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23年10月12日 (IT認証1380)
認証番号	C0362
認証申請者	富士ゼロックス株式会社
TOEの名称	Xerox D110/D125 Copier/Printer
TOEのバージョン	Controller+PS ROM Ver. 1.201.1、IOT ROM Ver. 83.25.0、IIT ROM Ver. 9.8.0、 ADF ROM Ver. 13.10.0
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24年7月30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 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 D110/D125 Copier/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 D110/D125 Copier/Printer、バージョン Controller+PS ROM Ver. 1.201.1、IOT ROM Ver. 83.25.0、IIT ROM Ver. 9.8.0、ADF ROM Ver. 13.10.0」（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 24 年 7 月 18 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、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 を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL3 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、スキャナー機能を有するデジタル複合機（以下「MFD」という。）である。ファクス機能は搭載していない。

本 TOE は、コピー機能、プリンター機能、スキャナー機能等の 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、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する。

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

本評価では、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、「7.4 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。

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。

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」[1]、「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 24 年 7 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。TOE の評価が CC（[3][4][5]または[6][7][8]）及び CEM（ [9][10]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 D110/D125 Copier/Printer	
バージョン：	Controller+PS ROM	Ver. 1.201.1
	IOT ROM	Ver. 83.25.0
	IIT ROM	Ver. 9.8.0
	ADF ROM	Ver. 13.10.0
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と、ガイダンスの当該記載を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。

・一般利用者

TOE が提供するコピー機能、プリンター機能、スキャナー機能等の TOE 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。

・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(指示書)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、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、暗号通信プロトコルの設定値、監査ログが該当する。

・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 では、TSF Confidential Data を除いた、セキュリティ機能の各種設定値が該当する。

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。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.PROT.ALT	TSF Protected 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

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(指示書)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、スキャナー機能やコピー機能(コピー蓄積)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、プレビュー、削除、スキャナー機能で蓄積された文書のネットワーク送信、コピー機能(コピー蓄積)で蓄積された文書の編集
- 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(指示書)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(指示書)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 256bit 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（SSL 3.0、TLS 1.0）、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、内部ハードディスク装置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。

⑵ 脅威「T.PROT.ALT」「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。

TOE 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.

識別子	組織のセキュリティ方針
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、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 を実現するための利用者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。ただし、TOE に蓄積された文書データの印刷等を行うためには、TOE の操作パネルでの操作が必要であり、利用者の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。

⑵ 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。

⑶ 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 及び内部ハードディスク装置に格納する。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。

⑷ 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 運用環境と構成

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 の一般的な運用環境を図 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。

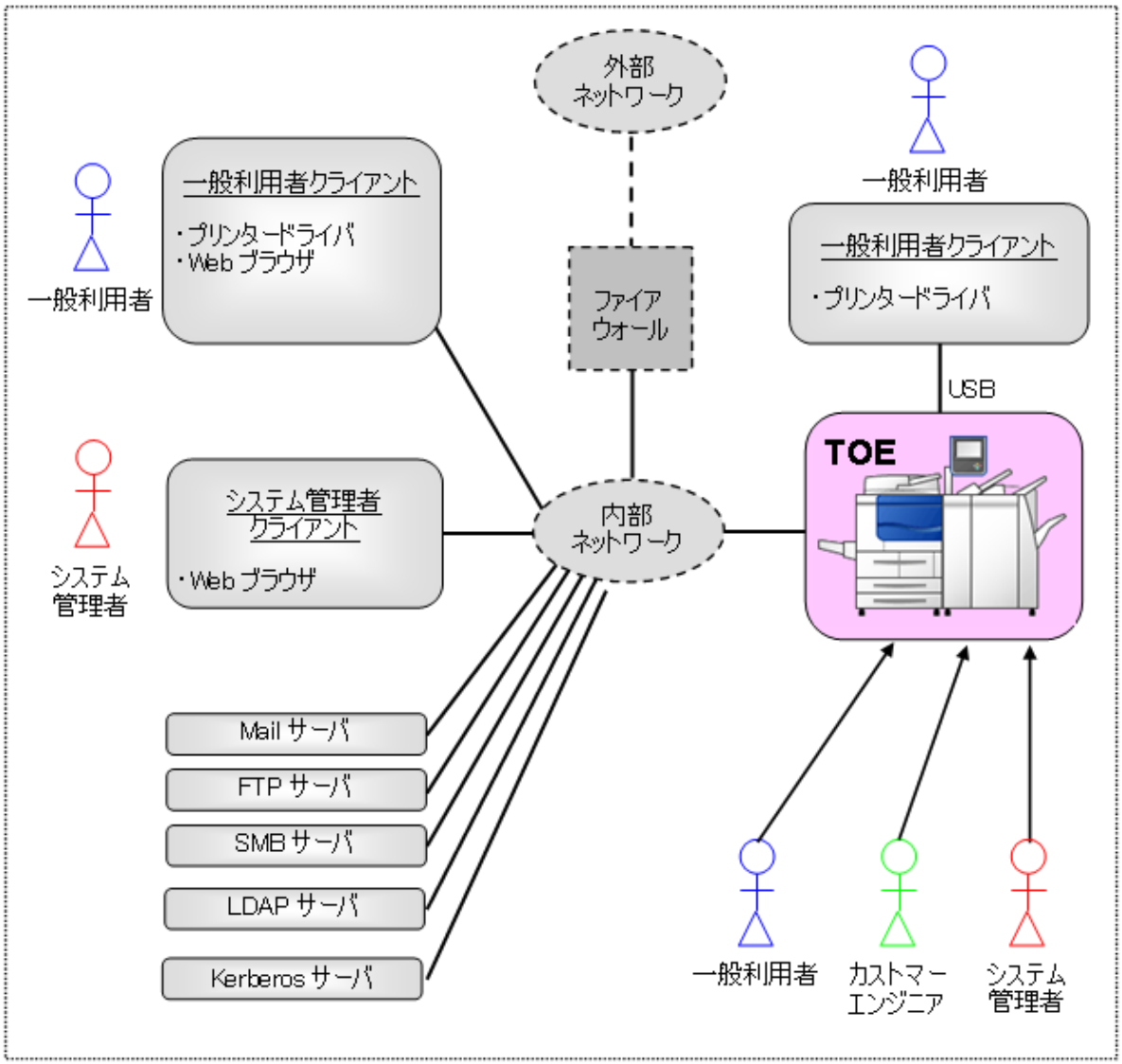

図4-1　TOEの運用環境

TOE の運用環境の構成品について以下に示す。

(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 XP、Windows Vista、Windows 7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)

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

(3) 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。

(4) Mail サーバ、FTP サーバ、SMB サーバ

TOE は、Mail サーバ、FTP サーバ、SMB サーバと文書データをやり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。

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

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。

・ 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。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、運用者の責任となる。

②印刷データ送信時の識別認証

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、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。

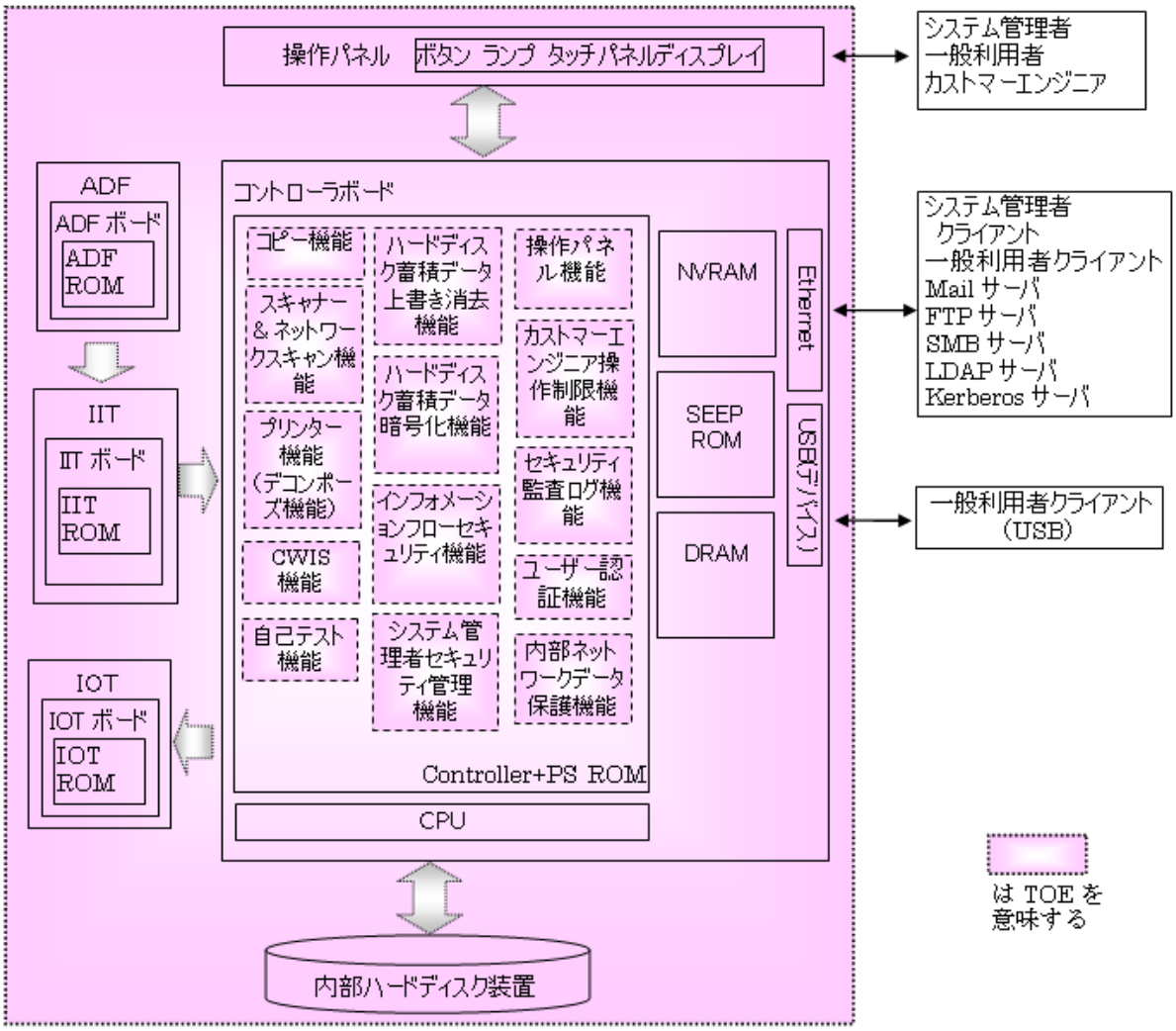

図5-1　TOE境界

TOE の機能は、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。スキャナー機能やコピー機能(コピー蓄積)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、文書データ等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。

③Web 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、文書データ等の所有者と管理者の操作だけが許可される。スキャナー機能で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。

④内部ハードディスク装置のデータ保護

①～③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。

⑤ネットワーク関連の保護

①～③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。

⑥監査ログの生成

①～③の利用時にセキュリティ機能を使用する際、及び、⑤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 の設定で外部認証を選択した場合は、TOE は、TOE 外の認証サーバ（LDAP サーバまたは Kerberos サーバ）から利用者の識別認証の結果を取得する。ただし、機械管理者は、TOE 外の認証サーバでは識別認証されず、TOE 内に登録した機械管理者の情報を使用して識別認証される。また、認証サーバとして LDAP サーバと Kerberos サーバのいずれを使用する場合であっても、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。

MFD と内部ネットワークで接続する各種サーバやクライアントは、各種暗号通信プロトコル使用して通信を行う。まず、TOE は、各種サーバやクライアントに対して IPsec 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。また、TOE と認証サーバ間の通信は、LDAP (SSL/TLS)、Kerberos プロトコルを用いて、識別認証に関するデータを暗号化する。

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。

- Xerox D95/D110/D125 Copier/Printer User Guide
  (Version 1.0, February 2012)
- Xerox D95/D110/D125 Copier/Printer System Administrator Guide
  (Version 1.0, February 2012)
- Xerox D95/D110/D125 Copier/Printer Security Function Supplementary Guide
  (Version 1.0, February 2012)

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。

7.2 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 23 年 10 月に始まり、平成 24 年 7 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 24 年 3 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・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。一部の開発・製造サイトについては、現地訪問は省略され、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 24 年 3 月及び 6 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、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価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。

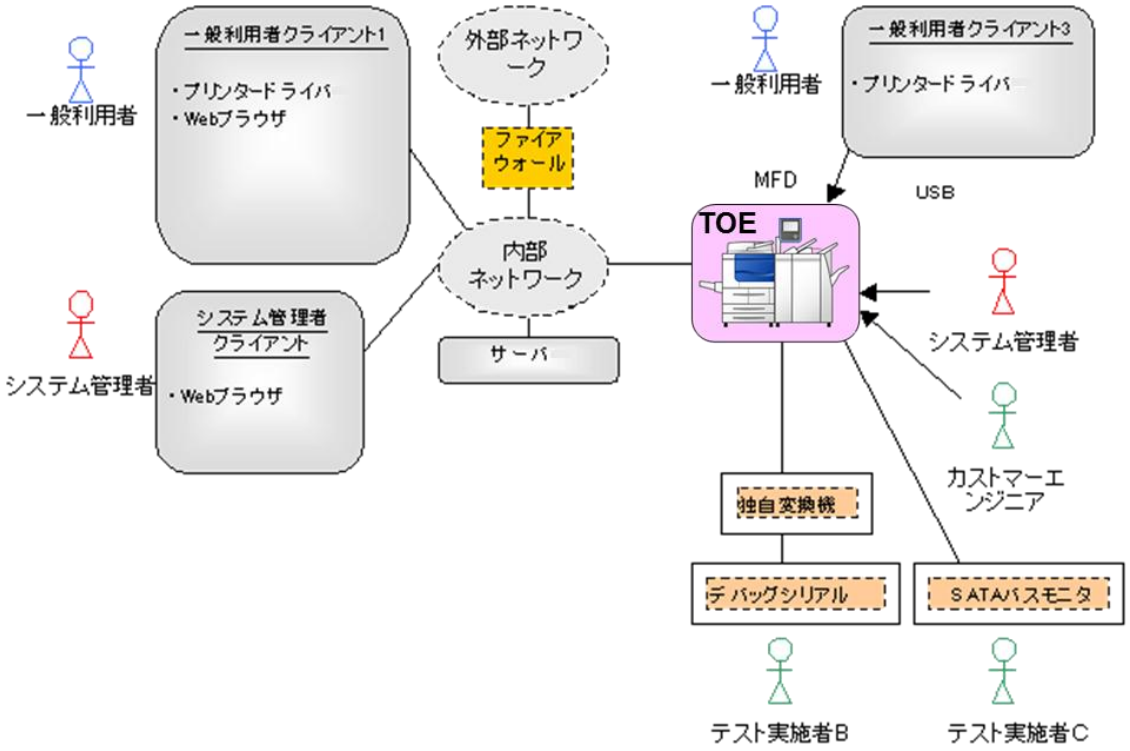

図7-1　開発者テストの構成図

開発者がテストした TOE は、Xerox D125 Copier/Printer であり、2 章の TOE 識別と同一の識別を持つ。他機種は、印刷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。

TOE である MFD 以外の構成要素を表 7-1 に示す。

表7-1　開発者テストの構成要素

名称	詳細
サーバ	Mailサーバ、LDAPサーバ、Kerberosサーバとして使用 ・Microsoft Windows Server 2008 SP2 搭載PC ・Mailサーバ： Xmail Version 1.27 ・LDAP、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3機種を使用 a) Microsoft Windows 7 Professional 搭載PC Webブラウザ：Microsoft Internet Explorer 8 b) Microsoft Windows XP Professional SP3 搭載PC Webブラウザ：Microsoft Internet Explorer 6 c) Microsoft Windows VISTA Business SP2 搭載PC Webブラウザ：Microsoft 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機種を使用 a) Microsoft Windows 7 Professional 搭載PC Webブラウザ：Microsoft Internet Explorer 8 b) Microsoft Windows XP Professional SP3 搭載PC Webブラウザ：Microsoft Internet Explorer 6 c) Microsoft Windows VISTA Business SP2 搭載PC Webブラウザ：Microsoft Internet Explorer 7 さらに、上記のa) b) c)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：PCL6 5.254.0.0.0.0.1 ・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3	一般利用者クライアント（プリンター用のUSBポート経由の接続）として使用 ・Microsoft Windows XP Professional SP3 搭載PC ・プリンタードライバ：PCL6 5.254.0.0.0.0.1
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 ST2-32-2-A）を接続したWindows XP搭載PC ・専用ソフトウェア：Serial ATA Analyzer V1.984.0401
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 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

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。また、FTP通信機能については別途独立して確認がされ動作に問題がないことを、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。

＜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 1.4.6)	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、SSL/TLS、SNMPv3であることを確認する。
メーラー (Microsoft Windows メール)	TOEとメールサーバを介して、電子メールを送受信し、S/MIMEによる暗号化と署名が仕様通りであることを確認する。
デバッグシリアル＋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。

＜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65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。深さ分析によって、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。

7.3.2 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同じである。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、親展ボックス及びプライベート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、50 項目のサンプリングテストと、8 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。

7.3.3 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、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。
⑥ 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＞

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の詳細を表 7-4 に示す。

表7-4　侵入テストツール

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。
	Zenmap+Nmap Ver.5.51	利用可能なネットワークサービスポートを検出するツール（ZenmapはポートスキャンツールNmapのGUIを提供）。
	Fiddler2 V2.3.4.3	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ツール。Fiddler2を使用することにより、Webブラウザの制約を受けずに、任意のデータをWebサーバに送信することができる。
	ContentsBridge Version 7.2.0	富士ゼロックス社製のPC用のプリントソフト。

＜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。
脆弱性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。
脆弱性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。

脆弱性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。
脆弱性⑥	・電源投入後の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。

7.4 評価構成について

本評価の前提となる TOE の構成条件はガイダンス「Xerox D95/D110/D125 Copier/Printer Security Function Supplementary Guide」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、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。

TOE の設定値の中には、セキュリティ機能を有効にするための設定の他に、以下のような設定も含まれている。

- カスタマーエンジニア操作制限機能：[有効]
- 蓄積プリント機能：[プライベートプリントに保存]
- 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]

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。

また、本 TOE には、別売のオプションである「USB プリント／保存」機能は含まれていない。本 TOE に「USB プリント／保存」のオプションを追加した構成は、本評価による保証の対象ではない。

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-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。

7.6 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。

認証機関は、これらの認証において問題点がないことを確認し、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 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「7.4 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。

本 TOE のコピー機能やプリント機能では、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調達者にとっては、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。

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。管理者は、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。

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 D110/D125 Copier/Printer セキュリティターゲット, Version 1.1.7, 2012 年 7 月 18 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	Center Ware Internet Service（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。

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 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
User Document Data（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の総称

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(指示書)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
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
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、スキャナー機能等のMFD基本機能の使用を許可された利用者
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
カストマーエンジニア	MFDの修理／保守を行うエンジニア
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。また、再出力用のデータを親展ボックスに保存することもできる（これを「コピー蓄積」という）。コピー蓄積された文書データは、操作パネルから編集や印刷ができる
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
ジョブフロー	スキャナー機能で読み込まれた文書データに対して、FTPサーバ、Mailサーバ、SMBサーバへの送信や、印刷の処理を、あらかじめ機器に設定したとおりに実行する機能
ジョブフロー(指示書)	ジョブフローのための設定。文書データの配信方法や配信先などの一連の処理の流れ(手順)を、あらかじめ機器に設定したもの
親展ボックス	スキャナー機能やコピー機能(コピー蓄積)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で原稿を読み取り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ブラウザを使用して取り出すことができる
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を操作するためのインタフェース機能
蓄積プリント	印刷データを一時的にMFDの内部ハードディスク装置に蓄積し、一般利用者が操作パネルから印刷指示をした時に印刷を行う。「プリンター機能」の説明参照
通常プリント	印刷データをMFDが受信するとすぐに印刷を行う。「プリンター機能」の説明参照

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、SMBサーバに送信する機能
プライベートプリント	一般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
プリンター機能	一般利用者が、一般利用者クライアントのプリンタードライバやWebブラウザ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。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

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24年3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24年3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24年3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 D110/D125 Copier/Printer セキュリティターゲット, Version 1.1.7, 2012年7月18日, 富士ゼロックス株式会社

[13] Xerox D110/D125 Copier/Printer 評価報告書, 第1.8版, 2012年7月18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