



JISEC

認 証 報 告 書

評価対象

申請受付年月日(受付番号)	平成15年12月22日(IT認証3018):当初の申請を取り下げし、CCRA認証マーク対応のため、再申請があった申請受付日 平成15年9月17日(IT認証3011):当初の申請受付日
認証申請者	東芝テック株式会社
TOEの名称	e-STUDIO 550/650/810用スクランブラボードGP-1010 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16年3月16日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
技術管理者 田淵 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。

ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security.

JIS X 5070(2000) セキュリティ技術 - 情報技術セキュリティの評価基準。

Common Criteria for Information Technology Security Evaluation.

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
Common Methodology for Information Technology Security Evaluation
認証機関が公開する および の翻訳文書
補足文書(補足-0210, CCIMB Interpretations-0210)

評価結果：合格

e-STUDIO 550/650/810用スクランブラードGP-1010 V2.0は、独立行政法人製品評価技術基盤機構が定める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
1.1	はじめに	1
1.2	評価製品	1
1.2.1	製品名称	1
1.2.2	製品概要	1
1.2.3	TOEの範囲と動作概要	2
1.3	評価の実施	5
1.4	評価の認証	5
1.5	報告概要	6
1.5.1	PP適合	6
1.5.2	EAL	6
1.5.3	セキュリティ機能強度	6
1.5.4	セキュリティ機能	6
1.5.5	脅威	7
1.5.6	組織のセキュリティ方針	7
1.5.7	構成条件	8
1.5.8	操作環境の前提条件	8
1.5.9	製品添付ドキュメント	8
2	評価機関による評価実施及び結果	10
2.1	評価方法	10
2.2	評価実施概要	10
2.3	製品テスト	10
2.3.1	開発者テスト	10
2.3.2	評価者テスト	13
2.4	評価結果	14
3	認証実施	15
4	結論	16
5	用語	22
6	参照	25

1 全体要約

1.1 はじめに

この認証報告書は、「e-STUDIO 550/650/810用スクランブラボードGP-1010 V2.0」(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、動作条件および機能仕様は本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。

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: e-STUDIO 550/650/810用スクランブラボードGP-1010
- 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TOEは、紙への複写をした後にデジタル複写機内に残存するイメージデータ(以降、「ユーザ文書残存データ」)が暴露する危険性を減ずることを目的とした、イメージデータ暗号化/復号を司るハードウェア(以降「スクランブラボード」)単体と、紙のドキュメント情報を電子的なイメージデータに変換する際にイメージデータの暗号化を行う機能及びHDDに記録されているイメージデータの実データ領域を全消去する機能を持つソフトウェアから構成される製品である。

また本TOEは、東芝テック株式会社製デジタル複写機「e-STUDIO 550/650/810」にオプションとして装着することにより利用することができる。

1.2.3 TOEの範囲と動作概要

本TOEはスクランブラードとソフトウェアから構成される。

物理的範囲として、図1、図2に本TOEを実装した「e-STUDIO 550/650/810」のハードウェア構成とソフトウェア構成を示す。

また、本TOEのソフトウェアは、システムボード上のFlash ROMに格納される。

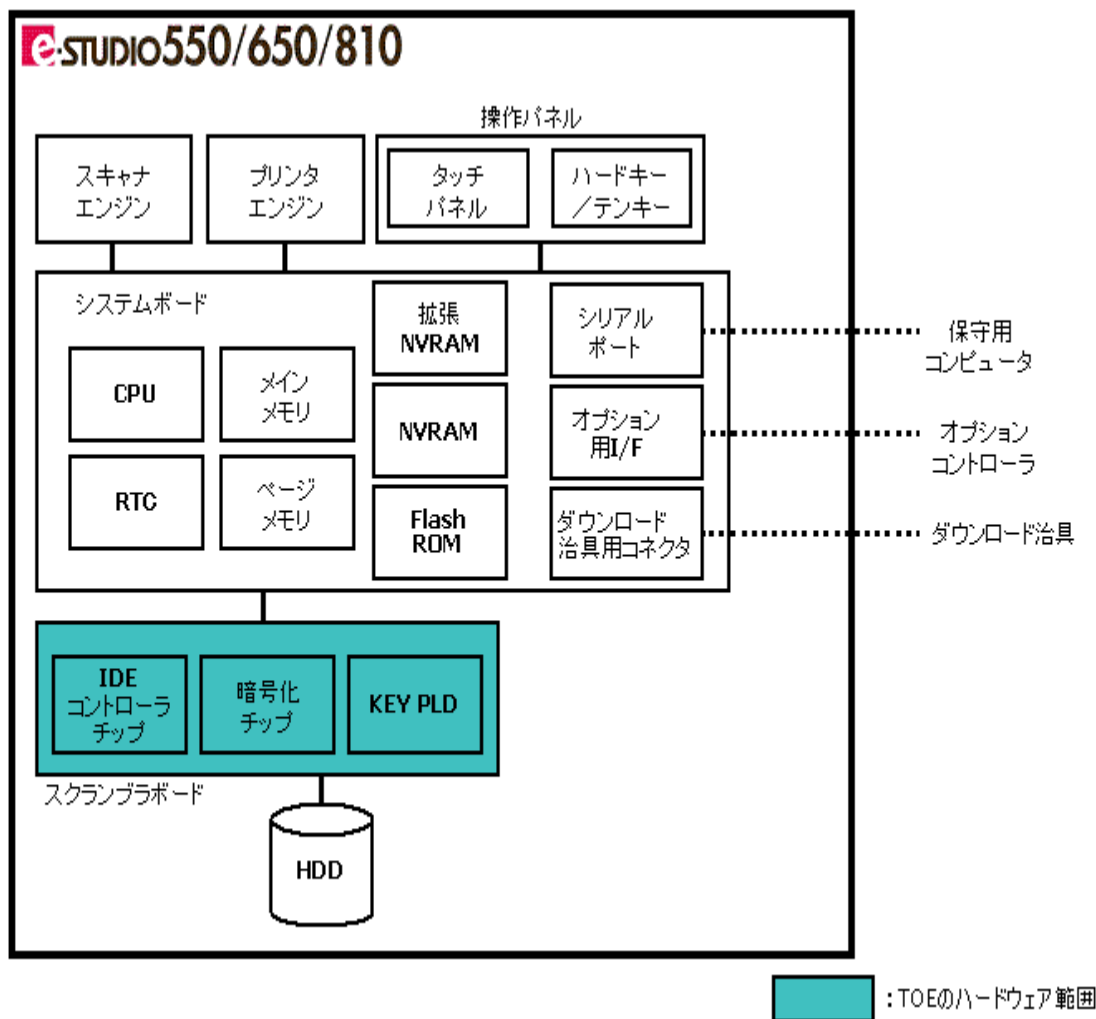


図1 本TOEを実装した「e-STUDIO 550/650/810」のハードウェア構成

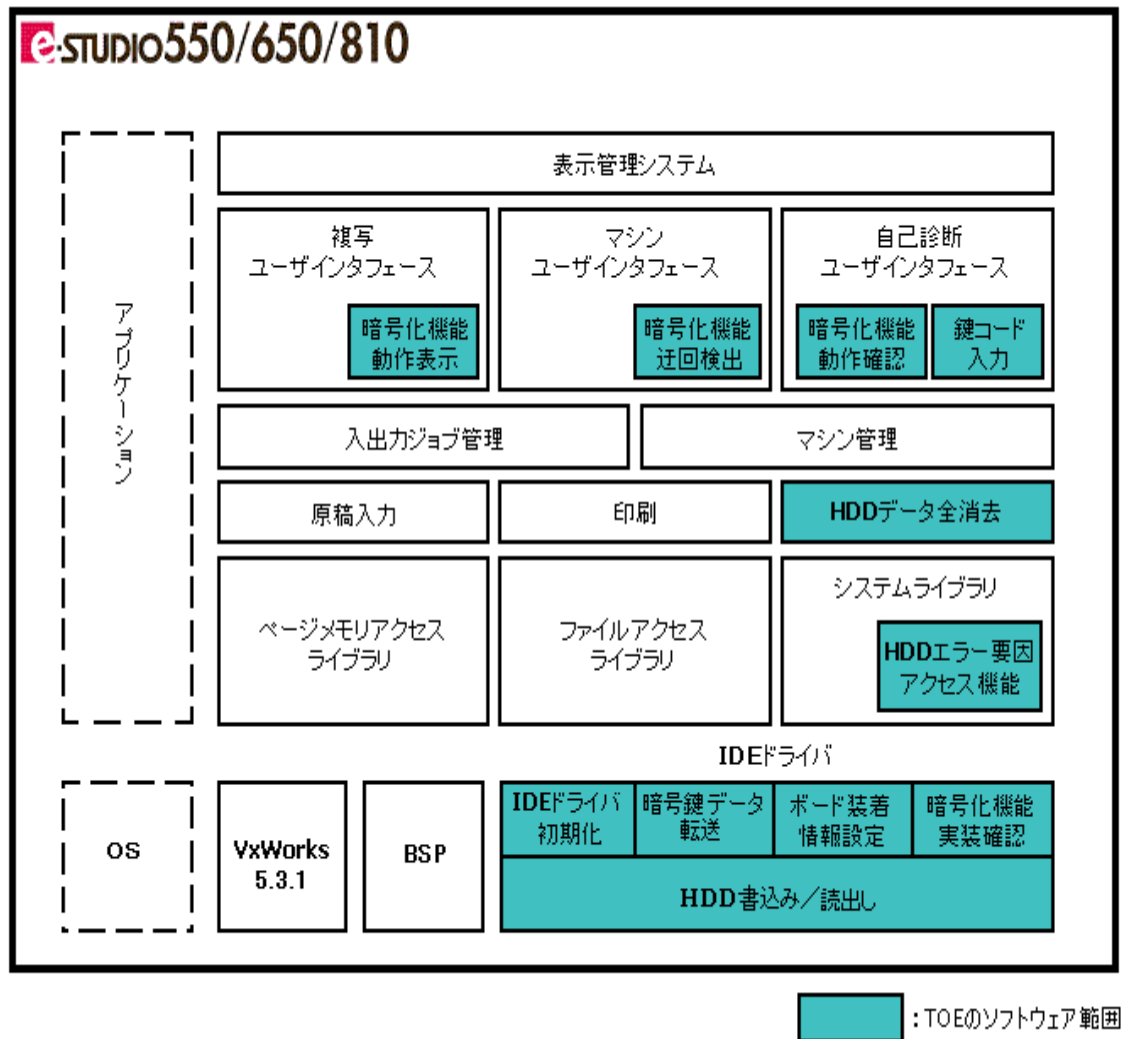


図2 本TOEを実装した「e-STUDIO 550/650/810」のソフトウェア構成

本TOEの論理的範囲を図3に示す。また、TOEのセキュリティ機能は以下の機能である。

- HDD データ暗号化 / 復号機能
- HDD データ全消去機能
- 暗号化機能迂回検出機能
- 暗号化機能実装確認機能
- 暗号化機能動作表示機能

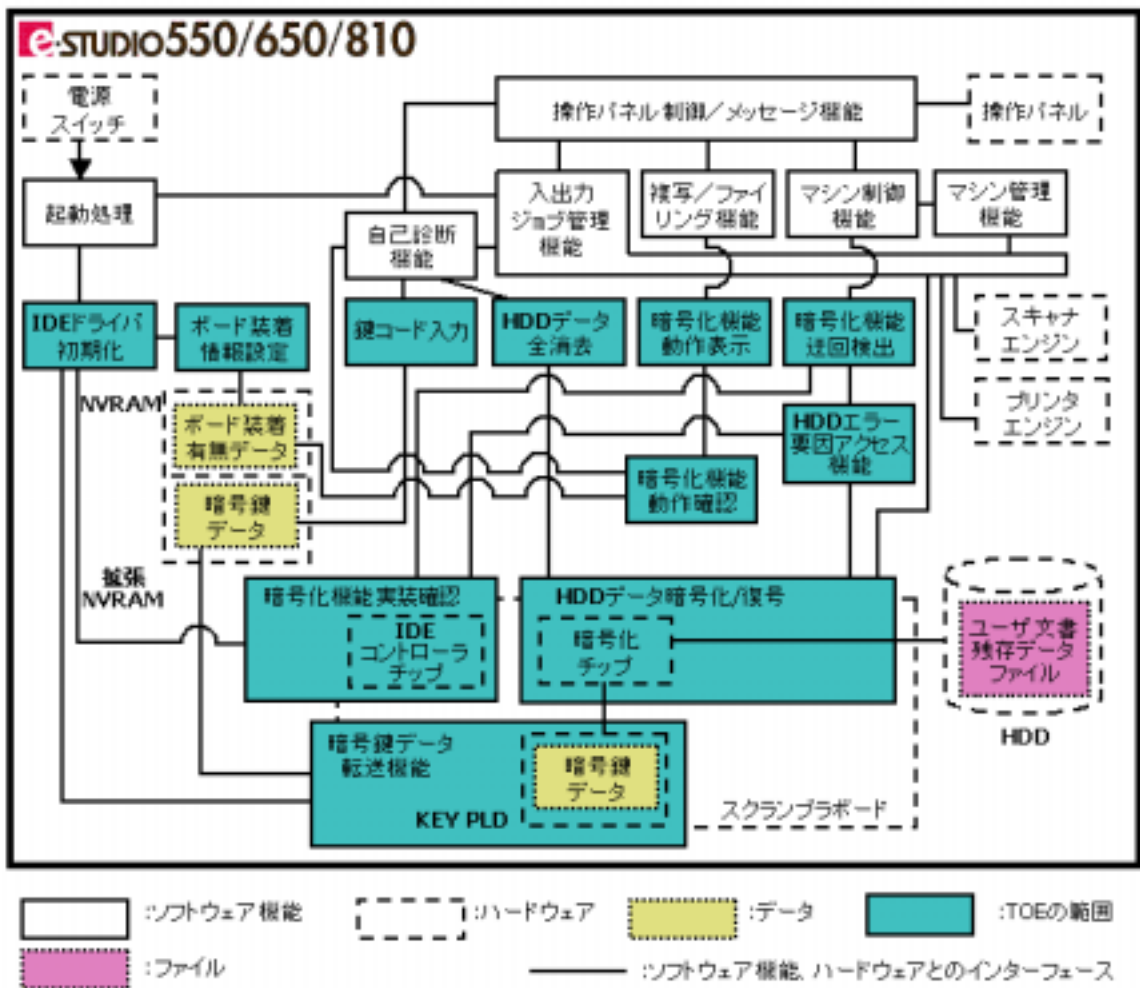


図 3 本TOEの論理的範囲

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 (平成15年)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「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14年4月)」[4]に規定された内容に従って、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、本TOEのセキュリティの基本設計である「e-SUTUDIO550/650/810用スクランブラード GP-1010 Security Target Ver 2.2」(以下「本ST」という。[1])、本TOE開発に関連する評価用提供物件及び本TOEの開発環境・製造・出荷の現場を調査し、本TOEとその開発環境等が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)の機能要件及び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することである。この評価手順及び結果は、「e-SUTUDIO550/650/810用スクランブラード GP-1010 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の各パートは評価基準補足文書([20][21])の内容を含む。

1.4 評価の認証

認証機関は、評価機関である社団法人 電子情報技術産業協会 ITセキュリティセンターが作成した、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、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16年3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が判明した。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TOEの評価保証レベルは、EAL2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、ネットワークで接続されない環境で使用される製品であり、想定される攻撃は、保護資産の不正な解釈やTOEの置き換えなどの不正行為である。また想定される攻撃者の攻撃力は低レベルであることから、これに対応できる最小機能強度は、“SOF-基本”で満足できる。

1.5.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。

(1) HDDデータ暗号化 / 復号機能

e-STUDIO利用者が複写機能を利用する時に、読込んだ紙のドキュメント情報を電子的なイメージデータに変換する際に暗号化してHDDに保存する。紙への印刷処理時にHDDに暗号化されて保存されているイメージデータを読み出して復号する。

(2) HDDデータ全消去機能

「e-STUDIO 550/650/810」のHDD廃棄または交換時に、HDDの実データ領域に存在する全データを上書き消去する。本機能は、サービスエンジニア向けの機能であり、e-STUDIO管理者からの依頼により実施される。

(3) 暗号化機能迂回検出機能

スクランブラ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呼出しを要求するサービスマンコール表示を行い、「e-STUDIO 550/650/810」の機能利用を停止する。

(4) 暗号化機能実装確認機能

「e-STUDIO 550/650/810」の起動時に、スクランブラードの装着状態の確認を行う。

(5) 暗号化機能動作表示機能

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バージョンの表示を行う。

1.5.5 脅威

本TOEは、表 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 想定する脅威

項番	脅威
1	e-STUDIO非関係者、または悪意を持ったe-STUDIO利用者が、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。
2	e-STUDIO非関係者、または悪意を持ったe-STUDIO利用者が、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することにより、セキュリティ機能が無効化され、ユーザ文書残存データが暴露されるかもしれない。

1.5.6 組織のセキュリティ方針

本TOEは、表 2に示す組織のセキュリティ方針に従う機能を備える。

表 2 組織のセキュリティ方針

項番	脅威
1	e-STUDIO 550/650/810本体を廃棄、または交換する時は、サービスエンジニアによってHDDのユーザ文書残存データを全て消去するものとする。

1.5.7 構成条件

本TOEが対象とするデジタル複写機のリストを以下に示す。

- ・ e-STUDIO 550
- ・ e-STUDIO 650
- ・ e-STUDIO 810

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 3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 3 TOE使用の前提条件

項番	前提条件
1	TOEの導入時にe-STUDIO管理者によって入力される鍵コードは、他人に知られないように管理すること。
2	e-STUDIO管理者は、デジタル複写機の運用管理を任された者であり、悪意をもった行為は行わないものとする。
3	サービスエンジニアは、メーカーまたはその関係会社、販売会社の正規の社員であり、セキュリティ違反を行わないものとする。
4	TOEの導入時に入力される鍵コードは、セキュアな値であることが保証された鍵コードであり、e-STUDIO管理者によってTOE導入時に入力する。

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。

- ・ドキュメント名：スクランブラード GP-1010 サービスマニュアル
- ・バージョン：Ver03
- ・対象者：サービスエンジニア
- ・内容：サービスエンジニアが携行するマニュアル。

TOEの設置手順、及びトラブルシューティング手順が記述されて

いる。TOEの設置に関し、e-STUDIO管理者と実施するTOEの装着及び立ち上げ作業における注意事項、TOEソフトウェアインストール手順が記述されている。また、TOEを含むデジタル複写機の廃棄（交換）時における、HDDデータの全消去手順も記述されている。

- ・ドキュメント名：スクランブラード GP-1010 取扱説明書
- ・バージョン：Ver03
- ・対象者：e-STUDIO管理者、e-STUDIO利用者
- ・内容：e-STUDIO利用者向けにTOEの機能説明及びTSFの動作確認方法、e-STUDIO管理者向けに鍵コードの入力や管理方法の説明及びHDDデータ全消去の確認方法が記述されている。

- ・ドキュメント名：Check Sheet
- ・バージョン：Ver02
- ・対象者：e-STUDIO管理者、サービスエンジニア
- ・内容：TOEの配付手続きに関する証拠資料。TOEの梱包状態、鍵コードの封筒の状態、TSFの作動などの確認を行うための項目が記述されたシート。またこのシートは、管理者による確認作業終了後、サービスエンジニアが回収する。

- ・ドキュメント名：スクランブラード GP-1010 開梱据付指示書
- ・バージョン：V04
- ・対象者：サービスエンジニア
- ・内容：TOEの開梱から設置までの手順書。サービスエンジニアが行う、TOEの開梱から設置までの手順が記述されている。

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15年9月に始まり、平成16年3月本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15年10月および11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を実施した。また、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記録され、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、評価に反映された。

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 4に示す。

e-STUDIO本体

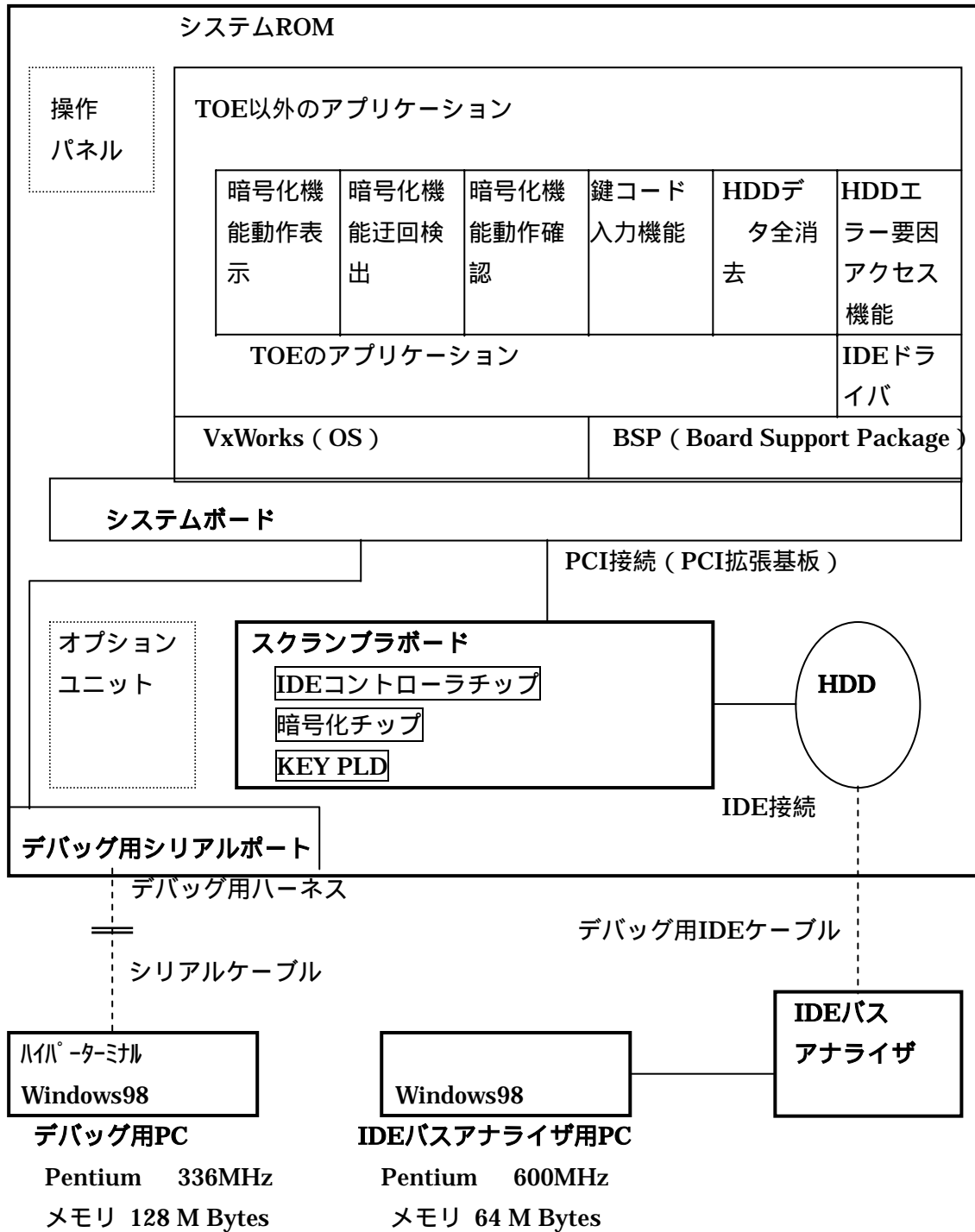


図 4 開発者テストシステム構成図

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の構成は図 4に示す。本構成は本STの記述と一致している。

b.テスト手法

TOEのセキュリティ機能のすべてのテストは、TOEテスト環境構成の環境下で実施された。

TOEのテスト環境は、下記の2種類である。

製品用テスト環境：

ユーザが実際に使用する環境と同じ構成。

デバッグ用のシリアルポートは未接続。

API確認用テスト環境：

製品用テスト環境に対して、システムボードをデバッグ用システムボードとし、デバッグ用システムボード上のシリアルポートにデバッグ用PCを接続、IDEケーブル上にIDEバスアナライザを接続した構成である。デバッグ用PCは、e-STUDIO上のshellに対してコマンド実行などの指示を行い、IDEバスアナライザ用PC上に出力結果を表示する。

c.実施テストの範囲

テストの項目数は全体で194項目である。

また、全体で194項目のテストのうち、セキュリティ機能別のテストの内訳は、以下のとおり。

- ・ SF.HDD_ERASE 6項目
- ・ SF.REMOVE_DETECT 2項目
- ・ SF.HDD_ENCRYPT 41項目（内コードレビュー確認6項目）
- ・ SF.SBOARD_CHECK 13項目
- ・ SF.RUN_MESSAGE 132項目

セキュリティ機能について網羅されており、開発者テスト数として妥当と判断した。

d.結果

194項目のテストのうち、実際に実行されたテストは、188項目である。評価者は、188項目のテスト項目において、予測したテスト結果と実際のテスト結果はすべて一致していることを確認した。また、実際にテストができないためにソースコードレビューを実施して検証した6項目については、すべて仕様通りの異常処理を行っていることが検証されており、セキュリティ上問題になる部分はないと判断した。

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システム構成を図 5に示す。

e-STUDIO本体

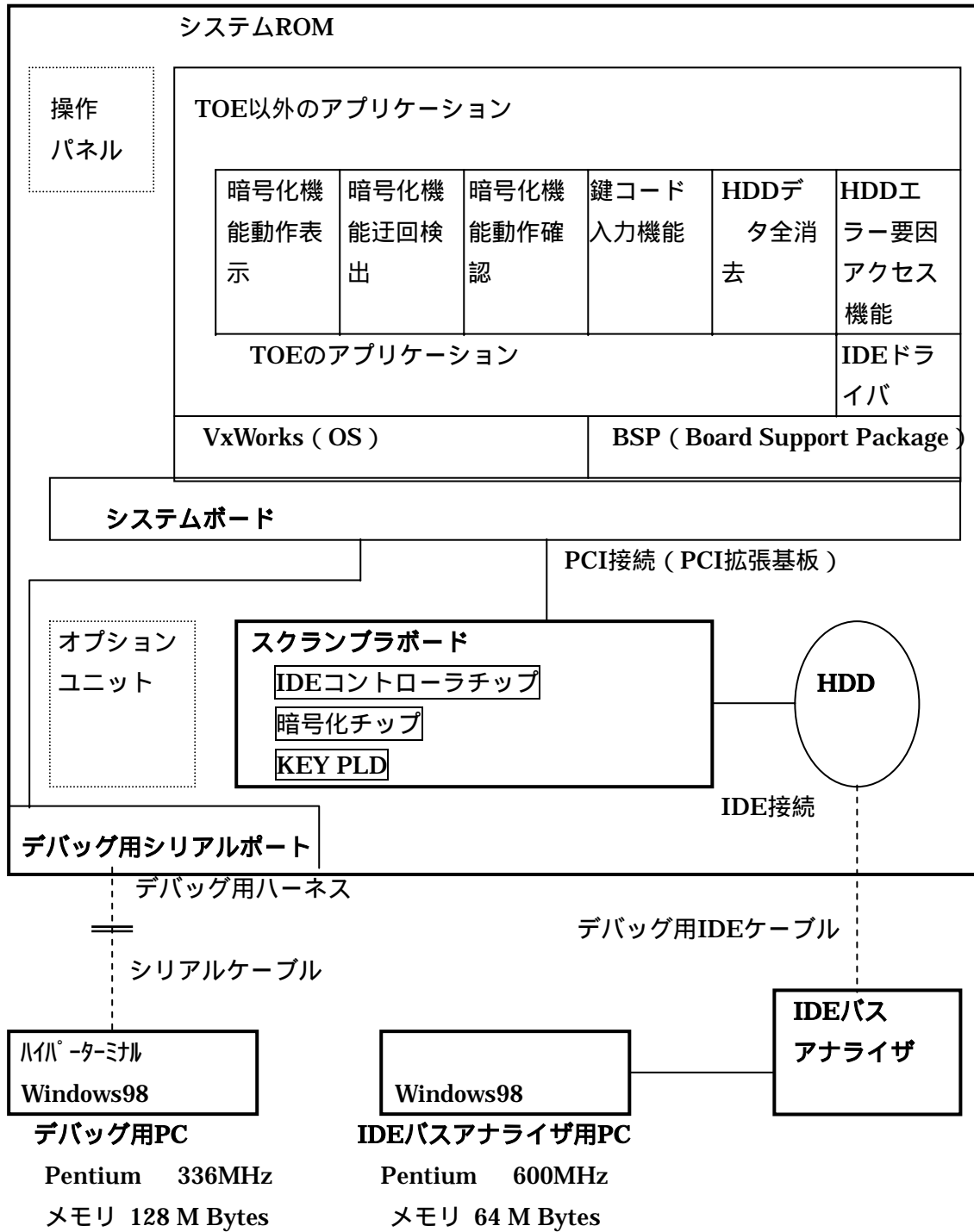


図 5 評価者テストシステム構成図

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は図 5に示す。本構成は本STの記述と一致しており、開発者のテスト環境とも一致する。

b. テスト手法

TOEのセキュリティ機能のすべてのテストは、TOEテスト環境構成の環境下で実施された。

TOEのテスト環境は、下記の2種類である。

製品用テスト環境：

ユーザが実際に使用する環境と同じ構成。

デバッグ用のシリアルポートは未接続。

API確認用テスト環境：

製品用テスト環境に対して、システムボードをデバッグ用システムボードとし、デバッグ用システムボード上のシリアルポートにデバッグ用PCを接続、IDEケーブル上にIDEバスアナライザを接続した構成である。デバッグ用PCは、e-STUDIO上のshellに対してコマンド実行などの指示を行い、IDEバスアナライザ用PC上に出力結果を表示する。

c. 実施テストの範囲

評価者による独立テストは、5つのセキュリティ機能すべてを対象とした。また評価者は、開発者テストのサンプリングについても、5つのセキュリティ機能すべてを対象とし、開発者が実施したそれぞれのセキュリティの項目数に応じてサンプリング数の配分を実施し、26項目が抽出された。

なお、サンプリング数26項目は開発者テストの総数に対して13.4%であるが、評価者が算出した開発者の重複したテスト項目を取り除いた実質的なテスト項目数は73項目となるため、サンプリング数26項目（実質35.6%）は妥当な数であると判断できる。

d. 結果

評価者テストを実施し、その実施結果において評価者テストでは期待される結果となり、開発者テストのサンプリングテストではテスト成績書に示されたものと一致することを確認した。

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は判断した。

3

認証実施

認証は、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。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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。

結論

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([7][10][13][16]のいずれか)に規定されたEAL2に対する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アクションエレメントについての検証結果を表 5にまとめる。

表 5 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	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識別、境界の記述が明瞭であ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指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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、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。また、当評価に至るまでなされた指摘も適切と判断される。
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、当評価に至るまでなされた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、当評価に至るまでなされた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。また、当評価に至るまでなされた指摘も適切と判断される。

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、当評価に至るまでなされた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。また、当評価に至るまでなされた指摘も適切と判断される。
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。また、当評価に至るまでなされた指摘も適切と判断される。
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.1.2E	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。
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実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、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。また、当評価に至るまでなされた指摘も適切と判断される。
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。また、当評価に至るまでなされた指摘も適切と判断される。
ガイダンス文書	適切な評価が実施された

AGD_ADM.1.1E	<p>評価はワークユニットに沿って行われ、管理者ガイドランスがTOEのセキュアな運用に必要な管理機能、権限、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。</p> <p>また、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については非適用であることを確認している。</p>
AGD_USR.1.1E	<p>評価はワークユニットに沿って行われ、利用者ガイドランスが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いることを確認している。また、特権に関する警告、IT環境に対するセキュリティ要件については非適用であることを確認している。</p>
テスト	適切な評価が実施された
ATE_COV.1.1E	<p>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。また、当評価に至るまでなされた指摘も適切と判断される。</p>
ATE_FUN.1.1E	<p>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。</p>
ATE_IND.2.1E	<p>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。</p>

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。また、本評価時に行われたテスト実施方法も適切と判断される。
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。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評価	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、確率的または順列的メカニズムが存在しないため非適用である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、確率的または順列的メカニズムが存在しないため非適用である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、当評価に至るまでなされた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。

注意事項

本TOEの守るべき資産はデジタル複写機内のHDDの実データ領域上に残存するユーザ文書残存データであり、対抗する脅威はそのHDDからのユーザ文書残存データの再生である。

ファイリング機能などを利用してデジタル複写機に蓄積するデータに対する保護は、本TOEのセキュリティ機能の対象ではない。このことを利用者に誤解を与えないようにしなければならない。

5

用語

本報告書で使用された用語、略語を以下に示す。

CC関連の略語

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

TOE関連の用語、略語

e-STUDIO550/650/810	一般的なオフィス等に設置される東芝テック株式会社製のデジタル複写機。TOEをオプションとして実装する。
HDD	Hard Disk Drive e-STUDIO 550/650/810に実装されているハードディスク装置。
Flash ROM	システムボード上に実装されているROMで、e-STUDIO 550/650/810本体、及びスクランブラボードGP-1010を制御するためのソフトウェアがインストールされている不揮発性メモリ。
NVRAM	NonVolatile RAM システムボード上に実装されているRAMで、e-STUDIO 550/650/810の各種設定情報を格納する不揮発性メモリ。設定情報の一部にスクランブラボードの装着有無情報が含まれる。
拡張NVRAM	システムボード上に実装されているRAMで、e-STUDIO

550/650/810の各種設定情報を格納する揮発性メモリ。設定情報の一部に暗号鍵データが含まれ、リチウムコイン電池により設定情報が保持されている。

RTC	Real Time Clock システムボード上に実装されているICで、実時間に準じた時間データを発生する内部時計。
KEY PLD	スクランブラボード上に実装されている論理素子(チップ)で、e-STUDIO550/650/810起動時にシステムボード上の拡張NVRAM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している。
BSP	Board Support Package e-STUDIO550/650/810のシステムボードに依存するデバイスの初期設定処理などをパッケージ化したソフトウェア。
ユーザ	e-STUDIO 550/650/810の複写機能などの一般機能を利用するお客様を指す。
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。
e-STUDIO利用者	e-STUDIO 550/650/810の複写等、一般的な機能を利用する。
e-STUDIO管理者	e-STUDIO 550/650/810に関する運用管理を行う。
サービスエンジニア	e-STUDIO 550/650/810の設置場所において、e-STUDIO 550/650/810の設置、インストール及び保守業務を行う。
e-STUDIO非関係者	特定な役割はなく、e-STUDIO 550/650/810に物理的にアクセス可能な人。
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。
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。
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)単体を指す。
スクランブラボード	TOE。暗号化/復号操作を司るハードウェアとHDDデータ

GP-1010

全消去機能を含む関連するソフトウェアを指す。

- [1] e-SUTUDIO550/650/810用スクランブラボード GP-1010 Security Target Ver 2.2
2004年2月25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15年 独立行政法人 製品評価技術基盤機構
適合性評価センター
- [3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技
術基盤機構 適合性評価センター 適合 - 部門 - IT機関要求 - 02
- [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14年4月 独立行政法人 製
品評価技術基盤機構 適合性評価センター 適合 - 部門 - IT申請要求 - 02
- [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-0210
- [21] 補足-0210
- [22] e-SUTUDIO550/650/810用スクランブラード GP-1010 V2.0 評価報告書
2004年3月3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
- [23] 所見報告書 ASE001-01～ASE014-01、ASE015-02、ASE016-01、ASE101-01～
ASE103-01、ASE104-02、ACM001-01～ACM002-01、ADV001-01～ADV002-01、
ATE001-01、AVA001-01
- [24] 認証レビュー CRV-T011-001 2004年1月13日発行 独立行政法人情報処理推進機構
セキュリティセンター
- [25] 認証レビュー CRV-T011-002 2004年1月16日発行 独立行政法人情報処理推進機構
セキュリティセンター
- [26] 認証レビュー CRV-T011-003 2004年1月20日発行 独立行政法人情報処理推進機構
セキュリティセンター
- [27] 認証レビュー CRV-T011-004 2004年2月17日発行 独立行政法人情報処理推進機構
セキュリティセンター
- [28] 認証レビュー CRV-T011-005 2004年2月24日発行 独立行政法人情報処理推進機構
セキュリティセンター
- [29] 認証レビュー CRV-T011-006 2004年2月25日発行 独立行政法人情報処理推進機構
セキュリティセンター