認　証　報　告　書

評価対象

申請受付年月日（受付番号）	平成16年9月3日（IT認証4033）
認証番号	C0023
認証申請者	東芝テック株式会社
TOEの名称	日本語名：スクランブラボードGP-1031 英語名　：Scrambler Board GP-1031
TOEのバージョン	V2.0
PP適合	なし
適合する保証要件	EAL2
TOE開発者	東芝テック株式会社
評価機関の名称	社団法人 電子情報技術産業協会 ITセキュリティセンター

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17年3月9日

独立行政法人 情報処理推進機構
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　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「日本語名：スクランブラボードGP-1031、英語名：Scrambler Board GP-1031」は、独立行政法人 情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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：スクランブラボードGP-1031、英語名：Scrambler Board GP-1031」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（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や本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応する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、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称: 日本語名：スクランブラボードGP-1031
英語名 ：Scrambler Board GP-1031
バージョン:V2.0
開発者: 東芝テック株式会社

1.2.2 製品概要

本製品は、東芝テック株式会社製デジタル複合機「e-STUDIO 3511/4511」にオプションとして実装される製品である。

本製品は、e-STUDIO 3511/4511の機能であるコピー、プリント、スキャン、FAXのジョブ完了後、及びファイリングボックスの削除後にHDD上に残存するイメージデータ（以下「ユーザ文書残存データ」という。）の保護を行う。

1.2.3 TOEの範囲と動作概要

本TOEは、スクランブラボード及び、スクランブラボードを操作させるソフトウェアから構成される。TOEの物理的範囲として、図1、図2にTOEを実装した「e-STUDIO 3511/4511」のハードウェア及びソフトウェア構成について示す。

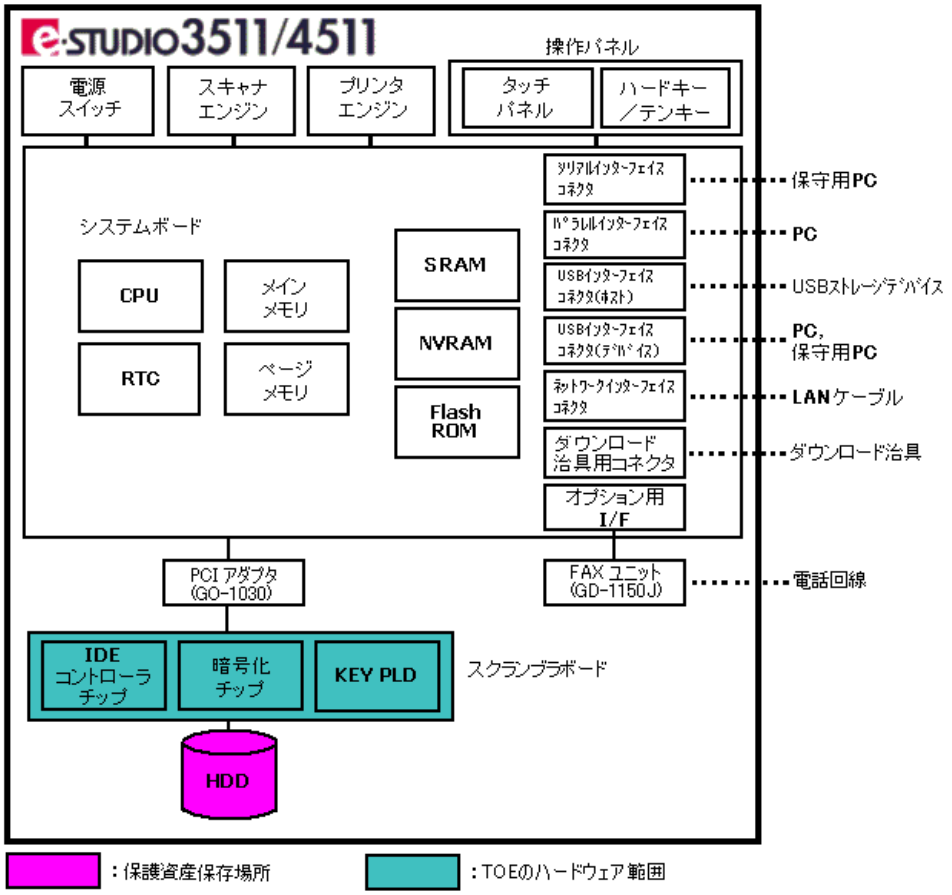

図1-1　TOEを実装した「e-STUDIO　3511/4511」のハードウェア構成

図1-1における、TOEのハードウェア構成要素は以下の通りである。

- スクランブラボード
  HDDにデータを書き込むときに暗号化を、データをHDDから読み出すときに復号を行う。「IDEコントローラチップ」「暗号化チップ」「KEY PLD」が実装されている。
- IDEコントローラチップ
  HDDへのデータ転送を制御する論理素子（チップ）。
- 暗号化チップ
  HDDに書込むデータを暗号化し、HDDから読出すデータを復号するチップ。
- KEY PLD
  e-STUDIO3511/4511起動時にシステムボード上のSRAMからスクランブラボード上に転送される暗号鍵データを保存する揮発性の論理素子(チップ)。

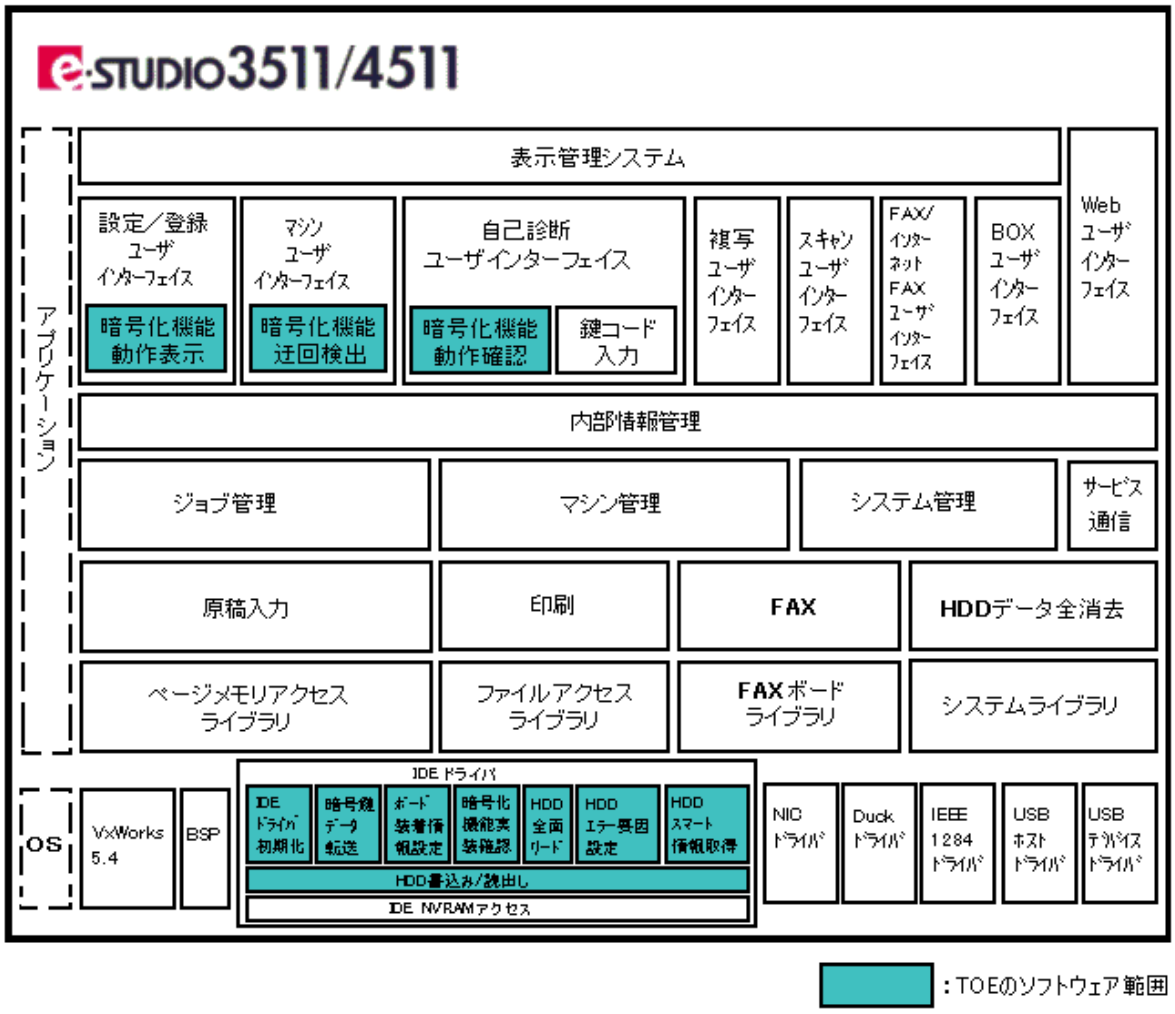

図1-2　TOEを実装した「e-STUDIO　3511/4511」のソフトウェア構成

図1-2における、TOEのソフトウェア構成要素は以下の通りである。

- 暗号化機能動作確認 V 1.1
  スクランブラボードの装着有無情報をNVRAMから読出す要求を行う
- IDEドライバ V 1.0
  HDDにアクセスするための基本的な機能を提供する。「HDD書込み/読出し」「IDEドライバ初期化」「暗号鍵データ転送」「ボード装着情報設定」「暗号化機能実装確認」「HDD全面リード」「HDDエラー要因設定」「HDDスマート情報取得」で構成される。
  - HDD書込み/読出し
    HDDへのすべての書込み/読出し処理を行う。
  - IDEドライバ初期化
    IDEドライバの初期化を行う。
  - 暗号鍵データ転送
    システムボード上のSRAM から暗号鍵データを取り出し、スクランブラボー

ド上のKEY PLDに暗号鍵データの転送を行う。また、転送時には暗号鍵データのチェックを行い、正しければ、システムライブラリを使用して暗号鍵データが正常に転送されたことを示す情報をSRAMに書込む。

- ボード装着情報設定
  システムボード上のNVRAMにスクランブラボードの装着有無情報の設定を行う。
- 暗号化機能実装確認
  スクランブラボードの装着状態の確認を行う。
- HDD全面リード
  HDDに書込み/読出しできない領域が無いか確認を行う。
- HDDエラー要因設定
  暗号化機能実装確認時のHDDエラー要因情報へのアクセスを行う。
- HDDスマート情報取得
  スマート情報(HDD自身によってHDD内に保存される動作履歴情報、通電時間、電源を入れた回数、内部エラー回数など)の取得を行う。

・ 暗号化機能動作表示 V1.0
  暗号化機能正常動作時に TOE の型名とバージョンの表示を行う。
・ 暗号化機能迂回検出 V1.0
  暗号化機能実装確認により設定されたHDDエラー要因情報を取り出し、エラーが検出された時、操作パネルにサービスマンコール表示を行う。

1.2.4 TOEの機能

TOEの機能とTOEの関係者を以下に示す。

(1) TOEの機能
TOEは以下に示す機能を持つ。

・ HDDデータ暗号化／復号
  e-STUDIO利用者が、e-STUDIO 3511/4511が提供する主な機能を利用する際に、ユーザ文書データを暗号化してHDDに保存する。ジョブ要求時に、HDDに暗号化されて保存されているユーザ文書データを読出して復号する。
・ 暗号化機能迂回検出
  スクランブラボードの装着状態の確認結果が異常であれば、操作パネル上にサービスエンジニアの呼出しを要求するサービスマンコール表示を行い、e-STUDIO 3511/4511の機能利用を停止する。
・ 暗号化機能実装確認
  e-STUDIO 3511/4511の起動時に、スクランブラボードの装着状態の確認を行う。

- 暗号化機能動作表示
  暗号化機能が正常に動作しているとき、操作パネルからの表示要求により、TOEの型名とバージョンの表示を行う。
- 暗号化機能動作確認
  NVRAMに設定されているスクランブラボードの装着有無情報を取得する。
- IDEドライバ初期化
  e-STUDIO 3511/4511 の起動時に、暗号化機能実装確認を実行する。暗号化機能実装確認による、スクランブラボードの装着状態の確認結果が正常であれば、暗号鍵データ転送を実行する。
- HDDエラー要因設定
  スクランブラボード装着確認で異常の場合、HDDエラー要因情報の取得を行う。
- 暗号鍵データ転送
  システムボードのSRAMから暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。
- ボード装着状態設定
  スクランブラボードの装着有無の情報をシステムボードのNVRAMに設定する。
- HDD全面リード
  HDDに書込み/読出しできない領域が無いか確認を行う。
- HDDスマート情報取得
  スマート情報の取得を行う。

(2) TOEの関係者

本TOEに関与する人物と役割を以下に定義する。

- e-STUDIO利用者
  e-STUDIO 3511/4511におけるコピー等、デジタル複合機の一般的な機能を利用する。
- e-STUDIO利用部門の責任者
  e-STUDIO管理者を任命する。
- e-STUDIO管理者
  e-STUDIO 3511/4511に関する運用管理を行う。
- サービスエンジニア
  e-STUDIO 3511/4511の設置場所において、e-STUDIO 3511/4511の設置、インストール、及び保守業務を行う。
- e-STUDIO非関係者
  特定の役割はないが、e-STUDIO 3511/4511に物理的、または外部ネットワークや電話回線を介してアクセスが可能である。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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-STUDIO 3511/4511用 スクランブラボードGP-1031 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][11][14]のいずれか）附属書C、CCパート2（[6][9][12][15]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][13][16]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、「e-STUDIO　3511/4511用スクランブラボードGP-1031 V2.0 評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、本評価報告書、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17年2月の評価機関による本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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

本STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、一般のオフィス等で使用される商業的製品であるデジタル複合機に実装されるものであり、想定される攻撃は公開情報を利用した不正行為である。一般のオフィス等で使用されるため、攻撃者である悪意を持ったe-STUDIO利用者及びe-STUDIO非関係者が攻撃を行う際は周囲に注意する必要があり、TOEにアクセス可能な時間を制限される。以上のことから攻撃者の攻撃能力は低レベルとなることが想定される。従って、最小機能強度として”SOF-基本”を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

- HDDデータ暗号化／復号機能
  TOEは、イメージデータのHDDへのデータの書き込み時の暗号化操作及び読出し時の復号操作に対し、暗号化アルゴリズムとして、Triple DES（FIPS PUB 46-3）、鍵長112bitを使用して暗号化、復号を行う。

- 暗号化機能迂回検出機能
  TOEは、セキュリティ侵害の可能性（スクランブラボードの取り外し事象または、スクランブラボード以外の不正なボード装着事象）を検出した場合、操作パネルへサービスエンジニア呼出しを要求するサービスマンコール表示を行い、「e-STUDIO3511/4511」の機能の利用を停止する。

- 暗号化機能動作表示機能
  TOEは、TOEの関係者に暗号化機能が適切に動作していることを確認できるように、監査記録情報を読出し、暗号化機能が適切に動作している場合、操作パネルからのボタン操作により、TOEの型名、バージョンの表示を行う。

- 暗号化機能実装確認機能
  TOEは、「e-STUDIO3511/4511」の電源投入による初期立ち上げ中に、システムボードにスクランブラボードが正常に装着していることを確認するために妥当性テスト（スクランブラボード上の識別情報の検知）を行う。妥当性テストにより、

スクランブラボードの正常事象、スクランブラボードの取り外し事象、スクランブラボード以外の不正なボードの装着事象を検知し、監査記録を生成する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.HDD_THEFT	悪意を持ったe-STUDIO利用者、またはe-STUDIO非関係者が、HDDに不正な解読装置を接続し、ユーザ文書残存データを暴露するかもしれない。
T.SBOARD_REMOVE	悪意を持ったe-STUDIO利用者、またはe-STUDIO非関係者が、スクランブラボードを取り外したり、スクランブラボードの代わりに不正なボードを装着してセキュリティ機能を無効化することにより、ユーザ文書残存データを暴露するかもしれない。

1.5.6 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。

1.5.7 構成条件

本TOEが対象とするデジタル複合機のリストを以下に示す。

- e-STUDIO3511
- e-STUDIO4511

1.5.8 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1-2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1-2　TOE使用の前提条件

識別子	前提条件
A.KEYCODE_MANAGE	e-STUDIO管理者は、TOEの生成時に入力する鍵コードを、本人以外の者に知られないように管理する。
A.NO_EVIL_ADM	e-STUDIO管理者は、悪意を持った行為を行わない。
A.NO_EVIL_ENG	サービスエンジニアは、悪意を持った行為を行わない。
A.SECURE_KEYCODE	TOEの生成時に入力される鍵コードは、機密性と一意性を保証された鍵コードであり、e-STUDIO管理者によって正しくTOEにインストールされる。

1.5.9　製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

(1) 日本語版

- スクランブラボード GP-1031　サービスマニュアル　Ver D
- スクランブラボード GP-1031　取扱説明書　Ver D
- GP-1031 with GO-1030　開梱据付指示書　Ver B1
- チェックシート　Ver B0

(2) 英語版

- Scrambler Board GP-1031　Service Manual　Ver D
- Scrambler Board GP-1031　Operator's Manual　Ver D
- GP-1031 with GO-1030　Unpacking Instruction　Ver B1
- Check sheet　Ver B0

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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。

2.2 評価実施概要

以下、本評価報告書による評価実施の履歴を示す。

評価は、平成16年9月に始まり、平成17年2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16年12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・配付と運用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と、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。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストのシステム構成を図2-1、図2-2に示す。

TOEが対象とするデジタル複合機本体（e-STUDIO3511）

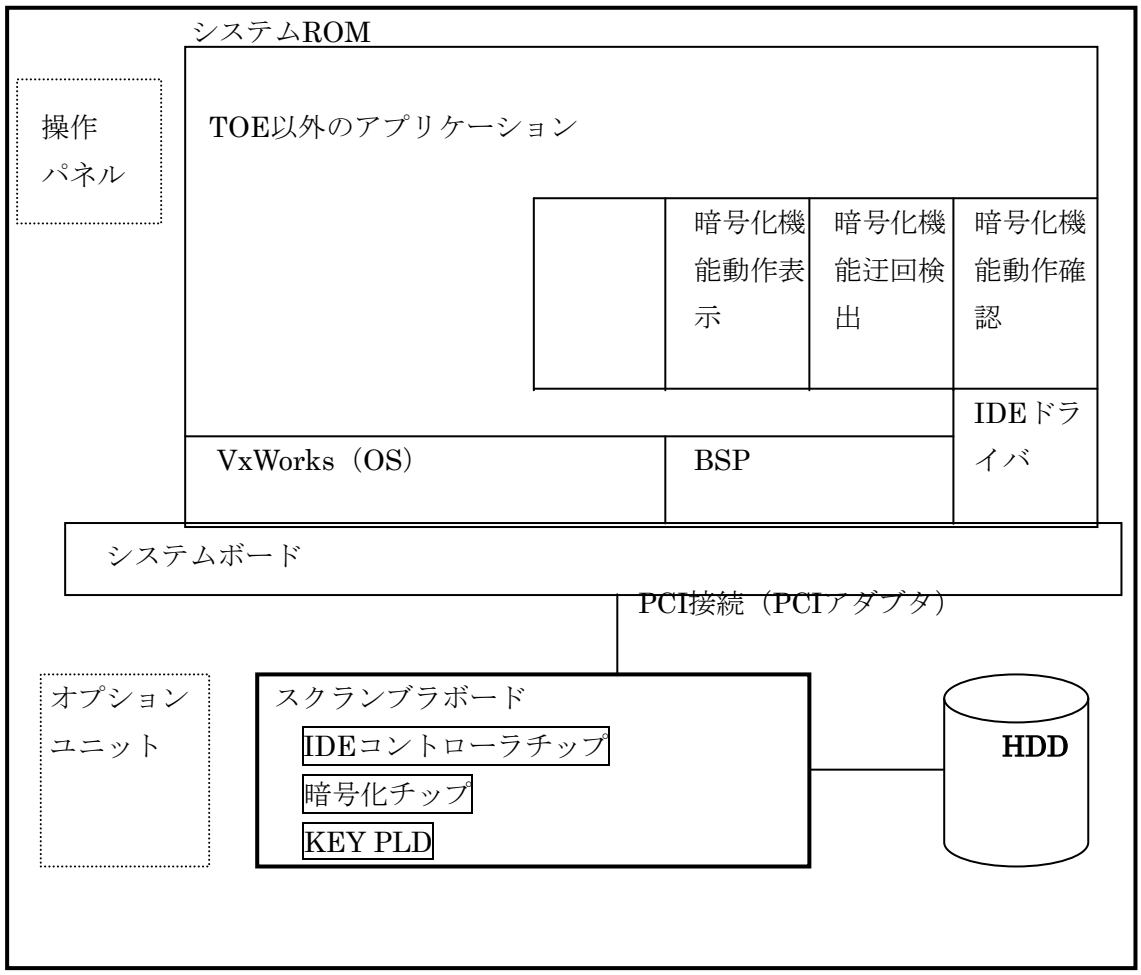

図2-1 製品用テスト構成

TOEが対象とするデジタル複合機本体（e-STUDIO4511）

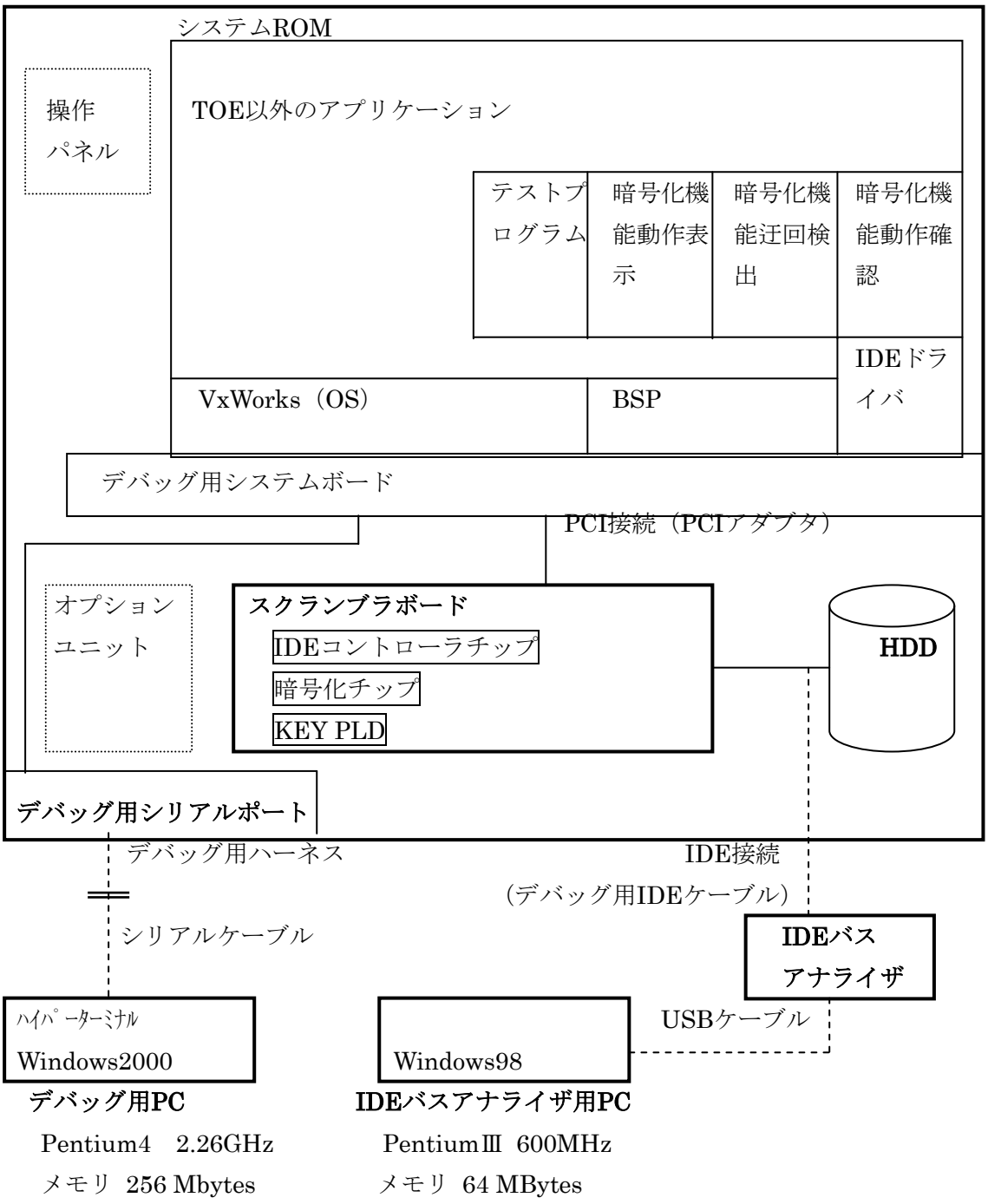

図2-2 API確認用テスト構成

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテスト構成は下表に示すとおり、3種類あり、STで識別されているTOE構成のほか、テスト用の構成を別途2つ準備し、テストが行われた。

表2-1　開発者テストの構成

テスト構成	内容
製品用テスト構成	出荷されている製品と同じ構成（詳細は、図2-1参照）
API確認用テスト構成	製品用テスト環境にデバッグ用システムボード、デバッグ用PC、IDEバスアナライザ、IDEバスアナライザ用PC、及びテストプログラムを追加したAPI確認のための構成（詳細は、図2-2参照）
API確認用例外テスト構成	API確認用テスト環境に対してテスト用にTOEを変更（IDEドライバ初期化、不良セクタ有無チェック）した例外テスト用の構成（詳細は、図2-2参照）

b.テスト手法

製品用テスト環境では､デジタル複合機本体の操作パネル上で実行及び表示が確認できるテストが行われた。

API確認用テスト環境は、デジタル複合機本体とTOE間のAPI及びHDD内のデータを確認するためのテストが行われた。API確認用テスト環境では、デバッグ用PCでテストプログラムの実行、入力及び結果の表示の確認を行い、IDEバスアナライザ及びIDEバスアナライザ用PCでHDDへの出力内容の表示の確認を行うこととなっている。さらに一部TSFIを変更しなければ確認できないテストは、API確認用例外テスト環境でテストが行われた。

c.実施テストの範囲

テストは開発者によって33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セキュリティ機能と外部インタフェースを考慮したテスト実施されていることが検証されている。

d.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。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストの構成に、図2-3を追加した構成である。

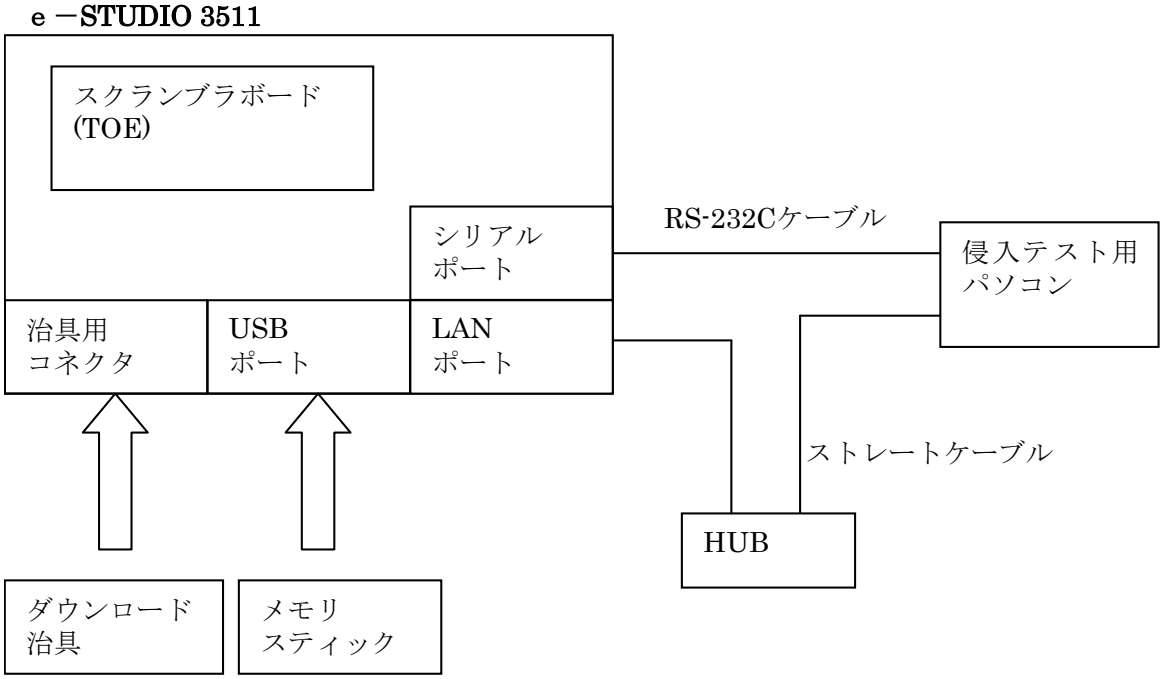

図2-3 侵入テスト構成

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を表2-2に示す。

表2-2 評価者テストの構成

テスト構成	内容
製品用テスト構成	出荷されている製品と同じ構成（詳細は、図2-1参照）
API確認用テスト構成	製品用テスト環境にデバッグ用システムボード、デバッグ用PC、IDEバスアナライザ、IDEバスアナライザ用PC、及びテストプログラムを追加したAPI確認のための構成（詳細は、図2-2参照）
API確認用例外テスト構成	API確認用テスト環境に対してテスト用にTOEを変更（IDEドライバ初期化、不良セクタ有無チェック）した例外テスト用の構成（詳細は、図2-2参照）
侵入テスト構成	外部インタフェースによる脆弱性及びTOE動作に必要なTSFデータ改ざんによるセキュリティ機能無効化から考案された構成

b.テスト手法

評価者は、開発者が行ったテスト手法が、セキュリティ機能の期待されたふるまいを検証するのに適していると判断し、開発者テストと同様の手法でテストを実施している。また侵入テストとして、シリアル及びLANインタフェースの悪用、暗号鍵データの窃取、暗号化機能の無効化、ダウンロード治具を利用したTOEソフトウェアの改ざんのテストを実施している。

c.実施テストの範囲

評価者は、評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを15項目、侵入テストを5項目、計25項目のテストを実施している。

評価者が独自に考案したテストは、以下に示す観点を考慮している。

①すべてのセキュリティ機能を網羅する。
②下記に示す要因を含ませる。
- 開発者の厳密さに対する追加テストの必要性
- 重要なセキュリティ機能
- TOEへのインタフェースタイプ
- 暗黙のテスト

サンプリングテストは、開発者が実施した33項目のテストの45.5%にあたる15項目をすべてのセキュリティ機能及びすべてのTSFIを網羅する項目を選択している。

侵入テストは、外部インタフェースによる脆弱性及びTOE動作に必要なTSFデータ改ざんによるセキュリティ機能無効化の観点から、5項目のテストを実施している。

d.結果

実施したすべての評価者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。また、悪用される可能性のある明白な脆弱性がないことを確認した。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

3 認証実施

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 当該所見報告書でなされた指摘内容が妥当であること。

② 当該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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された本評価報告書、当該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EAL2保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。

ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別､概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が明記され、それらが脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完結しており、理路整然とし、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認し

	ている。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.1.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.1.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。

AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果が含まれておりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。
脆弱性評定	**適切な評価が実施された**
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、SOF主張がなされている確率的または順列的セキュリティメカニズムは、ないことを確認している。

AVA_SOF.1.2E	評価はワークユニットに沿って行われ、SOF主張がなされている確率的または順列的セキュリティメカニズムは、ないことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

HDD	デジタル複合機に搭載されるハードディスクのこと。
TOEの関係者	e-STUDIO利用者、及びe-STUDIO管理者，サービスエンジニア，e-STUDIO非関係者。
暗号鍵データ	e-STUDIO管理者により入力された鍵コードが変換され、電子的に保存されている128bitのデータ。暗号化/復号操作で使用される暗号鍵は、パリティビットが除かれて112bitとなる。
解読装置	HDD内のデータを読み出し、解読する装置。
鍵コード	e-STUDIO管理者に提供される封筒に記載された、アルファベット(A～F)と数字(0～9)から成る暗号鍵のコード。
サービスマンコール表示	e-STUDIO 3511/4511の障害や故障、セキュリティ侵害の可能性検出時において、サービスエンジニア呼び出しの旨を示すメッセージ表示
スクランブラボード	暗号化/復号操作を司るハードウェア(基板)単体。
スクランブラボード GP-1031	TOE。暗号化/復号操作を司るハードウェアと、関連するソフトウェア。

デジタル複合機	コピー、FAX、プリンタなどの機能を1台に集約した多機能周辺機器。
ファイリングボックス	ユーザ文書データを保存するために、デジタル複合機のHDD内に生成されるフォルダ。
ユーザ文書	ユーザが扱う機密情報などの重要文書を含む文書。
ユーザ文書データ	ユーザ文書をデジタル化したデータ。

6 参照

[1] e-STUDIO 3511/4511用 スクランブラボードGP-1031 Security Target Ver 1.6 （2004年11月18日） 東芝テック株式会社

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人 情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-07

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-08

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032

[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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210第2版、補足-0407

[22] e-STUDIO　3511/4511用 スクランブラボードGP-1031 V2.0 評価報告書 第1.3版 2005年2月23日 社団法人 電子情報技術産業協会 ITセキュリティセンター