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7月9日** (IT**認証**0303)
認証番号	C0280
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific
TOE**のバージョン**	Controller ROM Ver. 1.103.0
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22年12月21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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific、 バージョン Controller ROM Ver. 1.103.0」（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22年12月10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一般消費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 C5570/C4470/C3370/C3371/C2270シリーズ及びDocuCentre-IV C5570/C4470/C3370/C3371/C2270シリーズで動作する。

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、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、それらの構成条件の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、DocuCentreIVシリーズでは提供していない。（DocuCentreIVシリーズでは、Eメール及びインターネットファクス機能は標準装備されておらず、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及び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に対応する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22年12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、本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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific
バージョン：	Controller ROM Ver. 1.103.0
開発者：	富士ゼロックス株式会社

本TOEは、MFDであるAsia Pacific向けのFuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 またはDocuCentre-IV C5570/C4470/C3370/C3371/C2270シリーズに、オプションの「データセキュリティキット」を搭載した状態の、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確認する。

オプションの「データセキュリティキット」は、製品に同梱されている「許諾書」と、当該オプションによって使用可能となるハードディスク蓄積データの上書き消去と暗号化機能について、ガイダンスに記載されたとおりの設定が可能であるか否かで、「データセキュリティキット」の有無を確認することができる。

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。

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。

「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。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、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。

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、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機構を備えている。

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。

TOEの利用者は、MFDの操作パネル、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。

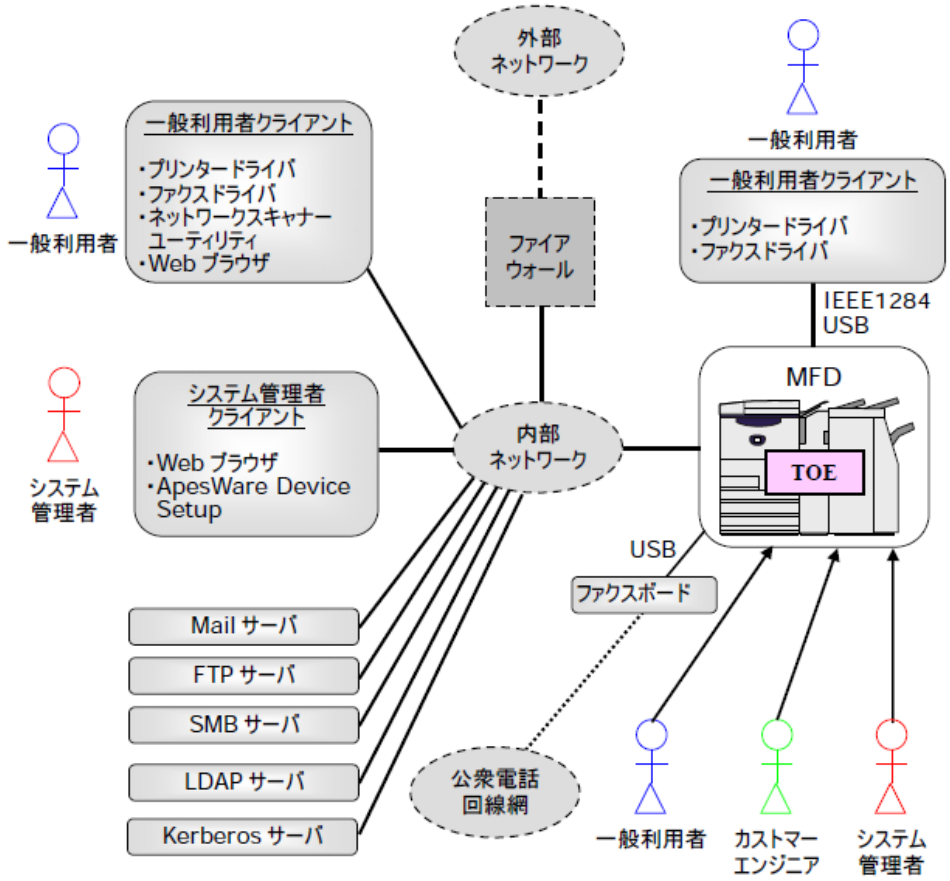

図4-1　TOEの使用環境

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 C5570/C4470/C3370/C3371/C2270シリーズ
・Fuji Xerox DocuCentre-IV C5570/C4470/C3370/C3371/C2270シリーズ

機種の中には、MFDの基本機能の内、スキャナー機能やファクス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、スキャナー機能やファクス機能が標準装備されている機種、スキャナー機能やファクス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やファクス機能を追加した構成の、すべてが評価対象の構成である。

ただし、DocuCentre-IVシリーズのEメールとインターネットファクス機能については、すべてのDocuCentre-IVシリーズの機種で標準装備されておらず、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PCであり、USBやIEEE1284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 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

MFDの基本機能を利用する際に、必要に応じて設置する。

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。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シリーズに対しては、「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、DocuCentreIVシリーズでは、Eメール及びインターネットファクス機能は標準装備されておらず、本評価対象の構成には含まれていない。）

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。

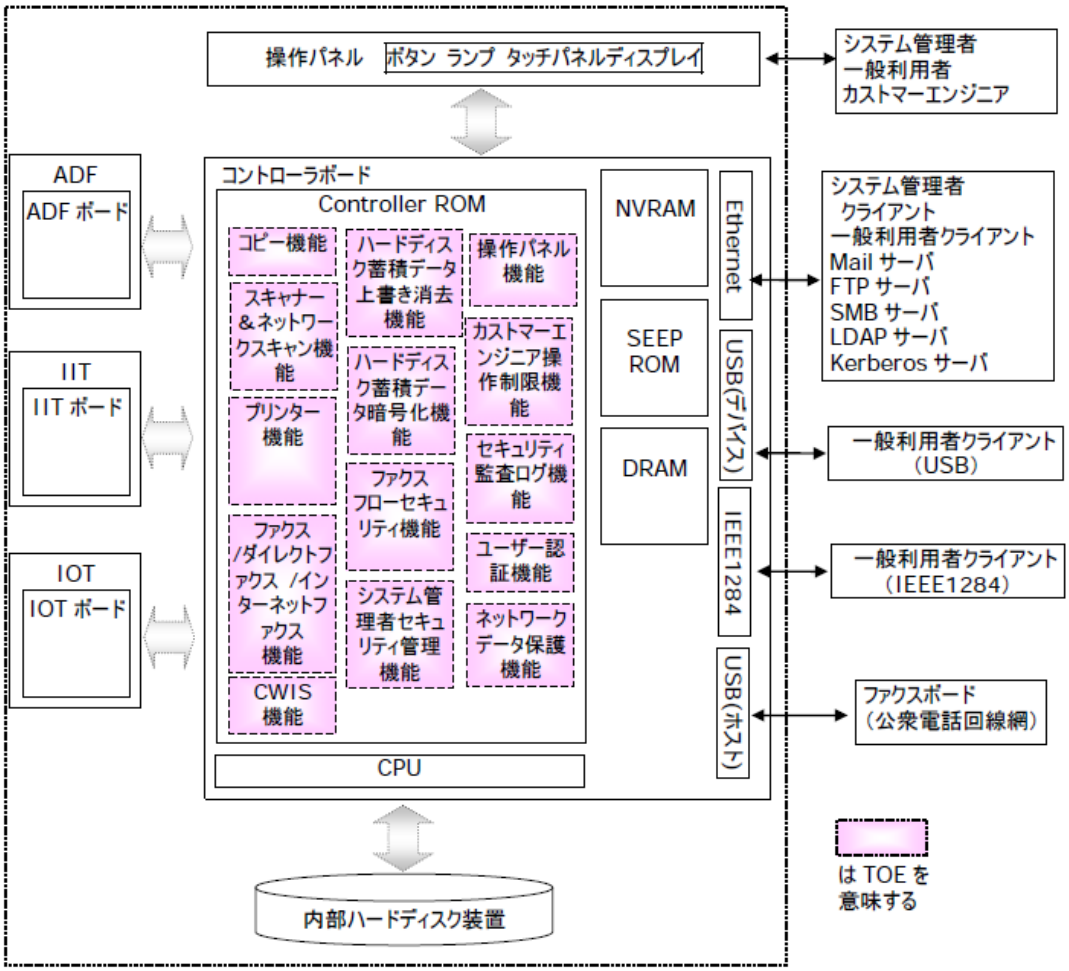

図5-1　TOE境界

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。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、内蔵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Ethernet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、MFDに搭載されて動作する。

MFDとEthernet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。

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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Administrator Guide (ME4564E2-3)

・ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 User Guide (ME4563E2-3)

・ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Security Function Supplementary Guide (DE4552E2-1)

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7月に始まり、平成22年12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22年9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・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22年9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。

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。

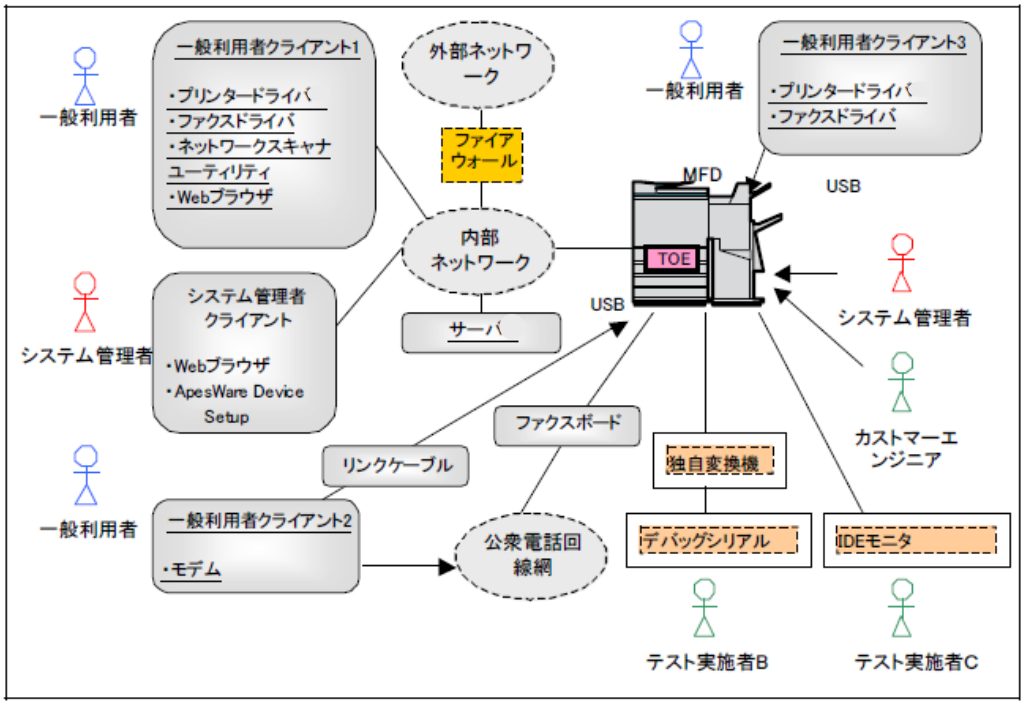

図7-1　開発者テストの構成図

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 C3370、DocuCentre-IV C5570の2機種である。TOEは、ApeosPort-IV C5570/C4470/C3370/C3371/C2270シリーズと、DocuCentre-IV C5570/C4470/C3370/C3371/C2270シリーズ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　開発者テストの使用機器

名称	詳細
サーバ	Mailサーバ、LDAPサーバ、Kerberosサーバとして使用。 ・Windows Server 2003 sp2搭載PC ・各種サーバ：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。 ・Windows XP professional sp2搭載PC ・Webブラウザ：Internet Explorer 6.0 sp2 ・ApeosWare Device Setup Version 1.0.0.1
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。 ・Windows 7搭載PC ・Webブラウザ：Internet Explorer 8 ・ネットワークスキャナーユーティリティ：Ver.1.7.3 ・プリンタードライバ／ファクスドライバ：Version 6.00 ・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。 ・Windows XP professional 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。
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やIEEE 1284ポート経由の接続）として使用。 ・Windows VISTA sp2搭載PC ・プリンタードライバ／ファクスドライバ：Version 6.00
IDEモニタ	HDD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 2000搭載PCに専用機器IDE-POCKET（東陽テクニカ製）を接続 ・ソフトウェア：IDE-WinU V1.9.3（東陽テクニカ製）
デバッグシリアル	MFDのデバッグ用端末。 ・使用機器：システム管理者クライアント用PC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 ・ソフトウェア：Tera Term Pro version 2.3
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 Ver 1.1.2

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 sp2）、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。

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＞

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IDEモニタを使用して、HDDへ書き込まれるデータと、書き込み後のHDD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、HDD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HDDを、他機種のHDD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 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 ※構成は表7-1。	MFD内のHDD接続用のIDEバスのデータをモニタし、HDDに書き込まれるデータを観測する。また、HDD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 1.2.3	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、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。

＜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による処理の中断と電源ONによる再開、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。

b.　実施テストの範囲

テストは開発者によって74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。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

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。

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

評価者が実施したテストの構成を、図7-2に示す。

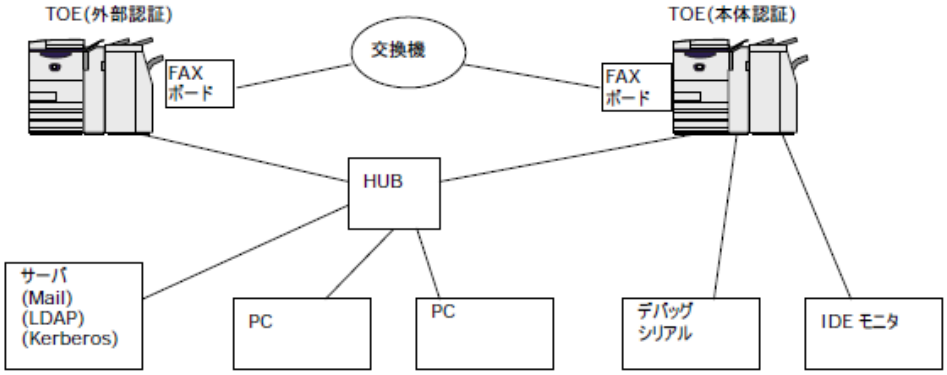

図7-2　評価者テストの構成図

評価者が実施したテストの構成は、開発者テストと同等の構成である。

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り、TOE（外部認証）ではApeosPort-IV C3370、TOE（本体認証）ではDocuCentre-IV C5570を使用した。ただし、MFDとのファクス送受信用に、開発者テストで使用したPCの代わりに、評価者テストではMFDを使用しているが、セキュリティ機能のテストに影響はないことが評価されている。

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＞

① 開発者テストのサンプリングの観点で、開発者が実施したすべてのテスト項目について、MFDの2機種のいずれかで同じテストを実施する。

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、テストされていないパラメタのふるまいを確認する。

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。

＜独立テスト手法＞

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。

＜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	開発者が実施したすべてのテスト項目を、MFDの2機種のいずれかで同じテストを実施し、開発者と同じ結果が得られることを確認する。
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、利用者IDの異なるシステム管理者の識別認証の成功と失敗が混在した場合のアカウントロックのふるまい、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。
②	Docucenterシリーズ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。
②	外部認証（Kerberosサーバ）で、利用者属性を格納したLDAPサーバを使用しない場合のアクセス制御のふるまいが、仕様どおりであることを確認する。（注：SAとしては認識されず、一般利用者として認識される。）

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。

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。

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＞

図7-2の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。使用したツールの詳細を表7-4に示す。

表7-4　侵入テスト構成

名称		概要・利用目的
侵入テスト用PC		Windows XP、Windows 7を搭載したPCであり、以下の侵入テスト用ツールを動作させる。
	①Zenmap+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）。
	②Fiddler2 V2.3.0.0	Webブラウザ（PC）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。

＜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

脆弱性	テスト概要
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PC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。
②	・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。
③	・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。
④	・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。
⑤	・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。

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、本機能は提供されない。）
8	ユーザー認証機能	[本体認証]または[外部認証]に設定 （注：両方の設定が評価されている。外部認証時は、さらにLDAPまたはKerberosのいずれかの設定が必須である。）
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 （注：本体認証時は、[有効]の設定で評価がされている。）
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 （注：本体認証時は、[有効]の設定で評価がされている。）
15	ユーザーパスワードの文字	[9]桁に設定

	数制限機能	（注:外部認証時は、LDAPやKerberosサーバ側において最低9桁のパスワードを設定する必要がある。）

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。

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機種によって、提供する機能が異なっている。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に興味のある消費者は、TOEを搭載したMFD製品購入時には、各自の想定する機能と運用が可能かどうかに留意して、MFD機種を選択する必要がある。

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。

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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/ C3370/C3371/C2270 Series Controller Software for Asia Pacific セキュリティターゲット バージョン V1.0.6　2010年11月29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）
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）
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。
CWIS機能	Webブラウザを使用して、親展ボックスに格納された文書データを取り出したり、システム管理者が設定データを管理したりする機能。CWISはセンターウェアインターネットサービスの略。
IEEE1284	プリンター用のパラレルポートの標準規格。
SA	「システム管理者」の説明参照。
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。

機械管理者	「システム管理者」の説明参照。
カストマーエンジニア	MFDの保守/修理を行うエンジニア。
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)の総称。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。
親展ボックス	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することができる。
スキャナー機能	一般利用者がMFDの操作パネルから指示をすることにより、IITで原稿を読み込み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の機能や、Webブラウザを使用してCWIS機能により取り出す。
操作パネル機能	一般利用者、システム管理者、カストマーエンジニアがMFDの機能を利用するための操作に必要なインタフェース機能。
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データをプリントジョブとして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	「プリンター機能」の説明参照。
通常プリント	「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をすることにより、IITで原稿を読み込み後に、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。
プリンター機能	一般利用者が一般利用者クライアントからプリント指示をして、プリンタードライバからMFDへ送信された印刷データを、IOTから印刷を行う機能。 プリンター機能には、印刷データをMFDが受信するとすぐに印刷を行う「通常プリント」と、印刷データを一時的にMFD内部のハードディスク装置に蓄積して、一般利用者が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」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。

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 C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/ C3370/C3371/C2270 Series Controller Software for Asia Pacific セキュリティターゲット バージョン V1.0.6　2010年11月29日　富士ゼロックス株式会社

[13] Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/ C3370/C3371/C2270 Series Controller Software for Asia Pacific 評価報告書 第1.5版 2010年12月10日　一般社団法人 ITセキュリティセンター 評価部