認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成28年1月19日 (IT認証6588)
認証番号	C0550
認証申請者	富士ゼロックス株式会社
TOEの名称	日本語名：富士ゼロックス ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ コントローラソフトウェア 英語名：Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 Series Controller Software
TOEのバージョン	Controller ROM Ver.1.0.19
PP適合	なし
適合する保証パッケージ	EAL2及び追加の保証コンポーネントALC_FLR.2
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29年5月25日

技術本部
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4
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4

評価結果：合格

「日本語名：富士ゼロックス ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズコントローラソフトウェア
英語名：Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 Series Controller Software」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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「日本語名：富士ゼロックス ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズコントローラソフトウェア 英語名：Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 Series Controller Software、バージョン Controller ROM Ver. 1.0.19」（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 29 年 5 月 12 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 に関心を持つ調達者や消費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、10 章の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、EAL2 及び追加の保証コンポーネント ALC_FLR.2 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、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。本 TOE が想定する脅威及び前提については次項のとおりである。

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 の操作や、MFD 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、それらの保護資産の不正な読出しや改ざんを防止するために、識別認証、アクセス制御、内部ハードディスク装置や通信データの暗号化等のセキュリティ機能を提供する。

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する。

本 TOE は、TOE を搭載した MFD の物理的部分やインタフェースが不正なアクセスから保護されるような環境に設置されることを想定している。また、TOE の運用にあたっては、ガイダンス文書に従って TOE を適切に設定し、維持管理しなければならない。

1.1.3 免責事項

本 TOE には、以下に示す運用や機能は保証の対象外である。

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、「7.5 評価構成について」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-VI シリーズでのみ有効であり、DocuCentre-VI シリーズでは提供していない。

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 セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[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 29 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。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。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][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識別

本 TOE は、以下のとおり識別される。

TOE名称：	日本語名：富士ゼロックス ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ コントローラソフトウェア 英語名：Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/ C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/ C2271 Series Controller Software
バージョン：	Controller ROM Ver. 1.0.19
開発者：	富士ゼロックス株式会社

本 TOE は、富士ゼロックス株式会社の以下の MFD のコントローラソフトウェア部分である。ただし、国内向けの MFD では、オプションの「データ上書き消去キット」が必要である。

（国内向け）

・ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ
・DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ

（海外向け）

・ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 シリーズ
・DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 シリーズ

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、画面に表示された機種名とバージョン情報、または、設定値リストのプリント出力に記述された機種名とバージョン情報を、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 が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

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、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監査ログを記録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（機械管理者と SA）

システム管理者は、TOE のセキュリティ機能の設定を行うための特別な権限を持つ利用者である。システム管理者には、すべての管理機能を使用できる「機械管理者」と、一部の管理機能を使用できる「SA」が含まれる。

・カストマーエンジニア

カストマーエンジニアは、MFD の保守や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と、ハードディスク装置に蓄積されたデータを削除する際の上書き消去及び自己テスト機能を備えている。

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。なお、各セキュリティ機能の詳細は、5 章に示す。

(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 TOE 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、識別認証されたシステム管理者だけに許可する。

「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 TOE 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システム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システム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。

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。

以上により、内部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 と利用者端末（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。

以上により、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	TOEは、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。
P.VERIFY	TOEは、TSF の実行コードおよびTSFデータの完全性に関し自己テストをしなければならない。
P.OVERWRITE	TOEは、内部ハードディスク装置に蓄積される利用済み文書データの上書き消去を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。なお、各セキュリティ機能の詳細は、5 章に示す。

(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、公衆電話回線網から受信したデータを内部ネットワークに受け渡さない。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。

(2) 組織のセキュリティ方針「P.VERIFY」への対応

TOE の「自己テスト機能」は、起動時に Controller ROM のチェックサムを照合する。また、NVRAM と SEEPROM に格納された TSF データをチェックし異常を検出する。これにより、TOE セキュリティ機能の実行コードとデータの完全性が検査される。

(3) 組織のセキュリティ方針「P.OVERWRITE」への対応

TOE の「ハードディスク蓄積データ上書き消去機能」は、MFD 基本機能の終了後に文書データが削除される際に、文書データが格納されていた内部ハードディスク装置の領域を上書き消去する。これにより、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は上書き消去される。

4 前提条件と評価範囲の明確化

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運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.USER	TOE 利用者は、組織の方針および製品のガイダンス文書に従い、TOEの使用方法及び注意事項に関する教育を受け、その能力を習得する。
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。
A.ACCESS	TOEが搭載されたMFDを監視下に置くか、MFDの物理的なコンポーネントとデータインタフェースへの許可されないアクセスに対する保護を提供する制限された環境に設置する。

4.2 運用環境と構成

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に接続され、さらに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 の一般的な運用環境を図 4-1 に示す。

内部ネットワークには、Mail サーバ、FTP サーバ、DNS サーバ、LDAP サーバ、Kerberos サーバといっ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 を利用することもできる。

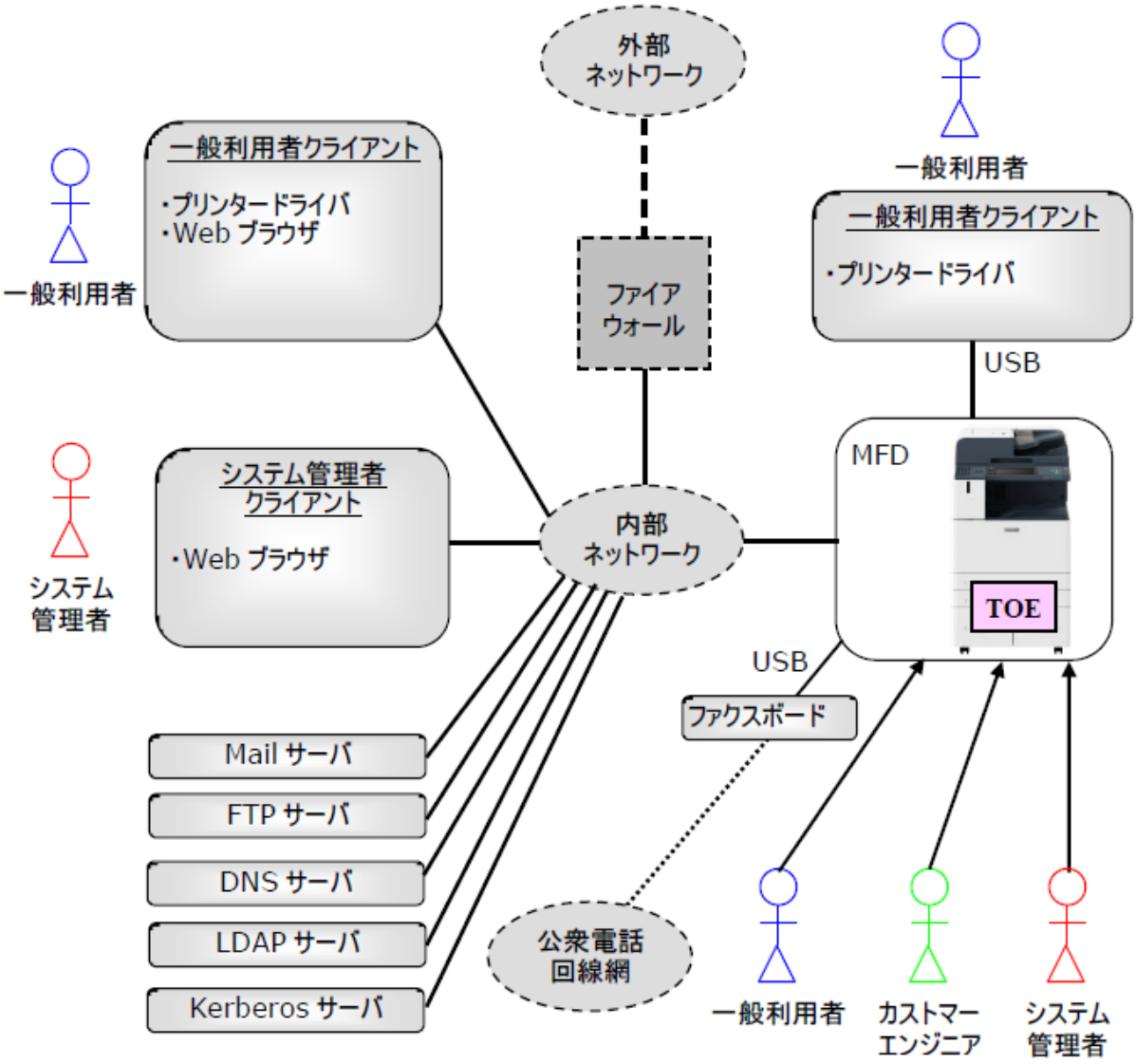

図4-1 TOEの運用環境

TOEの運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、富士ゼロックス株式会社の以下の機種である。

（国内向け）

・ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ

・DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271 シリーズ

（海外向け）

・ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 シリーズ

・DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 シリーズ

機種の中には、MFD の基本機能の内、スキャナー機能が標準装備されておらず、オプションとして提供されているものが存在する。本評価では、スキャナー機能が標準装備されている機種、スキャナー機能が装備されていない機種及びその機種にオプションのスキャナー機能を追加した構成の、すべてが評価対象構成である。

(2) ファクスボード

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、指定された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PCであり、USB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 Vista、Windows 7、Windows 8.1のいずれか。
・プリンタードライバ

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)

(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PC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 Vista、Windows 7、Windows 8.1のいずれか。
・Webブラウザ(OS附属のもの)

(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。

LDAPサーバ及びKerberosサーバとして、本評価では以下のソフトウェアを使用する。

・Windows Active Directory

(6) Mailサーバ、FTPサーバ

TOEは、Mailサーバ、FTPサーバと文書データをやりとりする基本機能を持つ。それらの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。

(7) DNSサーバ

TOEが、各種サーバ等のIPアドレスを取得するために使用。

なお、本構成に示されているTOE以外のハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本TOEの評価されたセキュリティ機能には、以下の制約条件がある。

(1) DocuCentre-VIシリーズ

DocuCentre-VIシリーズでは、「外部認証」とS/MIME機能は提供していない。S/MIME機能は電子メール及びインターネットファクス送信機能で使用される。DocuCentre-VIシリーズでは、電子メール及びインターネットファクス送信機能は提供されているが、使用できないように設定され、本評価対象の構成には含まれていない。

(2) 外部認証時の制約

外部認証サーバ（LDAPサーバまたはKerberosサーバ）に格納されている利用者パスワードに対しては、パスワード長を9文字以上に制限するTOEの機能は適用されない。外部認証サーバに格納されている利用者パスワードについて、推測を防止するための十分な長さの確保は、システム管理者の責任である。

(3) IPv6用のIPsec

本評価では、IPsecプロトコルについて、IPv4だけが評価されている。IPv6用のIPsecは評価されておらず保証の対象外である。

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。

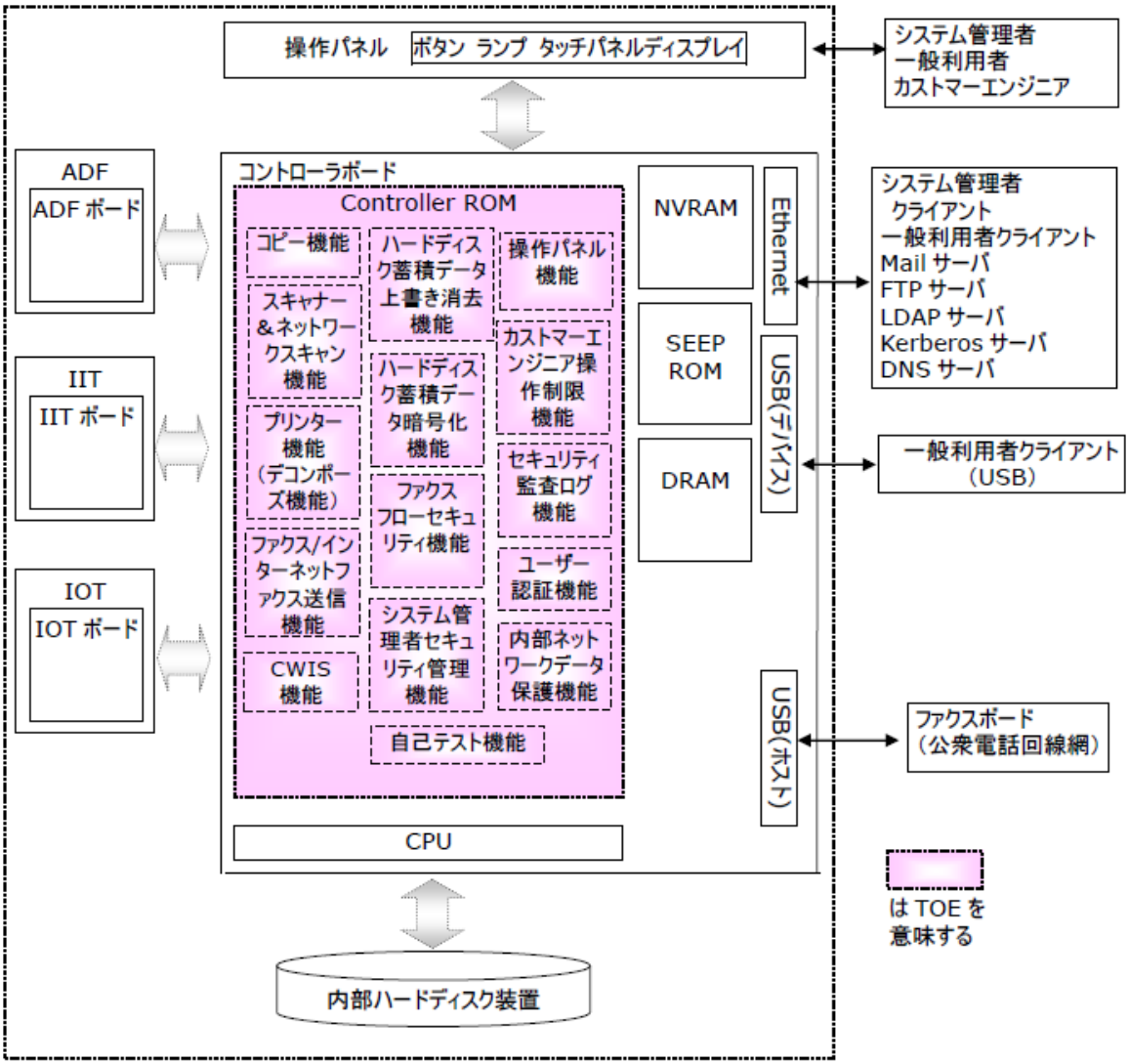

図 5-1 TOE境界

TOE の機能は、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。以下、TOE のセキュリティ機能について説明する。MFD の基本機能については、11 章の用語説明を参照。

(1) ユーザー認証機能

本機能には、利用者の識別認証、利用者データのアクセス制御の、2 種類の機能が含まれている。

① 利用者の識別認証

本機能は、TOE の利用者を、利用者の ID とパスワードで識別認証する機能である。識別認証は、以下に示す利用者インタフェースに適用される。

・操作パネル
・クライアント PC (Web ブラウザ、プリンタードライバ)

認証方式には、TOE に格納された利用者の ID とパスワードを使用する「本体認証」と、TOE 外部の LDAP サーバや Kerberos サーバを使用する「外部認証」がある。

識別認証機能を補強するために、以下の機能を備えている。

・本体認証の場合、パスワードは 9 文字以上が要求される。
・本体認証の場合、システム管理者が 5 回連続して認証失敗すると、認証を停止する。一般利用者に対しては適用されない。

② 利用者データのアクセス制御

本機能は、TOE に蓄積された文書データと親展ボックスに対するアクセスを、権限のある利用者のみに制限する機能である。

文書データ及び親展ボックスに対して、それらの所有者情報と一致する利用者の操作と、共用の親展ボックスに対する操作が許可される。

なお、システム管理者はすべての文書データの削除が可能である。

(2) システム管理者セキュリティ管理機能

本機能は、セキュリティ機能で使用されるデータの設定、参照、変更を、識別認証されたシステム管理者だけに許可する機能である。ただし、一般利用者は、本人のパスワードの変更が可能である。

(3) カストマーエンジニア操作制限機能

本機能は、システム管理者がカストマーエンジニアの操作を制限する機能である。識別認証されたシステム管理者だけが、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の参照と設定変更が可能である。カストマーエンジニアの操作制限が有効の場合、システム管理者が設定する本機能用のパスワードを入力しなければ、カストマーエンジニアは操作できない。

(4) セキュリティ監査ログ機能

本機能は、セキュリティ機能に関する監査事象を監査ログとして記録する機能である。TOE に格納された監査ログは、識別認証されたシステム管理者だけが、Web ブラウザで読出すことができる。監査ログの削除や改変はできない。

監査ログは 15,000 件のイベントを保存することができる。それを超える場合には最も古い記録を消去して新しい監査ログを記録する。

(5) ハードディスク蓄積データ暗号化機能

本機能は、内部ハードディスク装置に保存するデータを暗号化する機能である。暗号アルゴリズムは、256bit の AES である。暗号鍵は、導入時にシステム管理者が設定する 12 桁の英数字から成る暗号化キーを元に、富士ゼロックス社の独自アルゴリズムで生成する。暗号鍵は、電源 ON 時に毎回同じ値が生成されて揮発メモリ上に格納され、電源 OFF によって消滅する。

(6) ハードディスク蓄積データ上書き消去機能

本機能は、文書データを削除する際に、文書データが格納されていた内部ハードディスク装置の領域を上書き消去する機能である。本機能は、以下のタイミングで実行される。

- MFD の基本機能が終了し文書データが不要になった時。TOE の処理の都合で TOE 内に一時的に作成されたデータも対象に含まれる。
- 利用者の指示で文書データを削除した時。
- 電源 ON にした時。電源 OFF 時に上書き消去処理が未完了の場合には、電源 ON 時に処理が再開される。

上書きするデータのパターンは、システム管理者の設定で 1 回（「0(ゼロ)」による上書き）または 3 回（乱数・乱数・「0(ゼロ)」による上書き）を選択することができる。ただし、実際に内部ハードディスク装置に書き込まれるデータは、それらの上書きデータを暗号化したデータである。そのため、選択したデータと実際に書き込まれるデータは異なる。

(7) 内部ネットワークデータ保護機能

本機能は、IT 機器との通信において、以下の暗号化通信を行う機能である。

・IPsec、TLS（v1.0、v1.1、v1.2）、S/MIME

(8) ファクスフローセキュリティ機能

本機能は、公衆電話回線から内部ネットワークへのデータ転送を防止する機能である。TOE は、指定されたファクスボード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に渡さない構造になっている。これにより、TOE は、公衆電話回線から内部ネットワークにデータを受け渡すことはない。

(9) 自己テスト機能

本機能は、TOE の起動時に以下の自己テストを行う機能である。

- Controller ROM のチェックサムの検証
- NVRAM と SEEPROM に格納された TSF データの検証

5.2 IT環境

TOE は、外部認証方式の場合には、外部の認証サーバ（LDAP サーバまたは Kerberos サーバ）を使用して、利用者の識別認証を行う。さらに、外部認証方式の場合には、LDAP サーバを使用して利用者が SA 役割か否かを判別する。

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。

(1) 国内向け

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271
  管理者ガイド (ME7761J1-2)
  (SHA1ハッシュ値；3cade5a6853399ace0886ec39afec1d088c5c1ac)

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271
  ユーザーズガイド (ME7760J1-2)
  (SHA1ハッシュ値；07670fd069befa56c1087fada84a9d85bcc75f39)

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C2271
  セキュリティ機能補足ガイド (ME7762J1-3)
  (SHA1ハッシュ値；79682b8332aaf5be141237a2e36cac6f4501f753)

(2) 海外向け

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  Administrator Guide (ME7771E2-2)
  (SHA1ハッシュ値；70edb49875788650949a642f4cac8e4fa04d5454)

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  User Guide (ME7769E2-2)
  (SHA1ハッシュ値；332f55267d03effcc7342c56d716d1bf8dc85c2b)

- ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271
  Security Function Supplementary Guide (ME7770E2-3)
  (SHA1ハッシュ値；dcdacdc58282211eb880024eb95e8aeca12cd5c9)

※SHA1 ハッシュ値について

ガイダンスは MFD 製品に同梱の DVD に格納されている。TOE の購入者は、DVD に格納されたガイダンスファイルの SHA1 ハッシュ値を計算し比較することで、ガイダンスの完全性を確認することができる。

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した一般社団法人 IT セキュリティセンター 評価部は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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た。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 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 28 年 1 月に始まり、平成 29 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 28 年 7 月及び 11 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 28 年 11 月、平成 29 年 3 月及び 5 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、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。

認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 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。

7.4.1 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。評価者が評価した開発者テストの内容を以下に説明する。

(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。

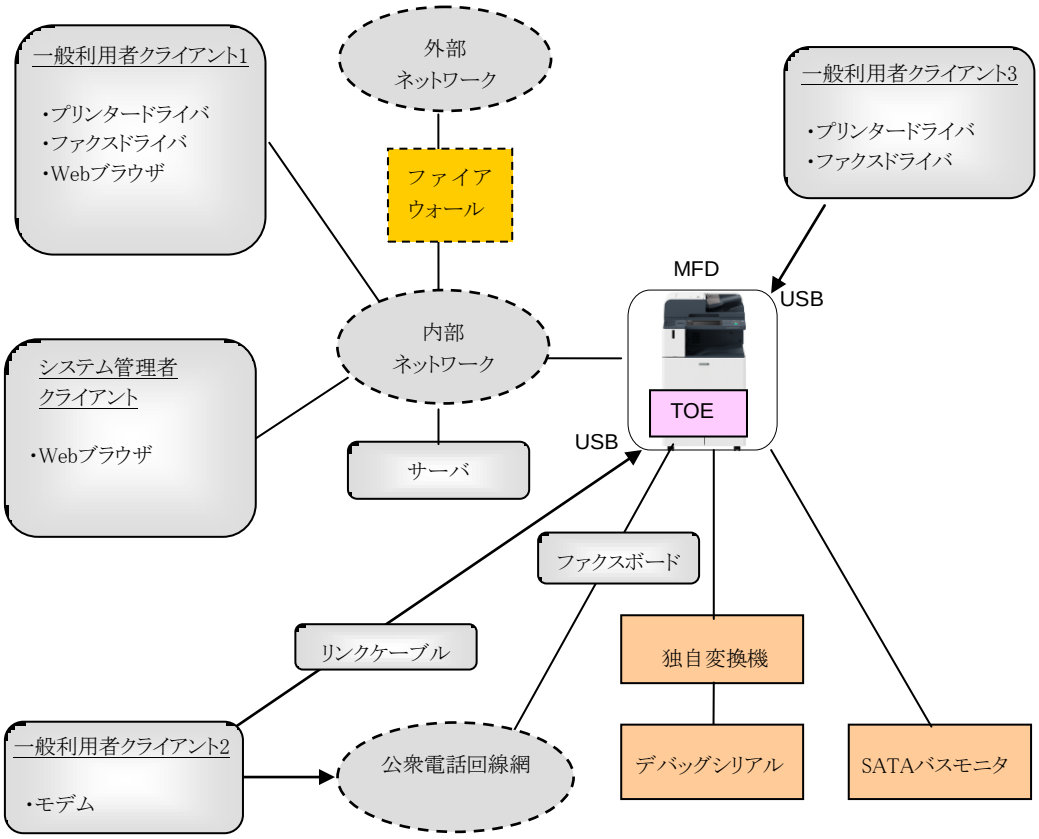

図7-1　開発者テストの構成図

開発者がテストした 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、2 章の TOE 識別に記述されている MFD の全機種である。

開発者テストの構成要素を表 7-1 に示す。

表7-1　開発者テストの構成要素

名称	詳細
MFD	(国内向け) ApeosPort-VI C7771, C6671, C5571, C4471, C3371, C2271 DocuCentre-VI C7771, C6671, C5571, C4471, C3371, C2271 (海外向け) ApeosPort-VI C7771, C6671, C5571, C4471, C3371, C3370, C2271 DocuCentre-VI C7771, C6671, C5571, C4471, C3371, C3370, C2271
サーバ	各種サーバとして使用。 ・Microsoft Windows Server 2008 R2 SP1搭載PC ・Mailサーバ： Xmail Version 1.27 ・FTPサーバ、DNSサーバ：OS標準搭載ソフトウェア ・LDAPサーバ、Kerberos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	一般利用者クライアント（内部ネットワーク経由の接続）及びインターネットファクス送信の通信相手として使用。以下の3機種を使用 a) Microsoft Windows 7 Professional SP1搭載PC Webブラウザ：Microsoft Internet Explorer 11 b) Microsoft Windows VISTA Business SP2 搭載PC Webブラウザ：Microsoft Internet Explorer 7 c) Microsoft Windows 8.1搭載PC Webブラウザ：Microsoft Internet Explorer 11 さらに、上記のいずれも、以下のソフトウェアを使用 （国内向け） ・プリンタードライバ：ART EX Print Driver Version 6.10.1 ・ファクスドライバ：ART EX DirectFax Driver Version 2.9.0 （海外向け） ・プリンタードライバ／ファクスドライバ：PCL6 Print Driver Version 6.10.0 ※ファクスドライバは使用できないことの確認に使用
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 ・Microsoft Windows VISTA Business SP2 搭載 PC ※PCのモデムポートを公衆電話回線網に接続。PC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

名称	詳細
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 VISTA Business SP2搭載PC （国内向け） ・プリンタードライバ : ART EX Print Driver Version 6.10.1 ・ファクスドライバ : ART EX DirectFax Driver Version 2.9.0 （海外向け） ・プリンタードライバ／ファクスドライバ : PCL6 Print Driver Version 6.10.0 ※ファクスドライバは使用できないことの確認に使用
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。以下の3機種を使用 a) Microsoft Windows 7 Professional SP1搭載PC Webブラウザ : Microsoft Internet Explorer 11 b) Microsoft Windows VISTA Business SP2 搭載PC Webブラウザ : Microsoft Internet Explorer 7 c) Microsoft Windows 8.1搭載PC Webブラウザ : Microsoft Internet Explorer 11
SATAバスモニタ	内部ハードディスク装置の接続されたSATAバスのデータをモニタするツール ・専用機器（Catalyst Enterprises社製 ST2-31-2-A）を接続したWindows 7 Professional SP1搭載PC ・専用ソフトウェア : stx_sata_protocolsuite V4.20
デバッグシリアル	MFDのデバッグ用端末。端末(PC)のシリアルポートを、独自変換機を経由して、MFDのデバッグ用の端末ポートと接続 ・Microsoft Windows 7 Professional SP1搭載PC ・端末ソフトウェア : Tera Term 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、富士ゼロックス製の独自の変換基板
公衆電話回線網	電話回線疑似交換機を使用（ハウ社N4T-EXCH）
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 Ver 2.0.8

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ことを、評価者が評価している。

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。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

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。

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 SATA バスモニタを使用して、内部ハードディスク装置へ書き込まれるデータと、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。

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データ等を直接参照し、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、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。

④ ハードディスク蓄積データ暗号化機能の確認のために、生成された暗号鍵と暗号化されたデータを、指定されたアルゴリズムによって算出された既知のデータと比較し、仕様どおりの暗号鍵生成アルゴリズムと暗号アルゴリズムであることを確認する。

⑤ 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、仕様どおりの暗号通信プロトコルであることを観測する。また、様々な Web 入力や印刷ジョブコマンドに対する保護機能を確認する。

⑥ 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　開発テストツール

ツール名称	概要・利用目的
SATAバスモニタ (PC＋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SATA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 1.10.6)	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、TLSであることを確認する。
メーラー (Microsoft Windows Live Mail 2011)	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。
HTTPデバッガ (Fiddler 2.4.7.1)	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。
デバッグシリアル＋独自変換機 ※構成は表7-1参照	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。
Nmap 6.46	利用可能なネットワークポートを検出するツール。

＜開発者テストの実施内容＞

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、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ふるまいが、仕様通りに動作することを確認した。

b) 開発者テストの実施範囲

開発者テストは開発者によって79項目実施された。カバレージ分析によって、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た。

c) 結果

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプリングテストを実施するとともに、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をより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、図 7-1 に示した開発者テストの構成と、以下を除いて同じである。

- TOE を搭載する MFD として、以下を使用。
  （国内向け）ApeosPort-VI C2271、DocuCentre-VI C2271
  （海外向け）ApeosPort-VI C4471、DocuCentre-VI C4471
- ファクス対向機として、TOE を搭載した ApeosPort-VI C2271 と ApeosPort-VI C4471 を使用。

評価者は、TOE を搭載する MFD について、国内向けと海外向け、ApeosPort-VI と DocuCentre-VI、機種による印刷速度の違いを考慮した上で、テスト対象の MFD を選択している。また、評価者は、ファクスの通信相手の違いは、TOE のセキュリティ機能に影響ないと判断している。

独立テストは、本 ST において識別されている TOE の構成と同一の環境で実施された。

なお、開発者独自のデバッグ環境（デバッグシリアルと独自変換機）をはじめとするテストツールは、開発者テストに用いられたものを利用しているが、それらの妥当性確認及び動作試験は、評価者によって実施されている。

(2) 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である。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① 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、テストされていないパラメタのふるまいを確認する。

② サンプリングテストでは、以下の観点で開発者テストの項目を抽出する。

- すべてのセキュリティ機能と外部インタフェースを確認する。
- すべての利用者種別と、親展ボックス及び蓄積プリントの組合せのアクセス制御を確認する。
- すべての認証方式（本体認証、kerberos による外部認証、LDAP による外部認証）を確認する。

b) 独立テスト概要

評価者は、独立テストの観点に基づいて、開発者テストのサンプリングテストと追加の独立テストを考案した。評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストと同じ手法を使用して、開発者と同じテスト及び入力パラメタを変更したテストを実施する。

＜独立テストツール＞

開発者テストと同じツールを使用した。

＜独立テストの実施内容＞

評価者は、独立テストの観点に基づいて、59 項目のサンプリングテストと、7 項目の追加の独立テストを実施した。

独立テストの観点とそれに対応した主なテスト内容を表 7-3 に示す。

表7-3 実施した主な独立テスト

観点	テスト概要
観点①	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。
観点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。
観点①	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が、仕様どおりであることを確認する。

観点①	TOE内に文書データが存在している状態で､所有者の利用者登録を削除する際のふるまいが、仕様どおりであることを確認する。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 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となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

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、TLS 暗号化通信で弱い暗号方式が使われる可能性について、本 TOE にも該当する懸念がある。

② 公知の脆弱性情報より、PDF ファイルによる予期しない処理の実行、印刷ジョブコマンドによる不正なアクセスについて、本 TOE にも該当する懸念がある。

③ 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。

④ 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。

⑤ 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。

⑥ 証拠資料に対する脆弱性分析より、親展ボックスの文書データに対して、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データの不整合が生じる懸念がある。

⑦ 初期化処理中の不正アクセスや、MFD のシステムクロック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懸念がある。

なお、暗号鍵については、設定する暗号化キーや暗号鍵の生成メカニズムの分析から、想定されている攻撃者の攻撃能力では暗号鍵の入手や推測ができないことが評価されている。

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を決定するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者独立テスト環境と同じ環境で実施した。ただし、侵入テスト用のツールを搭載した PC を追加して使用した。侵入テストで使用したツールを表 7-4 に示す。

表7-4　侵入テストツール

ツール名称	概要・利用目的
Nmap Version 6.40	利用可能なネットワークポートを検出するツール
netcat Version 1.11	ネットワークポートへのデータ送信に使用
Fiddler Version 4.4.9.0	Webブラウザ（クライアント）とWebサーバ（TOE）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
SSLScan Version 1.8.2	SSL/TLSの暗号スイーツのサポート有無を確認するツール
ContentsBridge Version 7.3.0	富士ゼロックス社製のPC用のプリントソフト
Metasploit Version 4.6.2	PDFの脆弱性を検査するための検査データの作成に使用
PRET Version 0.36	印刷処理の様々な脆弱性を検査するツール

＜侵入テストの実施内容＞

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

脆弱性	テスト概要
脆弱性①	・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Fiddler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。 ・SSLScanをTOEに対して実施し、弱い暗号方式をサポートしていないことを確認した。
脆弱性②	・不正な処理を含むPDFファイルを入力しても、処理が実行されないことを確認した。 ・印刷ジョブコマンドで、ディレクトリを探索しても、保護資産にアクセスできないことを確認した。
脆弱性③	・操作パネル、一般利用者クライアント（プリンタードライバ）、PRETより、規定外の文字長、文字コード、特殊キーを入力しても、無視またはエラーとなり、悪用できないことを確認した。
脆弱性④	・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。
脆弱性⑤	・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。
脆弱性⑥	・親展ボックスの文書データに対して、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。
脆弱性⑦	・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のシステムクロック用の電池が切れた状態で電源を投入すると、エラーが表示されMFDが使用できないことを確認した。

c) 結果

評価者が実施した侵入テストでは、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。

7.5 評価構成について

本評価の前提となる TOE の構成条件は、6 章に示したガイダンスに記述されているとおりである。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、TOE のシステム管理者は、当該ガイダンスの記述のとおりに TOE を設定しなければならない。これらの設定値をガイダンスと異なる値に変更した場合には、本評価による保証の対象ではない。

TOE の構成条件には、TOE の提供している機能を使用禁止にする設定があり、例えば、以下のような設定値も含まれている。

・カストマーエンジニア操作制限の有効化
・WebDAV(ネットワークスキャナーユーティリティの利用)の無効化
・ダイレクトファクス機能(ファクスドライバの利用)の無効化
・リモートメンテナンス機能の無効化
・メール受信の無効化
・SNMP機能の無効化

さらに、DocuCentre-VI シリーズでは以下の設定が必要である。

・メール送信の無効化

上記のようなTOEの提供している機能を使用禁止にする設定も含めて、TOEの構成条件である設定値をガイダンスと異なる値に変更した場合には、本評価による保証の対象ではなくなるので、TOEのシステム管理者は注意が必要である。

7.6 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。

・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。

・EAL2 パッケージのすべての保証コンポーネント
・追加の保証コンポーネント ALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達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。

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。

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 EAL2 及び追加の保証コンポーネント ALC_FLR.2 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 に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価対象範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

特に、保守機能を有効化した場合、それ以降の運用での本 TOE のセキュリティ機能への影響については本評価の保証の範囲外となるため、保守の受け入れについては管理者の責任において判断されたい。

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提供される。

Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 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, Version 1.1.3, 2017 年 4 月 21 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	CentreWare Internet Services（センターウェアインターネットサービス）
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 privilege（SA役割）
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。

CWIS機能	利用者クライアントのWebブラウザを介して、TOEの状態確認、設定変更、文書データの取出し、印刷要求ができるサービス
SA	一部の管理機能が使用できるシステム管理者。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
TOE設定データ	TOEのセキュリティ機能に影響を与える可能性のある設定データ
暗号化キー	システム管理者が設定する12桁の英数字。内部ハードディスク装置の暗号化時に、このデータをもとに暗号鍵を生成する
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送信機能	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
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」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、操作パネルやWebブラウザから指示して取り出す。
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
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
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、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。本TOEでは設定により使用できない
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。本TOEでは設定により使用できない
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の総称

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27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10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等に関する要求事項, 平成27年10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 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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4版, 2012年9月, CCMB-2012-09-001, (平成24年11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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 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, Version 1.1.3, 2017年4月21日, 富士ゼロックス株式会社

[13] Fuji Xerox ApeosPort-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 DocuCentre-VI C7771/C6671/C5571/C4471/C3371/C3370/C2271 シリーズコントローラソフトウェア 評価報告書, 第1.16版, 2017年5月12日, 一般社団法人ITセキュリティセンター 評価部