認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	平成20年2月21日 (IT認証8199)
認証番号	C0194
認証申請者	東芝テック株式会社
TOEの名称	日本語名：e-STUDIO5520C/6520C/6530C用 システムソフトウェア 英語名：System Software for e-STUDIO5520C/6520C/6530C
TOEのバージョン	V3.0
PP適合	なし
適合する保証パッケージ	EAL3
開発者	東芝テック株式会社
評価機関の名称	株式会社電子商取引安全技術研究所 評価センター

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年11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　鈴木　秀二

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1版（翻訳第1.2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1版 （翻訳第1.2版）

評価結果：合格

「日本語名：e-STUDIO5520C/6520C/6530C用 システムソフトウェア 英語名：System Software for e-STUDIO5520C/6520C/6530C」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「日本語名：e-STUDIO5520C/6520C/6530C用 システムソフトウェア　英語名：System Software for e-STUDIO5520C/6520C/6530C」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である東芝テック株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。STはデジタル複合機の調達者や利用者を読者と想定し、本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：　日本語名：e-STUDIO5520C/6520C/6530C用 システムソフトウェア
英語名：System Software for e-STUDIO5520C/6520C/6530C
バージョン：　V3.0
開発者：　東芝テック株式会社

1.2.2 製品概要

本TOE は東芝テック株式会社製デジタル複合機「e-STUDIO5520C/6520C/6530C」（以下「e-STUDIO」という。）の制御ソフトウェアであり、オプション製品GP

-1070 またはGP-1100 にて活性化され有効となる。

e-STUDIOの主な機能にはコピー、スキャン、プリント、ファクス、ファイリングボックス/共有フォルダ機能（以下「一般機能」という。）がある。TOE はこれら一般機能使用時にHDD に書き込まれたユーザ文書データを削除する際、復元不可能な方法にて消去を行う機能を提供する。また、HDD の廃棄・交換時の際、サービスエンジニアによって全ての記録領域を消去する機能を提供する。これらの機能によりHDD 内のユーザ文書データの復元を防止する。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOE の利用環境

TOEを搭載したe-STUDIOは、一般的なオフィス等に設置され、単独で複合機として利用される他に、図1-1に示すようなネットワーク環境でも、FAXとのデータ送受信端末、メールサーバへのメール発信端末、リモートにあるPCのリモートプリンタとして使われる。

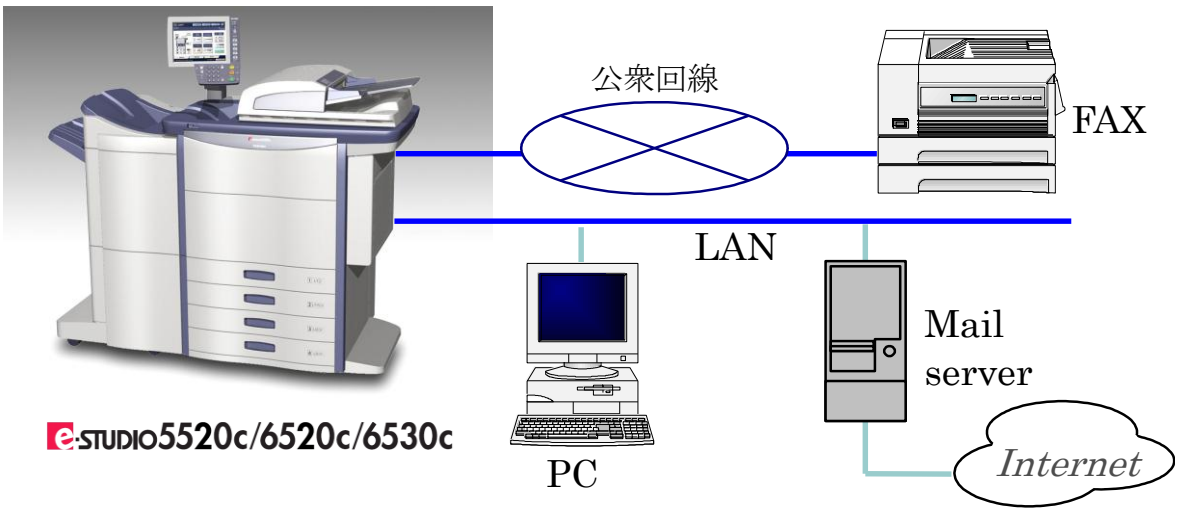

図1-1　利用環境例

1.2.3.2 TOE の機能

TOEは、利用者がコピーやスキャン等を行う「通常モード」とサービスエンジニアの保守のための「自己診断モード」がある。

① 通常モード

図1-2に通常モードの起動後の構成を示す。これは電源投入後、HDDよりプログラムデータをロードし、実行可能となった状態である。

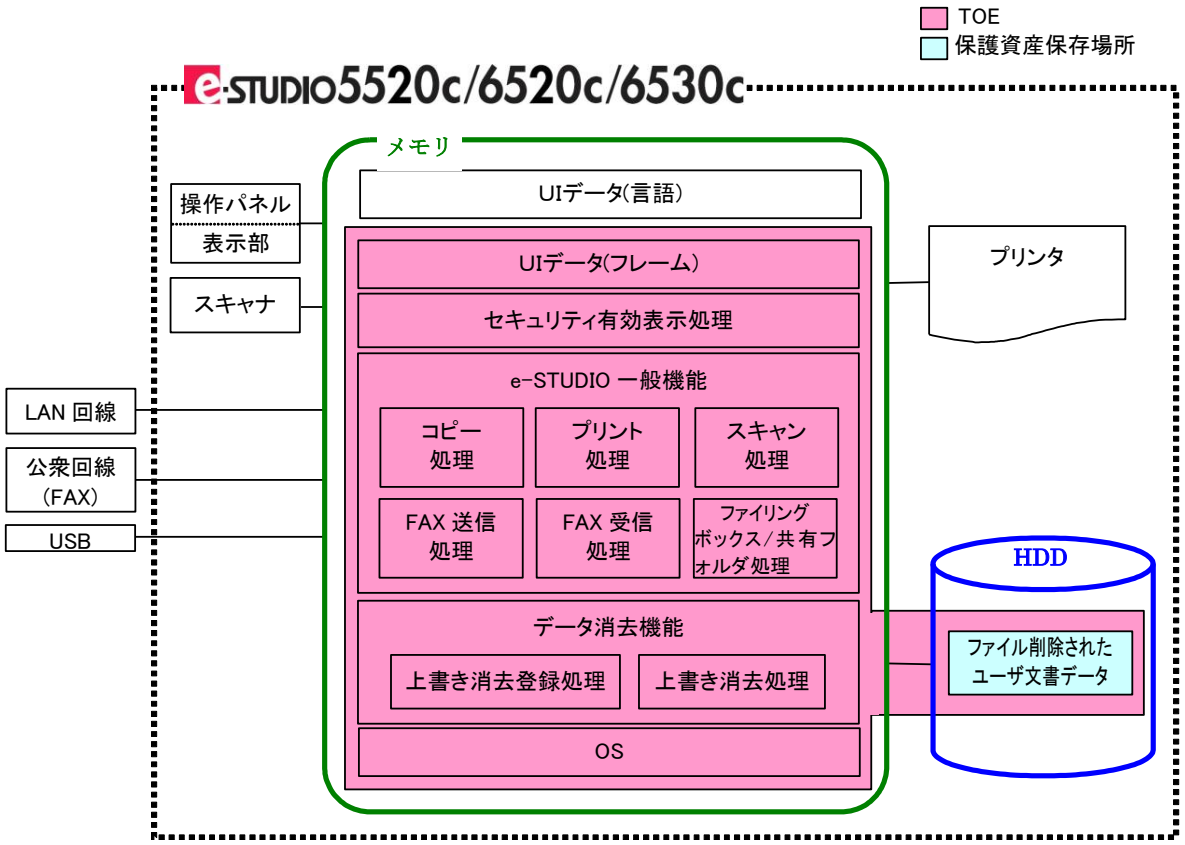

図1-2　通常モードの構成

以下にTOEの機能を説明する。

(1)　セキュリティ有効表示処理

操作パネルからカウンタボタンを押すと印刷カウンタ画面が表示され、セキュリティ機能が有効になっているとデータ消去を表すアイコンとTOEバージョン[SYS V3.0]の表示を行う。

(2)　コピー処理

操作パネルよりコピーボタンを選択し、スキャナからユーザ文書データを読み取りHDDの作業領域へ書き出し、その作業領域のデータを利用してプリンタより出力を行う。また、コピー設定にてプリンタ出力と同時にHDDのファイリングボックスまたは共有フォルダへの保存が行える。

(3)　プリント処理

プリント処理は以下に示す方法で使用できる。

・LAN回線、USB回線（e-STUDIOをプリンタとして使用）

・LAN回線（TopAccessからの使用）

・操作パネル

上記方法よりプリント処理が起動されるとユーザ文書データをHDD上の作業領域へ書き出し、プリンタより出力を行う。ユーザ文書データをファイリングボックスへ保存する場合は作業領域のデータを利用してデータの保存を行う。

(4)　スキャン処理

スキャン処理は操作パネルとLAN回線から使用できる。

操作パネルからはスキャンボタンを選択し、スキャナからユーザ文書データを読み取りHDD上の作業領域へ書き出し、ファイリングボックス、共有フォルダへの保存やUSBメディアへの保存や、指定した送信先へのE-Mail送信を行う。

LAN回線からは、Windows Vista搭載クライアントPCよりLAN上のe-STUDIOをスキャナとして使用できるWSスキャン機能があり、スキャナからユーザ文書データを読み取り、スキャン要求を行ったPCに画像データを送信する。

(5)　FAX送信処理

FAX送信処理は操作パネルとLAN回線及びUSB回線から使用できる。

操作パネルからはファクスボタンを選択し、スキャナからユーザ文書データを読み取りHDD上の作業領域へ書き出し、その作業領域のデータを利用して公衆回線(FAX)よりFAX送信、またはLAN回線よりインターネットファクスの送信を行う。

LAN回線及びUSB回線からは、クライアントPCでN/W-Faxドライバを選択すると、ユーザ文書データのFAX送信またはインターネットファクス送信が行える。

(6)　FAX受信処理

公衆回線(FAX)よりFAXデータを受信したとき、またはLAN回線よりインターネットファクスデータを受信したとき、受信したデータをHDD上の作業領域へ書き出し、そのデータを利用してプリンタへの出力やファイリングボックスまたは共有フォルダへ保存する。

(7)　ファイリングボックス/共有フォルダ処理

ファイリングボックス/共有フォルダ処理は、操作パネル、LAN回線(TopAccess)から使用される。

操作パネルからファイリングボックスボタンを選択し、ボックスに保存されているユーザ文書データの印刷、編集、削除、E-Mail送信を行う。

TopAccess画面よりボックスに保存されているユーザ文書データの印刷、編集、削除、E-Mail送信、アーカイブ、アーカイブのアップロードを行う。

また、ファイリングボックスや共有フォルダに保存され有効期限の切れたユーザ文書データファイルを削除する。

(8)　上書き消去登録処理(セキュリティ機能)

上記(2)～(7)の処理にてユーザ文書データを削除する際に、上書き消去登録(パスのみ登録)する。この処理により削除ファイルは上書き消去処理の対象ファイルとなる。

(9)　上書き消去処理(セキュリティ機能)

上書き消去登録処理により削除されるユーザ文書データの格納領域を監視し、その領域に対し完全消去を行う。ユーザ文書データの完全消去処理実行中は、「データ消去中」を操作パネルに表示する。

②　自己診断モード

図1-3に自己診断モードの起動後の構成を示す。これは電源投入後、HDDよりプログラムデータをロードし、実行可能となった状態である。

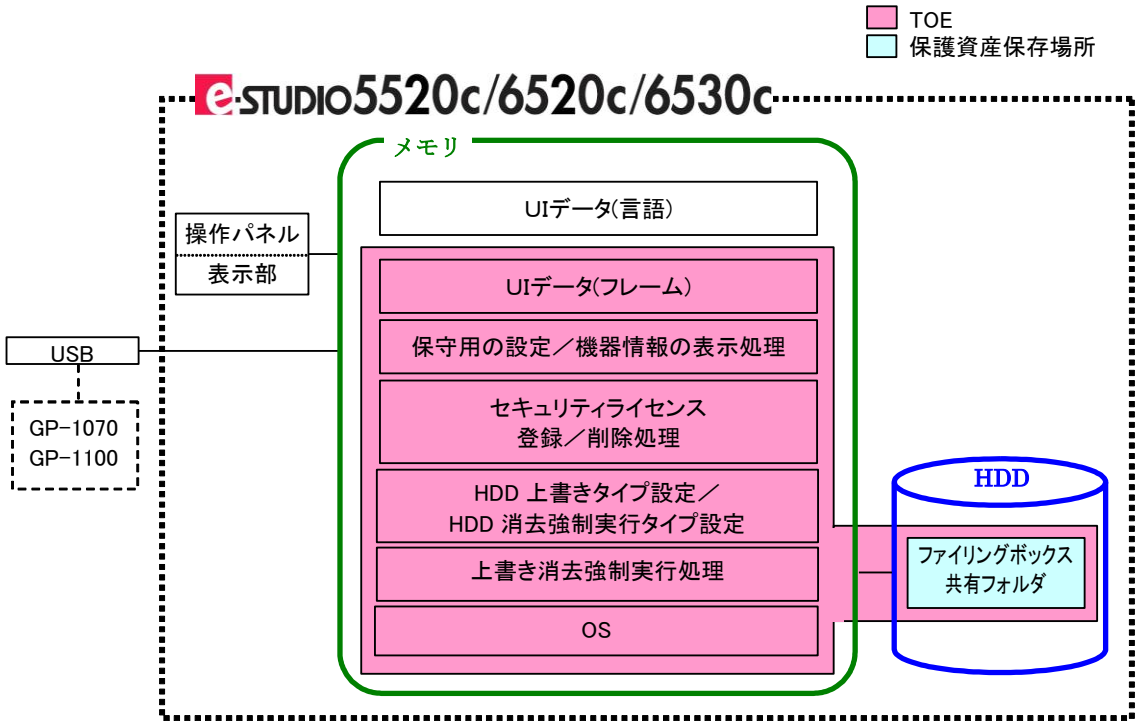

図1-3　自己診断モードの構成

以下にTOEの機能を説明する。

（1） 保守用の設定/機器情報の表示処理

テストプリントやハードウェアの調整、ファームウェアアップデート等のサービスエンジニアが使用する保守用の機能である。

（2） 上書き消去強制実行処理(セキュリティ機能)

e-STUDIOの廃棄やHDDの交換を行う際、操作パネルから実行し、HDDに残っているユーザ文書データを一括して完全消去する。

（3） セキュリティライセンス登録/削除処理

GP-1070またはGP-1100によりライセンス登録または削除を行う。本機能によりセキュリティ機能の有効/無効が設定される。

（4） HDD上書きタイプ設定/HDD消去強制実行タイプ設定

通常モード時のデータ消去機能と、自己診断モード時の上書き消去強制実行の上書きタイプの設定を行う。

1.2.3.2 TOE の保護資産

以下に通常モード及び自己診断モードにおける保護資産を記す。

- 通常モードにおける保護資産

  ユーザ文書データ削除後にHDDに磁気的に残っている残存データが保護資産である。保護資産は次の場合に発生する。

  ① 利用者が指定したジョブ中またはジョブの終了（キャンセルを含む）によりe-STUDIOがユーザ文書データを削除した場合

  ② e-STUDIOが有効期限の切れたユーザ文書データを自動的に削除した場合

- HDDの廃棄・交換時の保護資産

  廃棄するe-STUDIO内のHDDや交換するHDDに残っているユーザ文書データが保護資産である。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。

② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリ

ティ機能要件を満たしていること。

③　本TOEがセキュリティ設計に基づいて開発されていること。

④　上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「e-STUDIO5520C/6520C/6530C用 Security Target」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1（[5][8]のいずれか）附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「評価報告書(WOE-ETR-0001-00)」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4　評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。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。評価は、平成20年11月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
T.TEMPDATA_ACCESS	悪意を持った利用者または非関係者が人目につかずにe-STUDIOからHDD を取り外し、既存のツールを使用して、e-STUDIO のHDD から削除されたユーザ文書データを復元・解読することにより、ユーザ文書を取り出すかもしれない。
T.STOREDATA_ACCESS	悪意を持った利用者または非関係者が、既存のツールを使用して、廃棄または交換したe-STUDIOのHDDからユーザ文書を取り出すかもしれない。

2.1.2 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-2に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表2-2 TOE使用の前提条件

識別子	前提条件
A.TRUST_SE	サービスエンジニアはe-STUDIO の自己診断モードの操作に必要な知識を持ち、不正な操作は行わないと想定する。(注) (注:不正な操作には上書き消去強制実行中の電源の切断も含む)
A.NO_ERASE_STOP	電源の切断により通常モード時の上書き消去処理が中断されることは想定していない。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。読者は、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。

【日本版】

- 取扱説明書
  安全にお使いいただくために（OMJ080001A0）
  クイックスタートガイド（OMJ08000300）
- サービスマニュアル
  e-STUDIO5520C/6520C/6530Cサービスマニュアル(SMJ070017C0)

【海外版】

- 取扱説明書
  Safety Information（OME080002A0）
  Quick Start Guide（OME08000400）
- サービスマニュアル
  e-STUDIO5520C/6520C/6530C Service Manual（SME070016C0）

2.1.5 構成条件

本TOEは、東芝テック株式会社製デジタル複合機e-STUDIO5520C、e-STUDIO6520C、e-STUDIO6530Cで動作する。

2.2 セキュリティ対策

TOEは、2.1.1の脅威に対抗するために、以下のセキュリティ機能を具備する。

① データ消去機能

e-STUDIO の一般機能の処理によって一時的に作業領域を生成し格納されたユーザ文書データまたは、ファイリングボックス/共有フォルダ内に格納されているユーザ文書データは、次のタイミングでデータ消去機能により削除される。

- 利用者が操作したジョブの処理中またはジョブの終了
- ファイリングボックス/共有フォルダ内のユーザ文書データの保存期限切れ

データ消去機能は、上書き消去登録処理及び上書き消去処理から構成される。

上書き消去登録処理は、上記のタイミングで、消去対象の格納領域のパスを登録する。上書き消去処理は、登録されたパスから特定された格納領域に00、FF、ランダムのデータを上書した後、領域を開放し完全に消去する。上書き中「データ消去中」を操作パネルに表示する。

② 上書き消去強制実行機能

HDD に存在するユーザ文書データファイルを含む全記憶領域を00、FF、ランダムのデータで上書後初期化する。

3 評価機関による評価実施及び結果

3.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年2月に始まり、平成20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20年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20年8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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 製品テスト

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

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図3-1　開発者テストの構成図に示す。

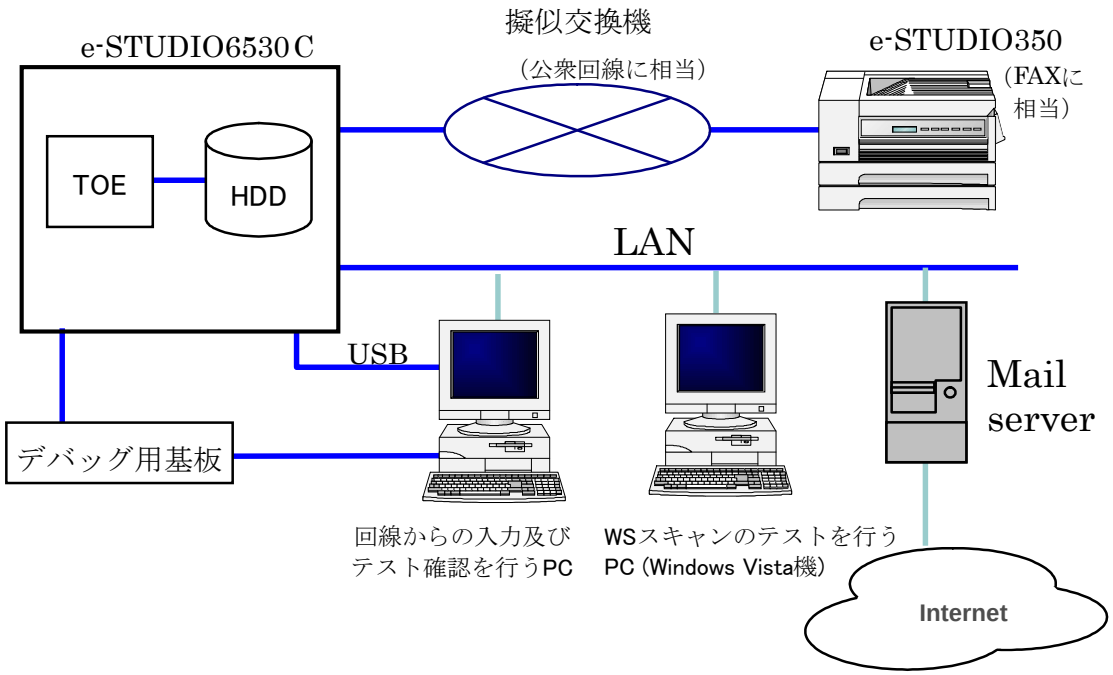

図3-1　開発者テストの構成図

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。

本TOEのセキュリティ機能は２つあり、２つの動作モード（通常モード、自己診断モード）で各々のセキュリティ機能は動作する。そのため、各モードでセキュリティ機能が動作する機能の全テスト、異常系テストを実施している。以下が代表的なテスト例である。

- 通常モード

  操作パネルからのコピー機能、スキャン機能、ファイリングボックス機能

  電源断、回線、大量データ、同時利用等の異常系テスト
- 自己診断モード

  上書き消去強制実行

  HDD上書きタイプ設定

  ファームウェアアップデート

また、上記テストからセキュリティ機能が確実に動作しているか、確認するために、入力用PC(デバック用PC)からHDDへの上書き消去の状況を処理単位に確認している。

b. 実施テストの範囲

テストは開発者によって104項目実施されている。

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

c. 結果

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

3.3.2 評価者独立テスト

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、開発者テストと同様の構成である。

評価者が実施したテストの構成を図3-1に示す。評価者テストは本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) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

① 開発者テストとは異なる手段を用いた通常モードのセキュリティ機能をテストする。

② 開発者テストで実施しているテストのパラメタを変化させてテストする。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

独立テストとして、6件のテストを実施した。テストの考案に当たっては、開発者テストとは異なる手段（異なるブラウザ、異なるメーラ、異なる条件での印刷）、開発者テストで実施しているテストのパラメタの変化（ファイリングボックスの消去、上書き消去タイプ）を考慮することにより、開発者テストの厳密性、十分性を補足した。

なお、評価者テストにおいても開発者テストと同様に、上書き消去が確実に行われているか、入力用PC(デバック用PC)からHDDへの上書き消去の状況を処理単位に確認している。

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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性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テストは以下のとおり。

a. 懸念される脆弱性

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

公知の脆弱性の探索の結果からは、IPAからの公開情報である、「SIP に係る既知の脆弱性に関する調査報告書」の「デバッガ機能へ接続可能な実装の問題」1件を識別し、合わせて、CEMの「一般的な脆弱性に関するガイダンス」の確認事項を証拠資料より探索を行って、バイパス、改ざんや誤使用に関する16件の侵入テストの候補となる脆弱性の識別を行い、分析した結果、5件の侵入テストの項目を設定した。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の5件の侵入テストを実施した。

	脆弱性	テストの目的
1	使用しないポートが閉じられていること	実績のあるスキャニングツール(Nmap)、及びインターネット上の脆弱性情報を使用し、TOE に存在

	を確認する。	する明白な脆弱性を検出する。
2	ライセンス情報削除時の処理	ライセンス情報を削除したときにユーザの気が付かないまま上書き消去機能が無効な状態にならないことを確認する。
3	処理繁忙によるデータ消去タスク機能の機能不全	多数のジョブが同時実行しデータ消去タスク機能が正しく動作することを確認する。実施するテストではE-Mail受信、FAX受信、共有ボックス内データの印刷、ボックス内データの削除、スキャンのジョブを同時実行させる。 e-STUDIOを繁忙状態においたときであっても、上書き消去機能が確実に動作することを確認する。
4	開発用インタフェースの不正利用によるTSFの改ざん	開発用インタフェースが不正に使用されないように、保護機能が働いており、操作の推測によって不正使用されないことを確認する。
5	ファームウェア更新インタフェースの不正利用によるTSFの改ざん	機種をチェックし不正更新を防止する機能を持っている。この保護機能が働いており不正なソフトウェアに改ざんできないことを確認する。

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超える潜在的な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 評価結果

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

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

4 認証実施

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

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

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。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たすものと判断する。

5.2 注意事項

特になし。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

HDD	Hard Disk Drive
LAN	Local Area Network
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。

e-STUDIO	東芝テック株式会社製デジタル複合機。主に、コピー、スキャン、プリンタ、ファックスの機能を1台に集約した多機能周辺機器。本書では、e-STUDIO5520C/6520C/6530Cを指す。
TopAccess	Webベースのジョブ、及びデバイスの管理ツール このツールを使用すると、インターネットを介してe-STUDIOの情報を取得することができ、ユーザ用、及び管理者用の2種類のWebサイトを使用することができる。
WSスキャン	WS（Web Service）スキャンは、Windows Vistaコンピュータに搭載される機能を利用し、ネットワークを介したコンピュータとのスキャン操作を行う機能。本機でスキャンを行った画像のコンピュータへの保存や、コンピュータのWIA(Windows Imaging Acquisition)Scan Driver対応アプリケーションから本機にスキャン要求を行っての画像取得ができる。
一般機能	e-STUDIOに実装されている機能の内、一般の利用者が利用可能な、コピー、スキャン、プリント、ファクス、ファイリングボックス/共有フォルダ機能を指す。
共有フォルダ	ユーザ文書データをJPEGやPDFといったファイル形式で保存し、ネットワーク上のクライアントPCよりファイルの取得

	が行える場所。ファイル保存の有効期限が過ぎると、保存されているユーザ文書データは削除される。
削除	資源の割り当てを解除し、ユーザにとって使用不可能な状態にすること。
消去	痕跡を残さずに消し去ること。
ジョブ	e-STUDIO一般機能の処理が行われる単位。
ファイリングボックス	利用者が、ユーザ文書データの保存を行う場所。保存後、操作パネルやTopAceessより、データの参照，印刷，編集が行える。ファイル保存の有効期限が過ぎると、保存されているユーザ文書データは削除される。
ユーザ文書データ	e-STUDIO内に存在する電子化された状態のユーザ文書を指す。スキャナにて電子化され取り込まれたユーザ文書や、e-STUDIOが受信した電子化されているユーザ文書や、それらをe-STUDIO内にて加工したデータ。

7 参照

[1] e-STUDIO5520C/6520C/6530C用 Security Target Ver.1.3 2008年11月17日 東芝テック株式会社

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

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

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

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

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 1 September 2006 CCMB-2006-09-003

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

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-002 (平成19年3月翻訳第1.2版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-003 (平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 Revision 1 September 2006 CCMB-2006-09-004

[12] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-004 (平成19年3月翻訳第1.2版)

[13] 評価報告書(WOE-ETR-0001-00) 2008年11月17日 株式会社電子商取引安全技術研究所 評価センター

JISEC

サーベイランス報告書

発行日　：　2012-08-17

資料番号：　SRP-C0194-01

下記評価対象(以下「本TOE」という。）について、ITセキュリティ認証申請手続等に関する規程(CCM-02)8.1に基づき、サーベイランスが実施されたことを報告いたします。認証報告書と合わせて参照願います。

評価対象：

認証番号	C0194
認証申請者	東芝テック株式会社
TOEの名称	日本語名：e-STUDIO5520C/6520C/6530C用 システムソフトウェア 英語名：System Software for e-STUDIO5520C/6520C/6530C
TOEのバージョン	V3.0
PP適合	なし
適合する保証パッケージ	EAL3
開発者	東芝テック株式会社
評価機関の名称	株式会社電子商取引安全技術研究所 評価センター

サーベイランス管理番号：JISEC-SV12-001

サーベイランス実施報告：

- サーベイランス結果

本サーベイランスに関し、評価機関により本TOEを安全に消費者が利用することが可能であることが確認されたため、本TOEに対する認証は維持されます。

- サーベイランス概要

本TOEに関して開発者より公開された以下の「お知らせ」の内容に関し、認証を維持することが適切かどうかを判断するために2012年4月から同年7月にかけてサーベイランスを実施しました。

http://www.toshibatec.co.jp/page.jsp?id=2330

「お知らせ」によると、公表された脆弱性を利用することで、Webベースの管理ユーティリ

ティ「TopAccess」の管理者向けのページにパスワードなしでアクセス可能とされています。

サーベイランスの結果、管理者向けのページへのアクセスは、評価対象のセキュリティ機能以外への影響は否定できないが、評価対象であるセキュリティ機能への影響がないことが、評価機関の責任において当時の評価で検証済であることが示されました。

詳細を以下に示します。

本TOEには有効期限が過ぎると保存されているユーザ文書データを自動的に削除する機能があり、削除後の残存データを保護資産としています。

「TopAccess」の管理者向けのページからは、MFPの時計の日時や、ユーザ文書データを保存する有効期限などを変更することができるため、本TOEのセキュリティ機能である上書き消去機能が利用者が想定した有効期限の通りに実施されないことが懸念されました。

ただし、公表された脆弱性を利用して「TopAccess」の管理者向けのページにアクセスした場合には、MFPの時計の日時や、ユーザ文書データを保存する有効期限などの変更はできないことが開発者より主張されています。

本懸念に対して、評価機関は当時の評価に基づく以下の判断をいたしました。

(1) 公表された脆弱性を利用して「TopAccess」の管理者向けのページにアクセスした場合、MFPの時計の日時や、ユーザ文書データを保存する有効期限などを変更できるかどうかは、当時の評価では未調査である。

(2) 保護資産は有効期限が切れて削除が実施された場合の残存情報であり、有効期限に関連する設定が変更されて削除されなかった場合は保護資産とならないことが、消費者にとって自明である。つまり、消費者が本懸念を抱くことはない。

(3) したがって、公表された脆弱性を利用して「TopAccess」の管理者向けのページにアクセスして、MFPの時計の日時や、ユーザ文書データを保存する有効期限などを変更できたとしても、保証されたセキュリティ機能には影響しない。

「TopAccess」の管理者向けのページから使用できるそれ以外の機能に対しても、評価対象であるセキュリティ機能への影響がないことが、評価機関において当時の評価で検証されていることが報告されています。

以上