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**2**月**22**日** (IT**認証**0292)
認証番号	C0274
認証申請者	**株式会社リコー**
TOE**の名称**	**以下のいずれかの製品名の**MFP**に**Fax Option**を装着したもの** **＜日本国内向け機種＞** MFP**製品名**: imagio MP 6001 SP, imagio MP 7501 SP Fax Option: imagio FAX**ユニット　タイプ**18 **＜海外向け機種＞** MFP**製品名**: Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP Fax Option: Fax Option Type 9001
TOE**のバージョン**	MFP**バージョン**: **ソフトウェア**　System/Copy　1.15 Network Support　8.65 Scanner　01.19 Printer　1.15 Fax　02.00.00 Web Support　1.09 Web Uapl　1.05 Network Doc Box　1.04 **ハードウェア**　Ic Key　1100 Ic Ctlr　03 FCU**バージョン**:　GWFCU3-16(WW)　02.00.00
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9月28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Fax Optionを装着したもの　＜日本国内向け機種＞MFP製品名:imagio MP 6001 SP, imagio MP 7501 SP　Fax Option: imagio FAXユニット タイプ18
＜海外向け機種＞MFP製品名:Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP　Fax Option: Fax Option Type 9001」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Fax Optionを装着したもの　＜日本国内向け機種＞MFP製品名:imagio MP 6001 SP, imagio MP 7501 SP　Fax Option: imagio FAXユニット タイプ18　＜海外向け機種＞MFP製品名:Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP, infotec MP 9001 SP　Fax Option: Fax Option Type 9001、MFPバージョン: ソフトウェア System/Copy 1.15, Network Support 8.65, Scanner 01.19, Printer 1.15, Fax 02.00.00, Web Support 1.09, Web Uapl 1.05, Network Doc Box 1.04, ハードウェア Ic Key 1100,Ic Ctlr 03, FCUバージョン: GWFCU3-16(WW) 02.00.00」（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。）が平成22年9月14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、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、コピー機能にスキャナ機能、プリンタ機能、ファクス機能（オプション）を組み合わせた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。ただし、本TOEは、ファクス機能（オプション）を搭載した状態の製品とする。本製品は、一般的な企業のオフィス等の書類を扱う環境において、文書データの入力、蓄積、出力に利用される。

本TOEは、文書データをTOEに蓄積する際やTOE外に送信する際、文書データや文書データを含む通信に対して暗号化を行い、意図しない開示から文書データを保護する機能を有する。また、TOEに蓄積している文書データの操作を特定の利用者だけに許可するために、文書データを扱う機能の実行や文書データの読み書きを制御し、安全なTOEから文書データの蓄積や印刷、送信を提供する。

これらのセキュリティ機能を管理するため、本TOEは、TOEの利用者（一般ユーザー、管理者、スーパーバイザー）に対して、セキュリティ管理機能の不正な操作を防ぐための識別認証を実施し、セキュリティ管理機能の利用を制限することで、許可されていない者からセキュリティ機能を保護している。

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。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

保護資産である文書データを、TOEの利用を許可されていない第三者からの閲覧及び改ざんから保護するために、TOEの利用者に対し利用者の識別と認証を実施、また利用者の役割を確認することでアクセスできる文書データや利用できる機能を制限する。これによりTOEの機能やTOEに蓄積された文書データに対するアクセスは、識別、認証され、機能の利用を許可された利用者のみが可能となる。

許可された利用者が内部ネットワークを経由して文書データをTOEに格納する際、通信途上の文書データの機密性と完全性を確保するために、内部ネットワーク上の通信について、接続されたコンピュータとTOE間での暗号化、及びコンピュータ上とTOE上での復号の機能を有する。これにより、第三者による内部ネットワー

クの盗聴による文書データの漏洩や改ざんを保護することができる。

上記のセキュリティ機能の設定について、TOEのセキュリティ機能の設定を許可されていない者がTOEのセキュリティ機能の変更や停止を行うことを防ぐため、利用者の識別において、スーパーバイザー、管理者を識別し、またスーパーバイザー、管理者が操作できるセキュリティ機能を必要最小限に制限することにより、権限の濫用におけるセキュリティ機能の停止のリスクを防止する。

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している。

本TOEは、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。また、TOEは、TOEの操作パネル、及び内部ネットワークや電話回線、USBを経由して接続されたクライアントコンピュータのプリンタドライバやWebブラウザを介して利用される。

内部ネットワークはIPv4を使用する。内部ネットワークには、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、及びクライアントコンピュータが接続される。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内部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内部ネットワークの境界にファイアウォールを設置して、内部ネットワーク及びTOEを保護する。

本TOEの管理者は、TOEをセキュアに運用するために必要な知識を持ち、TOE、及びTOEを運用するための環境をセキュアに保つ。管理者は、管理者の特権を濫用して、保護資産である文書データを漏洩、改ざんしたり、TOEのセキュリティ機能を無効にする等の不正な行為を行わない。また、MFPを利用する一般ユーザーに対して、TOEをセキュアに運用するために必要な助言や注意を行う。

スーパーバイザーやカスタマー・エンジニアも、TOEをセキュアに運用するために必要な知識を持ち、特権を濫用して、保護資産である文書データを漏洩、改ざんしたり、TOEのセキュリティ機能を無効にする等の不正な行為を行わない。

1.1.3 免責事項

本TOEは、以下の場合において、セキュリティを保証していない。

- 保守機能移行禁止機能の設定を解除した場合は、それ以降、TOE は CC による認証の適用対象外となる。
- 同様に、TOE が以下の設定を有効にした場合も、TOE は CC による認証の適用対象外となる。
  - IPv6 プロトコルの使用
  - IP ファクスやインターネットファクス機能の使用
  - ベーシック認証以外の認証方式の使用
- TOE が受信したファクスデータは、本評価の対象外であり、CC による評価において保証する範囲に含めない。
- アドレス帳データの SD カードへのバックアップ、及びバックアップしたデータからリストアしたアドレス帳データは、本評価の対象外であり、CC による評価において保証する範囲に含めない。
- USB インタフェース上または電話回線上にも「TOE が送受信する文書データや印刷データ」は存在するが、USB インタフェース上または電話回線上の文書データや印刷データの漏洩や改ざんは、本評価の対象外であり、CC による評価において保証する範囲に含めない。

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22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]、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。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Fax Optionを装着したもの

＜日本国内向け機種＞

MFP製品名:

imagio MP 6001 SP, imagio MP 7501 SP

Fax Option:

imagio FAXユニット タイプ18

＜海外向け機種＞

MFP製品名:

Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP,
Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp,
Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp,
Lanier LD370sp, Lanier LD380sp, Lanier LD390sp,
Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP,
Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP,
Gestetner MP 8001 SP, Gestetner MP 9001 SP,
nashuatec MP 6001 SP, nashuatec MP 7001 SP,
nashuatec MP 8001 SP, nashuatec MP 9001 SP,
Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP,
Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP,
infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 SP,
infotec MP 9001 SP

Fax Option: Fax Option Type 9001

バージョン： MFPバージョン:

ソフトウェア	System/Copy	1.15
	Network Support	8.65
	Scanner	01.19
	Printer	1.15
	Fax	02.00.00
	Web Support	1.09
	Web Uapl	1.05
	Network Doc Box	1.04
ハードウェア	Ic Key	1100
	Ic Ctlr	03
FCUバージョン:	GWFCU3-16(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。

TOEの操作パネルに表示されるMFP本体とファクスコントローラユニットのハードウェアとファームウェアの名称、及びバージョンと、TOE構成品一覧の当該記載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について述べる。

TOEは、利用者の紙文書を取り込んだり、ネットワークを経由して接続されたクライアントコンピュータから文書データを受信したりして、TOE内のHDDに機密性のある文書データを保管し、印刷、配布による出力を行う。そのため、TOEは、文書データの受信と保管、出力の処理に関して、セキュリティ機能を持つデジタル複合機(MFP)である。

TOEのセキュリティ機能は、TOEに格納された文書データや設定データを利用者の識別認証とアクセス制御と暗号化によって、内部ネットワーク上の通信データを通信の暗号化によって、第三者による改ざんと漏洩から守る。

また、TOEのセキュリティ機能は、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ソフトウェアであることを確認する機能や、TOE全体の稼働状況の確認、あるいはパスワード入力の連続失敗等のセキュリティ侵害の事象が発生した場合に、その事象を監査ログとして記録する機能等を持つ。

さらにTOEのセキュリティ機能は、セキュリティ機能に関係する設定等を管理する機能と、セキュリティ機能の処理を記録する 機能を有し、想定したTOEのセキュリティ機能の使用方法に違反した場合に対する予防及び検知を行い、これらの実装されたセキュリティ機能を保護する。

3.1 セキュリティ機能方針

TOEは、3.1.1に示す脅威に対抗し、3.1.2に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本TOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1 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へ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の利用者が、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ていない者が、セキュリティ管理機能を不正に利用し、セキュリティ機能を無効化するかもしれない。
T.SALVAGE	攻撃者が、TOEからHDDを持ち去り、文書データを暴露するかもしれない。
T.TRANSIT	攻撃者が、TOEが送受信した文書データと印刷データを内部ネットワーク上で不正に入手し、漏洩または改ざんするかもしれない。 (注) USBインタフェース上または電話回線上にも「TOEが送受信する文書データと印刷データ」は存在するが、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。

3.1.1.2 脅威に対するセキュリティ機能方針

本TOEは、表3-1に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.ILLEGAL_USE」への対抗

攻撃者がTOEに不正にアクセスし文書データを操作する恐れ「T.ILLEGAL_USE」には、以下の利用者の識別認証と監査によって対抗する。

TOEの機能を利用しようとする者（以下「操作者」という。）に対し、TOEは、利用者IDと認証情報（以下「パスワード」という。）の入力を求める。TOEは、入力された利用者IDとパスワードが正当なものであるかどうかを確認する。TOEが、操作者が入力した利用者IDとパスワードを確認した結果、操作者は、以下の1)、2)のいずれかの状態に分かれる。

1) 操作者が入力した利用者 ID とパスワード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る者は、正当な利用者 ID とパスワードを持ち、TOE の利用を許可されていない者は、正当な利用者 ID とパスワードを持たない。したがって、正当な利用者 ID とパスワードを持たない操作者は、TOE の利用を許可されていない者として、TOE の機能を利用できない。
2) 操作者が入力した利用者 ID とパスワード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。TOE は、この TOE の利用を許可された操作者（以下「利用者」という。）の役割に応じて、TOE の機能の利用を許可する。

TOEは、利用者IDとパスワード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。

1) 同じ利用者 ID で、連続して認証に失敗した場合、その回数が規定回数に達したときに、TOE はその利用者 ID をロックアウトする（その利用者 ID を用いた認証を行わないようにする）。
2) パスワードの登録または変更を要求されたときに、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。
3) 利用者 ID とパスワードの入力を監査ログとして記録し、利用者 ID とパスワードの入力試行によるなりすましの事後検出を可能にする。

以上により、TOEの利用を許可されていない者は、TOEの機能を利用できないことから、攻撃者がTOEに不正にアクセスし文書データを操作する恐れ「T.ILLEGAL_USE」は、利用者の識別認証と監査によって対抗される。

(2) 脅威「T.UNAUTH_ACCESS」への対抗

TOEの利用者が利用権限を越えて文書データにアクセスする恐れ「T.UNAUTH_ACCESS」には、利用者の識別認証と保護資産のアクセス制御によって対抗する。

TOEは、利用者からTOEの機能の利用を要求された場合、利用者の役割に応じて、そのTOEの機能を利用する権限があるかどうかを判断し、機能を利用する許可を与える。TOEに用意された役割は、以下のとおりである。

- 一般ユーザー
- スーパーバイザー
- 管理者
  管理者の場合、さらに以下の役割が与えられる。以下の役割は排他的ではなく、一人の管理者に対して複数の役割を与えてもよい。
  - ユーザー管理
  - 機器管理
  - ネットワーク管理
  - 文書管理

以下に、利用者の役割とTOEの機能と文書データの利用権限の関係を示す。

1) 一般ユーザーの場合
   一般ユーザーには、以下のMFPの基本機能とセキュリティ機能の一部を能動的に利用する権限が与えられる。

基本機能：

- 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
- Web サービス機能
- 管理機能

セキュリティ機能：

- セキュリティ管理機能
  （文書データ利用者リスト管理機能、一般ユーザー情報管理機能等）

文書データには、文書データ利用者リストが付加されている。文書データ

利用者リストには、その文書データを利用できる一般ユーザーと文書データ操作権限が記述されている。その文書データを利用できる一般ユーザーは、表3-2に示す文書データ操作権限の有無に応じて、文書データの読み出し、削除、印刷条件の変更、文書データ利用者リストの操作が許可される。また、一般ユーザーは、自分が文書オーナになっている文書データの文書データ利用者リストしか改変できない。また、一般ユーザーは、一般ユーザー情報管理機能を用いて、一般ユーザーIDを変更することもできない。

したがって、他の一般ユーザーが文書オーナになっている文書データの文書データ利用者リストを改変し、文書データを操作することはできない。

表3-2　文書データの操作権限と操作許可の関係（文書オーナ）

許可された操作	文書データ操作権限			
	閲覧	編集	編集／削除	フルコントロール
文書データの読み出し	○	○	○	○
文書データの削除	－	－	○	○
印刷条件の変更	－	○	○	○
文書データ利用者リストの改変 ・文書利用者の新規登録 ・文書利用者の削除 ・操作権限の変更	－	－	－	○

上記より、一般ユーザーには、文書データを扱う基本機能の利用が許可されるが、文書データに対して行える操作の範囲は、文書データ利用者リストによって制限されていることから、TOEの利用者が利用権限を越えて文書データにアクセスする恐れ「T.UNAUTH_ACCESS」は、利用者の識別認証と保護資産のアクセス制御によって対抗される。

2) スーパーバイザーの場合

スーパーバイザーには、以下の基本機能とセキュリティ機能を能動的に利用する権限が与えられている。

基本機能：

- Web サービス機能
- 管理機能

セキュリティ機能：

- セキュリティ管理機能
  （管理者情報管理、スーパーバイザー情報管理等、スーパーバイザーに許可された一部機能）

スーパーバイザーは、管理者のパスワードや、スーパーバイザーIDとパスワードを設定する等、管理者の情報やスーパーバイザーの情報を管理する役割をもった利用者である。

3) 管理者（文書管理）の場合

管理者（文書管理）には、以下の基本機能とセキュリティ機能を利用する権限が与えられている。

基本機能：

- ドキュメントボックス機能（削除のみ）
- Web サービス機能
- 管理機能

セキュリティ機能：

- セキュリティ管理機能
  （文書データ利用者リスト管理、管理者情報管理等、管理者（文書管理）に許可された一部機能）

管理者（文書管理）は、文書データ利用者リストの内容に関わらず、管理者（文書管理）という役割によって、全ての文書データの削除と文書データ利用者リストの改変（文書利用者の新規登録、文書利用者の削除、操作権限の変更、文書オーナの変更）が許可される。

上記より、管理者（文書管理）には、全ての文書データに対して、ドキュメントボックス機能の文書データの削除機能の利用が許可される。しかし、管理者（文書管理）は、前提条件「A.ADMIN （管理者の条件)」により、管理者に課せられた作業において、管理者の特権を濫用して悪意を持った不正をしないとする。よって、この場合において、TOEの利用者が利用権限を越えて文書データにアクセスする恐れ「T.UNAUTH_ACCESS」は、除外する。

4) 管理者（ユーザー管理、機器管理、ネットワーク管理）の場合

管理者（ユーザー管理、機器管理、ネットワーク管理）には、以下の基本機能とセキュリティ機能を利用する権限が与えられている。

基本機能：

- Web サービス機能
- 管理機能

セキュリティ機能：

- セキュリティ管理機能
  （管理者情報管理、一般ユーザー情報管理、機器制御データ管理等、管理者に許可された一部機能）

  管理者（ユーザー管理)、管理者（機器管理)、管理者（ネットワーク管理）は、一般ユーザー情報の管理、監査ログの管理、ネットワーク接続の管理等の役割をもった利用者である。

以上より、TOEの利用者が利用権限を越えて文書データにアクセスする恐れ「T.UNAUTH_ACCESS」は、一般ユーザーに存在する可能性がある。しかし、全ての一般ユーザーは、利用者IDとパスワードによって識別認証され、文書データ利用者リストによって、文書データに対して行える操作の範囲を制限されている。したがって、「T.UNAUTH_ACCESS」は、利用者の識別認証と保護資産のアクセス制御によって対抗される。

(3) 脅威「T.ABUSE_SEC_MNG」への対抗

セキュリティ管理機能の利用を許可されていない者が、セキュリティ管理機能を不正に利用する恐れ「T.ABUSE_SEC_MNG」には、以下の利用者の識別認証とセキュリティ管理、監査によって対抗する。

MFPの利用者の識別認証については、「(1) 脅威「T.ILLEGAL_USE」への対抗」と、「(2) 脅威「T.UNAUTH_ACCESS」への対抗」で述べたとおりである。

利用者は、その役割に応じて、セキュリティ管理機能の利用が許可される。利用者とその役割、役割に応じて利用が許可されたセキュリティ管理機能の対応は、以下のとおりである。

1) 文書データ利用者リスト管理機能
   - 一般ユーザー（文書オーナ、フルコントロールの権限を持つ文書利用者）
     文書データ利用者リストの問い合わせ
     文書データ利用者リストへ文書利用者を新規登録、削除
     文書データ利用者リストの文書データ操作権限を変更

- 管理者（文書管理）
  文書データ利用者リストの問い合わせ
  文書データ利用者リストへ文書利用者を新規登録、削除
  文書データ利用者リストの文書データ操作権限を変更
  文書オーナの変更

2) 管理者情報管理機能
- スーパーバイザー
  全管理者IDの問い合わせ
  全管理者パスワードの変更

- 管理者
  当該管理者IDの問い合わせ、変更、削除
  他管理者IDの新規作成
  当該管理者パスワードの変更
  当該管理者役割の問い合わせ
  当該管理者役割の削除（他管理者に当該管理者の管理者役割がある場合）
  他管理者へ管理者役割の追加（当該管理者が持つ管理者役割に限る）

3) 一般ユーザー情報管理機能
- 管理者（ユーザー管理）
  一般ユーザーIDの問い合わせ、新規作成、削除
  一般ユーザーパスワードの問い合わせ、新規作成、変更、削除
  S/MIME利用者情報の問い合わせ、新規作成、削除、変更
  文書データデフォルトアクセス権リストの問い合わせ、改変

- 一般ユーザー
  一般ユーザーIDの問い合わせ
  当該一般ユーザーパスワードの問い合わせ、変更
  当該一般ユーザーのS/MIME利用者情報の問い合わせ、新規作成、削除、変更
  当該一般ユーザーの文書データデフォルトアクセス権リストの問い合わせ、改変

4) スーパーバイザー情報管理機能
- スーパーバイザー
  スーパーバイザーIDの問い合わせ、変更
  スーパーバイザーのパスワードの変更

5) 機器制御データ管理機能

- 管理者（文書管理）
  システム時計の日時の問い合わせ
  保守機能移行禁止設定の問い合わせ

- 管理者（機器管理）
  ログインパスワード入力許容回数の問い合わせ、改変
  ロックアウト解除タイマー設定の問い合わせ、改変
  ロックアウト時間の問い合わせ、改変
  システム時計の日時の問い合わせ、改変
  スーパーバイザーのロックアウトフラグの問い合わせ、改変
  HDD暗号鍵の問い合わせ、新規作成
  監査ログの問い合わせ、全削除
  保守機能移行禁止設定の問い合わせ、改変

- 管理者（ユーザー管理）
  パスワード最小桁数の問い合わせ、改変
  パスワード複雑度の問い合わせ、改変
  システム時計の日時の問い合わせ
  保守機能移行禁止設定の問い合わせ
  一般ユーザーのロックアウトフラグの問い合わせ、改変
  フォルダ配信先情報の問い合わせ

- 管理者（ネットワーク管理）
  システム時計の日時の問い合わせ
  保守機能移行禁止設定の問い合わせ

- スーパーバイザー
  システム時計の日時の問い合わせ
  保守機能移行禁止設定の問い合わせ
  管理者のロックアウトフラグの問い合わせ、改変

- 一般ユーザー
  システム時計の日時の問い合わせ
  保守機能移行禁止設定の問い合わせ
  フォルダ配信先情報の問い合わせ

上記より、全てのセキュリティ管理機能1)～5)は、利用者の役割に応じて、利用できる機能を適切に許可している。

セキュリティ管理機能の実施状況を監査ログとして記録し、監査対象としたセキュリティ管理機能に対するセキュリティ侵害の事後検出を可能にする。

以上により、セキュリティ管理機能の利用を許可されていない者が、セキュリティ管理機能を不正に利用する恐れ「T.ABUSE_SEC_MNG」は、利用者の識別認証とセキュリティ管理、監査によって対抗される。

(4) 脅威「T.SALVAGE」への対抗

攻撃者がTOEからHDDを持ち去り、文書データを暴露するかもしれない恐れ「T.SALVAGE」には、メモリ蓄積データの暴露防止と監査によって対抗する。

TOEは、まずBSI-AIS 31に準拠の暗号鍵生成アルゴリズムを用いて鍵長256ビットの暗号鍵を生成する。つぎにTOEは、生成された暗号鍵とFIPS PUB 197に合致する暗号アルゴリズムAESを使って、文書データを暗号化し、HDDに保存する。TOEは、HDDから文書データを読み出すときにこれを復号する。さらにTOEは、起動時に暗号鍵の正当性のテストと、暗号化と復号の処理をするハードウェア「Ic Ctlr」の動作をテストし、暗号化の処理が正常に行われることを確認する。

また、暗号鍵生成と暗号化の処理の結果を監査ログとして記録し、暗号鍵生成と暗号化の処理が正しく行われなかった場合の事後検出を可能にする。

以上により、攻撃者がTOEからHDDを持ち去り、文書データを暴露するかもしれない恐れ「T.SALVAGE」は、メモリ蓄積データの暴露防止と監査によって対抗される。

(5) 脅威「T.TRANSIT」への対抗

攻撃者がTOEが送受信した文書データと印刷データを内部ネットワーク上から不正に入手し、漏洩または改ざんするかもしれない恐れ「T.TRANSIT」には、ネットワーク通信データの保護と監査によって対抗する。

TOEは、文書データをTOEとFTPサーバー間、及びTOEとSMBサーバー間でフォルダ配信する場合、その通信にIPSecプロトコルを使用して、文書データを含む通信を暗号化する。

TOEは、文書データをTOEからクライアントコンピュータへ電子メールで送信する場合、S/MIMEを使用して、文書データを含んだ電子メールデータを暗号化して通信する。

クライアントコンピュータから内部ネットワークを経由してTOEのWebサービスを利用する場合、クライアントコンピュータから内部ネットワークを経由してTOEへ印刷データを送信して印刷する場合、クライアントコンピュータから内部ネットワークを経由して文書データをファクス送信する場合、いずれの場合も内部ネットワーク上の通信はSSLプロトコルを使用して、文書データまたは印刷データを含む通信を暗号化する。

上記のように、内部ネットワーク上を流れるTOEによるWebサービスの通信、及び文書データや印刷データを含む通信を暗号化することによって、文書データや印刷データの漏洩と改ざんに対抗する。ただし、USBインタフェース上、または電話回線上にも、TOEが送受信する文書データや印刷データが存在するが、USBインタフェース上、または電話回線上のデータの漏洩や改ざんは脅威としない。

また、上記の暗号化された通信の実施状況を監査ログとして記録し、暗号化通信が正しく行われなかった場合の事後検出を可能にする。

以上により、攻撃者がTOEが送受信した文書データと印刷データを内部ネットワーク上から不正に入手し、漏洩または改ざんするかもしれない恐れ「T.TRANSIT」は、ネットワーク通信データの保護と監査によって対抗される。

(6) 脅威「T.FAX_LINE」への対抗

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恐れ「T.FAX_LINE」には、電話回線からの侵入防止と監査によって対抗する。

TOEは、ファクスユニットに接続された電話回線から受信したデータの種類がファクスデータのときのみ、ファクスユニットのファクスプロセスからコントローラボードのファクス受信プロセスに受信データを通過させる。

また、電話回線からの侵入防止の実施状況を監査ログとして記録し、電話回線からの侵入防止が正しく行われなかった場合の事後検出を可能にする。

以上により、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恐れ「T.FAX_LINE」は、電話回線からの侵入防止と監査によって対抗される。

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の利用にあたって要求される組織のセキュリティ方針を表3-3に示す。

表3-3 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	正規のMFP制御ソフトウェアであることの証明を消費者へ示すために、TOE内のMFP制御ソフトウェアが正規のソフトウェアであることを確認する手段が提供されていること。

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3-3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.SOFTWARE」への対応

TOEは、MFP制御ソフトウェア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、この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であることを確認できる。

このソフトウェアの完全性確認機能と、TOEが出力するバージョン情報の確認を合わせて、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。

4 前提条件と使用環境

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使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.ADMIN	本TOEの管理者は、TOEをセキュアに運用するために必要な知識を持ち、TOE、及びTOEを運用するための環境をセキュアに保つ。管理者は、管理者の特権を濫用して、保護資産である文書データを漏洩､改ざんしたり､TOEのセキュリティ機能を無効にする等の不正な行為を行わない。また、MFPを利用する一般ユーザーに対して、TOEをセキュアに運用するために必要な助言や注意を行う。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。 以下の機能や設定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 • 保守機能移行禁止機能の設定の解除 • IPv6プロトコルの使用 • IP-ファクスやインターネットファクス機能の使用 • ベーシック認証以外の認証方式の使用
A.SUPERVISOR	スーパーバイザーは、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濫用して、保護資産である文書データを漏洩、改ざんしたり、TOEのセキュリティ機能を無効にする等の不正な行為を行わない。
A.NETWORK	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内部ネットワークに接続する場合は、外部ネットワークからTOEへ通信による攻撃が及ばないように、外部ネットワークと内部ネットワークの境界にファイアウォールを設置して、内部ネットワーク及びTOEを保護する。

4.2 使用環境と構成

本TOEはオフィスに設置され、内部ネットワークで接続され、同様に内部ネットワークに接続されたクライアントから利用される。本TOEの一般的な使用環境を図4-1に示す。

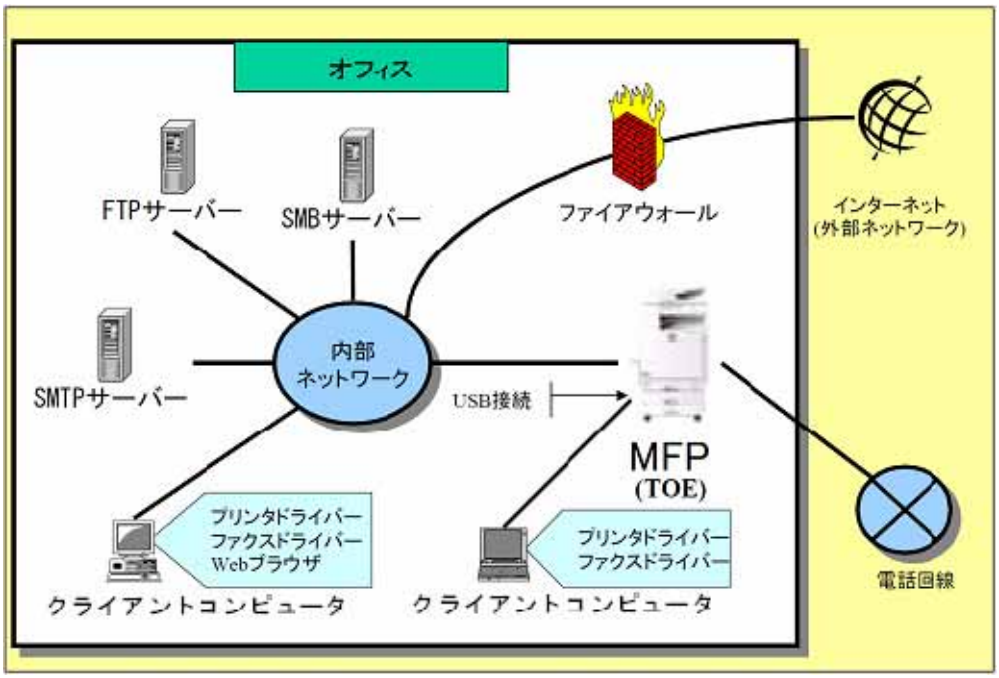

図4-1 TOEの使用環境

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、内部ネットワークや電話回線、USB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内部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内部ネットワークの境界にファイアウォールを設置して、内部ネットワーク及びTOEを保護する。内部ネットワークはIPv4を使用する。内部ネットワークには、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、及びクライアントコンピュータが接続され、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、クライアントコンピュータを使用する場合がある。クライアントコンピュータにプリンタドライバをインストールすることによって、クライアントコンピュータから、内部ネットワークまたはUSBを経由して、TOEへ印刷データを送信し、印刷を行うことができる。また、クライアントコンピュータから内部ネットワークを経由して、TOEへ文書データを送信し、TOEがファクス送信することもできる。クライアントコンピュータ上のWebブラウザから、TOEを操作することもできる。

またTOEは、SMTPサーバーを経由して、クライアントコンピュータへ文書データを電子メールで送信することや、TOEとFTPサーバー間、及びTOEとSMBサーバー間で、文書データをフォルダ配信することもできる。

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。

4.3 使用環境におけるTOE範囲

TOEの基本機能（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）と基本機能が扱う保護資産の情報、セキュリティ機能による保護の関係を表4-2に示す。

表4-2　基本機能とセキュリティ機能が保護対象とする情報の関係

基本機能	説明	保護資産	保護
コピー機能	コピー機能は、紙文書をスキャナエンジンから読み取り、指定された印刷条件に従い、プリンタエンジンから印刷する機能である。読み取ったイメージデータは、文書データ（以下「文書データ（スキャナ機能以外）」という。）としてD-BOXに保存する。	文書データ（スキャナ機能以外）	○
プリンタ機能	クライアントコンピュータから内部ネットワークを経由して印刷データを受信し、すぐに印刷する、または一旦、HDDに蓄積してから印刷する機能である。特にHDDに蓄積してから印刷する場合は、受信した印刷データが、文書データ（スキャナ機能以外）としてD-BOXに暗号化してから保存され、復号してから印刷される。	印刷データ	○
	クライアントコンピュータからUSBを経由して印刷データを受信する場合は、本評価の対象外である。	文書データ（スキャナ機能以外）	—(※)

※ 「1.1.3 免責事項」「8.2 注意事項」を参照。

基本機能	説明	保護資産	保護
ファクス機能（受信）	接続された電話回線からファクスデータを受信し、印刷またはHDDに蓄積する機能である。特にHDDに蓄積する場合は、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（暗号化してから）保存する。ただし、ファクス受信データは、本評価の対象外である。	ファクス受信データ	—(※)
ファクス機能（直接送信・メモリ送信）	紙文書をスキャナエンジンから読み取り、すぐに電話回線でファクスを送信する、または一旦、メモリに蓄積してから電話回線でファクスを送信する機能である。すぐに送信する場合（以下「直接送信」という。）は、送信先のファクス装置に電話回線を接続後、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装置に逐次送信する。メモリに蓄積してから送信する場合(以下「メモリ送信」という。）は、原稿をスキャンしてメモリに蓄積し終えてから、送信先のファクス装置に電話回線を接続してイメージデータを送信する。	なし	○
ファクス機能（蓄積文書ファクス送信）	D-BOXに保存されている文書データ（スキャナ機能以外）を復号して送信先のファクス装置に電話回線で送信する機能である。ただし、文書データ（スキャナ機能以外）が電話回線に送出された後は、本評価の対象外である。	文書データ（スキャナ機能以外）	—(※)
ファクス機能（PCファクス送信）	クライアントコンピュータから内部ネットワークを経由して印刷データを受信し、電話回線でファクスを送信する機能である。	印刷データ	○
	クライアントコンピュータからUSBを経由して印刷データを受信する場合は、本評価の対象外である。	印刷データ	—(※)

※ 「1.1.3 免責事項」「8.2 注意事項」を参照。

基本機能	説明	保護資産	保護
ファクス機能（IP-ファクス）	ファクス機能（IP-ファクス）は、本評価の対象外であるため、これを使用してはならない。	—(※)	—(※)
ファクス機能（インターネットファクス機能）	ファクス機能（インターネットファクス機能）は、本評価の対象外であるため、これを使用してはならない。	—(※)	—(※)
スキャナ機能（読み取り）	紙文書をスキャナエンジンから読み取り、メール送信する。読み取ったイメージデータは、暗号化して電子メールに添付し、指定された電子メールアドレス宛に送信する。	電子メール	○
	紙文書をスキャナエンジンから読み取り、FTPサーバーまたはSMBサーバーの決められたフォルダへ、暗号化されたFTPまたはSMBプロトコルを用いて送信する。	FTPまたはSMB通信	○
	紙文書をスキャナエンジンから読み取り、文書データ（以下「文書データ（スキャナ機能専用）」という。）に変換して、暗号化してD-BOXに保存する。	文書データ（スキャナ機能専用）	○
スキャナ機能（管理）	D-BOXに保存されている文書データ（スキャナ機能専用）を復号したあと、暗号化して電子メールに添付し、指定された電子メールアドレス宛に送信する。	電子メール	○
	D-BOXに保存されている文書データ（スキャナ機能専用）を復号したあと、FTPサーバーまたはSMBサーバーの決められたフォルダへ、暗号化されたFTPまたはSMBプロトコルを用いて送信する。	FTPまたはSMB通信	○
	D-BOXに保存されている文書データ（スキャナ機能専用）を復号して、クライアントコンピュータのWebブラウザが内部ネットワーク経由の暗号化された通信でダウンロードする。	Web通信	○

※ 「1.1.3 免責事項」「8.2 注意事項」を参照。

基本機能	説明	保護資産	保護
ドキュメントボックス機能（読み取り）	紙文書をスキャナエンジンから読み取り、文書データ（スキャナ機能以外）としてD-BOXに暗号化して保存する。「スキャナ機能（読み取り）」によってD-BOXに暗号化して保存された「文書データ（スキャナ機能専用）」は、取り扱うことができない。	文書データ（スキャナ機能以外）	○
ドキュメントボックス機能（管理）	D-BOXに保存されている文書データ（スキャナ機能以外）を復号し、印刷する。	文書データ（スキャナ機能以外）	○
	D-BOXに保存されている文書データ（スキャナ機能以外）を復号して、クライアントコンピュータのWebブラウザが内部ネットワーク経由の暗号化された通信でダウンロードする。	Web通信	○
	D-BOXに保存されているファクス受信データを復号し、印刷する。ただし、ファクス受信データは、本評価の対象外である。	ファクス受信データ	—(※)
管理機能	TOEの機器設定、ネットワークの接続設定、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。	設定情報	○
Webサービス機能	Webサービス機能は、TOEの利用者（一般ユーザー、管理者、スーパーバイザー）がクライアントコンピュータの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「コピー機能」～「管理機能」である。ただし、Webサービス機能からでは、一部、利用できない機能がある。	Web通信（コマンド、文書データ等）	○

※ 「1.1.3 免責事項」「8.2 注意事項」を参照。

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）について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

TOEは、図5-1に示す要素から構成される。TOEは、MFPにオプション製品であるファクスユニット(FCU)を取り付けたものである。

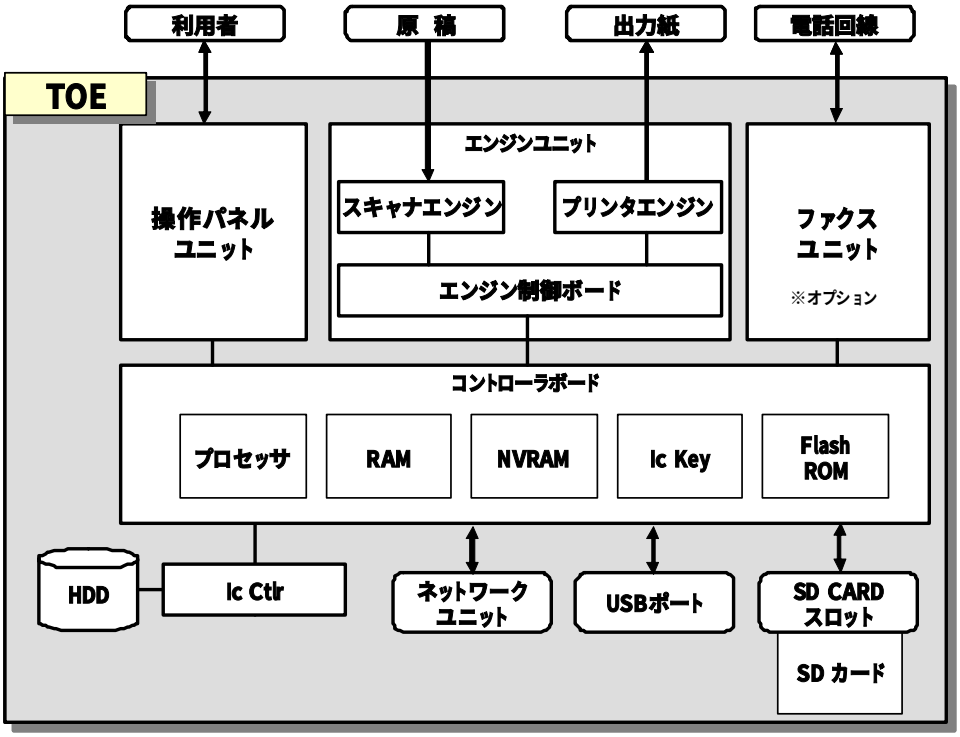

図5-1 TOE境界

TOEを構成する要素、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（オプション）、ネットワークユニット、コントローラボード、Ic Ctlr、HDD、USB ポート、及びSD CARD スロット/SDカードについて説明する。

(1) 操作パネルユニット

操作パネルユニット（以下「操作パネル」という。）は、TOEの利用者がTOEを直接操作するときに使用するTOEに組み付けられた物理的な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。

(2) 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み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。

(3) 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。本TOEは、ファクス機能（オプション）を搭載した状態の製品とする。

(4) 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と接続するためのインタフェース基板である。

(5) 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が搭載された基板である。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。

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、以下のソフトウェアSystem/Copy、Network Support、Fax、WebSupport、Web Uapl、Network Doc Boxから構成される。

(6) Ic Ctlr

Ic Ctlrは、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。

(7) HDD

HDDは、文書データ（スキャナ機能以外）、文書データ（スキャナ機能専用）、印刷データ、ファクス受信データ、識別認証に利用するユーザー情報、監査ログが書き込まれるハードディスクドライブである。文書データ（スキャナ機能以外）、文書データ（スキャナ機能専用）、印刷データ、ファクス受信データを保存する領域は、D-BOXと呼ばれる。

(8) USB ポート

USBポートは、クライアントコンピュータとTOEをUSB接続し、クライアントコンピュータから印刷あるいはファクス送信するために使用する。

(9) SD CARD スロット/SD カード

SD CARD スロットには、MFP制御ソフトウェアScannerとPrinterがインストールされたSDカードが挿入される。このMFP制御ソフトウェアは、MFPへ読み込まれ、TOEとして動作する。また、カスタマー・エンジニアは、SDカードを使った保守作業をするためにSD CARD スロットを使用する。SD CARD スロットは、TOE側面にあって、通常はカバーで覆われネジ止めされている。カスタマー・エンジニアは、保守作業する際に、このカバーを外してSDカードを出し入れする。TOEの設置時には、蓄積データ保護機能の有効化とHDD暗号化オプションの初期設定に使われる。本認証では、運用中の保守作業を想定しないため、設置時のみの使用となる。

5.2 IT環境

TOEは、内部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、及びクライアントコンピュータと通信を行う。またTOEは、USB接続されたクライアントコンピュータ、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。

TOEは、内部ネットワークを経由して接続された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へは、文書データの送信を行う。

内部ネットワーク及びUSBを経由して接続されたクライアントコンピュータは、プリンタドライバやWebブラウザを介してTOEを利用する。クライアントコンピュータは、文書データ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。

ただし、TOEは、以下の環境や設定を使用してはならない。

- SD カードを使用したアドレス帳のバックアップ/リストア
- IPv6 プロトコルの使用
- IP-ファクスやインターネットファクス機能の使用

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の違いにより、以下の3セットが存在する。英語版は、地域により2種類が存在する。違いを以下に説明する。説明した箇所以外は、同一の内容である。

- 英国英語、米国英語の違い（center:centre、enquirely:inquirely、color:colour）
- 用紙サイズの指定方法の違い
  - A4、B5 等の規格名称による指定（欧州向け）
  - インチによる指定（北米向け）
- 例示されているサンプル画面（日時、表示内容）の違い
- 国によるレギュレーションの記述の違い
  （それぞれの地域、国のレギュレーションを北米、欧州に分けて記述）
- 部番、文書名の違い

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 [日本語版] 日本国内向け製品添付ドキュメント

ドキュメント名	部番
imagio MP 9001/7501/6001 シリーズ使用説明書〈本機をお使いになる方へ〉	D062-7103
imagio MP 9001/7501/6001 シリーズ使用説明書〈トラブル解決編〉	D062-7140A
imagio MP 9001/7501/6001 シリーズ使用説明書〈コピー機能＆ドキュメントボックス機能編〉	D062-7120
imagio MP 9001/7501/6001 シリーズ使用説明書〈ファクス機能編〉	D418-7100
imagio MP 9001/7501/6001 シリーズ使用説明書〈セキュリティー編〉	D062-7150
使用説明書・ドライバー＆ユーティリティーimagioMP 9001/9001T/7501/6001	D066-8750A
imagio MP 9001/7501/6001 シリーズ使用説明書〈セキュリティー機能をお使いの方へ〉	D062-7157
ITセキュリティ評価及び認証制度に基づいた設定でお使いになる管理者の方へ	D062-7107

表6-2 [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	部番
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions About This Machine	D062-7133
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Troubleshooting	D062-7143
9060/9070/9080/9090 MP 6001/MP 7001/MP 8001/MP 9001 LD360/LD370/LD380/LD390 Aficio MP 6001/7001/8001/9001 Operating Instructions Copy and Document Server Reference	D062-7114
Quick Reference Copy Guide	D062-7116
Quick Reference Fax Guide	D418-7105
Quick Reference Printer Guide	D462-7104
Quick Reference Scanner Guide	D462-7124
Manuals for Users 9060/9060sp/9070/9070sp/9080/9080s p/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP LD360/LD360sp/LD370/LD370sp/LD38 0/LD380sp/LD390/LD390sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP	D066-7317

ドキュメント名	部番
Manuals for Administrators 9060/9060sp/9070/9070sp/9080/9080s p/9090/9090sp MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP LD360/LD360sp/LD370/LD370sp/LD38 0/LD380sp/LD390/LD390sp Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP	D066-7318
Notes for Security Functions	D062-7156
Notes for Administrators: Using this Machine in a CC-Certified Environment	D062-7108

表6-3 [**英語版**-2] **欧州向け製品添付ドキュメント**

ドキュメント名	部番
Manuals for This Machine	D062-7102
Quick Reference Copy Guide	D062-7113
Quick Reference Fax Guide	D418-7103
Quick Reference Printer Guide	D462-7102
Quick Reference Scanner Guide	D462-7122
Manuals for Users MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP A	D062-7000

ドキュメント名	部番
Manuals for Administrators Security Reference MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP Aficio MP 6001/MP 6001 SP/MP 7001/MP 7001 SP/MP 8001/MP 8001 SP/MP 9001/MP 9001 SP	D062-7002
Notes for Security Functions	D062-7156
Notes for Administrators: Using this Machine in a CC-Certified Environment	D062-7109

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。

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2月に始まり、平成22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、平成22年4月、5月、6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。本TOEは、米国・欧州・アジアを対象とした製品であるため、日本国内と海外の複数拠点において、TOEの製造と配付が行われている。評価機関は、日本、米国、欧州、アジアの調査が必要な製造現場へ赴き、複数拠点にまたがるTOEの製造・組み立て工程に注意した調査を行った。

また、平成22年6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。

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。

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7-1に示す。

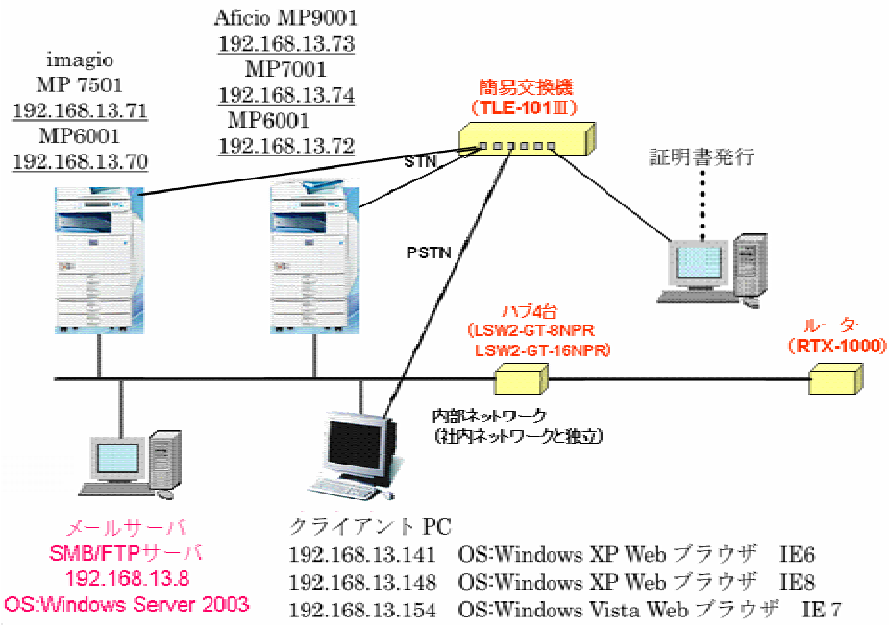

図7-1 開発者テストの構成図

評価の対象としたTOEは、国内機（imagio MP 7501 SP, imagio MP 6001 SP）、海外機（Aficio MP 9001 SP, Aficio MP 7001 SP, Aficio MP 6001 SP）である。

なおTOEは、以下の34機種（imagio MP 6001 SP, imagio MP 7501 SP, Ricoh Aficio MP 6001 SP, Ricoh Aficio MP 7001 SP, Ricoh Aficio MP 8001 SP, Ricoh Aficio MP 9001 SP, Savin 9060sp, Savin 9070sp, Savin 9080sp, Savin 9090sp, Lanier LD360sp, Lanier LD370sp, Lanier LD380sp, Lanier LD390sp, Lanier MP 6001 SP, Lanier MP 7001 SP, Lanier MP 8001 SP, Lanier MP 9001 SP, Gestetner MP 6001 SP, Gestetner MP 7001 SP, Gestetner MP 8001 SP, Gestetner MP 9001 SP, nashuatec MP 6001 SP, nashuatec MP 7001 SP, nashuatec MP 8001 SP, nashuatec MP 9001 SP, Rex-Rotary MP 6001 SP, Rex-Rotary MP 7001 SP, Rex-Rotary MP 8001 SP, Rex-Rotary MP 9001 SP, infotec MP 6001 SP, infotec MP 7001 SP, infotec MP 8001 S

P, infotec MP 9001 SP）を対象としている。これらの名称の違いを、以下に説明する。

- 以下の名称の違いは、販売地域及び販売会社の違いによって、呼称が異なるだけであり、TOE の構成やセキュリティ機能は同一である。
  （imagio MP, Ricoh Aficio MP, Savin, Lanier LD, Lanier MP, Gestetner MP, nashuatec MP, Rex-Rotary MP, infotec MP）
- TOE 名称に含まれる数字の違い（「9001/8001/7501/7001/6001」「9090/9080/9070/9060」「360/370/380/390」）は、TOE の印刷速度（90 枚/分、80 枚/分、75 枚/分、70 枚/分、60 枚/分）の違いのみであり、TOE の構成やセキュリティ機能は同一である。

評価の対象として、国内機（imagio MP 7501 SP, imagio MP 6001 SP）、海外機（Aficio MP 9001 SP, Aficio MP 7001 SP, Aficio MP 6001 SP）のTOEを選択した。印刷速度の違いにより、テスト結果に差異が発生する恐れを考慮し、上記の機種を選択した。それ以外の違いは呼称の違いのみであるため、この組み合わせにより、すべての34機種について、差異を考慮したテストを行った場合と同等とみなすことができる。

開発者テストの構成におけるTOE以外の構成要素について、表7-1に説明する。

表7-1　開発者テストの構成要素

構成要素	詳細
クライアントコンピュータ（3台）	Webブラウザ • Internet Explorer 6.0（IE6） • Internet Explorer 7.0（IE7） • Internet Explorer 8.0（IE8） ドライバ • 国内用 RPCS ドライバ V8.02 PC Fax ドライバ V1.61 • 海外用 PCL6 ドライバ V1.1.0.0 及び V1.0.0.0 LAN Fax ドライバ V1.61
メールサーバー	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
ファクス装置	Ricoh imagio MP 6001 SP、Ricoh Aficio MP 9001 SP
簡易交換機	TLE-101Ⅲ（エル・エス・アイ ジャパン社製）

構成要素	詳細
証明書発行機	Linux (Fedora 8)

開発者テストは、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。

(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

開発者テストで実施されたテストの概要は以下のとおり。

＜開発者テスト手法＞

開発者テストは、想定されるTOEの利用方法（TOEの操作パネルの操作、内部ネットワークまたはUSBで接続されたクライアントコンピュータの操作、ファクス装置の操作）に基づいて、TOEの外部インタフェースを刺激し、その結果を目視観察する方法が採られた。また、TOEのWebインタフェースに対して、Webアプリケーションの脆弱性診断ツールを使用して診断を行い、Webインタフェースの脆弱性も調査した。ただし、テスト結果を目視観察できない場合は、以下の手法が採られた。

- 内部ネットワークを流れる通信は、パケットキャプチャソフトを使用して取得し、通信プロトコル（SSL、IPSec）を確認する。
- 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から、TOE内部の動作を確認する。
- 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から、MFP制御ソフトウェアの完全性確認機能の動作を確認する。

＜開発者テストツール＞

開発者テストにおいて利用されたツールを表7-2に示す。「TOEの内部動作のモニター用デバッグコンソール」と「TOE内部構成要素変更・書換え用SDカード」は開発者によって作成され、正しく動作することが確認された後に使用された。

表7-2　開発テストツール

ツール名称	概要・利用目的
WireShark 1.0. 2	LAN 上を流れるパケットを採取・モニターするツール（ソフトウェア）
Zenmap 4.68	ネットワークに接続されたコンピュータの通信ポートの使用状況を調査するツール（ソフトウェア）
TOEの内部動作のモニター用デバッグコンソール	TOEの内部動作のモニター用デバッグコンソールは、一般的なコンピュータにインストールされたソフトウェア。株式会社リコーがテスト用に開発したツールであり、一般入手は困難である。TOEの内部動作のモニター用デバッグコンソールがインストールされたコンピュータとTOEのコントローラボードは、特殊なデバッグ用シリアルコネクタとシリアルケーブルで接続される。本ツールは、TOE内部動作確認が必要なテスト項目に限定して使用された。
TOE内部構成要素変更・書換え用SDカード	テスト項目に合わせて作成された、TOEの内部構成要素の変更や書換えを行うテスト用プログラムとテスト用データが格納されたSDカード。本ツールは、TOE内部動作の確認が必要なテスト項目に限定して使用された。

＜開発者テストの実施＞

開発者が提供した証拠資料「個別テスト仕様書」の「期待されるテスト結果」に記載されたあらかじめ期待されたテスト計画書の値と、同じく開発者が提供した証拠資料「個別テスト結果報告書」の「個別テスト項目結果記入欄（判定欄）」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とテスト証拠資料の実際のテスト結果が一貫していることが確認できた。

b.　実施テストの範囲

テストは開発者によって516項目（1011件）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。

7.3.2 評価者独立テスト

評価者は、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の再確認のための独立テストを実施した。評価者が実施した評価者独立テストの概要を以下に示す。

(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、図7-2に示すとおりである。

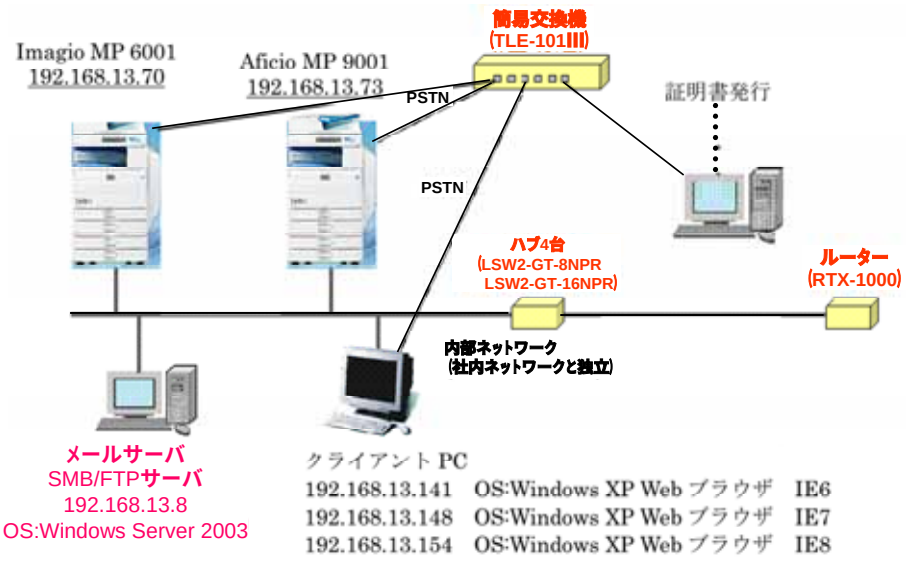

図7-2 評価者独立テストの構成図

評価の対象としたTOEは、imagio MP 6001 SP、Aficio MP 9001 SPである。本評価者独立テストでは、印刷速度の違いによって、評価者独立テストの結果に差異が発生する恐れがないため、上記の構成とした。評価者独立テストの構成におけるTOE以外の構成要素は、Internet Explorer 7.0（IE7）が搭載されたクライアントコンピュータを除いて、開発者テストの構成と同一である。ただし、クライアントコンピュータに搭載されたOSの違いによるInternet Explorer 7.0（IE7）の動作に違いは無いと判断した。よって、評価者独立テストの構成と開発者テストの構成は、同一とみなす。

評価者テストは、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。

(2) 評価者独立テスト概説

評価者の実施した評価者独立テストは以下のとおり。

a. 評価者独立テストの観点

＜独自テスト＞

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での評価者独立テストのうち、独自テスト40項目を考案した。

- (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。

＜サンプリングテスト＞

開発者テストからのサンプリングテストは、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195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、及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インタフェース等の分類）が含まれること。

b. 評価者独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜評価者独立テスト手法＞

独自テストの(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

独自テストの(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のテストの場合は、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のテストの場合は、メールが送信されないことをクライアントコンピュータから確認する。

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。

＜独立テストツール＞

評価者独立テストは､開発者テストにおいて利用した表7-2のツールを用いた。

＜独立テストの実施＞

評価者独立テストのうち独自テスト40項目とサンプリングテスト195項目について、その内容を表7-3と表7-4に示す。

表7-3　実施した独自テスト

項番	テスト項目分類名	テスト項目数
1	アクセス制御（保管文書）	2
2	利用者認証	4
3	ロックアウト	4
4	パスワードポリシー	7

項番	テスト項目分類名	テスト項目数
5	パスワード入力	7
6	TSF 管理/TSF データ管理（パネル経由）	3
7	TSF 管理/TSF データ管理（WIM 経由）	2
8	IPSec	2
9	SSL/TLS	1
10	S/MIME	4
11	同時アクセス	4
合計		40

表7-4　実施したサンプリングテスト

項番	テスト項目分類名	テスト項目数
1	アクセス制御（保管文書）	52
2	利用者認証	9
3	ロックアウト	7
4	パスワードポリシー	8
5	TSF管理/TSF データ管理（パネル経由）	32
6	TSF管理/TSFデータ管理（WIM経由）	44
7	IPSec	2
8	SSL/TLS	3
9	S/MIME	3
10	FAX回線侵入	2
11	バージョン表示	1
12	文書データ作成ログ	5
13	ログ溢れ	2
14	文書操作ログ	3
15	蓄積文書削除	4
16	パスワード入力	9
17	ファーム正当性確認	3
18	HDD データ暗号化	1
19	暗号鍵の生成・更新処理	2
20	ファームウェア構成変更禁止	3
合計		195

c. 結果

実施したすべての評価者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。

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の可能性について、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の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、評価者侵入テストを必要とする以下の懸念される脆弱性を識別した。

表7-5 懸念される脆弱性

項番	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と同じユーザー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	一般ユーザーIDと管理者IDが区別されず、管理者と同じIDの一般ユーザーが登録できて、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。及び、TOEのUSBポートにコンピュータ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。

項番	懸念される脆弱性
V 8	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。
V 9	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
V10	MFP制御ソフトウェアが格納されたSDカードの抜き取り、不正なMFP制御ソフトウェアが格納されたSDカードの差し込みによって、TOEが改変され、誤動作を起こすかもしれない。

b. 評価者侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の評価者侵入テストを実施した。

＜評価者侵入テスト環境＞

テスト環境は、評価者独立テストの環境と同じである。評価者侵入テストの構成図も、図7-2と同一である。本環境は、STの「TOEセキュリティ対策方針」及び「運用環境のセキュリティ対策方針」に従って、TOEがセキュアに設置・運用されている環境を想定した。例えば、外部ネットワークと内部ネットワークの境界において不要なポートは閉じられていることから、インターネット等の外部ネットワークからのネットワーク経由の攻撃は除外する。上記の条件の下で、管理者を除く、一般利用者、攻撃者による一般公開インタフェース及び一般に入手可能なツールを使用して攻撃を行うことを想定する。

評価者侵入テストの構成、使用したツールのうち、開発者テストや評価者独立テストの構成と異なる部分を表7-6に示す。

表7-6　評価者侵入テストの構成要素

構成要素	詳細
侵入テスト用コンピュータ	ハードウェア：Toshiba dynabookSS RX1
	OS：Windows XP Pro SP3
	ブラウザ：Internet Explorer 8.0（IE8）
	ポートスキャン用ソフトウェア：Zenmap 4.76
	回線トレース用ソフトウェア：Wireshark V1.0.6
	UNIX 系アクセスツール：Cygwin V2.573.23
	脆弱性検出ツール：Paros V3.2.13

＜脆弱性テストの実施＞

潜在的な脆弱性の探索において識別された表7-5の懸念される脆弱性について、これと対応する評価者侵入テストを表7-7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、以下の評価者侵入テストを実施した。

表7-7　評価者侵入テスト概要

項番	テスト概要	懸念される脆弱性の項番
T1	開放しているポートの確認	V8
T2	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
T3	開放しているポートへの侵入テスト	V1
T4	リモートクライアントコンピュータから、LANポートを経由して、TOEのOSに直接アクセスができないことを確認する。	V1
T5	Webからの不正文書アクセス	V3
T6	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。	V3
T7	直接URLを指定した各種システム情報取得	V9
T8	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。	V6, V7
T9	Webインタフェースから識別認証しないでTOEへアクセスする方法がないこと確認する。	V5
T10	Webインタフェースから識別認証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。	V2, V3
T11	操作パネルから識別認証しないでTOEへアクセスする方法がないこと確認する。	V4
T12	MFPの起動中や動作中にSDカードが取り出された場合、動作を停止し、警告表示と機器管理者のログイン要求を行うことを検査する。	V10

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。

7.4 評価構成について

本評価では、「7.3.2 評価者独立テスト」及び図7-2に示す構成において、評価を行った。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、上記の評価構成は、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：なし
- セキュリティ機能要件：　コモンクライテリア　パート２ 適合
- 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

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 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。

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。

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

TOEの運用中は、保守機能移行禁止機能を必ず設定しておくことが、ガイダンスに明示されており、本TOEを運用する際の前提条件を遵守する限り、保守モードに移行することはないと想定される。しかし、管理者が保守機能移行禁止機能の設定を解除して、TOE操作モードを保守モードへ変更した場合は、それ以降、TOEはCCによる認証の適用対象外となることに注意すること。

本TOEは、その他にも「1.1.3 免責事項」に記述したように、脅威に対抗できない場合やTOEがCCによる認証の適用対象外となる場合がある。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。

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、公表のため、本報告書とは別文書として、以下のとおり提供される。

imagio MP 7501/6001 シリーズ, Aficio MP 9001/8001/7001/6001 series セキュリティターゲット バージョン 1.00 2010年8月31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。

AES	Advanced Encryption Standard（AES暗号）
BSI-AIS 31	ドイツ連邦情報技術安全局(BSI)の発行したハードウェア乱数発生器のための規格
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
FIPS PUB 197	Federal Information Processing Standards Publication 197（米国連邦情報処理標準 197番 AES暗号についての規格）
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 Ctlr	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等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
NVRAM	MFPの動作を決定する設定値が保存された不揮発性メモリ

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サーバー	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ー
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い、動作を制御する。
PCファクス送信	クライアントコンピュータをネットワークまたはUSBで接続し、クライアントコンピュータ内の文書データを、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サーバー	Server Message Block（サーバー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ー

SMBプロトコル	Server Message Block（サーバーメッセージブロック）と呼ばれるコンピュータ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サーバー	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ー
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等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管理者（ネットワーク管理）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サーバー、FTPサーバー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ー認証方式。HTTPが標準で対応しており、多くのWebサーバーと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管理者（ユーザー管理）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するレコード。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	クライアントコンピュータ内の文書を、印刷またはファクス送信するためにクライアントコンピュータから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コンピュータ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、集約等）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管理者（機器管理）という。
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いう。
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。

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の利用者が、以下に記す2通りの操作のいずれかでMFPに取り込んだ電子データ • MFPの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 • MFPの利用者がMFPに送信した印刷データを、MFPが受信しMFPが扱う形式に変換した電子データ
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管理者（文書管理）という。

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 1 September 2006 CCMB-2006-09-001

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

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

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0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2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

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

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[12] imagio MP 7501/6001 シリーズ, Aficio MP 9001/8001/7001/6001 series セキュリティターゲット バージョン 1.00 2010年8月31日 株式会社リコー

[13] 株式会社リコーimagio MP 7501/6001シリーズ, Aficio MP 9001/8001/7001/6001 series 評価報告書 第1.3版 2010年9月14日 一般社団法人 ITセキュリティセンター 評価部