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5月27日 (IT認証0296)
認証番号	C0328
認証申請者	東芝テック株式会社
TOEの名称	TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS
TOEのバージョン	SYS V1.0
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23年10月28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 3

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

評価結果：合格

「TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C 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、東芝テック株式会社が開発した「TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS、Version SYS V1.0」（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 23 年 10 月 13 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である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ックス機能等を有するデジタル複合機（以下「MFP」という。）、TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS である。

本 TOE は、上記の基本機能に加えて、基本機能で扱う文書データやセキュリティに影響する設定データ等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、また利用者の誤使用による漏えい等の脅威がある。

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、利用者権限毎のアクセス制御、データ暗号化、監査ログ生成等の機能を提供する。

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 のハードディスクドライブ（以下「HDD」という。）の上書き消去機能を提供するオプションキット「GP-1070」がインストールされていること。

ハードウェア取り外しや分解等の不正な物理的アクセスから保護されるような安全な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、ファイアウォール等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

本評価では、ハイセキュリティモードに設定された TOE のみが評価対象となっており、その他のモードへ設定変更された場合には、本評価による保証の対象外となる。

本 TOE は配送中の改ざんを検出するよう東芝テック株式会社から段ボールに梱包し、東芝テック株式会社が契約した販売会社経由で配送される。本 TOE の購入者は、納入時にオフィスでの設置作業時間を短縮するため、販売会社に対して梱包された段ボールを開梱する指示を出し、開梱された状態で納入することも可能となっている。

本評価では東芝テック株式会社から顧客オフィスまで梱包された状態での配送手段は保証されるが、購入者が上記の開梱指示を出した場合には、改ざん防止の梱包が解かれるため販売会社と顧客オフィス間の配送手段は保証されない。

そのため､開梱指示を出した場合には､TOE は本評価による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 セキュリティ認証申請手続等に関する規程」[2]、「IT セキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 23 年 10 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-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS
バージョン：	SYS V1.0
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。

操作パネル上のカウンタボタンを押下することにより、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ックス機能等を提供しており、利用者の文書データを内部の HDD に蓄積したり、ネットワークを介して利用者の端末や各種サーバとやりとりしたり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 の蓄積データの暗号化とデータ削除時の上書き消去、暗号通信プロトコル等が含まれており、保護資産である利用者の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、使用に関して以下の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ックス機能（送信のみ）等を利用する TOE の一般利用者。

・U.FAXOPERATOR（ファックスオペレータ）
インターネットファックス機能（送信・受信）の利用が許可される利用者。インターネットファックス機能により受信した文書データの印刷は、一般利用者には許可されず、ファックスオペレータのみが実行できる。

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

・U.ACCOUNTMANAGER（アカウント管理者）
TOE 管理者が実行できる管理権限の内、利用者のアカウント情報（利用者のユーザ ID、利用者に付与される基本機能の実行権限等）の変更のみが行えるアカウント管理者。

・U.AUDITOR（ログ監査者）
TOE 管理者が実行できる管理権限の内、ネットワーク経由で監査ログの閲覧のみが許可されたログ監査者。

また、TOE の保護資産は以下のものである。

・User Document Data
利用者の文書データ。

・User Function Data
TOE によって処理される利用者の文書データやジョブに関連する情報。印刷待ちのプリントジョブ情報、e-mail のアドレス帳等が含まれる。

・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。利用者役割ごとの権限情報、TOE の設定情報、ネットワーク設定情報等が含まれる。

・TSF Confidential Data
セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められるデータ。HDD の暗号鍵や、監査ログ、利用者のパスワード等が含まれる。

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

識別子	脅威
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。認証用のパスワードを 8 文字以上に限定すること、一定回数以上認証に失敗した場合にはユーザ ID をロックアウトすること、一定時間以上 TOE が操作されなかった時に強制的にログアウトする機能が備わっている。

「User Access Control 機能」により、識別認証された利用者のユーザ ID と利用者役割毎の権限を基に利用者データへの操作に対してアクセス制御を実施する。一般利用者からの操作要求に対しては、ログインユーザ ID と文書データに付けられたユーザ ID の一致/不一致を確認し、各種操作の許可/拒否の制御を行う。TOE 管理者やファックスオペレータ等の一般利用者以外の特別な役割を持つ利用者は、その役割毎に利用者データに対して特定の操作が許可される。

「Secure Erase 機能」により、コピー等 MFP の基本機能の完了時に、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、削除された文書データが HDD から読み出されることを防止する。

「Secure Channel 機能」に含まれるセキュア通信機能により、TOE とクライアント PC や各種サーバとの通信時に、SSL プロトコルを用いる。これにより、通信データを秘匿し、改ざんを検知することができる。

(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」、「User Access Control 機能」、「Secure Channel 機能」で対抗する。

「TSF Data Protection 機能」により、識別認証された TOE 管理者にのみ TOE の設定情報の変更や、プルトコル等の有効/無効の設定変更を許可する。

「User Authentication 機能」「User Access Control 機能」「Secure Channel 機能」は(1)の場合と同じである。

以上の機能により、TOE は、TOE の権限外使用や、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し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、P.CRYPTOGRAPHY 以外は、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.
P.CRYPTOGRAPHY	User document data stored in an HDD must be encrypted to improve the secrecy of the document.

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、プリント機能、スキャン機能、コピー機能、ファイリング機能、インターネットファックス機能の各機能を使用する際にアクセス制御を行い、権限のある利用者のみに実行を許可する。アクセス制御では、各機能において利用者に割り当てられた役割情報を参照し、対象機能の実行が許可されているかを判断する。

(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。

TOE の操作パネルから TSF 自己テストを実行し、全 TSF の実行コード、HDD 暗号鍵の完全性を検証し、異常が検出された場合には TOE を使用不可とする。なお、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、日付、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。監査ログの閲覧は、ログ管理者や TOE 管理者等許可された利用者だけに制限される。

(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、セッションを遮断する。

「Secure Channel 機能」に含まれるデータ転送制限機能により、本 TOE の各外部インタフェース（USB インタフェースや操作パネル）から LAN インタフェースへの不正なデータ転送を防止する。

なお、ファイアウォール等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。

(5) 組織のセキュリティ方針「P.CRYPTOGRAPHY」への対応

TOE は「Data Encryption 機能」で本方針を実現する。

TOE の HDD 内に保存される文書データに対して、FIPS PUB 197 の AES に基づく 128 ビットの暗号鍵を用いた暗号化、復号処理を行う。

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、社内ネットワークで接続され、同様に社内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 の一般的な運用環境を図 4-1 に示す。

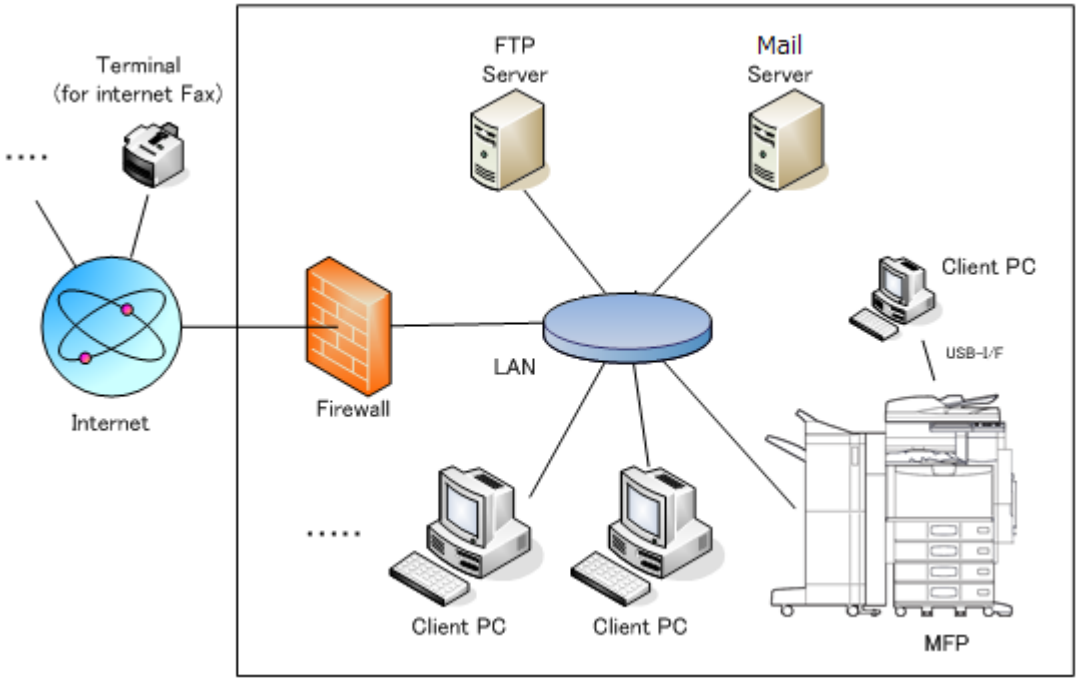

図 4-1 TOEの運用環境

(1)Client PC

LAN 及び USB インタフェースを介して TOE に接続し、一般利用者が TOE に文書の印刷要求や、登録したファイリングボックスに対して文書データを保存、取り出しを行うことを用途とする。また、TOE 管理者も Web ブラウザを用いて MFP の設定データを参照・変更することができる。

なお、利用においては以下のソフトウェアが必要となる。

OS：Windows XP、Windows Vista のいずれか

ブラウザ：Internet Explorer Ver.8.0

以下のバージョンの Client Utility Software

Address Book Viewer	3.2.20.0
e-Filing Back Up/Restore Utility	3.2.22.0
File Down Loader	3.2.24.0
TWAIN Driver	3.2.25.0
Printer Driver	6.20.2521.6

(2)Mail Server、FTP Server

スキャン機能やインターネットファックス機能等 MFP の基本機能を利用する際に設置する。TOE と各サーバ間の通信には SSL プロトコルを用いる。

(3)Firewall

外部ネットワークからの不正アクセスを防ぐために設置する.

なお、本構成に示されている 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）。

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付されるプリントデータの受信、Mail 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プリントデータを TOE に格納する場合の認証機能

・Mail サーバからの e-mail を TOE に格納する場合の識別認証機能

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」内で色づけされた部分が TOE の基本機能であり、その他の色づけられされた部分が TOE のセキュリティ機能である。

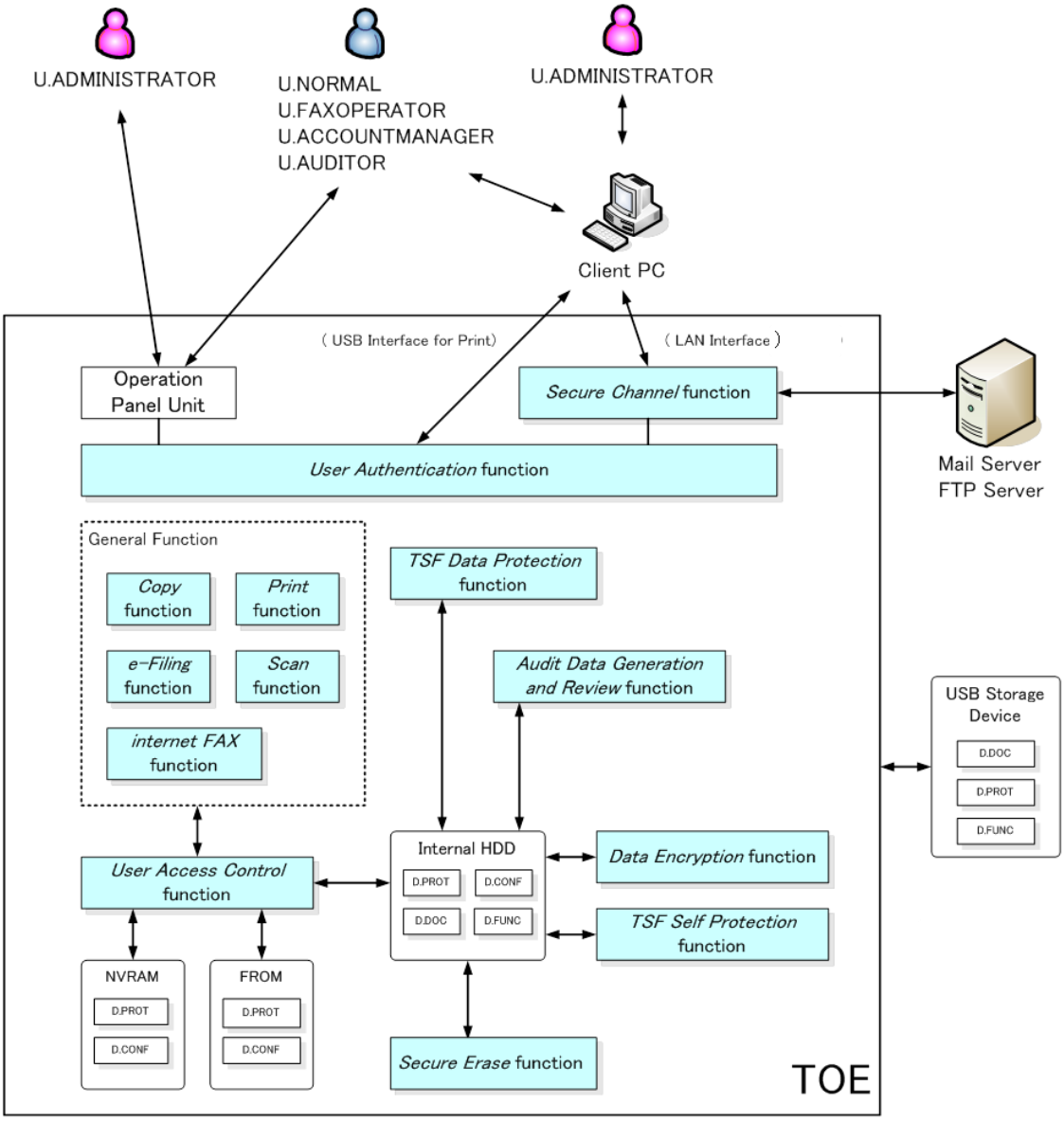

図 5-1 TOE境界

TOE のセキュリティ機能は、利用者が TOE の基本機能を使用する際に適用される。以下、セキュリティ機能と TOE の基本機能の関係について説明する。

① クライアント PC からの利用

クライアントPCはTOEとLAN接続またはUSB接続することができる。TOEとLAN接続されたクライアントPC間の通信はSSLプロトコルを用い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。

(ア) Webブラウザ

LAN接続されたクライアントPCから、Webブラウザを操作して、アカウント管理、TOEの設定変更、ログの監視、TOE内部のファイリングボックスに格納された文書データへのアクセス等の操作の際には、「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。

(イ) プリンタドライバ

LAN接続もしくはUSB接続されたクライアントPCから、プリンタドライバにより文書データのプリント要求をする際には、「User Authentication機能」により利用者の識別が行われ、TOEにプリントデータがTOEに蓄積される。

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、コピー機能、プリント機能、スキャナ機能、インターネットファックス機能、TOE内部のファイリングボックスに格納された文書データへのアクセス等の基本機能を使用する際には、「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。

①、②における基本機能の操作の際には、「User Access Control機能」により、TOE管理者もしくはアカウント管理者によって使用権限を付与された利用者にのみ制限される。
また、文書データ、ジョブデータの削除においては、文書データを作成した一般利用者もしくはTOE管理者にのみ削除操作が許可される。（プリント機能については権限のあるファックスオペレータにも文書データ、ジョブデータの削除操作が許可される。）

③ Internal HDDのデータ保護

「Data Encryption機能」によりHDDに格納される文書データは、TOEに内蔵された暗号化チップを用いた暗号化が行われる。

また、「Secure Erase 機能」により、削除された文書データの 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 ネットワーク関連の保護

TOE と、クライアント PC や Mail サーバ、FTP サーバ等の IT 機器が LAN を経由して通信する場合には、「Secure Channel 機能」により通信に SSL プロトコルを用いた通信データの保護や、TOE の外部インタフェースから LAN インタフェースへの不正なデータ転送の防止を行う。

⑤ 監査ログの生成

「Audit Data Generation and Review 機能」により、セキュリティに関連した監査対象事象が発生した際に、監査ログを生成する。また、監査ログの削除操作を TOE 管理者のみに制限する。

⑥ TOE の自己テスト

「TSF Self Protection 機能」により、TOE 管理者の要求に応じて、TSF 自己テストを実行し、全 TSF の実行コード・HDD 暗号鍵の完全性を検証し、異常を検出した場合には TOE の使用を防止する機能を提供する。

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に影響する設定変更等の操作を TOE 管理者のみに、利用者の基本機能の使用許可権限の変更等を TOE 管理者と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。

TOE に接続した USB Storage Device には文書データの保存が行えるが、USB Storage Device に保存した文書データは本評価の対象外であり保証されない。

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** 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	OME100038A0
Safety Information	OME100050B0
Copying Guide	OME100040A0
Scanning Guide	OME100062A0
e-Filing Guide	OME100056B0
MFP Management Guide	OME100058A0
Software Installation Guide	OME100052A0
Printing Guide	OME100054A0
TopAccess Guide	OME100060B0
Troubleshooting Guide	OME100042A0
High Security Mode Management Guide	OME100078B0

表 6-2 ガイダンス（日本語版）

Title	Version
かんたん操作ガイド	OMJ100037A0
安全にお使いいただくために	OMJ100049B0
コピーガイド	OMJ100039A0
スキャンガイド	OMJ100061A0
ファイリングボックスガイド	OMJ100055B0
設定管理ガイド	OMJ100057A0
インストールガイド	OMJ100051A0
印刷ガイド	OMJ10005300
TopAccessガイド	OMJ100059B0
トラブルシューティングガイド	OMJ100041A0
ハイセキュリティモード管理ガイド	OMJ100077B0

7 評価機関による評価実施及び結果

7.1 評価方法

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

7.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 22 年 5 月に始まり、平成 23 年 10 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 23 年 2 月、5 月及び 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。また、平成 23 年 5、6 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 製品テスト

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

7.3.1 開発者テスト

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

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に示す。

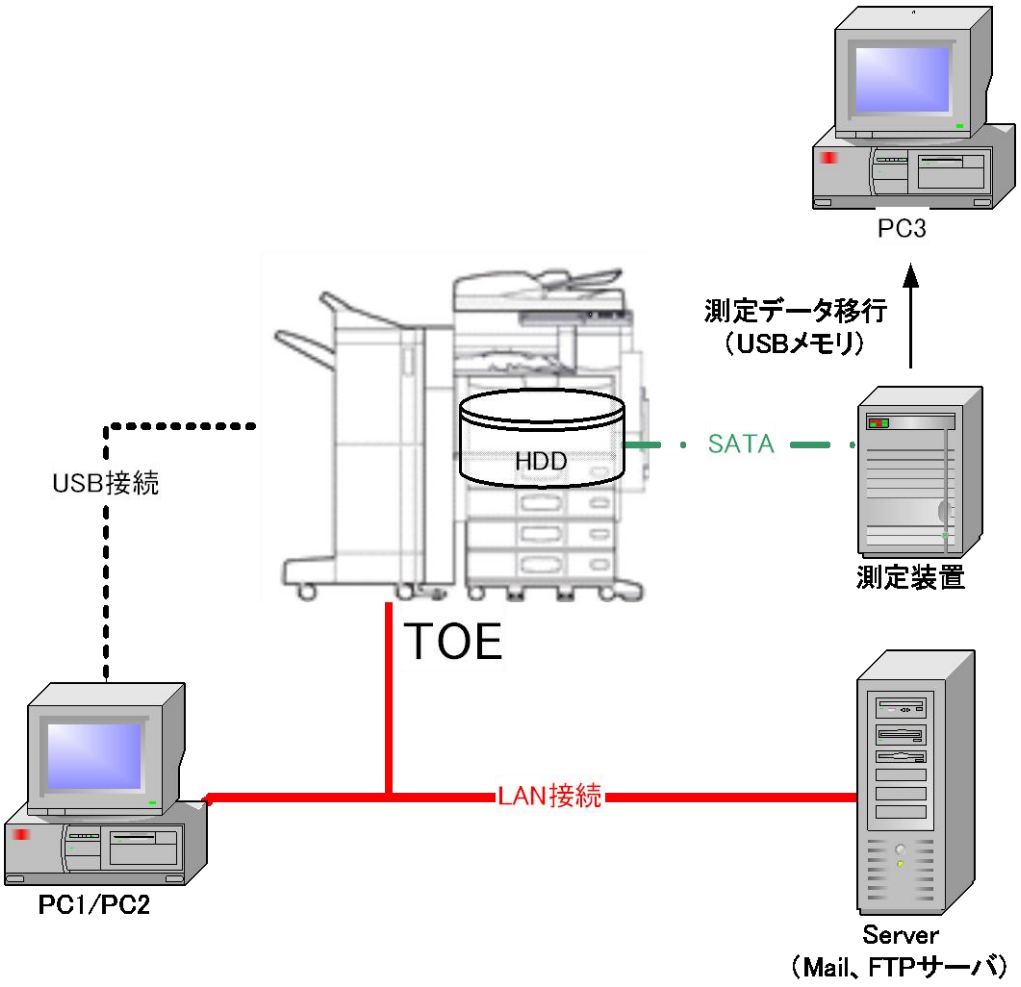

図 7-1　開発者テストの構成図

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	バージョン
TOSHIBA e-STUDIO2040C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO2540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO3040C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO3540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO4540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0

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	TOSHIBA EQUIUM 3270	
	OS	WindowsXP Professional Version2002 ServicePack3
	Client Utility Software	Print Driver　version 6.20.2521.6
		Address Viewer　version 3.2.20.0
		e-Filing BackUp/Restore Utility version 3.2.22.0
		File DownLoader　version 3.2.24.0
		TwainDriver　version 3.2.25.0
	ブラウザ	InternetExplorer8
	メーラー	OutlookExpress6
	CSV 閲覧ソフト	EXCEL2007
	Twaindriver 確認用ソフト	Microsoft Office Document Imaging Viewer version　12.0.6423.1000
PC2	DELL OPTIPLEX320	
	OS	WindowsVISTA SP2
	Client Utility Software	Print Driver　version 6.20.2521.6
		Address Viewer　version 3.2.20.0

		e-Filing BackUp/Restore Utility version 3.2.22.0
		File DownLoader version 3.2.24.0
		TwainDriver version 3.2.25.0
	ブラウザ	InternetExplorer8
PC3	HP COMPAQ dc5000sff	
	OS	WindowsXP Version2002 ServicePack3
	測定装置用ドライバ	Application Software for Serial ATA(Ver.6.20)
Server	DELL PowerEdge2650	
	OS	WindowsServer2008R2 Enterprise ServicePack1
	Mailサーバ	Exchange Server 2010 ver14.01.0270.001（POP,SMTP） ※FTPはOS機能で設定
測定装置	LeCroy SAS Suite SATA アナライザMODEL SAS001MA	

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。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

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 MFP パネルに表示されたふるまいの結果の確認
② MFP からの印刷出力結果の確認
③ MFP にアナライザ類のツールを接続し、HDD 入出力経路上のデータを解析
④ 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

⑤ 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

＜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
TeraTermPro （version 2.3）	開発者ログ取得および操作
WireShark（version 1.2.7）	プロトコルキャプチャ
PupSQLite（version 1.9.13.3）	ログデータベース確認

＜開発者テストの実施内容＞

HDD 上の対象データが暗号化されていること、アクセス制御が正しく実行されていること、SSL 通信が正常に動作していること等、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。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165項目実施された。

カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) 結果

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.3.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確

信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの環境は、開発者テストと同じ環境である。

評価の対象とした TOE を以下に示す。本 TOE には、いくつかのバリエーションが存在するが、TOSHIBA e-STUDIO3540C は TOSHIBA e-STUDIO2040C、TOSHIBA e-STUDIO2540C、TOSHIBA e-STUDIO 3040C、TOSHIBA e-STUDIO 4540C と印刷速度が異なるだけであり、セキュリティ機能の違いは無い。よって、独立テストでは、下記の TOSHIBA e-STUDIO3540C を用いてテストを実施した。独立テストの構成は、識別された TOE をすべて含んでいるとみなすことができる。

表 7-4　TOEのバリエーション

製品名	バージョン
TOSHIBA e-STUDIO3540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0

(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、厳密さにか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 TOE が提供する全てのインタフェースのタイプが、開発者テストのサンプリングテスト及び、評価者考案のテストによりカバーされるようにテストするインタフェースを選択する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストからサンプリングしたテスト項目を実施すると共に、開発者テストで考慮されていないことが懸念される入力パラメタやアクセス権限に関する TOE のふるまいをテストする。

＜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 36 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 7-5 に示す。

表 7-5 実施した独立テスト

観点	テスト概要
①	パスワードポリシーとして許可されない文字列設定時のふるまい、重複したユーザIDの登録時のふるまい、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、ファイリングボックスの排他制御、ログの操作権限、一般機能の操作権限に関して、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。

7.3.3 評価者侵入テスト

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

(3) 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、Webの各種脆弱性について懸念される。
② 公知の一般的攻撃についての探索から、操作パネル等のWeb以外のインタフェースについても、制限値を超えた入力や、想定外の文字コード入力により、TOEの予期せぬ動作が懸念される。
③ 開発証拠資料についての探索から、操作パネルからの操作と、クライアントPCからの操作が競合することによるTOEの予期せぬ動作が懸念される。
④ 開発証拠資料についての探索から、HDDの暗号化・複号、SSLプロトコルを用いた通信等のセキュリティ機能が正常に機能しないことが懸念される。

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。

侵入テスト用 PC と用いたツールの詳細を表 7-6 に示す。

表 7-6　侵入テスト用PCと使用ツール

構成品	概要
侵入テスト用PC	NEC VersaPro VJ10A/C-5 OS：Windows XP SP3
使用ツール	nmap version 5.51（ポートスキャンツール）

＜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 7-7 に示す。

表 7-7　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。 インタフェースに対して、OSコマンドや不正スクリプト等の入力を行い、各種インジェクション等の公知の脆弱性がないことを確認した。
②	操作パネルからの識別認証時に、パスワード・ユーザIDに対して、制限値以上のデータ、無効なデータ入力等の操作をしても、TOEがセキュリティ機能に影響する動作をしないことを確認した。 USBインタフェースから不正なプログラムがTOEに設置されないことを確認した。
③	利用者のパスワード変更や、TOEの設定等に関して、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。
④	紙詰まり等のエラー時の処理が暗号化操作に影響を及ぼさないこと、SSLプロトコルを用いない通信の要求があった場合に必ず接続が拒否されること、暗号鍵が正常に運用できない場合にはTOEを操作できないこと等を確認した。

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。

7.4 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。

7.5 評価結果

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

評価では以下について確認された。

PP 適合：

2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
（IEEE Std 2600.1-2009）

また、上記 PP で定義された以下の SFR パッケージに適合する。

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A 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　追加

セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

EAL3 パッケージのすべての保証コンポーネント

追加の保証コンポーネント　ALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.6 評価者コメント/勧告

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。

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 では、クライアント PC のプリンタドライバから送付されるプリントデータの受信については利用者の認証無し、Mail サーバからの e-mail の受信については利用者の識別認証無しに許可される。そのため、プリントデータの受信時、e-mail の受信時に識別認証を期待する消費者にとっては、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、消費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。

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-STUDIO2040C/2540C/3040C/3540C/4540C
MULTIFUNCTIONAL DIGITAL SYSTEMS Security Target Version 1.1
October 13, 2011　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。

AES	Advanced Encryption Standard
CSV	Comma Separated Values
DoD	United States Department of Defense
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HDD	Hard Disk Drive
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
SATA	Serial Advanced Technology Attachment
SMB	Server Message Block
SSL	Secure Socket Layer
TWAIN	Tool Without An Interesting Name
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。

Address Book Viewer	クライアントPCからe-mail Address Bookの管理が行えるソフトウェア
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
e-Filing Box Backup/Restore Utility	クライアントPCからファイリングボックス内のデータをクライアントPCにバックアップ/リストアすることができるソフトウェア

Built-in Administrator Account	MFPに初期登録される管理者アカウント
TWAIN Driver/ File Downloader	クライアントPCからTCP/IPネットワーク経由でMFP内のファイリングボックスに格納されたデータをダウンロードすることができるソフトウェア
TopAccess	クライアントPCからジョブデータやMFPの管理及びファイリングボックスの操作が行える、Webベースのソフトウェア
U.ACCOUNTMANAGER（アカウント管理者）	ユーザアカウント情報（利用者のユーザIDや基本機能の使用許可権限の変更）の変更等が行える特権利用者。
U.ADMINISTRATOR（TOE管理者）	TOEのセキュリティポリシーに影響を与える設定の管理・変更が行える特権利用者
U.AUDITOR（ログ監査者）	外部ネットワークからMFPのログを閲覧・データマイニングすることができる特別な利用者
U.FAXOPERATOR（ファックスオペレータ）	インターネットファックス機能を用いて文書データの送信、受信データのプリント、文書データ・ジョブデータの操作が行える特別な利用者
U.NORMAL（一般利用者）	TOEの文書データ処理機能（コピー/プリント/スキャン/ファイリング）が利用できる一般利用者
Internet Fax function（インターネットファックス機能）	スキャンした文書データをTIFF-FX(Profile S)ファイルとしてe-mailに添付し送信する機能 インターネットファックスでは、スキャンした文書を送信する際に、電話番号の代わりに、インターネットFAX機器またはクライアントPCのe-mailアドレスを指定する必要がある
Copy function（コピー機能）	操作パネルから一般利用者がMFPに読み込んだデータを紙に印刷する機能
Scan function（スキャン機能）	HDDにスキャンデータを保存し、保存されたデータを読み取ることができる機能 一般利用者がスキャナユニットから文書データを読み込むと、MFPに設定された情報に基づいて自動的にクライアントPC、MailサーバまたはFTPサーバに通知する 一般利用者は、操作パネルからこの機能を実施することができる
e-Filing function（ファイリング機能）	利用者がファイリングボックスを作成できる機能 特定の一般利用者もしくはTOE管理者が秘密文書を保存することができ、その文書のプリント、編集等も行える
e-Filing Box（ファイリングボックス）	利用者が文書データを保存することができる記憶領域 操作パネルもしくはクライアントPCから保存したデータの参照、プリント、編集が行える
Print function（プリント機能）	TOEとLANもしくはUSB接続されたクライアントPCからのプリントデータを受け取り、紙に印刷する機能

12 参照

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

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

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

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

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

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

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

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

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

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

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

[12] TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS Security Target Version 1.1 October 13, 2011 TOSHIBA TEC CORPORATION

[13] TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS 評価報告書, 第2.10版, 2011年10月13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