認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成22年11月5日 (IT認証0321)
認証番号	C0298
認証申請者	富士ゼロックス株式会社
TOEの名称	Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific
TOEのバージョン	Controller ROM Ver. 1.101.7
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	一般社団法人 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23年6月23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　山里　拓己

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 リリース3
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 リリース3

評価結果：合格

「Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 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

この認証報告書は、富士ゼロックス株式会社が開発した「Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific、 バージョン Controller ROM Ver. 1.101.7」（以下「本TOE」という。）について一般社団法人 ITセキュリティセンター 評価部（以下「評価機関」という。）が平成23年5月30日に完了した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とともに、本TOEに関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本TOEのセキュリティ機能要件、保証要件及びその十分性の根拠は、STにおいて詳述されている。

本認証報告書は、本TOEを搭載したデジタル複合機を購入する調達者を読者と想定している。本認証報告書は、本TOEが適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

本TOEの保証パッケージは、EAL3である。

1.1.2 TOEとセキュリティ機能性

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デジタル複合機（以下「MFD」という。）に搭載される、MFD全体の制御を行うコントローラソフトウェアある。本TOEは、富士ゼロックス株式会社製のMFDである、Fuji Xerox ApeosPort-IV C7780/C6680/C5580 Series及びFuji Xerox DocuCentre-IV C7780/C6680/C5580 Seriesで動作する。

本TOEは、コピー機能、プリンター機能、スキャナー機能、ファクス機能等のMFDの基本機能に加えて、基本機能で扱う文書データやセキュリティに影響する設定データ等を漏えいや改ざんから保護するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

TOEの保護資産である利用者の文書データ及びセキュリティに影響する設定データは、TOEの不正操作、TOE内の内部ハードディスク装置からの直接読出し、TOEが設置されているネットワーク上の通信データへのアクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

そのためTOEは、TOEの利用者を識別認証し、その利用者が可能な操作だけを許可することで、TOEの不正操作を防止する。また、保護資産を内部ハードディスク装置に格納する際には暗号化を行い、保護資産を削除する際には上書き消去することで、内部ハードディスク装置からの直接読出しを防止する。さらに、ネットワーク通信の際に暗号通信プロトコルを適用することで、通信データの不正な読出しや改ざんを防止する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定している。

本TOEを搭載したMFDは、一般的な業務オフィスにおいて、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワークに接続されて利用されることを想定している。

本TOEの運用にあたっては、信頼できる管理者を任命し、ガイダンス文書に従って、TOEを搭載したMFD及びTOEとデータをやり取りするその他のIT機器を正確に構成設置し、維持管理しなければならない。

1.1.3 免責事項

本TOEには、以下に示す運用上の条件やセキュリティ機能を提供しない場合が存在する。

本評価では、カストマーエンジニア操作制限をはじめとする設定条件が適用された構成だけがTOEとして評価されている。従って、「表 7-6　TOEの構成条件」に示す設定を変更した場合、それ以降は本評価による保証の対象外となる。

TOEは、外部認証機能とS/MIME機能を有しているが、それらの機能はApeosPort-IVシリーズでのみ有効であり、DocuCentre-IVシリーズでは提供していない。（DocuCentre-IVシリーズには、電子メール及びインターネットファクス機能は提供されているが、上記の「表 7-6　TOEの構成条件」に従って使用できないように設定されるため、本評価対象の構成には含まれていない。）

TOEは、ダイレクトファクス機能を提供しているが、それらの機能は本体認証時

に限定され、外部認証時は評価の対象外である。

1.2 評価の実施

認証機関が運営するITセキュリティ評価・認証制度に基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本TOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成23年5月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本TOEの評価が所定の手続きに沿って行われたことを確認した。本TOEの評価がCC（[5][6]または[8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本TOEは、以下のとおり識別される。

TOE名称：	Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific
バージョン：	Controller ROM Ver. 1.101.7
開発者：	富士ゼロックス株式会社

本TOEは、MFDであるFuji Xerox ApeosPort-IV C7780/C6680/C5580 SeriesまたはFuji Xerox DocuCentre-IV C7780/C6680/C5580 Seriesのコントローラソフトウェア部分である。

製品が評価･認証を受けた本TOEであることを、利用者は以下の方法によって確認することができる。

ガイダンスに記載された手順に従って操作パネルを操作し、画面に表示されたバージョン情報、または、設定値リストのプリント出力に記述されたバージョン情報をガイダンスの当該記載と比較することにより、設置された製品が評価を受けた本TOEであることを確認する。

3 セキュリティ方針

本章では、本TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEは、コピー機能、プリンター機能、スキャナー機能、ファクス機能等のMFD機能を提供しており、利用者の文書データを内部のハードディスク装置に蓄積したり、ネットワークを介して利用者の端末や各種サーバとやりとりしたりする機能を有している。

TOEは、それらのMFD機能を使用する際に、利用者の識別認証とアクセス制御、ハードディスク装置の蓄積データの暗号化とデータ削除時の上書き消去、暗号通信プロトコルといったセキュリティ機能を適用することで、保護資産である利用者の文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。また、TOEは、セキュリティ機能に関するログを記録する機能や、TOE自身の改ざんをチェックする機能を備えている。

なお、TOEは、使用に関して以下の役割を想定し、役割に応じたアクセス制御機能を提供する。

・一般利用者

一般利用者は、TOEが提供するコピー機能、プリンター機能、スキャナー機能、ファクス機能等の利用者である。

・システム管理者（機械管理者＋SA）

システム管理者は、TOEのセキュリティ機能の設定や、その他機器設定を行うための、特別な権限を持つ利用者である。システム管理者は、機械管理者とSA(System Administrator)の総称である。機械管理者はすべての管理機能が使用可能であり、SAは一部の管理機能が使用可能である。SAの役割は、利用組織の必要に応じて機械管理者が設定する。

・カストマーエンジニア

カストマーエンジニアは、MFDの保守/修理を行うエンジニアである。

また、TOEは、組織のセキュリティ方針により、ファクスで使用する公衆電話網から内部ネットワークにアクセスすることを防止する機構を備えている。

3.1 セキュリティ機能方針

TOEは、3.1.1に示す脅威に対抗し、3.1.2に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本TOEは、表 3-1に示す脅威を想定し、これに対抗する機能を備える。

表 3-1 想定する脅威

識別子	脅 威
T.CONSUME	TOEの利用を許可されていない者が、TOEを不正に利用するかもしれない。
T.DATA_SEC	TOEの利用を許可されている利用者が、許可されている権限範囲を超えて、文書データ及びセキュリティ監査ログデータを不正に読み出すかもしれない。
T.CONFDATA	TOEの利用を許可されている一般利用者が、システム管理者のみアクセスが許可されているTOE設定データに対して、不正な読み出しや設定の変更を行うかもしれない。
T.RECOVER	攻撃者が、内部ハードディスク装置を取り出して、内部ハードディスク装置上の利用済み文書データや文書データ、及びセキュリティ監査ログデータを不正に読み出して漏洩するかもしれない。
T.COMM_TAP	攻撃者が、内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータ及びTOE設定データを盗聴や改ざんをするかもしれない。

3.1.1.2 脅威に対するセキュリティ機能方針

本TOEは、表3-1に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.CONSUME」「T.DATA_SEC」「T.CONFDATA」への対抗

TOEは、「ユーザー認証機能」、「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」及び「セキュリティ監査ログ機能」で対抗する。

「ユーザー認証機能」は、識別認証の成功した利用者だけにTOEの利用を許可する。また、識別認証された利用者が、親展ボックスや文書データを操作する際には、当該利用者に許可された操作だけが実行できる。

「システム管理者セキュリティ管理機能」は、セキュリティ機能に関する設定データの参照と設定変更及びセキュリティ機能の有効/無効の設定変更を、識別認証された管理者だけに許可する。従って、システム管理者以外が、誰でも文書データやセキュリティ監査ログデータを読み出せるようにTOEを設定することはできない。

「カストマーエンジニア操作制限機能」は、カストマーエンジニアの操作制限の有効/無効を制御する設定データについて、その参照と設定変更を識別認証された管理者だけに許可する。

「セキュリティ監査ログ機能」は、利用者のログイン/ログアウト、ジョブ終了、設定変更等の監査ログを取得し、その読出しを識別認証された管理者だけに許可する。これにより、利用者へのなりすましなどの不正操作を検出できる。なお、監査ログを格納する領域が満杯になった時は、最も古い監査ログに上書きして記録される。

以上により、TOEの正当な利用者に対して利用者毎の権限範囲で許可された操作だけが実行可能であり、TOEの不正な利用や保護資産の不正アクセスが防止される。

(2) 脅威「T.RECOVER」への対抗

TOEは、「ハードディスク蓄積データ上書き消去機能」と「ハードディスク蓄積データ暗号化機能」で対抗する。

「ハードディスク蓄積データ暗号化機能」は、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、ファクス機能及びダイレクトファクス機能といったMFD基本機能の動作時に、文書データを内部ハードディスク装置に蓄積する際に、文書データの暗号化を行う。また、セキュリティ監査ログ機能で生成した監査ログデータを内部ハードディスク装置に蓄積する際に、監査ログデータの暗号化を行う。

「ハードディスク蓄積データ上書き消去機能」は、各MFD基本機能のジョブの完了後に、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、利用が終了した文書データを内部ハードディスク装置から削除する前に内部ハードディスク装置の文書データ領域のデータを上書きにより消去する。

以上により、ハードディスク装置に蓄積された文書データは暗号化によって不正な読出しが防止され、利用済み文書データは上書き消去によって再生や復元が不可能になる。

(3) 脅威「T.COMM_TAP」への対抗

TOEは、「内部ネットワークデータ保護機能」で対抗する。

「内部ネットワークデータ保護機能」は、TOEとクライアント端末（以下、「クライアント」という。）や各種サーバとの通信時に、暗号通信プロトコルを適用する。対応している暗号通信プロトコルは、SSL/TLS、IPsec、SNMPv3、S/MIMEである。

これにより、内部ネットワークでやり取りされる文書データ、セキュリティ監査ログデータ及びTOE設定データは、暗号通信プロトコルが適用され、盗

聴や改ざんが防止される。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 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 3-2に示す。

表 3-2 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。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOEは、表 3-2に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.FAX_OPT」への対応

TOEの「ファクスフローセキュリティ機能」は、指定されたファクスモデムからのみファクスデータを受信し、そのデータをファクス機能以外へ渡さない構造により、公衆回線網から受信したデータを、いかなる場合においても内部ネットワークへの送信に受け渡さない。

これにより、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する。

4 前提条件と使用環境

本章では、想定する読者が本TOEの利用の判断に有用な情報として、本TOEを運用するための前提条件及び使用環境について記述する。

4.1 使用及び環境に関する前提条件

本TOEを運用する際の前提条件を表4-1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 4-1 前提条件

識別子	前提条件
A.ADMIN	システム管理者は、TOEセキュリティ機能に関する必要な知識を持ち、課せられた役割に従い、悪意をもった不正を行わないものとする。
A.SECMODE	システム管理者はTOEを運用するにあたり、組織のセキュリティポリシー及び製品のガイダンス文書に従ってTOEを正確に構成設置し、TOEとその外部環境の維持管理を遂行するものとする。

4.2 使用環境と構成

本TOEを搭載したMFDは、一般的な業務オフィスにおいて、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワーク、及びファクスボードを介して公衆電話回線網に接続されて利用されることを想定している。本TOEの一般的な使用環境を図 4-1に示す。

内部ネットワークには、Mailサーバ、FTPサーバ、SMBサーバ、LDAPサーバ、Kerberosサーバが搭載されたサーバコンピュータ、及び一般利用者用のクライアント、システム管理者用のクライアントが接続され、TOEと文書データ等の通信を行う。

TOEの利用者は、MFDの操作パネル、内部ネットワークに接続された一般利用者クライアント、システム管理者クライアントを操作して、TOEを使用する。一般利用者クライアントは、USBを経由してTOEを操作することもできる。

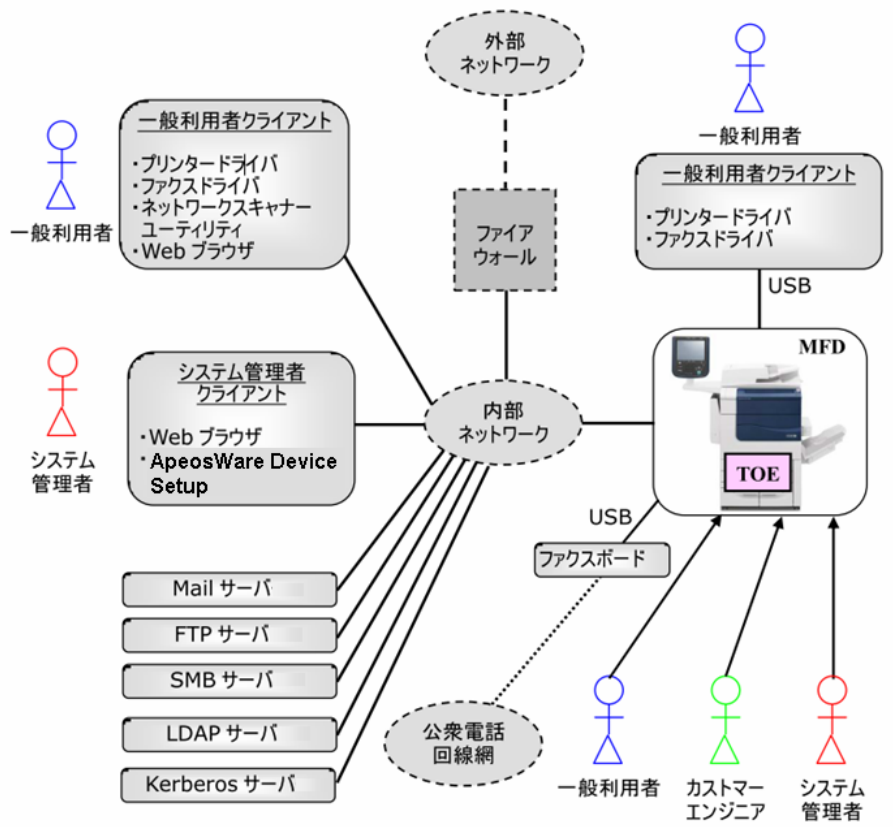

図 4-1 TOEの使用環境

TOEの使用環境の構成品について以下に示す。

(1) MFD

TOEが搭載されるデジタル複合機である。本TOEを搭載可能なMFDは、以下の機種である。

・Fuji Xerox ApeosPort-IV C7780/C6680/C5580 Series
・Fuji Xerox DocuCentre-IV C7780/C6680/C5580 Series

ただし、DocuCentre-IVシリーズの電子メールとインターネットファクス機能については、使用できないように設定されるため、評価対象外である。

(2) ファクスボード

MFDにファクス機能が搭載されていても、MFDとUSBで接続するファクスボードは別売りである。ファクス機能を使用したい利用者は、ファクス機能が搭載されているMFD機種を選択すると共に、富士ゼロックス株式会社が指定するファクスボードを別途購入する必要がある。

(3) 一般利用者クライアント

一般利用者が使用する汎用のパソコンであり、USBポート、または内部ネッ

トワークを介してTOEと接続する。以下のソフトウェアが必要である。

・OSは、Windows XP、Windows Vista、Windows 7のいずれか。
・プリンタードライバ、ファクスドライバ

内部ネットワーク接続の場合には、上記に加えて、以下のソフトウェアが必要である。

・Webブラウザ(OS附属のもの)
・ネットワークスキャナーユーティリティ

(4) システム管理者クライアント

システム管理者が使用する汎用のパソコンであり、内部ネットワークを介してTOEと接続する。以下のソフトウェアが必要である。

・OSは、Windows XP、Windows Vista、Windows 7のいずれか。
・Webブラウザ(OS附属のもの)
・ApeosWare Device Setup

(5) LDAPサーバ、Kerberosサーバ

ユーザー認証機能として「外部認証」を設定した場合、LDAPサーバ、Kerberosサーバのいずれかの認証サーバが必要となる。ユーザー認証機能として「本体認証」を設定した場合は、どちらも必要ない。

また、LDAPサーバは、「外部認証」時に、SA役割を判別するための利用者属性を取得するためにも使用される。従って、Kerberosサーバによる認証の場合であっても、SA役割を使用する場合には、LDAPサーバが必要である。

(6) Mailサーバ、FTPサーバ、SMBサーバ

TOEは、Mailサーバ、FTPサーバ、SMBサーバと文書データをやり取りする基本機能を持つため、これらのMFDの基本機能を利用する際に、必要に応じてこれらのサーバを設置する。

なお、本構成に示されているTOE以外のソフトウェアやハードウェアの信頼性は本評価の範囲ではない。

4.3 使用環境におけるTOE範囲

① TOEのプリンター機能には、TOEが一般利用者クライアントから受信した印刷データを、一旦、内部ハードディスク装置に蓄積して操作パネルから印刷指示をした時点で印刷を行う「蓄積プリント」と、受信すると即時に印刷する「通常プ

リント」がある。TOEのセキュリティ機能が有効に設定された場合は、一般利用者クライアントから「通常プリント」を実行しても、TOEにおいて必ず自動的に「蓄積プリント」に置き換えて実行する。本評価では、「蓄積プリント」だけが評価の対象であり、「通常プリント」は評価の対象外である。

② TOEのユーザー認証機能では、TOE内に登録した情報を使用して識別認証を行う「本体認証」と、TOE外の認証サーバ（LDAPまたはKerberosプロトコル）を使用して識別認証を行う「外部認証」をサポートしている。TOEで「外部認証」を使用している場合、以下の制約がある。「本体認証」の場合には、これらの制約はない。

- 外部認証時、MFD基本機能のダイレクトファクス機能は、評価対象外である。
- 外部認証時、一般利用者クライアントのネットワークスキャナーユーティリティの使用は、評価対象外である。
- 外部認証時、TOEが印刷データを受信した時点では、識別認証は行われない。（ただし、本評価では「蓄積プリント」機能により、TOEが受信したデータを印刷するためには、操作パネルからの識別認証後、印刷指示が必要である。）

③ DocuCentre-IV Seriesに対しては、「外部認証」とS/MIME機能は提供していない。

（S/MIME機能は、Eメール及びインターネットファクス機能で使用される。しかし、DocuCentre-IV Seriesでは、電子メール及びインターネットファクス機能は提供されているが、使用できないように設定されるため、本評価対象の構成には含まれていない。）

これらの禁止された機能を使用した場合、文書データが漏えいするなどの問題が発生する恐れがある。これらへ対抗するためには、ガイダンスに従ってTOEやIT環境を正しく設定することが必要であり、それらは運用者の責任となる。

5 アーキテクチャに関する情報

本章では、本TOEの範囲と主要な構成について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

図 5-1に、TOEを搭載したMFDの構成を、MFD以外のIT環境と共に示す。図 5-1で、MFDは、コントローラボード、操作パネル、内部ハードディスク装置、ADF、IIT、IOTの部分である。その中でTOEは、コントローラボードのController ROMに格納された、各種機能を実現するソフトウェア部分である。MFDのハードウェアやファクスボード等は、TOEの範囲ではない。

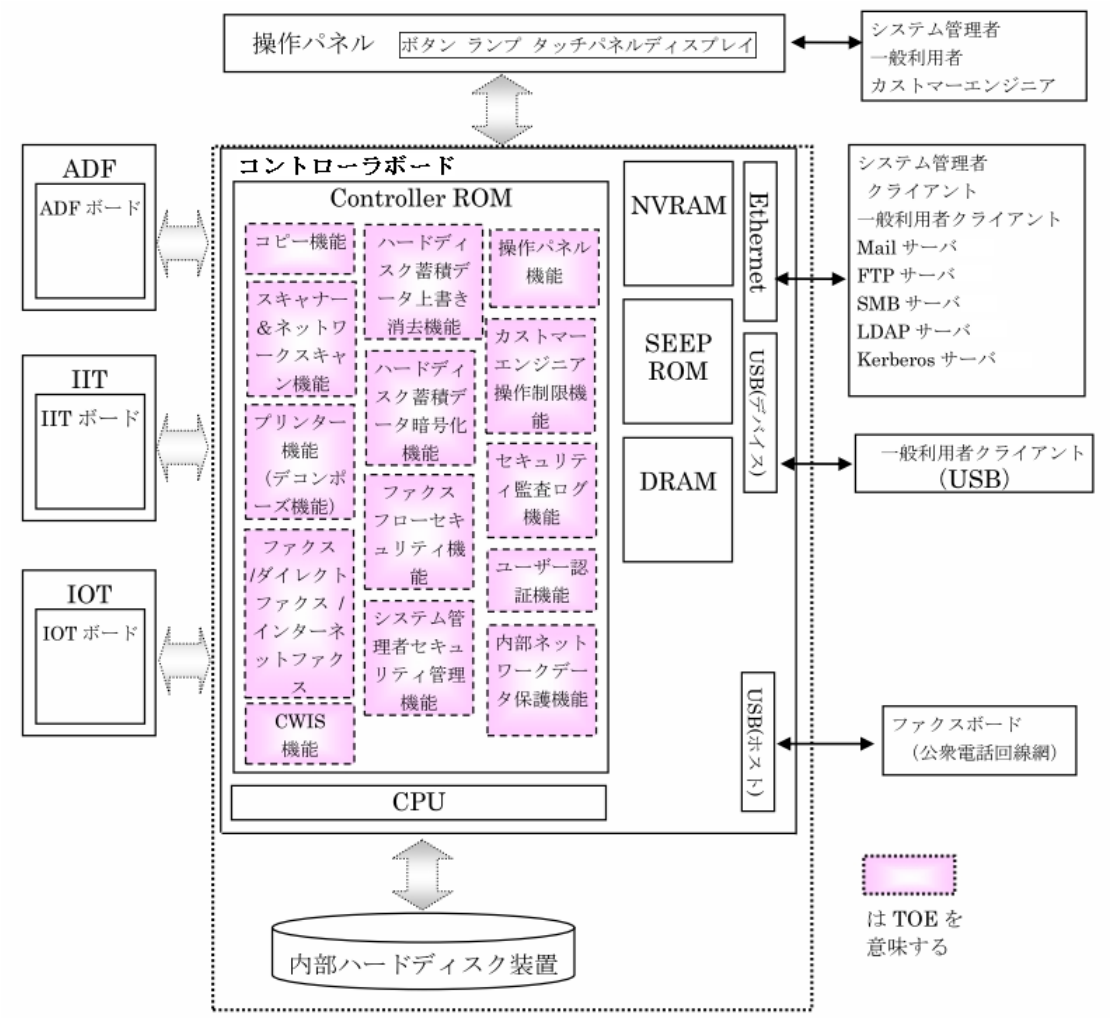

図 5-1 TOE境界

TOEは、3章で説明したセキュリティ機能と、それ以外のMFDの基本機能で構成される。MFDの基本機能については、11章の用語説明を参照。

TOEのセキュリティ機能は、利用者がMFDの基本機能を使用する際に適用される。以下、セキュリティ機能とMFDの基本機能の関係について説明する。

① 利用者が、MFDの基本機能、システム管理者セキュリティ管理機能、セキュリティ監査ログ機能の中の監査ログを参照する機能を使用する際には、ユーザー認証機能が適用され、識別認証された利用者はその役割に応じた操作を許可される。識別認証された利用者には、その役割に応じたメニューが表示され、MFDの基本機能、システム管理者セキュリティ管理機能、セキュリティ監査ログ機能が使用できる。利用者の操作入力は、権限に照らし合わせて許可／不許可が判断され、実行される。また、これらの機能を使用する際に、セキュリティ監査ログ機能によって、監査ログが生成される。

② ①の利用時に、内部ハードディスク装置に格納される文書データ及び監査ログに対しては、ハードディスク蓄積データ暗号化機能が適用され、文書データを削除する際には、ハードディスク蓄積データ上書き消去機能が適用される。これらの処理は、利用者が意識して蓄積や削除した文書データだけでなく、コピー機能等の処理の都合で利用者が意識することなく一時的にハードディスク装置に蓄積された文書データも対象となる。

③ ①の利用時に、TOEを搭載したMFDと、その他のIT機器が内部ネットワークを経由して通信する場合には、内部ネットワークデータ保護機能が適用される。また、ファクスに対しては、ファクスフローセキュリティ機能が適用される。

5.2 IT環境

TOEは、Controller ROMに格納され、Controller ROMが実装されたコントローラボードがMFDに搭載されて動作する。

MFDと内部ネットワークで接続する各種サーバ、システム管理者クライアント、一般利用者クライアントは、暗号通信プロトコルIPsecを使用して通信を行う。さらに、クライアントに搭載されるWebブラウザに対してはSSL/TLS、Mailサーバとやり取りするメールに対してはS/MIME、ネットワーク管理にはSNMPv3を使用する。TOEと認証サーバ間の通信は、LDAP(SSL/TLS)、Kerberosプロトコルを用いて、TOEと通信相手を相互に認証し、内部ネットワーク上に流れる識別認証に関連するデータ暗号化する。

「外部認証」によるユーザー認証機能を有効に設定した場合、TOEは、外部認証サーバへ利用者の識別認証の判断を問い合わせる。ただし、機械管理者は、外部認証サーバでは識別認証されず、TOE内に登録した機械管理者の情報を使用して識別

認証される。TOEの設定で、LDAPサーバによる外部認証を選択した場合は、LDAPサーバ内で利用者IDとパスワードの照合が行われ、TOEはその結果を利用する。Kerberosサーバによる外部認証を選択した場合は、KerberosサーバとTOEの協調動作で識別認証が実施される。いずれの場合も、9桁以上のパスワードを設定することが必要である。また、TOEの設定で外部認証を選択した場合は、LDAPサーバとKerberosサーバのいずれの場合であっても、TOEは、LDAPサーバから取得した利用者属性を使用して、利用者がSA役割であるかどうかを判断する。

一般利用者は、プリンタードライバ、ファクスドライバ、ネットワークスキャナーユーティリティ、Webブラウザのいずれかがインストールされた一般利用者クライアントから、内部ネットワークもしくはUSB接続を経由してTOEを利用することができる。システム管理者は、Webブラウザ、ApeosWare Device Setupのいずれかがインストールされたシステム管理者クライアントから、ネットワークを経由してTOEを設定することができる。

TOEとクライアント間の通信は、暗号化通信プロトコル（SSL/TLS，IPsec，SNMPv3，S/MIME）を用いて、通信相手の識別認証や内部ネットワーク上に流れる文書データ、セキュリティ監査ログデータ及びTOE設定データの暗号化を行う。

6 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。TOEの利用者は、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-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Administrator Guide (ME4906E1-1)
- ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 User Guide(ME4905E2-1)
- ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Security Function Supplementary Guide (ME5155E2-1)

7 評価機関による評価実施及び結果

7.1 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。

7.2 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22年11月に始まり、平成23年5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23年2月から3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・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。平成23年5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、配付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23年2月から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。

7.3 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。

7.3.1 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 7-1に示す。

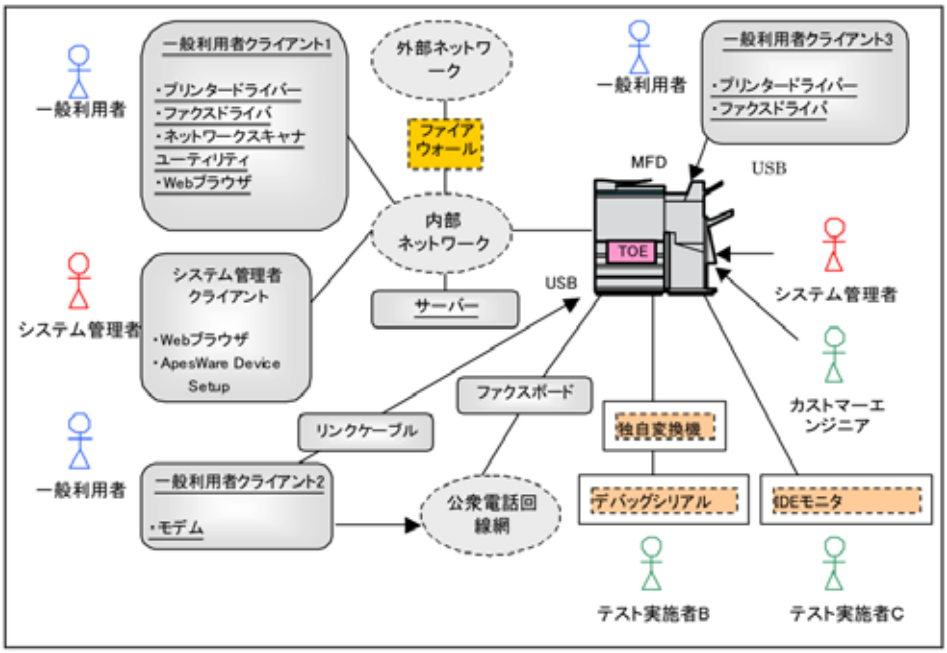

図 7-1 開発者テストの構成

評価の対象となったTOEは、2章のTOE識別と同一のTOEである。

テストに使用したMFDは、ApeosPort-IV C7780(AP)、DocuCentre-IV C7780(AP)の2機種である。TOEは、Fuji Xerox ApeosPort-IV C7780/C6680/C5580 Seriesと、Fuji Xerox DocuCentre-IV C7780/C6680/C5580 Seriesで共通のコントローラソフトウェアであり、両シリーズの代表機種をテストすることで、機種による差異を含めてすべての機能を確認することができ、十分であることが、評価者により評価されている。

TOEを搭載したMFD以外の構成要素を表 7-1に示す。

表 7-1　開発者テストの構成要素

名称	詳細
サーバ	Mailサーバ、LDAPサーバ、Kerberosサーバとして使用 • Microsoft Windows Server 2008 Service Pack 2 (LDAPサーバ、Kerberosサーバ) • Wireshark Version 1.4.1 • Xmail Version 1.27
システム管理者クライアント	システム管理者クライアントとして使用
システム管理者クライアント(1)	• Microsoft Windows 7 Professional • Microsoft Internet Explorer 8 • ApeosWare Device Setup Version 1.1.0 • Wireshark Version 1.4.1
システム管理者クライアント(2)	• Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6 • ApeosWare Device Setup Version 1.1.0
システム管理者クライアント(3)	• Microsoft Windows VISTA Business Service Pack 2 • Microsoft Internet Explorer 7 • ApeosWare Device Setup Version 1.1.0 • Microsoft Windows メール
一般利用者クライアント1	一般利用者クライアント（内部ネットワーク経由の接続）及びSMBサーバとして使用 • SMBサーバ（OS標準搭載ソフトウェア）
一般利用者クライアント1(1)	• Microsoft Windows 7 Professional • Microsoft Internet Explorer 8 • ネットワークスキャナーユーティリティ Ver.1.7.6 • プリンタードライバ／ファクスドライバ Version 6.4.3 • Wireshark Version 1.4.1
一般利用者クライアント1(2)	• Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6
一般利用者クライアント1(3)	• Microsoft Windows VISTA Business Service Pack 2 • Microsoft Internet Explorer 7 • Microsoft Windows メール
一般利用者クライアント2	ファクス送受信と、MFDのファクス接続用USBポートが他用途に使用できないことの確認に使用。パソコンのモデムポートを公衆電話回線網に接続。パソコンのUSBポートを、リンクケーブル（USBケーブル）を介してMFDのファクスボード用USBポートに接続 • Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6 • ネットワークスキャナーユーティリティ Ver.1.7.6 • プリンタードライバ／ファクスドライバ Version 6.4.3
一般利用者クライアント3	一般利用者クライアント（プリンター用のUSBポート経由の接続）として使用 • Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6 • ネットワークスキャナーユーティリティ Ver.1.7.6 • プリンタードライバ／ファクスドライバ Version 6.4.3

名称	詳細
IDEモニタ (パソコン+専用機器)	内部ハードディスク装置の接続されたIDEバスを流れるデータをモニタするツール。Windows XP搭載パソコンにIDEバスから直接モニタできる専用機器(Catalyst Enterprises社)を接続し、専用ソフトウェア(Serial ATA Analyzer)を使用する。 • Microsoft Windows XP • Serial ATA Analyzer Version 1.984.0401
デバッグシリアル	MFDのデバッグ用端末。システム管理者クライアント用パソコンのシリアルポートを、富士ゼロックス製の独自の変換基盤を経由して、MFDのデバッグ用の端末ポートと接続 • Microsoft Windows 7 Professional • TeraTerm Pro Version 2.3
独自変換機	MFDとデバッグシリアルを接続するための開発用機材
内部ネットワーク	スイッチングハブを使用
公衆電話回線網	公衆電話回線網の代替として疑似交換機(ハウ社)を使用。
ファクスボード	富士ゼロックス製のMFDのオプション。 • Fax ROM Version 1.1.2
リンクケーブル	MFDと一般利用者クライアント2をUSB接続するケーブル

外部ネットワークとファイアウォールは、テスト内容に影響しないため、使用しない。

開発者テストは本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。

なお、STでは、利用者クライアントとして、開発者テストで用いられたWindows XP（WebブラウザはInternet Explorer 6.0）、Windows 7（WebブラウザはInternet Explorer 8）の他に、Windows VISTA（WebブラウザはInternet Explorer 7）が記載されているが、本TOEに依存する機能の確認は、Windows XPとWindows 7のテストで十分であり、Windows VISTAの動作も問題ないことが評価者により評価されている。

FTPサーバのテストは、FTPサービスのテストとセキュアなFTP通信のテストに分離して行われた。FTP通信はFTPサービスとは独立したIPsecのしくみによって保護されるため、それぞれ独立したテストによって確認している。

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。

＜開発者テスト手法＞

開発者は、以下のセキュリティ機能に関するテストを実施する。

① MFDの操作パネル、システム管理者クライアント、一般利用者クライアントからMFDの基本機能やセキュリティ管理機能を操作して、その結果のMFDのふるまい、パネル表示、監査ログ内容を確認する。
一般利用者とシステム管理者について、本体認証機能と外部認証機能(LDAP, Kerberos)を用いたログイン処理やログイン後の機能制限をテストする。認証失敗によるロック機能やパスワード変更機能などのアカウントの管理機能、一般利用者とシステム管理者の機能が分離されていることも、テストする。ユーザー認証機能（本体認証、外部認証）や各種処理など、監査対象とした事象が、ログに記録されることをテストする。カストマーエンジニアの操作制限機能が有効に設定されている場合は、カストマーエンジニアがログインできないことを確認する。
また、システム管理者がWebブラウザ(CWIS)からログを取得するテストを行う。

② ハードディスク蓄積データ上書き消去機能の確認のために、テスト用ツールであるIDEモニタを使用して、内部ハードディスク装置へ書き込まれる上書き消去用データと、上書き消去用データの書き込み後の内部ハードディスク装置の内容を読み出して観測する。上書き消去回数の変更や上書き消去中のエラー、上書き消去再開処理についてもテストする。

③ ハードディスク蓄積データ暗号化機能の確認のために、デバッグ用のシリアルポートを使用して、内部ハードディスク装置に格納された文書等を直接参照し、暗号化されていることを観測する。また、暗号化された内部ハードディスク装置を、同一機種の暗号鍵の異なるMFDの内部ハードディスク装置と入れ替えても、操作パネルにエラーが表示され、使用できないことを確認する。また、暗号鍵を変更した時に、暗号化された文書データ等が消去される等、内部ハードディスク装置が工場出荷状態に初期化されることを確認する。

④ IPsec等の暗号通信プロトコル機能の確認のために、後述するテストツールを使用して、仕様通りの暗号通信プロトコルが適用されていることを観測する。

⑤ 一般利用者クライアント2を公衆電話回線網経由で接続し、MFDとのファクス送受信用に使用する。また、ファクスフローセキュリティ機能の確認のために、一般利用者クライアント2から公衆電話回線網を経由してTOEにダイアルアップ接続ができないことを観測する。さらに、一般利用者クライアント2からファクスボード接続用のUSBポートに直接接続しても、TOEの操作ができないことを観測する。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-2に示す。

表 7-2　開発者テストツール

ツール名称	概要・利用目的
IDEモニタ(パソコン＋専用機器) ※構成は表 7-1参照	MFD内の内部ハードディスク装置接続用のIDEバスのデータをモニタし、内部ハードディスク装置に書き込まれるデータを観測する。また、内部ハードディスク装置に書き込まれたデータを読み出す。
プロトコルアナライザ (Wireshark Version 1.4.1)	内部ネットワーク上の通信データをモニタし、暗号通信プロトコルが、仕様通りにIPsec、SSL/TLS、SNMPv3であることを確認する。
メーラー (Windows Live Mail Version 2009)	TOEとメールサーバを介して、電子メールを送受信し、S/MIMEによる暗号化と署名が仕様通りであることを確認する。
デバッグシリアル (MFDのデバッグ用パソコン)	内部ハードディスク装置に書き込まれたデータを読み出して、その内容を確認する。
独自変換機	コントローラボードの出力コネクタとデバッグシリアル(デバッグ用パソコン)を接続するための独自の変換機

＜開発者テストの実施＞

各種インタフェースより、MFDの基本機能とセキュリティ管理機能を操作し、様々な入力パラメタに対して、適用されるセキュリティ機能が仕様通りに動作することを開発者のテスト結果とあらかじめ期待されたテスト計画書の値との比較によって確認した。なお、ユーザー認証機能については、利用者の役割毎に、本体認証、外部認証（LDAPサーバ）、外部認証（Kerberosサーバ）の各場合について、仕様通りに動作することを確認した。

また、パスワード誤りによるアカウントロックやMFD本体の電源OFFによる上書き消去処理の中断と電源ONによる再開などのエラー時に関するテスト、ファクスからの内部ネットワークへのアクセス防止が、仕様通りに動作することを確認した。暗号化通信については、プロトコルアナライザ(Wireshark)を利用して通信をモニタして確認した。

b. 実施テストの範囲

テストは開発者によって、以下の範囲から65項目が実施されている。

- ユーザー認証機能テスト
- 上書き消去機能テスト
- 暗号化機能テスト
- カストマーエンジニアの操作制限機能テスト
- ファクスフローセキュリティテスト
- セキュリティ監査ログテスト
- ネットワーク保護機能テスト

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。深さ分析が実施され、TOE設計に記述されたすべてのサブシステムとサブシステム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

評価者は、開発者によるテスト結果が、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。

7.3.2 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

評価者が実施した独立テストの構成を、図 7-2に示す。

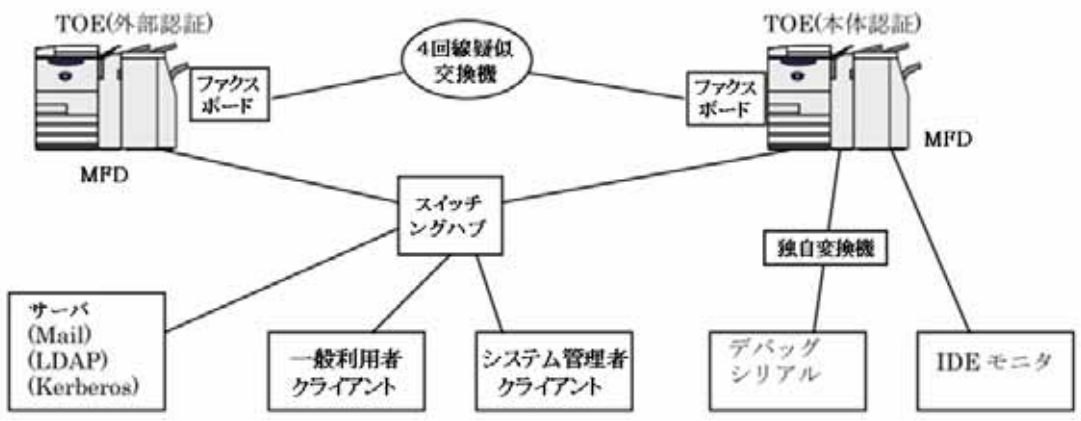

図 7-2 評価者独立テストの構成

評価者が実施した独立テストの構成要素は、開発者テストと同等である。対象としたTOEおよびTOEを搭載するMFDは、開発者テストと同一である。評価者は、ApeosPort-IV C7780(AP)、DocuCentre-IV C7780(AP)の2機種をテストすることにより、機種による差異を含めてすべての機能を確認することができると判断している。

評価者テストは本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。

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、TOEのセキュリティ機能が仕様どおりに機能することを評価者自らが実証するために、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。

＜独立テストの観点＞

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やパラメタが存在するため、それらのふるまいを確認する。

[1] テスト項目の追加

[2] テストの入力パターン（限界値分析）の追加

b. 独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜独立テスト手法＞

開発者テストに該当するテスト手法がない場合は、評価者が、テスト環境や手順、確認方法、期待される結果を新たに作成し、評価者独立テストを追加実施した。追加した入力パターンについては、開発者テストと同じ手法を使用して、同じテスト及び入力パラメタを変更したテストを追加実施する。

＜独立テストツール＞

開発者テストと同じツールを用いた。評価者独立テストにおいて利用したツールを表 7-2に示す。

＜独立テストの実施＞

評価者が実施した独立テストの観点とその対応したテスト内容を表 7-3 に示す。

表 7-3 実施した独立テスト

独立テストの観点	テスト概要
[1]	システム管理者の親展ボックスに対するアクセス制御が、仕様どおりであることを確認する。 • 一般利用者のID,SAのIDを削除した時(所有者情報を削除した時)の文書データ、ジョブに関するテスト
[2]	システム管理者の親展ボックスに対するアクセス制御が、仕様どおりであることを確認する。 • システム管理者(機械管理者)の権限における親展ボックスのテスト • 一般利用者、システム管理者の権限における共用親展ボックスのテスト
[1]	アカウントロック時にURLダイレクト入力によってWebブラウザ接続(CWIS)するテスト。アカウントロック状態の判定や、複数の利用者アカウントのロック状態の管理に関するテスト
[1]	Fuji Xerox DocuCentre-IV C7780/C6680/C5580 Seriesで提供されていない機能について、システム管理者セキュリティ管理機能で設定ができないことを確認する。 • 外部認証サーバにKerberosサーバを指定した場合に、ユーザー認証機能がLDAPサーバから利用者属性情報を取得するテスト
[2]	パスワード変更や入力時の長さ制限の限界値のふるまいが、仕様どおりであることを確認する。 • 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機械管理者ID、パスワード変更の入力に対する限界値分析 • 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システム管理者パスワードの入力に対する限界値分析

c. 結果

評価者は、実施したすべての評価者独立テストが正しく完了し、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が期待されるふるまいと一致していることを確認した。

7.3.3 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。

① 公知の脆弱性情報であるネットワークサービスの不正利用、Webの各種脆弱性、SSL通信時に安全でない暗号が選択される可能性について、本TOEにも該当する懸念がある。
② 操作パネル等のWeb以外のインタフェースについても、制限値を超えた長さの入力や、想定外の文字コード入力に対して、TOEが予期しない動作をする懸念がある。
③ 証拠資料に対する脆弱性分析より、USBポートによる不正アクセスの懸念がある。
④ 証拠資料に対する脆弱性分析より、設定データが格納されたNVRAM、SEEPROMが初期化された場合、セキュリティ機能が無効化される懸念がある。
⑤ 証拠資料に対する脆弱性分析より、親展ボックスの文書に対して、複数の利用者のアクセスが競合した場合に、保護資産である文書の不整合が生じる懸念がある。
⑥ システム管理者クライアントや利用者クライアントから不要なインタフェースや識別認証機能の問題を悪用し、認証機能を迂回してログインする恐れがある。
⑦ 初期化処理中の不正アクセスや、MFDのタイマーの電池切れによってセキュリティ機能が誤った動作を行う恐れがある。

b. 侵入テストの概要

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。

＜侵入テスト環境＞

侵入テスト環境を図 7-3に示す。本環境は、インターネットから独立したネットワーク環境を用いた。図 7-2の評価者独立テスト環境と同じ構成要素を用いて実施した。ただし、侵入テスト用のツールを搭載したパソコンを追加して使用した。使用したツールの詳細を表 7-4に示す。

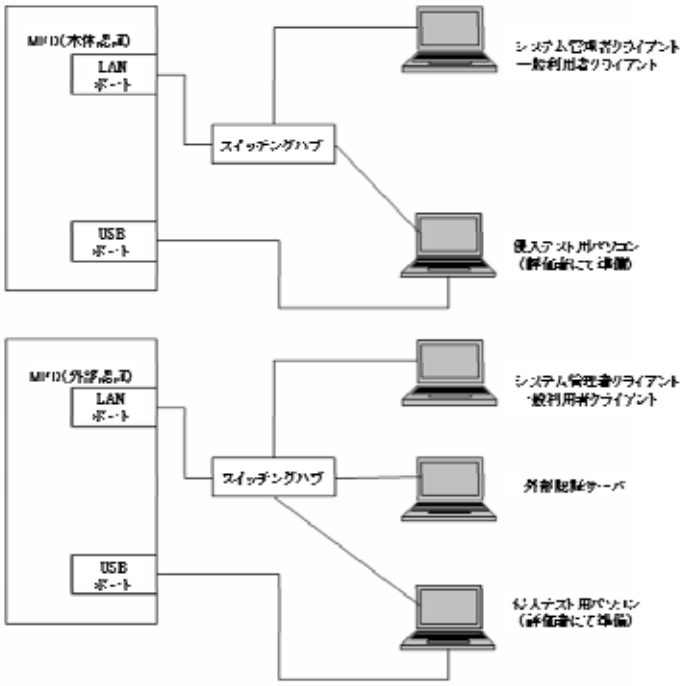

図 7-3　侵入テスト環境

表 7-4　侵入テスト用のツール

名称		概要・利用目的
侵入テスト用パソコン		Windows XP、Windows Vista、Windows 7を搭載したクライアントであり、以下の侵入テスト用ツールを動作させる。
	Zenmap+Nmap Ver.5.21	利用可能なネットワークサービスポートを検出するツール（Zenmapはポートスキャンツール NmapのGUIを提供）。
	Fiddler2 V2.3.0.0	Webブラウザ（クライアント）とWebサーバ（MFD）間の通信を仲介し、その間の通信データの参照と変更を行うツール。Fiddler2を使用することにより、Webブラウザの制約を受けずに、任意のデータをWebサーバに送信することができる。
	ContentsBridge Utility Version 7.1.1	富士ゼロックス社製のパソコン用のプリントソフト

＜侵入テスト手法＞

一般利用者クライアントやシステム管理者クライアントのWebブラウザから、URLを直接入力してアクセスした場合や、操作パネルやWebブラウザなどから制限値を越えた値や想定外の文字コードを入力した場合のふるまいなど、TOEへの入力に関するテストを行う。

MFDのハードウェアに関するテストを行い、セキュリティ機能が無効化されたり、セキュリティ機能が誤った動作を行ったりしないことを確認する。

＜脆弱性テストの実施＞

懸念される脆弱性と対応する侵入テスト内容を表 7-5に示す。

表 7-5　侵入テスト概要

テスト概要	対応する脆弱性
・NmapをTOEに対して実施し、オープンされているポートが悪用できないことを確認した。 ・Webブラウザ及びFiddler2を使用して、Webサーバ（TOE）に各種入力を行い、識別認証のバイパス、バッファオーバフロー、各種インジェクション等の公知の脆弱性がないことを確認した。 ・暗号通信プロトコルに関して、クライアントとして使用するパソコンの設定を推奨されない値に変更しても、TOEが指定する暗号通信プロトコル以外は通信できないことを確認した。	① ② ⑥
・操作パネル、システム管理者クライアント（ApeosWare Device Setup）、一般利用者クライアント（ネットワークスキャナーユーティリティ、プリンタードライバ）より、規定外の文字長、文字コード、特殊キーを入力しても、エラーとなることを確認した。	②
・TOEが備える各種USBポートに対して、侵入テスト用クライアントを接続してTOEにアクセスを試みても、プリンターやファクス等の意図された機能以外の利用はできないことを確認した。	③
・NVRAMやSEEPROMを設定のされていない新品と交換しても、エラーとなりTOEが使用できないことを確認した。	④
・親展ボックスの文書に対して、複数の利用者がアクセスしても、他で操作中の場合はアクセスが拒否されることを確認した。	⑤
・電源投入直後のMFDの初期化処理中は、操作を受け付けないことを確認した。 ・MFDのタイマー用の電池が切れて時刻の表示が不能となった場合、高信頼タイムスタンプに関わるセキュリティ機能が誤った動作を行わないことを確認した。	⑦

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持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.4 評価構成について

本TOEのセキュリティ機能を有効にし、安全に使用するためには、システム管理者は、事前にTOEの環境設定を行わなければならないなど、満たさなければならない条件が存在する。本評価の前提となるTOEの構成条件を表 7-6に示す。

表 7-6 TOEの構成条件

項番	設定項目	設定値
1	ハードディスク蓄積データ上書き消去機能	[1回]あるいは[3回]に設定
2	ハードディスク蓄積データ暗号化機能	[有効]に設定
3	本体パネルからの認証時のパスワード使用機能	[有効]に設定
4	システム管理者認証失敗によるアクセス拒否機能	[5]回に設定
5	SSL/TLS通信機能	[有効]に設定
6	IPsec通信機能	[有効]に設定
7	S/MIME通信機能	ApeosPort-IVシリーズでは、[有効]に設定（注：DocuCentre-IVシリーズでは、本機能は設定条件に従って使用不可に設定される。）
8	ユーザー認証機能	[本体認証]または[外部認証]に設定。 [外部認証]に設定する時は、LDAPサーバが必須である。
9	蓄積プリント機能	[プライベートプリントに保存]に設定
10	監査ログ機能	[有効]に設定
11	SNMPv3 通信機能	[有効]に設定
12	カストマーエンジニア操作制限機能	[する]に設定
13	ダイレクトファクス設定	[外部認証]時は、[無効]に設定
14	ネットワークスキャナーユーティリティの使用（WebDAV設定）	[外部認証]時は、[無効]に設定
15	ユーザーパスワードの文字数制限機能	[9]桁に設定 （注:外部認証時は、LDAPやKerberosサーバへ最低9桁のパスワードを設定する必要がある。）
16	SNMPv3のパスワード文字数	認証パスワードとプライバシー（暗号化）パスワードは、8文字以上に設定
17	電子メール機能	DocuCentre-IV Seriesは、[無効]に設定
18	インターネットファクス機能	DocuCentre-IV Seriesは、[無効]に設定

7.5 評価結果

評価者は、評価報告書をもって本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。

評価では、以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート２　適合
- セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL3 パッケージのすべての保証コンポーネント

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

8 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解決されていること。
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。

8.1 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。

8.2 注意事項

本TOEは、搭載するMFD機種（ApeosPort-IVとDocuCentre-IV）によって、提供する機能が異なる。また、本TOEは、ユーザー認証機能として本体認証と外部認証を備えているが、外部認証による運用を選択した場合、本体認証の場合と比べて、評価対象機能に制約がある。

本TOEの運用において、TOEを添付ドキュメントに従って設定を行うと、本評価が行われた構成条件が満たされる。TOEの設定値を構成条件以外の設定にした場合、本評価による保証の範囲ではないので注意が必要である。

TOEを搭載したMFD製品の購入時、本TOEに興味のある消費者は、本TOEの機能と運用上の条件と、各自の想定する機能と運用上の条件の対応に留意して、MFD機種を選択する必要がある。

9 附属書

特になし。

10 セキュリティターゲット

本TOEのセキュリティターゲット[12]は、本報告書とは別文書として、以下のとおり本認証報告書とともに提供される。

Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific セキュリティターゲット バージョン 1.0.8　2011年4月27日 富士ゼロックス株式会社

11 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）

本報告書で使用されたTOEに関する略語を以下に示す。

ADF	Auto Document Feeder（自動原稿送り装置）
CWIS	センターウェアインターネットサービスの略。利用者が、利用者クライアントのWebブラウザから、文書データの取り出し、印刷、TOEの状態確認／設定変更ができるサービス
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）
MFD	Multi Function Device（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）
SA	System Administratorの略。SAは、一部の管理機能が使用可能である。SAの役割は、利用組織の必要に応じて、機械管理者が設定する。「システム管理者」の説明参照
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）

本報告書で使用された用語の定義を以下に示す。

ApeosWare Device Setup	機械管理者が、システム管理者クライアントからMFDの設定管理をするためのソフトウェア
IDEバス	MFDのコントローラボードと内蔵ハードディスク装置の間でデータを送受信するためのデータ通信路
暗号鍵	文書データを暗号化／復号する時に、このデータを使用する。
一般利用者	TOEが提供するコピー機能、プリンター機能、スキャナー機能、ファクス機能等の基本機能の使用を許可された利用者
インターネットファクス機能	公衆電話回線網を使用することなく、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
カストマーエンジニア	MFDの保守／修理を行うエンジニア
機械管理者	すべての管理機能が使用可能なシステム管理者。「システム管理者」の説明参照
コピー機能	一般利用者がMFDの操作パネルから指示をして、IITから原稿を読み取り、IOTから印刷する機能

システム管理者	TOEのセキュリティ機能の設定や、その他機器設定を行うための特別な権限を持つ管理者。機械管理者とSA(System Administrator)の総称。
親展ボックス	文書データを蓄積するためにMFD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。スキャナー機能やファクス受信により読み込まれた文書データを登録ユーザー別や送信元別に蓄積できる。
スキャナー機能	一般利用者がMFDの操作パネルから指示して、IITから原稿を読み込み、MFD内部の親展ボックスに蓄積する機能。蓄積された文書データは、ネットワークスキャナーユーティリティやWebブラウザから取り出す。
セキュリティ監査ログデータ	障害や構成変更、ユーザー操作など、デバイス内で発生した重要な事象を時系列に記録したもの
操作パネル	MFD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
ダイレクトファクス機能	一般利用者が、一般利用者クライアントから文書データをMFDに送り、紙に印刷することなく、公衆電話回線網を使用してファクス送信する機能
蓄積プリント	印刷データを一時的にMFDの内部ハードディスク装置に蓄積し、一般利用者が操作パネルから印刷指示をした時に印刷を行う。「プリンター機能」の説明参照
通常プリント	印刷データをMFDが受信するとすぐに印刷を行う。「プリンター機能」の説明参照
TOE設定データ	TOEの動作に影響を与える可能性のあるデータ
ネットワークスキャン機能	一般利用者が、MFDの操作パネルから指示して、IITから原稿を読み込み、MFDの設定情報に従って自動的にFTPサーバ、SMBサーバ、Mailサーバに送信する機能
ネットワークスキャナーユーティリティ	MFD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
ファクス機能	ファクス送受信を行う機能。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から原稿を読み込み、公衆電話回線網を経由して、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された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。
ファクスドライバ	印刷と同じ操作で、一般利用者クライアント上からMFDへ文書データを送信し、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
プリンター機能	一般利用者が、印刷データを一般利用者クライアントからMFDへ送信して、IOTから印刷を行う機能。 プリンター機能には、「通常プリント」と「蓄積プリント」がある。本評価では、蓄積プリントだけが評価の対象である。
プリンタードライバ	一般利用者クライアント上の文書データを、MFDが解釈可能なページ記述言語で構成された印刷データに変換するソフトウェア
文書データ	MFDのコピー機能、プリンター機能、スキャナー機能、ファクス機能が処理する文字や画像の情報を含むデータを総称して文書データとよぶ。

12 参照

[1] 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

[2] 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

[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　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] 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3版 2009年7月 CCMB-2009-07-001 (平成21年12月翻訳第1.0版)

[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3版 2009年7月 CCMB-2009-07-002 (平成21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3版 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[11] 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3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific セキュリティターゲット バージョン 1.0.8　2011年4月27日 富士ゼロックス株式会社

[13] Fuji Xerox ApeosPort-IV C7780/C6680/C5580 DocuCentre-IV C7780/C6680/C5580 Series Controller Software for Asia Pacific 評価報告書 第1.8版 2011年5月30日 IT セキュリティセンター 評価部