認 証 報 告 書

東京都文京区本駒込2丁目28番8号
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

IT製品（TOE）

申請受付日（受付番号）	平成29年10月6日（IT認証7653）
認証識別	JISEC-C0602
製品名称	LX-10000F/LX-7000F/WF-C20590/WF-C17590
バージョン及びリリース番号	2.00
製品製造者	セイコーエプソン株式会社
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
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
ITセキュリティ評価機関の名称	みずほ情報総研株式会社 情報セキュリティ評価室

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6月15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 Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

評価結果：合格

「LX-10000F/LX-7000F/WF-C20590/WF-C17590」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、セイコーエプソン株式会社が開発した「LX-10000F/LX-7000F/WF-C20590/WF-C17590　バージョン 2.00」（以下「本TOE」という。）について、みずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」という。）が平成 30 年 5 月に完了した 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セイコーエプソン株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、10 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を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、プリント機能、スキャン機能、コピー機能、FAX 機能を有するデジタル複合機（以下「MFP」という。）である。

本 TOE は、MFP 用の Protection Profile である U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) [14][15]（以下、「適合 PP」という。）で要求されるセキュリティ機能、及び TOE が運用される組織が要求するセキュリティ方針を実現するための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 が扱う文書やセキュリティ機能に関する設定情報等の保護資産に対して、TOE への不正アクセスやネットワーク上の通信データへの不正アクセスによる、暴露や改ざんの脅威が存在する。

本 TOE では、それら保護資産に対する不正な暴露や改ざんを防止するため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

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 では、保守員が製品保守のために使用する「メンテナンス・サービス機能」を無効化して運用することが前提となる。この設定を変更して運用された場合、それ以降は本評価における保証の対象外となる。

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」[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 5 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。

認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	LX-10000F/LX-7000F/WF-C20590/WF-C17590
バージョン：	2.00
開発者：	セイコーエプソン株式会社

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 TOE 名称及び TOE バージョンが上記 TOE 名称及び TOE バージョンと同一であることを確認した上で、ガイダンスの指示に従い TOE 名称及びファームウェアのバージョンが記載されるステータスシートを印刷し、そのステータスシートの内容と、ガイダンスに記載された構成要素のバージョンの当該記載と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 であることを確認できる。

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、MFP 内部に格納された文書データ等の保護資産に対する不正なアクセスに対抗するためのセキュリティ機能、及びネットワーク上の通信データを保護するためのセキュリティ機能を提供する。

また、上記セキュリティ機能に関する各種設定を管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

本 TOE の利用において想定される利用者役割を以下に示す。

・一般利用者
TOE が提供する基本機能の使用を許可された利用者。

・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利用者。

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ユーザの文書データやジョブに関連する情報。

・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、ログインパスワード、外部サーバーへアクセスするためのパスワード、監査ログ等が該当する。

・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、利用者のユーザ ID、利用者権限情報、時刻設定情報、ネットワーク設定情報等が該当する。

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、適合 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。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 脅威「T.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらは利用者データ（User Document Data と User Function Data）に対する脅威であり、TOE は、「ユーザ識別・認証機能」、「TOE 機能アクセス制御機能」、「利用者データアクセス制御機能」、「残存データ消去機能」及び「ネットワーク保護機能」で対抗する。

「ユーザ識別・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。

「TOE 機能アクセス制御機能」、「利用者データアクセス制御機能」は、識別認証された利用者が、プリント機能、スキャン機能、コピー機能、FAX 機能等の MFP

の基本機能を使用する際に、利用者に付与された権限をチェックし、権限のある利用者だけに機能の使用を許可すると共に、その際に操作対象となる文書データに対するアクセス制御も行い、アクセス権限のある利用者だけに、その文書データに対するアクセスを許可する。

「残存データ消去機能」は、削除された文書及び一時的に保存された文書を HDD 等の記憶装置から上書き消去し、残存情報への不正アクセスを防ぐ。

「ネットワーク保護機能」は、TOE と各種サーバーやクライアント PC と通信する際に暗号化通信機能を提供し、通信データを保護する。

以上の機能により、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、保護対象の利用者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。

(2) 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で使用されるデータ（TSF Confidential Data と TSF Protected Data）に対する脅威であり、TOE は、「ユーザ識別・認証機能」、「セキュリティ管理機能」及び「ネットワーク保護機能」で対抗する。

「ユーザ識別・認証機能」と「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に対する、利用者の権限を越えた不正なアクセスを防ぐため、利用者の役割によってこれらデータに対するアクセス制御を行う。

「ネットワーク保護機能」は、TOE と各種サーバーやクライアント PC と通信する際に暗号化通信機能を提供し、通信データを保護する。

以上の機能により、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、保護対象の利用者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。これらの組織のセキュリティ方針は、適合 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.AUDT.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、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。

(1) 組織のセキュリティ方針「P.USER.AUTHORIZATION」への対応

TOE は、「ユーザ識別・認証機能」及び「TOE 機能アクセス制御機能」で本方針を実現する。

「ユーザ識別・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。

「TOE 機能アクセス制御機能」は、識別認証された利用者が、プリント機能、スキャン機能、コピー機能、FAX 機能等の MFP の基本機能を使用する際に、利用者に付与された権限をチェックし、権限のある利用者だけに機能の使用を許可する。

(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。

「自己テスト機能」は、MFP の起動時にセキュリティ機能の実行コードの完全性を検証する。

(3) 組織のセキュリティ方針「P.AUDT.LOGGING」への対応

TOE は、「監査ログ機能」で本方針を実現する。

「監査ログ機能」は、セキュリティ機能に関連する事象を監査ログとして記録する。TOE に格納された監査ログは、識別認証された管理者だけが、読み出しを行うことができる。

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

TOE は、「ユーザ識別・認証機能」及び「ネットワーク保護機能」で本方針を実現する。

「ユーザ識別・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、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。

「ネットワーク保護機能」は、有線 LAN と電話回線との間でのデータ転送を制限する機能を提供し、不正なデータ転送を防ぐ。

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、適合 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

本 TOE はオフィスに設置され、LAN に接続し、同様に LAN 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。

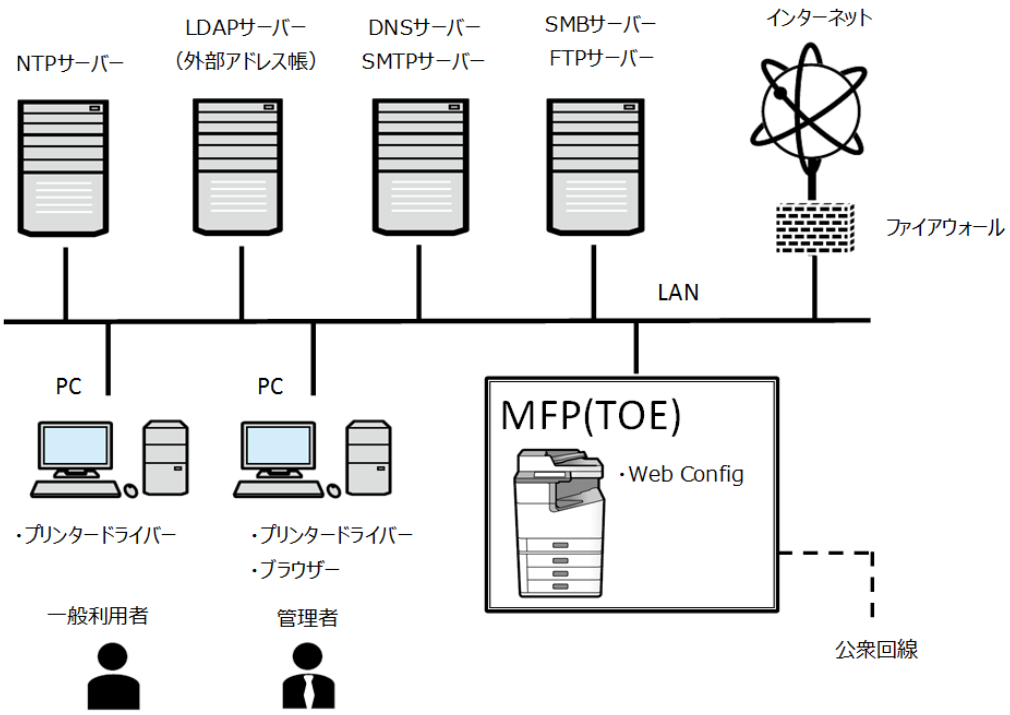

図 4-1 TOEの運用環境

TOE は、図 4-1 に示すようなオフィス等の書類を扱う環境において使用されることを想定している。TOE には LAN 及び公衆回線が接続される。

LAN には LDAP サーバー、SMB サーバー、FTP サーバー等の各種サーバーコンピューターが接続され、TOE と文書、各種情報収集等の通信を行う。また、インターネット等の外部ネットワークの脅威から LAN 及び TOE を保護するためにファイアウォールが設置される。表 4-2 に本評価で使用したサーバーソフトウェアを示す。

TOE の操作は、TOE 自身の操作パネルを使用する場合と、LAN に接続されたクライアント PC を使用する場合とがある。クライアント PC には表 4-3 に示すソフトウェアがインストールされる。

なお、本構成に示されている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）。

表 4-2　本評価で使用したサーバーソフトウェア

ソフトウェア	名称及びバージョン
DNSサーバー	Microsoft Windows Server 2012 R2 Standard
FTPサーバー	Microsoft Windows Server 2012 R2 Standard
LDAPサーバー	Microsoft Windows Server 2012 R2 Standard
NTPサーバー	Microsoft Windows Server 2012 R2 Standard
SMBサーバー	Microsoft Windows Server 2012 R2 Standard
SMTPサーバー	hMailServer 5.6.6-B2383

表 4-3　クライアントPCのソフトウェア

ソフトウェア	名称及びバージョン
プリンタードライバー	Microsoft Windows用 Epson Printing System Version 2.67.00
ブラウザー	Internet Explorer 11

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) 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（サブシステム）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。

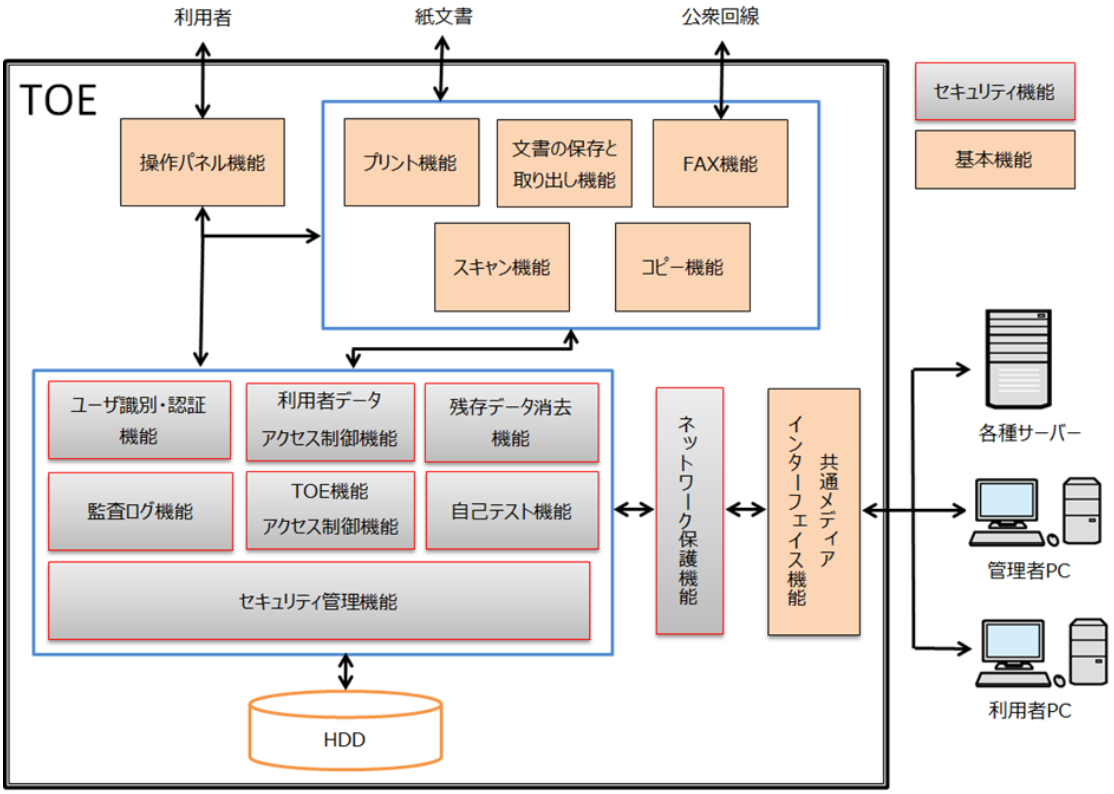

図 5-1 TOEの構成

TOE の機能は、セキュリティ機能と、それ以外の MFP 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。MFP の基本機能については用語説明を参照のこと。

(1) ユーザ識別・認証機能

本機能は、入力されたユーザID及びパスワードがTOE内部で管理されているユーザID及びパスワードと一致することを確認することにより、利用者を識別認証する機能である。本機能は以下の操作時に適用される。

・操作パネルからのログイン時

・クライアントPCからの管理者ログイン時（Web Configの使用）
・クライアントPCからの印刷ジョブ送信時

また、必要な認証強度を確保するために、以下の機能を提供する。

・認証に失敗すると一定時間当該アカウントをロック状態にする
・パスワードについてはその長さ（桁数）、文字種別に関して一定品質以上のものが設定時に要求される
・ログイン後、一定時間操作がない場合には、セッションを終了する

パスワードの正当性が確認された場合、その利用者の役割毎に予め規定されたTOEの利用権限が与えられ、TOEの利用が許可される。TOEが特定する役割は、一般利用者、管理者である。

(2) TOE 機能アクセス制御機能

本機能は、プリント、スキャン、コピー、FAXといったMFPの基本機能の使用を制限する機能である。

利用者がMFPの基本機能を使用する際に、利用者毎に設定された基本機能の利用権限を参照し、当該機能の操作の可否が決定される。

(3) 利用者データアクセス制御機能

本機能は、利用者からの処理要求に対して、その利用者のユーザID 、役割毎の権限を元に文書データ及びジョブに対するアクセス制御を実施する。ネットワーク経由で投入されたプリントジョブやTOEに保存された文書データには、その操作を実施した利用者のユーザIDが関連付けられており、利用者からの処理要求時にその利用者のユーザIDと操作権限から、許可もしくは拒否の制御を行う。利用者が管理者である場合は、全ての文書データ及びジョブの削除が許可される。

(4) 残存データ消去機能

本機能は、削除された文書及び一時的に保存された文書を、格納領域であるHDD等のデバイスから完全に消去するため特定の値（0x00）で上書きし、残存するデータへのアクセスを不可能にする機能である。

(5) ネットワーク保護機能

本機能は、TOEが外部との通信を行う際に通信データの保護等を行う目的で、下記2つの機能を提供する。

・TOEがLANを経由して各種サーバー及びクライアントPCと通信する際に、暗号通信プロトコルであるIPsecを適用し、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。

・有線LANと電話回線との間でのデータ転送を制限する機能を提供し、不正なデータ転送を防ぐ。

(6) セキュリティ管理機能

本機能は、利用者情報や各種設定情報等のセキュリティ機能で使用されるデータに対して、利用者の役割に応じたアクセス制御を行うことにより、権限を越えた不正なアクセスを防ぐための機能である。

(7) 自己テスト機能

本機能は、TOEの本体起動時にファームウェアのハッシュ値検証を行い、セキュリティ機能の実行コードの完全性を検証する機能である。

(8) 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、識別認証された管理者だけがクライアントPCへのダウンロードを行うことができる。監査ログの改変はできない。

5.2 IT環境

TOE は、LAN に接続され、FTP サーバー、SMB サーバー、LDAP サーバー等のサーバーコンピューター及びクライアント PC と通信を行う。また TOE は、電話回線で接続された送信先のファクス装置とも通信を行う。

LAN を経由して接続されたクライアント PC は、プリンタードライバーや、ブラウザーを介して TOE を利用する。

これら TOE の運用に必要なサーバーコンピューターやクライアント PC は利用者の責任において用意されなければならない。

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。

（日本語版）

名称	バージョン
ユーザーズガイド	NPD5875-00 JA
システム管理者ガイド	NPD5680-01 JA
セキュリティー機能補足ガイド	NPD5895-00 JA
ご使用の前に	4135818-00

（英語版）

名称	バージョン
User's Guide	NPD5875-00 EN
Administrator's Guide	NPD5680-01 EN
Supplemental Security Guide	NPD5895-00 EN
Before Use	4135818-00

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、みずほ情報総研株式会社 情報セキュリティ評価室は、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 29 年 10 月に始まり、平成 30 年 5 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 30 年 2 月に開発現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 30 年 2 月及び 3 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。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

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

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に、主な構成要素を表 7-1 に示す。

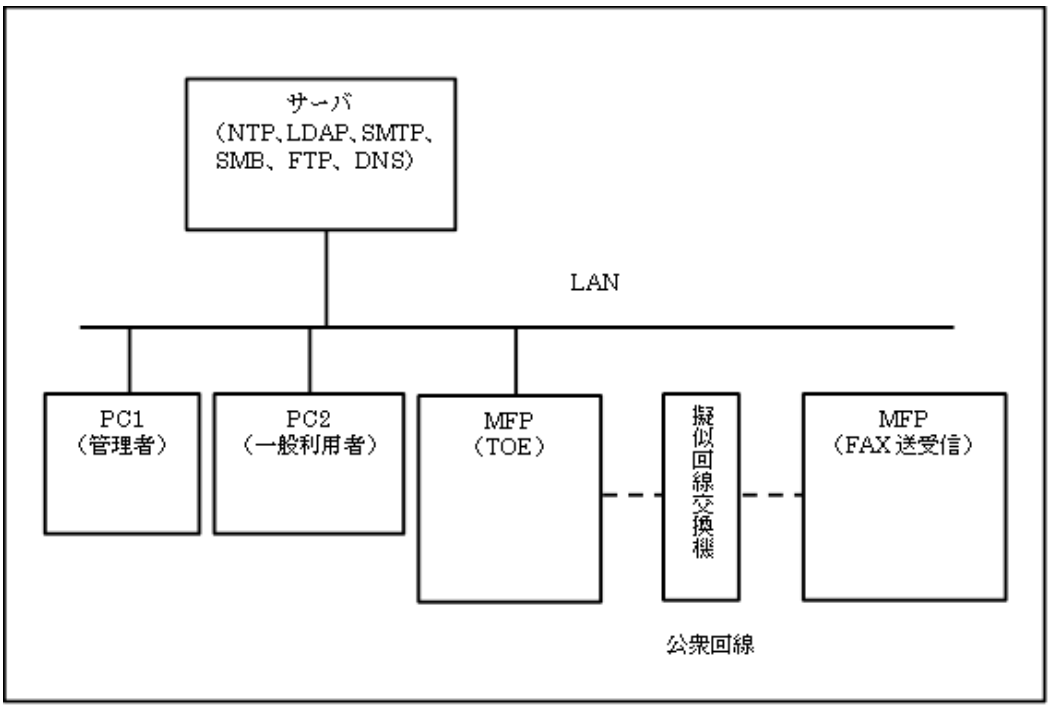

図 7-1 開発者テストの構成図

表 7-1　テスト構成要素

構成要素	詳細
TOE	LX-10000F　Version 2.00 LX-7000F　Version 2.00 WF-C20590　Version 2.00 WF-C17590　Version 2.00
NTPサーバー	Microsoft Windows Server 2012 R2 Standard
LDAPサーバー	Microsoft Windows Server 2012 R2 Standard （アドレス帳を管理し、FAXデータの宛先指定時に使用）
SMBサーバー、FTPサーバー	Microsoft Windows Server 2012 R2 Standard
DNSサーバー	Microsoft Windows Server 2012 R2 Standard
SMTPサーバー	hMailServer 5.6.6-B2383
MFP（FAX対向機）	EW-M5071FT
擬似回線交換機	EXCEL-N008（ニシヤマ）
クライアントPC1、2	OS: Windows7 ブラウザー: Internet Explorer 11 プリンタードライバー: Epson Printing system Version 2.67.00

開発者テストは本 ST において識別されている TOE 構成と同一の TOE テスト環境で実施された。

(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＞

開発者テストは通常の TOE の使用において想定される外部インタフェース（操作パネル、LAN インタフェース等）を刺激し、結果を目視観察する方法の他、生成された監査ログ、及び開発用インタフェースを用いた内部状態の確認、パケットキャプチャによるクライアント PC、及び各種サーバーと TOE 間の通信プロトコルの確認等も行われている。

＜開発者テストの実施＞

開発者が提供したテスト仕様書に記載された期待されるテスト結果の値と、同じく開発者が提供したテスト結果報告書に記載された開発者テストの結果の値を比較した。その結果、期待されるテスト結果の値と実際のテスト結果の値が一致していることが確認された。

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41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ルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

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

・TOE として ST に識別された MFP の一部の機種（LX-10000F、WF-C17590）を使用

評価者は、TOE 機種の違いは印刷速度等であり、これらの差異を考慮した上記 2 機種のテストで十分であると判断している。

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。

⑵ 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 入力パラメタの種類が多く、網羅性の観点で開発者テストが不足していると思われる操作に関して、パラメタの組み合わせ等のバリエーションを追加する。

② 複数の TSF の実行タイミング、実行の組み合わせに関して条件を追加したテスト項目を実施する。

③ サンプリングテストにおいては下記観点からテスト項目を選択する。

- 網羅性の観点から、全ての TSF、TSFI が含まれるように項目を選択する。
- 異なるテスト手法、テスト環境を網羅するように項目を選択する。
- 多くの SFR が対応付けられ、効率よくテストが実施できる TSFI に関する項目を重点的に選択する。

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。

＜独立テストの実施内容＞

独立テストの観点に基づき、独立テスト 6 件、サンプリングテスト 29 件のテストが実施された。

実施された主な独立テストの概要と、対応する独立テストの観点を表 7-2 に示す。

表 7-2 実施した独立テスト

独立テストの観点	テスト概要
①	・パスワード設定時の品質チェックが仕様通り実施されることを、入力するパスワードのバリエーションを増やして確認する。

	・外部との通信プロトコルの設定パラメタを変更し、仕様通りの挙動になること確認する。
②	・ログイン中のアカウント削除、権限変更時のふるまいが仕様通りであることを確認する。 ・複数インタフェースからの操作に対して仕様通りのアクセス制御が行われることを確認する。

c) **結果**

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

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 意図しないネットワークポートインタフェースが存在し、そこから TOE にアクセスできる可能性がある。
② インタフェースに対して TOE が意図しない値、形式のデータ入力が行われた場合、セキュリティ機能がバイパスされる可能性がある。
③ 過負荷状態で TOE を運用することにより、セキュリティ機能がバイパスされる可能性がある。
④ 想定外のタイミングで電源 OFF 操作をすることにより、セキュリティ機能の正しい動作が侵害される可能性がある。

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＞

侵入テストは図 7-1 に示した開発者テスト及び評価者独立テストと同様の環境で実施された。

侵入テストで使用した主なツールを表 7-3 に示す。

表 7-3　侵入テスト使用ツール

構成品	概要
Nessus Version 7.0.1	脆弱性スキャンツール （脆弱性データベースは2018年2月2日時点、2018年3月6日時点で最新のもの）
Nikto Version 2.1.5	Web用の脆弱性スキャンツール （脆弱性データベースは2018年2月2日時点、2018年3月6日時点で最新のもの）
Tamper IE Version 1.0.1.13	プロキシ型のWeb脆弱性検査ツール
Burp Suite Version 1.7.23	プロキシ型のWeb脆弱性検査ツール
ZAP Version 2.7.0	プロキシ型のWeb脆弱性検査ツール （脆弱性データベースは2018年2月2日時点、2018年3月6日時点で最新のもの）
nmap Version 7.60	ポートスキャンツール
PRET Version 0.40	PJL、Postscriptテストツール

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-4 に示す。

表 7-4　侵入テスト概要

脆弱性	テスト概要
①	ポートスキャンツール、脆弱性スキャンツールを使用し、想定しないネットワークポートが開いていないことを確認する。また使用可能なポートについても不正入力に対する脆弱性が存在しないことを確認する。
②	脆弱性検査ツールを使用してTOEへのアクセスを行うWebインタフェースに公知の脆弱性が存在しないことを確認する。

	Webブラウザー経由でのTOEへの接続時に指定するURLによりセキュリティ機能がバイパスされないことを確認する。 PJL、PostScriptに関して実装上の脆弱性がないことをテストツールを使用して確認する。
③	リソース枯渇状態においてTOEが非セキュアな状態にならないことを確認する。
④	TOE起動処理中などの通常運用時とは異なる状況で電源操作を行い、TOEが非セキュアな状態にならないことを確認する。

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。

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。

・ PP 適合：

U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-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。

- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
- 2600.2-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment B
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

・ 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。

・ EAL2 パッケージのすべての保証コンポーネント

・ 追加の保証コンポーネント　ALC_FLR.2

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

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL2 及び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

保守員が製品保守のために使用する「メンテナンス・サービス機能」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。

また本 TOE の利用者は、「4.2 運用環境と構成」及び「7.5 評価構成について」を参照し、本 TOE の評価対象範囲や運用上の要求事項が実際の TOE 運用環境において対応可能かどうかについて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提供される。

LX-10000F/LX-7000F/WF-C20590/WF-C17590 セキュリティターゲット
Rev.10　2018 年 05 月 15 日　セイコーエプソン株式会社

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。

HDD	Hard Disk Drive: MFP内に搭載された記憶装置
MFP	Multi Function Peripheral: デジタル複合機

本報告書で使用された用語の定義を以下に示す。

FTPサーバー	FTP（File Transfer Protocol）を利用してファイル送受信を行うためのサーバー。 TOEがスキャン機能を使用して作成したスキャンデータ及びFAX受信データの転送用に使用する。
LDAPサーバー	LDAP（Light Directory Access Protocol）を利用してディレクトリサービスを提供するサーバー。 本TOEでは、LDAPサーバで管理されるアドレス帳を参照し、FAXの送信宛先に利用する。
MFP基本機能	MFPとしての基本的な機能であり、下記機能により構成される。 プリント機能（クライアントPCから受信した文書データの印刷）、スキャン機能、コピー機能、FAX機能、文書の保存と取り出し機能（FAX機能で送受信するデジタル文書を保存したり取り出したりする機能）
SMBサーバー	SMB（Server Message Block）を利用してファイル共有、プリンター共有などを行うためのサーバー。 TOEがスキャン機能を使用して作成したスキャンデータ及びFAX受信データの転送用に使用する。

SMTPサーバー	SMTP（Simple Mail Transfer Protocol）を利用して電子メールを伝送するためのサーバー。 TOEがスキャン機能を使用して作成したスキャンデータをメール送信する際に使用する。
Web Config	ブラウザー経由にてアクセスすることにより、各種設定（プリント設定、ネットワーク設定、利用者制限設定、管理者パスワード設定等）を行うMFP内蔵機能。

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] LX-10000F/LX-7000F/WF-C20590/WF-C17590 セキュリティターゲット, Rev. 10, 2018年05月15日, セイコーエプソン株式会社

[13] LX-10000F/LX-7000F/WF-C20590/WF-C17590評価報告書, 第2版, 2018年5月22日, みずほ情報総研株式会社 情報セキュリティ評価室

[14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

[15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership