



# Certification Report

Koji Nishigaki, Chairman  
Information-technology Promotion Agency, Japan

## Target of Evaluation

Application date/ID	2009-3-3 (ITC-9249)
Certification No.	C0219
Sponsor	TOSHIBA TEC CORPORATION
Name of TOE	[Japanese] e-STUDIO555/655/755/855 System Software [English] System Software for e-STUDIO555/655/755/855
Version of TOE	V3.0
PP Conformance	None
Conformed Claim	EAL3
Developer	TOSHIBA TEC CORPORATION
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.

2009-06-29

Takumi Yamasato, Technical Manager  
Information Security Certification Office  
IT Security Center

**Evaluation Criteria, etc.:** This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation  
Version 3.1 Revision 2
- Common Methodology for Information Technology Security Evaluation  
Version 3.1 Revision 2

## Evaluation Result: Pass

"[Japanese]: e-STUDIO555/655/755/855 System Software V3.0

[English]: System Software for e-STUDIO555/655/755/855 V3.0" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met

the specified assurance requirements.

Notice:

This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

**Table of Contents**

---

1. Executive Summary .....	1
1.1 Introduction .....	1
1.1.1 EAL .....	1
1.1.2 PP Conformance.....	1
1.2 Evaluated Product .....	1
1.2.1 Name of Product .....	1
1.2.2 Product Overview .....	1
1.2.3 Scope of TOE and Security Functions .....	2
1.3 Conduct of Evaluation.....	7
1.4 Certification .....	8
2. Summary of TOE .....	8
2.1 Security Problem and assumptions .....	8
2.1.1 Threat.....	8
2.1.2 Organisational Security Policy .....	8
2.1.3 Assumptions for Operational Environment .....	8
2.1.4 Documents Attached to Product .....	9
2.1.5 Configuration Requirements .....	9
2.2 Security Objectives .....	10
3. Conduct and Results of Evaluation by Evaluation Facility.....	11
3.1 Evaluation Methods .....	11
3.2 Overview of Evaluation Conducted .....	11
3.3 Product Testing .....	11
3.3.1 Developer Testing.....	11
3.3.2 Evaluator Independent Testing.....	13
3.3.3 Evaluator Penetration Testing .....	14
3.4 Evaluation Result .....	15
3.4.1 Evaluation Result .....	15
3.4.2 Evaluator comments/Recommendation .....	15
4. Conduct of Certification .....	16
5. Conclusion.....	17
5.1 Certification Result.....	17
5.2 Recommendations.....	17
6. Glossary .....	18
7. Bibliography .....	20

## 1. Executive Summary

### 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "[Japanese] e-STUDIO555/655/755/855 System Software V3.0 [English] System Software for e-STUDIO555/655/755/855 V3.0" (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, TOSHIBA TEC CORPORATION and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in ST.

This certification report assumes "purchasers and/or administrators of Digital MFP" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

#### 1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

#### 1.1.2 PP Conformance

There is no PP to be conformed.

### 1.2 Evaluated Product

#### 1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	[Japanese] e-STUDIO555/655/755/855 System Software [English] System Software for e-STUDIO555/655/755/855
Version:	V3.0
Developer:	TOSHIBA TEC CORPORATION

#### 1.2.2 Product Overview

The TOE is the control software for the digital MFPs "e-STUDIO555/655/755/855" (hereinafter referred to as "the e-STUDIO") manufactured by TOSHIBA TEC CORPORATION. The TOE is enabled when the security functions of the e-STUDIO are activated by the optional GP-1070 or GP-1170.

The main functions of the e-STUDIO include copy, print, Fax and e-Filing Box/shared folder functions (hereinafter referred to as "the general functions"). The TOE enables deletion of user document data written into the HDD and permanently erases in an unrecoverable manner when the e-STUDIO functions are used.

The e-STUDIO555 will not be marketed for Japan.

### 1.2.3 Scope of TOE and Security Functions

#### 1.2.3.1 Usage of TOE

As shown in Figure 1-1 below, the e-STUDIO is used as a terminal to send/receive data to/from facsimile machines, a terminal to send email messages to email servers, and a remote printer for remote PCs in network environments as well as installed in general offices as a standalone device.

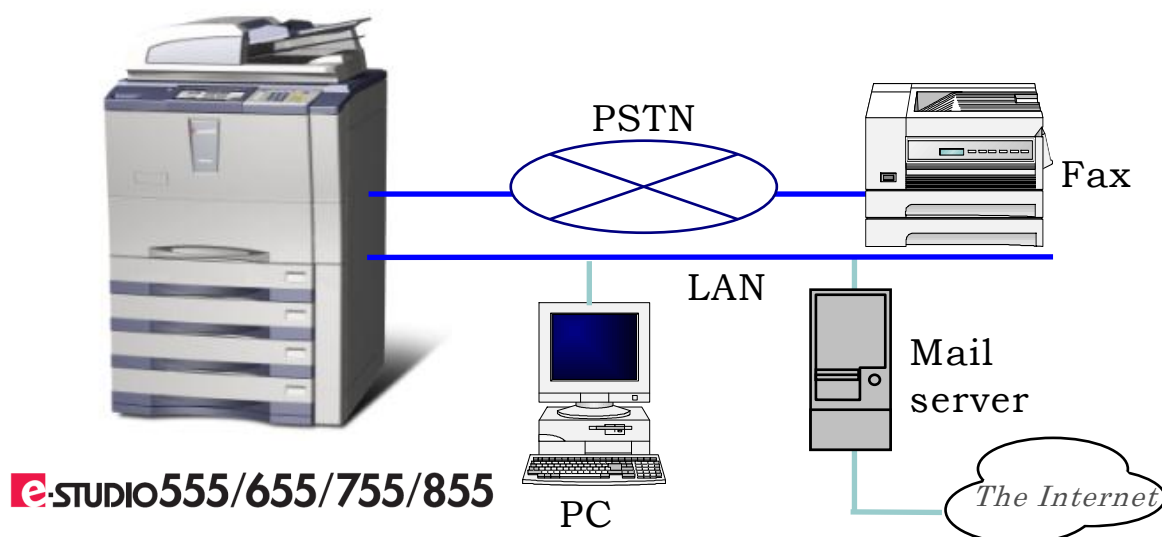


Figure 1-1 Typical operating environment of the TOE

#### 1.2.3.2 TOE function

TOE has two modes. One is the normal mode for users to copy and scan, and the other is the self-diagnostic mode for service engineers.

##### 1. Normal mode:

The Product Configuration in Normal Mode is shown in Figure 1-2. It shows the operable state of this product after the power is turned on and program data is downloaded from the HDD.

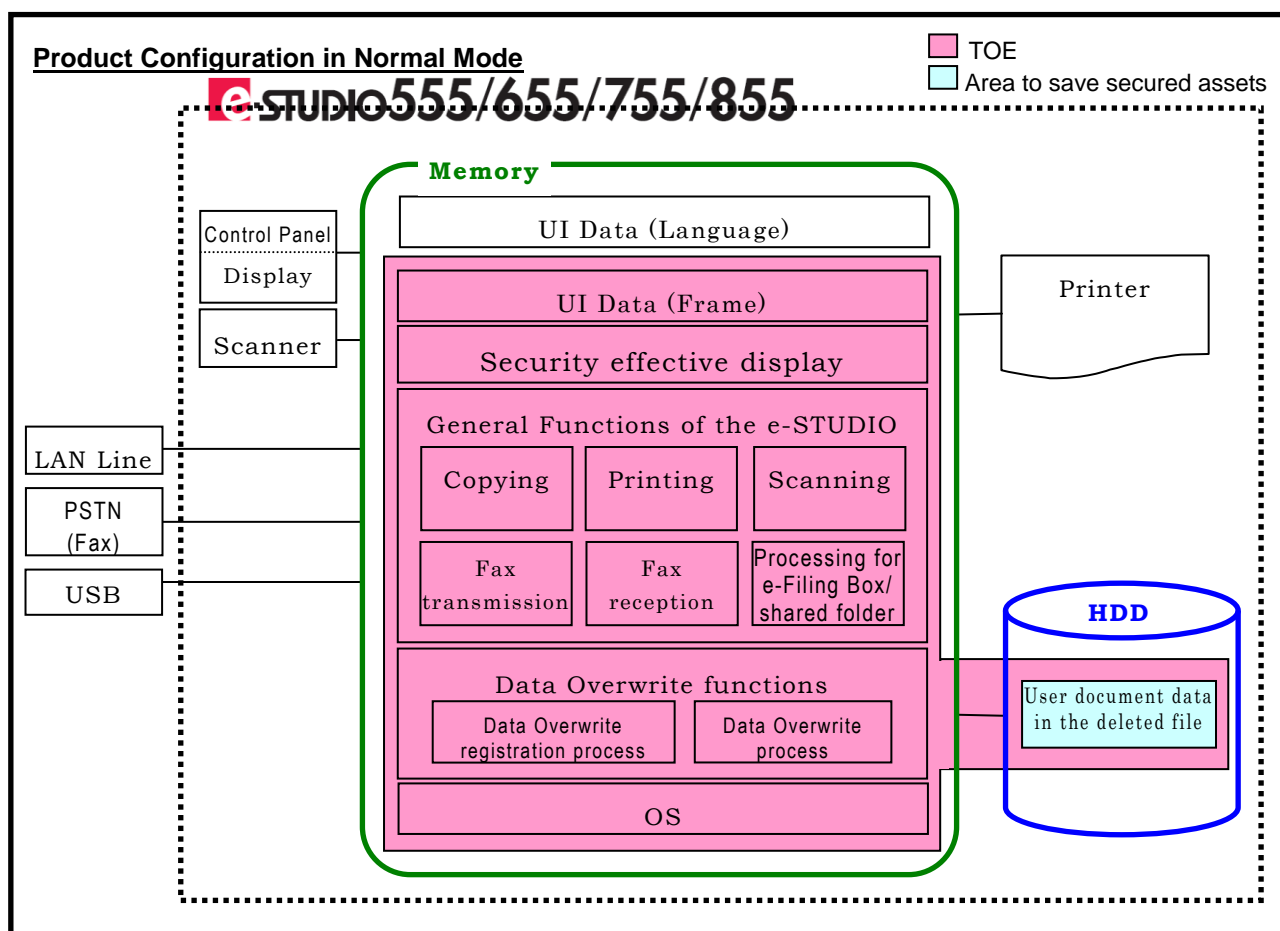


Figure 1-2 Product Configuration in Normal Mode

TOE functions are described below:

(1) Security Effective display

When the COUNTER button is pressed on the control panel, the print count screen appears. When the security functions are enabled, the icon indicating data overwrite and TOE version [SYS V3.0] are shown.

(2) Copying

When the COPY button is selected on the control panel, the e-STUDIO scans user document data from the scanner, writes them in the work area of the HDD, and outputs the data in the work area from the printer. In addition, the copy settings enable the data to be saved in the e-Filing Box or shared folder of the HDD, while being output from the printer at the same time.

(3) Printing

Printing function can be enabled by the operation shown below:

- Start through LAN and USB lines (the eSTUDIO used as a printer)
- Start through LAN lines (TopAccess)
- Start on the control panel

When Printing function is enabled by the operation above, the e-STUDIO writes user document data in the work area of the HDD, and outputs the data in the work area from the printer. The e-STUDIO saves the user document data in the work area in the e-Filing Box.

#### (4) Scanning

Scanning function can be enabled by the operation on the control panel and through LAN lines.

When the SCAN button is selected on the control panel, the e-STUDIO scans user document data from the scanner, writes them in the work area of the HDD and saves the data in the work area in the e-Filing Box, shared folder or USB media, or sends them to the specified destination by e-mail.

Start through LAN lines provides a WS Scan function allowing the e-STUDIO on the LAN to be used as a scanner on a Windows Vista PC, and the e-STUDIO scans user document data from the scanner and sends image data to the PC that sent a scan request.

#### (5) Fax transmission

Fax transmission function can be enabled by the operation on the control panel and through LAN and USB lines.

When the FAX button is selected on the control panel, the e-STUDIO scans user document data from the scanner, writes them in the work area of the HDD, and sends the data in the work area by Fax through PSTN (Fax) or by the Internet Fax through LAN lines.

Through LAN and USB lines the Network Fax driver is selected on the client PC, the e-STUDIO starts Fax transmission or the Internet Fax transmission of the user document data.

#### (6) Fax reception

When receiving Fax data through PSTN (Fax) or the Internet Fax data through LAN lines, the e-STUDIO writes the received user document data in the work area of the HDD, outputs the data from the printer and saves the received data in the specified e-Filing Box or shared folder.

#### (7) Processing for e-Filing Box/shared folder

Processing for e-Filing Box and shared folder can be enabled by the operation on the control panel, through LAN lines (TopAccess).



Selecting the E-FILING button on the control panel, this function enables to print, edit or delete the user document data saved in the Box or send the data by e-mail.

On the TopAccess screen, when printing, editing or deleting the user document data saved in the Box, sending the data by e-mail or archiving them or uploading their archives.

This function enables expired user data files saved in the e-Filing Box or shared folder to be deleted.

(8)Data Overwrite registration process (Security Function)

When user document data are deleted in processing of (2) to (7) above, Data Overwrite registration process (registers only its path) can be enabled. This function makes the deleted files targeted for Data Overwrite process.

(9)Data Overwrite process (Security Function)

This function monitors the storage area of user document data to start and be deleted by Data Overwrite process and permanently erases the area. While the user document data are being permanently erased, "ERASING DATA" appears on the control panel.

## 2. Self-Diagnostic Mode

The Product Configuration in Self-Diagnostic Mode is shown in Figure 1-3. It shows the operable state of this product after the power is turned on and program data is downloaded from the HDD.

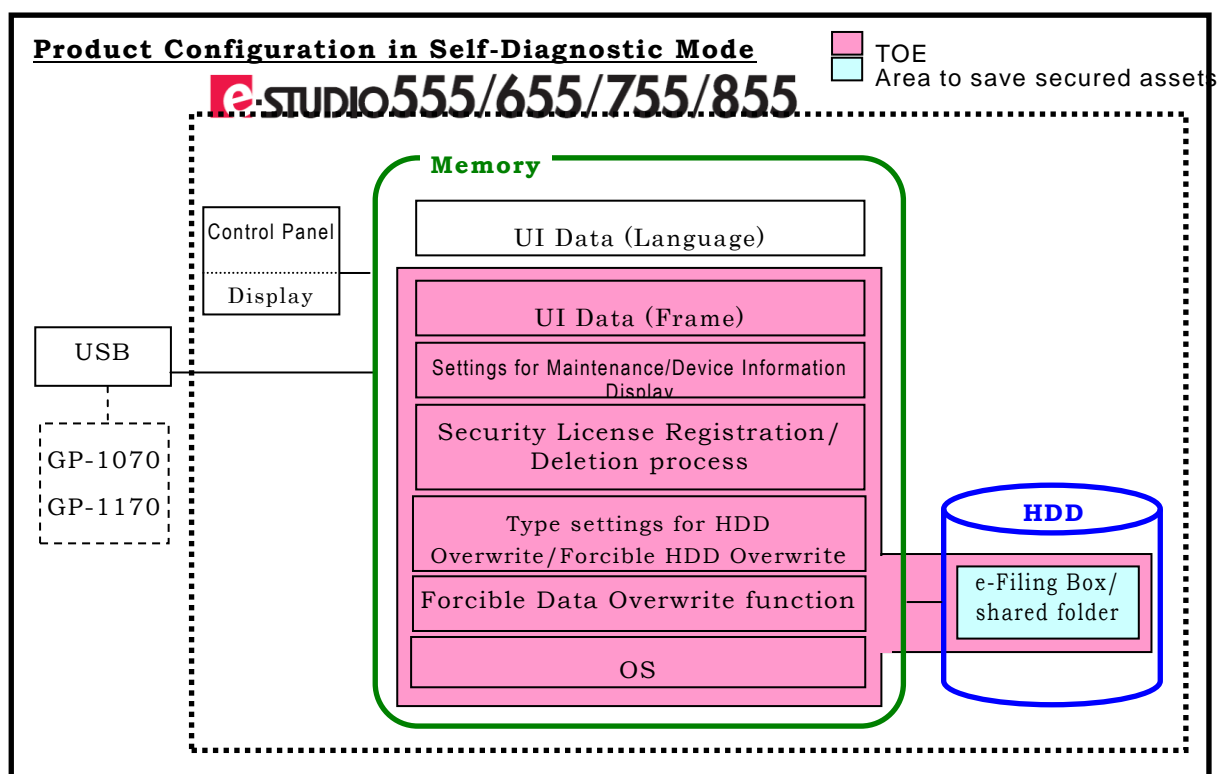


Figure 1-3 Product Configuration in Self-Diagnostic Mode

TOE functions are described below:

(1) Settings for Maintenance/Device Information Display

This function is the maintenance functions for service engineers such as Test Print, Hardware Adjustment and Firmware Update, etc.

(2) Forcible Data Overwrite function (Security Function)

This function is implemented on the control panel when the e-STUDIO is disposed of or the HDD is replaced, the remaining user document data in the HDD are collectively and permanently erased.

(3) Security License Registration/Deletion process

The GP-1070 or GP-1170 is used to register or delete the license. This function sets Valid/Invalid of Security Functions.

(4) Type settings for HDD Overwrite/Forcible HDD Overwrite

The overwrite types of Data Overwrite function in normal mode and forcible Data Overwrite in self-diagnostic mode are set.

### 1.2.3.3 Secured Assets of TOE

Secured assets in normal and self-diagnostic modes are described below:

- Secured assets in normal mode

The remaining magnetic data in the HDD after deletion of user document data indicate secured assets. Secured assets are generated in the following situations:

- (1) When the e-STUDIO deletes user document data during a job specified by the user or after the job is finished (or cancelled).
- (2) When the e-STUDIO automatically deletes expired user document data.

- Secured assets when the HDD is disposed of or replaced

The remaining user document data in the HDD of the e-STUDIO to be disposed of or in the HDD to be replaced indicate secured assets.

## 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Security Target for e-STUDIO555/655/755/855" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "Evaluation Technical Report (DCI-ETR-0002-00)" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

## 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Evaluation is completed with the Evaluation Technical Report dated 2009-06 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

## 2. Summary of TOE

### 2.1 Security Problem and assumptions

Problems should be solved by TOE and necessary assumptions are as follows.

#### 2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them.

**Table 2-1 Assumed Threats**

Identifier	Threat
T.TEMPDATA_ACCESS	A malicious user or unrelated user may attempt to retrieve user documents while surreptitiously removing the HDD from the e-STUDIO, restoring and decoding user document data deleted from the HDD of the e-STUDIO, using existing tools.
T.STOREDATA_ACCESS	A malicious user or unrelated user may attempt to retrieve user documents from the HDD disposed of or replaced of the e-STUDIO, using existing tools.

#### 2.1.2 Organisational Security Policy

There are no organisational security policies for the TOE.

#### 2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-2.

The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

**Table 2-2 Assumptions in Use of the TOE**

Identifier	Assumptions
A.TRUST_SE	It is assumed that the service engineer has knowledge required to operate the e-STUDIO in self-diagnostic mode and does not perform invalid operations. (NOTE: Power shutdown during Forcible Data Overwrite is included in invalid operations.)
A.NO_ERASE_STOP	It is not assumed that Data Overwrite process in normal mode is stopped due to power shutdown.
A.SECURITY_ENABLED	It is assumed that the e-STUDIO user and administrator use the TOE by making sure the security functions are running.

#### 2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. Readers are required full understanding of following documents and compliance with descriptions.

[Japanese]

- Operator's Manual
  - Safely Information (OMJ080001C0)
  - e-STUIDO655/755/855 Quick Start Guide (OMJ08016600)
- Service Manual
  - e-STUIDO655/755/855 Service Manual (SMJ08001700)
  - e-STUIDO655/755/855 Service Handbook (SHJ08000200)

[English]

- Operator's Manual
  - Safely Information (OME080002C0)
  - e-STUIDO555/655/755/855 Quick Start Guide (OME08016700)
- Service Manual
  - e-STUIDO555/655/755/855 Service Manual (SME08001600)
  - e-STUIDO555/655/755/855 Service Handbook (SHE08000100)

#### 2.1.5 Configuration Requirements

The TOE is effective on Digital MFP "e-STUDIO555, e-STUDIO655, eSTUDIO755, e-STUDIO855" manufactured by TOSHIBA TEC CORPORATION.

## 2.2 Security Objectives

TOE counters against threats described in 2.1.1 as follows by implemented security functions.

### 1. Data Overwrite Function

The general functions of the e-STUDIO allow user document data temporarily generated and stored in the work area or stored in the e-Filing Box/shared folder, to de-allocate resources when these storage areas are deleted.

- During a job started by the user or when it is finished
- The period to save data in the e-Filing Box or shared folder expires.

Data overwrite functions are comprised of Data Overwrite registration process and Data Overwrite process.

Data overwrite registration process registers the path to storage area to be deleted. Data Overwrite process overwrites 00, FF and random data in the storage area specified by the path and then releases the area, to permanently erase the area. While the process is overwriting, "ERASING DATA" appears on the control panel.

### 2. Forcible Data Overwrite Function

The forcible Data Overwrite function overwrites all HDD storage areas including existing user document data files in the HDD with 00, FF and random data, and initializes the areas.

### 3. Conduct and Results of Evaluation by Evaluation Facility

#### 3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

#### 3.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2009-03 and concluded by completion the Evaluation Technical Report dated 2009-06. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing on 2009-05. And the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-05.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

#### 3.3 Product Testing

The evaluator confirmed the validity of the test that the developer had executed. The evaluator executed reappearance tests, additional tests and penetration tests based on vulnerability assessments judged to be necessary from the evidence shown by the process of the evaluation and results by the verification of the developer testing.

##### 3.3.1 Developer Testing

The evaluator evaluated the integrity of developer testing that the developer executed and the test documentation of actual test results. The overview of evaluated tests performed by the developer is shown as follows;

## 1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1.

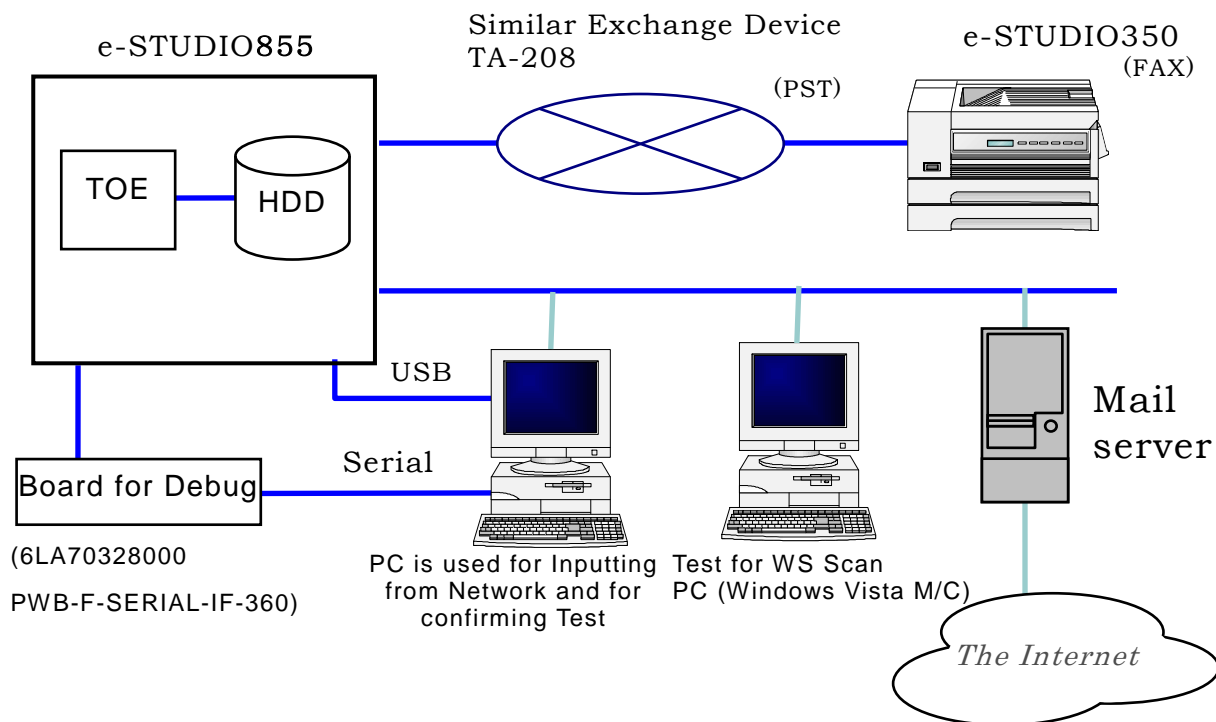


Figure 3-1 Developer test configuration

The developer testing is executed on the same TOE test environment as TOE configuration identified in ST.

## 2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow;

### a. Test outline

Outlining of the testing performed by the developer is as follows;

The TOE has two Security functions, each security functions are performed in two modes (Normal Mode, Self Diagnostic Mode). Therefore, all functional testing and abnormality testing regarding Security functions are performed in each mode. Followings are the typical test samples:

#### - Normal Mode

Copying function, Scanning function and Processing for e-Filing Box/shared folder on Operation Panel

Abnormality test such as Power Shut-down, Network Communication, the bulk data, usage at the same timing



- Self Diagnostic Mode
  - Execution of Forcible Overwriting
  - Setting of HDD Overwriting Type
  - Firmware Update

In order to confirm Security functions perform completely in above testing, developer confirmed the status of HDD overwriting with PC for Input from Network communication by processing unit.

#### b. Scope of Testing Performed

Testing is performed about 119 items by the developer.

The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

#### c. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

### 3.3.2 Evaluator Independent Testing

Evaluator executed the independent testing to reconfirm that Security functions are certainly implemented from the evidence shown by the process of the evaluation. Outlining of the independent testing performed by the developer is as follow;

#### 1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.

Test configuration performed by the evaluator is showed in the Figure 3-1.

Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.

#### 2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

##### a. In terms of Evaluator Independent Testing

Evaluator devised the independent testing from the developer testing and the provided documentation in terms of followings.

1. Testing in the different configurations and setting (Overwriting setting, Browser Setting) from one of the developer testing.
2. Testing in changed parameter from one that the developer tests.

b. Outlining of Evaluator Independent Testing

Outlining of evaluator independent testing performed by the evaluator is as follows;

There are 6 tests performed as Independent testing. Taking account of another means (Different Browsers, different Mail User Agent and different printing condition) different from developer testing and the change of testing parameters (Deletion of Filing Box, Type of Overwriting) performed in developer testing, Evaluator devised the independent testing for supplementing developer testing with its strictness and sufficiency.

In Evaluator testing the evaluator confirmed that Data overwriting is performed completely by means of checking the status of HDD overwriting processing from PC for input from network communication in each transaction as same as developer testing.

c. Result

All evaluator independent testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

### 3.3.3 Evaluator Penetration Testing

Evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level. Outlining of f Evaluator penetration testing is as follows;

1) Outlining of Evaluator Penetration Testing

Outlining of penetration testing performed by the evaluator is as follows;

a. Vulnerability of concern

Evaluator searched the potential vulnerability from information which is within the public domain and provided evidence to identify the following vulnerability that requires penetration testing.

From searching result of the official vulnerabilities, one item is identified, which is "The implementation problem connectable to Debugger Function" of "the research report related to already –known vulnerabilities about SIP" sourced from the official information of IPA. Additionally, the evaluator searched the confirmation items of "Guidance related to general vulnerability" described in CEM from the evidence documents, and identified vulnerabilities which are candidates of 20 penetration tests related to by-pass, falsification or misuse. In the result of analyzing, 8 penetration tests are set. And from the result of penetration test, additional 3 penetration tests were set.

## b. Scope of Test Performed

Evaluator conducted the following 11 penetration tests to determine the exploitable potential vulnerability.

	Vulnerability to be tested
1	Existence of vulnerability in usage of ports
2	Access to the residual data of HDD in utilizing FTP or telnet
3	Impact to Security functions of printing PDF file in which illegal codes are included
4	Impact to Security functions when MFP is busy(1)
5	Impact to Security functions when MFP is busy(2)
6	Bypass by TopAccess Parameter
7	Actions to various attacks to TopAccess
8	Bypass by Uploading Archiving Files
9	Existence of vulnerability in case of HDD Full
10	Occurrence of Buffer Overflow
11	Operation in deactivation of Security functions

## c. Result

In the conducted evaluator penetration testing, the exploitable vulnerability that attackers who have the assumed attack potential could not be found.

## 3.4 Evaluation Result

### 3.4.1 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

### 3.4.2 Evaluator comments/Recommendations

There is no special comment/recommendation to notify to customers.

#### 4. Conduct of Certification

The certification body conducted the following certification based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

The Certification Body confirmed such concerns pointed out in Observation Report, the ST and the Evaluation Technical Report, and issued this certification report.

## 5. Conclusion

### 5.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted, and the Certification Body determined the TOE is satisfied the assurance requirements of EAL3 components prescribed in CC Part 3.

### 5.2 Recommendations

There is no recommendation to notify to the consumers.

## 6. Glossary

The abbreviations relating to CC used in this report are listed below.

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

The abbreviations relating to TOE used in this report are listed below.

HDD:	Hard Disk Drive
LAN:	Local Area Network
USB:	Universal Serial Bus

The definition of terms used in this report is listed below.

e-STUIDO:	Digital Multi-functional Product made by Toshiba TEC Corp. A single multi-functional peripheral device which integrates several functions such as copy, scan, print, and fax. In this report, e-STUIO means e-STUDIO555/655/755/855.
TopAccess:	Job based on Web and Device management tool. When using this tool, information of e-STUIO can be gained through the Internet and two kinds of Web-sites for users and administrators can be utilized.
WS Scan:	WS(Web Service) Scan uses the functionality which is installed in Windows Vista Computer, and is a function of scan operation to computer through network. Image data scanned in this device can be stored in the Computer device, or image data can be gained by requesting scan from the application corresponded to WIA(Windows Imaging Acquisition) Scan Driver to this device.
General Functions:	Functions are Copy, Scan, Print, Fax, Filing Box/Shared Folder out of functions which are implemented in e-STUDIO.

**Shared folder:** A temporary area where the e-STUDIO users stores and refers their user document data. The e-STUDIO users delete user document data stored themselves. Such user document data is automatically deleted from an area after a specified effective period expires and this data is no longer recognized as assets to be protected.

**Delete:** Allocation of resources is released, and put it into the state that cannot be used for users.

**Erase:** Erase without leaving signs.

**Job:** Unit which general functions are processed by.

**Filing Box:** The place where User document data is stored. After storing, data reference, printing out, and editing can be performed through Operational Panel or TopAccess. When the date of storing files is expired, user document data can be deleted.

**User document data:**

e-STUDIO user's document data digitized utilizing the e-STUDIO General Functions. Note that data received by the e-STUDIO using its fax function is not user document data of the e-STUDIO users but the data of a person who has sent it.

## 7. Bibliography

- [1] e-STUIDO555/655/755/855 Security Target Ver.1.1, June 11 2009, TOSHIBA TEC CORPORATION
- [2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01
- [3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02
- [4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03
- [5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001
- [6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002
- [7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003
- [8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Translation Version 1.2, March 2007)
- [9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Translation Version 2.0, March 2008)
- [10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Translation Version 2.0, March 2008)
- [11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004
- [12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Translation Version 2.0, March 2008)
- [13] Evaluation Technical Report (DCI-ETR-0002-00), June 19, 2009, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center



# Surveillance Report

Issue Date: 2012-08-17

Document No.: SRP-C0219-01

This is to report that surveillance has been conducted on the following Target of Evaluation (hereinafter referred to as “TOE”), based on IT Security Certification Procedure (CCM-02) 8.1. It is recommended to use as a reference along with the Certification Report.

**TOE:**

Certification No.	C0219
Sponsor	TOSHIBA TEC CORPORATION
Name of the TOE	[Japanese] e-STUDIO555/655/755/855 System Software [English] System Software for e-STUDIO555/655/755/855
Version of the TOE	V3.0
PP Conformance	None
Assurance Package	EAL3
Developer	TOSHIBA TEC CORPORATION
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

**Surveillance Number: JISEC-SV12-001****Report on Surveillance Conducted:**

- **Surveillance Result**

In regard to this surveillance, it is confirmed by the Evaluation Facility that consumers are able to safely use the TOE; therefore, it is concluded that the certification of this TOE is maintained.

- **Surveillance Summary**

As for the contents of the following “Announcement”, which was released by the developer regarding this TOE, surveillance has been conducted from 2012-04 to 2012-07 in order to determine whether it is appropriate to maintain its certification.

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

( Translation notes: English information can be found at:  
<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1239> )

According to the “Announcement”, there is a possibility that the administrator page of the web-based management utility “TopAccess” site could be accessed without passwords by using the released vulnerability.

As a result of surveillance, it was verified in the previous evaluation under the responsibility of the Evaluation Facility that the access to the administrator page of “TopAccess” does not affect the security functions of the TOE, although the effects on other functions outside the security functions of the TOE cannot be denied.

The details are described as follows:

The TOE has a function to automatically delete the stored user document data after passing the expiration date, and it specifies that the residual data after being deleted is recognized as an asset to be protected.

From the administrator page of “TopAccess”, it is possible to change the time and date of MFP clock as well as the expiration date for storing user document data, etc. Therefore, there is a concern that Data Overwrite Function, which is one of the security functions of the TOE, might not be enforced as the user’s assumed expiration date.

However, the developer claims that the time and date of MFP clock as well as the expiration date for storing user document data, etc., cannot be changed when accessing the administrator page of “TopAccess” by using the released vulnerability.

Regarding this concern, the Evaluation Facility has made the following decision based on the previous evaluation.

- 1) The previous evaluation did not examine whether it is possible to change the time and date of MFP clock as well as the expiration date for storing user document data, etc., by using the released vulnerability when accessing the administrator page of “TopAccess”.
- 2) It is obvious for consumers that an asset to be protected is the residual information in case of being deleted after passing its expiration date, and that the information itself is not recognized as an asset to be protected if the setting related to the expiration date was changed and not deleted. Thus, consumers would not raise such a concern.
- 3) Therefore, even if the administrator page of “TopAccess” is accessed and such settings as the time and date of MFP clock as well as the expiration date for storing user



document data, etc., are changed, it does not affect the assured security functions of the TOE.

As with other functions which can be used from the administrator page of “TopAccess”, it is reported that the previous evaluation by the Evaluation Facility verified there was no effect on the security functions of the Target of Evaluation.