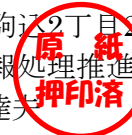




認証報告書

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



IT製品 (TOE)

申請受付日 (受付番号)	令和3年2月24日 (IT認証1778)
認証識別	JISEC-C0730
製品名称	RICOH IM 9000/9000T/8000/7000
バージョン及びリリース番号	J-1.00
製品製造者	株式会社リコー
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	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3年9月17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 9000/9000T/8000/7000 バージョン J-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	1
1.1	評価対象製品概要	1
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	1
1.1.2	TOEとセキュリティ機能性.....	1
1.1.2.1	脅威とセキュリティ対策方針	2
1.1.2.2	構成要件と前提条件.....	2
1.1.3	免責事項	2
1.2	評価の実施.....	3
1.3	評価の認証.....	3
2	TOE識別	4
3	セキュリティ方針	5
3.1	セキュリティ機能方針.....	6
3.1.1	脅威とセキュリティ機能方針.....	6
3.1.1.1	脅威	6
3.1.1.2	脅威に対するセキュリティ機能方針	7
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.....	8
3.1.2.1	組織のセキュリティ方針.....	8
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.....	9
4	前提条件と評価範囲の明確化	11
4.1	使用及び環境に関する前提条件	11
4.2	運用環境と構成.....	11
4.3	運用環境におけるTOE範囲	13
5	アーキテクチャに関する情報	14
5.1	TOE境界とコンポーネント構成.....	14
5.2	IT環境	16
6	製品添付ドキュメント	17
7	評価機関による評価実施及び結果.....	19
7.1	評価機関.....	19
7.2	評価方法.....	19
7.3	評価実施概要	19
7.4	製品テスト	20
7.4.1	開発者テスト	20
7.4.2	評価者独立テスト	22
7.4.3	評価者侵入テスト	24
7.5	評価構成について	27
7.6	評価結果.....	28

7.7	評価者コメント/勧告	28
8	認証実施	29
8.1	認証結果.....	29
8.2	注意事項.....	29
9	附属書.....	30
10	セキュリティターゲット.....	30
11	用語.....	31
12	参照.....	32

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 9000/9000T/8000/7000 バージョン J-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 3 年 9 月 13 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、保証要件及びその充分性の根拠は、ST において詳述されている。

本認証報告書は、市販される本 TOE を購入する一般消費者、及び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 は、次のプロテクションプロファイル[14][15](以下「適合 PP」という。)に適合する。

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

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、コピー機能、スキャナー機能、プリンター機能、ファクス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。

本 TOE は、MFP の扱う文書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に、適合 PP が要求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いる。

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。

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、適合PPが要求する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、ガイドラ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、以下の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。

- ・保守機能への移行
- ・IP-Fax機能、及びInternet Fax機能の使用
- ・ベーシック認証（本体認証時）以外の認証方式の使用

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 3 年 9 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。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： RICOH IM 9000/9000T/8000/7000

バージョン： J-1.00

開発者： 株式会社リコー

本 TOE は、MFP 本体とオプション製品で構成される。TOE の構成品を表 2-1 に示す。

表2-1 TOEの構成品

MFP本体		オプション製品
製品名	機種コード	
RICOH IM 9000	D0D1-00	FAXユニット タイプM44
RICOH IM 9000T	D0D1-01	FAXユニット タイプM44
RICOH IM 8000	D0D0-00	FAXユニット タイプM44
RICOH IM 7000	D0CZ-00	FAXユニット タイプM44

また、TOE のバージョンは、TOE 内部の複数のソフトウェアとハード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。
- ファクスオプションの梱包箱上のラベルシールに記載された名称が、表2-1のファクスユニット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とハード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。

TOEはMFPに蓄積された文書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。

TOEは組織のセキュリティ方針を満たすため、内部の保存データを上書き消去する機能、HDDの記録データを暗号化する機能、及びファクスI/Fを経由した電話回線網からの不正アクセスを防ぐ機能を提供する。

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、管理者はスーパーバイザーとMFP管理者に分類される。

表3-1 TOE利用者

利用者定義		説明
一般利用者		TOEの使用を許可された利用者。ログインユーザー名を付与され通常のMFP機能の利用ができる。
管理者	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を持つ。
	MFP管理者	TOEの管理を許可された利用者。一般利用者の管理、機器管理、文書管理、ネットワーク管理の管理業務を行う。

本TOEのセキュリティ機能において保護の対象とする資産を表3-2及び表3-3に示す。

表3-2 TOE保護資産（利用者情報）

種別	資産内容
文書情報	デジタル化されたTOEの管理下にある文書、削除された文書、一時的な文書あるいはその断片。
利用者ジョブ	利用者が指示したジョブ。

表3-3 TOE保護資産（TSF情報）

種別	資産内容
TSF保護情報	編集権限を持った利用者以外の変更から保護しなければならない情報。 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秘密情報を除くセキュリティ機能の各種設定値が該当する。
TSF秘密情報	編集権限を持った利用者以外の変更から保護し、参照権限を持った利用者以外の読出しから保護しなければならない情報。 ログインパスワード、監査ログ、HDD暗号鍵がある。

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 3-4 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 に記載されているものと同等の内容であることが評価で確認されている。

表3-4 想定する脅威

識別子	脅威
T.DOC.DIS (文書の開示)	TOEが管理している文書が、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.DOC.ALT (文書の改変)	TOEが管理している文書が、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.FUNC.ALT (利用者ジョブの改変)	TOEが管理している利用者ジョブが、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。

識別子	脅威
T.PROT.ALT (TSF保護情報の改変)	TOEが管理しているTSF保護情報が、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保護情報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.CONF.DIS (TSF秘密情報の開示)	TOEが管理しているTSF秘密情報が、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秘密情報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.CONF.ALT (TSF秘密情報の改変)	TOEが管理しているTSF秘密情報が、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秘密情報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.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらは表3-2の利用者情報に対する脅威であり、TOEは、「識別認証機能」、「利用者制限機能」、「文書アクセス制御機能」、「残存情報消去機能」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。

「利用者制限機能」は、識別認証された利用者が、MFPの基本機能であるコピー機能、プリンター機能、スキャナー機能、ドキュメントボックス機能、及びファクス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、その機能の使用を許可する。

「文書アクセス制御機能」は、利用者が利用者情報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、その利用者情報に対するアクセスを許可する。

「残存情報消去機能」は、削除された文書やその断片等が格納されていたHDD上の領域を上書きすることで、残存情報の再利用を不可能にする。

「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、保護対象の利用者情報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

これらは表 3-3 の TSF 情報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 情報へのアクセスを、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 情報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。適合 PP に対して P.STORAGE.ENCRYPTION が追加されている。P.STORAGE.ENCRYPTION を除く組織のセキュリティ方針は、適合 PP に記載されているものと同等であることが評価で確認されている。

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.USER. 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ならなければならない。
P.SOFTWARE. VERIFICATION (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.LOGGING (監査ログ記録管理)	TOEはTOEの使用及びセキュリティに関連する事象のログを監査ログとして記録維持し、監査ログが権限を持たな

	い者によって開示あるいは改変されないように管理できなければならない。さらに権限を持つものが、そのログを閲覧できるようにしなければならない。
P.INTERFACE. MANAGEMENT (外部インタフェース管理)	TOEの外部インタフェースが権限外のものに利用されることを防ぐため、それらのインタフェースはTOEとIT環境により、適切に制御されていなければならない。
P.STORAGE. ENCRYPTION (記憶装置暗号化)	TOEのHDD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.USER.AUTHORIZATION」への対応

TOE は、「識別認証機能」及び「利用者制限機能」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。

「利用者制限機能」は、識別認証された利用者が、MFPの基本機能であるコピー機能、プリンター機能、スキャナー機能、ドキュメントボックス機能、及びファクス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、その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、「ソフトウェア検証機能」で本方針を実現する。

「ソフトウェア検証機能」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.LOGGING」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.INTERFACE.MANAGEMENT」への対応

TOE は、「識別認証機能」及び「ファクス回線分離機能」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。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。さらに、操作パネルや LAN から受信したデータの不正な転送も防止する。

「ファクス回線分離機能」は、電話回線から受信したデータを制御し、電話回線から LAN への不正なデータ転送を防止する。

(5) 組織のセキュリティ方針「P.STORAGE. 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、HDD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。表 4-1 の前提条件は、適合 PP と同等の内容であることが評価で確認されている。

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 (アクセス管理)	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、権限を持たない者に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.USER.TRAINING (利用者教育)	MFP 管理責任者は、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.TRAINING (管理者教育)	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.ADMIN.TRUST (信頼できる管理者)	MFP 管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任しているものとする。

※「MFP 管理責任者」は運用環境の組織の責任者等である。

4.2 運用環境と構成

本 TOE は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。）で接続され、TOE 本体の操作パネル及び同様に 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。

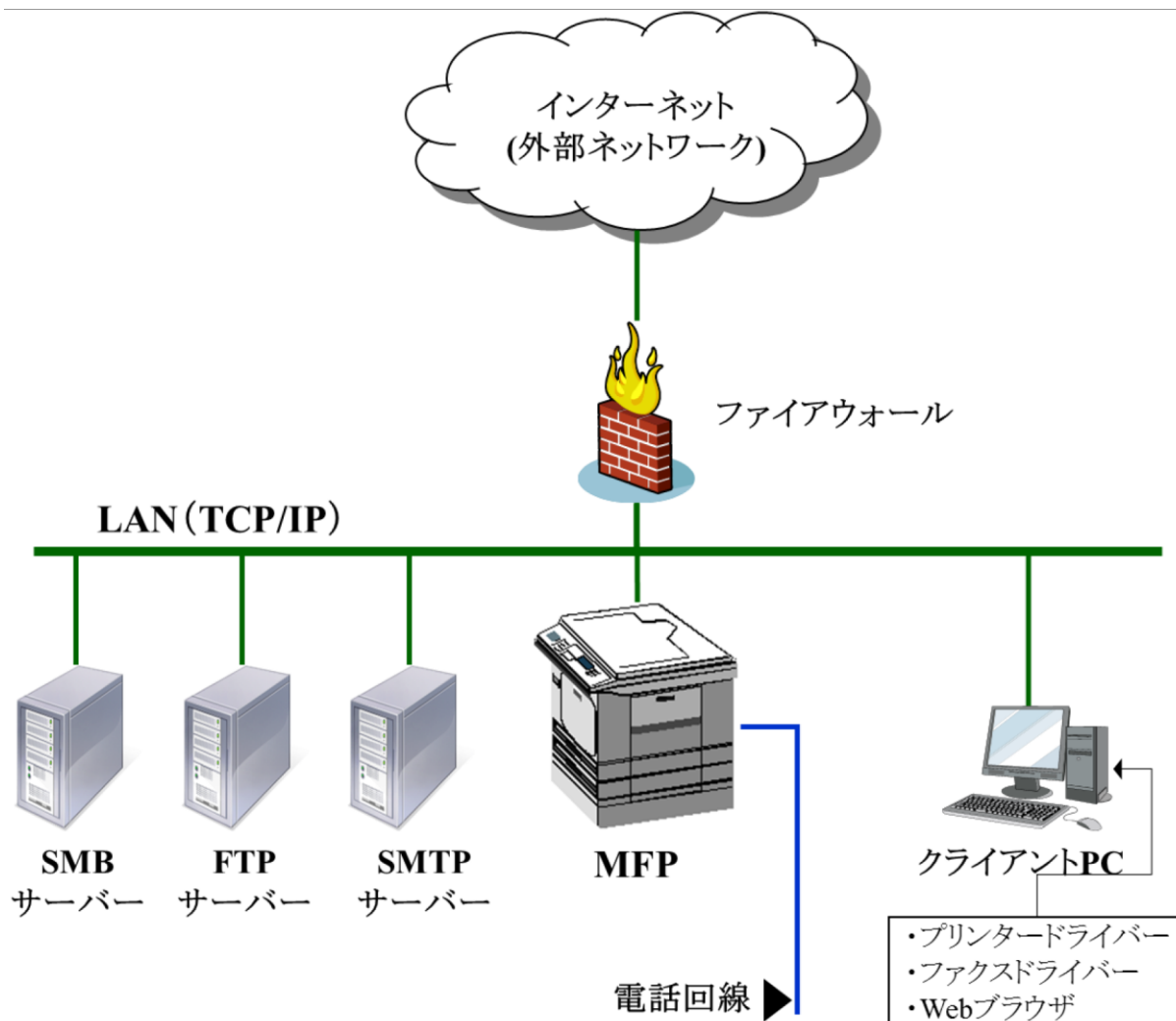


図4-1 TOEの運用環境

本TOEは、図4-1に示すような一般的な企業の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、及び電話回線が接続される。

TOEをインターネット等の外部ネットワークに接続されたLANに接続する場合は、ネットワークを通じて、外部ネットワークからTOEへ攻撃が及ばないように、外部ネットワークとLANの境界にファイアウォールを設置して、LAN及びTOEを保護する。LANには、FTPサーバー、SMBサーバー、SMTPサーバー等のサーバーコンピュータ、及びクライアントPCが接続され、TOEと文書、各種情報収集等の通信を行う。

TOEの操作は、TOEの操作パネルを使用する場合と、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にプリンタードライバーあるいはファクスドライバーをインストールすることによって、クライアントPCからLANを経由した印刷等を行うことができる。

運用環境の各機器の想定は以下のとおりである。

- クライアントPC
 - OS : Windows 8.1/10
 - Webブラウザ : Internet Explorer11, Microsoft Edge 44
 - プリンタードライバー : RPCS ドライバー 1.0.0.0
 - ファクスドライバー : PC FAX Generic ドライバー 9.4.0.0
- SMTPサーバー : Windows Server2012 P-Mail Server Manager
- FTPサーバー : Windows Server2012 (IIS8), Linux (Fedora20) vsftpd
- SMBサーバー : Windows Server2012

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

TOE とクライアント PC、TOE と各種サーバーの通信経路上のデータの保護のためには、クライアント PC や各種サーバーにおいても通信プロトコルが正しく動作するようにセキュアに運用されることが必要である。

クライアント PC や各種サーバーがセキュアに運用されることは、運用者の責任となる。

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。

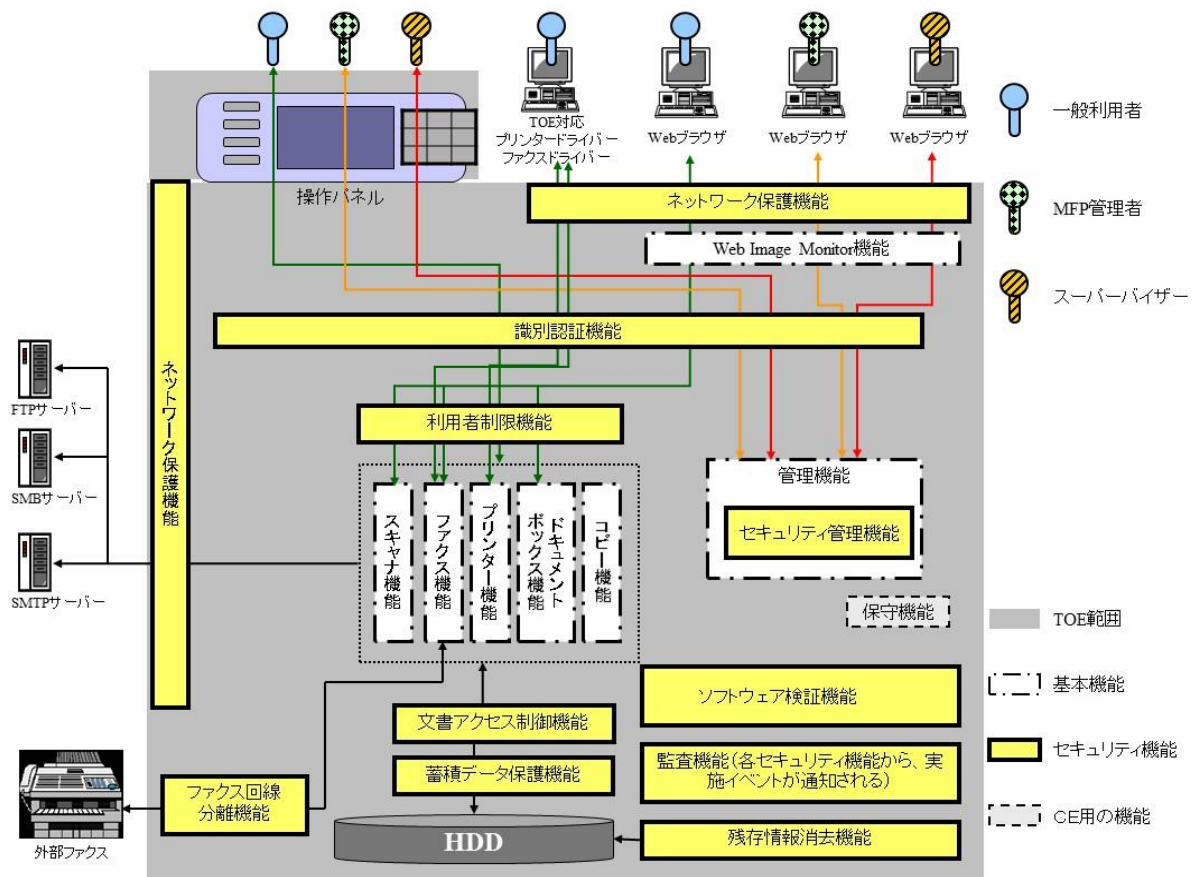


図5-1 TOEの構成

TOE の機能は、セキュリティ機能と、それ以外の MFP の基本機能等で構成される。以下、TOE のセキュリティ機能について説明する。

(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、ファクスドライバー）からTOEを使用するとき、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) 利用者制限機能

本機能は、MFPの基本機能の利用を、許可された利用者に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、利用者の役割と利用者毎に設定された権限に基づいて、当該機能の使用可否が決定される。

(3) 文書アクセス制御機能

本機能は、MFPの基本機能で文書情報及び利用者ジョブを操作するときに、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、文書情報及び利用者ジョブの所有者情報と、利用者の識別情報及び役割に基づいて行われる。

(4) 蓄積データ保護機能

本機能は、HDD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。

(5) 残存情報消去機能

本機能は、文書情報が格納されていたHDDの領域を指定されたデータで上書きする機能である。本機能は以下のタイミングで実行される。

- ・利用者が文書情報を削除したとき
- ・利用者ジョブが終了したとき
- ・MFP管理者が一括消去を指示したとき

上書きの方式は、MFP管理者が設定可能である。ただし、利用者による削除と利用者ジョブの終了の場合は、上書きデータが暗号化されてHDDに書き込まれる。そのため、MFP管理者の設定した上書き方式のデータと、実際にHDDに書き込まれるデータは異なる。

(6) ネットワーク保護機能

本機能は、IT機器との通信において、以下の暗号化通信を行う機能である。

- ・クライアントPC: TLS 1.2対応のHTTPとIPP
- ・FTPサーバー: IPsec
- ・SMBサーバー: IPsec
- ・SMTPサーバー: S/MIME

(7) ファクス回線分離機能

本機能は、電話回線から受信したデータを制御し、電話回線からLANへの不正なデータ転送を防止する機能である。

(8) 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。

(9) ソフトウェア検証機能

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証明書を使用する。ただし、TOE内部のファクス制御ユニットの場合は、本機能は完全性検証のための情報を出力し、利用者が出力された情報とガイダンスに記載されている情報を比較する。

(10) 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。

5.2 IT環境

TOEは、LANに接続され、FTPサーバー、SMBサーバー、SMTPサーバー等のサーバーコンピュータ及びクライアント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、ファクスドライバー、Webブラウザを介してTOEを利用する。クライアントPCは、文書情報の送受信だけでなく、Webブラウザを介して管理機能の一部の操作やTOEの状態確認を行うことができる。

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表 6-1 及び表 6-2 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 (RICOH IM 8000/7000)

ドキュメント名	バージョン
本機を安全にご利用いただくために	D0CM-7019
本機をお使いのお客様へ	D0CM-7020
本製品をお使いのお客様へ	D0CM-7021
かんたん操作ガイド	D0D0-7102
RICOH IM 8000/7000 シリーズをお使いのお客様へ	D0D0-7121
本製品をお使いのお客様へ	D0D0-7141
安全上のご注意	D0D0-7125
セキュリティーリファレンス	D0D0-7127
セットアップ	D0D0-7128
本機の紹介と基本操作	D0D0-7129
コピー	D0D0-7130
ドキュメントボックス	D0D0-7131
ファクス	D0D0-7132
スキャナー	D0D0-7133
プリンター	D0D0-7134
メンテナンス	D0D0-7135
こまったときには	D0D0-7136
設定	D0D0-7137
仕様	D0D0-7138
セキュリティー	D0D0-7139
ドライバーインストールガイド	D0D0-7140
セキュリティー機能をお使いになるお客様へ	D0BQ-7504 2019.03.27
IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ	D0D0-7122 2021.09.06
ヘルプ	83NHEOJAR1 .00 v252

表 6-2 製品添付ドキュメント (RICOH IM 9000/9000T)

ドキュメント名	バージョン
本機を安全にご利用いただくために	D0CM-7019
本機をお使いのお客様へ	D0CM-7020
本製品をお使いのお客様へ	D0CM-7021
かんたん操作ガイド	D0D0-7102
本製品をお使いのお客様へ	D0D0-7141
安全上のご注意	D0D0-7125
セキュリティーリファレンス	D0D0-7127
セットアップ	D0D0-7128
本機の紹介と基本操作	D0D0-7129
コピー	D0D0-7130
ドキュメントボックス	D0D0-7131
ファクス	D0D0-7132
スキャナー	D0D0-7133
プリンター	D0D0-7134
メンテナンス	D0D0-7135
こまったときには	D0D0-7136
設定	D0D0-7137
仕様	D0D0-7138
セキュリティー	D0D0-7139
ドライバーインストールガイド	D0D0-7140
セキュリティー機能をお使いになるお客様へ	D0BQ-7504 2019.03.27
IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ	D0D0-7122 2021.09.06
ヘルプ	83NHEOJAR1 .00 v252

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 3 年 2 月に始まり、令和 3 年 9 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 3 年 3 月、4 月及び 6 月に、開発現場への訪問及び製造現場へのリモート検査により、構成管理と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、令和 3 年 6 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。

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価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。

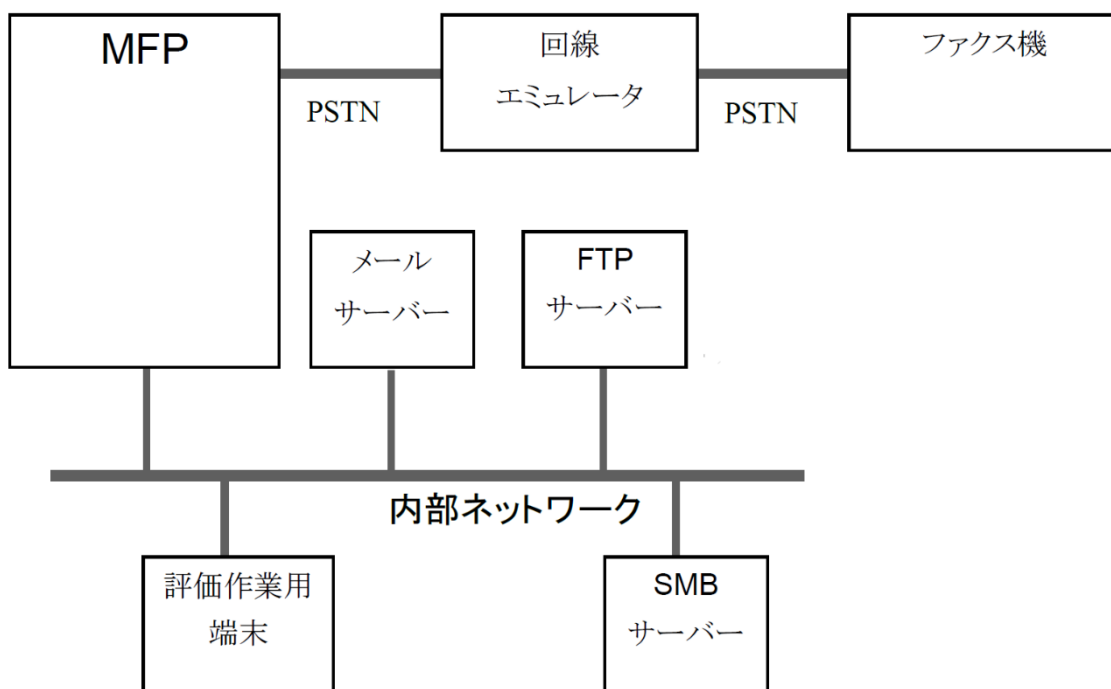


図7-1 開発者テスト構成図

表7-1 テスト構成要素

構成要素	詳細
TOE	<ul style="list-style-type: none"> ・ RICOH IM 7000 (D0CZ-00), FAXユニット タイプM44 ・ RICOH IM 8000 (D0D0-00), FAXユニット タイプM44 ・ RICOH IM 9000 (D0D1-00), FAXユニット タイプM44
クライアントPC	OS : Windows 8.1/10 Webブラウザ : Internet Explorer11, Microsoft Edge 44 プリンタードライバー : RPCS ドライバー 1.0.0.0 ファクスドライバー : PC FAX Generic ドライバー 9.4.0.0
メールサーバー (SMTPサーバー)	Windows Server 2012 P-Mail Server Manager version 1.91
FTPサーバー	Windows Server 2012 IIS8 V8.0.9200.16384 Linux(Fedora20) vsftpd 3.0.2
SMBサーバー	Windows Server 2012
回線エミュレータ	XF-A150 (パナソニック社)
ファクス機	MP C6503

開発者がテストしたTOEは、「RICOH IM 9000T」を除く機種である。評価者は、機種名の末尾の「T」の有無は給紙トレイの違いを表していることから、TOE全機種のセキュリティ機能がテストされたと見なすことができると判断している。

このことから、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ことが評価者により判断された。

(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、Webブラウザ等）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、及びデバッグ用ログデータの解析、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、TSF実装の一部を改造して異常なイベントを発生させる異常系テスト等も行われている。

<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約500項目実施された。カバレッジ分析によって、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。

- 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。

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、開発者テストとは異なる初期条件の設定や異なるパラメタを使用した上で、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、Web ブラウザ等) 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の解析、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が行われている。

<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 21 件、サンプリングテスト 19 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	<ul style="list-style-type: none"> ・ユーザーアカウントロックやアクセス制御等が仕様どおりであることを、条件を変更して確認する。 ・操作パネルの入力の文字数制限や表示のカスタマイズが仕様どおりであることを確認する。 ・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の処理が仕様どおりであることを確認する。 ・ファクス機能のエラー発生時や、送信待機がフルの状態において、ファクス機能の動作が仕様どおりであることを確認する。
②	<ul style="list-style-type: none"> ・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 (2.7.0)	プロキシ型のWeb脆弱性検査ツール
nmap (7.70)	ポートスキャンツール
Netcat (1.12)	パケット通信ツール
Nessus (8.8.0) Plugin 202105130021	脆弱性スキャンツール
Burp Suite Professional (1.7.37)	プロキシ型のWeb脆弱性検査ツール
Wireshark (2.2.5, 3.0.11)	パケットキャプチャツール
OpenSSL (1.0.1j)	SSL/TLSプロトコルを提供するソフトウェアライブラリ
PRET (0.40)	PJL、Postscriptテストツール
Android Debug Bridge (1.0.41)	Android OSを搭載したデバイス用のデバッグツール (TOEにAndroid OSが動作する部分があるため使用された)

<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、脆弱性スキャンツール、デバッグツールを使用し、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	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、SQLに関して実装上の脆弱性がないことを確認する。
③	TLS、IPsecを使用した暗号通信に関して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。

脆弱性	テスト概要
④	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。

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、第 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は、ガイダンスの記述のとおり 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。

- 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。

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

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 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」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。

2 章で説明したように TOE 識別の確認には、TOE の表示等に加えて、梱包箱上のラベルシールの確認が必要である。TOE 識別を確認できるようにするために、ラベルシールに記載されている情報を保持する必要があるため、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 9000/9000T/8000/7000 セキュリティターゲット, バージョン 1.00,
2021 年 9 月 10 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)
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	ハードディスクドライブの略称。本書で、単にHDDと記載した場合はTOE内に取り付けられたHDDを指す。
IPsec	Security Architecture for Internet Protocol 暗号技術を用いて、IPパケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルである。
MFP	デジタル複合機の略称。
S/MIME	Secure / Multipurpose Internet Mail Extensions 公開鍵方式による電子メールの暗号化とデジタル署名に関する標準規格である。

本報告書で使用された用語の定義を以下に示す。

Internet Fax	メール送受信の仕組みを使ってファクス通信を行う機能。 インターネット回線を利用する。
IP-Fax	国際標準ITU-T T.38勧告に準拠したリコーのリアルタイム型インターネットファクスの総称。 ファクス番号の代わりに相手機のIPアドレスを指定する。
保守機能	保守機能は機器故障時の保守サービス処理を実行する機能である。本TOEの運用においては、本機能を無効化する保守機能移行禁止設定が行われていることが前提となる。

12 参照

- [1] ITセキュリティ評価及び認証制度の基本規程, 令和2年10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2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, 令和2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 9000/9000T/8000/7000 セキュリティターゲット, バージョン 1.00, 2021年9月10日, 株式会社リコー
- [13] RICOH 9000/9000T/8000/7000 評価報告書, 第1.1版, 2021年9月13日, 株式会社 ECSEC Laboratory 評価センター
- [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