認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司

原紙押印済

評価対象

申請受付日(受付番号)	**平成22年2月22日** (IT**認証**0291)
認証番号	C0261
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(Fax Option Type 3351)**を装着したもの** MFP**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
TOE**のバージョン**	MFP **ソフトウェア/ハードウェアバージョン** : **ソフトウェア** System/Copy 1.00 Network Support 7.29.3 Scanner 01.12 Printer 1.01 Fax 01.00.00 Web Support 1.01 Web Uapl 1.03 Network Doc Box 1.00 **ハードウェア** Ic Key 1100 Ic Hdd 01 FCU **バージョン** : GWFCU3-20(WW) 01.00.00
PP**適合**	**なし**
適合する保証パッケージ	EAL3
開発者	**株式会社リコー**
評価機関の名称	**一般社団法人** IT**セキュリティセンター 評価部**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成22年6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 改訂第2版 (翻訳第2.0版)

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 改訂第2版 (翻訳第2.0版)

評価結果：合格

「以下のいずれかの名称のMFPにFCU(Fax Option Type 3351)を装着したもの
MFP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 Fax Option: Fax Option Type 3351」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

1.1 はじめに

この認証報告書は、「以下のいずれかの名称のMFPにFCU(Fax Option Type 3351)を装着したもの　MFP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　Fax Option: Fax Option Type 3351」(以下「本TOE」という。)について一般社団法人 ITセキュリティセンター 評価部(以下「評価機関」という。)が行った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に関心を持つ利用者や運用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、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、「本TOEを導入する組織において、導入される本TOEの管理責任を持つ者」を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： 以下のいずれかの名称のMFPにFCU(Fax Option Type 3351)を装着したもの

MFP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

バージョン： MFP ソフトウェア/ハードウェアバージョン：

	ソフトウェア	System/Copy 1.00
		Network Support 7.29.3
		Scanner 01.12
		Printer 1.01
		Fax 01.00.00
		Web Support 1.01
		Web Uapl 1.03
		Network Doc Box 1.00
	ハードウェア	Ic Key 1100
		Ic Hdd 01
FCU バージョン：		GWFCU3-20(WW) 01.00.00

開発者： 株式会社リコー

1.2.2 製品概要

本認証が対象とする製品は、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(オプション)を提供する株式会社リコー製のデジタル複合機(以下MFP)である。ただし、本認証は、ファクス機能(オプション)を搭載した状態の製品を対象とする。

この製品は、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画像I/O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。この製品は、内部に蓄積された文書データを意図しない開示や操作から保護し、クライアントとの間で送受信する文書データの

漏洩に対処する。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOEの範囲

TOEは、以下のすべての条件を満たした場合、本認証が対象とする製品である。製品が以下のいずれかの設定を満たさない場合は、TOEではない。保守機能への移行を許可するように設定し、保守機能が使用された場合、これ以降はTOEではなくなる可能性がある(保守機能により、製品自体への変更が行われる可能性が否定できないからである)。

- 保守機能への移行を許可しない
- IPv4プロトコルを使用する (IPv6プロトコルを使用しない)
- IP-ファクスとインターネットファクス機能を使用しない
- 識別・認証機能としてはベーシック認証を使用する (ベーシック認証以外の方式を使用しない)

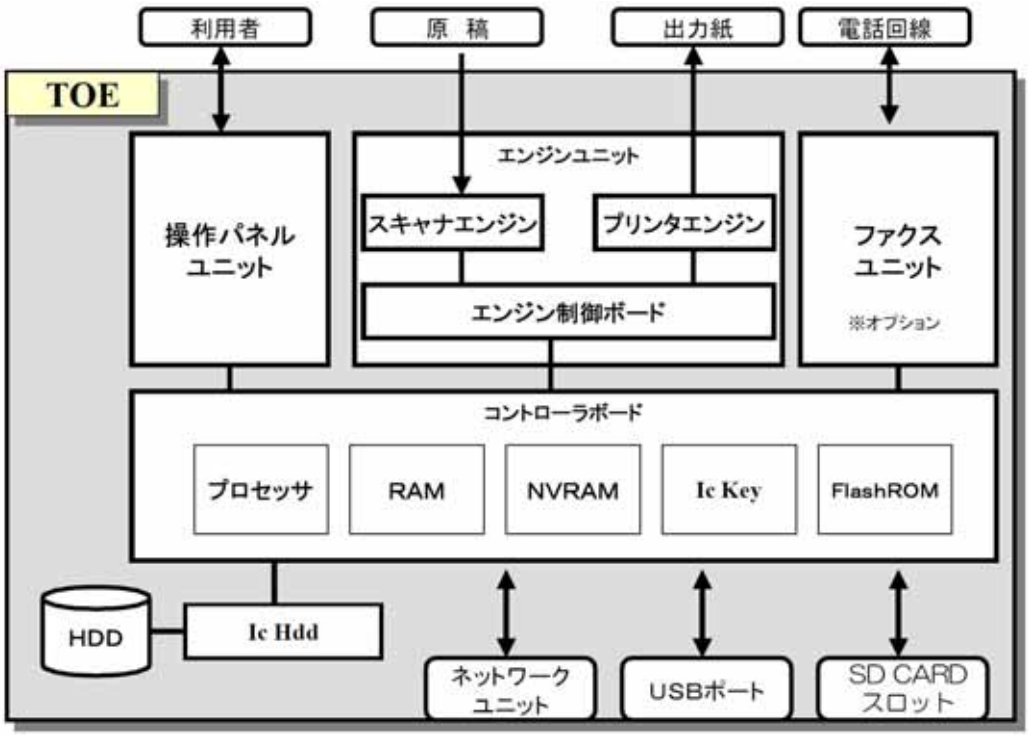

図1-1 TOEの構成

図1-1が、TOEを構成する物理的な要素である。以下に各要素の説明を簡潔に示す。

- 操作パネルユニット(以下、操作パネルと言う)

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
  エンジンユニットは、スキャナエンジン、プリンタエンジン、エンジン制御ボードで構成される。スキャナエンジンは紙文書を読込むための入力装置で、プリンタエンジンは紙文書を印刷し排出する出力装置である。

- ファクスユニット(オプション)
  ファクスユニットはモデム機能を持ち電話回線と接続してファクスの送受信を行う装置である。

- 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。このコントローラボード上にあるFlashROMには、MFP制御ソフトウェアがインストールされている。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、WebSupport、Web Uapl、Network Doc Boxを含んでいる。Ic Keyは、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である。

- Ic Hdd
  Ic HddはHDDに保管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。

- HDD
  HDDはイメージデータ、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。イメージデータを文書データとして保管する領域は、D-BOXと呼ばれる。

- ネットワークユニット
  ネットワークユニットはイーサネット(100BASE-TX/10BASE-T)規格をサポートしたネットワークのインタフェース基板である。

- USB ポート
  USBポートは、クライアントPCとTOEをUSB接続し、クライアントPCから印刷あるいはファクス送信するために使用する。

- SD CARD スロット
  TOEの設置時の蓄積データ保護機能有効化と、保守時に使われるインタフェースである。ただし、本認証では保守作業が想定されないので、設置時のみの使用となる。

1.2.3.2 TOEの動作概要

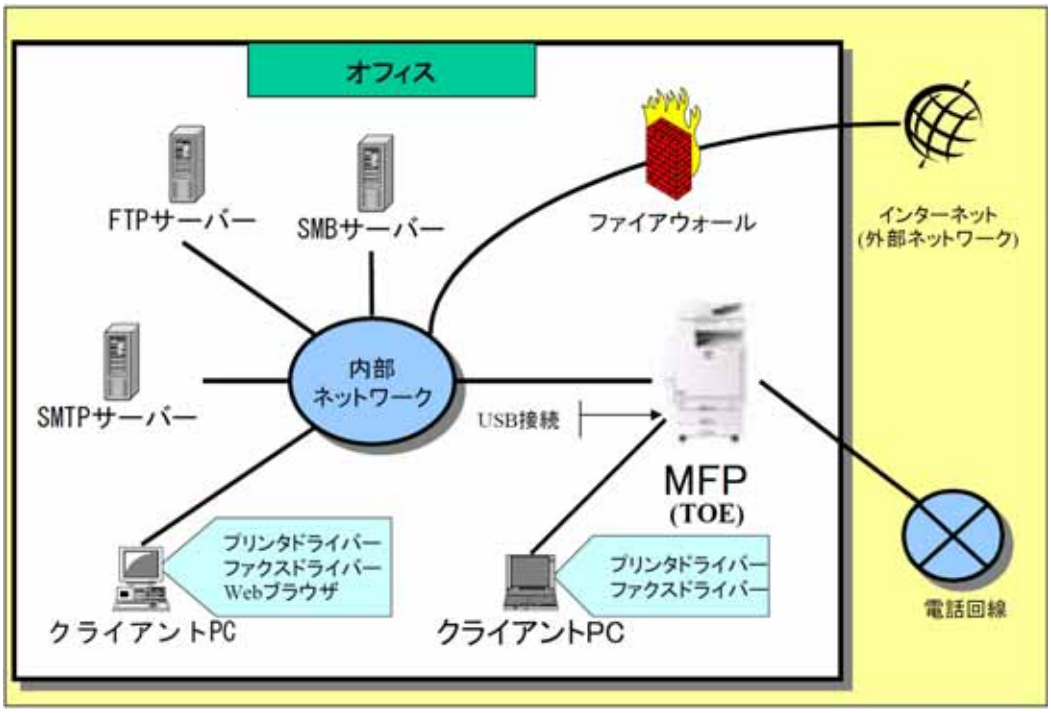

図1-2　TOEの利用環境の例

TOEは、例えば図1-2のような環境で利用され、主目的はイメージデータの入出力と蓄積である。入出力の手段は以下のとおりである。TOEは入力したイメージデータを単に出力することも、蓄積しておくこともできる。

- TOEがイメージデータの入力を受ける手段
  - 原稿をスキャナエンジンから光学的に読み取る。
  - クライアントPCからネットワークユニットまたはUSBポート経由で受信する。
  - 電話回線からファクスユニット経由で受信する。
- TOEがイメージデータを出力する手段
  - プリンタエンジンから印刷する。
  - ネットワークユニットから、クライアントPCへ転送する。
  - ネットワークユニットから、イメージデータを添付したメールを送信する。
  - ネットワークユニットから、FTPでFTPサーバ、またはSMBプロトコルでSMBサーバへ送信する。

- ファクスユニットから、電話回線を通してファクス送信する。

1.2.3.3 TOEの機能

TOEは、コピー機能、プリンタ機能、ファクス機能、スキャナ機能、ドキュメントボックス機能、管理機能、Webサービス機能を持つ。各機能を以下に説明する。

1) コピー機能

コピー機能は、スキャナエンジンから原稿をイメージデータとして読み取り、指定された印刷条件に従い、プリンタエンジンからイメージデータを印刷する機能である。

読み取ったイメージデータは、スキャナ機能以外によって生成された文書データ (以下、「文書データ(スキャナ機能以外)」とする) としてD-BOXに蓄積することができる。

2) プリンタ機能

プリンタ機能は、クライアントPCからネットワークユニットまたはUSBポート経由で印刷データを受信し、直接印刷あるいは蓄積印刷をする機能である。

直接印刷の場合は、単に受信した印刷データをプリンタエンジンから印刷する。

蓄積印刷の場合は、印刷データを文書データ(スキャナ機能以外)としてD-BOXに蓄積する。すぐには印刷されない。実際の印刷は、後述の「1.2.3.3 8) ドキュメントボックス機能(管理)」で行われる。

3) ファクス機能(受信)

ファクス機能(受信)は、ファクスユニットからファクスデータを受信し、印刷または蓄積する機能である。

印刷の場合は、単に受信したファクスデータをプリンタエンジンから印刷する。

蓄積の場合は、ファクスデータをファクス受信データに変換してD-BOXに蓄積する。すぐには印刷されない。実際の印刷は、後述の「1.2.3.3 8) ドキュメントボックス機能(管理)」で行われる。

(注) TOEが受信したファクスデータは、本認証では保護の対象ではない。
(「5.2.1 保護の対象となる資産についての注意」参照)

4) ファクス機能(直接送信・メモリ送信)

ファクス機能(直接送信・メモリ送信)は、スキャナエンジンから原稿をイメージデータとして読み取り、直接送信またはメモリ送信によりファクスユニットから送信する機能である。

直接送信の場合は、送信先のファクスに接続後、原稿をスキャンしながら、生成されたイメージデータを送信先のファクスに逐次送信する。

メモリ送信の場合は、ファクスに接続する前に原稿のスキャンを済ませ、その後に送信先のファクスに接続してイメージデータを送信する。

5) ファクス機能(蓄積文書ファクス送信)

ファクス機能(蓄積文書ファクス送信)は、「D-BOXに蓄積された文書データの中から指定されたもの」をファクスユニットから送信する機能である。

6) ファクス機能(PCファクス送信)

ファクス機能(PCファクス送信)は、クライアントPCからネットワークユニットまたはUSBポート経由で印刷データを受信し、ファクスユニットから送信する機能である。

7) ドキュメントボックス機能(スキャン)

ドキュメントボックス機能(スキャン)は、スキャナエンジンから原稿をイメージデータとして読み取り、文書データ(スキャナ機能以外)としてD-BOXに蓄積する機能である。

8) ドキュメントボックス機能(管理)

ドキュメントボックス機能(管理)は、「D-BOX内の文書データ(スキャナ機能以外)またはファクス受信データの中から指定されたもの」に対し、以下に示す指定された処理を行う機能である。

- 印刷 (プリンタエンジンから印刷する)
- 削除 (D-BOXから削除する)
- ダウンロード (ネットワークユニット経由でクライアントPCへ転送する)

(補足) 「スキャナ機能(スキャン)」から得られるスキャナ機能専用の文書データ (以下、「文書データ(スキャナ機能専用)」とする) は、「ドキュメントボックス機能(管理)」では扱われず、「スキャナ機能(管理)」で扱われる。

9) スキャナ機能(スキャン)

スキャナ機能(スキャン)は、スキャナエンジンから原稿をイメージデータとして読み取り、メール送信、フォルダ送信または蓄積する機能である。

メール送信の場合は、ネットワークユニットから指定されたメールアドレス宛に、イメージデータが添付されたメールを送信する。

フォルダ送信の場合は、ネットワークユニットから指定されたフォルダへ、イメージデータをFTPまたはSMBプロトコルで転送する。

蓄積の場合は、イメージデータを文書データ(スキャナ機能専用)としてD-BOXに蓄積する。

(補足) この機能で得られる文書データ(スキャナ機能専用)と他の機能で得られる文書データ(スキャナ機能以外)は扱いが異なる。この機能で得られる文書データ(スキャナ機能専用)は「スキャナ機能(管理)」で扱われ、他の機能で得られる文書データ(スキャナ機能以外)は「ドキュメントボックス機能(管理)」で扱われる。

10)スキャナ機能(管理)

スキャナ機能(管理)は、「D-BOX内の文書データ(スキャナ機能専用)の中から指定されたもの」に対し、以下に示す指定された処理を行う機能である。

- 送信 (「スキャナ機能(スキャン)」のメール送信またはフォルダ送信)
- 削除 (D-BOXから削除する)
- ダウンロード (ネットワークユニット経由でクライアントPCへ転送する)

(補足) この機能の対象となる文書データ(スキャナ機能専用)は、「スキャナ機能(スキャン)」により蓄積されたものに限られる。それ以外の機能で蓄積された文書データ(スキャナ機能以外)は「ドキュメントボックス機能(管理)」で扱われる。

11)管理機能

管理機能は、TOEの機器設定、ネットワークの接続設定、許可利用者情報の設定、文書データ利用制限情報の設定を行う機能である。設定できる情報は、TOEの許可利用者(一般ユーザー、管理者、スーパーバイザー)の役割に応じて、それぞれ定められている。

12)Webサービス機能

Webサービス機能は、TOEの許可利用者(一般ユーザー、管理者、スーパーバイザー)がクライアントPCのWebブラウザからTOEを操作するための機能である。

Webサービス機能の対象となるのは、上記「1) コピー機能」～「11) 管理機能」で説明した機能であるが、Webサービス機能では利用できない機能も一部ある。

1.2.3.4 TOEのセキュリティ機能

1) 識別認証機能、文書データアクセス制御機能

「1.2.3.3 TOEの機能」においては、文書データを読み出すための操作(印刷や送信など、TOEに文書データとして保存されているものを何らかの形式で取り出すこと)、文書データを削除するための操作がある。TOEは、これらの操作が文書データの所有者の意図に反して行われないように、TOEを操作する者を識別・認証し、アクセス制御する機能を持つ。

2) 蓄積データ保護機能

TOEの廃棄後等にHDDから情報が漏洩することを防ぐために、TOEは、HDDに書き込まれるデータを暗号化する機能を持つ。

3) ネットワーク通信データ保護機能

内部ネットワークの盗聴から情報が漏洩することを防ぐために、TOEは、TOEが内部ネットワークを通じてやりとりするデータを暗号化する機能を持つ。

暗号化する対象はTOEが内部ネットワークを通じてやりとりするデータに限定され、TOEがUSBまたは電話回線を通じてやりとりするデータは対象にならない。

4) 電話回線からの侵入防止機能

電話回線からTOEが不正に使用されることを防ぐために、TOEは、電話回線からは許可された通信だけを受け付けるようにする。

5) MFP制御ソフトウェア検証機能

TOEは、MFP制御ソフトウェアが株式会社リコーにより正規に提供されたものであることを確認する機能を持つ。

6) 監査機能

TOEは、運用状況の確認、あるいはセキュリティ侵害の検知に必要な事象が発生した場合に、事象を監査ログとして記録する機能を持つ。

7) セキュリティ管理機能

TOEは、セキュリティ機能の動作に係わる情報を設定する機能を提供する。設定できる情報は、TOEの許可利用者(一般ユーザー、管理者、スーパーバイザー)の役割に応じて、セキュリティの維持に支障がないようにそれぞれ定められている。

8) 保守機能移行禁止機能

保守機能の操作を、機器管理者が明示的に許可しない限り禁止する機能である。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[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」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート3及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Aficio MP 2851/3351 series with Fax Option Type 3351 セキュリティターゲット」(以下「本ST」という。)[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1([5][8]のいずれか) 附属書A、CCパート2([6][9]のいずれか)の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3([7][10]のいずれか)の保証要件を満たしていることを評価した。この評価手順及び結果は、「株式会社リコー Aficio MP 2851/3351 series with Fax Option Type 3351 評価報告書」(以下「評価報告書」という。)[13]に示されている。なお、評価方法は、CEM([11][12]のいずれか)に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE評価が所定の手続きに沿って行われたことを確認した。評価は、平成22年6月の評価機関による評価報告書の提出をもって完了し、本TOE評価がCC及びCEM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概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
T.ILLEGAL_USE	攻撃者が、TOEの外部インタフェース(操作パネル、ネットワークインターフェース、USBインタフェース、またはSD CARDインタフェース)からTOEに不正にアクセスし文書データを読み出す、あるいは文書データを削除するかもしれない。
T.UNAUTH_ACCESS	TOEの許可利用者が、TOEの許可利用者に提供するTOEの外部インタフェース(操作パネル、ネットワークインターフェース、あるいはUSBインタフェース)から文書データに対して利用権限を越えたアクセスをするかもしれない。
T.ABUSE_SEC_MNG	セキュリティ管理機能の利用を許可されないものが、セキュリティ管理機能を不正に利用するかもしれない。
T.SALVAGE	攻撃者が、TOEからHDDを持去り、文書データを暴露するかもしれない。
T.TRANSIT	攻撃者が、内部ネットワーク上のTOEが送受信する文書データと印刷データを不正に入手し漏洩、または改ざんするかもしれない。 (注) 「TOEが送受信する文書データと印刷データ」はUSBインタフェース上または電話回線上にも存在しうるが、USBインタフェース上または電話回線上のデータの入手や改ざんは脅威としては扱われない。
T.FAX_LINE	攻撃者が電話回線からTOE に不正にアクセスするかもしれない。

2.1.2 組織のセキュリティ方針

TOEの利用にあたって要求される組織のセキュリティ方針を表2-2に示す。

表2-2 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.SOFTWARE	TOE内のFlashROMにインストールされているMFP制御ソフトウェアが正規のものであることを確認する手段が提供されていること。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-3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2-3 TOE使用の前提条件

識別子	前提条件
A.ADMIN	管理者は、管理者に課せられた作業においてTOEをセキュアに運用するために必要な知識を持ち、一般ユーザーにTOEをセキュアに運用させるものとする。さらに、管理者は、管理者の特権を利用して悪意を持った不正をしないものとする。 (注) 「TOEをセキュアに運用するために必要な知識」には、以下の内容も含まれる。 ● 以下の機能を使用してはならない。 ➢ アドレス帳のバックアップ/リストア ● 以下の設定を維持したまま使用しなければならない。 ➢ 保守機能への移行を許可しない ➢ IPv4プロトコルを使用する (IPv6プロトコルを使用しない) ➢ IP-ファクスとインターネットファクス機能を使用しない ➢ 識別・認証機能としてはベーシック認証を使用する (ベーシック認証以外の方式を使用しない)

識別子	前提条件
A.SUPERVISOR	スーパーバイザーは、スーパーバイザーに課せられた作業においてTOEをセキュアに運用するために必要な知識を持ち、スーパーバイザーの特権を利用して悪意を持った不正をしないものとする。
A.NETWORK	TOEが接続されるネットワークをインターネットなどの外部ネットワークと接続する場合は、外部ネットワークから内部ネットワークを保護するものとする。

2.1.4 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。

表2-4 [英語版-1]

ガイダンス文書名
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions About This Machine
9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351 Operating Instructions Troubleshooting
Notes for Users
App2Me Start Guide
Manuals for Users 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Manuals for Administrators 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

表2-5 [英語版-2]

ガイダンス文書名
Quick Reference Copy Guide
Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Manuals for This Machine
Safety Information for Aficio MP 2851/Aficio MP 3351
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351

ガイダンス文書名
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

表2-6　[英語版-3]

ガイダンス文書名
Quick Reference Copy Guide
Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Manuals for This Machine
Safety Information for MP 2851/MP 3351
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351 A
Manuals for Administrators Security Reference MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

表2-7　[英語版-4]

ガイダンス文書名
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions　About This Machine
MP 2851/MP 3351 MP 2851/MP 3351 Aficio MP 2851/3351 Operating Instructions　Troubleshooting
Quick Reference Copy Guide
Quick Reference Fax Guide
Quick Reference Printer Guide
Quick Reference Scanner Guide
Notes for Users
App2Me Start Guide
Manuals for Users MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators MP 2851/3351 Aficio MP 2851/3351
Manuals for Administrators Security Reference Supplement 9228/9233 MP 2851/3351 LD528/LD533 Aficio MP 2851/3351
Notes for Administrators: Using this Machine in a CC-Certified Environment
VM Card Manuals

2.1.5 構成条件

図1-2にTOEと外部環境の接続を示す。TOEと以下の全ての外部環境との接続が必要ということではなく、TOEの利用形態に応じて、TOEは必要な外部環境と接続する。

- TOEとUSB経由で接続するクライアントPC
- TOEとイーサネット経由で接続するクライアントPC
- TOEとイーサネット経由で接続するSMTPサーバ
- TOEとイーサネット経由で接続するFTPサーバ
  (FTPサーバは、IPSec通信をサポートする必要がある)
- TOEとイーサネット経由で接続するSMBサーバ
  (SMBサーバは、IPSec通信をサポートする必要がある)
- 公衆電話回線、またはそれと同等の回線

クライアントPCからドライバを通してTOEを利用する場合、ユーザーズガイダンスに記されたWebページから入手したドライバが必要である。本評価時点のドライバの情報は以下のとおりである。

- PCL 6　ドライバ　V1.0.0.0
- LAN Fax ドライバ　V1.61

「TOEとイーサネット経由で接続するクライアントPC」において、ブラウザからTOEを利用する場合、ブラウザにはInternet Explorer 6.0以降が必要である。

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

2.2.1 T.ILLEGAL_USE, T.UNAUTH_ACCESS, T.ABUSE_SEC_MNGへの対抗

これらの脅威には、識別・認証とアクセス制御の一連の流れによって対抗する。

TOEの機能を利用しようとする者(操作者)に対し、TOEは、利用者IDと認証情報(パスワード)の入力を求める。TOEは、入力された利用者IDと認証情報が正当なものであるかどうかを確認する。

TOEは、利用者IDと認証情報の入力試行によるなりすましに対抗するため、以下の機能を持つ。

- ロックアウトに関する方針に従い、同じ利用者IDで認証に連続で失敗した回数が規定回数に達した場合は、TOEはその利用者IDをロックアウトする

(そのIDでの使用ができないようにする)。

- 認証情報の登録または変更を受け付ける際に、パスワード最小桁数とパスワード複雑度の条件を満たすパスワードだけを受け付ける。

TOEが利用者IDと認証情報を確認した結果として、以下の(1)、(2)いずれかの状況となる。

(1) 利用者IDと認証情報が正当であることを確認できない場合、TOEは操作者に対してTOEの機能を利用させない。

TOEの利用を許可されていない者は正当な利用者IDと認証情報を持たないので、(1)は、TOEの利用を許可されていない者がTOEの機能を利用できないということである。これはT.ILLEGAL_USEへの対抗となる。

(2) 利用者IDと認証情報が正当であることを確認できた場合、TOEは利用者IDによって操作者を特定し、さらに利用者IDより操作者の持つ役割を特定することになる。TOEは、それらを特定したうえで、TOEの機能の利用を許可する。

TOEが特定する役割は以下のとおりである。

- 一般ユーザー
- 管理者
- スーパーバイザー

役割が管理者である場合、さらに以下の役割が特定される。以下の役割は排他的ではなく、一つの管理者の利用者IDに対して複数の役割が対応してもよい。

- ユーザー管理
- 機器管理
- ネットワーク管理
- 文書管理

操作者は、(2)の後に、TOEに対して実際にやりたいことの指示を行う。その指示は、「文書データに対する操作」または「管理機能の使用」の指示を含む可能性がある。どちらの指示を含むかにより、以下の(3)、(4)いずれかの状況となる。

(3) 「文書データに対する操作」の指示を含む場合、TOEは、(2)で認識した利用者IDと操作者の持つ役割に基づき、指示された操作が許可されたものであるかどうかの判定をする。許可されている場合に限り指示に従った操作を実行する。判定は以下の基準で行われる。

- 操作者の役割が一般ユーザーである場合

個々の文書データには、利用者とその利用者の操作を許可する程度(読み出し許可、印刷条件の変更許可、削除許可、文書データ利用者リストの許可)をあらわす情報(文書データ利用者リスト)が付加されている。TOEは、(2)で特定した利用者IDと文書データ利用者リストに基づいて指示された操作が許可されているかどうかを判定する。

- 操作者の役割が一般ユーザーでない場合

  (2)で特定した操作者の役割が管理者で、かつ文書管理の役割も持つ場合は、任意の文書データの削除が許可される。それ以外の場合は、文書データに対する操作は許可されない。

(3)は、TOEの許可利用者を対象として、利用制限(文書データ利用者リストで許可された一般ユーザーか、許可された管理者か)に従い文書データへの操作を制限していることになるため、これでT.UNAUTH_ACCESSへの対抗となる。

(4) 「管理機能の使用」の指示を含む場合、TOEは、(2)で認識した利用者IDと操作者の持つ役割に基づき、指示された操作が許可されたものであるかどうかの判定をする。許可されている場合に限り指示に従い「セキュリティ管理機能」を適用する。

セキュリティ管理機能は、TOEが保持する以下のデータに対する操作である。

- 文書データ利用者リスト
- 利用者の登録情報
- ロックアウトに関する方針(ロックアウトされるまでの連続した認証失敗の回数、ロックアウトを時間経過で解除するかどうか、ロックアウトする時間)
- システム日付、時刻
- HDD暗号鍵
- 監査ログ
- 保守機能移行禁止設定
- 受け入れられるパスワードの強度の方針(最小文字数、最低限使用しなければならない文字種)

TOEは、これらのデータへの操作に対して、操作者の役割が管理者またはスーパーバイザーである場合に許可する[*1]。ただし、以下のように、セキュリティの維持に支障のない範囲において、操作者が一般ユーザーである場合

[*1]管理者またはスーパーバイザーであっても全ての操作を許可されるわけではない。管理者を細分化した役割(ユーザー管理、機器管理、ネットワーク管理、文書管理)及びスーパーバイザーに対し、どの操作が許可されるかの規則が定められている。その詳細は本報告書では割愛する。

にも許可する。

- 文書データ利用者リストに対する操作(所有者の変更は除く)は、文書の所有者、及び文書データ利用者リストで個別に指定された一般ユーザーにも許可される。

- 利用者の登録情報のうちの「認証情報」「文書データデフォルトアクセス権リスト(所有者は除く)」「S/MIME利用者情報」の変更は、本人であれば一般ユーザーにも許可される。

(4)は、セキュリティ管理機能の利用を、「セキュリティ管理機能の利用を許可される者」に制限していることになるため、T.ABUSE_SEC_MNGへの対抗となる。

2.2.2 T.SALVAGEへの対抗

TOEは、T.SALVAGEに対抗するために、文書データを正規の方法(操作パネルまたはクライアントPCから、「1.2.3.3 TOEの機能」で示した機能を利用すること)で読み出したとき以外は文書データの内容を理解することを困難にする。(蓄積データ保護機能)

この機能は、以下の暗号アルゴリズムと鍵長により、HDDに書込む直前にデータを暗号化し、HDDから読み出した直後にデータを復号することで実現される。

- 暗号アルゴリズム：AES
- 鍵長：256ビット

2.2.3 T.TRANSITへの対抗

TOEは、T.TRANSITに対抗するために、TOEが内部ネットワークを経由して送受信する文書データと印刷データを、盗聴や改ざんから保護する。

使用するメカニズムは、保護の対象に応じてSSL、IPSec、S/MIMEのいずれかとなる。S/MIMEの場合はTOEの機能により実現される。SSLの場合はTOEとクライアントPCの機能の双方の協力によって通信路が確立される。IPSecの場合はTOEとSMBサーバまたはFTPサーバの機能の双方の協力によって通信路が確立される。

保護される範囲は、保護のために使用するメカニズムによって決まる。具体的には表2-8 (1)～表2-8 (3)に示すとおりとなる。

表2-8 (1)　具体的なデータ、メカニズム、範囲

対象となるデータ
「プリンタ機能」でクライアントPCから内部ネットワーク経由でネットワークユニットへ送信される印刷データ (USB経由は対象外)
保護のメカニズムと保護される範囲
SSLのメカニズムにより、クライアントPCからネットワークユニットへと到達するまでの内部ネットワークの部分が保護される

表2-8 (2)　具体的なデータ、メカニズム、範囲

対象となるデータ
「ファクス機能(PCファクス送信)」でクライアントPCから内部ネットワーク経由でネットワークユニットへ送信される印刷データ (USB経由は対象外)
保護のメカニズムと保護される範囲
SSLのメカニズムにより、クライアントPCからネットワークユニットへと到達するまでの内部ネットワークの部分が保護される

表2-8 (3)　具体的なデータ、メカニズム、範囲

対象となるデータ
「スキャナ機能(スキャン)」または「スキャナ機能(管理)」でネットワークユニットから出力される文書データ
保護のメカニズムと保護される範囲
送信で、送信先がフォルダの場合： IPSecのメカニズムにより、ネットワークユニットから「指定したフォルダのあるSMBサーバまたはFTPサーバ」へと到達するまでの内部ネットワークの部分が保護される 送信で、送信先がメールアドレスの場合： S/MIMEのメカニズムにより、ネットワークユニットから「メール送信先のメールクライアント」へと到達するまでのネットワーク(内部ネットワークを含む)の部分が保護される ダウンロードの場合： SSLのメカニズムにより、ネットワークユニットからクライアントPCへと到達するまでの内部ネットワークの部分が保護される

2.2.4 T.FAX_LINEへの対抗

TOEは、T.FAX_LINEに対抗するための能動的なメカニズムを持つわけではない。

TOEが電話回線を介してファクス送受信以外の動作を行わないことにより、T.FAX_LINEへの対抗となる。

2.2.5 P.SOFTWAREの実現

TOEは、P.SOFTWAREを実現するために、FlashROMにインストールされているMFP制御ソフトウェアの実行コードが、株式会社リコーにより正規に提供された状態と相違ないことを確認する機能を持つ。

この機能は、実行コードに付加された電子署名を検証することにより実現される。

この機能と、TOEが出力する各要素のバージョンの確認を合わせて、「株式会社リコーが正規の手段で提供した正しい版のソフトウェア」であることが確認される。

STの記述の範囲から、MFP制御ソフトウェアの実行コードに対する具体的な脅威を想定できないが、正規のMFP制御ソフトウェアかどうかが確認できることを消費者に明示するために、この組織のセキュリティ方針が定義された。

2.2.6 他のセキュリティ機能のサポート

脅威への直接の対抗ではないが、セキュリティ侵害の検出に利用できる機能として、TOEは監査機能を持つ。

この機能は、セキュリティ侵害の検出に利用できる事象が発生した場合に、事象を監査ログとして記録する。

3 評価機関による評価実施及び結果

3.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 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2月に始まり、平成22年6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4月、及び5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。また、平成22年4月に開発者サイトで開発者のテスト環境を使用し、開発者が実施した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。ただし、開発セキュリティの各ワークユニットに関する一部のプロセスの施行状況については、同一の保証レベルの他のTOEに関して実施された平成21年10月、及び11月の調査結果が、現時点でも信頼できるとの判断により採用された。

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。

3.3 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。

3.3.1 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。評価した開発者テストの概要を以下に示す。

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3-1に示す。

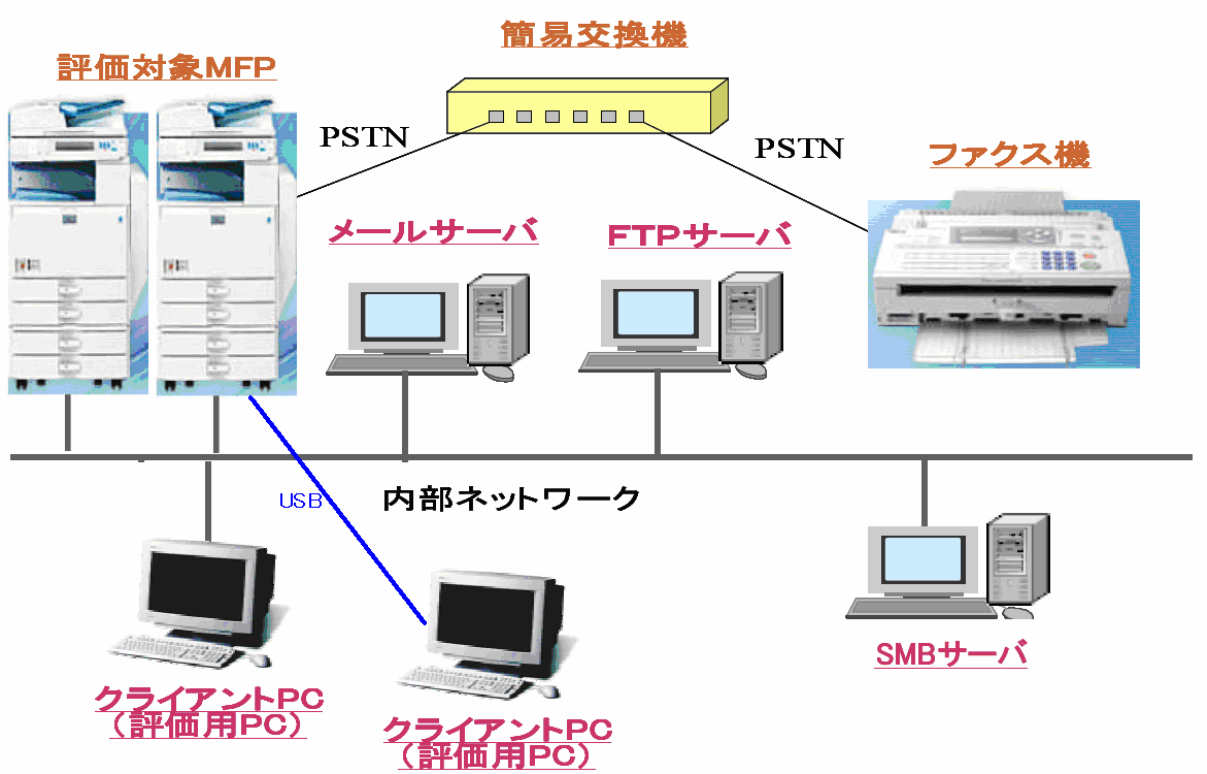

図3-1　開発者テストの構成図

以下に、テスト構成要素の概略を示す。

- 評価対象MFP

  以下の機種がテスト対象となった。

  Aficio MP 2851

  Aficio MP 3351

- クライアントPC

  Webブラウザとしては以下が使用された。

  - Internet Explorer 6.0
  - Internet Explorer 7.0
  - Internet Explorer 8.0

  ドライバは以下が使用された。

  - PCL 6　ドライバ　V1.0.0.0
  - LAN Fax ドライバ　V1.61

- メールサーバ

  SMTPサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- FTPサーバ

  FTPサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- SMBサーバ

  SMBサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- ファクス機

  ファクス機能を持つ機器として、Ricoh Aficio MP 2851、Ricoh Aficio MP 3351が使用された。

- 簡易交換機

  公衆回線と同等とみなせる機器としてTLE-101Ⅲ(エル・エス・アイジャパン社製)が使用された。

「Ricoh Aficio MP 2851/3351」以外の機種(「Savin 9228/9233」、「Lanier LD528/LD533」、「Lanier MP2851/3351」、「Gestetner MP 2851/3351」、「nashuatec MP 2851/3351」、「Rex-Rotary MP 2851/3351」、「Infotec MP 2851/3351」)は、「Ricoh Aficio MP 2851/3351」のOEM製品であり、各地域によって異なる製品名としている。よって、「Ricoh Aficio MP 2851/3351」とこれ以外の機種は、製品名の違い以外は、全く同一機種である。「Ricoh Aficio MP 2851」と「Ricoh Aficio MP 3351」は、印刷速度(28枚/分、33枚/分)の違いがあるが、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。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

テストは、主として、想定されるTOEの利用方法(操作パネルの操作、内部ネットワークまたはUSBで接続されたクライアントPCの操作、ファクス機の操作)によりTOEの外部インタフェースを刺激し、結果を目視観察する方法で行われた。そのような方法が適切でない場合もあり、その場合は以下のような手法が使用された。

①パケットキャプチャソフトを使用して内部ネットワークを流れる通信をキャプチャし、通信プロトコル（SSL、IPSec）を確認する

②TOE内部の動作を確認するためにデバッグ情報を出力する内部ツールを使用し、出力されたデバッグ情報を確認する。

③MFP制御ソフトウェアの完全性確認機能を確かめるために、MFP制御ソフトウェアを「完全性が損なわれたもの」に差し替え、デバッグ情報を出力する内部ツールを使用し、出力されたデバッグ情報を確認する。

さらに、Webアプリケーションの脆弱性を検出するための脆弱性診断ツールを使用した、Webインタフェースの脆弱性の診断も実施された。

b. 実施テストの範囲

テストは、開発者によって513項目(1008件)が実施されている。

カバレージ分析が実施され、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ている。深さ分析が実施され、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ている。

c. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

3.3.2 評価者独立テスト

1) 評価者独立テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

評価者が実施したテストの構成を図3-1に示す。

- 評価対象MFP

  以下の機種がテスト対象となった。

  Aficio MP 2851

  Aficio MP 3351

- クライアントPC

  Webブラウザとしては以下が使用された。

  - Internet Explorer 6.0
  - Internet Explorer 7.0
  - Internet Explorer 8.0

  ドライバは以下が使用された。

  - PCL 6　ドライバ　V1.0.0.0
  - LAN Fax ドライバ　V1.61

- メールサーバ

  SMTPサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- FTPサーバ

  FTPサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- SMBサーバ

  SMBサーバ機能を持つソフトウェアとして、Windows Server 2003 SP2が使用された。

- ファクス機

  ファクス機能を持つ機器として、Ricoh Aficio MP 2851、Ricoh Aficio MP 3351が使用された。

- 簡易交換機

  公衆回線と同等とみなせる機器としてTLE-101Ⅲ(エル・エス・アイジャパン社製)が使用された。

評価者テストのTOE構成は、開発者テストのTOE構成と同一のTOEテスト環境で実施されている。よって、評価者テストは、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。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、以下の観点に基づき、独自にテスト項目を40項目、考案した。

(観点1) テストの厳密さを増すために、開発者が実施したテストを、パラメータや条件を変更して実施する。

(観点2) 通信の保護のための特徴的なセキュリティ機能(SSL、IPSec、S/MIME)について、これらの機能が必ず有効に動作することを確認するための補完的なテストを実施する。

開発者テストのサンプリングは、テスト対象のセキュリティ機能とインタフェースのテストをカバーし、かつ以下の観点も考慮した192項目を選択した。

- 以下のセキュリティ機能の正しい動作を確信したい重要なふるまいについて、重点的に選択する。
  - 蓄積文書に対するアクセス制御機能における各種条件の組合せ
  - セキュリティ管理機能における操作許可者と許可操作の組合せ
  - 認証失敗時アクションにおける各種条件の組合せ
  - ソフトウェア正当性検証機能の動作確認
  - パスワード強度チェックの機能
  - パスワード失敗によるロックアウト機能とロックアウト解除機能
  - 蓄積文書の暗号化機能
  - TOE初期起動時の暗号化に関する自己テスト機能
  - ネットワーク通信データ保護機能
- 監査ログの網羅性に関するテスト、および取得した監査ログ記録の内容を確認するテストが含まれること。
- すべてのインタフェース種別(操作パネル、Webインタフェースなどの分類)が含まれること。

b. 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。

(観点1)については、開発者テストと同様のテスト手法により、例えば以下のようなテストが実施された。

- 同一の文書への操作が競合する場合の開発者テストにおいて､操作するインタフェースの組み合わせが異なる場合のテスト
- アクセス制御の開発者テストにおいて､操作するインタフェースと役割の組み合わせが異なる場合のテスト

(観点2)については、SSL、IPSec、S/MIMEが無効な状態であることが懸念される設定及び環境において、TOEが、SSLやIPSec、S/MIMEによる暗号化がされていない通信を行わないことを確認するテストを実施した。SSL、IPSecの場合は、通信の内容を確認するためにパケットキャプチャソフトによって通信をキャプチャする。S/MIMEの場合は、メールが送信されないことをクライアントPCから確認する。

開発者テストからサンプリングされたテストは、開発者テストと同様のテスト手法により実施された。

c. 結果

実施したすべての評価者の独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

3.3.3 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、必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

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。

表3-1　懸念される脆弱性

No.	懸念される脆弱性
V1	WebブラウザからTOEにアクセスする際にCGIを直接コールすることにより、識別認証の手順を踏まないでTOEにアクセスできるかもしれない。
V2	管理者IDと同じユーザIDで一般利用者を登録することにより、一般利用者でログイン時に管理者役割が付与されるかもしれない。
V3	操作パネル、Webブラウザにおいて、識別認証前にTOEの保護資産にアクセスできるインタフェースが存在するかもしれない。
V4	一般ユーザIDと管理者IDが区別されず、管理者と同じIDの一般ユーザが登録できて、管理者の権限を取得することができるかもしれない。
V5	USBポートから不正なプログラムが起動され、保護資産が漏洩するかもしれない。および、TOEのUSBポートにPCを接続することにより、不正にHDDアクセスできるかもしれない。
V6	起動時のHDDチェックでエラーが発生してHDD初期化のシーケンスに入ったときに、セキュアでない状態になる場合があるかもしれない。
V7	MFP起動中に、操作パネル、WebブラウザからTOEアクセスを行うことにより、セキュアな初期状態になる前にTOEにアクセスできるかもしれない。
V8	TOEが意図しないTCP/IPポートを開放していることにより、そのポートを利用してSFR実施に影響を与えることができるかもしれない。
V9	クロスサイトスクリプティング、クロスサイト・リクエスト・フォージェリの脆弱性

b.　実施テストの範囲

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、以下の侵入テストを実施した。

表3-2　侵入テストの概要

No.	侵入テストの概要	懸念される脆弱性
T1	開放しているポートの確認 LANポートにポートスキャンを実施し、不要なポートが開かれていないことを確認する。	V8
T2	開放しているポートへの侵入テスト LANポートを経由したリモートPCから、TOEのOSに直接アクセスができないことを確認する。	V8
T3	Webからの不正文書アクセス 許可されない利用者が、URLリンク配信情報を用いて直接URL指定しても、文書にアクセスできないことを確認する。	V1

No.	侵入テストの概要	懸念される脆弱性
T4	直接URLを使っての各種システム情報取得 TOEが使用するURLの内容から保護資産、TOE資源のURLを推測しても、アクセスが拒否されることを確認する。	V1
T5	Webインタフェースから識別認証不要なTOEアクセスの正当性確認 Webインタフェースから識別認証を経由しないで使用できるセキュリティ機能がないことを確認する。	V3
T6	操作パネルからTOEへの識別認証不要なアクセスの確認 操作パネルから識別認証を経由しないで使用できるセキュリティ機能がないことを確認する。	V3
T7	Webアプリケーションの脆弱性の確認 TOEに対する各種Webアクセスについて、脆弱性ツールを用いて、脆弱性の有無を確認する。	V9
T8	初期化時のTOEアクセスの確認 初期化中、Webインタフェースおよび操作パネルからTOEへアクセスし、セキュアな状態になる前にTOEが使用可能となるような脆弱性の有無を確認する。	V6、V7
T9	USBポートの悪用 USBポートに接続したPCから、プリント、FAX以外のTOEの操作ができないことを確認する。	V5
T10	利用権の無いユーザによる認証なしの操作 Webインタフェースからのアクセス中に、他の利用者に切り替えた場合、識別認証が行われることを確認する。	V2、V3
T11	同一IDでの誤識別認証 同一IDで、別役割を持つ利用者が登録できないことを確認する。	V4

c. 結果

実施した評価者侵入テストでは、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。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

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

認証機関は、本ST及び評価報告書において、問題点が存在しないことを確認し、本認証報告書を発行した。

5 結論

5.1 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に対する保証要件を満たすものと判断する。

5.2 注意事項

5.2.1 保護の対象となる資産についての注意

以下のデータは、本認証においては保護の対象ではない。

- ファクス機能によりTOEが受信したデータ

5.2.2 利用が制限される設定及び機能についての注意

本製品は、本製品の一部の設定項目が指定された設定を継続的に満たしている場合のみ、評価した対象と一致すると定めている。これは、指定された設定でない状態が存在した場合、製品自体への変更が行われた可能性を否定できないため、「本認証のTOEではない」ということを意味する。具体的な設定項目と制限については、「1.2.3.1 TOEの範囲」参照のこと。

TOEが持つ一部の機能には、その機能の使用が制限されるものがある。これは、TOEの管理者がそのような機能を使用しない、または利用者に使用させないようにしなければTOEを安全に使用できないためである。具体的に制限される機能については、「2.1.3 操作環境の前提条件」のA.ADMIN参照のこと。

消費者は、本製品を購入する前に、本製品を導入する環境において、製品に期待する設定及び機能と、上記の利用が制限される設定及び機能が、重複しないことを特に気をつけて調査する必要がある。

6 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。

D-BOX	HDD上の文書データを格納する領域の名称。
FCU	ファクスコントローラユニット
FTP	File Transfer Protocol(ファイル転送プロトコル)
HDD	ハードディスクドライブの略称。TOE内に取り付けられたHDDを指す。
Ic Hdd	HDDに書込むデータを暗号化し、HDDから読込むデータを復号するハードウェア装置
Ic Key	暗号処理専用のマイクロプロセッサと、セキュア通信で利用される秘密鍵を含んだEEPROMが内蔵されたチップの名称。 正当性確認や暗号処理などに利用する鍵と乱数の種が保管されている
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竄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。
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。
PSTN	Public Switched Telephone Networksの略で、公衆交換電話網の意味。
RAM	画像メモリとして利用される揮発性メモリ。
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。

SSL	Secure Socket Layer セキュリティーを要求される通信のためのプロトコルである。
USB	Universal Serial Busの略で、コンピュータにさまざまな周辺機器を接続するためのシリアルバス規格の1つである。

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	File Transfer Protocol(ファイル転送プロトコル)を用いて、クライアントとファイルを送受信するためのサーバ。
IPv4プロトコル	現在、広く利用されているインターネットを通じてコンピューター間でデータをやりとりするために定められた手順・規約。32ビットのアドレス表記を用いる。
IPv6プロトコル	広く普及しているIPv4から、アドレス空間の拡大、セキュリティーの強化を図ったもの。128ビットのアドレス表記を用いる。
IP-ファクス	TCP/IPを使用しているネットワークに直接接続されたファクス同士で文書の送受信をする機能のこと。また、電話回線に接続されたファクスに文書を送信することもできる。
MFP管理責任者	MFPを設置する組織の中で、MFPの管理者とスーパーバイザーを選任する権限を持った者(あるいは、組織の責任者)。 例：MFPの購入者、MFPの所有者、MFPを設置する部署の責任者、IT部門の責任者
MFP制御ソフトウェア	TOEに組込むソフトウェアの1つで、TOEを識別する要素のうち、System/Copy、Network Support、Scanner、Printer、Fax、WebSupport、Web Uapl、Network Doc Box を含んでいる。 MFPを構成するユニットやデバイスのリソース管理を行ない、動作を制御する。
MFP制御データ	MFPの動作を決定する設定値項目の総称。
PCファクス送信	クライアントPCをネットワークまたはUSBで接続し、クライアントPC内の文書データを、TOEを介してファクス送信する機能のこと。
S/MIME利用者情報	S/MIMEを利用するにあたって必要となる一般ユーザー毎の情報。メールアドレス、ユーザー証明書、S/MIME利用規定値が含まれる。
SMBサーバ	Server Message Block(サーバメッセージブロック)プロトコルを用いて、クライアントとファイルを共有するためのサーバ。
SMBプロトコル	Server Message Block(サーバメッセージブロック)と呼ばれるコンピューター間でデータをやりとりするために定められた手順・規約。

SMTPサーバ	Simple Mail Transfer Protocol(簡易メール転送プロトコル)を用いて、電子メールを送信するためのサーバ。
アドレス帳	一般ユーザー情報をレコードとして登録したデータ。
イーサネット	イーサネット(Ethernet)は、コンピュータネットワークの規格のひとつで、世界中のオフィスや家庭の通信ネットワークで、最も一般的に使用されている技術規格である。さらに100BASE-TX、10BASE-Tなどの細かな規格がある。
インターネットファクス	ファクスの原稿を読込んでからE-Mail形式に変換し、インターネットを使ってメールアドレスを持っている機器に送信する機能のこと。
スーパーバイザー	TOE の許可利用者のひとつで、管理者のパスワードを管理する者。
ネットワーク管理	管理者役割のひとつで、TOEネットワーク接続の管理を実施する役割。ネットワーク管理の役割を持った管理者をネットワーク管理者と言う。
パケットキャプチャソフト	ネットワークに流れる通信を傍受して、通信を記録したり、中身を閲覧したりできるソフトウェア。
パスワード最小桁数	登録可能なパスワードの最小桁数。
パスワード複雑度	登録可能なパスワードの文字種組合せ数の最小数。 文字種は、英大文字、英小文字、数字、記号の4種がある。 パスワード複雑度には、複雑度1と複雑度2がある。複雑度1の場合は2種類以上の文字種、複雑度2の場合は3種類以上の文字種を組合せてパスワードを作らなければいけない。
フォルダ配信	TOEからネットワーク経由でSMBサーバ、FTPサーバのフォルダに文書データを送信する機能のこと。
プロセッサ	コンピュータの中で、ソフトウェアを動作させるためのハードウェアであり、演算器、周辺回路、命令や情報を格納するメモリから構成される。
ベーシック認証	インターネット上で利用者を識別して正当性を検証する最も基本的なユーザ認証方式。HTTPが標準で対応しており、多くのWebサーバとWebブラウザが対応している。ユーザー名とパスワードによりアクセスの可否を検証する。
メール送信	TOEから文書データを添付した電子メールを送信する機能のこと。
メモリ送信	スキャンした原稿をメモリに蓄積してからダイヤルし、ファクスデータをファクス送信する機能のこと。
ユーザー管理	管理者役割のひとつで、一般ユーザーの管理を実施する役割。 ユーザー管理の役割を持った管理者をユーザー管理者と言う。

ロックアウト	特定の利用者IDに対してTOEへのアクセスを禁止すること。
一般ユーザー	TOEの許可利用者のひとつで、TOEの基本機能を利用する者。
一般ユーザー情報	一般ユーザーに関する情報をデータ項目として構成されるレコード。データ項目には、一般ユーザーID、一般ユーザー認証情報、文書データデフォルトアクセス権リスト、S/MIME利用者情報が含まれる。
印刷データ	クライアントPC内の文書を、印刷またはファクス送信するためにクライアントPCからTOEへ送信するデータ。印刷データを印刷するためにはプリンタドライバ、ファクス送信するためにはファクスドライバをクライアントPCにインストールしておく必要がある。 印刷データはネットワークユニット及びUSBポートからTOEに取り込まれる。
印刷条件	印刷時の用紙サイズ、変倍率、加工印刷情報(両面、集約など)のこと。
外部ネットワーク	MFPが設置されている組織が管理できないネットワーク。一般的には汎用インターネットのことを指す。
管理者	TOEの許可利用者のひとつで、TOEを管理する者。管理者には、管理者役割が付与され、管理者役割に沿った管理作業を実施する。管理者は4名まで登録でき、1つ以上の管理者役割が付与される。
管理者役割	管理者に付与する管理機能。管理者役割にはユーザー管理、機器管理、ネットワーク管理、文書管理の4つがあり、それぞれの管理者役割は、登録されている管理者のいずれかに割り当てられる。
機器管理	管理者役割のひとつで、機器の管理、及び監査を実施する役割。機器管理の役割を持った管理者を機器管理者と言う。
操作パネル	タッチパネル付き液晶ディスプレイ、ハードキー、LEDで構成され、利用者がMFPの操作に利用する表示入力装置。 操作パネルユニットとも言う。
蓄積データ保護機能	HDDに記録されている文書データを漏洩から保護する機能。
蓄積印刷	TOEが受信した印刷データを文書データに変換しD-BOXに蓄積する機能のこと。D-BOXに蓄積した文書データは、後から印刷することができる。
蓄積文書ファクス送信	予めファクス送信のためにD-BOXに蓄積されている文書データをファクス送信する機能のこと。
直接印刷	TOEが受信した印刷データを、用紙に印刷する機能のこと。

直接送信	原稿スキャン前にダイヤルし、原稿をスキャンしながらファクスデータをファクス送信する機能のこと。
内部ネットワーク	MFPが設置されている組織が管理するネットワーク。通常はイントラネットとして構築されているオフィス内LAN環境のこと。
文書データ	MFPの許可利用者が、以下に記す2通りの操作のいずれかでMFPに取込んだ電子データ。 1. MFPの許可利用者の操作によって、紙原稿のイメージをスキャンしデジタル化した電子データ。 2. MFPの許可利用者がMFPに送信した印刷データを、MFPが受信しMFPが扱う形式にした電子データ。
文書データデフォルトアクセス権リスト	一般ユーザー情報のデータ項目のひとつ。 新規で蓄積する文書データの文書データ利用者リストに設定するデフォルト値のこと。
文書データ利用者リスト	文書データ毎に設定される一般ユーザーのアクセス制御リスト。
文書管理	管理者役割のひとつで、TOEに蓄積されている文書データが保存されているD-BOXと、文書データのアクセス制御リストである文書データ利用者リストの管理を実施する役割。文書管理の役割を持った管理者を文書管理者と言う。

7 参照

[1] Aficio MP 2851/3351 series with Fax Option Type 3351 セキュリティターゲット　バージョン 1.00　2010年6月17日　株式会社リコー

[2] 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

[3] 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

[4] 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

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2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2版 2007年9月 CCMB-2007-09-002　(平成20年3月翻訳第2.0版)

[10] 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2版 2007年9月 CCMB-2007-09-003　(平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] 株式会社リコー Aficio MP 2851/3351 series with Fax Option Type 3351 評価報告書 第1.6版 2010年6月18日 一般社団法人 ITセキュリティセンター 評価部