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21日 (IT認証0305)
認証番号	C0294
認証申請者	富士ゼロックス株式会社
TOEの名称	Xerox Color 550/560 Printer
TOEのバージョン	Controller ROM Ver. 1.203.1、IOT ROM Ver. 62.23.0、IIT ROM Ver. 6.13.0、ADF ROM Ver. 12.4.0
PP適合	IEEE Std 2600.1-2009
適合する保証パッケージ	EAL3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 Common Criteria for Information Technology Security Evaluation
Version 3.1 Release 3

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

評価結果：合格

「Xerox Color 550/560 Printer」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「Xerox Color 550/560 Printer、 バージョン Controller ROM Ver. 1.203.1、IOT ROM Ver. 62.23.0、IIT ROM Ver. 6.13.0、ADF ROM Ver. 12.4.0」（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23年6月8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、ファクス機能等を有するデジタル複合機（以下「MFD」という。）、Xerox Color 550/560 Printerである。

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。

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、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、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している。

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

本評価の対象となる利用者の認証は、利用者クライアントのプリンタードライバからの印刷データ送信には適用されない。TOEは、本体認証時に、印刷データ送信の際にも利用者の認証を実施しているが、その利用者認証は本評価の対象外である。

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。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、ダイレクトファクス機能を提供しているが、そ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6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：	Xerox Color 550/560 Printer	
バージョン：	Controller ROM	Ver. 1.203.1
	IOT ROM	Ver. 62.23.0
	IIT ROM	Ver. 6.13.0
	ADF ROM	Ver. 12.4.0
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。

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TOE名称とバージョン情報、または、設定値リストのプリント出力に記述されたTOE名称とバージョン情報を確認する。

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、MFD機能を使用する際に、デジタル複合機用のProtection Profileであ るIEEE Std 2600.1-2009 [14]（以下「PP」という。）で要求されているセキュリティ機能要件を満たすセキュリティ機能を提供する。TOEの提供するセキュリティ機能には、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等が含まれており、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ている。

・U.NORMAL
　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TOEの利用者である。一般利用者に該当する。

・U.ADMINISTRATOR
　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（機械管理者とSA）に該当する。

・TOE Owner
　TOE資産の保護や、TOEの運用環境のセキュリティ対策方針の実現に責任を持つ人物または組織である。

・カストマーエンジニア
　MFDの保守/修理を行うエンジニアである。

また、TOEの保護資産は以下のものである。

・User Document Data
　利用者の文書データ。

・User Function Data
　TOEによって処理される利用者の文書データやジョブに関連する情報。ジョブフローと親展ボックスが含まれる。

・TSF Confidential Data

セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められるデータ。本TOEでは、セキュリティ機能で使用されるデータは、すべて、TSF Confidential Dataであると定義されている。例えば、利用者のパスワード、暗号鍵の生成に使用される暗号化キー、セキュリティ機能の設定値、監査ログの他に、ユーザーIDも含まれる。

・TSF Protected Data

セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。本TOEの定義では、該当するデータはない。

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。これらの脅威は、PPに記述されているものと同じである。

表3-1 想定する脅威

識別子	脅 威
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

※PPでは、上記に加えてT.PROT.ALT(TSF Protected Data may be altered by unauthorized persons)の脅威が存在する。本TOEでは、TSF DataはすべてTSF Confidential Dataであると定義されており、TSF Protected Dataは存在しないため、脅威T.PROT.ALTは想定していない。

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.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらは利用者のデータに対する脅威であり、TOEは、「ユーザー認証機能」、「ハードディスク蓄積データ上書き消去機能」、「ハードディスク蓄積データ暗号化機能」及び「内部ネットワークデータ保護機能」で対抗する。

TOEの「ユーザー認証機能」に含まれる識別認証機能とMFD基本機能に対するアクセス制御機能は、正当な利用者だけにTOEの利用を許可する。これらの機能の詳細は、3.1.2.2のP.USER_AUTHORIZATIONの項目を参照。

さらに、TOEの「ユーザー認証機能」に含まれる利用者データに対するアクセス制御機能は、識別認証された利用者が、文書データ、親展ボックス、ジョブフローに対して、以下の操作を行う際にアクセス制御を行い、操作対象の所有者とシステム管理者に当該操作を許可する。なお、文書データは、スキャナー機能やファクス受信機能で「親展ボックス」と呼ばれる領域に蓄積される場合と、利用者端末のプリンタードライバから送信されて「プライベートプリント」と呼ばれる領域に蓄積される場合があり、各場合で提供される操作が異なる。

- 親展ボックスに蓄積された文書データに対する操作:
  印刷、ファクス送信、ネットワーク送信、削除
- プライベートプリントに蓄積された文書データに対する操作:
  印刷、削除
- 親展ボックスに対する操作:
  文書データの登録、ジョブフローの登録、親展ボックスの名称等の修正、親展ボックスの削除
- ジョブフローに対する操作:
  実行、修正、削除

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、削除した文書データの内容が内部ハードディスク装置から読み出されることを防止する。

TOEの「ハードディスク蓄積データ暗号化機能」は、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。これにより、保守や廃棄の際にTOEから取り外された内部ハードディスク装置から、削除されていない文書データが漏えいすることを防止する。なお、暗号アルゴリズムは128bitのAESである。暗号鍵は、TOE設置時にシステム管理者によって設定された12桁の英数字から成る暗号化キーを元に、TOE起動時に富士ゼロックス社の独自方式に従って生成され、電源オフにより消去される。

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、通信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。

以上の機能により、TOEは、TOEの権限外使用や、HDDに格納されたデータや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したりすることを防止する。

(2) 脅威「T.CONF.DIS」「T.CONF.ALT」への対抗

これらはセキュリティ機能に影響するTSFデータに対する脅威であり、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「内部ネットワークデータ保護機能」で対抗する。

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、識別認証されたシステム管理者だけに許可する。

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。

その他の「ユーザー認証機能」及び「内部ネットワークデータ保護機能」は、(1)の場合と同じである。

以上の機能により、TOEは、TOEの権限外使用や、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し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。これらの組織のセキュリティ方針は、PPに記述されているものと同じである。

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.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in

	the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

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.USER.AUTHORIZATION」への対応

TOEは、「ユーザー認証機能」で本方針を実現する。

TOEの「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。さらにTOEは、識別認証機能を補強するために、認証用のパスワードをTOEに登録する際に、9文字以上の文字列に限定する。

なお、ファクス受信や、利用者クライアントのプリンタードライバから送信された印刷データの受信は、上記のP.USER.AUTHORIZATIONを実現するための識別認証は適用されずに許可され、受信した文書データはTOE内に蓄積される。TOEに蓄積された文書データの印刷等を行うためには、TOEの操作パネル等での操作が必要であり、識別認証が要求される。

TOEの「ユーザー認証機能」に含まれるMFD基本機能に対するアクセス制御機能は、識別認証された利用者が、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基本機能を使用する際にアクセス制御を行い、権限のある利用者だけに実行を許可する。アクセス制御では、MFD基本機能毎に設定された許可利用者の識別情報を参照し、対象機能の実行が許可されているかどうかを判断する。

これらにより、TOEは、正当な利用者だけにTOEの利用を許可する。

(2) 組織のセキュリティ方針「P.SOFTWARE.VERIFICATION」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の完全

性が検査される。

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

TOEは、「セキュリティ監査ログ機能」で本方針を実現する。

TOEの「セキュリティ監査ログ機能」は、セキュリティ機能の使用において、セキュリティ事象が発生した際に監査ログを生成しTOEのNVRAM及びHDDに格納する。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Webブラウザを使用して読み出すことができる。

(4) 組織のセキュリティ方針「P.INTERFACE.MANAGEMENT」への対応

TOEは、「ユーザー認証機能」と「インフォメーションフローセキュリティ機能」で、本方針を実現する。

TOEの「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、利用者が操作をしない状態が規定時間経過した場合には、セッションを切断する。

また、TOEの「インフォメーションフローセキュリティ機能」は、TOEの各種インタフェースから受信したデータを、TOEが処理せずにLANに転送することができないしくみになっている。

これらにより、TOEのインタフェースが不正に使用されることを防止する。

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。これらの前提条件は、PPに記述されているものと同じである。

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.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 使用環境と構成

TOEであるデジタル複合機は、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、TOE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。

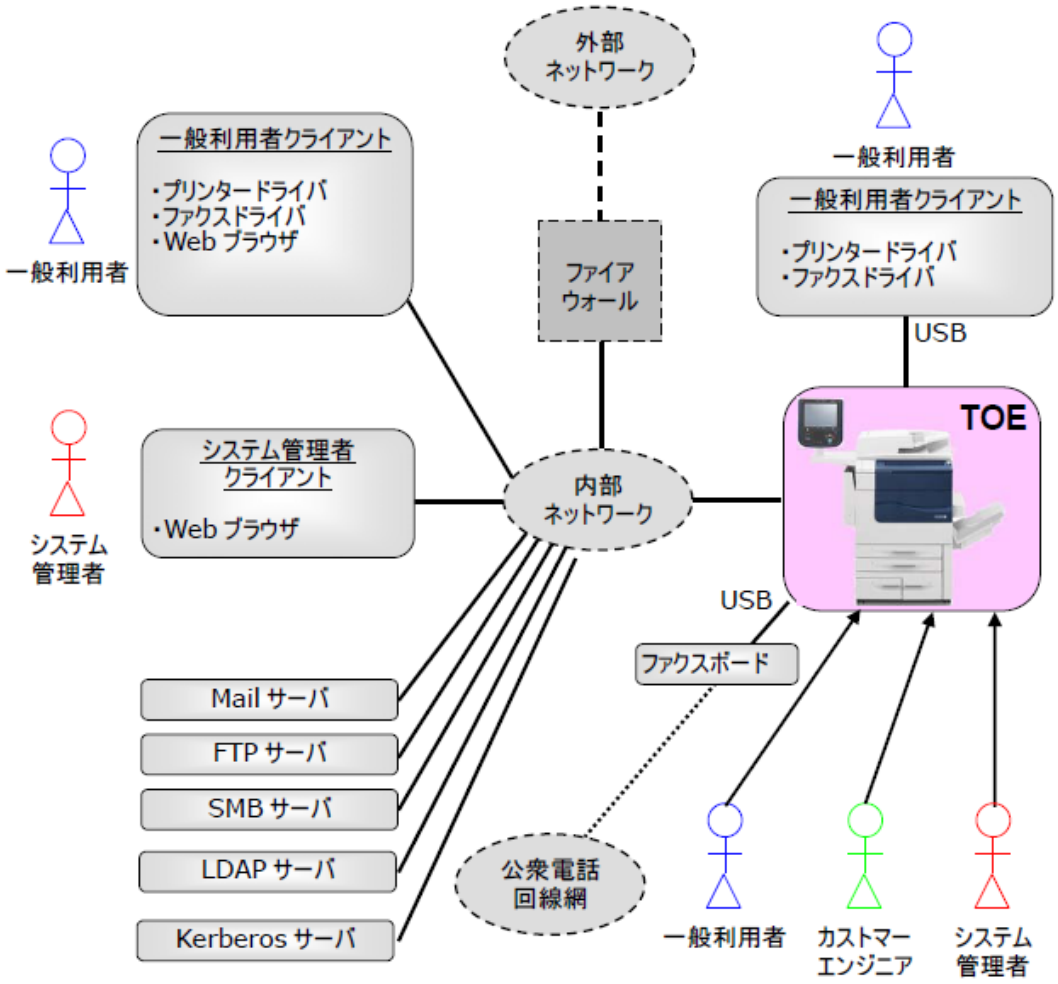

図4-1　TOEの使用環境

TOEの使用環境の構成品について以下に示す。

(1) ファクスボード

TOEにはファクス機能が搭載されているが、TOE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するためには、指定されたファクスボードを別途購入する必要がある。

(2) 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 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)

(3) 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)

(4) 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。

(5) 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。

② 本評価では、PPが要求している識別認証のセキュリティ機能要件は、利用者クライアントのプリンタードライバから印刷データをMFDに送信する操作は適用対象外であるという解釈がされている。そのため、以下は評価対象のセキュリ

ティ機能ではない。

・ プリンタードライバでは、ユーザーIDとパスワードの入力を求められる。そのユーザーパスワードによる認証は、評価の対象外である。
（実際には、本体認証の場合には、TOEで認証処理が行われる。外部認証の場合には、TOEではパスワードは使用されない。）

なお、プリンタードライバで指定するユーザーIDはTOE内で識別処理が行われ、印刷データはユーザーID毎に分類されて蓄積される。その識別処理は、TOEの実装のために必要な機能であり、評価対象のセキュリティ機能に含まれる。

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であるMFDの構成を、MFD以外のIT環境と共に示す。図5-1で、TOEは中央の色付けして囲まれている部分の全体である。

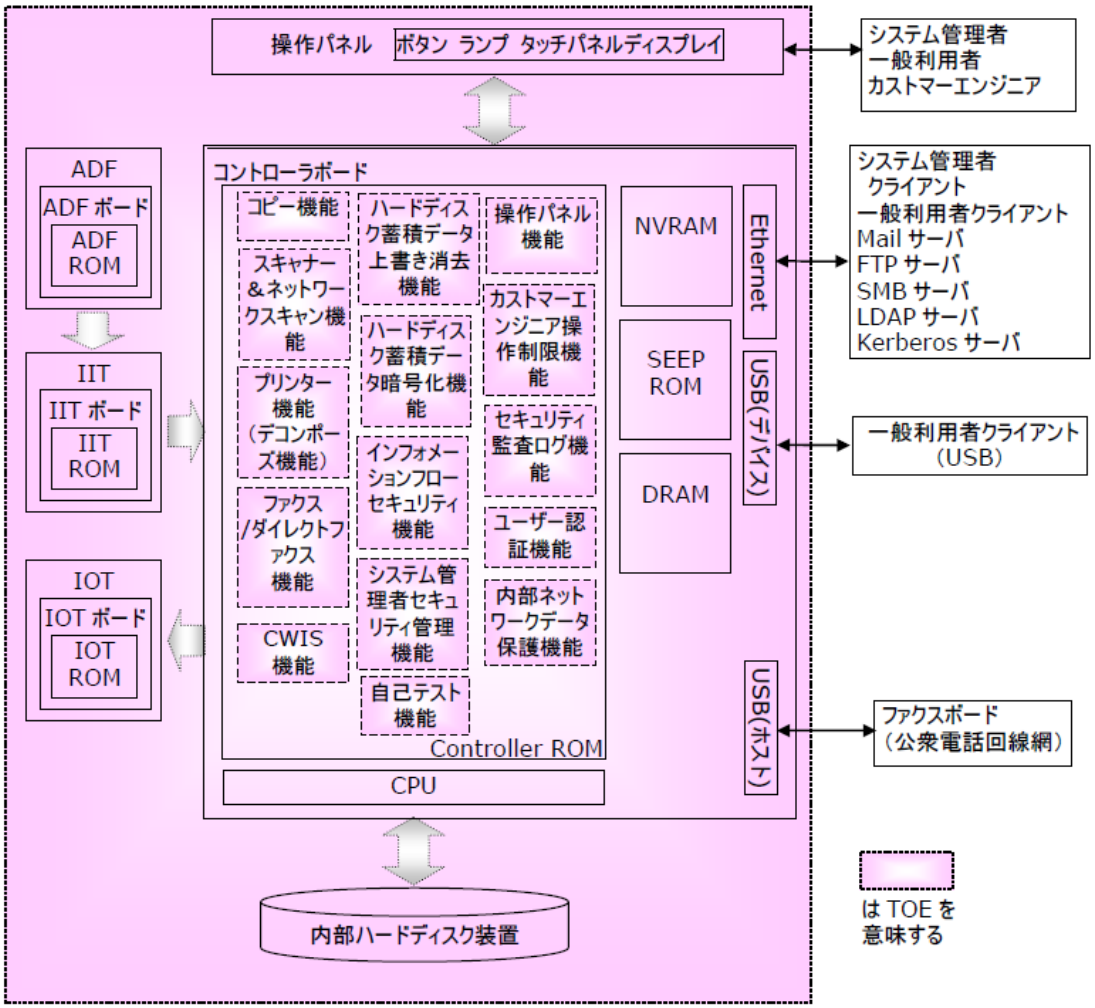

図5-1　TOE境界

また、図5-1で、コントローラボードに搭載されている機能は、3章で説明したセキュリティ機能と、それ以外のMFDの基本機能である。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 一般利用者クライアント（プリンタードライバ）からの利用

利用者が、EthernetまたはUSB接続された一般利用者クライアントのプリンタードライバから文書データのプリント要求をする際には、「ユーザー認証機能」によって、文書データは利用者の識別情報と共に、内部ハードディスク装置のプライベートプリントに蓄積される。（注：本体認証の場合には、実際には利用者の認証も行われるが、その動作は評価対象のセキュリティ機能ではない。）プライベートプリントに蓄積された文書データは、操作パネルを操作して印刷出力する。

② 一般利用者クライアント（ファクスドライバ）からの利用

利用者が、EthernetまたはUSB接続された一般利用者クライアントのファクスドライバから文書データのファクス送信指示をする際には、「ユーザー認証機能」によって利用者の識別認証が行われ、識別認証の成功した利用者の文書データは、TOE内には格納されず、ただちにファクス送信される。（注：本機能はダイレクトファクス機能と呼ばれ、本評価の構成では、本体認証の場合のみ使用でき、外部認証の場合には使用できない。）

③ 操作パネルからの利用

利用者が、操作パネルを操作して、TOEのコピー機能、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、ファクス機能等の基本機能を使用する際には、「ユーザー認証機能」によって利用者の識別認証が行われ、正当な利用者だけにTOEの操作が許可される。スキャナー機能やファックス受信でTOEに取り込まれた文書データは、内部ハードディスク装置の親展ボックスに蓄積される。

識別認証された利用者が内部ハードディスク装置の親展ボックス及びプライベートプリントに蓄積されている文書データ等を操作する際には「ユーザー認証機能」によってアクセス制御が行われ、操作対象の所有者と管理者の操作だけが許可される。

利用者が、操作パネルを操作して、セキュリティ機能の「システム管理者セキュリティ管理機能」を使用する際には、「ユーザー認証機能」が適用され、識別認証された管理者権限を持つ利用者だけに、「システム管理者セキュリティ管理機能」の使用が許可される。

④ Webブラウザからの利用

利用者が、Webブラウザを操作して、内部ハードディスク装置の親展ボックスに蓄積されている文書データ等を操作する際には、「ユーザー認証機能」によって利用者の識別認証が行われ、正当な利用者だけにTOEの操作が許可される。さらにアクセス制御が行われ、操作対象の所有者と管理者の操作だけが許可される。親展ボックスに蓄積された文書データは、操作パネルだけでなくWebブラウザの操作でも、印刷出力が可能である。

利用者が、Webブラウザを操作して、セキュリティ機能の「システム管理者セキュリティ管理機能」や「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、識別認証された管理者権限を持つ利用者だけにTOEの操作が許可される。

⑤ 内部ハードディスク装置のデータ保護

①～④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内部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。

⑥ ネットワーク関連の保護

①～④の利用時に、TOEと、その他のIT機器がLAN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」により暗号通信プロトコルが使用される。また、「インフォメーションフローセキュリティ機能」により、各種インタフェースから入力されたデータに対して、TOEのセキュリティ機能が介在しない不正な中継が防止される。

⑦ 監査ログの生成

①～④の利用時にセキュリティ機能を使用する際、及び、⑥の暗号通信プロトコルの確立に失敗した際に、「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。

5.2 IT環境

TOEがネットワークを介して外部のIT機器と通信する際には、IPsecプロトコルを使用する。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サーバ内でユーザー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。

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 Color 550/560 Printer User Guide
(Version 1.0, August 2010)

・Xerox Color 550/560 Printer System Administrator Guide
(Version 1.0, August 2010)

・Xerox Color 550/560 Printer Security Function Supplementary Guide
(Version 1.0, April 2011)

なお、これらのドキュメントは製品には添付されず、利用者がXerox社のWebサイト http://www.support.xerox.com/support/ からダウンロードする。

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23年6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12月及び平成23年2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。ただし、本TOEの組立工場は中国と韓国の2ヶ所にあり、両方から製品が出荷される。中国の工場は評価者が現場を訪問し調査を実施している。しかし、韓国の工場については、現場訪問による調査は行われず、記録による調査と現地の状況を把握している日本のスタッフへのヒアリングによって、同じ手続きを採用している中国の工場と同様に、セキュリティ手段が確実に実施されていると評価機関によって判断されている。

また、平成22年12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。

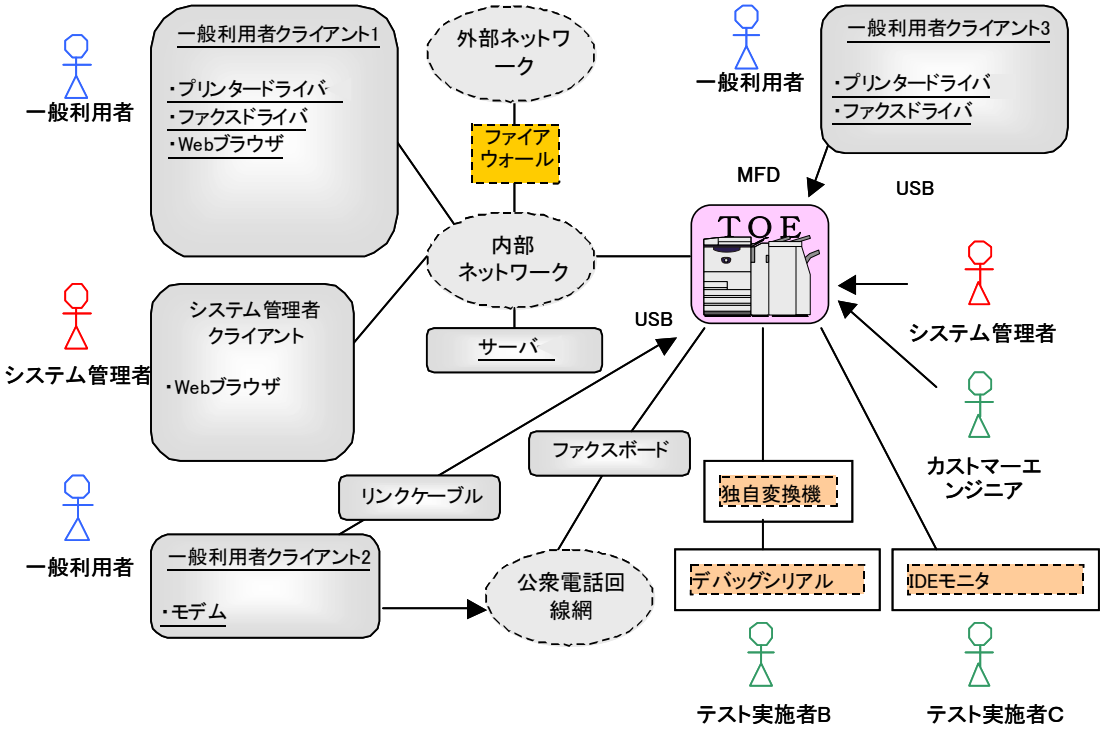

図7-1　開発者テストの構成図

評価の対象となったTOEは、Xerox Color 560 Printerであり、2章のTOE識別と同一の識別を持つ。他機種は、スキャンやプリント等のハードウェア処理速度が異なるだけで、ソフトウェアは同一でセキュリティ機能の振る舞いに違いはなく、1機種によるテストで十分であることが評価者によって評価されている。

テスト環境のTOE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 2008 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。 以下の3機種のいずれかでテストを実施。 a) Windows 7 professional搭載PC （Webブラウザ：Internet Explorer 8） b) Windows XP professional sp3搭載PC （Webブラウザ：Internet Explorer 6） c) Windows VISTA business sp2搭載PC （Webブラウザ：Internet Explorer 7）
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。 以下の3機種のいずれかでテストを実施。 a) Windows 7 professional搭載PC （Webブラウザ：Internet Explorer 8） b) Windows XP professional sp3搭載PC （Webブラウザ：Internet Explorer 6） c) Windows VISTA business sp2搭載PC （Webブラウザ：Internet Explorer 7） また、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：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ポート経由の接続）として使用。 ・Windows XP professional 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 XP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。

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 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。

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､インフォメーション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72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。

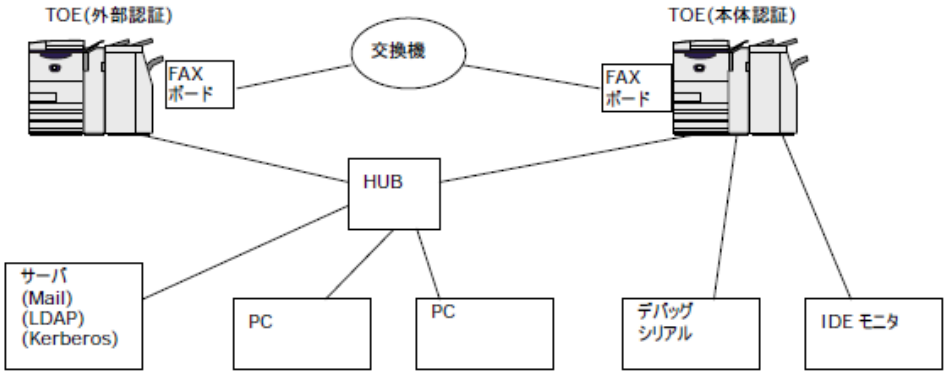

図7-2 評価者テストの構成図

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は、開発者テストと同一であり、TOE（外部認証）とTOE（本体認証）のいずれもXerox Color 560 Printer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 TOEが開発者のテストしたとおりに動作することを確信するために、開発者が実施したテスト項目について同じテストを実施し、その妥当性を確認する。

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、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について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した。 （ただし、暗号鍵生成アルゴリズムと暗号アルゴリズムが仕様どおりであることを確認するテストは除く。）
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、ユーザー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した。
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した。(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。

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、Windows VISTA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。
	①Nmap 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。
	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、一般利用者クライアント（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。

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	[有効]に設定
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	オートクリア機能	[有効]に設定
11	監査ログ機能	[有効]に設定
12	SNMPv3 通信機能	[有効]に設定
13	カストマーエンジニア操作制限機能	[有効]に設定
14	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。）

15	ネットワークスキャナーユーティリティの使用（WebDAV設定）	[無効]に設定
16	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：

2600.1, Protection Profile for Hardcopy Devices, Operational Environment A

（IEEE Std 2600.1-2009）

また、上記PPで定義された以下のSFRパッケージに適合する。

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A 適合
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A 適合
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A 適合
- 2600.1-FAX, SFR Package for Hardcopy Device FAX Functions, Operational Environment A 適合
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A 適合
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A 適合

・ セキュリティ機能要件： コモンクライテリア パート２拡張

・ 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

・ 追加の保証コンポーネント ALC_FLR.2

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。

本評価では、ドキュメントの配付について、Xerox社のWebサイト掲載までが評価されており、その後のダウンロードは利用者に委ねられている。利用者は、正当なWebサイト http://www.support.xerox.com/support/ からドキュメントをダウンロードするよう、注意する必要がある。

本評価では、PPで要求されているセキュリティ機能要件について、利用者クライアントのプリンタードライバからのプリント要求時には、識別認証の要件は存在せず、実際に紙に印刷するときに識別認証を要求するという解釈がされている。そのため、利用者クライアントのプリンタードライバからのプリント要求時にも識別認証を期待する消費者にとっては、ニーズに合致しない可能性があるので、注意が必

要である。

利用者クライアントのプリンタードライバ利用時には、紙印刷出力をするためには、操作パネルからの操作が必要である。しかし、スキャナー機能やファクス受信で蓄積された文書データは、操作パネルだけでなく、利用者クライアントのWebブラウザからの操作で紙印刷出力が可能である。出力された紙のセキュリティ確保のために、紙印刷出力を操作パネルからの操作に制限することを期待する消費者にとっては、ニーズに合致しない可能性があるので、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。

Xerox Color 550/560 Printer セキュリティターゲット, Version 1.1.8, 2011年6月6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。

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。
SA	「システム管理者」の説明参照。
TOE Owner	TOE資産の保護や、TOEの運用環境のセキュリティ対策方針の実現に責任を持つ人物または組織。
U. ADMINISTRATOR	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。システム管理者（機械管理者とSA）に該当する。
U.NORMAL	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。一般利用者に該当

	する。
User Document Data（文書データ）	利用者の文書データ。一般利用者がMFDのコピー機能、プリンター機能、スキャナー機能、ファクス機能を利用する際に、MFD内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。
User Function Data	TOEによって処理される利用者の文書データやジョブに関連する情報。ジョブフローと親展ボックスが含まれる。
TSF Confidential Data	セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められるデータ。本TOEでは、セキュリティ機能で使用されるデータは、すべて、TSF Confidential Dataであると定義されている。
TSF Protected Data	セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。本TOEの定義では、該当するデータはない。
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、ファクス機能等の利用者。
オートクリア機能	操作パネルおよびWebブラウザから何も操作をしない状態で一定の時間が経過したとき、自動的にログアウトされる機能。
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。
ジョブフロー	スキャン文書やファクス受信文書の処理を行うために、スキャナー設定情報や変換フォーマット、データの配信方法/配信先など一連の処理の流れ(手順)を、あらかじめ機器に設定したもの。
親展ボックス	MFDの内部ハードディスク装置に作成され、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

	タを蓄積する論理的なボックス。
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、操作パネル機能や、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。
プライベートプリント	プリンタードライバからMFDへ送信された印刷データを保存する内部ハードディスク装置の領域。
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] Xerox Color 550/560 Printer セキュリティターゲット, Version 1.1.8, 2011年6月6日, 富士ゼロックス株式会社

[13] Xerox Color 550/560 Printer 評価報告書, 第1.9版, 2011年6月8日, 一般社団法人 ITセキュリティセンター 評価部

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009