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26年1月24日 (IT認証4482)
認証番号	C0489
認証申請者	東芝テック株式会社
TOEの名称	TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS
TOEのバージョン	SYS V3.0
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	東芝テック株式会社
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27年11月27日

技術本部
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 Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

評価結果：合格

「TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、東芝テック株式会社が開発した「TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS バージョン SYS V3.0」（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 27 年 11 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東芝テック株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、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、コピー機能、プリント機能、スキャナ機能、ファイリング機能、インターネットファクス機能などを有するデジタル複合機である。

本 TOE は、上記の基本機能に加えて、基本機能で扱う利用者文書データやセキュリティに影響する設定データなどを漏えいや改ざんから保護するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下の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。

保護資産である利用者文書データやセキュリティに影響する設定データに対して､TOE の利用が許可されていな第三者からの閲覧及び改ざん､また権限外の利用者への漏えいなどの脅威がある。

これらの脅威に対抗するために、本 TOE は利用者の識別認証、利用者役割及び操作権限によるアクセス制御､データ暗号化､監査ログ生成などの機能を提供する。

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。

TOE の HDD 上書き消去機能を有効化するオプションキット「GP-1070」を購入し、これによって TOE の HDD 上書き消去機能が有効化されていること。

ハードウェア取り外しや分解などの不正な物理的アクセスから保護されるように管理された場所に設置されること。

外部ネットワークからの不正なアクセスから保護されるよう、ファイアウォールなどで保護されたネットワーク環境で使用すること。

1.1.3 免責事項

本 TOE は、HDD に書き込むデータを暗号化する機能を持つ。ただし、この機能は本評価の保証の対象外となる。

本 TOE では、評価されたすべてのセキュリティ機能を有効にするために、TOE をハイセキュリティモードに設定して運用することが前提となる。ハイセキュリティモード以外に設定を変更して運用した場合、それ以降は本評価における保証の対象外となる。

本 TOE は、保守員による保守作業として運用状態から保守モードへ切り替えて行う作業がある。保守モードへ切り替えた時点で、それ以降の本 TOE のセキュリティ機能への影響については評価はなされていないため、本評価の保証の範囲外となる。

本 TOE は､出荷の際に TOE 及び各種ガイダンスを段ボールに梱包した状態で配送を行い、製品引渡し時に梱包の状態を確認することで配送中の TOE の改ざんを検知できることが本評価により保証されている。上記とは別の配送手段として、製

品設置時の効率化のため、TOE を段ボールに梱包せず出荷しての納品も選択可能ではあるが、この配送手段についての評価はなされていないため、保証の対象外となる。

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 セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 27 年 11 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、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： TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS
バージョン： SYS V3.0
開発者： 東芝テック株式会社

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 本体の表面に、TOE 名称が印字されている。操作パネル上のカウンタボタンを押下することによって、TOE のバージョンが操作パネル内の液晶画面に表示される。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOE は、コピー機能、プリント機能、スキャン機能、ファイリング機能、インターネットファクス送信機能、インターネットファクス受信機能などを提供しており、利用者文書データを内部の HDD に保存したり、ネットワークを介して利用者の端末や各種サーバと通信する機能を有している。

TOE は、上記の機能を使用する際に、デジタル複合機用の Protection Profile である IEEE Std 2600.1-2009 [14](以下「PP」という。)で要求されているセキュリティ機能要件を満たすセキュリティ機能を提供する。TOE の提供するセキュリティ機能には、利用者の識別認証とアクセス制御、HDD のデータ削除時の上書き消去、暗号化通信などが含まれており、保護資産である利用者文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。

なお、TOE は、以下の利用者役割を想定している。

・U.NORMAL(一般利用者)
TOE の基本機能であるコピー機能・プリント機能・スキャン機能・ファイリング機能・インターネットファクス送信機能を実行できる利用者。一般利用者は、各基本機能ごとに操作権限を付与され、付与された機能だけを実行できる。

・U.FAXOPERATOR(ファクスオペレータ)
インターネットファクス送信機能及びインターネットファクス受信機能を実行できる利用者。

・U.ADMINISTRATOR(TOE 管理者)
TOE のセキュリティ機能に係わる設定、利用者のアカウント情報の変更、監査ログの閲覧など、TOE 全般の管理権限を持つ管理者。

・U.ACCOUNTMANAGER(アカウント管理者)
利用者のアカウント情報(利用者の役割、利用者に付与される基本機能の操作権限など)の設定が行える管理者。

・U.AUDITOR(監査ログ管理者)
TOE のすべての監査ログの閲覧が許可された管理者。

また、TOE の保護資産は以下となる。

・User Document Data
利用者文書データ。

・User Function Data
TOE の基本機能の実行により生成されるジョブや、または処理に使用されるためのデータ。プリント待ちのプリントジョブ、インターネットファクス送信機能で送信先として使用される e-mail のアドレス帳が該当する。

・TSF Protected Data
セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。利用者のユーザ ID、利用者の役割及び操作権限、TOE のセキュリティに関する設定情報、ネットワーク設定情報が該当する。

・TSF Confidential Data
セキュリティ機能で使用されるデータの中で、完全性及び秘匿性が求められるデータ。監査ログ、利用者のパスワードが該当する。

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。これらの脅威は、PP に記述されているものと同じである。

表3-1 想定する脅威

識別子	脅威
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

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.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらの脅威は、利用者のデータに対する脅威であり、TOE は「User Authentication 機能」、「User Access Control 機能」、「Secure Erase 機能」、「Secure Channel 機能」で対抗する。

「User Authentication 機能」により、識別認証が成功した利用者にのみ TOE の利用を許可する。

「User Access Control 機能」により、利用者文書データ及びジョブへの操作に対して、利用者の利用者役割または操作権限及びユーザ ID を基に、アクセス制御を実施する。TOE 管理者の場合は、すべての利用者文書データに対して操作が許可されるが、TOE 管理者以外の場合、操作要求に該当する操作権限が付与されていて、かつ利用者のユーザ ID と利用者文書データが持つユーザ ID が同じであれば、操作が許可される。

「Secure Erase 機能」により、コピーなどの基本機能の終了時に、利用者文書データが格納されていた HDD の領域を上書き消去する。これにより、削除された利用者文書データの残存情報が HDD から読み出されることを防止する。

「Secure Channel 機能」により、TOE とクライアント PC や各種サーバとの通信に TLS 通信を用いる。これにより、通信データを秘匿し、改ざん及び漏えいを防止することができる。

(2) 脅威「T.PROT.ALT」「T.CONF.DIS」「T.CONF.ALT」への対抗

これらの脅威は、TSF データに対する脅威であり、TOE は「TSF Data Protection 機能」、「User Authentication 機能」、「Secure Channel 機能」で対抗する。

「TSF Data Protection 機能」により、TOE 管理者にのみ、TOE のセキュリティに関する設定情報の管理を許可する。利用者のパスワードについては、利用者本人または TOE 管理者及びアカウント管理者だけが変更を行える。監査ログについては、基本機能の操作に関する監査ログの閲覧は利用者本人または TOE 管理者及び監査ログ管理者のみに制限し、それ以外の監査ログの閲覧は TOE 管理者及び監査ログ管理者のみが行える。

「User Authentication 機能」、「Secure Channel 機能」は(1)と同様である。

以上の機能により、TOE は、TOE の権限外操作や、通信データの不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE 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 3-2 に示す。これらの組織のセキュリティ方針は、PP に記述されているものと同じである。

表3-2 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.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect malfunction of the TOE, procedures will exist to self-verify executable code in the TOE.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

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 3-2 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

TOE は「User Authentication 機能」、「User Access Control 機能」で本方針を実現する。

「User Authentication 機能」により、識別認証が成功した利用者にのみ TOE の利用を許可する。

「User Access Control 機能」により、各基本機能への操作要求に対して、利用者の操作権限を基にアクセス制御を行い、操作要求に該当する操作権限が付与されていれば、操作が許可される。また、利用者文書データ及びジョブへのアクセスは、利用者本人または TOE 管理者のみに制限される。

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

TOE は「TSF Self Protection 機能」で本方針を実現する。

「TSF Self Protection 機能」により、TOE は、全 TSF の実行コード、Hash value-acquiring code の完全性を検証する TSF 自己テストを行い、異常が検出された場合には TOE を使用不可とする。TSF 自己テストの実行は TOE 管理者のみが許可される。

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

TOE は「Audit Data Generation and Review 機能」で本方針を実現する。

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、日時、利用者識別情報、事象の結果(成功/失敗)の項目からなる監査ログを生成する。監査ログについては、基本機能の操作に関する監査ログの閲覧を利用者本人または TOE 管理者及び監査ログ管理者のみに制限し、それ以外の監査ログの閲覧は TOE 管理者及び監査ログ管理者のみが行える。また、すべての監査ログの削除及び出力を TOE 管理者に制限する。

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

TOE は「User Authentication 機能」、「Secure Channel 機能」で本方針を実現する。

「User Authentication 機能」により、識別認証の成功した利用者のみに TOE の利用を許可する。また、利用者が操作をしない状態が規定時間経過した場合には、該当のセッションを無効化する。

TOE の外部インタフェースから入力されたデータに対して、別の外部インタフェースへのデータ転送を行う機能を提供していないことで、TOE を中継してデータを不正に転送することを防止する。

なお、前提条件により、ファイアウォールなどセキュリティ手段によって、外部ネットワークからの不正なアクセスから保護される IT 環境で TOE を利用しなければならない。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を**表 4-1** に示す。これらの前提条件は、PP に記述されているものと同じである。

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	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 運用環境と構成

本 TOE はオフィスに設置され、社内ネットワークに接続をし、同様に社内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。

なお、図 4-1 に示されている TOE 以外の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(十分に信頼できるものとする)。

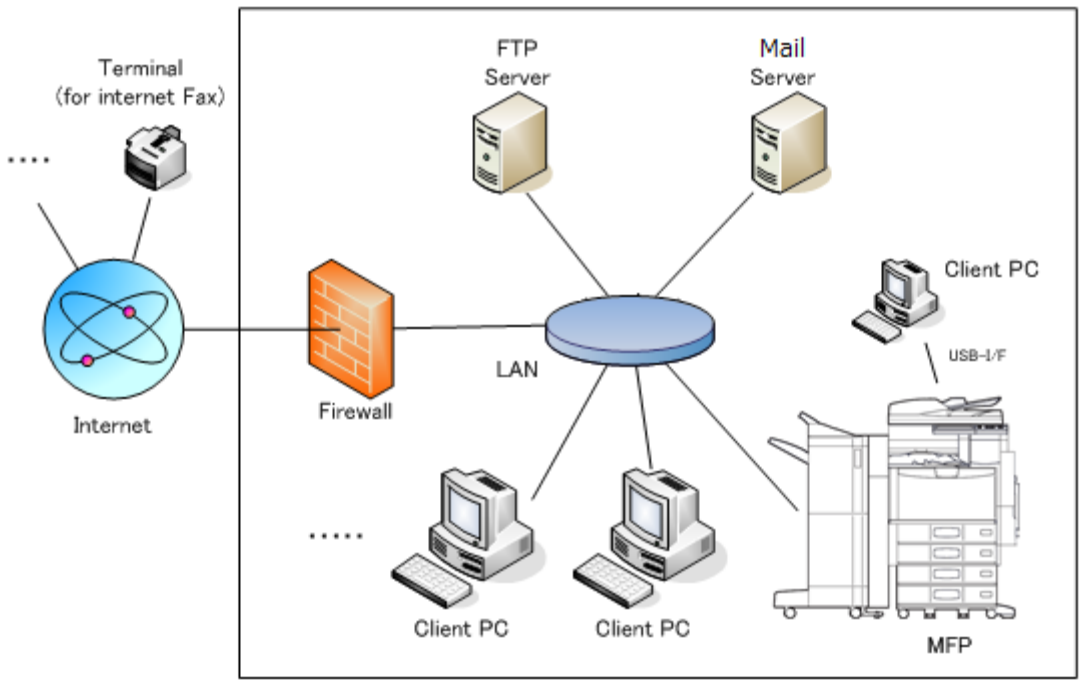

図4-1 TOEの運用環境

(1) クライアント PC

クライアント PC を TOE に対し LAN 接続または USB ケーブルで直接接続させることによって、利用者がプリントなど TOE の基本機能の利用を可能とする。また、利用者及び管理者が、利用者文書データ及びジョブの操作や監査ログの閲覧、TOE の各種管理などを行うことができる。これらの機能の利用は、下記のプリンタドライバや、WEB ブラウザベースの TOE の管理ツール「TopAccess」を介して行う。

なお、クライアント PC には以下のソフトウェアの導入が必須となる。

- Internet Explorer 9
- 東芝テック株式会社提供のプリンタドライバ
  TOSHIBA Universal Printer 2 (Version 7.149.3660.0)

(2) メールサーバ/FTP サーバ

Mail Server 及び FTP Server は、スキャン機能やインターネットファクス送信機能、インターネットファクス受信機能を利用するために、メールの送受信やデータの格納に用いられる。TOE と各サーバ間の通信には TLS 通信を使用。

(3) ファイアウォール

外部ネットワークからの不正アクセスを防ぐためにファイアウォールを設置する。

4.3 運用環境におけるTOE範囲

(1) 本 TOE では LDAP サーバ、Domain サーバ、SMB サーバ、NTP サーバを使用して運用した場合は、評価対象外となる。

(2) 本評価では、PP が要求している識別認証のセキュリティ要件について、クライアント PC のプリンタドライバから送信される利用者文書データの受信、メールサーバからの e-mail の受信については、適用対象外であると解釈されており、本 TOE では以下の機能を提供しないことが本評価において確認された。

- クライアント PC のプリンタドライバからのプリンタ要求によって利用者文書データを TOE が受信する際の認証機能
- メールサーバから e-mail を TOE が受信する際の識別認証機能

(3) TOE は、TOE に接続した USB メモリに格納した文書データを印刷する機能を提供している。USB メモリに格納された文書データは、操作パネルからの利用者は誰でもアクセスが可能である。USB メモリの置き忘れ等の対策は、利用者の責任となる。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（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。「General Function」内の色づけ部分が TOE の基本機能であり、その他の色づけ部分が TOE のセキュリティ機能である。

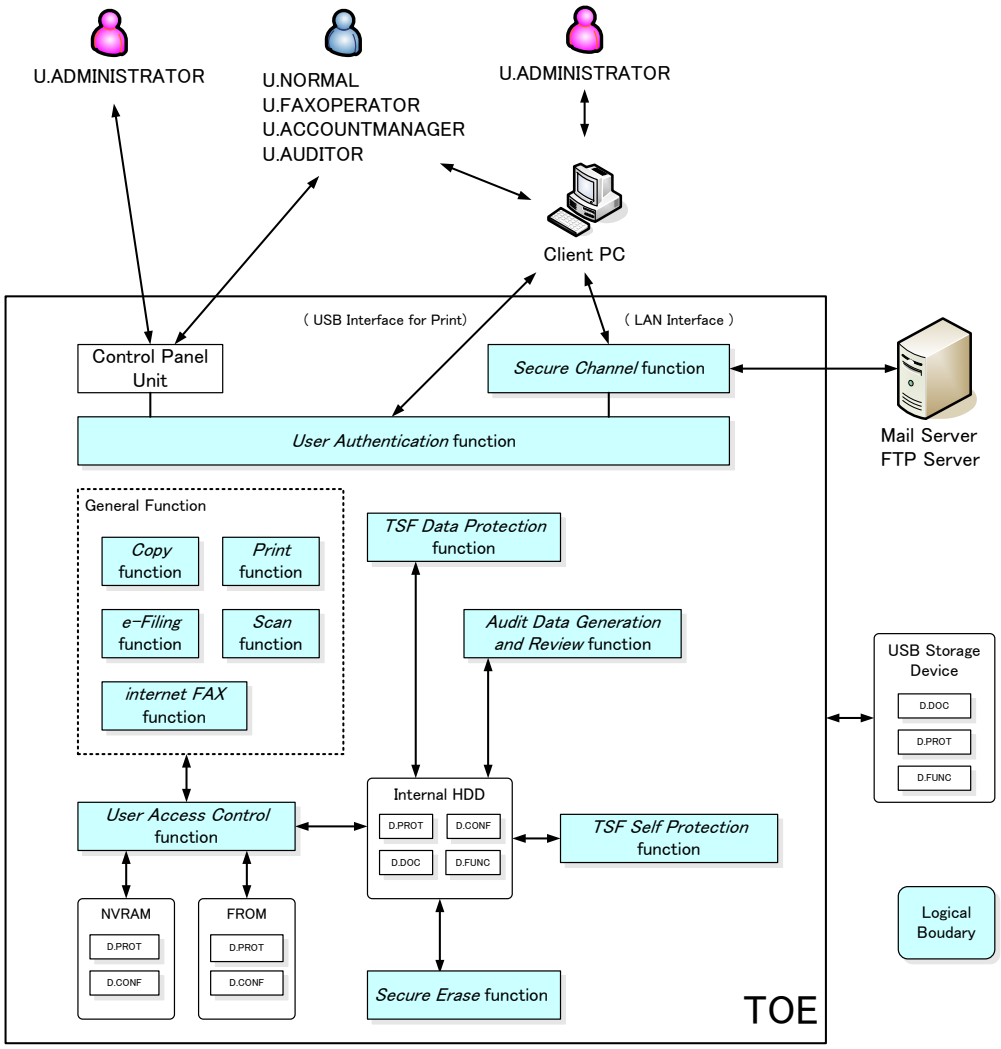

図5-1　TOE境界

以下、TOE の利用方法とセキュリティ機能の関係について、インタフェースごとに説明する。

(1) クライアント PC からの利用

クライアント PC は LAN 接続または USB ケーブルで直接接続される。TOE と LAN 接続されたクライアント PC 間は TLS 通信を使用して通信データを

保護する。利用者はクライント PC から以下のツールを用いて、TOE を利用することができる。

① プリンタドライバ

TOE と LAN 接続または USB 接続されたクライアント PC から、プリンタドライバを介してプリント要求を TOE へ送信する。送信の際には、プリンタドライバはクライアント PC にログインしたユーザ ID を利用者のユーザ ID として自動的にプリント要求にセットする。

プリント要求を受信した TOE は、「User Authentication 機能」により、プリント要求にセットされた利用者のユーザ ID と TOE 内の登録データを突合して識別を行い、識別された場合はプリント対象の利用者文書データにユーザ ID が付与され、TOE 内にプリント待ちのジョブとして格納する。

格納された利用者文書データをプリントするには、TOE の操作パネルからプリントの操作を行う。操作の際には「User Authentication 機能」により利用者にログインを要求し、操作パネルから入力されたユーザ ID とパスワードにより識別認証を行う。

識別認証が成功すると、さらに「User Access Control 機能」により、ユーザ ID に付与された操作権限を基にチェックを行い、プリントの操作権限があった場合にプリントが許可される。

② WEB アプリケーション

TOE と LAN 接続されたクライアント PC から、WEB ブラウザを介して、TOE が提供する WEB アプリケーション「TopAccess」へアクセスを行うと、アカウント管理、TOE の設定変更、監査ログの閲覧、TOE 内部のファイリングボックスに格納された利用者文書データへのアクセスなどの各種操作が行える。これらの TOE に対する各種操作を行う際には、「User Authentication 機能」によって識別認証が行われ、正当な利用者のみに TOE の操作が許可される。

(2) 操作パネル(Operation Panel Unit)からの利用

利用者が操作パネルを操作して、TOE の基本機能を利用できる。操作を行う際には「User Authentication 機能」によって識別認証が行われ、正当な利用者のみに TOE の操作が許可される。

以下、TOE のセキュリティ機能について説明する。

(1) 識別認証

「User Authentication 機能」により、TOE は、プリント要求を受信した場合は､送信されたユーザ ID と TOE 内の登録データとの突合で識別を行い、識別できた場合はプリント対象の利用者文書データにユーザ ID が付与される。

上記以外の場合は、「User Authentication 機能」により、TOE は、送信されたユーザ ID とパスワードを基に TOE 内の登録データとの突合で識別認証を行い、正当な利用者にのみログイン並びに TOE の利用を許可する。

また、「User Authentication 機能」により、ログイン後、管理者により定められた時間まで無操作状態が続いた場合には、該当の利用者のセッションを無効化する。

(2) アクセス制御

「User Access Control 機能」により、利用者による各基本機能の操作の際には、該当の機能の操作権限を付与されているかチェックが行われ、付与されている利用者にのみに操作が制限される。

また、「User Access Control 機能」により、利用者による利用者文書データ及びジョブへのアクセスの際には、それぞれのデータが利用者本人にひもづいたデータであるかのチェックが行われ、利用者本人の場合のみアクセスが許可される。TOE 管理者の場合はすべての利用者文書データ及びジョブへのアクセスが可能となっている。

(3) HDD 内のデータ保護

「Secure Erase 機能」により、削除された利用者文書データの HDD 上での保存領域に対して、DoD 消去方式を用いた上書き消去による保護が行われる。

(4) 通信の保護

「Secure Channel 機能」により、TOE とクライアント PC やメールサーバ、FTP サーバなどの IT 機器と LAN を経由して通信する場合には、TLS プロトコルを用いた通信データの保護を行う。

また、TOE の各インタフェースから受信した利用者文書データに対して、TOE が仲介となって直接的に外部インタフェースへデータを転送する機能を提供していないことにより、不正な転送の防止を行う。

(5) 監査ログの生成

「Audit Data Generation and Review 機能」により、監査対象事象が発生した際に、監査ログを生成する。監査ログの閲覧は、以下のとおり利用者の役割ごとに制限する。また、すべての監査ログの削除と出力操作を TOE 管理者のみに制限する。

一般利用者	利用者本人の各基本機能の実行により生成されたジョブの監査ログを閲覧可能
TOE管理者	TOEのすべての監査ログを閲覧可能
監査ログ管理者	TOEのすべての監査ログを閲覧可能
ファクスオペレータ	利用者本人のインターネットファクス送信機能の実行により生成されたジョブの監査ログを閲覧可能

また、「Audit Data Generation and Review 機能」により、監査ログの件数が上限を超えた際には古いデータから順に上書きしていくことで、監査ログの消失を防いでいる。

(6) TOE の自己テスト

「TSF Self Protection function」は、全 TSF の実行コード・Hash value-acquiring code の完全性を検証し、異常を検出した場合には TOE の使用を不可とする機能を提供する。本機能は TOE 管理者のみが実行できる。

(7) TSF データの保護

「TSF Data Protection 機能」により、TOE のセキュリティ機能の管理機能の操作を TOE 管理者のみに、利用者の登録や基本機能の操作権限の変更などアカウント管理の操作を TOE 管理者とアカウント管理者のみに制限する。

また、「TSF Data Protection 機能」により、利用者のパスワードの変更については、利用者本人または TOE 管理者及びアカウント管理者のみに制限する。

5.2 IT環境

TOE の監査ログに記録される時刻情報は、TOE が保持している時刻のみが使用される。NTP プロトコルによる外部のタイムサーバとの同期は評価対象外である。

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の表 6-1、表 6-2 に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

表 6-1 ガイダンス(英語版)

Title	Version
Quick Start Guide	OME140023A0
Safety Information	OME120008F0
Copying Guide	OME140025B0
Scanning Guide	OME120020H0
e-Filing Guide	OME120014E0
MFP Management Guide	OME120016G0
Software Installation Guide	OME120010J0
Printing Guide	OME120012J0
TopAccess Guide	OME120018I0
Troubleshooting Guide	OME140027A0
High Security Mode Management Guide	OME100078P0

表 6-2 ガイダンス(日本語版)

Title	Version
かんたん操作ガイド	OMJ140022A0
安全にお使いいただくために	OMJ120007G0
コピーガイド	OMJ140024B0
スキャンガイド	OMJ120019H0
ファイリングボックスガイド	OMJ120013F0
設定管理ガイド	OMJ120015F0
インストールガイド	OMJ120009H0
印刷ガイド	OMJ120011J0
TopAccessガイド	OMJ120017I0
トラブルシューティングガイド	OMJ140026A0
ハイセキュリティモード管理ガイド	OMJ100077N0

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した一般社団法人 IT セキュリティセンター 評価部は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 26 年 1 月に始まり、平成 27 年 11 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 26 年 2 月、3 月、平成 27 年 7 月、及び 8 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 26 年 6 月、8 月、及び 11 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。

7.4 製品テスト

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

7.4.1 開発者テスト

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

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に示す。

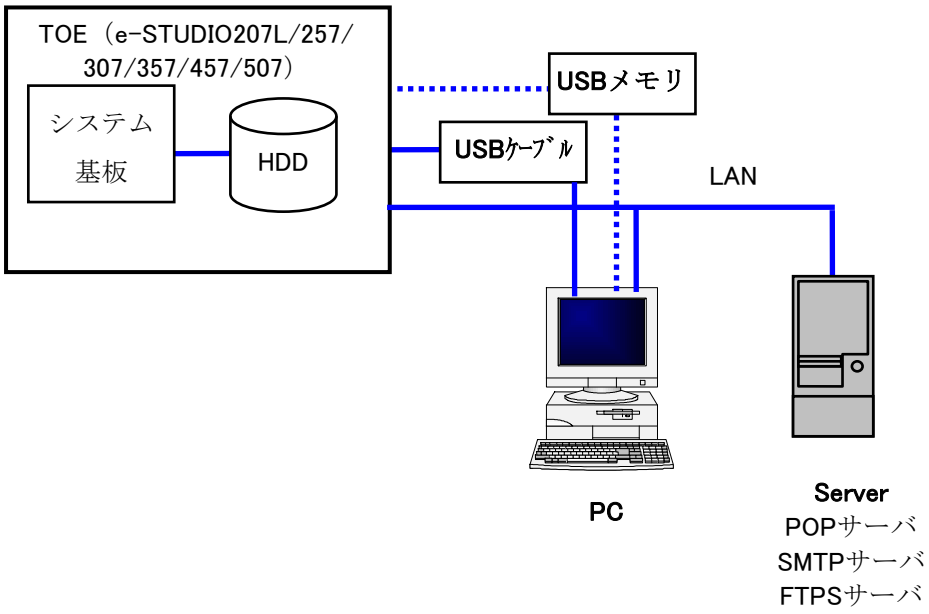

図7-1　開発者テストの構成図

開発者テストが対象とした TOE は以下のとおり、識別された TOE をすべて含んでいる。

表7-1　TOEのバリエーション

製品名（モデル）	バージョン
TOSHIBA e-STUDIO207L MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0
TOSHIBA e-STUDIO257 MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0
TOSHIBA e-STUDIO307 MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0
TOSHIBA e-STUDIO357 MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0
TOSHIBA e-STUDIO457 MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0

製品名（モデル）	バージョン
TOSHIBA e-STUDIO507 MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V3.0

テスト環境の TOE 以外の構成要素を表 7-2 に示す。

表7-2 開発者テストの使用機器

機器	仕様	
PC1	OS	Windows7 Professional Service Pack1 (32ビット)
	Client Utility Software	TOSHIBA UniversalPrinter2 Version 7.149.3660.0
	ブラウザ	Internet Explorer 9
	メーラー	WindowsLiveMail version2012
Server	OS	WindowsServer2008R2 Enterprise ServicePack1 (64ビット)
	メールサーバ	Exchange Server 2010 ver14.02.0247.005 (POP,SMTP) ※FTPはOS機能で設定
USBメモリ	512MB 以上	

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。

⑵ 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＞

本 TOE で利用可能な外部インタフェースを刺激する手法として、操作パネル及びクライアント PC からの手動操作によるテストを実施し、そのふるまいの確認を行った。

本 TOE の応答を観察する手法としては、以下を実施した。

① 操作パネルに表示されたふるまいの結果の確認

② TOE からプリントされた出力結果の確認

③ クライアント PC の画面に表示されたふるまいの結果の確認

④ ネットワークプロトコルアナライザを用いて通信パケットをキャプチャ

本 TOE の応答を観察することでは確認が困難なふるまいに関しては、以下の手法が用いられた。

① TOE の内部的なインタフェースを操作できる仕組みを別途用意して、TOE の内部的なプログラムの出力やログ、HDD の内容、テスト用プログラムの出力を確認

② TOE のソースコードを確認

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-3 に示す。

表7-3　開発テストツール

ツール名称(バージョン)	利用目的
WireShark(version 1.12.3)	プロトコルキャプチャ
Fiddler Web Debugger (version 4.4.9.7)	Web通信キャプチャ・変更

＜開発者テストの実施内容＞

アクセス制御が正しく実行されていること、TLS 通信が正常に動作していることなど､全てのセキュリティ機能を網羅した開発者テストが実施された。以下は、開発者テストに関する特記事項である。

- TOE のインタフェースからの不正な入力(想定外の値や、SQL インジェクションなどの脆弱性への攻撃となるパターン)に対する TOE の動作が確認されている。不正な入力としては、以下のようなものも含まれている。
  - Fiddler Web Debugger を使用して WEB ブラウザの制約を受けずに WEB インタフェースへ不正な入力をする。
  - 不正な内容の文書データを USB メモリに格納し、TOE の USB インタフェースからの印刷を試みる。

- HDD の上書き消去の確認のために、TOE の内部的なインタフェースを操作して、TOE の内部的なプログラムの出力やログ、HDD の内容を確認する手法が用いられた。

- TOE 内のプロセスの動作が他のプロセスや特権で動作する重要な部分に想定外の影響を与えないことを確認するために、TOE の内部的なインタフェースを操作してテスト用プログラムの出力を確認する手法と、TOE のソースコードを確認する手法が用いられた。

期待したテスト結果と実際のテスト結果はすべて一致しており、期待した結果とテスト結果が異なっている項目は１つもない。

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240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。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実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環境は、開発者テストと同じ環境である。

TOE には複数のモデルが存在するが、その中の TOSHIBA e-STUDIO507 MULTIFUNCTIONAL DIGITAL SYSTEMS が使用された。他のモデルはハードウェアの印刷速度の相違のみという理由で、特定のモデルのテストで十分であることが判断されている。

テスト環境の要素やテスト用プログラムは、開発者テストに用いられたものを利用しているが、これらの仕様確認及び動作試験と校正は評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① 開発者テストのテスト計画で、厳密さに欠けるインタフェース・機能がある場合は、それらを独立テストの対象とする。

② インタフェースのタイプ、ソースコードの確認を含めたテスト手法がカバーされるように開発者テストのサンプリングテストを実施する。

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＞

開発者テストと同じ手法を用いた。

＜独立テストツール＞

開発者テストと同じツールを用いた。

＜独立テストの実施内容＞

独立テストは、開発者によって開発者テストのサンプリングテスト 40 項目、評価者考案テスト 6 項目が実施された。

独立テストの観点とそれに対応したテスト内容を表 7-4 に示す。

表7-4 実施した独立テスト

観点	テスト概要
①	開発者テストでパラメタにバリエーションがあるテストについて、パラメタを変更してテストを行う。 ログインパスワードの変更時に許可されない文字列入力時のふるまい、重複したユーザIDの登録時のふるまい、ファイリングボックスのパスワード変更後に旧パスワードでアクセスした場合のふるまい、別々のインタフェースからによるファイリングボックス内の利用者文書データへの同時更新における排他制御、一般利用者に付与された基本機能の操作権限のアクセス制御に関して、仕様通りであることを確認した。
②	TOEが提供する全てのインタフェースのタイプ、及びソースコードの確認を含めたテスト手法が含まれるよう、開発者テストからサンプリングしたテスト項目を評価者が実施し、すべての実際のテスト結果が期待されたテスト結果に一致することを確認した。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 公知の脆弱性情報であるネットワークサービスの不正利用について懸念される。

② 開発証拠資料の探索から、以下のことが懸念される。

・操作パネルからの操作とクライアントPCからの操作で同じデータに対して更新を行い、競合することによるTOEの予期せぬ動作が懸念される。

・印刷時の紙切れなどのエラーによる処理中断によって識別認証やHDDの上書き消去機能が正しく動作されないことが懸念される。

・保守モードの場合のみUSBメモリから入力可能なデータが、通常の運用状態で入力できてしまうことが懸念される。

・TLSを無効化した通信が許可されることが懸念される。

・SNMP経由で想定されない情報を取得できることが懸念される。

③ TOEのセキュアな初期化について、TOEの初期化中にWEBインタフェースや操作パネルからログインを試み、識別認証のバイパスが起こることが懸念される。

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＞

評価者が実施した侵入テストは、開発者テスト環境に侵入テスト用 PC を追加で LAN 接続した環境で実施された。評価者独立テストと同じ理由で、TOE として TOSHIBA e-STUDIO507 MULTIFUNCTIONAL DIGITAL SYSTEMS が使用された。

侵入テストに用いたツールの詳細を表 7-5 に示す。これらの仕様確認及び動作試験と校正は評価者によって実施されている。

表7-5 侵入テストの使用ツール

ツール名称(バージョン)	利用目的
nmap (version 6.47)	ポートスキャンツール
snmpwalk (version 5.4.3)	MIB情報取得ツール
sslscan (OpenSSL 1.0.1m)	SSL/TLS接続においてサポートされる暗号化方式を調査するツール

＜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内容を表 7-6 に示す。

表7-6　侵入テスト概要

脆弱性	テスト概要
①	nmapをTOEに対して実行し、意図しないポートがオープンしていないことを確認した。
②	利用者のパスワード変更やTOEの設定などに関して、同一のデータに対し操作パネルからの操作とクライアントPCからの操作を同時に行い、TOEが競合による予期せぬ動作をしないことを確認した。
②	紙切れなどの印刷時のエラーによる処理中断がHDD上書き消去機能に影響を及ぼさないことを確認した。
②	TOEのUSBインタフェースに対して、保守モードの場合のみUSBメモリから入力可能なデータを格納したUSBメモリの読み込みを試み、TOEが不正なプログラムを認識しないことを確認した。
②	TLSプロトコルを用いない(暗号化が行われない)通信の要求を試み、接続が拒否されることを確認した。 SSLによる接続が無効であることをsslscanにより確認した。
②	SNMP経由で得られるデータをsnmpwalkにより調査し、想定外のデータがないことを確認した。
③	TOEの初期化中に、WEBインタフェース及び操作パネルからTOEへのアクセスを試みて、ログイン画面が表示されなかったことを確認した。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本評価の前提となる TOE の構成条件はガイダンスに記述されているとおりであり、ガイダンス「Safety Information／安全にお使いいただくために」及び「High Security Mode Management Guide／ハイセキュリティモード管理ガイド」に従い、設定する必要がある。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

PP 適合：

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 適合
2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A 適合
2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A 適合
2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A 適合
2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A 適合

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。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

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

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

本 TOE は、HDD に書き込むデータを暗号化する機能を持つ。ただし、この機能は本評価の保証の対象外となる。そのため、HDD 上のデータが暗号化されていることにより情報漏洩が防がれることを期待する調達者にとっては、本評価による保証はニーズに合致しない可能性があるので、注意が必要である。

本 TOE では、クライアント PC 上のプリンタドライバを介して TOE へ送信されるプリント要求の利用者文書データの HDD への保存については利用者の認証は不要であり、インターネットファクスとしてメールサーバから送信される e-mail の HDD への保存については利用者の識別認証は不要となる。そのため、プリンタドライバの使用や e-mail によるインターネットファクスの受信データの保存において、識別認証機能により利用制限できることを期待する調達者にとっては、ニーズに合致しない可能性があるので、注意が必要である。

本 TOE では、LDAP サーバ、Domain サーバ、SMB サーバ、NTP サーバを使用して運用した場合は評価対象外となるため、調達者は購入前に自身が想定する運用環境について注意が必要である。

本 TOE では、通常の運用状態から保守作業のため保守モードに遷移した場合、それ以降の運用での本 TOE のセキュリティ機能への影響については本評価の保証の範囲外となるため、保守の受け入れについては管理者の責任において判断されたい。

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。

TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS Security Target Version 1.3 September 3, 2015 TOSHIBA TEC CORPORATION

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。

DoD	United States Department of Defense
FTP	File Transfer Protocol
HDD	Hard Disk Drive
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
SMB	Server Message Block
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus

本報告書で使用された用語の定義を以下に示す。

DoD消去方式	アメリカ国防総省標準に準拠したHDD消去方式。
Hash value-acquiring code	TSFの実行コードの電子署名からハッシュ値を取り出すために使用するデータ。
TOE管理者 (U.ADMINISTRATOR)	TOEのセキュリティポリシーに影響を与える設定及び利用者のアカウント管理、監査ログの閲覧・削除・エクスポートなど、TOEの管理機能全般が操作できる管理者。
TopAccess	クライアントPCからブラウザを介して、利用者文書データ・ジョブの操作、TOEの管理設定や利用者の管理が行える、TOEが提供するWEBアプリケーション。
アカウント管理者 (U.ACCOUNTMANAGER)	利用者のアカウント管理(利用者のユーザIDや役割設定、基本機能の操作権限など)の設定が行える管理者。
一般利用者 (U.NORMAL)	TOEの基本機能である「コピー機能」、「プリント機能」、「スキャン機能」、「ファイリング機能」、「インターネットファクス送信機能」を操作できる利用者。ただし、ファイリング機能の場合、ファイリングボックスのバックアップ及びリストアの操作は行えない。 一般利用者は、実行できる基本機能ごとに該当する操作権限が付与される。
インターネットファクス送信機能 (Internet Fax transmission function)	利用者文書データをTIFF-FX(Profile S)ファイルに変換してe-mailに添付したものをファクスとしてインターネット経由で送信する機能。本機能では、送信先として、電話番号の代わりにe-mailアドレスを指定する必要がある。 利用者は本機能の操作権限が付与されることで実行できる。
インターネットファクス受信機能 (Internet Fax reception function)	TOEがメールサーバからEメールをインターネットファクスとして自動的に受信しHDDに保存された利用者文書データに対して、アクセス及びプリントできる機能。 ファクスオペレータのみに本機能の操作権限が付与される。
監査ログ管理者 (U.AUDITOR)	TOEのすべての監査ログを閲覧できる管理者。
基本機能	TOEが提供している基本的な機能。「コピー機能」、「プリント機能」、「スキャン機能」、「ファイリング機能」、「インターネットファクス送信機能」の5種類。利用者には、実行できる基本機能ごとに該当する操作権限が付与される。

クライアントPC (Client PC)	TOEとLANもしくはUSBで接続された汎用PC。 OS : Windows XPまたはWindows Vista、ブラウザ : Internet Explorer .8、東芝テック株式会社提供の各Client Utility Softwareを搭載して使用される。
コピー機能 (Copy function)	TOEが読み込んだ利用者文書データを印刷する基本機能。 利用者は、操作パネルからログインを行い識別認証された上で、本機能の操作権限が付与されていることで実行できる。
ジョブ (Job)	利用者がTOEの基本機能を操作することにより生成される実行処理のこと。1回の処理で1つのジョブという単位。 基本機能名と組み合わせて、「コピージョブ」、「プリントジョブ」、「スキャンジョブ」など、各基本機能のジョブを呼ぶ。
スキャン機能 (Scan function)	TOEが読み込んだ利用者文書データをHDDに保存し、保存された利用者文書データへアクセスができる機能。 利用者が利用者文書データをスキャンすると、利用者によりTOEに設定された情報に基づいて自動的にクライアントPC、メールサーバまたはFTPサーバに転送される。操作パネルから、この機能の操作を行う。 利用者は本機能の操作権限が付与されることで実行できる。
操作権限	利用者へ付与される、TOEの各基本機能を操作できる権限のこと。
操作パネル (Control Panel)	TOE本体の表面に装備されているタッチパネル式のインタフェース。
ファイリング機能 (e-Filing function)	TOE内にファイリングボックスを作成し、その中へ利用者文書データを格納したり、格納した利用者文書データを読出し・編集・印刷できる機能。操作パネル・クライアントPCの両方から、この機能の操作が行える。 ただし、ファイリングボックスのバックアップ及びリストアの操作は行えず、TOE管理者のみが操作可能となる。
ファイリングボックス (e-Filing Box)	利用者文書データを格納するボックス形式の記憶領域。ファイル及びフォルダを格納できる。
ファクスオペレータ (U.FAXOPERATOR)	「インターネットファクス送信機能」と「インターネットファクス受信機能」の操作権限を付与された利用者。 利用者文書データのインターネットファクス送信と、TOEがインターネットファクスとして受信しHDDに保存されたすべての利用者文書データへのアクセス及びプリントが実行できる。

プリント機能 (Print function)	プリント要求によりTOEへ送信されて蓄積されている利用者文書データを、読出し・印刷する機能。
プリント要求	利用者がクライアントPC上のプリンタドライバを介して、TOEへプリントしたい利用者文書データを送信する要求のこと。 この要求時には、クライアントPCにログインした際のユーザIDが自動的にプリンタドライバからTOEへ送信される。 TOEは受信したユーザIDをTOE内の登録情報と照合し識別を行い、利用者文書データをTOE内に格納する。 この要求の送信には、プリント機能の操作権限は不要である。
利用者 (U.USER)	各管理者やファクスオペレータ、一般利用者を含んだTOEの利用者全般のこと。
利用者文書データ (User Document Data)	TOEの基本機能での処理対象となるデータの総称。

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27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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4版, 2012年9月, CCMB-2012-09-001, (平成24年11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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS Security Target Version 1.3 September 3, 2015 TOSHIBA TEC CORPORATION

[13] TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS 評価報告書, 第1.13版, 2015年11月12日, 一般社団法人 IT セキュリティセンター 評価部

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