。 |
| PESS 用 HDD 蓄積データ暗号化機能 | DocuCentre の PESS 用 HDD に蓄積された文書データを暗号化する機能。 |

### 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 |
|---|---|
| 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。 |

## 2.8. TOE 利用方法

TOE を利用するための設定は、機械管理者によって行われる。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暗証番号を入力し認証された後、以下設定項目の設定を行う。

- **機械管理者暗証番号の変更**

  デフォルト値以外の 7～12 桁の数字を設定する。

- **サービスエンジニアアクセス制限機能の設定**

  「制限する」に設定する。

- **HDD 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。

- **HDD 蓄積データ暗号化機能の設定**

  「する」に設定する。

- **HDD 蓄積データ暗号化パスワードの設定**

  12 桁の数字を設定する。(12 桁以下の数字が設定された場合、不足分は自動的に「0」が設定される。)

一般利用者が DocuCentre のデジタルコピー機能、プリンター機能およびスキャナー機能を利用する際、利用済み文書データは、「表 5 DocuCentre の各機能におけるデータの流れ」 に示す様に、DC 用 HDD および PESS 用 HDD 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 5に、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5 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 |
|---|---|---|---|
| デジタルコピー | 通常コピー | 制御データ | 操作パネル→MF-SYS→DC-SYS/IPS |
| | | 文書データ | IIT→DC-SYS/IPS→DC 用 HDD→DC-SYS/IPS→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→PESS→MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | 文書データ(印刷データ) | 利用者クライアント→PESS<br>↓(PESS 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) | PESS→MF-SYS→DC-SYS/IPS→DC 用 HDD→DC-SYS/IPS→IOT |
| | 通常プリント(HDD スプール) | 制御データ | 利用者クライアント→PESS→PESS 用 HDD→PESS→MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | 文書データ(印刷データ) | 利用者クライアント→PESS→PESS 用 HDD→PESS<br>↓(PESS 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<br>(ビットマップデータ) | PESS→MF-SYS→DC-SYS/IPS→DC 用 HDD→DC-SYS/IPS→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<br>利用者クライアント→PESS→PESS 用 HDD<br>②文書データのプリント出力<br>(操作パネルでの操作により起動される)<br>PESS 用 HDD→PESS→MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | 文書データ<br>(印刷データ) | ①文書データのディスク蓄積<br>利用者クライアント→PESS<br>↓(PESS 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<br>(ビットマップデータ) | PESS→PESS 用 HDD<br><br>②文書データのプリント出力<br>(操作パネルでの操作により起動される)<br>PESS 用 HDD→PESS→MF-SYS→DC-SYS/IPS→DC 用 HDD→DC-SYS/IPS→IOT |
| | 蓄積プリント(HDDスプール) | 制御データ | ①文書データのディスク蓄積<br>利用者クライアント→PESS→PESS 用 HDD→PESS→PESS 用 HDD<br>②文書データのプリント出力<br>(操作パネルでの操作により起動される)<br>PESS 用 HDD→PESS→MF-SYS→DC-SYS/IPS→DC-SYS/IPS→IOT |
| | | 文書データ<br>(印刷データ) | ①文書データのディスク蓄積<br>利用者クライアント→PESS→PESS 用 HDD→PESS<br>↓(PESS 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<br>(ビットマップデータ) | PESS→PESS 用 HDD<br><br>②文書データのプリント出力<br>(操作パネルでの操作により起動される)<br>PESS 用 HDD→PESS→MF-SYS→DC-SYS/IPS→DC 用 HDD→DC-SYS/IPS→IOT |
| スキャナー | スキャン蓄積 | 制御データ | 操作パネル→MF-SYS→DC-SYS/IPS<br>操作パネル→MF-SYS→PESS |
| | | 文書データ | IIT→DC-SYS/IPS→MF-SYS→PESS→PESS 用 HDD |
| | スキャン取り出し | 制御データ | 利用者クライアント→PESS |
| | | 文書データ | PESS 用 HDD→PESS→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→MF-SYS→DC-SYS/IPS<br>操作パネル→MF-SYS→PESS |

# 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 6に示す。

表6 前提条件

| 前提条件 | 内容 |
|---|---|
| A.SECMODE | <保護モード><br>機械管理者は、「機械管理者暗証番号」を 7 桁～12 桁の値に設定し、「サービスエンジニアアクセス制限機能」が動作する様に設定された状態で、TOE を運用するものとする。 |
| A.ADMIN | <管理者の信頼><br>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。 |

## 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 7に示す。

攻撃者は低レベルの攻撃力を持つものとする。

表7 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><br>一般利用者および TOE の非関連者が HDD 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<br>・非関連者 | R.DOCDATA.D<br>R.DOCDATA.P |
| T.CONFDATA | <TOE 設定データの不正アクセス><br>一般利用者および TOE の非関連者が、操作パネルから、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<br>・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 8に示す。

表8 TOE のセキュリティー対策方針

| | 説明 |
|---|---|
| O.RESIDUAL.D | TOE は、DC 用 HDD に蓄積された利用済み文書データの再生を不可能にしなければならない。 |
| O.RESIDUAL.P | TOE は、PESS 用 HDD に蓄積された利用済み文書データの再生を不可能にしなければならない。 |
| O.DECIPHER.P | TOE は、PESS 用 HDD に蓄積された利用済み文書データの解析を困難に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を表 9に示す。

表9 IT 環境のセキュリティー対策方針

| 対策方針 | 説明 |
|---|---|
| OE.MANAGE | UI 制御機能は、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。 |

### 4.2.2. 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 10に示す。

表10 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「機械管理者暗証番号」の推測や暴露を防ぐ様に管理しなくてはならない。<br>また、「機械管理者暗証番号」は 7 桁～12 桁の値に設定しなくてはならない。 |
| OE.FUNCON | 機械管理者は「HDD 蓄積データ上書き消去機能」、「HDD 蓄積データ暗号化機能」、および「サービスエンジニアアクセス制限機能」が動作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.POWEROFF | 組織の責任者は、一般利用者が DocuCentre の電源を Off する前に、実行中の処理がない事が確認し、実行中の処理がある場合は、その処理の終了後に電源を Off する様に、教育を行わなければならない。 |

# 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 アルゴリズム

[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 Standard)

[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]

PESS 用 HDD に蓄積される文書データの暗号化

PESS 用 HDD 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]**

DC 用 HDD に蓄積された利用済み文書データファイル

PESS 用 HDD 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 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11 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<br>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 | 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<br>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<br>ADV_ADM.1<br>AGD_USR.1<br>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<br>ADV_HLD.1 |
| | AVA_VLA.1 | 開発者脆弱性分析 | ADV_FSP.1<br>ADV_HLD.1<br>AGD_ADM.1<br>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を規定する。

### 5.3.1. クラス FIA： 識別と認証

**FIA_UID.2 アクション前の利用者識別**

下位階層: FIA_UID.1

FIA_UAU.2.1 **[詳細化： UI 制御機能]**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 **[詳細化： UI 制御機能]**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： 機械管理者暗証番号による]**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 **[詳細化： UI 制御機能]**は、**[詳細化： 操作パネルの機械管理者認証のための機械管理者暗証番号]**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]**

暗証番号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

### 5.3.2. 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 **[詳細化： UI 制御機能]**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]**

DC 用 HDD 蓄積データ上書き消去機能

PESS 用 HDD 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 **[詳細化： UI 制御機能]**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]**

PESS 用 HDD 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_MTD.1　TSF データの管理**

下位階層: なし

FMT_MTD.1.1 **[詳細化： UI 制御機能]**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]**

HDD 蓄積データ上書き消去機能設定

HDD 蓄積データ暗号化機能設定

HDD 蓄積データ暗号化パスワード

**[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_SMF.1 管理機能の特定**

下位階層: なし

FMT_SMF.1.1 **[詳細化: UI 制御機能]**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 12に示す管理項目を管理する機能

表12 管理項目を管理する機能

| 機能要件 | 管理要件 | 管理項目 |
|---|---|---|
| FIA_UID.2 | 利用者識別情報の管理 | なし |
| 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 | 機械管理者暗証番号 |
| 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_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 | 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<br>(機械管理者暗証番号を知るものだけが、機械管理者となれる。) |

FIA_UID.2 に関し、利用者識別する対象が管理者固定であり識別情報を管理する必要はないため、該当する管理項目はない。

FMT_MOF.1, FMT_MTD.1, FMT_SMR.1 に関し、唯一、機械管理者暗証番号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 **[詳細化: UI 制御機能]**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 **[詳細化： UI 制御機能]**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

## 5.4. 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。

セキュリティー機能強度主張の対象となるセキュリティー機能要件はない。

# 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。

- DC 用 HDD 蓄積データ上書き消去機能 (SF.OVERWRITE.D)
- PESS 用 HDD 蓄積データ上書き消去機能 (SF.OVERWRITE.P)
- PESS 用 HDD 蓄積データ暗号化機能 (SF.ENCRYPTION.P)

表 13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13 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.D | SF.OVERWRITE.P | SF.ENCRYPTION.P |
|---|---|---|---|
| FCS_CKM.1 | | | ○ |
| FCS_COP.1 | | | ○ |
| FDP_RIP.1 | ○ | ○ | |
| FPT_RVM.1 | ○ | ○ | ○ |

### 6.1.1. DC 用 HDD 蓄積データ上書き消去機能（SF.OVERWRITE.D）

この機能は、機械管理者により設定された「HDD 蓄積データ上書き消去機能設定」に従い、、DC 用 HDD 上の利用済み文書データ領域を表 14に示す方法により上書き消去する。

DC 用 HDD 上には、現在文書データが存在するか否かのフラグを持ち、システム起動時にこのフラグが文書データの存在する事を示している場合、TOE は、DC 用 HDD 全体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14 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<br>2 回目: 乱数<br>3 回目: 0 |

### 6.1.2. PESS 用 HDD 蓄積データ上書き消去機能（SF.OVERWRITE.P）

この機能は、機械管理者により設定された「HDD 蓄積データ上書き消去機能設定」に従い、PESS 用 HDD 上の利用済み文書データ領域を表 15に示す方法により上書き消去する。

PESS 用 HDD 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15 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<br>2 回目: 乱数<br>3 回目: 0 |

### 6.1.3. PESS 用 HDD 蓄積データ暗号化機能（SF.ENCRYPTION.P）

この機能は、機械管理者により設定された「HDD 蓄積データ暗号化機能設定」に従い、PESS 用 HDD に蓄積される文書データの暗号化および復号を行う。暗号鍵は機械管理者により設定された「HDD 蓄積データ暗号化パスワード」を使用し、起動時に富士ゼロックスオリジナルの FXOSENC アルゴリズムによって、128 ビットの暗号鍵生成を行う。（「HDD 蓄積データ暗号化パスワード」が同じであれば、同じ暗号鍵が生成される。）

TOE は、PESS 用 HDD 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、DocuCentre 内の PESS 用 RAM(揮発性 RAM)に記憶する。なお、暗号鍵は 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。

### 6.1.4. 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ない。

## 6.2. 保証手段

### 6.2.1. 構成管理説明書 (AS.CONFIGURATION)

「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. TOE 構成リスト (AS.CONFIGURATIONLIST)

「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. 配布、導入、運用手続き説明書 (AS.DELIVERY)

「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. 機能仕様書 (AS.FUNCSPEC)

「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. 上位レベル設様書 (AS.HIGHLDESIGN)

「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. 対応分析書 (AS.REPRESENT)

「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. DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編) (AS. GUIDANCE)

富士ゼロックスは、TOE の開発において、マニュアル(「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」)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

「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」は、機械管理者および一般利用者共通である。

「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」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. テスト計画書 (AS.TESTPLAN)

「テスト計画書」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「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

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. テスト結果報告書 (AS.TESTSPEC)

「テスト結果報告書」には、以下の内容が記述されている。

- テストの目的
- テストの実施方法
- テストにおける期待結果
- テストの実施日およびテスト実施者名
- テストの結果

対応するセキュリティー保証要件

- ATE_FUN.1

### 6.2.10. 脆弱性分析書 (AS.VULNERABILITY)

「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 の識別された脆弱性が問題とならないことを検証する。

- 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_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 16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 16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16 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.SECMODE | A.ADMIN |
|---|---|---|---|---|
| O.RESIDUAL.D | ○ | | | |
| O.RESIDUAL.P | ○ | | | |
| O.DECIPHER.P | ○ | | | |
| OE.MANAGE | | ○ | | |
| OE.AUTH | | | ○ | |
| OE.FUNCON | ○ | | ○ | |
| OE.ADMIN | | | | ○ |
| OE.POWEROFF | ○ | | | |

○: 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 16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 16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 17に示す。

表17 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 DC 用 HDD と PESS 用 HDD 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。<br>**O.RESIDUAL.D** により、TOE は DC 用 HDD 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。<br>**O.RESIDUAL.P**、および **O.DECIPHER.P** により、TOE は PESS 用 HDD 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。<br>DC 用 HDD に蓄積されている利用済み文書データは、ビットマップデータであり、富士ゼロックス独自方式で画像圧縮して記録されているためデータ自体の解析が困難であり、更に **O.RESIDUAL.D** により上書き消去することによって、データの再生を不可能にできる。一方、 |

| | |
|---|---|
| | PESS 用 HDD に蓄積されている利用済み文書データは、プリンター機能で使用される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.P** によって、PESS 用 HDD に蓄積される文書データを暗号化した上で、更に **O.RESIDUAL.D** により上書き消去することによって、TOE は PESS 用 HDD に蓄積する利用済み文書データの再生を不可能にする。<br>これらの対策方針により、DC 用 HDD および PESS 用 HDD 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。<br>**OE.FUNCON** により、機械管理者は TOE セキュリティー機能(DC 用 HDD 蓄積データ上書き消去機能、PESS 用 HDD 蓄積データ上書き消去機能、および PESS 用 HDD 蓄積データ暗号化機能)を有効な状態で運用する。<br>また、セキュリティー機能(DC 用 HDD 蓄積データ上書き消去機能、および PESS 用 HDD 蓄積データ上書き消去機能)の実行が電源断により途中終了しないように **OE.POWEROFF** により、組織の責任者は、処理が終了してから電源 Off するように一般利用者を教育する。<br>これらの対策方針により、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。<br>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。<br>**OE.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。<br>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「機械管理者暗証番号」を 7～12 桁の値に設定する。また **OE.FUNCON** により、機械管理者は「サービスエンジニアアクセス制限機能」が動作する様に設定された状態で TOE の運用を行う。<br>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。<br>この対策方針により、**A.ADMIN** 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 18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。

表18 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.D | O.RESIDUAL.P | O.DECIPHER.P | OE.MANAGE |
|---|---|---|---|---|
| FCS_CKM.1 | | | ○ | |
| FCS_COP.1 | | | ○ | |
| FDP_RIP.1 | ○ | ○ | | |
| FPT_RVM.1 | ○ | ○ | ○ | |
| FIA_UID.2 | | | | ● |
| FIA_UAU.2 | | | | ● |
| FIA_UAU.7 | | | | ● |
| FMT_MOF.1 (1) | | | | ● |
| FMT_MOF.1 (2) | | | | ● |
| FMT_MTD.1 | | | | ● |
| FMT_SMF.1 | | | | ● |
| FMT_SMR.1 | | | | ● |

○: TOE に対する機能要件
●: IT 環境に対する機能要件

#### (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 19に示す。

表19 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.D** | **FDP_RIP.1**<br>**FPT_RVM.1** | **FDP_RIP.1** により、DC 用 HDD 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。<br>**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。<br>これらのセキュリティー機能要件によって、TOE は DC 用 HDD 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というセキュリティー対策方針 **O.RESIDUAL.D** を実現できる。 |
| **O.RESIDUAL.P** | **FDP_RIP.1**<br>**FPT_RVM.1** | **FDP_RIP.1** により、PESS 用 HDD 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。<br>**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。<br>これらのセキュリティー機能要件によって、TOE は PESS 用 HDD 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というセキュリティー対策方針 **O.RESIDUAL.P** を実現できる。 |

| | | |
|---|---|---|
| **O.DECIPHER.P** | **FCS_CKM.1**<br>**FCS_COP.1**<br>**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 PESS 用 HDD 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。<br>**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。<br>これらのセキュリティー機能要件によって、TOE は PESS 用 HDD に蓄積された利用済み文書データの解析を困難にするというセキュリティー対策方針 **O.DECIPHER.P** を実現できる。 |
| **OE.MANAGE** | **FIA_UID.2**<br>**FIA_UAU.2**<br>**FIA_UAU.7**<br>**FMT_MOF.1 (1)**<br>**FMT_MOF.1 (2)**<br>**FMT_MTD.1**<br>**FMT_SMF.1**<br>**FMT_SMR.1** | **FIA_UID.2** および **FIA_UAU.2** により、DocuCentre の UI 制御機能によって、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による操作の前には識別/認証が行われる。<br>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。<br>**FMT_MTD.1** により、DocuCentre の UI 制御機能によって、TOE 設定データである「HDD 蓄積データ上書き消去機能設定」、「HDD 蓄積データ暗号化機能設定」、「HDD 蓄積データ暗号化パスワード」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 DC 用 HDD 蓄積データ上書き消去機能、PESS 用 HDD 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、「DC 用 HDD 蓄積データ上書き消去機能」と「PESS 用 HDD 蓄積データ上書き消去機能」の確実な実行が保証される。さらに、**FMT_MOF.1 (2)** により、TOE セキュリティー機能である PESS 用 HDD 蓄積データ暗号化機能の停止、および機能の動作を機械管理者に限定しているので、「PESS 用 HDD 蓄積データ暗号化機能」の確実な実行が保証される。<br>なお、**FMT_SMR.1** により、DocuCentre の UI 制御機能は、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。<br>また、**FMT_SMF.1** により、DocuCentre の UI 制御機能は、機械管理者暗証番号を管理するためのセキュリティー管理機能を提供する。<br>これら、セキュリティー機能要件によって、**OE.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。ただし、本 TOE には機能強度に関連するメカニズムはない。

### (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 20に示す。

表20 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<br>暗号鍵は、DocuCentre の起動時に生成され PESS 用 RAM(揮発性 RAM)に格納される。この暗号鍵は、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。<br>よって FCS_CKM.4 への依存性を満たす必要はない。<br>FMT_MSA.2<br>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「HDD 蓄積データ暗号化パスワード」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。<br>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。<br>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<br>暗号鍵は、DocuCentre の起動時に生成され PESS 用 RAM(揮発性 RAM)に格納される。この暗号鍵は、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。<br>よって FCS_CKM.4 への依存性を満たす必要はない。<br>FMT_MSA.2<br>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「HDD 蓄積データ暗号化パスワード」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。<br>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。<br>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_UID2 | なし | なし |
| FIA_UAU.2 | FIA_UID.2 | FIA_UID.1<br>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<br>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<br>FMT_SMR.1 | なし |
| FMT_MOF.1 (2) | FMT_SMF.1<br>FMT_SMR.1 | なし |
| FMT_MTD.1 | FMT_SMF.1<br>FMT_SMR.1 | なし |
| FMT_SMF.1 | なし | なし |
| FMT_SMR.1 | FIA_UID.2 | FIA_UID.1<br>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 21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21 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 | 防御を提供している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_UID.2 | N/A | N/A |
| FIA_UAU.2 | N/A | N/A |
| FIA_UAU.7 | N/A | N/A |
| FMT_MOF.1 (1) | N/A | N/A |
| FMT_MOF.1 (2) | N/A | N/A |
| FMT_MTD.1 | 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。

<u>○迂回</u>

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。

○非活性化

FMT_MOF.1 (1)

DC 用 HDD 蓄積データ上書き消去機能、および PESS 用 HDD 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)

PESS 用 HDD 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。

### 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 22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22 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.D | SF.OVERWRITE.P | SF.ENCRYPTION.P |
|---|---|---|---|
| FCS_CKM.1 | | | ○ |
| FCS_COP.1 | | | ○ |
| FDP_RIP.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 23に示す。

表23 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.P により、TOE は機械管理者により設定された「HDD 蓄積データ暗号化パスワード」を使用し、起動時に富士ゼロックスオリジナルの FXOSENC 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 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。<br>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.P により、TOE は自動生成された暗号鍵を使用して、PESS 用 HDD 内に蓄積される文書データを暗号化する。<br>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.D により、TOE は DC 用 HDD 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。<br>SF.OVERWRITE.P により、TOE は PESS 用 HDD 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。<br>SF.OVERWRITE.D、SF.OVERWRITE.P のいずれにおいても、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。<br>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。<br>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。<br>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。<br>これら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。 |
| FPT_RVM.1 | SF.ENCRYPTION.P, SF.OVERWRITE.D, SF.OVERWRITE.P 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。<br>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。 |

## 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表 24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24 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.TESTPLAN | AS.TESTSPEC | 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。
―: 対象のセキュリティー保証要件を満たすための保証手段が必要ない事を示す。

### (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。

- 「構成管理説明書」 (AS. CONFIGURATION)
- 「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。

- 「配布、導入、運用手続き説明書」 (AS. DELIVERY)
- 「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」 (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。

- 「配布、導入、運用手続き説明書」 (AS. DELIVERY)
- 「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」 (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。

- 「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。

- 「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。

- 「対応分析書」 (AS.REPRESENT)

**⑦ AGD_ADM.1　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、管理者が利用可能な管理機能とインタフェースの記述、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。

- 「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」 (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。

- 「DocuCentre 719/659/559 シリーズ取扱説明書 (データセキュリティーキット編)」 (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。

・ 「テスト計画書」 (AS.TESTPLAN)

**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。

・ 「テスト計画書」 (AS.TESTPLAN)

・ 「テスト結果報告書」 (AS.TESTSPEC)

**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。

・ 「テスト計画書」 (AS.TESTPLAN)

**⑫ AVA_SOF.1　セキュリティー機能強度評価**

本 TOE は、機能強度に関連するメカニズムを持たない。

よって、対象となる保証手段はない。

**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。

・ 「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。