認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日 (受付番号)	**平成20年2月22日** (IT**認証**8203)
認証番号	C0170
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	**富士ゼロックス** DocuCentre-**III** 3000/2000 **シリーズ コントローラソフトウェア**
TOE**のバージョン**	Controller ROM Ver 1.0.12
PP**適合**	**なし**
適合する保証パッケージ	EAL3
開発者	**富士ゼロックス株式会社**
評価機関の名称	**有限責任中間法人** IT**セキュリティセンター 評価部**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年6月13日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア」（以下「本TOE」という。）について、有限責任中間法人　ITセキュリティセンター　評価部（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である富士ゼロックス株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:　富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア

バージョン:　Controller ROM Ver.1.0.12

開発者:　富士ゼロックス株式会社

1.2.2 製品概要

本製品は、コピー機能、プリンター機能、スキャナー機能及びファクス機能を有するデジタル複合機（Multi Function Peripheral、略称MFP）「富士ゼロックス DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア」（以降、これら2機種の複合機を総称して「MFP」という）のオプション製品であるデータセキュリティキットのコントローラソフトウェアである。

データセキュリティキットは、MFPにより処理された後、内部ハードディスク装置

に蓄積された文書データを、不正な暴露から保護するための専用オプションである。

また、データセキュリティキットは、公衆電話回線網からファクス機能を踏み台に、内部ネットワーク上に存在する文書データ及びTOE設定データにアクセスする脅威からの保護も行う。

データセキュリティキットのコントローラソフトウェアが提供するセキュリティ機能を以下に示す。

・ハードディスク蓄積データ上書き消去機能
・ハードディスク蓄積データ暗号化機能
・システム管理者セキュリティ管理機能
・カストマーエンジニア操作制限機能
・ファクスフローセキュリティ機能

1.2.3 TOEの範囲と動作概要

本TOEの物理的範囲は、MFPのコントローラボードに装着されているController ROMの中に記録されているプログラム（コントローラソフトウェア）であり、図1-1にMFP内の各ユニット構成と、TOEの物理的範囲を示す。

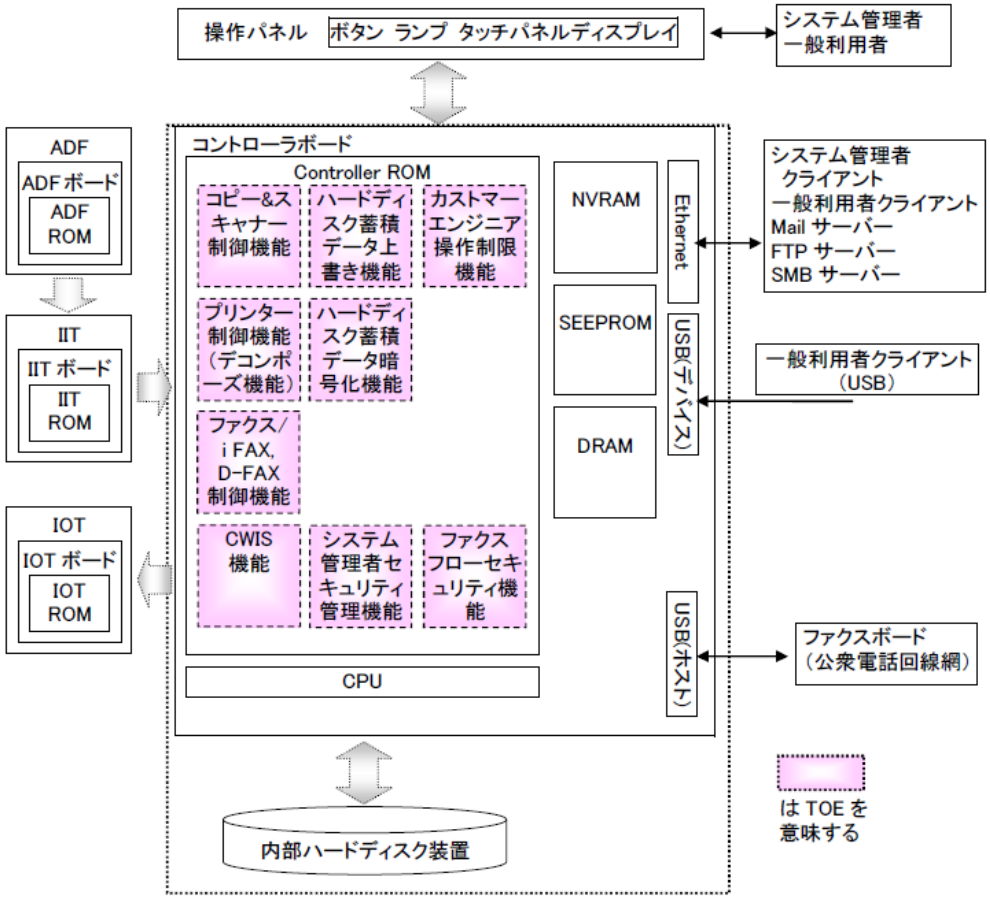

図1-1　TOEの物理的構成

また、TOEの機能を利用したMFPの利用イメージを以下の図に示す。

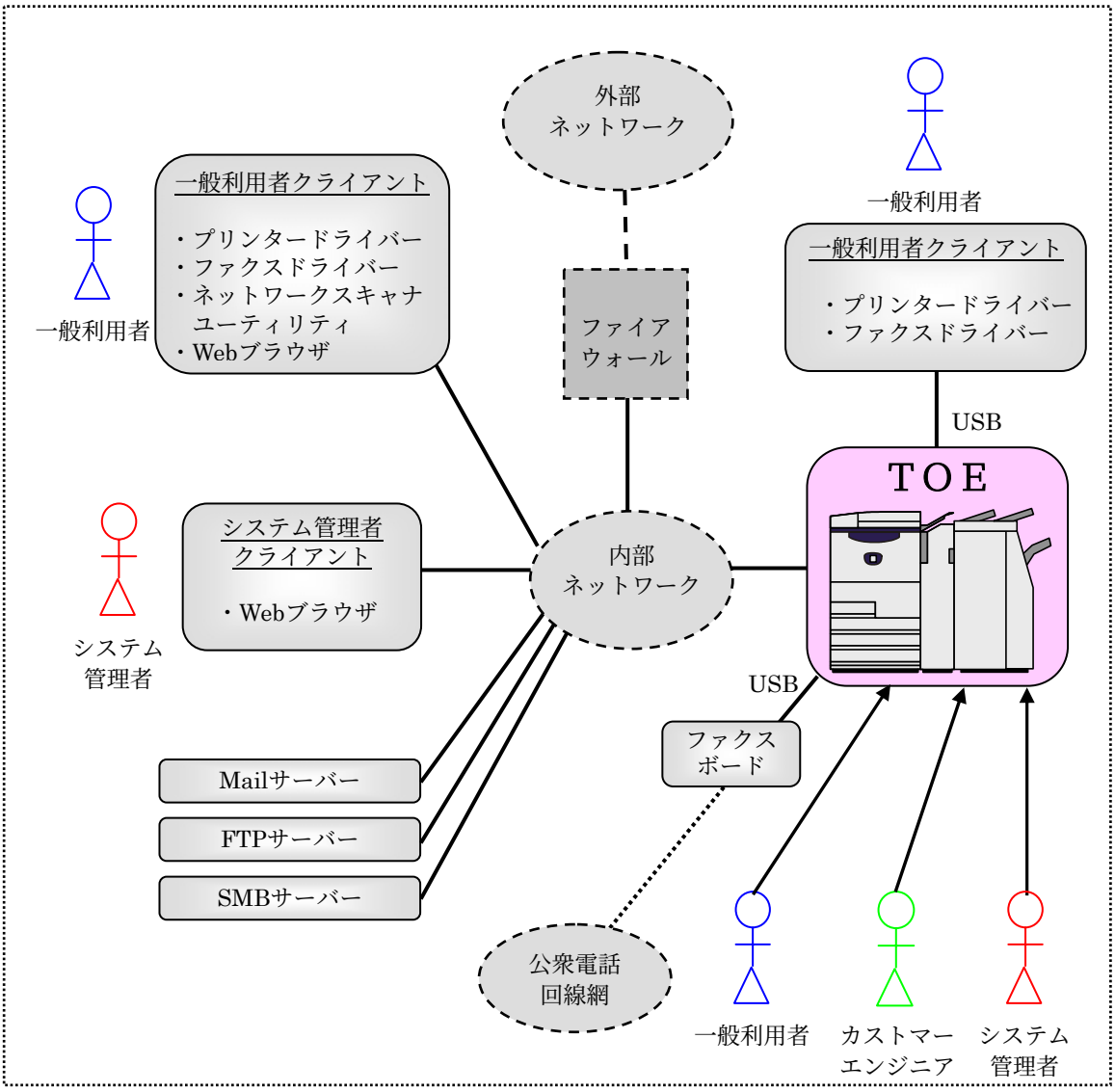

図1-2　利用イメージ

TOEの機能を利用したMFPの利用イメージと動作概要は以下のとおりである。

① 操作パネル：

一般利用者は、コピー、ファクス、スキャン、プリントなどの機能を利用することができる。

また、システム管理者は、TOEに対してTOE設定データの設定、確認や変更を行うことができる。

② 一般利用者クライアント：

ネットワーク接続されている場合、プリンタードライバー、ネットワークスキャナユーティリティ、及びファクスドライバーがインストールされており、MFPに対して文書データのプリント要求、文書データのファクス要求、及び文書データの取り出し要求を行うことができる。

また、Webブラウザを使用して、MFPに対してスキャナー機能によりスキャンした文書データの取り出し要求を行う。また、一般利用者がMFPに登録した親展ボックスのボックス名称、パスワード、アクセス制限、及び文書の自動削除指定の設定変更ができる。

USBでローカル接続されている場合、プリンタードライバー、及びファクスドライバーがインストールされており、MFPに対して文書データのプリント要求、及び文書データのファクス要求を行うことができる。

③ システム管理者クライアント：

Webブラウザを使用して、TOEに対してTOE設定データの設定、確認や変更を行うことができる。

④ Mailサーバー：

MFPはメールプロトコルを用いて、Mailサーバーに文書データ（一般利用者がMFPのスキャナー機能により作成したもの）を送信することができる。

⑤ FTPサーバー：

MFPはFTPプロトコルを用いて、FTPサーバーに文書データ（一般利用者がMFPのスキャナー機能により作成したもの）を送信することができる。

⑥ SMBサーバー：

MFPはSMBプロトコル（Windowsでネットワークを通じてファイル共有等を実現するプロトコル）を用いて、SMBサーバーに文書データ（一般利用者がMFPのスキャナー機能により作成したもの）を送信することができる。

⑦ ファクスボード

外部公衆回線に接続されておりG3/G4プロトコル（ファクスの国際規格）に対応する
ファクスボードである。MFPとはUSBのインタフェースで接続されファクスデータの送受信を行う。

1.2.4 TOEの機能

TOEは一般利用者に対して、基本機能として、操作パネル機能、コピー機能、プリ

ンター機能、スキャナー機能、ファクス機能、及びCWIS機能を提供する。

TOEは上記基本機能の使用に関連し、保護対象とする資産を守るために、以下に示すセキュリティ機能を持つ。

・ハードディスク蓄積データ上書き消去機能
・ハードディスク蓄積データ暗号化機能
・システム管理者セキュリティ管理機能
・カストマーエンジニア操作制限機能
・ファクスフローセキュリティ機能

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。

② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

③ 本TOEがセキュリティ設計に基づいて開発されていること。

④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア　セキュリティターゲット」（以下「ST」という。）[1]、本TOE開発に関連する評価用提供物件、及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート１（[5][8][11]のいずれか）附属書B、CCパート２（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート３（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア　評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において、特に問題点は見られなかった。評価は、平成20年5月の評価機関による評価報告書の提出をもって完了し、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEが想定する攻撃者の攻撃レベルは低レベルである。従って、最小機能強度として“SOF-基本”を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

・ハードディスク蓄積データ上書き消去機能

内部ハードディスク装置に蓄積される文書データは、利用が終了して削除される際に管理情報だけが削除され、蓄積された文書データ自体は削除されない。このため内部ハードディスク装置上に利用済み文書データとして残存した状態になる。このため、各ジョブの完了後に、内部ハードディスク装置に蓄積された利用済み文書データに対して、上書き消去機能を提供する。

・ハードディスク蓄積データ暗号化機能

内部ハードディスク装置に文書データを蓄積する際に、文書データの暗号化機能を提供する。

・システム管理者セキュリティ管理機能

本TOEは、ある特定の利用者へ特別な権限を持たせるために、システム管理者モードへのアクセスをシステム管理者にのみに制限して、認証されたシステム管理者

のみに、操作パネルから下記のセキュリティ機能の設定を行う権限を許可する。

- ハードディスク蓄積データ上書き消去有効/無効にする
- ハードディスク蓄積データ暗号化する/しない
- ハードディスク蓄積データ暗号化キーを設定する
- 本体パネルからの認証時のパスワードの使用　有効/無効にする
- 機械管理者のIDとパスワード変更
- SAのパスワード変更
- システム管理者ID認証失敗によるアクセス拒否設定
- カストマーエンジニア操作機能制限する/しない

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

- 機械管理者のIDとパスワード変更
- SAのパスワード変更
- システム管理者ID認証失敗によるアクセス拒否設定

・カストマーエンジニア操作制限機能

本TOEは、カストマーエンジニアが、以下のTOEセキュリティ機能に関する設定の参照及び変更ができないように、システム管理者がカストマーエンジニアのシステム管理者モードでの操作を、制限する機能を提供する。この機能により、カストマーエンジニアのなりすましによる設定変更ができないようにする。

- ハードディスク蓄積データ上書き消去機能設定
- ハードディスク蓄積データ暗号化機能設定
- 機械管理者IDとパスワード設定
- SAのパスワード設定
- システム管理者ID認証失敗によるアクセス拒否設定
- カストマーエンジニア操作制限機能設定

・ファクスフローセキュリティ機能

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

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

脅威 （識別子）	内容説明
内部ハードディスク装置に蓄積される文書データの不正再生	
T.RECOVER	攻撃者が、内部ハードディスク装置を取り出して、その内容を読み取るために市販のツール等に接続して、内部ハードディスク装置上の利用済み文書データを読み出して漏洩させるかもしれない。
TOE設定データの不正アクセス	
T.CONFDATA	攻撃者が、操作パネルやWebブラウザから、システム管理者のみアクセスが許可されている、TOE設定データにアクセスして、データの改ざん、または不正に読み出すかもしれない。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

表1-2 組織のセキュリティ方針

組織の方針 （識別子）	内容説明
P.FAX_OPT	在日米軍の要請により、公衆電話回線網から内部ネットワークへのアクセスができないことを保証しなければならない。

1.5.7 構成条件

本TOEは、コピー機能、プリンター機能、スキャナー機能及びファクス機能を有するデジタル複合機「富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ」のオプション製品として使用される、データセキュリティキットのコントローラソフトウェアである。

上記以外に、ファクス機能を使用する場合のオプション機器としてファクスボードの装備とファクスカードの装着、またリモートのクライアントPC（一般利用者、システム管理者用）から使用する場合のOSとして、Windows 2000、Windows XP、またはWindows VISTAのインストールが必要である。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-3 TOE使用の前提条件

前提条件 （識別子）	内容説明
人的な信頼	
A.ADMIN	システム管理者は、TOEの機器管理に課せられた役割を遂行するために、TOEセキュリティ機能に関する必要な知識を持ち、悪意をもった不正を行わないものとする。
保護モード	
A.SECMODE	システム管理者は、TOEを運用するにあたり、下記の通りに設定するものとする。 • 本体パネルからの認証時のパスワード使用設定：する • システム管理者パスワード：7 桁以上 • システム管理者 ID 認証失敗によるアクセス拒否：する • システム管理者 ID 認証失敗によるアクセス拒否回数：5 • カストマーエンジニア操作制限機能設定：する • ハードディスク蓄積データ上書き消去設定：有効にする • ハードディスク蓄積データ暗号化設定：有効にする • ハードディスク蓄積データ暗号化キー設定：12 文字
ネットワークの接続条件	
A.NET	• TOE が搭載された MFP を設置する内部ネットワークは盗聴されない環境を構成する。 • TOE が搭載された MFP を設置する内部ネットワークが外部ネットワークと接続される場合は、外部ネットワークから MFP へアクセスできない。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

・富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　管理者ガイド
DE3788J1-1 第1.2版

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年2月に始まり、平成20年5月の評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年4月に開発現場へ赴き、現物・記録の確認、及びスタッフへのヒアリングにより、ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行い、また、図面・記録・現物の確認、及びスタッフへのヒアリングにより、配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年4月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は存在しなかった。

また、評価の過程で認証機関により指摘された問題点は存在しなかった。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を、以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

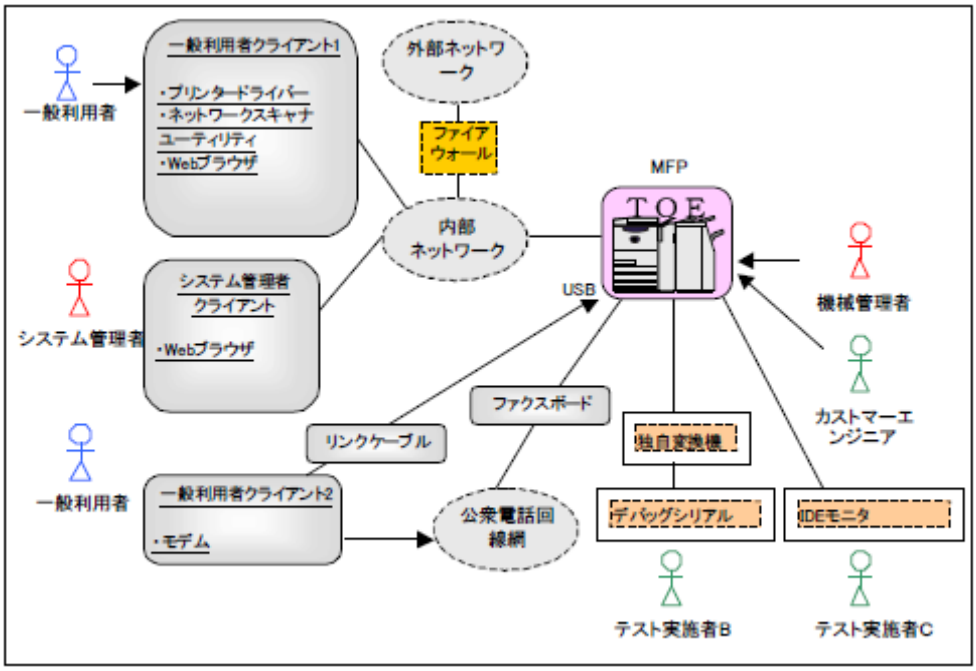

図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストは、STにおいて識別されているTOEの構成及び動作環境と同等のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

① テスト用のMFPとしては、DocuCentre-Ⅲ 2000を使用している。本TOEは、DocuCentre-Ⅲ 2000シリーズとDocuCentre-Ⅲ 3000シリーズの2機種に共通するコントロールソフトウェアである。それぞれ、Cモデル（コピー機能、スキャナー機能あり）、CFモデル（コピー機能、ファクス機能、スキャナー機能あり）、及びCPFモデル（コピー機能、プリンター機能、ファクス機能、スキャナー機能あり）の構成を取れるが、全モデルをまとめて、DocuCentre-Ⅲ 2000/3000シリーズと総称している。テストは、すべてのインタフェースを装着したDocuCentre-Ⅲ 2000のCPFモデルにて実施している。

② MFPは、テスト用ネットワーク(Ethernet)を通してMFP用のプリンタードライバー、ネットワークスキャナユーティリティがインストールされた利用者クライアント1(PC)と接続される。

③　利用者クライアント2(PC)は公衆電話回線網に接続されており、TOEとファクスの送受信を行う。

④　システム管理者クライアントは、テスト用ネットワーク(Ethernet)を通して、テストに使用するMFPにWEBブラウザでアクセスする。

⑤　デバッグシリアルは、MFPに独自変換機を介して接続され、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によるハードディスク内の最終的なデータの状態を確認するために使用する。

⑥　IDEモニタは、MFP内のコントローラボードとハードディスクとの間に接続され、ボードとHDD間の通信データをモニタリングすることにより、ハードディスク上書き消去機能及びハードディスク蓄積データ暗号化機能による通信データの内容を確認するために使用する。

⑦　ハードディスクのエラーを擬似的に発生させるために、HDD電源OFF用スイッチ付き中継ケーブルをハードディスクに接続し、上書き消去機能の動作エラーに関するテストを実施している。

c.実施テストの範囲

テストは開発者によって30項目実施されている。

30項目のテスト項目の内訳として、セキュリティ機能別のテスト数は次のとおりである。

- 上書き消去機能テスト　19 項目
- 暗号化機能テスト　4 項目
- システム管理者認証機能テスト　4 項目
- カストマーエンジニアの操作制限機能テスト　1 項目
- ファクスフローセキュリティテスト　2 項目

テストの範囲としては各機能のふるまいが網羅されており、全体として適切な実施量、及び範囲である。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2　評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同等の構成であることが評価

者により検証されている。評価者テストに使用したシステムの構成を図2-2に示す。

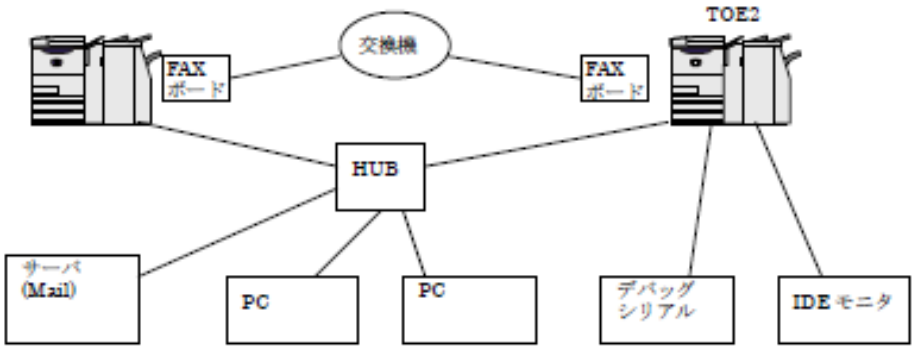

図2-2　評価者テストの構成図

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-2に示す。評価者テストは、STにおいて識別されているTOEの構成及び動作環境と同等のTOEテスト環境で実施されている。

b.テスト手法

評価者は、開発者テストと同等のテスト環境において、開発者テストと同様のテスト手法でテストを実施している。

c.実施テストの範囲

評価者が独自に考案したテストを3項目、開発者テストのサンプリングによるテストを30項目、計33項目のテストを実施している。テスト項目の選択基準として、下記を考慮している。

① 独立テスト

セキュリティ機能の開発者テストの厳密さ（システム管理者に関するパラメタの限界値分析の観点）

② 開発者テストのサンプリング

開発者テスト全30項目を全て実施した。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。

ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された。**
ACM_CAP.3.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理・追跡が可能な手続きが妥当であり正しく運用されていることを確認している。

ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された。**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、使用されている図面・記録等の確認、関係者へのヒアリングにより確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された。**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。

ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された。**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された。**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
テスト	**適切な評価が実施された。**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全

	に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された。**

AVA_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（情報技術セキュリティ評価のためのコモンクライテリア）
CEM	Common Methodology for Information Technology Security Evaluation（情報技術セキュリティ評価のための共通手法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
SOF	Strength of Function（機能強度）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functions（TOEセキュリティ機能）

本報告書で使用されたTOE特有の略語を以下に示す。

ADF	Auto Document Feeder（自動原稿送り装置）
G3/G4	Group3/Group4（G3ファクシミリ/G4ファクシミリ）
IIT	Image Input Terminal（画像入力ターミナル）
IOT	Image Output Terminal（画像出力ターミナル）
MFP	Multi Function Peripheral（デジタル複合機）
NVRAM	Non Volatile Random Access Memory（不揮発性ランダムアクセスメモリ）
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory（シリアスバスに接続された電気的に書き換え可能なROM）
SMB	Server Message Block（サーバーメッセージブロック）

本報告書で使用された用語を以下に示す（順不同。なお、当該用語を理解するために必要な関連用語の説明を含む）。

用語	定義内容
一般利用者	MFPのコピー機能、スキャナー機能、ファクス機能及びプリンター機能を利用する者。
機械管理者	MFPの機械管理やTOEセキュリティ機能の設定を行う管理者。
SA(System Administrator)	機械管理者から、MFPの機械管理やTOE セキュリティ機能の設定を許可された者。
システム管理者	MFPの機械管理やTOEセキュリティ機能の設定を行う管理者。 機械管理者とSAの総称。
カストマーエンジニア	MFPの保守/修理を行う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	MFPの操作に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネル。
一般利用者クライアント	一般利用者がMFPを利用するためのクライアント。
システム管理者 クライアント	システム管理者が利用するクライアント。システム管理者はWebブラウザを使いMFPに対して、TOE設定データの確認や書き換えを行う。
センターウェア インターネット サービス（CWIS）	MFPのスキャナー機能によりスキャンして親展ボックスに格納された文書データを、取り出す機能を提供する。 さらにシステム管理者に、Webブラウザを使いMFPに対して、TOE設定データの確認や書き換えを行う機能を提供する。
プリンタードライバー	一般利用者クライアント上のデータを、MFPが解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウェアで、一般利用者クライアントで使用する。
ファクスドライバー	一般利用者クライアント上のデータを印刷と同じ操作で、MFPへデータを送信し、直接ファクス送信する（ダイレクトファクス機能）ためのソフトウェアであり一般利用者クライアントで使用する。
ネットワークスキャナユーティリティ	MFP内の親展ボックスに保存されている文書データを、一般利用者クライアントから取り出すためのソフトウェア。
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こと。
プリンター機能	利用者クライアントから送信された印刷データをデコンポーズして印刷する機能。
プリンター制御機能	プリンター機能を実現するために装置を制御する機能。
蓄積プリント	プリンター機能において、印刷データをデコンポーズして作成したビットマップデータを、MFPの内部ハードディスク装置に一旦蓄積し、一般利用者が操作パネルより指示する事で印刷を開始するプ

用語	定義内容
	リント方法で、以下の3種類がある。 • セキュリティプリント： 一般利用者クライアント上のプリンタードライバーよりパスワードを設定し、操作パネルよりその暗証番号を入力することにより印刷が可能となる蓄積プリント。 • サンプルプリント： 1 部目は通常に印刷を行い、印刷結果を確認後、操作パネルより指示することにより残り部数の印刷を行う蓄積プリント方法。 親展ボックスを使った印刷： 親展ボックスに、デコンポーズされたビットマップデータを蓄積し、操作パネルより指示することにより印刷を行う蓄積プリント。
コピー機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み、IOTより印刷を行う機能。 同一原稿の複数部のコピーが指示された場合、IITで読み込んだ文書データは、一旦MFPの内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
スキャナー機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み、MFPの内部ハードディスク装置に作られた親展ボックスに蓄積する。 蓄積された文書データは、一般的なWebブラウザを使用して、CWISやネットワークスキャナユーティリティの機能により取り出す。
ネットワークスキャン機能	操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み後にMFPに設定されている情報に従って、FTPサーバー、SMBサーバー、Mailサーバーへ文書データの送信を行う。
ファクス機能	ファクス送受信を行う。ファクス送信は操作パネルからの一般利用者の指示に従い、IITで原稿を読み込み、公衆電話回線網により接続された相手機に文書データを送信する。ファクス受信は公衆電話回線網により接続相手機から送られた文書データを受信し、IOTから印刷を行う。
ダイレクトファクス（D-FAX）機能	データをプリントジョブとしてMFPに送り、紙に印刷するのではなく、ファクス機能により公衆電話回線網を使用して送信する機能。
インターネットファクス（i FAX）機能	公衆電話回線網を使用するのではなく、インターネットを経由してファクスの送受信を行う機能。
親展ボックス	MFPの内部ハードディスク装置に作成される論理的なボックス。

用語	定義内容
	スキャナー機能により読み込まれた文書データや親展ボックスを使った印刷のための文書データを蓄積することが出来る。個別親展ボックスと共用親展ボックスがある。
文書データ	一般利用者がMFPのコピー機能、プリンター機能、スキャナー機能、ファクス機能を利用する際に、MFP内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。文書データには以下の様な物が含まれる。 コピー機能を使用する際に、IITで読み込まれ、IOTで印刷されるビットマップデータ。 プリンター機能を利用する際に、一般利用者クライアントから送信される印刷データ、及びそれをデコンポーズした結果作成されるビットマップデータ。 スキャナー機能を利用する際に、IITから読み込まれ内部ハードディスク装置に蓄積されるビットマップデータ。 ファクス機能を利用する際に、IITから読み込まれ接続相手機に送信するビットマップデータ、及び接続相手機から受信しIOTで印刷されるビットマップデータ。
利用済み文書データ	MFPの内部ハードディスク装置に蓄積された後、利用が終了しファイルとしては削除されたが、内部ハードディスク装置内には、データ部が残存している状態の文書データ。
TOE設定データ	TOEによって作成された及びTOEに関して作成されたデータであり、TOEの動作に影響を与える可能性のあるもの。具体的には、ハードディスク蓄積データ上書き情報、ハードディスク暗号化情報、システム管理者情報、カストマーエンジニア操作制限情報、親展ボックス情報など。
上書き消去	内部ハードディスク装置上に蓄積された文書データを削除する際に、そのデータ領域を特定データで上書きすることを示す。
外部ネットワーク	TOEを管理する組織では管理ができない内部ネットワーク以外のネットワークを指す。
内部ネットワーク	TOEが設置される組織の内部にあり、外部ネットワークからのセキュリティの脅威に対して保護されているネットワーク内の、MFPとMFPへアクセスが必要なリモートの高信頼なサーバーやクライアントPC間のチャネルを指す。

6 参照

[1] 富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア セキュリティターゲット　V 1.0.1 (2008年3月19日)　富士ゼロックス株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001 (平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002 (平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003 (平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] 富士ゼロックス　DocuCentre-Ⅲ 3000/2000 シリーズ　コントローラソフトウェア 評価報告書 第1.0版 2008年5月22日 有限責任中間法人　ITセキュリティセンター 評価部