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4月10日** (IT**認証**8225)
認証番号	C0196
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	Fuji Xerox ApeosPort-Ⅱ7000/6000 Series Controller Software for Asia Pacific
TOE**のバージョン**	Controller ROM Ver.1.180.7
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11月28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 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 バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific」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、「Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific」（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を併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series
バージョン： Controller ROM Ver.1.180.7
開発者： 富士ゼロックス株式会社

1.2.2 製品概要

Fuji Xerox ApeosPort-Ⅱ 7000/6000 Seriesは、コピー機能、プリンター機能、スキャナー機能等を有するデジタル複合機（MFP）である（以下、上記SeriesをMFPと呼ぶ）。

MFPは、一般的な業務オフィスに設置され、利用者クライアント（一般利用者クライアント及びシステム管理者クライアント）が接続された内部ネットワーク、

公衆電話回線網、及び直接に一般利用者クライアントと接続されて利用されることを想定している。

TOEは、MFPのコントローラボード上のコントローラROMにインストールされMFP全体の制御を行う一般機能、及び利用済み文書データとTOE設定データを脅威から保護するセキュリティ機能を提供している。

TOEは、一般機能として下記の機能を提供している。

*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

*D-FAX機能
データをプリントジョブとしてMFPに送り、紙に印刷することなしにファクス機能により公衆電話回線網を使用してファクス送信する機能

*iFAX機能
公衆電話回線網を使用することなしに、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

*CWIS機能
一般利用者が操作パネルから指示してスキャンし、MFPの親展ボックスに格納された文書データを、Webブラウザを使用して一般利用者クライアントから取り出す機能。また、システム管理者がTOE設定データの確認や書き換えを行う際に、Webブラウザを使用して行う機能。

*ネットワークスキャン機能
一般利用者が操作パネルから指示してMFPにスキャンした文書データを、MFPに設定されている情報に従い、FTPサーバ、SMBサーバまたはMailサーバに送信する機能

1.2.3 TOE範囲とセキュリティ機能

TOEは、1.2.2で説明した一般機能と下記(1)～(5)のセキュリティ機能を提供している。

TOEの下記セキュリティ機能は、上記一般機能の使用に関連した利用済みの文書データを漏洩の脅威から保護したり、TOEのセキュリティ機能の使用に関連するTOE設定データを変更や漏洩の脅威から保護するためのものである。また、TOEは、組織のセキュリティ方針（2.1.2参照）で要請される、公衆電話回線網から内部

ネットワークに不正アクセスにされないことを実現するセキュリティ機能を提供している。

(1) ハードディスク蓄積データ上書き消去機能
コピー、プリンター及びスキャナー等の各機能の動作後、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機能

(2) ハードディスク蓄積データ暗号化機能
コピー、プリンター及びスキャナー等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能

(3) システム管理者セキュリティ管理機能
操作パネルまたはシステム管理者クライアントから、システム管理者の識別及び認証を行い、TOEのセキュリティ機能に関する設定の参照及び変更をシステム管理者のみが行えるようにする機能

(4) カストマーエンジニア操作制限機能
カストマーエンジニアがTOEのセキュリティ機能に関する設定の変更をできないようにする、システム管理者のみが行える設定機能

(5) ファクスフローセキュリティ機能
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を防ぐ機能

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「Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific セキュリティターゲット」（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]のいずれか）附属書A、CCパート2（[6][9]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]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、「Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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、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20年11月の評価機関による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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。
攻撃者は低レベルの攻撃能力を持つ者であり、TOEの動作について公開されている情報知識を持っていると想定する。

表2-1 想定する脅威

識別子	脅 威
T.RECOVER（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）	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。
T.CONFDATA（TOE設定データへの不正アクセス）	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設定の変更、または不正な読み出しを行うかもしれない。

2.1.2 組織のセキュリティ方針

本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2-2に示す。

表2-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.FAX_OPT	オーストラリア政府機関の要請により、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。

2.1.3 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2-3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2-3　TOE使用の前提条件

識別子	前提条件
A.ADMIN （人的な信頼）	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。
A.SECMODE （保護モード）	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：有効にする * システム管理者パスワード長：7文字以上 * システム管理者ID 認証失敗によるアクセス拒否：有効にする * 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：有効にする * 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
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。

2.1.4　製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。読者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

* ApeosPort-Ⅱ 7000/6000 DocuCentre-Ⅱ 7000/6000 Administrator Guide
* ApeosPort-Ⅱ 7000/6000 Security Function Supplementary Guide

2.1.5　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、ファクス機能等を有するMFPのコントローラソフトウェアである。

本TOEがインストールされたMFP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、またリモートのクライアントPC（一般利用者クライアント及びシステム管理者クライアント）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。

2.2 セキュリティ対策

TOEは、2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たすために以下のセキュリティ機能を具備する。

まず、内部ハードディスク装置に蓄積される文書データを読み出し、不正な再生を行う脅威に対しては、TOEのセキュリティ機能であるハードディスク蓄積データ暗号化機能とハードディスク蓄積データ上書き消去機能により対抗する。

ハードディスク蓄積データ暗号化機能は、システム管理者により「ハードディスク蓄積データ暗号化機能設定」が有効に設定されると、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能、ファクス機能、iFAX機能及びD-FAX機能の動作時に、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を行う。

例えば、同一原稿の複数部数のコピーが指示された場合、コピー対象として読み込まれた文書データは、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。この場合、上記のように読み込まれ、蓄積される文書データは暗号化され、さらに、内部ハードディスク装置から印刷のために読み出される度に復号される。印刷されて利用済みになった文書データは暗号化され、内部ハードディスク装置に蓄積される。

ハードディスク蓄積データ上書き消去機能は、システム管理者により「ハードディスク蓄積データ上書き消去機能設定」が有効に設定されると、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能、ファクス機能、iFAX機能及びD-FAX機能の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、内部ハードディスク装置の文書データ領域を上書きにより消去する。

なお、上記各ジョブの完了時には、利用済みになった文書データがハードディスク蓄積データ暗号化機能により暗号化された後、内部ハードディスク装置に蓄積されるため、暗号化された利用済み文書データに対して上書き消去を行うこととなる。

また、TOE設定データへの不正アクセスの脅威に対しては、TOEのセキュリティ機能であるシステム管理者セキュリティ管理機能とカストマーエンジニア操作制限機能により対抗する。

システム管理者セキュリティ管理機能は、システム管理者のみに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パスワード認証によりシステム管理者のみに制限し、認証されたシステム管理者のみに操作パネル及びシステム管理者クライアントから、TOEのセキュリティ機能の設定に関する参照と変更を行う権限を許可する。

カストマーエンジニア操作制限機能は、システム管理者により「カストマーエンジニア操作制限機能設定」が有効に設定されると、カストマーエンジニアがTOEのセキュリティ機能の設定の変更ができないように、カストマーエンジニアのシステム管理者モードへの操作を制限する機能である。

また、ファクスフローセキュリティ機能は、公衆電話回線網から内部ネットワークに不正アクセスできないことを要請する組織のセキュリティ方針を実現するために、正規のファクス受信以外のいかなる場合においても、USBインタフェースでコントローラボードと接続されているファクスボードを通じて、公衆電話回線網からTOEや内部ネットワークに公衆電話回線データを受け渡さない機能である。

3 評価機関による評価実施及び結果

3.1 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。

3.2 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4月に始まり、平成20年11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20年7月に開発現場へ赴き、図面、記録、現物及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティ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7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。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

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3-1に示す。

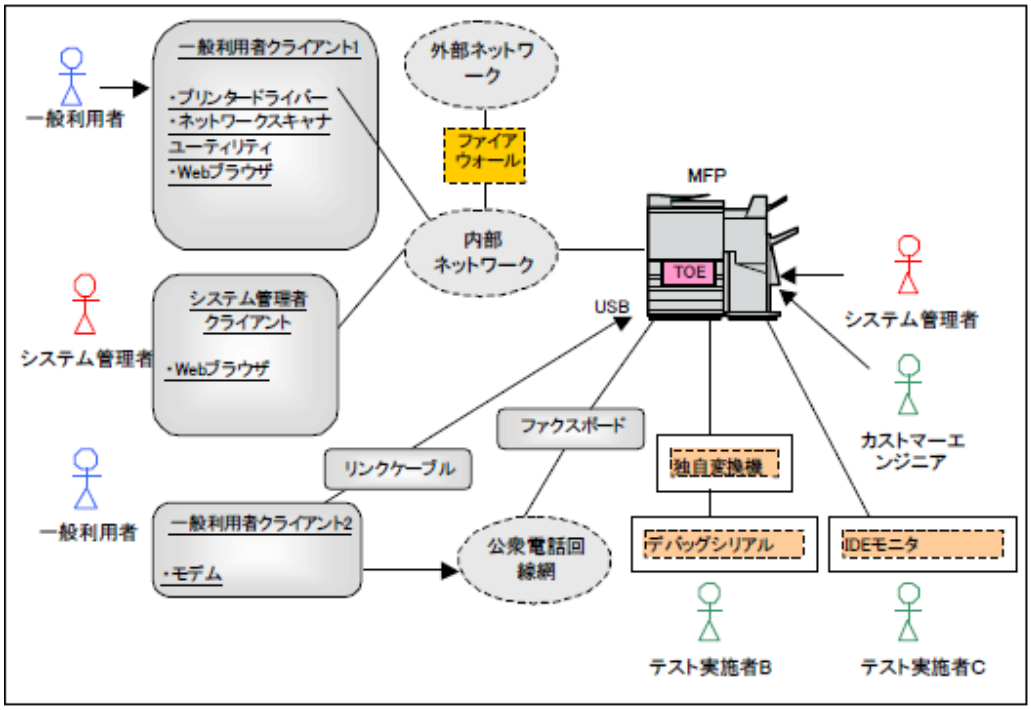

図3-1　開発者テストの構成

開発者テストはSTにおいて識別されているTOE構成（TOEを含むTOE利用のための構成）と同等のTOEテスト環境で実施されている。

本TOEは、ApeosPort-Ⅱ 6000シリーズとApeosPort-Ⅱ 7000シリーズに共通するコントローラソフトウェアであるため、本開発者テストではMFP本体としてApeosPort-Ⅱ 6000が使用された。

また、STでは利用者クライアント（一般利用者クライアント及びシステム管理者クライアント）のOSとして、Windows2000、WindowsXP、またはWindowsVistaをインストールすることが記載されているが、本開発者テストはWindowsXPがインストールされた利用者クライアントのみで実施された。

これは、TOEがOSの標準通信プロトコル機能の上にセキュリティ機能を実装し上記3つのOSは標準通信プロトコル機能が共通しているため、標準通信プロトコル機能とTOEのセキュリティ機能の連携について、WindowsXPでテストし確認できれば、他の2つのOSについても問題ないと判断されたためである。なお、他の2つのOSの標準通信プロトコル機能自体については、開発者として別途テストを実施しており、問題ないことが確認されている。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

（1）TOEのTSFIには、MFPの操作パネル及びシステム管理者クライアントのWebブラウザからアクセスできる。また、一般利用者が操作パネル及び一般利用者クライアント（プリンタードライバー等）からTOEの一般機能を使用すると、自動的にTOEのセキュリティ機能（ハードディスク蓄積データ上書き消去機能等）が動作することとなる。この3つの方法でTSFIにデータを入力する等の刺激を与え、TOEのセキュリティ機能をテストした。

（2）TOEのセキュリティ機能のテスト結果の観測のため、図3-1のデバッグシリアル、及びIDEモニタが使用された。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、及びハードディスク蓄積データ暗号化機能の実行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された。また、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の間のIDEバスに接続され、IDEバスを流れる通信データをモニタリングすることにより、ハードディスク蓄積データ上書き消去機能、及びハードディスク蓄積データ暗号化機能の実行による通信データの内容を確認するために使用された。

（3）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用スイッチ付きの中継ケーブルをハードディスクに接続し、ハードディスクデータ上書き消去機能の動作エラーに関するテスト（電源OFFによる動作エラー後、電源ONにより、動作再開）を実施した。

（4）TOEとのファクス送受信に関わるテスト実施のため、図3-1の一般利用者クライアント2を公衆電話回線網に接続し、ファクス送受信を行った。

b. 実施テストの範囲

テストは開発者によって31項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

c. 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。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、図3-1に示した開発者テストの構成と同等である図3-2に示した構成である。評価者テストはSTにおいて識別されているTOE構成と同等のTOEテスト環境で実施されている。

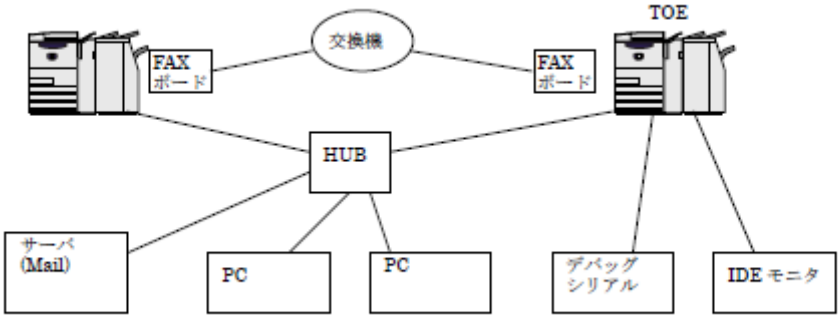

図3-2　評価者テストの構成

なお、本評価者テストは、MFP本体機種としてApeosPort-Ⅱ 6000のみ、クライアントPCにおけるOSとしてWindowsXPのみで実施されたが、STで識別されているすべての種類で実施していない妥当性の根拠は、開発者テスト（3.3.1 1)）記載のものと同一である。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

（1）開発者テストのサンプリングという観点では、開発者が実施したすべてのテスト項目をテストした（サンプリング率100%）。

（2）開発者テストにおいて、セキュリティ機能のふるまいについて厳密なテストが実施されていないインタフェースが存在するため、パラメタの限界値分析の観点で、3項目を独立テストとして取り上げた。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

（1）開発者テストのサンプリングテストにおいては、3.3.1 2) a.記載の開発者テストのテスト手法（デバッグシリアル、IDEモニタ等を使用）と同等（同一であるものを含む）のテスト手法により、テストを実施した。

（2）評価者独自テストとしては、システム管理者セキュリティ管理機能のインタフェースのパラメタ限界値分析として、システム管理者のIDやパスワードの入力、及びパスワードの変更について、設定可能範囲以外のデータが入力された際のふるまいの妥当性をテストした。

c. 結果

実施したすべての評価者独立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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について、必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

評価者は、探索した公知情報から本TOE運用における潜在的な脆弱性4件（Web経由でのクロスサイトスクリプティング、開放ポートによる不正侵入関係）を、また、提供された証拠資料から本TOE運用における潜在的な脆弱性23件を識別し、悪用可能性を判定するために侵入テストが必要であると判断した。

証拠資料から識別された上記潜在的な脆弱性23件の概要を以下に示す。

*保守用ローカルインタフェースによる不正侵入関係

*TOE設定不適切による非セキュア関係

*システム管理者クライアントでの認証迂回

*初期化プロセスへの侵入

*複数システム管理者の同時操作による非セキュア

*システム管理者クライアントの入力フォームへの不正入力関係

*USBポートからの侵入関係

*CWISからのプリント要求インタフェースの不正使用

*操作パネルでの不正操作・設定関係

*CWISからの不正設定関係

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

侵入テストは、上記a.で識別された27件の潜在的な脆弱性に対して、相互類似も考慮し、10項目としてまとめられ、詳細にテストされた。

主な侵入テストは以下のとおりである。

*MFPのLANポートからの不要なポート開放に関するポートスキャン調査

*USBポートからのTOE不正アクセス試行

*システム管理者クライアントのWebブラウザからの不正試行（ユーザ認証URLを記録し認証迂回、操作パネルや別のシステム管理者クライアントとの同時TOE設定操作、入力フォームにスクリプト等不正データ入力、パラメタ入力で制限を越えた種類・値を入力）

*TOE設定データ格納媒体のすり替え

*一般利用者クライアントのWebブラウザからの不正試行（プリント要求で不正プログラム混入、初期化処理中のTOEアクセス）

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を超える潜在的な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 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。

3.4.2　　評価者コメント/勧告

特になし。

4 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 所見報告書でなされた指摘内容が妥当であること。
② 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、本ST及び評価報告書において、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、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、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すものと判断する。

5.2 注意事項

特になし。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
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）
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 Functionality（TOEセキュリティ機能）
TSFI	TSF Interface（TSFインタフェース）

本報告書で使用されたTOEに関する略語を以下に示す。

CWIS	Centre Ware Internet Service（センターウェアインターネットサービス）
D-FAX	Direct FAX（ダイレクトファクス）
iFAX	Internet FAX（インターネットファクス）
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）。本報告書では、Fuji Xerox ApeosPort-Ⅱ 7000/6000 Seriesを指す。
PDL	Page Description Language（ページ記述言語）

本報告書で使用された用語の定義を以下に示す（順不同。左記用語を理解するための関連用語を含む）。

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。
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。
カストマーエンジニア	MFPの保守/修理を行うエンジニア。
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。
利用者クライアント	一般利用者クライアントとシステム管理者クライアントの総称。
システム管理者モード	一般利用者がMFPの機能を利用する動作モードとは別に、システム管理者がTOEの使用環境に合わせて、TOE機器の動作設定やTOEセキュリティ機能設定の参照/更新といった、設定値の変更を行う動作モード。
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。
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（iFAX）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。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できる。
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ものが含まれる。 *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、内部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、カストマーエンジニア操作制限情報、本体パネルからの認証時のパスワード使用情報、システム管理者ID とパスワード情報、システム管理者認証失敗によるアクセス拒否情報。
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とMFP間のチャネルを指す。

7 参照

[1] Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific セキュリティターゲット バージョン 1.0.9 2008年9月26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 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] Fuji Xerox ApeosPort-Ⅱ 7000/6000 Series Controller Software for Asia Pacific 評価報告書 第2.4版 2008年11月4日 有限責任中間法人 ITセキュリティセンター 評価部