認　証　報　告　書

評価対象

申請受付年月日（受付番号）	**平成15年12月22日（IT認証3017）：当初の申請を取り下げし、CCRA認証マーク対応のため、再申請があった申請受付日** **平成15年10月20日（IT認証3015）：当初の申請受付日**
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 719/659/559**シリーズ　データセキュリティーキット**
TOE**のバージョン**	DC**システム**ROM**バージョン**　V512 PESS**システム**ROM**バージョン**　V3.0.4
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16年9月15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セキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 ― 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法

⑤　Common Methodology for Information Technology Security Evaluation Version 1.0
⑥　CCIMB Interpretations-0210
⑦　認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「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」は、独立行政法人情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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 719/659/559シリーズ　データセキュリティーキット」（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 719/659/559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
PESSシステムROMバージョン　V3.0.4

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、デジタルコピー機能、プリンター機能及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」及びデジタル複写機「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」及び「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ファームウェア製品である。本製品は以下のセキュリティ機能を提供する。

- 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

1.2.3 TOEの範囲と動作概要

図1-1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）及び操作パネルの4つの基板ユニットから構成される。

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1-1に示す。

表1-1　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。 ・ 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。 ・ 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 ・ デコンポーズ機能

一般利用者がDocuCentreのデジタルコピー機能、プリンター機能及びスキャナー機能を利用する際、利用済み文書データは、DC用HDD及び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こと無く、機械管理者の設定に従いTOEのセキュリティ機能が動作する。

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」、及び「サービスエンジニアアクセス制限機能」が動作するように設定された状態でTOEを運用しなければならない。

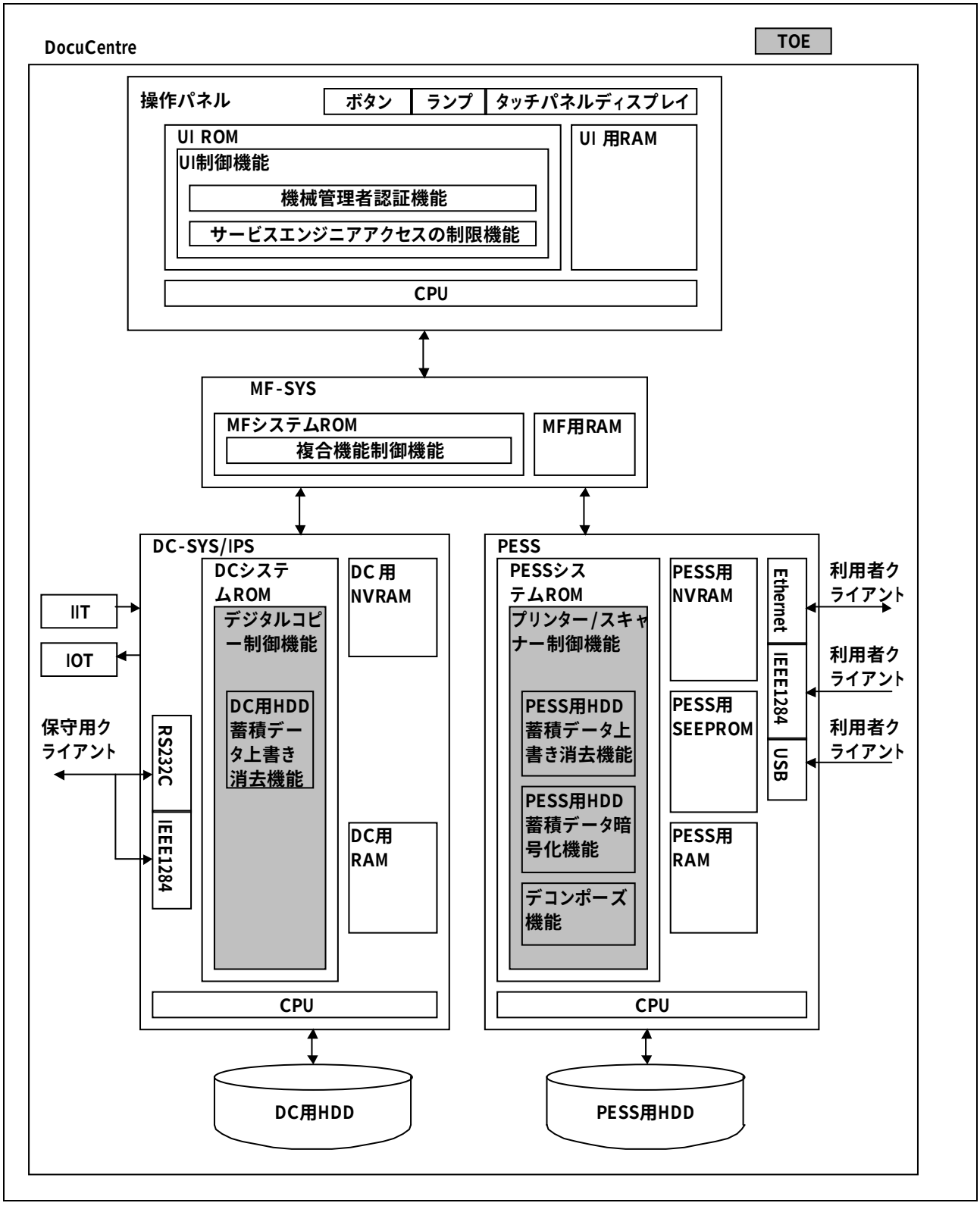

図1-1 DocuCentre**内の各ユニットと、**TOE**の物理的境界**

1.2.4 TOEの機能

DocuCentreは一般利用者に対し、デジタルコピー機能、プリンター機能及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(画像入力ターミナル)で原稿を読み取り、IOT(画像出力ターミナル)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。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。

DocuCentreはDC用HDD とPESS用HDD の2つの内部HDDを持つ。DC用HDDは、デジタルコピー機能によるコピー時、及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、PESS用HDD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、及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、以下のセキュリティ機能を提供する。

- DC用HDD蓄積データ上書き消去機能
  DC用HDDに蓄積された利用済み文書データを上書き消去する機能。
- PESS用HDD蓄積データ上書き消去機能
  PESS用HDDに蓄積された利用済み文書データを上書き消去する機能。
- PESS用HDD蓄積データ暗号化機能
  DC用HDDに蓄積されている利用済み文書データは、富士ゼロックス独自方式で画像圧縮したビットマップデータであり、データ自体の解析が困難であるが、PESS用HDDに蓄積されている利用済み文書データは、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、PESS用HDDに蓄積される文書データを暗号化する機能。

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。

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セキュリティ認証申請等の手引き (平成15年10月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項 (平成14年4月)」[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「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　V1.12」（以下「本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][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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 719/659/559シリーズ　データセキュリティーキット 評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]）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、本評価報告書、所見報告書、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発見された問題については、認証レビューを作成した。評価は、平成16年8月の評価機関による本評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、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

本STが規定するTOEの評価保証レベルは、EAL2である。

1.5.3 セキュリティ機能強度

本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。

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。

(1) 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。
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。

(2) 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。
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。

(3) 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。
電源断などで上書き未終了の状態で残っても、HDDを取り外し、直接ツールに接続するなどしての暴露から、利用済み文書データを保護する。

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 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> 一般利用者及び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。
T.CONFDATA	<TOE設定データの不正アクセス> 一般利用者及び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。

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TOEは、富士ゼロックス社製デジタル複合機「DocuCentre 719CP」、「DocuCentre 659CP」、「DocuCentre 559CP」、及びデジタル複写機「DocuCentre 719」、「DocuCentre 659」、「DocuCentre 559」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1-3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

識別子	前提条件
A.SECMODE	<保護モード> 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> 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。

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。

- 配布、導入、運用手続き説明書（K1.3）
- 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）2.2 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、本評価報告書において報告されている。本評価報告書では、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、本評価報告書による評価実施の履歴を示す。

評価は、平成15年10月に始まり、平成16年8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15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16年3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、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

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

開発者テストに使用したシステムの構成を図2-1に示す。

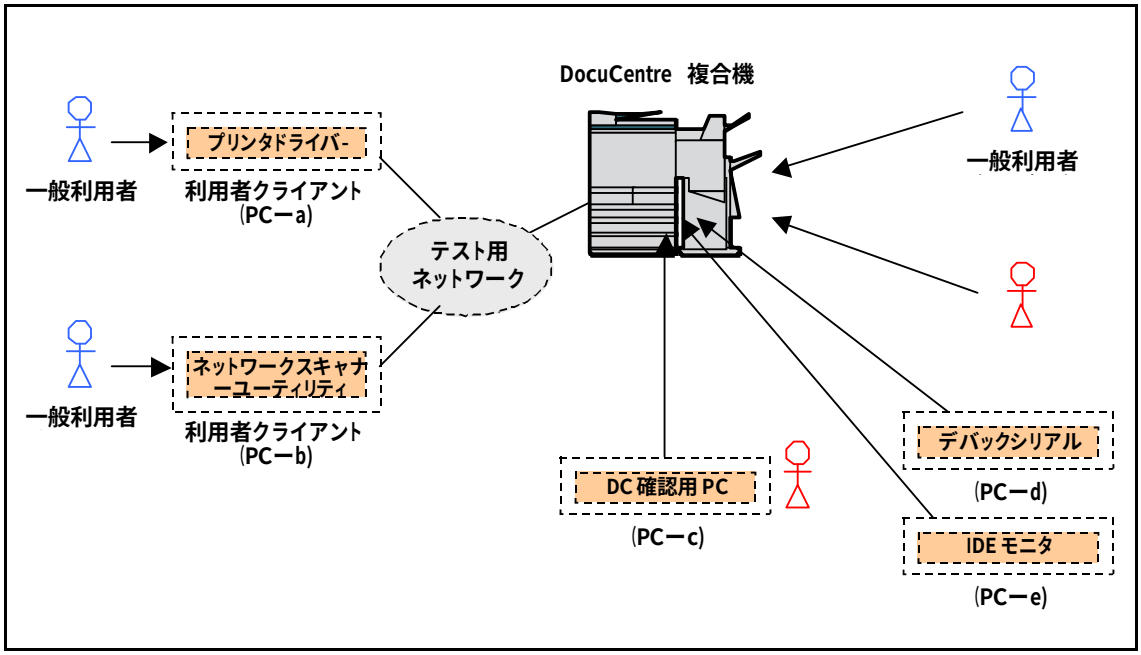

図2-1　テストに使用したシステムの構成

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。

利用者クライアントPC-aは主にプリンター機能に関連するテストのために使用し、PC-bは主にスキャナー機能に関連するテストのために使用する。

PC-cは、DocuCentre複合機内のDCボードに専用の接続ケーブルによりシリアル接続され、DC用HDD蓄積データ上書き消去機能によるDC用HDDの最終的なデータの状態を確認するために使用する。

デバッグシリアル（PC-d）は、DocuCentre複合機内のPESSボードに専用の接続ケーブルによりシリアル接続され、PESS用HDD蓄積データ上書き消去機能、及びPESS用HDD蓄積データ暗号化機能によるPESS用HDDの最終的なデータの状態を確認するために使用する。

IDEモニタ（PC-e）は、DocuCentre複合機内のPESSボードとPESS用HDD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、PESS用HDD蓄積データ上書き消去機能、及びPESS用HDD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。

c.実施テストの範囲

テストは開発者によって100項目実施されており、セキュリティ機能別のテスト数は次の通りである。

①DC用HDD蓄積データ上書き消去機能　85項目

- 上書き消去設定確認　8項目
- Power On時の上書き消去　28項目
- 印刷終了時の上書き消去　26項目
- コンカレント禁止確認　23項目

②PESS用HDD蓄積データ上書き消去機能　10項目

③PESS用HDD蓄積データ暗号化機能　5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。

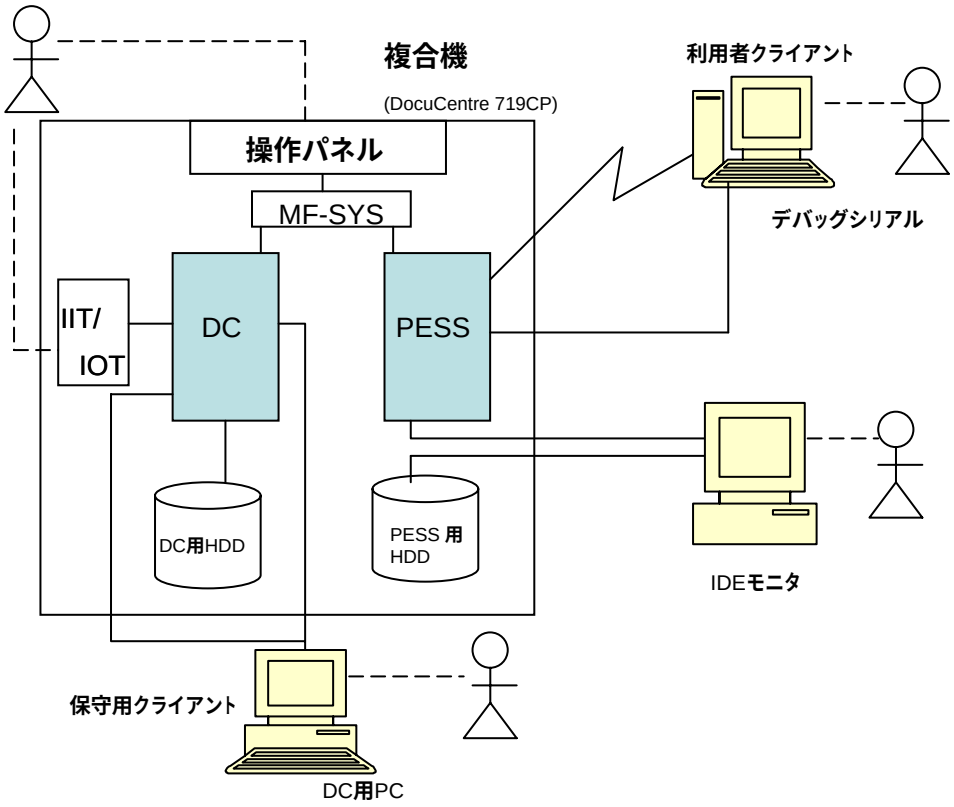

図2-2　評価者テストに使用したシステムの構成

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

テストには、以下の手法が使用された。

利用者クライアントは主にプリンター機能及びスキャナー機能に関連するテストのために使用する。

DC用PCは、DocuCentre複合機内のDCボードに専用の接続ケーブルによりシリアル接続され、DC用HDD蓄積データ上書き消去機能によるDC用HDDの最終的なデータの状態を確認するために使用する。

デバッグシリアルは、DocuCentre複合機内のPESSボードに専用の接続ケーブルによりシリアル接続され、PESS用HDD蓄積データ上書き消去機能、及びPESS用HDD蓄積データ暗号化機能によるPESS用HDDの最終的なデータの状態を確認するために使用する。

IDEモニタは、DocuCentre複合機内のPESSボードとPESS用HDD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、PESS

用HDD蓄積データ上書き消去機能、及びPESS用HDD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。

c.実施テストの範囲

評価者が独自に考案したテストを6項目、開発者テストのサンプリングによるテストを26項目、計32項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 独自に考案したテスト

- すべてのセキュリティ機能を対象とする
- DC用HDD蓄積データ上書き消去機能については、よりマクロ的でユーザの視点に近いもので特に異常系を中心とする
- PESS用HDD蓄積データ上書き消去機能については、開発者テストでは実施されていない操作での確認を行う
- PESS用HDD蓄積データ暗号化機能については、開発者テストとは異なる方法で暗号化の確認を行う

② サンプリングテスト

- すべてのセキュリティ機能を対象とする
- 開発者が実施したそれぞれのセキュリティ機能に対するテストの項目数を参考にしてサンプリング数の配分する

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

本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 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本評価報告書で示されたように評価されていること。

④ 本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 本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、本ST及び本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

提出された本評価報告書、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 ([7][10][13][16]のいずれか) 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識別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあ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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書に

	よる指摘も適切と判断される。
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明記され、それらが脅威、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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理路整然とし、完結しており、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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結しており、理路整然とし、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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が含まれて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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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がないため非適用であ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、STでSOF主張がなされているセキュリティメカニズムがないため非適用である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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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
DC	Digital Copire (デジタルコピー)
DC-SYS/IPS	DC Control System/Image Processing System (デジタルコピー制御システム)
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive (ハードディスク装置)
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)
MF-SYS	Multi Function Control System (複合機能制御システム)
NVRAM	Non Volatile Random Access Memory (不揮発性ランダムアクセスメモリ)
PP	Protection Profile
PESS	Printer Electorical Sub System (プリンターサブシステム)
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory (シリアルバスに接続された電気的に書き換え可能なROM)
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
UI	User Interface (ユーザーインタフェース)

本報告書で使用された用語を以下に示す。

DocuCentre	「 DocuCentre 719CP 」、「 DocuCentre 659CP 」、「DocuCentre 559CP」、「DocuCentre 719」、「DocuCentre 659」及び「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、プリンター機能及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のプリンター機能及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、及びスキャナー機能により読み込まれたデータ、及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。
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。
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。
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ことを示す。

6 参照

[1] 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

[2] ITセキュリティ認証申請等の手引き 平成15年10月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0210

[21] 補足-0210

[22] 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 評価報告書 第4.1版 2004年8月6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