Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-05-27 (ITC-0296)
Certification No.	C0328
Sponsor	Toshiba Tec Corporation
Name of the TOE	TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS
Version of the TOE	SYS V1.0
PP Conformance	IEEE Std 2600.1-2009
Assurance Package	EAL3 Augmented with ALC_FLR.2
Developer	Toshiba Tec Corporation
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.
2011-10-28

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS" has been evaluated based on the standards required in accordance with the provisions 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

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS, Version SYS V1.0" (hereinafter referred to as the "TOE") developed by Toshiba Tec Corporation, and the evaluation of the TOE was finished on 2011-10-13 by Information Technology Security Center Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It reports to the sponsor, Toshiba Tec Corporation and provides security information to consumers and procurement personnel who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes general consumers who purchase this TOE to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The target of evaluation, the TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS (hereinafter referred to as "MFP") has copy, print, scan, e-Filing and Internet Fax functions.

In addition to the above basic functions, the TOE provides security functions to protect the document data handled by the basic functions and the setting data affecting security, from being disclosed or altered.

Regarding such security functionality, the validity of the design policy and the accuracy of implementation have been evaluated in the scope of the assurance package. The threats and the assumptions that this TOE assumes are as follows:

1.1.2.1 Threats and Security Objectives

This TOE offers security functions to oppose the following threats:

There are assumed threats that the document data that are assets to be protected and the setting data affecting security might be accessed or modified by a third party who is not allowed to use the TOE, or disclosed due to improper use by a user.

In order to counter these threats, the TOE provides functions such as identification/ authentication of users, access control by user authority, data encryption and audit log generation.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

The optional "GP-1070" Kit shall be installed to overwrite hard disk drive (hereinafter referred to as "HDD") of the TOE.

The product shall be set up in a safe area protected from unauthorized physical access, such as removal or disassembly of hardware.

The product shall be used in a network environment protected from unauthorized access on the external network by firewall.

1.1.3 Disclaimers

Since this evaluation is conducted only on the TOE set in high security mode, the TOE that is changed to another mode is not assured by this evaluation.

In order to detect tampering during transportation, this TOE is packed in a cardboard box from TOSHIBA TEC Corporation and delivered via a sales company contracted by TOSHIBA TEC Corporation. When a purchaser of this TOE instructs the sales company to unpack the packed TOE from the cardboard box in order to reduce setup time in the office, the TOE can be delivered unpacked.

This evaluation assures the means of transportation packed from TOSHIBA TEC Corporation to its customer' office; however, once the purchaser gives the above instruction, the tamper-proof packaging is removed, causing the means of transportation between the sales company and the customer office not to be assured.

Therefore, once an instruction to unpack the TOE is given, the TOE is not assured by this evaluation.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2011-10 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], and "Evaluation Facility Approval Procedure"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report and Observation Reports prepared by the Evaluation Facility as well as evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. Certification oversight reviews were also prepared for those concerns found in

the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE	TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS
Version of the TOE	SYS V1.0
Developer	Toshiba TEC Corporation

Users can verify that a product is the evaluated and certified TOE by the following means.

When the counter button on the Operation Panel Unit is pressed, the TOE version can be displayed on the LCD of the Operation Panel Unit.

3. Security Policy

This chapter describes security function policies and organisational security policies.

The TOE provides copy, print, scan, e-Filing and Internet Fax functions, and has functions to store the user document data to the internal HDD and to communicate with user clients and various servers via network.

When the above functions are used, the TOE provides security functions that fulfill the security functional requirements required by the Protection Profile for digital MFPs, IEEE Std 2600.1-2009 [14] (hereinafter referred to as the "PP"). The security functions provided by the TOE include user identification/authentication, access control of users, encryption of data stored on HDD, data overwrite in deleting data on HDD, and encryption communication protocol. The TOE prevents the user's document data that are assets to be protected and the setting data affecting security from being disclosed or altered.

The TOE assumes the following roles when it is used:

- U.NORMAL (General user)
  Any general user of the TOE who uses basic copy, print, scan, e-Filing and Internet Fax functions (transmission only) of the TOE.

- U.FAXOPERATOR (Fax operator)
  A user who is allowed to use the Internet Fax functions (transmission/reception). General users are not allowed, but only Fax operators are allowed to print the document data received by the Internet Fax function.

- U.ADMINISTRATOR (TOE administrator)
  A TOE administrator who has management authorities to configure the settings of TOE security functions, to change the user's account information, and to access audit logs.

- U.ACCOUNTMANAGER (Account administrator)
  An account administrator who can only change the user's account information (user ID, authority to perform the basic functions given to users) among management authorities that the TOE administrator can implement.

- U.AUDITOR (Log auditor)
  A log auditor who is allowed to only access audit logs via network among management authorities that the TOE administrator can implement.

The TOE's assets to be protected are as follows:

- User Document Data
  User's document data

- User Function Data
  Information on the user's document data or jobs to be processed by the TOE. Print queue job information and e-mail address book are included.

- TSF Protected Data
  Among data used for security functions, only the integrity of which is required. Authority information by user role, TOE setting information and network setting information are included.

- TSF Confidential Data
  Among data used for security functions, the integrity and confidentiality of which are required. HDD encryption key, audit logs and user password are included.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1., and to meet the organisational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions to counter them. These threats are the same as those described in the PP.

Table 3-1 Assumed Threats

Identifier	Threat
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasures against threats "T.DOC.DIS," "T.DOC.ALT" and "T.FUNC.ALT"

These are threats to the user data. The TOE counters the threats by the User Authentication, User Access Control, Secure Erase and Secure Channel functions.

The User Authentication function allows only identified and authenticated users to use the TOE. The TOE restricts the number of characters of authentication password to be eight or more. If successive attempts by a user fail for a predefined number of times, the user's account ID for the TOE is locked. A function to forcibly log out authentication is prepared when a user does not operate the TOE for a specified amount of time.

The User Access Control function controls access when a user operates the user data based on the user ID of the identified and authenticated users as well as the authority of user roles. For operation requests from general users, the TOE checks whether or not the login user ID is consistent with the user ID attached to the document data, and controls whether to allow or deny each operation. Users who have special roles other than general users, such as TOE administrators and Fax operators, are allowed to perform the operation specific to the user data on a role basis.

The Secure Erase function overwrites the HDD area where the document data are stored after a job of the MFP basic functions, such as a copy job, is completed. This function prevents the deleted document data from being read out from the HDD.

The secure communication function included in the Secure Channel function uses the SSL protocol when the TOE communicates with client PCs or servers. This function can keep the communication data secret and detect tampering.

(2) Countermeasures against threats "T.PROT.ALT," "T.CONF.DIS" and "T.CONF.ALT"

These are threats to the TSF data. The TOE counters the threats by the TSF Data Protection, User Authentication, User Access Control and Secure Channel functions.

The TSF Data Protection function allows only identified and authenticated TOE administrators to change the setting information of the TOE, and to enable or disable protocols.

The User Authentication function, the User Access Control function and the Secure Channel function are the same as those described in (1).

With the above functions, the TOE prevents the data to be protected from being disclosed or altered by unauthorized usage of the TOE and by unauthorized access to the communication data.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies imposed on the use of the TOE are shown in Table 3-2. These organisational security policies other than P.CRYPTOGRAPHY are the same as those described in the PP.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect malfunction of the TOE, procedures will exist to self-verify executable code in the TOE.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be

	controlled by the TOE and its IT environment.
P.CRYPTOGRAPHY	User document data stored in an HDD must be encrypted to improve the secrecy of the document.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to fulfill the Organisational Security Policies shown in Table 3-2.

(1) Means for organisational security policy "P.USER.AUTHORIZATION"

The TOE realizes this policy by the User Authentication function and the User Access Control function.

The User Authentication function allows only identified and authenticated users to use the TOE.

The User Access Control function controls access when a user uses print, scan, copy, e-Filing and Internet Fax functions, and allows only authorized users to use those functions. With this function, the TOE refers to information on the roles assigned to users for each function to check whether the user is allowed to use the function.

(2) Means for organisational security policy "P.SOFTWARE.VERIFICATION"

The TOE realizes this policy by the TSF Self Protection function.

The TSF Self Protection function performs the TSF self-test on the Operation Panel Unit of the TOE and verifies the integrity of all TSF execution codes and the HDD encryption key. If an error is detected, this function disables the use of the TOE. Only TOE administrators are allowed to perform the TSF self-test.

(3) Means for organisational security policy "P.AUDIT.LOGGING"

The TOE realizes this policy by the Audit Data Generation and Review function.

The Audit Data Generation and Review function generates audit logs, comprised of the event type, date, user identifier and event result (success/failure), when security events to be audited occur. Access to audit logs is restricted only to authorized users, such as log administrators and TOE administrators.

(4) Means for organisational security policy "P.INTERFACE.MANAGEMENT"

The TOE realizes this policy by the User Authentication function and the Secure Channel function.

The User Authentication function allows only identified and authenticated users to use the TOE. The TOE terminates a session when the state that a user does not perform operations continues for a specified amount of time.

The data transfer limitation function included in the Secure Channel function prevents data from being improperly transferred from the external interface of the TOE (USB interface and Operation Panel Unit) to the LAN interface.

The TOE needs to be used in an IT environment protected from unauthorized access on the external network by security measures, such as firewall.

(5) Means for organisational security policy "P.CRYPTOGRAPHY"

The TOE realizes this policy by the Data Encryption function.

The Data Encryption function encrypts and decrypts the document data saved on the HDD of the TOE using an AES (FIPS PUB 197) 128-bit encryption key.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to judge the use of the TOE.

4.1 Usage Assumptions

Assumptions required in the use of the TOE are shown in Table 4-1. These assumptions are the same as those described in the PP.

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

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organisation, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organisation, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environment Assumptions

This TOE is assumed to be set up in an office, connected to an in-house network and used from the clients connected to the in-house network in the same manner as the TOE. The general operational environment of this TOE is shown in Figure 4-1.

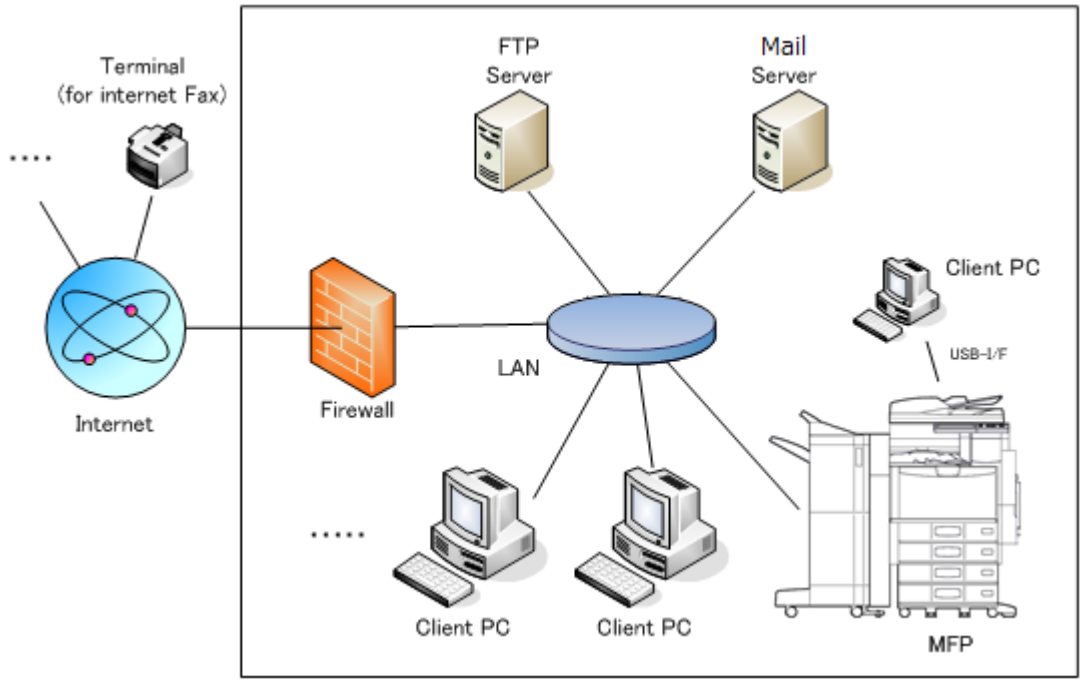

Figure 4-1 Operational Environment and Configuration

(1) Client PC

A client PC is connected to the TOE via LAN and USB interface, and intended to help general users request the TOE to print a document, to save document data in the registered e-Filing Box, and to retrieve the data from the e-Filing Box. TOE administrators can also refer to and change the setting data in the MFP using a web browser.

The following software is required:
OS: Windows XP or Windows Vista
Browser: Internet Explorer Ver.8.0
The following versions of the Client Utility Software

OS: Windows XP or Windows Vista	
Address Book Viewer	3.2.20.0
e-Filing Back Up/Restore Utility	3.2.22.0
File Down Loader	3.2.24.0
TWAIN Driver	3.2.25.0
Printer Driver	6.20.2521.6

(2) Mail Server, FTP Server

These servers are installed when the MFP basic functions, such as scan and Internet Fax, are used. The SSL protocol is used when the TOE communicates with servers.

(3) Firewall

Firewall is installed to prevent unauthorized access from the external network.

The reliability of the hardware and the cooperating software shown in this configuration is out of the scope of the evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

(1) If this TOE is operated using the LDAP server, the Domain server, the SMB server or the NTP server, it is not subject to evaluation.

(2) In this evaluation, it is confirmed that the TOE does not provide the following functions, because it is considered that the reception of print data sent from the printer driver of the user client PC and the reception of e-mail from the mail server are not subject to the security functional requirements for identification/authentication required by the PP.

- Authentication function when print data from the client PC are stored in the TOE
- Identification/authentication function when email from the mail server is stored in the TOE

5. Architectural Information

This chapter explains the scope of the TOE and the main components (subsystems).

5.1 TOE Boundary and Component

The configuration of the TOE is shown in Figure 5-1. The colored area within "General Function" indicates the basic functions of the TOE and any other colored area indicates the security functions of the TOE.

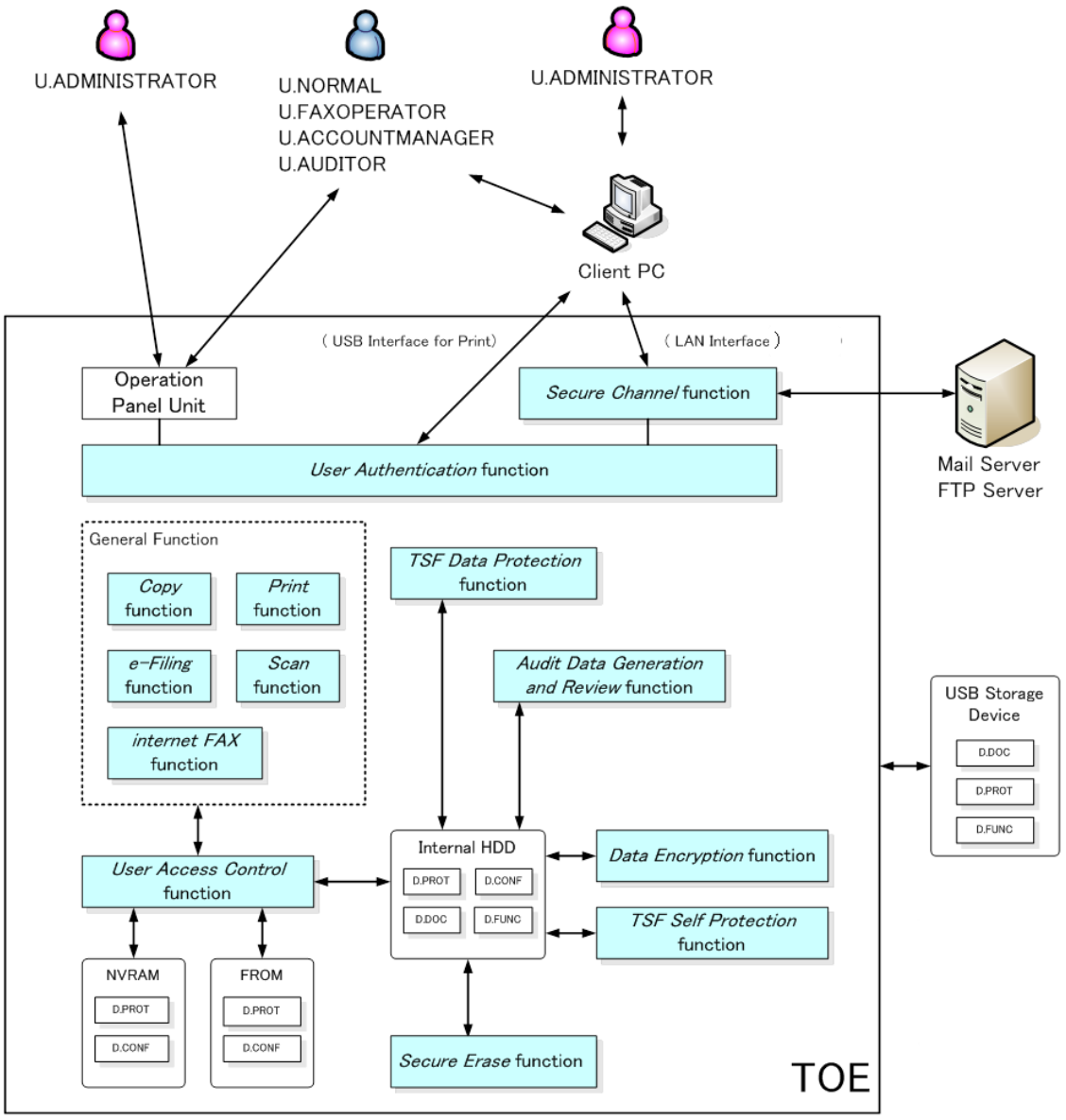

Figure 5.1 TOE boundary

The security functions of the TOE are used when a user uses the basic functions of the TOE. The relation between the security functions and the basic functions of the TOE is described below:

(1) Operations from client PC

A client PC can be connected to the TOE via LAN or USB. When the TOE communicates the client PC connected via LAN, the SSL protocol is used to protect communication data. Users can use the TOE from the client PC using the following tools:

(a) Web browser
When a user performs operations, such as account management, TOE setting changes, log audit and access to the document data stored in the e-Filing Box of the internal TOE, by operating a web browser from a client PC connected to the TOE via LAN, the User Authentication function identifies and authenticates the user and allows only authorized users to operate the TOE.

(b) Printer driver
When a user sends a request to print document data from the printer driver of the client PC connected to the TOE via LAN or USB, the User Authentication function identifies the user and the print data are stored in the TOE.

(2) Operation from Operation Panel Unit

When a user the basic functions, such as copy, print, scan, Internet Fax and access to the document data stored in the e-Filing Box of the internal TOE, by operating the Operation Panel Unit, the User Authentication function identifies and authenticates the user and allows only authorized users to operate the TOE.

The User Access Control function restricts operations of the basic functions in (1) and (2) only to users authorized by TOE administrators or account administrators.

Only general users who prepare document data or TOE administrators are allowed to delete the document data or job data. (As for the print function, authorized Fax operators are also allowed to delete document data and job data.)

(3) Internal HDD data protection

The Data Encryption function encrypts data to be stored on the HDD using an encryption chip incorporated into the TOE.

The Secure Erase function protects the area on the HDD, where the deleted document data are saved, by overwriting with the Department of Defense (DoD) Erase function.

(4) Network protection

The Secure Channel function uses the SSL protocol to protect communication data and to prevent data from being improperly transferred from the external interface of the TOE to the LAN interface when the TOE communicates with IT devices such as client PC, mail server and FTP server via LAN.

(5) Generation of audit logs

The Audit Data Generation and Review function generates audit logs when security-related events to be audited occur. Deletion of audit logs is restricted only to TOE administrators.

(6) TOE self-test

The TSF Self Protection function performs the TSF self-test and verifies the integrity of all TSF execution codes and the HDD encryption key upon the request of the TOE

administrator. If an error is detected, this function provides a function to disable the use of the TOE.

(7) TSF data protection
The TSF Data Protection function allows only TOE administrators to perform operations, such as changes in settings affecting the security functions of the TOE, and allows only TOE administrators and account administrators to perform operations, such as changes in user authorities to use the basic functions.

5.2 IT Environment

Only the time that the TOE retains is used as the time information recorded in the audit log of the TOE. The TOE that synchronizes with the external time server via NTP protocol is not subject to evaluation.

Document data can be saved in the USB Storage Device connected to the TOE; however, the document data saved in the USB Storage Device are not subject to this evaluation and not assured.

6. Documentation

The identification of documents attached to the TOE is listed below.

TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Guidance (English version)

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

Table 6-2 Guidance (Japanese version)

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

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3.

Details for evaluation activities were reported in the Evaluation Technical Report.

In the Evaluation Technical Report, it explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.2 Overview of Evaluation Activity

The history of evaluation conducted is described in the Evaluation Technical Report as follows.

Evaluation has started on 2010-05 and concluded upon completion of the Evaluation Technical Report dated 2011-10.

The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2011-02 and 2011-05 and 2011-06, and examined procedural status conducted in relation to each work unit for the operation in life-cycle support, such as configuration management, delivery, and development security, by investigating records and interviewing staff.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-05 and 2011-06.

Concerns found in evaluation activities for each work unit were all issued as the Observation Report and were reported to the developer.

These concerns were reviewed by the developer, and all concerns were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as a certification oversight review, and it was sent to the Evaluation Facility.

After the Evaluation Facility and the developer examined them, these concerns were reflected in the Evaluation Technical Report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had executed.

As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator executed the reappearance testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the documentation of actual testing results.

The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration executed by the developer.

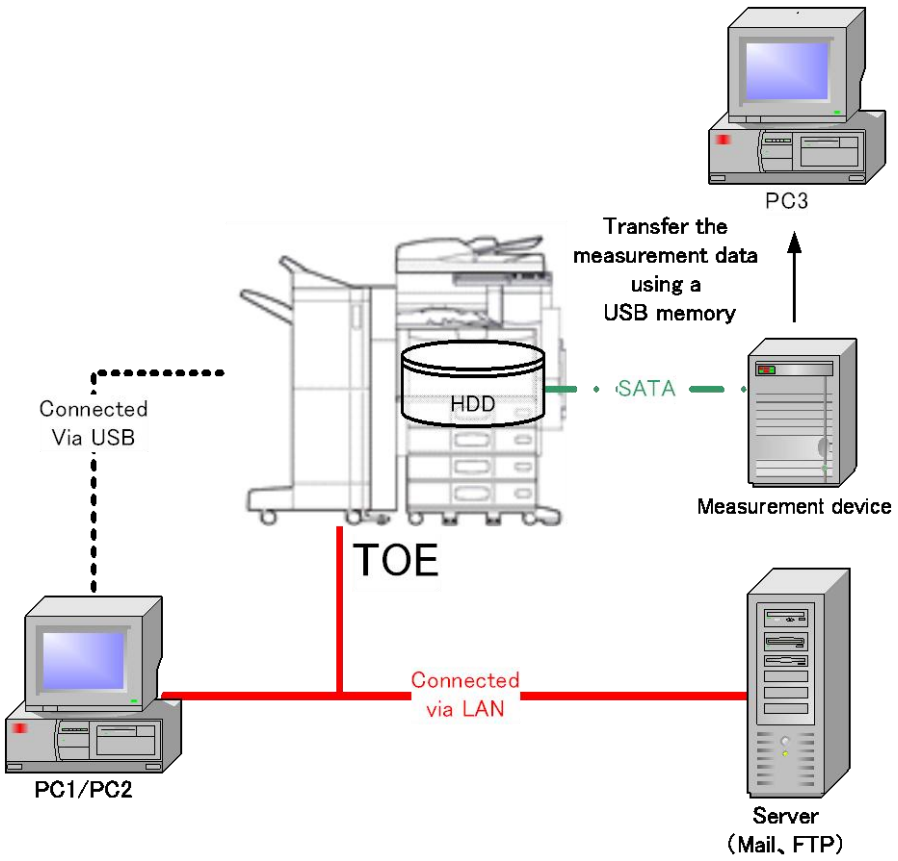

Figure 7-1 Configuration of the Developer Testing

The TOE subject to the developer testing is shown, and all TOEs identified are included.

Table 7-1 Variations of the TOE

Product Name	Version
TOSHIBA e-STUDIO2040C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO2540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO3040C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO3540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0
TOSHIBA e-STUDIO4540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0

The components other than the TOE are shown in Table 7-2.

Table 7-2 Variations of the TOE

Device	Specification	
PC1	TOSHIBA EQUIUM 3270	
	OS	Windows XP Professional Version2002 ServicePack3
	Client Utility Software	Print Driver version 6.20.2521.6
		Address Viewer version 3.2.20.0
		e-Filing BackUp/Restore Utility version 3.2.22.0
		File DownLoader version 3.2.24.0
		TwainDriver version 3.2.25.0
	Brower	InternetExplorer8
	Mailer	OutlookExpress6
	CSV browser	EXCEL2007
	Twain driver check software	Microsoft Office Document Imaging Viewer version 12.0.6423.1000
PC2	DELL OPTIPLEX320	
	OS	Windows VISTA SP2
	Client Utility Software	Print Driver version 6.20.2521.6
		Address Viewer version 3.2.20.0
		e-Filing BackUp/Restore Utility version 3.2.22.0
		File DownLoader version 3.2.24.0
		TwainDriver version 3.2.25.0

	Brower	InternetExplorer8
PC3	HP COMPAQ dc5000sff	
	OS	Windows XP Version2002 ServicePack3
	Measurement device driver	Application Software for Serial ATA(Ver.6.20)
Server	DELL PowerEdge2650	
	OS	WindowsServer2008R2 Enterprise ServicePack1
	Mail server	Exchange Server 2010 ver14.01.0270.001 (POP, SMTP) * FTP is set by OS functions.
Measurement device	LeCroy SAS Suite SATA Analyzer MODEL SAS001MA	

The developer testing was conducted in the same TOE testing environment as the TOE configuration identified in this ST.

2) Summary of Developer Testing

A summary of the developer testing is as follows.

a. Outline of Developer Testing
The testing conducted by the developer is outlined as follows:

<Developer Testing Approaches>
As an approach to stimulating the external interface that is available from this TOE, the testing was conducted by manual operation from the Operation Panel Unit or the client PC to check the behavior.

The following were carried out as the approaches to observing the responses from this TOE:

(1) To check the behavior results displayed on the MFP panel.

(2) To check the printout results from the MFP.

(3) To analyze data on the HDD input/output pathways by attaching the analyzer tool to the MFP.

(4) To check the behavior results displayed on the client PC screen.

(5) To capture communication packets using the network protocol analyzer.

<Tools for Developer Testing>
The tools used for developer testing are shown in Table 7-3.

Table 7-3 Tools for the Developer Testing

Name of Tool (Version)	Purpose of Use

TeraTermPro (version 2.3)	To obtain and operate developer logs
WireShark (version1.2.7)	To capture protocols
PupSQLite (version 1.9.13.3)	To check log databases

<Detailed Testing conducted by Developer>
The developer testing that covers all security functions, such as applicable data on the HDD to be encrypted, access control to be properly implemented, and SSL communication to be properly working, was conducted. Actual testing results are all consistent with the expected ones, and there is no difference between the actual testing results and the expected results.

b. Scope of the Executed Developer Testing

The developer testing was conducted on 165 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

By the depth analysis, it was verified that all subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

The evaluator confirmed the approach of the executed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach.

The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results executed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by the test items extracted from the developer testing. The evaluator executed the evaluator independent testing (hereinafter referred to as the "independent Testing") to reconfirm that security functions are certainly implemented from the evidence shown in the process of the evaluation.

The independent testing executed by the evaluator is explained as follows.

1) Independent Testing Environment

The environment where the independent testing was conducted by the evaluator is the same as the environment where the developer testing was conducted.

The TOE to be evaluated is shown below. This TOE has several variations; however, there is only a difference in print speed between the TOSHIBA e-STUDIO3540C and the others, namely, TOSHIBA e-STUDIO2040C, TOSHIBA e-STUDIO2540C, TOSHIBA e-STUDIO3040C and TOSHIBA e-STUDIO4540C, and there is no difference in security

functions. Therefore, the following TOSHIBA e-STUDIO3540C was used to conduct the independent testing. The configuration of the independent testing is deemed to include all TOEs identified.

Table 7-4 Variations of the TOE

Product Name	Version
TOSHIBA e-STUDIO3540C MULTIFUNCTIONAL DIGITAL SYSTEMS	SYS V1.0

2) Summary of Independent Testing

The independent testing conducted by the evaluator is as follows:

a. Independent Testing Points of View

The points of view for the independent testing that the evaluator designed from the developer testing and the provided evaluation evidential materials are shown below.

(1) If there is any interface or function lacking in strictness in the testing plan for developer testing, it is applied to the independent testing.

(2) To select the interface to be tested, allowing all interface types provided by the TOE to be covered by the sample testing in the developer testing and the testing designed by the evaluator.

b. Independent Testing Outline

The independent testing conducted by the evaluator is outlined as follows:

<Independent Testing Approaches>
The test items sampled from the developer testing are implemented. The TOE behavior related to input parameters and access authorities that raise concerns about not being taken into account by the developer testing is tested.

<Tools for Independent Testing>
The same testing tools as those used in the developer testing were used.

<Detailed Independent Testing>
The independent testing was conducted by the developer on 36 items of the sample testing in the developer testing and 6 items of the testing the evaluator designed.

Table 7-5 shows the points of view for the independent testing and the content of the testing corresponding to them.

Table 7-5 Points of View for the Independent Testing

Points of View	Outline of Independent Testing
(1)	It was confirmed that the following are as specified: - Behavior for setting character strings that are disallowed by the password policy

	- Behavior for registering the same user ID - Behavior for accessing with the old password after changing the password - Exclusive control of e-Filing Box - Authority to operate logs - Authority to operate general functions
(2)	The evaluator implemented test items sampled from the developer testing, allowing all interface types provided by the TOE to be covered. It was confirmed that all actual testing results were consistent with the expected testing results.

c. Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of the TOE.

The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and executed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") for the possibility of exploitable concern at assumed environment of use and attack level from the evidence shown in the process of the evaluation.

The penetration testing executed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing executed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided evidence and the public domain information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

(1) There are concerns about unauthorized use of network services as vulnerability information in the public domain as well as various web vulnerabilities.

(2) There are concerns about the unexpected behavior of the TOE due to entries exceeding the limit and entries of unexpected character codes on the interface other than the web, such as the Operation Control Unit, when a search is made into general attacks in the public domain.

(3) There are concerns about the unexpected behavior of the TOE due to competing operations from the Operation Control Unit and the client PC when a search is made

into development evidential materials.

(4) There are concerns that security functions, such as HDD encryption/decryption and communication using the SSL protocol, do not properly operate when a search is made into development evidential materials.

b. Penetration Testing Outline

The evaluator executed the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>

The penetration testing was conducted by the evaluator in the developer-testing environment where the PC for penetration testing was additionally installed and connected via LAN.

Details of the PC for penetration testing and the tool used are shown in Table 7-6.

Table 7-6 PC for Penetration Testing and Tool Used

Component	Outline
PC for penetration testing	NEC VersaPro VJ10A/C-5 OS: Windows XP SP3
Tool used	nmap version 5.51 (port scan tool)

<List of Executed Penetration Testing>

Table 7-7 shows concerned vulnerabilities and the content of the related penetration testing.

Table 7-7 Outline of Penetration Testing

Vulnerability	Outline of Testing
(1)	By executing nmap to the TOE, it was confirmed that the unintended port is not open. By entering OS commands or improper scripts into the interface, it was confirmed that there is no vulnerability in the public domain, such as various injections.
(2)	By entering data exceeding the limit or invalid data for password and user ID, it was confirmed that the TOE did not produce behavior affecting security functions when identification/authentication was carried out on the Operation Control Unit. It was confirmed that improper programs were not incorporated into the TOE via the USB interface.

(3)	By simultaneously performing operations from the Operation Control Unit and the client PC to change a user password or set the TOE, it was confirmed that TOE did not produce unexpected behavior due to competing.
(4)	The following were confirmed; error handling, for example, in the case of a paper jam, did not affect encryption; access was always denied upon the request of communication without using the SSL protocol; and the TOE was inoperable when the encryption key was not properly used.

c. Result

In the penetration testing conducted by the evaluator, the evaluator did not find any exploitable vulnerability that attackers who have the assumed attack potential could exploit.

7.4 Evaluated Configuration

TOE configuration conditions for assumption of this evaluation are described in the guidance. The TOE needs to be set in accordance with "Safety Information" and "High Security Mode Management Guide".

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.
- PP Conformance:
  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  (IEEE Std 2600.1-2009)

  SFR packages conformance defined in the above PP:
  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A: Conformant
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A: Conformant
  - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A: Conformant
  - 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A: Conformant
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A: Conformant

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

- Additional assurance component ALC_FLR.2

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the 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. Submitted evidential materials shall be sampled, the contents shall be examined, and the 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.

Concerns found in the certification process were prepared as certification oversight reviews and were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the Observation Report and certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 and assurance components ALC_FLR.2 in the CC part 3.

8.2 Recommendations

This TOE allows users to receive print data from the printer driver of the client PC without being authenticated, and allows users to receive e-mail from the mail server without being identified and authenticated. Therefore, it should be noted that the TOE might not meet the needs of consumers who expect to be authenticated and identified when receiving print data or e-mail.

If this TOE is operated using the LDAP server, the Domain server, the SMB server or the NTP server, it is not subject to evaluation; thus, consumers need to pay attention to their assumed operational environment before purchasing the product.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

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

11. Glossary

The abbreviations relating to the 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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

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

The definitions of terms used in this report are listed below.

Address Book Viewer	Software that allows managing the E-mail Address Book from a client PC.
DoD Erase function	HDD erase function that complies with Department of Defense Standard.
e-Filing Box Backup/Restore Utility	Software that allows backing up/restoring data in the e-Filing Box from a client PC to the client PC.
Built-in Administrator	Administrator account that is initially registered in the MFP.
TWAIN Driver/ File Downloader	Software that allows downloading data stored in the e-Filing Box of the MFP via TCP/IP network from a

	client PC.
TopAccess	Web-based software that allows operating job data, MFP management and e-Filing Box from a client PC.
U.ACCOUNTMANAGER (Account administrator)	A specially authorized user who can change user account information (permitted authorities to change user ID and basic functions).
U.ADMINISTRATOR (TOE administrator)	A specially authorized user who can manage and change the settings affecting the TOE security policy (TSP).
U.AUDITOR (Log auditor)	A special user who can view and perform data mining on MFP logs from the external network.
U.FAXOPERATOR (Fax operator)	A special user who can send document data, print received data, and operate document data or job data using the Internet Fax functions.
U.NORMAL (General user)	A general user who can use the document data processing functions of the TOE (copy/print/scan/e-Filing).
Internet Fax function	A function that allows scanned document data to be sent as a TIFF-FX (Profile S) attached to e-mail. When this function is used to send a scanned document to Internet Fax equipment or a client PC, the e-mail address of the equipment or the PC needs to be specified in place of the telephone number.
Copy function	A function that allows data that a general user scans in the MFP from the Operation Panel Unit to be printed on paper.
Scan function	A function that allows scanned data to be saved on the HDD and the saved data to be read. When a general user reads document data from the scanner unit, this function automatically notifies the event to a client PC, mail server or FTP server based on the information set to the MFP. A general user can use this function on the Operation Panel Unit.
e-Filing function	A function that allows a user to create an e-Filing Box. Specific users or TOE administrators can save, print and edit confidential documents.
e-Filing Box	Storage area that allows a user to save document

	data. This area allows data saved from the Operation Panel Unit or the client PC to be referred to, print or edit.
Print function	A function that allows print data to be received from the client PC connected to the TOE via LAN or USB, and the received data to be printed on paper.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, February 2011, Information-technology Promotion Agency, Japan, CCS-01

[2] IT Security Certification Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-02

[3] Evaluation Facility Approval Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-03

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

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

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

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)

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

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)

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

[13] TOSHIBA e-STUDIO2040C/2540C/3040C/3540C/4540C MULTIFUNCTIONAL DIGITAL SYSTEMS Evaluation Technical Report, Version 2.10, October 13, 2011, Information Technology Security Center Evaluation Department

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009