認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成18年12月12日（IT認証6123）**
認証番号	C0082
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-Ⅱ4000/3000 **シリーズ データセキュリティーキット**
TOEのバージョン	Controller ROM Ver1.0.17
PP適合	**なし**
適合する保証要件	EAL2
TOE開発者	**富士ゼロックス株式会社**
評価機関の名称	**社団法人　電子情報技術産業協会　ITセキュリティセンター**

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19年2月22日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

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-Ⅱ4000/3000 シリーズ データセキュリティーキット Controller ROM Ver1.0.17」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証手続規程に従い、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-Ⅱ4000/3000 シリーズ データセキュリティーキット Controller ROM Ver1.0.17」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（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。

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-Ⅱ4000/3000 シリーズ データセキュリティーキット

バージョン: Controller ROM Ver1.0.17

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、スキャナー機能およびファクス機能を有する富士ゼロックス社製デジタル複合機「DocuCentre-Ⅱ4000」および「DocuCentre-Ⅱ3000」（以降、「MFP」という。）のオプション製品として提供されるファームウェアである。

本製品は、MFPがコピー、プリント、スキャン、ファクス処理を実施した際にハードディスク装置内に蓄積される文書データを不正な暴露から保護する。本製品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
- 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

1.2.3 TOEの範囲と動作概要

MFPは、コントローラボード、操作パネル、ファクスカードの3つの基盤ユニットから構成されており、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。図1-1にTOEの物理的構成イメージとTOEが持つ機能を示す。

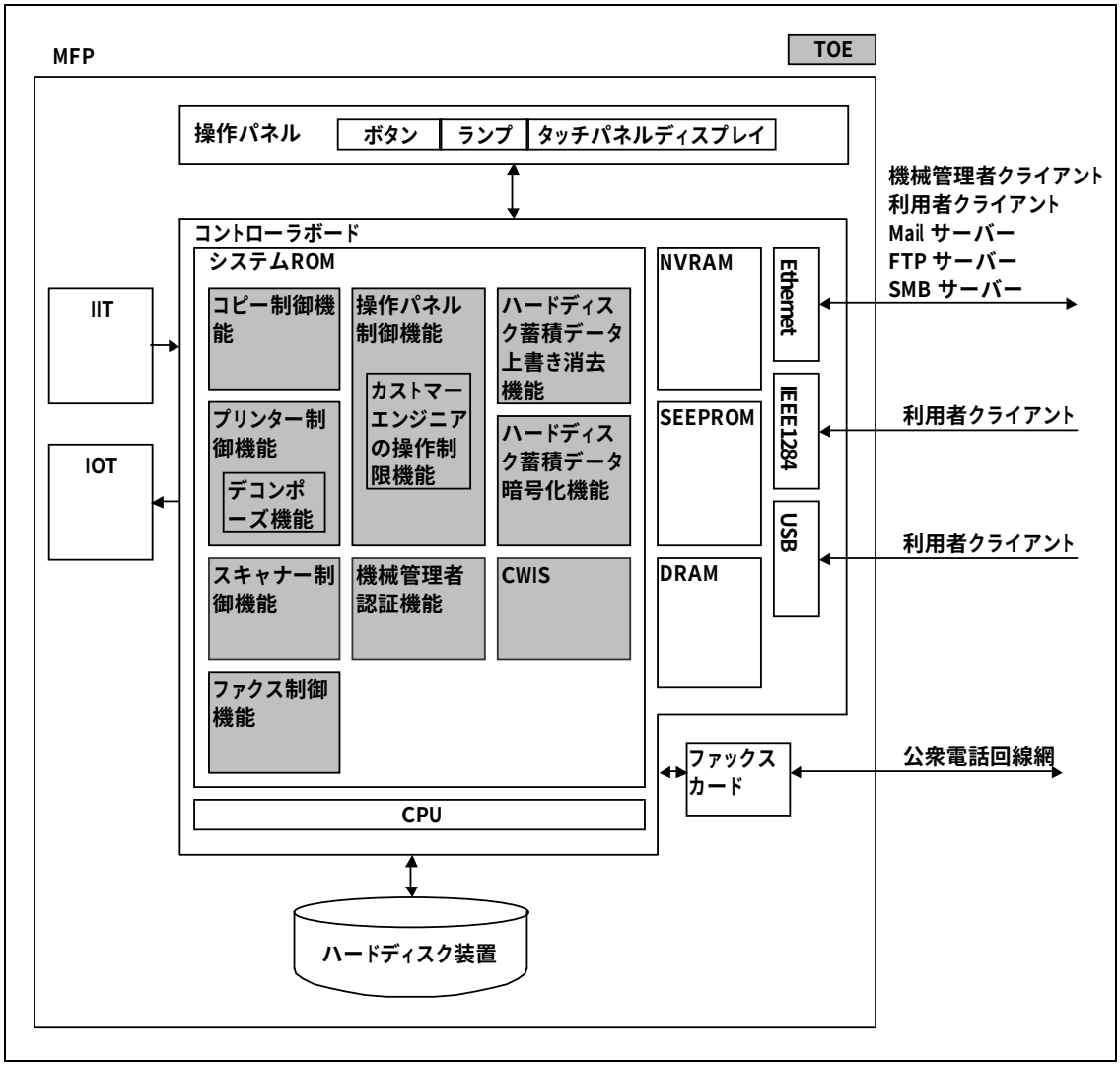

図1-1　TOEの物理的構成イメージ

TOEのセキュリティ機能を利用したMFPの利用イメージと動作概要を以下に示す。

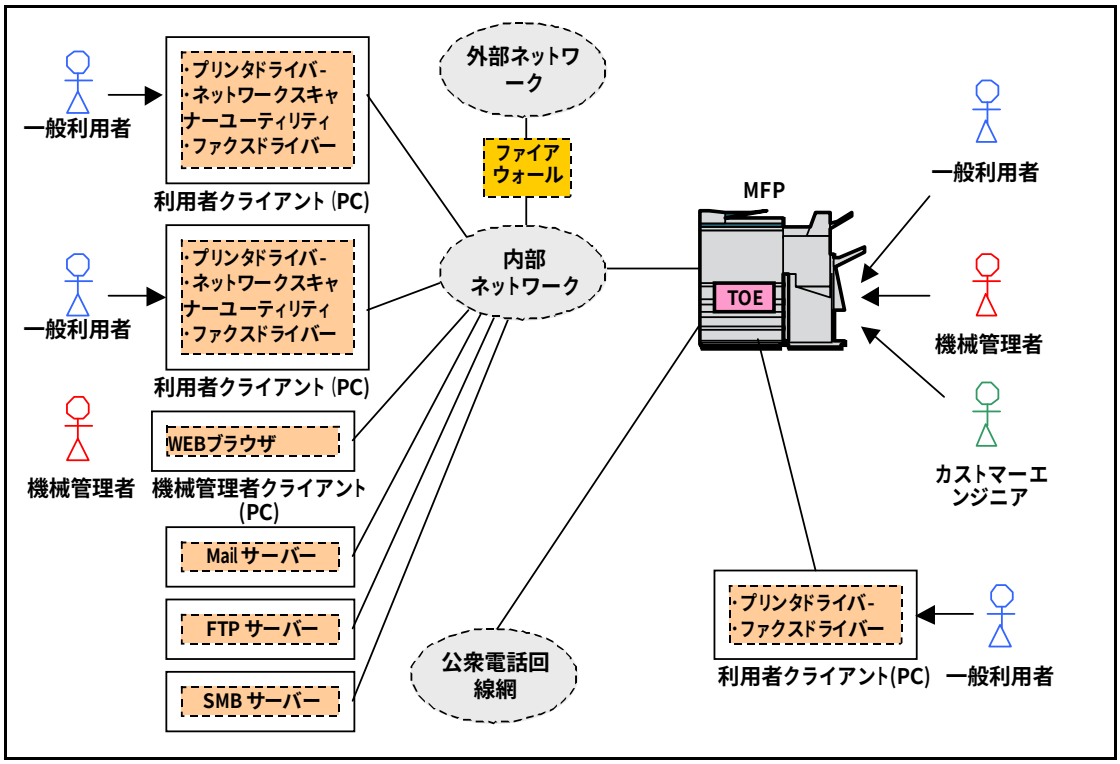

図1-2　利用イメージ

・ 機械管理者に関連するTOEの動作概要

MFPの操作パネルまたは機械管理者クライアントにおいて識別認証を行う。機械管理者として識別認証された後、表1-1に示す内容の設定を行う。

表1-1　設定データ

項番	設定データ
1	ハードディスク蓄積データ上書き消去機能設定
2	パスワードの使用設定
3	機械管理者パスワード
4	カストマーエンジニアの操作制限機能設定
5	機械管理者IDの認証失敗によるアクセス拒否
6	ハードディスク蓄積データ暗号化機能設定
7	ハードディスク蓄積データ暗号化キー

・ 一般利用者に関連するTOEの動作概要

MFPの操作パネルあるいは利用者クライアントを操作してコピー、プリント、スキャン、ファクスを実施することにより利用済み文書データがMFPの内蔵ハードディスクに蓄積される。この時、一般利用者は意識することなく、表1の設定データに従って自動的にセキュリティ機能が動作する（ハードディスク蓄積データ上書き消去機能設定とハードディスク蓄積データ暗号化機能設定が有効になっている場合、利用済み文書データは暗号化されて蓄積され、各処

理の完了と共に上書き消去される)。

1.2.4 TOEの機能

TOEは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
  コピー、プリンター、スキャナーおよびファクスの各機能の動作後、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、スキャナーおよびファクスの各機能の動作時に、ハードディスク装置に文書データを蓄積する際に、文書データの暗号化を行う。
- 機械管理者認証機能
  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う。
  また、以下に示すTOEのセキュリティ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。
  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
  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
  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
  カストマーエンジニアの操作制限機能設定を機械管理者のみが行えるようにする。

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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-Ⅱ4000/3000 シリーズ データセキュリティーキット セキュリティターゲット V1.00」（以下「ST」という。）[1] 及び本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C、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-Ⅱ4000/3000 シリーズ データセキュリティーキット 評価報告書 第1.0版」（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パート2（[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問題は発見されなかった。評価は、平成19年1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、EAL2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（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1-2に示す方法により上書き消去する。
  また、ハードディスク装置上に上書き消去予定の利用済み文書データの一覧を持つことにより、電源断などにより利用済み文書データの上書きが未終了となってしまっても、次回のシステム起動時に上書き消去される。

表1-2　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

- 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、起動時に暗号鍵生成を行う。
  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。
  暗号鍵はMFP本体の電源を切断すると消滅する。

- 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。

- 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。「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。

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅　威
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。
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。

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はない。

1.5.7 構成条件

本製品は、富士ゼロックス社製デジタル複合機「DocuCentre-Ⅱ4000」および「DocuCentre-Ⅱ3000」に搭載されるオプション製品として提供される。

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1-4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1-4　TOE使用の前提条件

識別子	前提条件
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。

- ApeosPort-Ⅱ4000/3000 DocuCentre-Ⅱ4000/3000 ユーザーズガイド
  2006年11月 第3.1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パート2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パート2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18年12月に始まり、平成19年1月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18年12月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・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18年12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。

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。

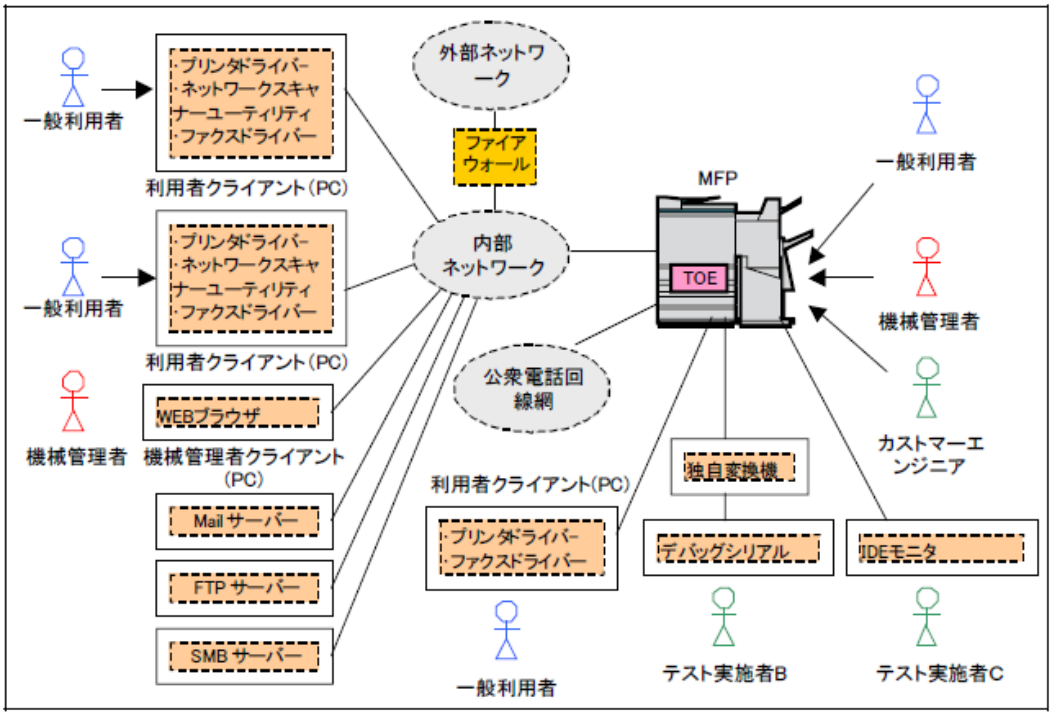

図2-1　開発者テストの構成図

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構成と同一の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。

①MFP、PCを操作して、セキュリティ機能の外部インタフェースを刺激し、外部インタフェースのふるまいを直接観察する。

②外部インタフェースのふるまいを直接観察することができないセキュリティ機能（ハードディスク蓄積上書き消去機能、ハードディスク蓄積データ暗号化機能）については、ツール（デバックシリアル及びIDEモニタ）を使用してセキュリティ機能のふるまいを確認する。

デバッグシリアルは、MFPに独自変換機を介して接続され、ハードディスク内のデータの状態を確認するために使用し、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間の通信データをモニタリングして通信データの内容を確認するために使用する。また、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

テストの項目数は全体で28 項目である。

全体で28 項目のテスト項目があり、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
- 機械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

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。

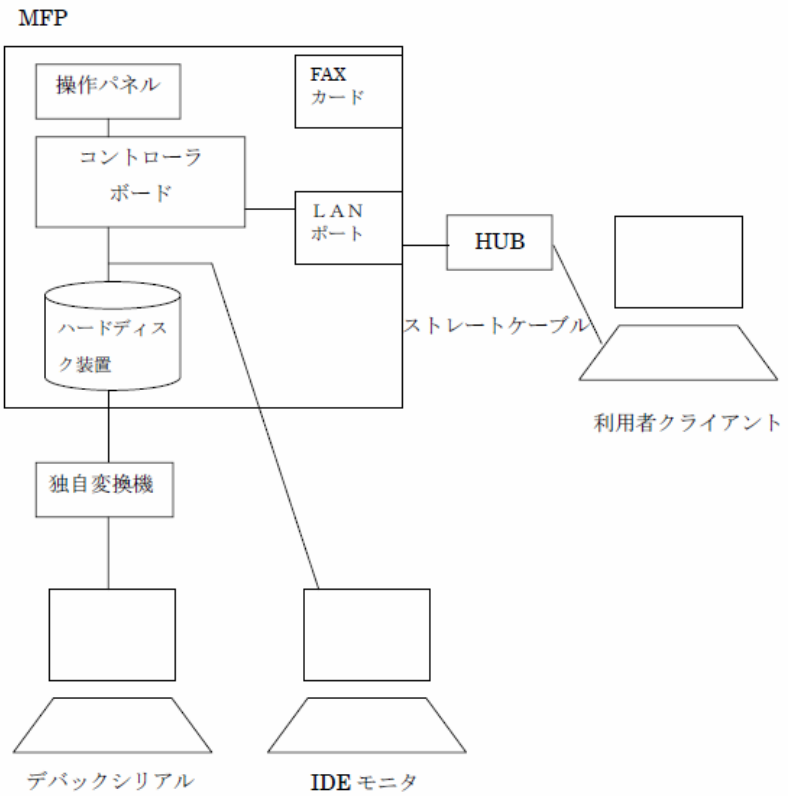

図2-2　評価者テストの構成

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構成と同一のTOEテスト環境で実施されている。

b.テスト手法

評価者は、開発者が行ったテスト手法が、セキュリティ機能の期待されたふるまいを検証するのに適していると判断し、開発者テストと同様の手法でテストを実施している。

c.実施テストの範囲

評価者は、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16項目、侵入テストを5項目、計24項目のテストを実施している。

評価者が独自に考案したテストは、セキュリティ機能に対する開発者テストの厳密さを考慮して実施している。

サンプリングテストは、開発者が実施した28項目のテストの57%にあたる16項目を選択している。

侵入テストは、開発者の脆弱性分析結果に基づき脆弱性分析を行い、その分析結果に基づいて5項目のテストを実施している。

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パート2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

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 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。

② 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。

③ 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問題は発見されなかった。

4 結論

4.1 認証結果

提出された評価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EAL2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.2.1E	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。
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、実地検査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.1.1E	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.1.2E	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いることを確認している。IT環境に対するセキュリティ要件はないので、それに関しては管理者ガイダンスへの記述は不要で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が記述してあり、他の証拠資料と一貫していることを確認している。TOEのセキュアな操作に必要な利用者責任およびIT環境に対するセキュリティ要件はないので、それに関しては利用者ガイダンスへの記述は不要であることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.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機能仕様に正確に対応してい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_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
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
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)

本報告書で使用された用語を以下に示す。

一般利用者	MFP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	MFPの機械管理を行う者。
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。
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。
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MFP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、MFPに対して、TOE設定データの確認や書き換えを行う。
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MFPが解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウエア。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MFP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。
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。
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。
拡張親展ボックス	MFP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	STでは、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。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。 ファクス機能を利用する際に、IITから読み込まれ接続相手機に送信するビットマップデータ、および、接続相手機から受信しIOTで印刷されるビットマップデータ。
利用済み文書データ	MFP の内部ハードディスク装置に蓄積され、利用が終了した文書データ。
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。

6 参照

[1] 富士ゼロックス DocuCentre-Ⅱ4000/3000 シリーズ データセキュリティーキット セキュリティターゲット V1.00（2006年11月30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18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

[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-Ⅱ4000/3000 シリーズ データセキュリティーキット 評価報告書 第1.0版（2007年1月26日）社団法人 電子情報技術産業協会 IT セキュリティセンター