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　齊藤　裕

原紙押印済

IT製品（TOE）

申請受付日（受付番号）	令和5年11月27日（IT認証3869）
認証識別	JISEC-C0810
製品名称	RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370
バージョン及びリリース番号	E-1.00
製品製造者	株式会社リコー
機能要件適合	製品独自セキュリティターゲット、CCパート2拡張
保証パッケージ	EAL2
ITセキュリティ評価機関の名称	株式会社 ECSEC Laboratory 評価センター

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。

令和6年3月26日

セキュリティセンター セキュリティ技術評価部
技術管理者　矢野 達朗

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5
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5

評価結果：合格

「RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370 バージョン E-1.00」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、株式会社リコーが開発した「RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370 バージョン E-1.00」（以下「本 TOE」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 6 年 3 月 15 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株式会社リコー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 プロテクションプロファイルまたは保証パッケージ

本 TOE の保証パッケージは、EAL2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、スキャナー機能及びドキュメントボックス機能を提供するデジタル複合機（以下「MFP」という。）である。ファクス機能は提供していない。

本TOEは、MFPの扱う文書データやセキュリティに影響する設定情報等が暴露されたり改ざんされたりすることを防止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いる。

TOEが扱う文書データ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。

それらの脅威に対抗するために、本TOEは、識別認証、アクセス制御、暗号化などのセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

本 TOE は、次のような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、以下の運用を保証していない。

- 「4.2 運用環境と構成」の記載と異なる運用環境や構成
- 「7.5 評価構成について」の記載と異なる設定の TOE

1.2 評価の実施

認証機関が運営するITセキュリティ評価及び認証制度に基づき、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、令和6年3月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]及び関連する評価証拠資料を検証し、本TOEの評価が所定の手続きに沿って行われたことを確認した。また、TOEの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： RICOH IM 370,
nashuatec IM 370,
Rex Rotary IM 370,
Gestetner IM 370
バージョン： E-1.00
開発者： 株式会社リコー

本 TOE は、MFP 本体のみで構成される。TOE の構成品を表 2-1 に示す。

表2-1 TOEの構成品

MFP本体	
製品名	機種コード
IM 370	D0DM-27

また、TOE のバージョンは、TOE 内部の複数のソフトウェアのバージョンの組合せである。TOE のバージョンの内訳は、ST の 1.2 章を参照。

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

- 製品外装に記載された製品名と機種コードが、表2-1の製品名と機種コードと一致することを確認する。
- 製品のガイダンスの記載に従って操作し、製品の操作パネルに表示されたソフトウェアの名称とバージョンと部番が、ST の1.2章の記載と一致することを確認する。

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。

本 TOE は、MFP の基本機能としてコピー機能、プリンター機能、スキャナー機能及びドキュメントボックス機能を提供しており、利用者の文書データを TOE 内部に保存したり、ネットワークを介して利用者の端末や各種サーバーとやりとりしたりする機能を持つ。

本TOEは、TOEの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保護するためのセキュリティ機能を提供する。

本TOEの利用者を表3-1に示す。TOEの利用者は一般利用者と管理者に分類され、さらに、管理者はMFP管理者とスーパーバイザーに分類される。

表3-1　TOE利用者

利用者定義		説明
一般利用者		TOEの基本機能の使用を許可された利用者。
管理者	MFP管理者	TOEの管理を許可された利用者。
	スーパーバイザー	MFP管理者のログインパスワードを変更する権限と、MFP管理者のロックアウト状態を解除する権限を持つ利用者。

本TOEの保護資産を表3-2及び表3-3に示す。

表3-2　TOE保護資産（利用者データ）

分類	定義
文書データ	電子的またはハードコピーの形式で、利用者の文書に含まれる情報。TOEに保存されたデータとネットワーク通信中のデータが保護の対象である。
利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報

表3-3　TOE保護資産（TSFデータ）

分類	定義
TSF秘密データ	セキュリティ機能で使用されるデータの中で、完全性と機密性が求められるデータ。 本TOEでは、ログインパスワード、監査ログ、eMMC暗号鍵が該当する。

TSF保護データ	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、ログインユーザー名、パスワード最小桁数、アクセス制御に関する設定など、TSF秘密データを除く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

本 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 3-4 に示す脅威を想定し、これに対抗する機能を備える。

表3-4 脅威

識別子	脅 威
T.DOCUMENT_DATA_DIS （文書データの開示）	TOEが管理している文書データが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがその文書データへのアクセス権限を持たない者によって閲覧されるかもしれない。
T.DOCUMENT_DATA_ALT （文書データの改変）	TOEが管理している文書データが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがその文書データへのアクセス権限を持たない者によって改変されるかもしれない。
T.JOB_ALT （利用者ジョブデータの改変）	TOEが管理している利用者ジョブデータが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがその利用者ジョブデータへのアクセス権限を持たない者によって改変されるかもしれない。
T.PROTECT_DATA_ALT （TSF保護データの改変）	TOEが管理しているTSF保護データが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF保護データへのアクセス権限を持たない者によって改変されるかもしれない。
T.CONFIDENTIAL_DATA_DIS （TSF秘密データの開示）	TOEが管理しているTSF秘密データが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF秘密データへのアクセス権限を持たない者によって閲覧されるかもしれない。

T.CONFIDENTIAL_DATA_ALT（TSF秘密データの改変）	TOEが管理しているTSF秘密データが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF秘密データへのアクセス権限を持たない者によって改変されるかもしれない。

※「ログインユーザー名を持つ者」とはTOEの利用を許可された者を表す。

3.1.1.2 脅威に対するセキュリティ機能方針

本TOEは、表3-4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.DOCUMENT_DATA_DIS」「T.DOCUMENT_DATA_ALT」「T.JOB_ALT」への対抗

これらは表3-2の利用者データに対する脅威であり、TOEは、「識別認証機能」、「文書アクセス制御機能」及び「ネットワーク保護機能」で対抗する。

「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。

「文書アクセス制御機能」は、利用者が利用者データを操作する際にアクセス制御を行い、アクセス権限のある利用者だけに、その利用者データに対するアクセスを許可する。

「ネットワーク保護機能」は、TOEがクライアントPCや各種サーバーと通信する際に暗号化通信を行い、通信データを保護する。

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.PROTECT_DATA_ALT」「T.CONFIDENTIAL_DATA_DIS」「T.CONFIDENTIAL_DATA_ALT」への対抗

これらは表3-3のTSFデータに対する脅威であり、TOEは、「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。

「識別認証機能」と「セキュリティ管理機能」は、TSFデータへのアクセスを、権限のある利用者だけに許可する。

「ネットワーク保護機能」は、TOEがクライアントPCや各種サーバーと通信する際に暗号化通信を行い、通信データを保護する。

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 TSF 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 に要求される組織のセキュリティ方針を表 3-5 に示す。

表3-5 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.AUTHORIZATION （利用者の識別認証）	TOE利用の許可を受けた利用者だけがTOEを利用することができるようにしなければならない。
P.VALIDATION （ソフトウェア検証）	TSFの実行コードを自己検証できる手段を持たなければならない。
P.AUDIT （監査ログ記録管理）	運用の説明責任とセキュリティを維持するために、TOEのセキュリティ関連イベントの監査証跡を提供する記録は、作成され、維持され、権限を持たない者からの開示や改ざんから保護され、権限をもつ者によって確認されなければならない。
P.ENCRYPTION （eMMC暗号化）	TOEのeMMCに記録しているデータは、暗号化されていなければならない。

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 3-5 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.AUTHORIZATION」への対応

TOE は、「識別認証機能」で本方針を実現する。

「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。

(2) 組織のセキュリティ方針「P.VALIDATION」への対応

TOE は、「完全性検証機能」で本方針を実現する。

「完全性検証機能」は、TOE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.AUDIT」への対応

TOE は、「監査機能」で本方針を実現する。

「監査機能」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MFP管理者だけが、読み出しと削除を行うことができる。

(4) 組織のセキュリティ方針「P.ENCRYPTION」への対応

TOEは、「蓄積データ保護機能」で本方針を実現する。

「蓄積データ保護機能」は、TOE内部のストレージ（eMMC）に書き込むデータを暗号化する。

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.PHYSICAL_PROTECTION （アクセス管理）	MFP管理者は、ガイダンスに従ってTOEを安全で監視下における場所に設置し、不特定多数の者から物理的にアクセスされる機会を制限しているものとする。
A.NETWORK_PROTECTION （ネットワーク管理）	MFP管理者は、TOEのLANインタフェースが外部から直接アクセスされることから保護される運用環境にTOEを設置するものとする。
A.USER （利用者教育）	MFP管理者は、一般利用者が組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っているものとする。
A.ADMIN （管理者教育）	MFP管理者は組織のセキュリティポリシーやその手順を認識しており、ガイダンスに従ってそれらのポリシーや手順に沿ったTOE の設定や処理ができるものとする。
A.TRUSTED_ADMIN （信頼できる管理者）	管理者には、ガイダンスに従ってその特権を悪用しない者が選任されているものとする。

4.2 運用環境と構成

本 TOE の想定する運用環境を図 4-1 に示す。本 TOE は一般的なオフィスに設置され、ローカルエリアネットワーク（以下「LAN」という。）に接続して使用される。利用者は、本 TOE の操作パネルや LAN に接続されたクライアント PC を操作して本 TOE を使用する。

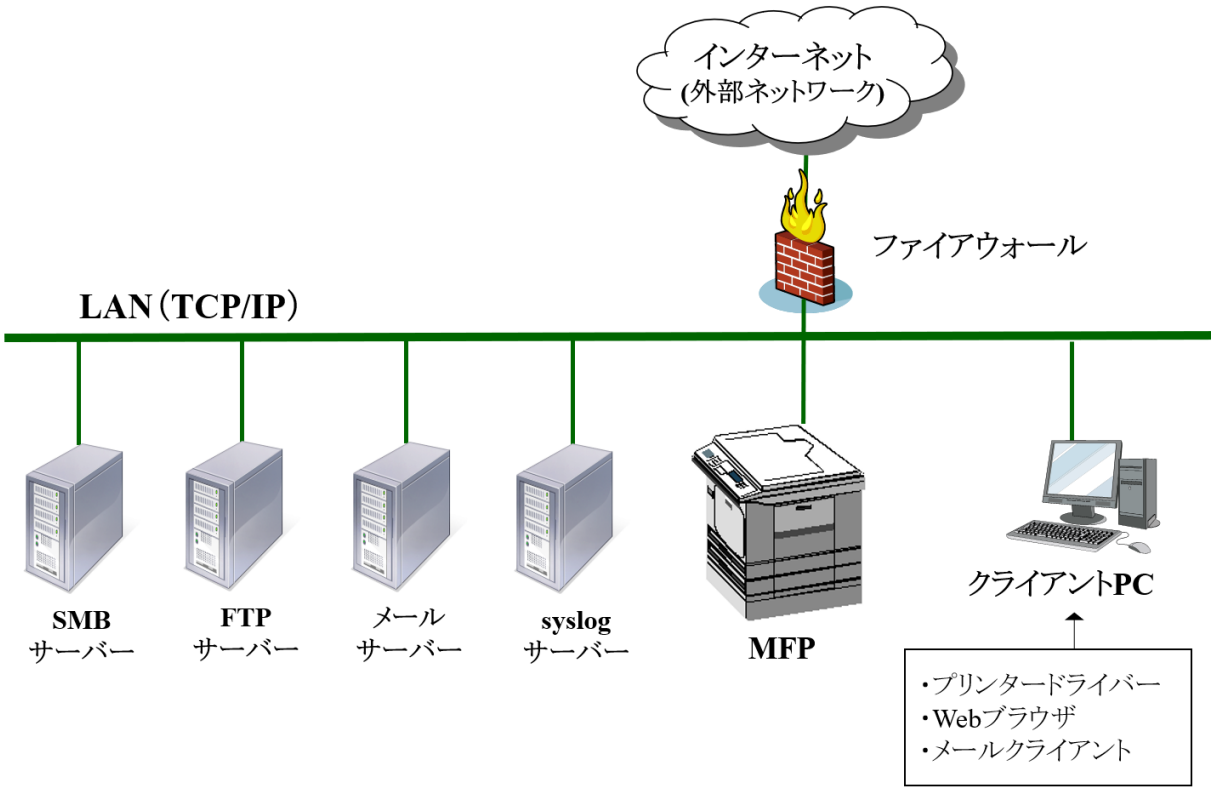

図4-1 TOEの運用環境

本TOEの運用環境の構成品を以下に示す。

(1) クライアントPC

利用者が使用する汎用のPCである。Webブラウザ、S/MIME対応のメールクライアント、リコー提供のPCL6 Driver（バージョン1.1.0.0以降）が必要である。本評価では以下のソフトウェアを使用。

・OS：Windows 10, Windows 11
・Webブラウザ：Microsoft Edge 107
・メールクライアント：Thunderbird 102.6.0
・プリンタードライバー：PCL6 Driver 1.1.0.0

(2) SMBサーバー、FTPサーバー、メールサーバー

TOEでスキャンした文書データを送信する場合に使用するサーバーである。各サーバーは、それぞれ、IPsec及びSMBプロトコル、IPsec及びFTPプロトコル、SMTPプロトコルをサポートするソフトウェアが必要である。本評価では以下のソフトウェアを使用。

(SMBサーバー)

・OS：Windows 10

・SMBソフトウェア：OS付属

(FTPサーバー)

・構成a：

- OS：Windows 10
- FTPソフトウェア：IIS10 V10.0.19041.804

・構成b：

- OS：Linux (Ubuntu 20.04)
- FTPソフトウェア：vsftpd 3.0.3

(メールサーバー)

・OS：Windows 10

・SMTPソフトウェア：P-Mail Server Manager 1.91

(3) syslogサーバー

TOEの生成した監査ログを保存するためのサーバーである。TOEの設定で、監査ログの転送を有効にした場合に使用される。TLS対応のsyslogプロトコルをサポートするソフトウェアが必要である。本評価では以下のソフトウェアを使用。

・OS：Linux(Ubuntu 20.04)

・syslogソフトウェア：rsyslogd 8.2001.0

なお、本構成に示されているTOE以外のハードウェア及びソフトウェアの信頼性は本評価の範囲ではないが、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 の提供する機能、及び、本評価で保証される本 TOE の機能には、以下の制約がある。

(1) 各種サーバー及びクライアント PC

TOE と連携して動作する各種サーバーやクライアント PC がセキュアに運用されることは、それらの機器の管理者の責任である。

(2) 残存情報消去機能

TOE 内部のストレージ（eMMC）に保存されたデータに対して、それらのデータを上書きして消去する残存情報消去機能は、本評価による保証の対象外である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。TOE は MFP 製品全体である。

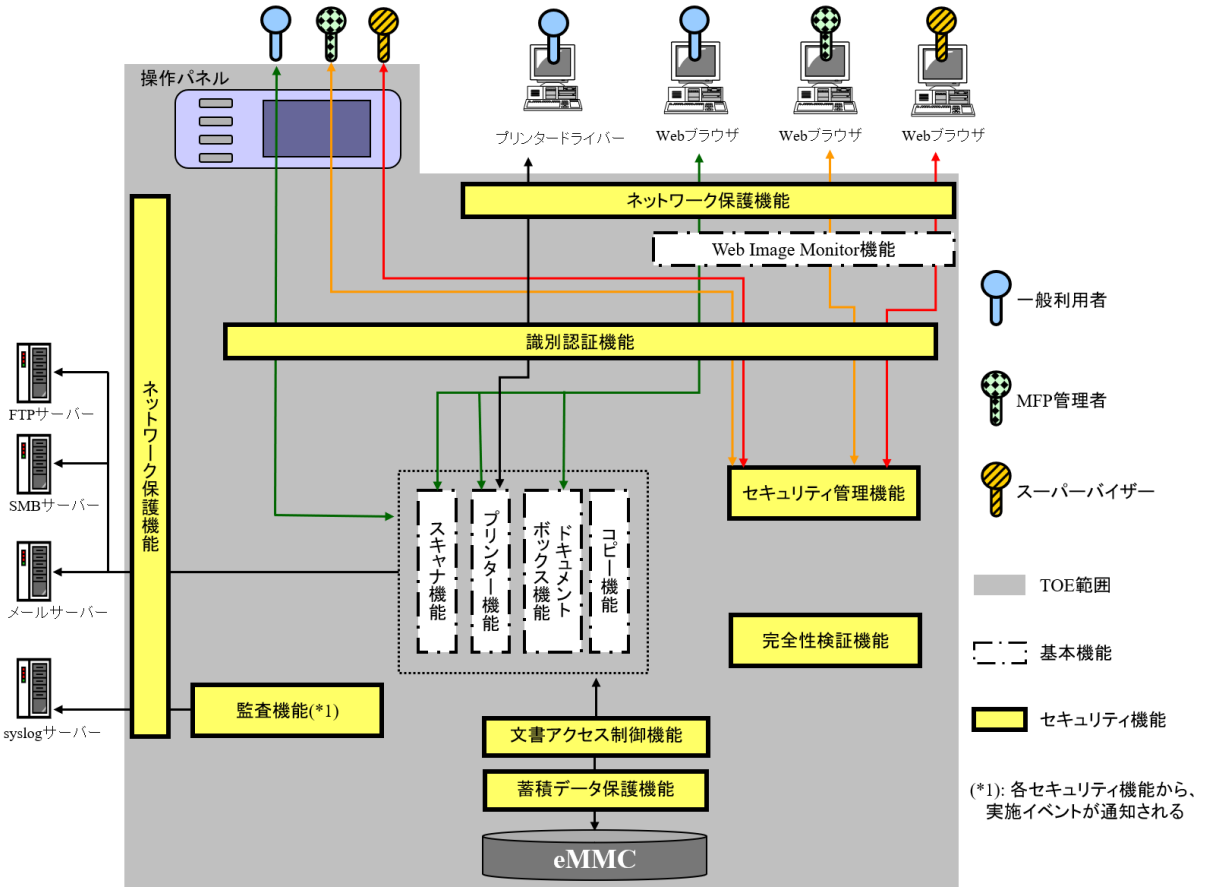

図5-1　TOEの構成

TOE の機能は、セキュリティ機能と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。基本機能については 11 章を参照。

(1) 識別認証機能

本機能は、利用者がTOEの操作パネルやクライアントPC（Webブラウザ、プリンタードライバー）からTOEを使用するときに、ログインユーザー名とログインパスワードで利用者を識別認証する機能である。

また、識別認証を補強するために以下の機能性を提供する。

・連続した認証失敗時のアカウントのロックアウト
・パスワードの最小桁数と必須文字種の要求

・認証成功後、一定時間操作がない場合のセッション切断

(2) 文書アクセス制御機能

本機能は、MFPの基本機能で文書データ及び利用者ジョブデータを操作するときに、それらのデータへのアクセス制御を行う機能である。アクセス制御は、文書データ及び利用者ジョブデータの所有者情報と、利用者の識別情報及び役割に基づいて行われる。

(3) 蓄積データ保護機能

本機能は、TOE内部のストレージ（eMMC）に保存するデータを暗号化する機能である。暗号アルゴリズムは、鍵長256ビットのAESを使用する。

(4) ネットワーク保護機能

本機能は、TOEと各種IT機器との間の通信データを、暗号通信プロトコルで保護する機能である。

(5) セキュリティ管理機能

本機能は、セキュリティ機能の設定等をMFP管理者に制限する機能である。ただし、すべての利用者は本人のログインパスワードの変更が可能であり、スーパーバイザーはMFP管理者のログインパスワードの変更が可能である。

(6) 完全性検証機能

本機能は、TOE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機能である。検証には、TOE内部の各種ソフトウェアのハッシュ値またはデジタル署名を使用する。

(7) 監査機能

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MFP管理者だけが、読み出しと削除を行うことができる。TOEの設定により、監査ログをsyslogサーバーへ転送することもできる。

5.2 IT環境

TOE は、LAN を介して各種サーバーやクライアント PC と通信を行う。TOE のネットワーク保護機能は、それら IT 機器と連携して実現され、以下のプロトコルを使用する。

・クライアント PC（Web ブラウザ）：HTTP over TLS (TLS 1.2, TLS 1.3)
・クライアント PC（プリンタードライバー）：
IPP over TLS (TLS 1.2, TLS 1.3)
・SMB サーバー：IPsec
・FTP サーバー：IPsec
・メールサーバー：S/MIME
・syslog サーバー：Syslog over TLS (TLS 1.2, TLS 1.3)

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表 6-1 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。

表 6-1 製品添付ドキュメント（英語版）

ドキュメント名	バージョン
Safe Use of This Machine	D0E3-7546
Safety Information	D0DM-7310
User Guide IM 370/370F/460F/460FTL	D0DM7314
Security Reference	D0E37534
Notes for Administrators: Using This Machine in a Network Environment Compliant with Common Criteria	D0DM-7318 2023.12.13
Notes on Security Functions	D0DM-7319 2023.09.29
Help	83NHEZ-ENZ1.00 v281

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、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、令和 5 年 11 月に始まり、令和 6 年 3 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、令和 5 年 12 月に、開発現場への訪問により、構成管理のワークユニットの要件の実施状況の調査を行った。製造現場については、配付の検査は省略され、過去の認証案件での評価内容の再利用が可能であると、評価機関によって判断されている。また、令和 5 年 12 月に評価機関及び開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

7.4 製品テスト

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

7.4.1 開発者テスト

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

(1) 開発者テスト環境

開発者が実施したテストの構成を図7-1に、主な構成要素を表7-1に示す。

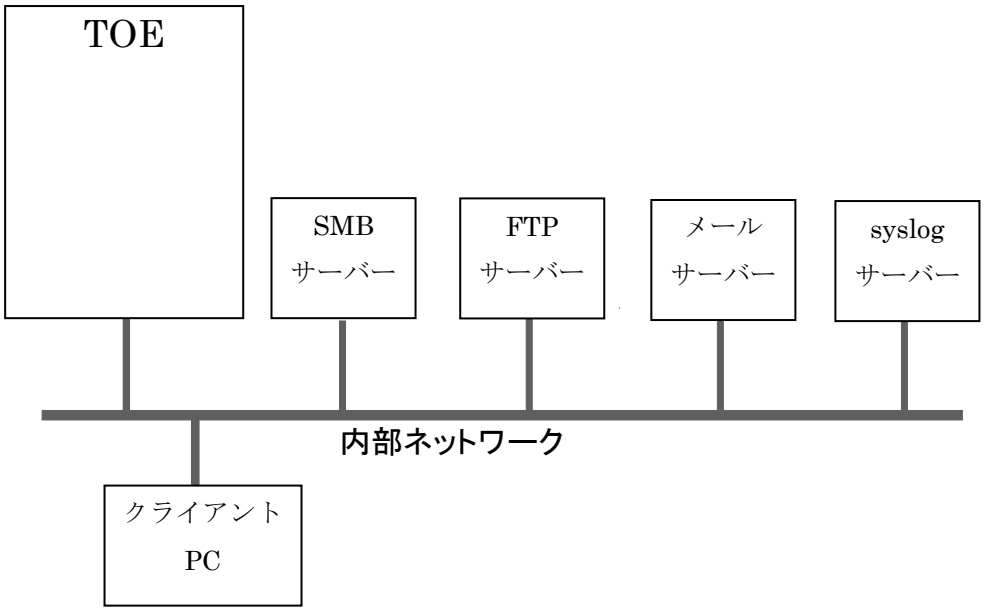

図7-1　開発者テスト構成図

表7-1　テスト構成要素

構成要素	詳細
TOE	・IM 370 E-1.00 (D0DM-27)
クライアントPC	OS：Windows 10, Windows 11 Webブラウザ：Microsoft Edge 107 メールクライアント：Thunderbird 102.6.0 プリンタードライバー：PCL6 Driver 1.1.0.0
SMBサーバー	OS：Windows 10 SMBソフトウェア：OS付属
FTPサーバー	・構成a OS：Windows 10 V10.0.19041.804 FTPソフトウェア：IIS10 (OS付属) ・構成b OS：Linux(Ubuntu 20.04) FTPソフトウェア：vsftpd 3.0.3
メールサーバー	OS：Windows 10 SMTPソフトウェア：P-Mail Server Manager 1.91
syslogサーバー	OS：Linux(Ubuntu 20.04) syslogソフトウェア：rsyslogd 8.2001.0

開発者がテストしたTOEは、TOEの全機種である。なお、ブランド名（RICOH、nashuatec、Rex Rotary、Gestetner）の異なる機種は、販売名称が異なるだけであり、機種コードが同じであれば同一のハードウェアである。

開発者テストは、本STにおいて識別されているTOE構成と一貫する環境で実施された。

(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＞

TOE の操作パネルやクライアント PC を操作して TOE の外部インタフェースを刺激し、その応答、TOE のふるまい、通信データ、監査ログを確認する。TOE の外部インタフェースで確認できないふるまいについては、TOE の開発者用インタフェースを使用して、TOE 内部の動作を確認する。

＜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440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現されてい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現されていることをより確信するための評価者独立テスト（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と同様の構成である。

(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 開発者テストとは異なる入力や操作のバリエーションを確認する。

② 開発者がテストしていない、複数の TSF の実行タイミング、実行の組み合わせを確認する。

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。

-すべてのセキュリティ機能と TSF のインタフェース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。

- 脆弱性評価に寄与する項目を選択する。

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 12 件、サンプリングテスト 33 件のテストが実施された。

独立テストの観点に対応する主な独立テストの内容を表 7-2 に示す。

表7-2 実施した主な独立テスト

独立テストの観点	テスト概要
①	・ユーザーアカウントロック、アクセス制御、パスワード長の制限等が仕様どおりであることを、条件を変更して確認する。 ・無効に設定された機能やインタフェースが、実際に無効になっていることを確認する。 ・有効期限切れの証明書を用いた場合のIPsec及びTLSのふるまいを確認する。
②	・オートログアウトについて、複数のログインやログイン中の設定変更のふるまいが、仕様どおりであることを確認する。 ・複数のインタフェースから同じデータを操作したときのふるまいが、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。

7.4.3 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 想定しない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 セキュアチャネルの実装に脆弱性が存在し、結果としてTOEのセキュリティ機能がバイパスされる可能性がある。

④ 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。

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

名称（バージョン）	概要
ZAP（2.14.0）	プロキシ型のWeb脆弱性検査ツール
nmap（7.92）	ポートスキャンツール
Burp Suite Professional（1.7.37）	プロキシ型のWeb脆弱性検査ツール

Wireshark（3.6.2）	パケットキャプチャツール
PRET（0.40）	印刷処理の様々な脆弱性を検査するツール

＜侵入テストの実施項目＞

懸念される脆弱性に対応する侵入テスト概要を表 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等を使用し、想定外の利用可能なインタフェースが存在しないことを確認する。
②	・Webブラウザやプロキシ型のツールを使用して、TOEの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。 ・印刷処理の検査ツールを使用して、TOEの印刷処理に公知の脆弱性がないことを確認する。 ・TOEの操作パネルに、不正な処理を発生させる可能性のある文字列を入力しても、意図しない動作をしないことを確認する。
③	・TOEのIPsecとTLS処理に、実装上の脆弱性がないことを確認する。 ・Webインタフェースで使用されるパラメタの乱数性検証を行い、容易に推測されないことを確認する。
④	・TOE全機能の同時使用時においてTOEが非セキュアな状態にならないことを確認する。

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 を評価で保証されたとおりに安全に使用するためには、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。ガイダンスと異なる設定にした場合は、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。

・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

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、以下の観点で認証を実施した。

① 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

② 評価報告書に示された評価者の評価判断の根拠が妥当であること。

③ 評価報告書に示された評価者の評価方法がCEMに適合していること。

8.1 認証結果

評価機関より提出された評価報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE の評価が CC パート 3 の EAL2 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、「4.2 運用環境と構成」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価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。

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。

RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370 セキュリティターゲット, バージョン 1.00, 2024 年 2 月 26 日, 株式会社リコー

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）
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。

eMMC	Embedded Multi-Media Card (組み込み用マルチメディアカード)
MFP	Multifunction Product (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。

Web Image Monitor 機能	クライアントPCのWebブラウザからTOEを操作する機能
コピー機能	TOEの操作パネルからの操作で、紙文書をスキャンして複写印刷する機能
スキャナー機能	TOEの操作パネルからの操作で、紙文書をスキャンして外部のサーバーに送信する機能
ドキュメントボックス機能	文書データを蓄積したり、取り出したりする機能
プリンター機能	クライアントPCのプリンタードライバーから送信された利用者文書データを受信し、TOEの操作パネルからの操作で印刷する機能

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和5年12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, 令和5年12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, 令和3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 Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[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5版, 2017年4月, CCMB-2017-04-001 (平成29年7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5版, 2017年4月, CCMB-2017-04-002 (平成29年7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5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[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5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370 セキュリティターゲット, バージョン 1.00, 2024年2月16日, 株式会社リコー

[13] RICOH IM 370, nashuatec IM 370, Rex Rotary IM 370, Gestetner IM 370 評価報告書, 第1.2版, 2024年3月15日, 株式会社 ECSEC Laboratory 評価センター