認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成22年6月15日 (IT認証0300)
認証番号	C0286
認証申請者	株式会社リコー
TOEの名称	以下のいずれかの名称のMFPにFCU、セキュリティカード、蓄積文書暗号化カードを装着したもの MFP製品名称： Ricoh Aficio MP 2851、Ricoh Aficio MP 3351、Savin 9228、Savin 9233、Lanier LD528、Lanier LD533、Lanier MP 2851、Lanier MP 3351、Gestetner MP 2851、Gestetner MP 3351、nashuatec MP 2851、nashuatec MP 3351、Rex-Rotary MP 2851、Rex-Rotary MP 3351、infotec MP 2851、infotec MP 3351 FCU名称： Fax Option Type 3351 セキュリティカード名称： DataOverwriteSecurity Unit Type I 蓄積文書暗号化カード名称： HDD Encryption Unit Type A
TOEのバージョン	・ソフトウェア System/Copy 1.02　Network Support 7.34 Scanner 01.12　Printer 1.02 Fax 02.00.00　RemoteFax 02.00.00 Web Support 1.05　Web Uapl 1.03 Network DocBox 1.00　animation 1.1 Option PCL 1.03　OptionPCLFont 1.01 Engine 1.00:01　OpePanel 1.10 LANG0 1.09　LANG1 1.09 ・ハードウェア Ic Key 1100　Ic Hdd 01 Data Erase Opt 1.01m　GWFCU3-20(WW) 02.00.00
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	株式会社リコー
評価機関の名称	株式会社電子商取引安全技術研究所 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。
平成23年3月29日

セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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３
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３

評価結果：合格

「以下のいずれかの名称のMFPにFCU、セキュリティカード、蓄積文書暗号化カードを装着したもの
MFP製品名称 : Ricoh Aficio MP 2851、Ricoh Aficio MP 3351、Savin 9228、Savin 9233、Lanier LD528、Lanier LD533、Lanier MP 2851、Lanier MP 3351、Gestetner MP 2851、Gestetner MP 3351、 nashuatec MP 2851、nashuatec MP 3351、Rex-Rotary MP 2851、Rex-Rotary MP 3351、infotec MP 2851、infotec MP 3351
FCU名称： Fax Option Type 3351
セキュリティカード名称： DataOverwriteSecurity Unit Type I
蓄積文書暗号化カード名称： HDD Encryption Unit Type A」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、株式会社リコーが開発した「以下のいずれかの名称のMFPにFCU、セキュリティカード、蓄積文書暗号化カードを装着したもの
MFP製品名称 : Ricoh Aficio MP 2851、Ricoh Aficio MP 3351、Savin 9228、Savin 9233、Lanier LD528、Lanier LD533、Lanier MP 2851、Lanier MP 3351、Gestetner MP 2851、Gestetner MP 3351、 nashuatec MP 2851、nashuatec MP 3351、Rex-Rotary MP 2851、Rex-Rotary MP 3351、infotec MP 2851、infotec MP 3351
FCU名称： Fax Option Type 3351
セキュリティカード名称： DataOverwriteSecurity Unit Type I
蓄積文書暗号化カード名称： HDD Encryption Unit Type A」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が平成23年3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株式会社リコーに報告するとともに、本TOEに関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

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

本認証報告書は、市販される本TOEを購入する一般消費者を読者と想定している。本認証報告書は、本TOEが適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

本TOEの保証パッケージは、EAL3及び追加の保証コンポーネントALC_FLR.2である。

1.1.2 TOEとセキュリティ機能性

本TOEは、紙文書の電子化、文書管理、印刷をするためのコピー機能、スキャナ機能、プリンタ機能、ファクス機能を提供する株式会社リコー製のデジタル複合機（以下「MFP」という。）である。

MFPは、コピー機能にスキャナ、プリンタ、ファクスの各機能を組み合わせて構成される製品であり、一般的にはオフィスのLANに接続され、文書データの入力・蓄積・出力に利用される。

本TOEは、デジタル複合機用のProtection ProfileであるIEEE Std 2600.1-2009 [14]（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。

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

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、MFPにファクス機能を提供するファクスコントローラユニット（以下「FCU」という。）、残存情報消去オプションであるセキュリティカード、及びストレージの暗号化機能を提供する蓄積文書暗号化カードを取り付けた形で構成される。

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のセキュリティは保証されない。

・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・認証制度に基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本TOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成23年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]、所見報告書、及び関連する評価証拠資料を検証し、本TOEの評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、本TOEの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は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： 以下のいずれかの名称のMFPにFCU、セキュリティカード、蓄積文書暗号化カードを装着したもの
MFP製品名称：Ricoh Aficio MP 2851、Ricoh Aficio MP 3351、Savin 9228、Savin 9233、Lanier LD528、Lanier LD533、Lanier MP 2851、Lanier MP 3351、Gestetner MP 2851、Gestetner MP 3351、 nashuatec MP 2851、nashuatec MP 3351、Rex-Rotary MP 2851、Rex-Rotary MP 3351、infotec MP 2851、infotec MP 3351
FCU名称： Fax Option Type 3351
セキュリティカード名称： DataOverwriteSecurity Unit Type I
蓄積文書暗号化カード名称： HDD Encryption Unit Type A

バージョン：

・ソフトウェア

System/Copy	1.02	Network Support	7.34
Scanner	01.12	Printer	1.02
Fax	02.00.00	RemoteFax	02.00.00
Web Support	1.05	Web Uapl	1.03
Network DocBox	1.00	animation	1.1
Option PCL	1.03	OptionPCLFont	1.01
Engine	1.00:01	OpePanel	1.10
LANG0	1.09	LANG1	1.09

・ハードウェア

Ic Key	1100	Ic Hdd	01
Data Erase Opt	1.01m	GWFCU3-20(WW)	02.00.00

開発者： 株式会社リコー

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い、MFP外装に表示されている名称、及びTOEの操作パネルに表示されたバージョンと、TOE構成品一覧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がセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEはMFPに蓄積された文書データ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3-1、及び表3-2に示す。

表3-1　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の管理下にある利用者文書、削除された文書、一時的な文書あるいはその断片。（以下、「文書」という。）
機能情報	利用者が指示したジョブ。（以下、「利用者ジョブ」という。）

表3-2　TOE保護資産（TSF情報）

種別	資産内容
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、ログインパスワード入力許容回数、年月日、時刻、パスワード最小桁数等が含まれる。 （以下、「TSF保護情報」という。）
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。 （以下、「TSF秘密情報」という。）

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3-3に示す脅威を想定し、これに対抗する機能を備える。表3-3の脅威は、適合PPで定義された脅威を、原文の英文から日本語に翻訳したものであり、両者の同等性については評価の過程において確認されている。

表3-3 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。
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

表3-3に示す全ての脅威は、TOEの正当な利用者以外の者、もしくは正当な権限を有さない者による利用者情報、TSF情報への侵害（閲覧、改ざん）に関するものである。

これら脅威に対しては下記のセキュリティ機能により対抗する。

(1) 利用者の識別認証

TOEを利用しようとする者に対して、ログインユーザー名、ログインパスワードの入力要求を行い、TOE内部で管理されている利用者情報に一致することを確認する。入力手段としては、TOE本体操作パネルからの入力、クライアントPCのWebブラウザ上からの入力、プリンタ機能使用時及びPCファクス機能使用時のドライバー経由での入力がある。

必要な機能強度を確保する手段として下記の機能を有する。

・MFP管理者により設定された規定回数連続して認証に失敗すると、そのユーザーアカウントはロックアウトされる（ロックアウト時間（60分）が経過、または解除されるまでそのユーザーアカウントは使用できなくなる）
・ログイン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

ログインユーザー名、パスワードが正当であると確認されると、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が特定する役割は以下の通りである。

・一般利用者
・MFP管理者
・スーパーバイザー

また、識別認証機能をサポートする手段として下記の機能を有する。

・入力画面に入力されたログインパスワードに対して、ダミー文字を表示する
・ログイン後一定時間TOEに対する操作が行われない場合には自動的にログアウトする

(2) アクセス制御（利用者情報に対するアクセス制御）

利用者からの処理要求に対して、その利用者のログインユーザー名、役割毎の権限を元に文書情報、及び利用者ジョブへの操作に対してアクセス制御を実施する。利用者文書には、どの利用者に対して操作（削除、印刷、ダウンロード等）を許可するかを規定する情報（文書利用者リスト）が関連付けられており、一般利用者からの操作要求に対してそのログインユーザー名と文書利用者リストの情報から、許可もしくは拒否の制御を行う。MFP管理者の利用者文書に対する操作としては、全

ての利用者文書に対して削除権限のみが与えられる。

利用者ジョブに対しても、そのジョブを作成したログインユーザー名が関連付けられており、ログインユーザー名が一致する一般利用者には該当ジョブの削除操作が許可される。MFP管理者に対しては全ての利用者ジョブに対して削除権限が与えられる。スーパーバイザーに対しては、利用者情報に関して全ての操作が禁止される。

(3) 残存情報削除

HDDに残存する削除済みの利用者文書、一時的に利用された文書、その断片に対する不正なアクセスを防ぐため、文書データが削除される際に指定データを上書きし残存情報が残らないようにする。

(4) ネットワーク保護

通信経路のモニタリングによる情報漏えいを防ぐため、TOEとクライアント間のWebブラウザ経由での操作に関する通信、プリンタ機能及びPCファクス機能を使用した通信についてSSL暗号化通信を使用する。また、TOEと相手先との通信にはIPsec通信、及びS/MIME通信を使用する。

(5) セキュリティ管理

TSF情報に対する、利用者の権限を超えた不正なアクセスを防ぐためTOE利用者の役割によってTOE設定情報の参照・改変、利用者情報の新規登録、改変等に対するアクセス制御を行う。情報の改変（変更）に関する権限のポリシーとしては、一般利用者は自身のログインパスワード改変のみ権限を有し、スーパーバイザーは自身、及びMFP管理者のログインパスワード改変のみ権限を有している。それ以外の改変はMFP管理者にのみ許可される。

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3-4に示す。P.STORAGE.ENCRYPTIONを除く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の過程で確認されている。P.STORAGE.ENCRYPTIONはHDDへのデータ書き込みを、直接読み取れない形式で行なうことを想定したセキュリティ方針である。

表3-4　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利用のログインユーザー名を持った者だけが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.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(操作パネル、LAN、USB、電話回線)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は、内蔵するHDDに対して、その記録内容を暗号化しなければならない。

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3-4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

このセキュリティ方針は、TOEに正式に登録されたユーザーのみにTOEを使用させることを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a)　利用者の識別認証

3.1.1.2に記載の識別認証により、TOEを利用しようとする者に対してログインユーザー名、ログインパスワードの入力を要求し、TOEに登録された正当な利用者であることを確認し、そのログインユーザー名に対応した役割を関連付ける。

TOEは正当な利用者であると確認された利用者にのみ、TOEが提供する機能の使用を許可する。

(b) セキュリティ管理

TSF情報に対する、利用者の権限を超えた不正なアクセスを防ぐため、TOE利用者の役割によってTOE設定情報の参照・改変に対するアクセス制御を行う。

利用機能リストの改変はMFP管理者のみに許可される。

(2) 組織のセキュリティ方針「P.SOFTWARE.VERIFICATION」への対応

このセキュリティ方針は、TOEの実行コードの正当性について、自己検証できることを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a) 自己テスト

TOE（FCU以外の構成要素）は、電源投入後の初期立ち上げ中に自己テストを実行し、MFP制御ソフトウェアの実行コードの完全性、正当性の確認を行う。自己テストではファームウェアのハッシュ値を検証し実行コードの完全性を確認し、各アプリケーションに対して、署名鍵ベースでの検証を行い実行コードの正当性を確認する。

自己テスト中に何らかの異常が認められた場合には、操作パネルにエラー表示を行い、一般利用者がTOEを利用できない状態で動作停止する。自己テストで異常が認められなかった場合は、立上げ処理を続行し利用者がTOEを利用できる状態にする。

FCUについては、完全性検証を行うための検証情報を利用者が確認できる形で提供し、利用者がこの情報を基に確認を行い、問題がない場合にTOEを使用する。

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

このセキュリティ方針は、TOEのセキュリティ事象に関する監査ログを取得し、適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a) セキュリティ監査

TOEは、監査対象となるセキュリティ事象が発生した際に、事象種別、利用者識別、発生日時、結果等の項目から成る監査ログを生成し、監査ログファイルに追加保存する。生成した監査ログファイルは識別認証に成功したMFP管理者のみに読出し、削除を許可する。監査ログファイルの読出しはクライアントPCのWebブラウザを介してテキスト形式で行う。

また、監査ログの事象発生日時を記録するため、日付、時間情報をTOEのシステム時計から取得する。

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

このセキュリティ方針は、TOEが提供する外部インタフェース（操作パネル、LANインタフェース、USBインタフェース、電話回線）が不正な利用者に使用されないように適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する

(a)利用者の識別認証

3.1.1.2に記載の識別認証により、TOEを利用しようとする者に対してログインユーザー名、ログインパスワードの入力を要求し、TOEに登録された正当な利用者であることを確認し、TOEの利用を許可する。

(b)外部インタフェース間の情報転送制御

本機能は能動的なメカニズムの実装ではなく、外部インタフェースのアーキテクチャ設計として対応するもので、外部から入力された情報に対する処理、及び外部インタフェースから送信される情報の制御についてはかならずTOEが関与することにより、外部インタフェース間で不正な情報転送が実施されることを防ぐ。

USBインタフェースについては、使用を無効化する設定で運用することにより、このインタフェースを使用した不正な情報転送を防ぐ。

(5)　組織のセキュリティ方針「P.STORAGE. ENCRYPTION」への対応

このセキュリティ方針は、TOEに内蔵するHDDの記録内容を暗号化することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a)蓄積データ保護機能

HDDに対して書き込み、読み出しを行う全てのデータを対象にAESによる暗号化、復号処理を行う。暗号化、復号処理の際には管理者操作により初期設置時に作成されTOE内に格納される256ビット長の鍵が使用される。

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で定義された前提条件を、原文の英文から日本語に翻訳したものであり、両者の同等性については評価の過程において確認されている。

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。

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で接続され、TOE本体の操作パネル及び同様にローカルエリアネットワーク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。

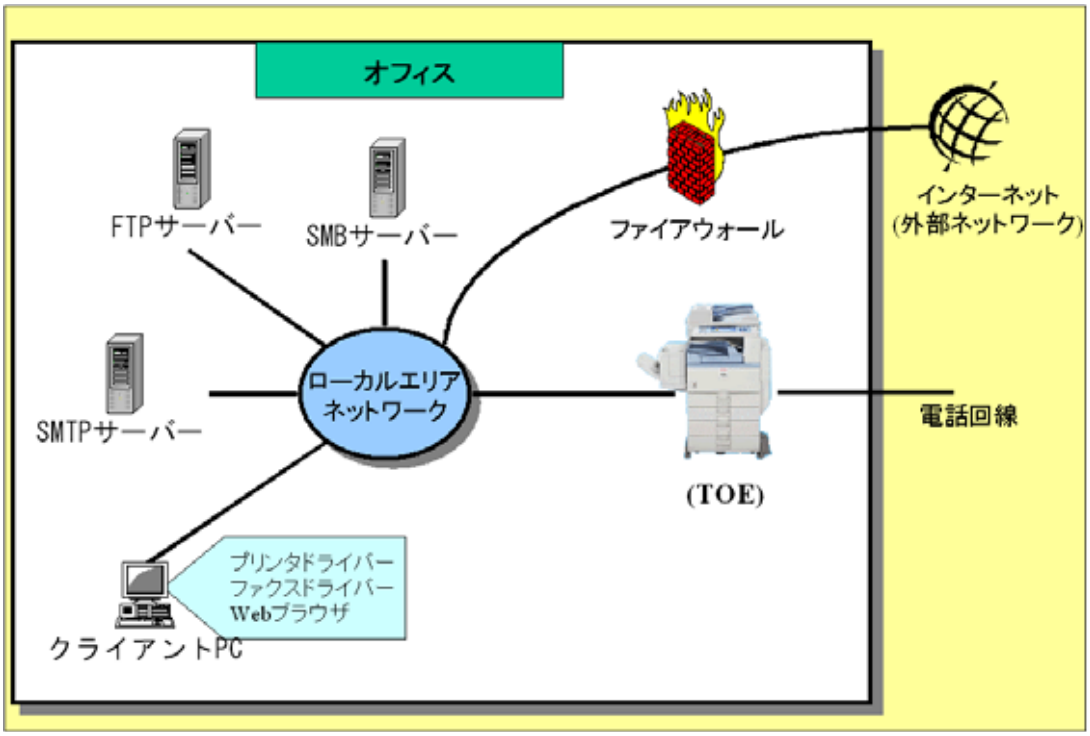

図4-1 TOEの運用環境

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、ローカルエリアネットワーク、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ローカルエリアネットワークに接続する場合は、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ローカルエリアネットワークの境界にファイアウォールを設置して、ローカルエリアネットワーク及びTOEを保護する。ローカルエリアネットワークには、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と文書データ等の通信を行う。

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PC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からローカルエリアネットワーク経由した印刷等を行うことができる。

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が、十分に信頼できるものとする。

また、本環境においてTOEを利用するにあたり、関連する利用者を表4-2に示す。

表4-2　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の削除と新規登録をする権限を持つ。
	MFP管理者	TOEの管理を許可された利用者。一般利用者のユーザー情報管理、機器管理、文書管理、ネットワーク管理の管理業務を行う。

表4-2に示すとおり、TOEの利用者は一般利用者と管理者に分類され、さらにその役割によって管理者はスーパーバイザーとMFP管理者とに分類される。TOEを直接利用する利用者としては表4-2に示すとおりであるが、それ以外にMFP管理者及びスーパーバイザーの選任権限を持つMFP管理責任者がTOEの間接的な利用者として存在する。MFP管理責任者は運用環境における組織の責任者等を想定している。

4.3　運用環境におけるTOE範囲

本TOEの範囲は、MFPにファクス機能を提供するFCU、残存情報消去オプションであるセキュリティカード、及びストレージの暗号化機能を提供する蓄積文書暗号化カードを取り付けた形で利用者に販売される製品全体である。開発者が利用者サイトにてMFP本体にオプションを設置し、動作確認を行った上でTOEとして利用者に引き継がれる。

また、本TOEではメール送信相手先との通信保護機能としてS/MIMEをサポートするが、ここで使用される送信相手の証明書については、その有効性、正当性を管理者の責任において管理する必要がある。

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。TOEはオプションを取り付けたMFP製品全体である。

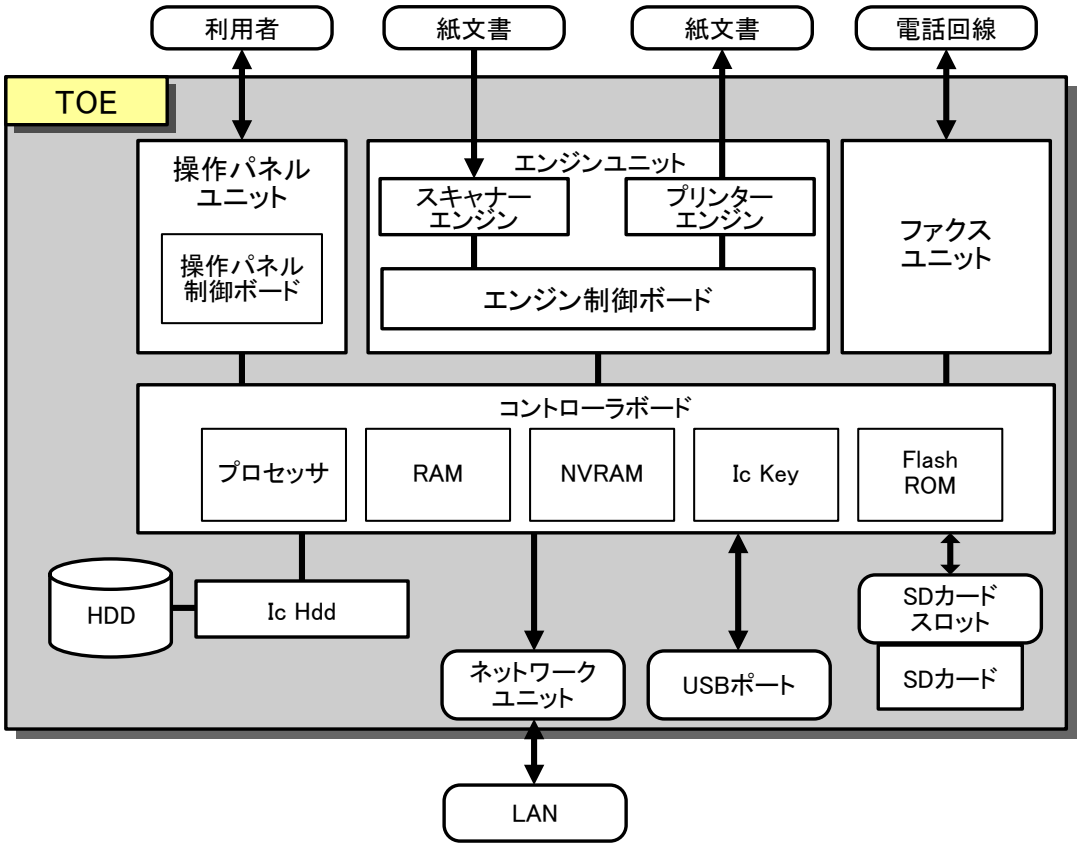

図5-1　TOE境界

図5-1に示すとおり、TOEは操作パネルユニット、エンジンユニット、ファクスユニット、コントローラボード、HDD、Ic Hdd、ネットワークユニット、USBポート、SDカードスロット/SDカードのハードウェアから構成される。以下に各構成要素の概要を示す。

【操作パネルユニット（以下、「操作パネル」という。）】

操作パネルは、TOEに組み付けられている、TOEの利用者がTOE操作に使用するインタフェース装置である。ハードキー、LED、タッチパネル付き液晶ディスプレイと操作パネル制御ボードで構成される。

【エンジンユニット】

紙文書を読込むためのデバイスであるスキャナエンジン、紙文書を印刷し排出するデバイスであるプリンタエンジン、各エンジンを制御するエンジン制御ボード

から構成される。

【ファクスユニット】

モデム機能を持ち電話回線と接続し、G3規格で他のファクス装置とファクスの送受信をするユニット。TOEを識別する要素のうちFCUが該当する。

【コントローラボード】

コントローラボードはプロセッサ、RAM、NVRAM、Ic Key、FlashROM が載った基板である。各要素の簡潔な説明は以下の通り。

プロセッサ	：MFP動作における基本的な演算処理を行う半導体チップ。
RAM	：画像メモリとして利用される揮発性メモリ。
NVRAM	：MFPの動作を決定するMFP制御データが入った不揮発性メモリ。
Ic Key	：乱数発生、暗号鍵生成の機能を持ち、MFP制御ソフトウェアの改ざん検知に利用されるセキュリティチップ。
FlashROM	:MFP制御ソフトウェアがインストールされている不揮発性メモリ。MFP制御ソフトウェアは、TOE を識別する要素のうち、System/Copy 、Network Support 、Scanner 、Printer 、Fax、RemoteFax、Web Support、Web Uapl、Network DocBox、animation、Option PCL、OptionPCLFont、LANG0、LANG1を含む。

【HDD】

イメージデータ、識別認証に利用するユーザー情報が書込まれるハードディスクドライブである。

【Ic Hdd】

HDDに保存する情報を暗号化し、HDDから読み出す情報を復号する機能を持ったセキュリティチップである。

【ネットワークユニット】

Ethernet(100BASE-TX/10BASE-T)をサポートしたLAN用の外部インタフェースである。

【USBポート】

PCから直結して印刷を行う場合に、TOEとPCを接続する外部インタフェースである。なお本TOEでは設置時に利用禁止設定とする。

【SDカード/SDカードスロット】

SDカードを挿入するためのスロット、及び残存情報消去機能ソフトウェア（Data Erase Opt）が保持されているSDカードである。SDカードスロットは機器内部に存在し、通常運用においてはSDカードが操作されることはない。

5.2 IT環境

TOEは、ローカルエリアネットワークに接続され、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。

ローカルエリアネットワーク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、PC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以下に示す。本TOEに添付されるドキュメントは販売地域、及び販売会社により4種類のセットが存在する。各ドキュメントセット間の差異としては、英語表記の違い、ドキュメント構成の違い、国・地域によるレギュレーションの違い等があるが、内容の同一性については評価の過程で確認されている。

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。

［英語版-1］（北米向け製品添付ドキュメント）

ドキュメント名	バージョン
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions About This Machine	D085-7753
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions Troubleshooting	D085-7803
Notes for Users	D085-7897
App2Me Start Guide	D085-7906B
Manuals for Users 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7502
Manuals for Administrators 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7504
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7522

Notes for Users	D060-7781
Notes for Users	G189-6775
Notes for Users	D092-7905
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857810
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1-2009	D0857807
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

［英語版-2］（欧州向けリコー社製品添付ドキュメント）

ドキュメント名	バージョン
Quick Reference Copy Guide	D092-7714
Quick Reference Fax Guide	D509-8534
Quick Reference Printer Guide	D381-7303
Quick Reference Scanner Guide	D381-7309
Manuals for This Machine	D085-7538
Safety Information for Aficio MP 2851/Aficio MP 3351	D085-7500
Notes for Users	D085-7896A
App2Me Start Guide	D085-7904B
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A	D085-7510
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351	D085-7512
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7522
Notes for Users	D060-7781
Notes for Users	G189-6786
Notes for Users	D092-7906
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857809
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1-2009	D0857806
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver.1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A

Notes for Users	D377-7250

［英語版-3］（欧州向けOEM製品添付ドキュメント）

ドキュメント名	バージョン
Quick Reference Copy Guide	D092-7714
Quick Reference Fax Guide	D509-8534
Quick Reference Printer Guide	D381-7303
Quick Reference Scanner Guide	D381-7309
Manuals for This Machine	D085-7538
Safety Information for MP 2851/MP 3351	D085-7501
Notes for Users	D085-7896A
App2Me Start Guide	D085-7904B
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A	D085-7510
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351	D085-7512
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7522
Notes for Users	D060-7781
Notes for Users	G189-6786
Notes for Users	D092-7906
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857809
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1TM-2009	D0857806
VM card Manuals	D377-7500
Help(83NHAQENZ)	Ver.1.20
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

［英語版-4］（アジア太平洋向け製品添付ドキュメント）

ドキュメント名	バージョン
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions About This Machine	D085-7755
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions Troubleshooting	D085-7805
Quick Reference Copy Guide	D092-7715
Quick Reference Printer Guide	D381-7307
Quick Reference Scanner Guide	D381-7407

Notes for Users	D085-7899
App2Me Start Guide	D085-7906B
Manuals for Users MP 2851/3351 Aficio MP 2851/3351	D085-7506
Manuals for Administrators MP 2851/3351 Aficio MP 2851/3351	D085-7508
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351	D085-7522
Notes for Users	D060-7781
Notes for Users	G189-6775
Notes for Users	D092-7905
To Users of This Machine	D029-7904
Operating Instructions Notes On Security Functions	D0857810
Notes for Administrators: Using this Machine in a Network Environment Compliant with IEEE Std.2600.1TM-2009	D0857807
VM Card Manuals	D377-7500
Help(83NHAQENZ)	Ver1.20
Quick Reference FAX Guide	D509-8535
Manuals DataOverwriteSecurity Unit Type H/I	D377-7900A
Notes for Users	D377-7250

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22年6月に始まり、平成23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、平成22年7月、8月、9月、10月、11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。一部開発サイトの評価に関しては、過去案件での評価内容の再利用、及び代替資料の確認により評価機関として現地訪問と同様の確信が得られたため、現地訪問の省略を行っている。

また、平成22年12月に開発者サイトで開発者のテスト環境を使用し、開発者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。

7.3 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、主な構成要素を表7-1に示す。

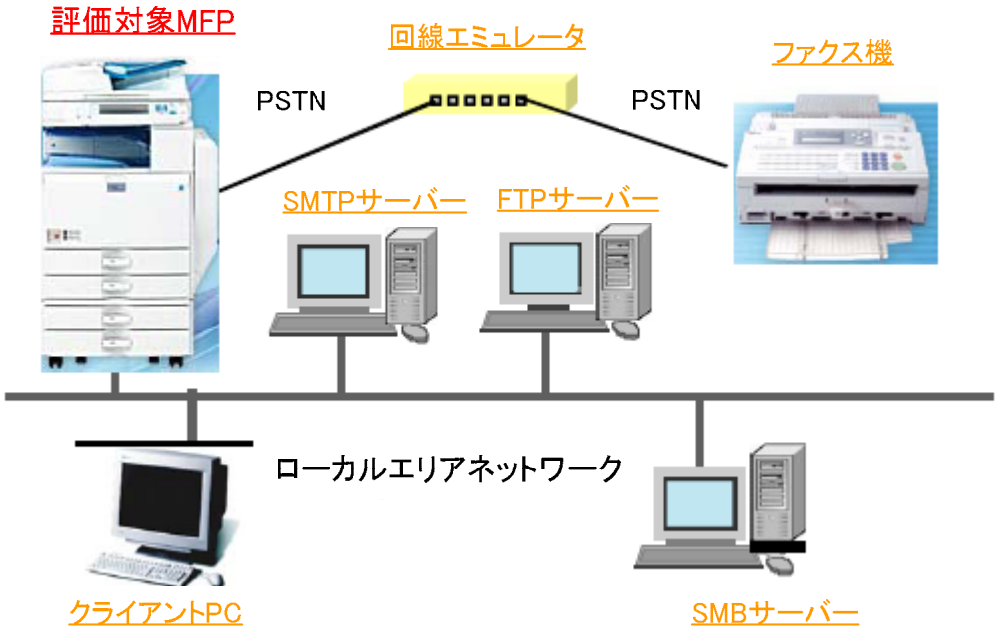

図7-1　開発者テスト構成図

表7-1　テスト構成要素

構成要素	詳細
TOE	・Ricoh Aficio MP 2851 ・Ricoh Aficio MP 3351 バージョン ・ソフトウェア System/Copy　1.02　Network Support　7.34

	Scanner 01.12 Printer 1.02 Fax 02.00.00 RemoteFax 02.00.00 Web Support 1.05 Web Uapl 1.03 Network DocBox 1.00 animation 1.1 Option PCL 1.03 OptionPCLFont 1.01 Engine 1.00:01 OpePanel 1.10 LANG0 1.09 LANG1 1.09 ・ハードウェア Ic Key 1100 Ic Hdd 01 Data Erase Opt 1.01m GWFCU3-20(WW) 02.00.00
クライアントPC	OS：Windows XP Pro SP3 / Windows Vista Business SP1 Webブラウザ： Internet Explorer6.0/7.0/8.0 プリンタードライバー：PCL6 Driver Ver.1.0.0.0 PCファクスドライバー：LAN FAX Driver Ver.1.6.2
SMTPサーバー	Windows Server 2003 SP2のSMTPサーバー機能
FTPサーバー	Windows Server 2003 SP2のFTPサーバー機能
SMBサーバー	Windows Server 2003 SP2のSMBサーバー機能
ファクス機	Aficio C3501（ファクス機能を持つRICOH社MFPを使用）
簡易交換機	TLE-101Ⅲ（AVM社）

開発者テストで使用されたTOE（2機種のMFP）はSTで識別されている複数のMFPの一部の機種であるが、他の機種はテストで使用したMFPのOEM製品であり、製品名の違い以外は同一機種である。また、テストで使用した2機種の間では印刷速度の違いはあるが、セキュリティ機能は同一である。

このことから、開発者テストにおいてテスト対象に選択された2機種「Ricoh Aficio MP 2851」と「Ricoh Aficio MP 3351」は、STの記載内容と矛盾がなく、STにおいて識別されているTOE構成を、カバーしている。よって、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ているとみなすことができる。

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＞

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、不正なTSF実装を使用した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645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 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TSFIに関して、パラメタの組み合わせ、境界値、異常値等のテスト項目を追加する。

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 例外処理、キャンセル処理に関して開発者テストと異なるバリエーションを追加したテスト項目を実施する。

④ 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。
- 認証取得済みの類似製品との機能性の差異を考慮し、本TOEにおいて新規に追加されたTSF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14件、サンプリングテスト26件のテストが実施された。

実施された主な独立テスト概要と、対応する独立テストの観点を表7-2に示す。

表7-2 実施した主な独立テスト

独立テストの観点	テスト概要
①	・複数インタフェースからアクセスされた場合の識別認証機能の挙動が仕様通りであることを、アクセスタイミング等を変えながら確認する。
②	・一般ユーザーと管理者が同時にログインしている状態でアカウントのロックアウト処理が仕様通りに動作することを確認する。 ・複数の一般機能が並行して動作する状況においても、セキュリティ機能が仕様通りに動作することを確認する。
③	・クライアントPCのドライバーから想定されない設定でTOEにアクセスされた場合の挙動が仕様通りであることを確認する。 ・TOE内部に設置されたSDカードが抜かれた状態で電源がONになった場合の挙動が仕様通りであることを確認する。 ・有効期限切れの証明書を用いた場合のS/MIMEの処理が仕様通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 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 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。

⑤ 想定外のユーザー操作､例外事象の発生タイミング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。

⑥ 内部基板等への物理的な操作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
Paros（3.2.13）	プロキシ型のWeb脆弱性検査ツール
Nmap Zenmap（5.00）	ポートスキャンツール
Wireshark（0.99.8）	パケットキャプチャツール

＜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概要を表7-4に示す｡評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、11件の侵入テストを実施した。

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を使用し､必要と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	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。
③	SSL、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。
④	CPU過負荷状態、リソース枯渇状態においてTOEがアンセキュアな状態にならないことを確認する。
⑤	ミスフィード等のハードウェアに関する例外処理時、もしくは電話回線の強制的な遮断時においてもセキュリティ機能がバイパスされないことを確認する。
⑥	バージョンが異なるFCU、及び一部が改ざんされたFCUがTOEに設置された場合でもセキュリティ機能がバイパスされ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。

7.4 評価構成について

本評価では、図7-1に示す構成において評価を行った。ネットワークはIPv4を使用している。本TOEは、上記と構成要素が大きく異なる構成において運用される場合はない。よって評価者は、上記評価構成が適切であると判断した。

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
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A

- 2600.1-CPY, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
- 2600.1-FAX, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
- 2600.1-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment A
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

・ 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

評価者により、利用者に対する以下の勧告が評価報告書にてなされている。

・本TOEのガイダンスに記載された下記機能については、本評価の範囲外となる。
- 不正コピーガード機能
- 機密印刷
- 管理者役割毎のアクセス制御
（機器管理者、ユーザー管理者、ネットワーク管理者、文書管理者）
- IP-Fax、及びInternet Fax
- App2Me

また、本TOEでは無効される保守機能に関連する下記機能については、TOEに含まれるガイダンスに従った設置生成手順により無効化される。
- ＠Remote
- RFU（リモートファームウェア更新）

8 認証実施

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

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が解決されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3及び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

1.1.3にも示したとおり、本TOEの評価環境として、保守機能についてはその使用が無効化されていることが前提となる。保守機能が有効化され使用された場合、それ以降はTOEではなくなる可能性がある。

また本TOEの利用者は、4.3 運用環境におけるTOE範囲、及び7.6 評価者コメント/勧告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。

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。

Aficio MP 2851/3351 series with DataOverwriteSecurity Unit Type I
セキュリティターゲット バージョン 1.00　2011年03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。
PSTN	Public Switched Telephone Networksの略で、公衆交換電話網の意味
RFU	リモートファームウェア更新の略称。 TOEにリモート接続し、ファームウェアを更新する機能。 （本機能は評価の範囲外となる）
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。

App2Me	MFP操作、設定を支援するためのクライアントPC用アプリケーション。
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。
PCファクス機能	ファクス機能の１つ。クライアントPC上のPCファクスドライバーを利用して、ファクス送信、文書蓄積を行う機能。
@Remote	インターネット経由でTOEをリモート操作する機能。遠隔故障診断、カウンター情報収集、トナー情報収集等がリモート操作の対象となる。 （本機能は評価の範囲外となる）
機密印刷	蓄積した文書を印刷する際に予め設定されたパスワード入力を要求する機能。 （本機能は評価の範囲外となる）
管理者役割	MFP管理者に割り当てることができる予め定義された役割。 以下の4種類の管理者役割が定義され、それぞれ別の管理者に割り当てることが可能であるが、本TOEにおいては全ての役割が割り当てられたMFP管理者を想定している。 （細分類された管理者役割毎のアクセス制御は本TOEの評価対象外となる） ・機器管理者（機器管理、監査の実施を行う） ・ユーザー管理者（一般利用者の管理を行う） ・ネットワーク管理者 （TOEのネットワーク接続管理を行う） ・文書管理者 （利用者文書、及び文書利用者リストの管理を行う）
文書	コピー機能、プリンタ機能、スキャナ機能、ドキュメントボックス機能、ファクス機能を利用して生成されるTOE管理下のデジタル画像情報。 本体内のHDDに蓄積されている文書を本STでは明示的に利用者文書と呼ぶ。 単に文書と記述する場合はコピー時や印刷時の削除された文書、一時的な文書あるいはその断片も含む。
不正コピーガード機能	文書の背景に印刷された特殊な地紋をコピー時に検出し、それに対応した処理を行うことにより、文書コピーによる情報漏えいを防ぐ機能。（本機能は評価の範囲外となる）

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。
利用者ジョブ	利用者がTOEに対して操作を要求する作業。開始と終了を持つひと続きの作業を１ジョブとする。対象となる操作は、利用者文書の蓄積操作、印刷操作、ダウンロード操作、削除操作である。
ログイン パスワード	各ログインユーザー名に対応したパスワード。
ログインパスワード入力許容回数	識別認証時にユーザーアカウントがロックアウトされるまでに許容される、認証連続失敗回数。 1～5回の設定値をMFP管理者がTOEの初期設定時に設定し、設定後は変更されない。
ログイン ユーザー名	利用者に与えられている識別子。TOEはその識別子により利用者を特定する。
ロックアウト	ユーザーアカウントが使用できなくなる状態。
ロックアウト時間	ユーザーアカウントがロックアウト状態から自動的に解除されるまでの時間。 本TOEではMFP管理者により60分が設定され運用される。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[2] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[3] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-001 (平成21年12月翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-002 (平成21年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] Aficio MP 2851/3351 series with DataOverwriteSecurity Unit Type I セキュリティターゲット バージョン 1.00　2011年3月10日　株式会社リコー

[13] Aficio MP 2851/3351 series with DataOverwriteSecurity Unit Type I 評価報告書 第2.0版 2011年3月11日　株式会社電子商取引安全技術研究所 評価センター

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