CRP-C0595-01

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9月2日 (IT認証6609)
認証番号	C0595
認証申請者	Xerox Corporation
TOEの名称	Xerox VersaLink B405 Multifunction Printer ディスクレスモデル
TOEのバージョン	Controller ROM Ver. 1.0.31
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30年4月16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　真鍋　史明

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

「Xerox VersaLink B405 Multifunction Printer ディスクレスモデル」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「Xerox VersaLink B405 Multifunction Printer ディスクレスモデル、バージョン Controller ROM Ver. 1.0.31」（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 30 年 4 月 5 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 Xerox Corporation 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、ネットワークスキャン機能、ファクス機能といった基本機能を有するデジタル複合機（以下「MFD」という。）である。

本 TOE は、それらの 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等は、TOE の操作や、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。

それらの脅威に対抗するために、TOE は、識別認証、アクセス制御、暗号化など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、対象機種の MFD で、オプションの大容量記憶装置を搭載していない構成である。

本 TOE は、TOE 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 の機能や評価で保証された範囲には次のような制約がある。

(1) 本 TOE は、以下の機能は提供していない。

・eMMC メモリの暗号化に使用する暗号鍵の破棄や変更

(2) 本評価では、以下の運用を行った場合、それ以降は保証の対象外となる。

・カストマーエンジニア用の保守機能の使用

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 30 年 4 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]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。また、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：	Xerox VersaLink B405 Multifunction Printer ディスクレスモデル
バージョン：	Controller ROM Ver. 1.0.31
開発者：	富士ゼロックス株式会社

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。

製品のガイダンスの記載に従って操作パネルを操作し、画面表示または設定値リストのプリント出力に記述された、機種名及びバージョンの情報を確認する。

- 機種名：Xerox VersaLink B405 Multifunction Printer
- Controller ROM のバージョン

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、ネットワークスキャン機能、ファクス機能といった MFD の基本機能を提供しており、利用者の文書データを TOE 内部の eMMC メモリに蓄積したり、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、それらの機能を使用する際に、利用者の識別認証とアクセス制御、eMMC メモリに蓄積した文書データの暗号化、暗号化通信などの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等が、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。

なお、TOE は以下の利用者役割を想定している。

・一般利用者

TOE が提供するコピー機能、プリンター機能、ネットワークスキャン機能、ファクス機能といった MFD の基本機能の利用者である。

・システム管理者

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 TOE の利用者である。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

MFD の保守や修理を行うエンジニアである。

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の不正な読み出しや改変を行うかもしれない。
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.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。

TOE の「ユーザー認証機能」は、識別認証が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、TOE に蓄積された文書データの操作をする際には、文書データに対してアクセス権限のある利用者だけにアクセスを許可する。

TOE の「システム管理者セキュリティ管理機能」は、セキュリティ機能で使用されるデータの参照と変更を、識別認証されたシステム管理者だけに許可する。ただし、一般利用者は、本人のパスワードの変更は可能である。

TOE の「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システム管理者だけに許可する。

TOE の「セキュリティ監査ログ機能」は、セキュリティに関連する事象を監査ログとして記録する。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、読み出すことができる。監査ログの削除と改変はできない。

以上の機能により、TOE は、TOE への不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

⑵ 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。

TOE の「内部ネットワークデータ保護機能」は、TOE とクライアント PC や各種サーバとの通信時に、暗号通信プロトコルを適用し、通信データを保護する。

以上の機能により、TOE は、通信データへの不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

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.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.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.CIPHER	TOEは、eMMCメモリに蓄積されている文書データおよびセキュリティ監査ログデータを暗号化しなければならない。(暗号鍵を破棄する必要はない。)

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、以下のセキュリティ機能を具備する。なお、各セキュリティ機能の詳細は、5 章に示す。

⑴ 組織のセキュリティ方針「P.VERIFY」への対応

TOE は、「自己テスト機能」で本方針を実現する。

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。それにより、TOE セキュリティ機能の実行コードと TSF データの完全性が検査される。

⑵ 組織のセキュリティ方針「P.FAX_OPT」への対応

TOE は、「ファクスフローセキュリティ機能」で、本方針を実現する。

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。

⑶ 組織のセキュリティ方針「P.CIPHER」への対応

TOE は、「フラッシュメモリ蓄積データ暗号化機能」で本方針を実現する。

TOE の「フラッシュメモリ蓄積データ暗号化機能」は、TOE 内部の eMMC メモリに書き込むデータを暗号化する。暗号アルゴリズムは 256bit の AES である。

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を監視下に置くか、TOE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 は、オフィスに設置されて、内部ネットワークに接続し、同様に内部ネットワークに接続されたクライアント PC から利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

なお、クライアント PC は、USB ポート経由で TOE と接続し、TOE のプリンター機能を使用することもできる。

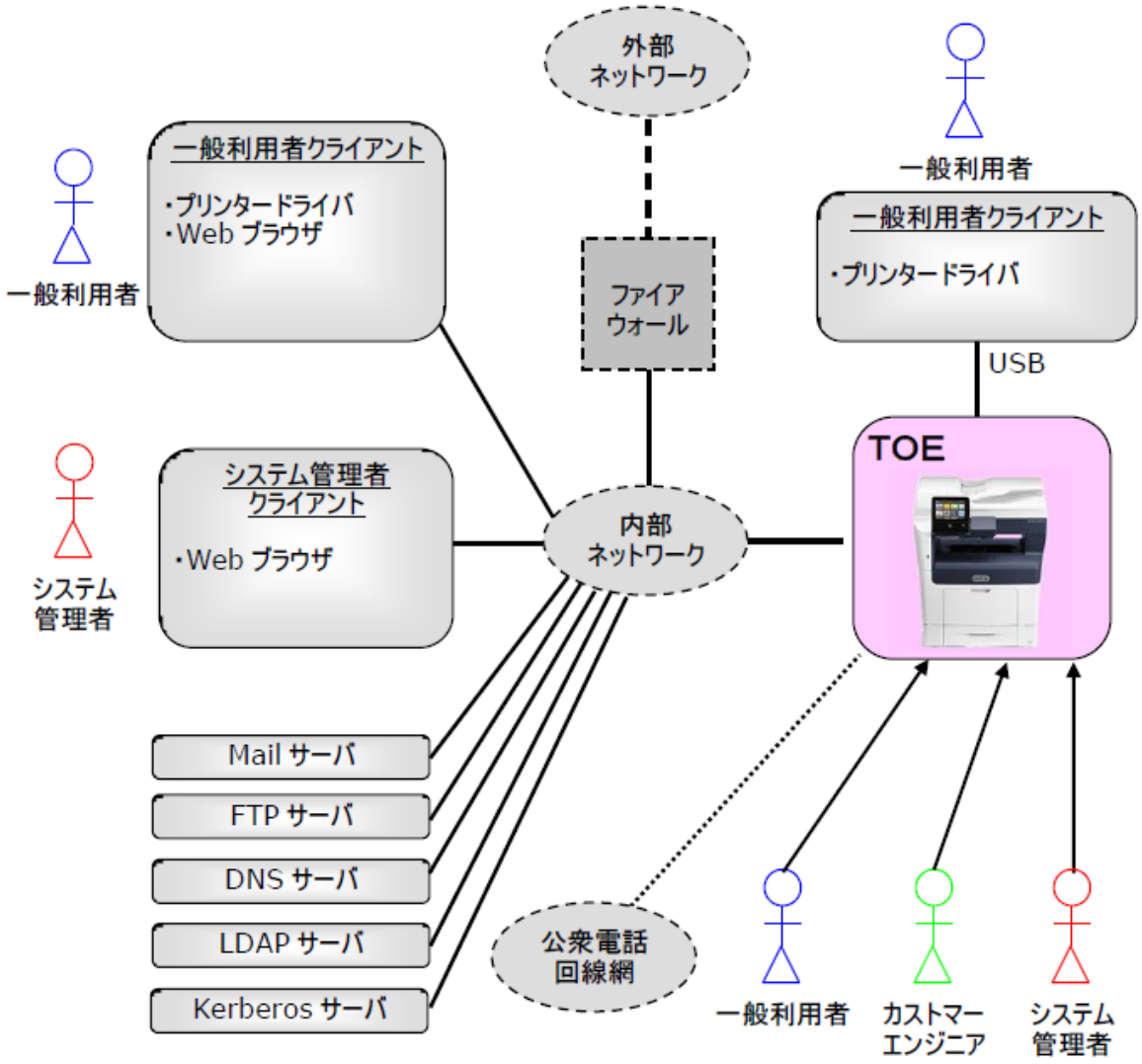

図 4-1　TOE の運用環境

TOE の運用環境において、TOE 以外の構成品を以下に示す。

(1) 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 7またはWindows 8.1
・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)

(2) 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 7 または Windows 8.1
・Web ブラウザ(OS 附属のもの)

(3) LDAP サーバ、Kerberos サーバ

TOE の設定で、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

(4) 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場合に必要である。

(5) 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する。

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) 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。

(2) 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

TOE の構成を図 5-1 に示す。TOE は MFD 全体である。

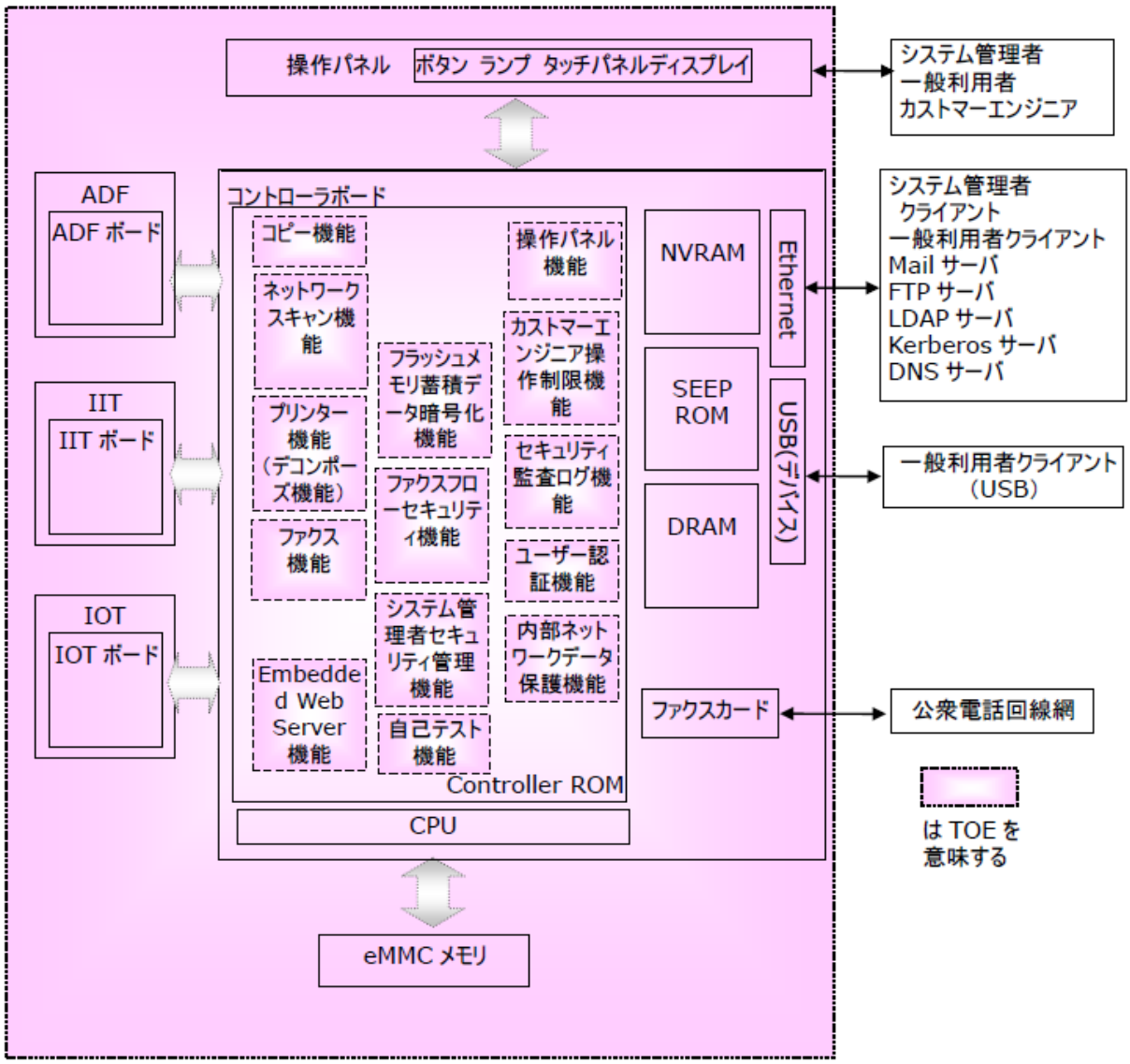

図 5-1　TOE の構成

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)

なお、クライアント PC(プリンタードライバ)は、利用者 ID の識別だけが行われ、パスワードによる認証は行われない。

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。

蓄積プリントに蓄積された文書データの場合には、それらの所有者情報と一致する利用者の操作が許可される。ファクス受信ボックスに蓄積された文書データの場合には、システム管理者の操作だけが許可される。

(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) フラッシュメモリ蓄積データ暗号化機能

本機能は、TOE 内部の eMMC メモリ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、TOE が生成したランダムな値を元に SHA-256 アルゴリズムを用いて生成する。暗号鍵は TOE の初回起動時に自動的に生成され、暗号鍵を破棄したり変更したりすることはできない。

(6) 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

(7) 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、ファクスカードで受信したファクスデータを、ファクス機能以外に渡さない構造になっている。

(8) 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 の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。

- Xerox VersaLink Series Multifunction and Single Function Printers
  System Administrator Guide; Version 2.0 October 2017
  (SHA1ハッシュ値；4ddc82babd4351f692018db85e37b397e915c9d7)
- Xerox VersaLink B405 Multifunction Printer
  User Guide; Version 2.0 October 2017
  (SHA1ハッシュ値；d7bed81e38fc7099f34fc849afe4dda1743fd2dd)
- Xerox VersaLink C405/B405 Multifunction Printer
  Security Function Supplementary Guide; Version 1.0 March 2018
  (SHA1ハッシュ値；3079046e77b61e2368a22efbcb1b93017dc2ffa4)

これらのドキュメントは、製品には添付されず、TOE の購入者が Xerox 社の Web サイトからダウンロードする。TOE の購入者は、ダウンロードしたファイルの SHA1 ハッシュ値を計算し、上記と比較することで、TOE のドキュメント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 9 月に始まり、平成 30 年 4 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 29 年 4 月及び 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、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。一部の製造サイトについては、現地での調査は省略され、過去の認証案件での評価内容の再利用が可能であると、評価機関によって判断されている。また、平成 29 年 5 月、6 月及び 11 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。

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。

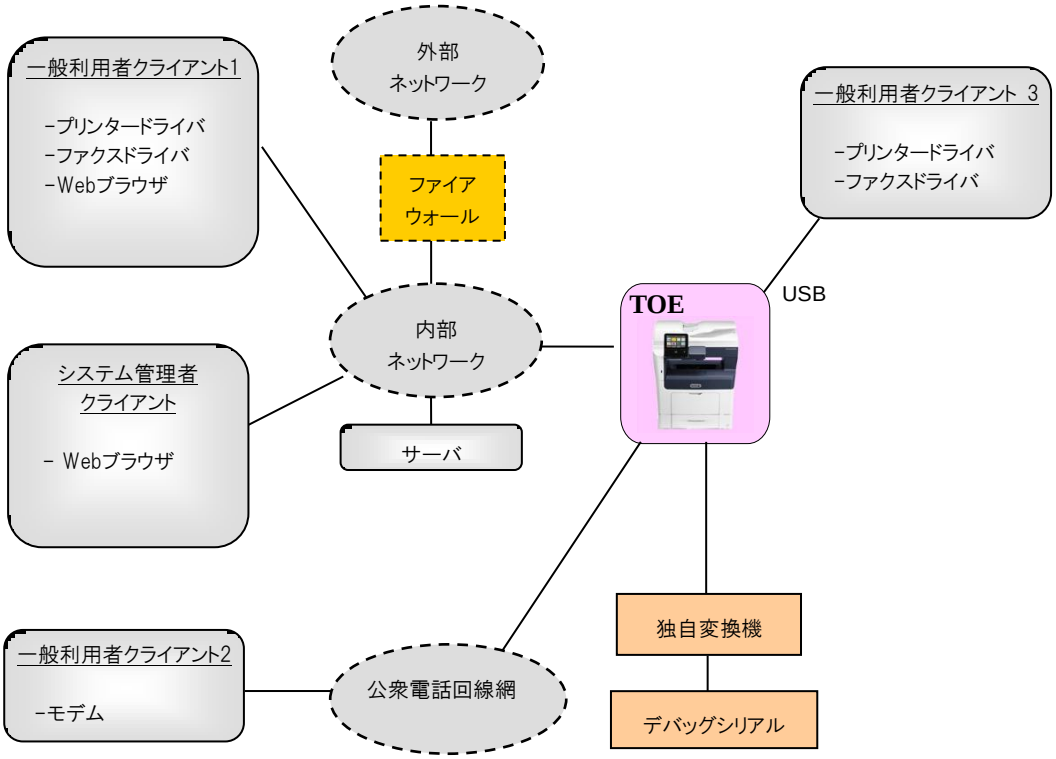

図7-1　開発者テストの構成図

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
TOE	Xerox VersaLink B405 Multifunction Printer (Controller ROM Ver. 1.0.31)
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
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2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 8.1搭載PC Webブラウザ：Microsoft Internet Explorer 11
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）として使用。以下の2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 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 ・プリンタードライバ／ファクスドライバ：PCL6 Print Driver Version 5.511.8 ※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	ファクス送受信の確認に使用 ・Microsoft Windows 8.1 搭載 PC ※PCのモデムポートを公衆電話回線網に接続
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 8.1搭載PC ・プリンタードライバ／ファクスドライバ：PCL6 Print Driver Version 5.511.8 ※ファクスドライバは使用できないことの確認に使用
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

名称	詳細
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）

開発者がテストしたTOEは、2章のTOE識別と同一の識別を持つ。

開発者テストは本STにおいて識別されているTOE構成と同じ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 TOEの外部インタフェースで確認可能なふるまい

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、その応答、MFDのふるまい、通信データ、監査ログを確認する。

② TOEの外部インタフェースでは確認できないふるまい

TOEの外部インタフェースでは確認できないふるまいについては、以下の手法が用いられた。

・開発者用インタフェースを使用して、TOE内部の動作を確認する。
・テスト用に変更したファームウェアを使用して、暗号機能等のモジュールの動作を確認する。
・暗号アルゴリズムについては、上記の方法で取得したデータを別の方法で算出した既知のデータと比較し、仕様どおりの暗号アルゴリズムが実装されていることを確認する。

＜開発者テストツール＞

開発者テストで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
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、仕様どおりにIPsec、TLSであることを確認する。
メーラー (Microsoft Windows Live Mail 2011)	TOEとMail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どお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。
デバッグシリアル＋独自変換機 ※構成は表7-1参照	eMMCメモリ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 Ver.7.31	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どお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、仕様どおりに動作することを確認した。

入力パラメタのバリエーションには、Web ブラウザと TOE の間の通信データの書き換えも含まれている。

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67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。

- ファクス対向機として、一般利用者クライアント 2 の代わりに、複合機である Xerox VersaLink C405 を使用。

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 の構成と同じ環境で実施された。

なお、独立テスト環境の構成品やテストツールは、開発者テストに用いられたものを利用しており、開発者が独自に開発したものも含まれているが、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、ファクス受信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＞

独立テストは、開発者テストと同じテスト手法で実施された。

＜独立テストツール＞

独立テストツールは、開発者テストと同じである。

＜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、50 項目のサンプリングテストと、4 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	外部認証時の利用者役割やアカウントロックが、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。
観点①	プリンタードライバ側で蓄積プリント以外のオプションを指定すると、TOEに受け付けられないことを確認する。

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 ネットワークインタフェースに、公知の脆弱性が存在する懸念がある。

② 印刷処理に、公知の脆弱性が存在する懸念がある。

③ 操作パネルに想定外の入力を行うと、TOE が予期しない動作をする懸念がある。

④ USB ポートによる不正アクセスの懸念がある。

⑤ 初期化処理中の不正アクセスによってセキュリティ機能が誤った動作をする懸念がある。

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を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは、独立テストの環境に、侵入テスト用の PC を追加した環境で実施した。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 7.40	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
OWASP ZAP Version 2.6.0	Webアプリケーションの脆弱性を診断するツール
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
Metasploit Version 4.6.2 及び 4.13.0	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。 ・OWASP ZAP、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、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	・不正な処理を含む印刷ジョブコマンドや印刷ファイルをTOEに入力しても、不正な処理が実行されないことを確認した。
脆弱性③	・操作パネルに、規定外の文字長、文字コード、特殊キーが入力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PCを接続してTOEにアクセスを試みても、プリンター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	・電源投入後のTOEの初期化処理中は、操作を受け付け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
・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
・SNMP機能の無効化
・USBプリント/保存機能の無効化

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 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
② 評価報告書に示された評価者の評価判断の根拠が妥当であること。
③ 評価報告書に示された評価者の評価方法が CEM に適合していること。

8.1 認証結果

提出された評価報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL2 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、保守機能を使用した場合、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。

Xerox VersaLink B405 Multifunction Printer ディスクレスモデル セキュリティターゲット, Version 1.2.3, 2018 年 3 月 22 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）
eMMC	Embedded Multi-Media Card（組み込み用マルチメディアカード）
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RAM）
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。

Embedded Web Server機能	一般利用者やシステム管理者がWebブラウザを介して、TOEの状態確認、設定変更、ジョブ削除ができるサービス
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
カストマーエンジニア	MFDの修理／保守を行うエンジニア
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することにより、IITで原稿を読み取りIOTから印刷を行う機能

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 privilege)の総称
蓄積プリント	利用者クライアントから送信された印刷データを蓄積する領域
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をすることにより、IITで原稿を読み取り後、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
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、一般利用者がMFDの操作パネルから指示をすることにより、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、公衆電話回線網を介して受信した文書データをファクス受信ボックスに格納し、システム管理者が操作パネルから印刷指示をした時に印刷を行う
ファクス受信ボックス	ファクス受信により読み込まれた文書データを蓄積する領域
プリンター機能	一般利用者が、利用者クライアントのプリンタードライバを使用して印刷データをMFDに送信し、IOTから印刷を行う機能。MFDが受信した印刷データはMFD内部の蓄積プリントに蓄積され、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

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 Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: 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] Xerox VersaLink B405 Multifunction Printer ディスクレスモデル セキュリティターゲット, Version 1.2.3, 2018年3月22日, 富士ゼロックス株式会社

[13] Xerox VersaLink B405 Multifunction Printer ディスクレスモデル 評価報告書, 第1.11版, 2018年4月5日, 一般社団法人ITセキュリティセンター 評価部