Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	August 8, 2006 (ITC-6097)
Certification No.	C0070
Sponsor	Panasonic Communications Co., Ltd
Name of TOE	DATA SECURITY KIT DA-SC02
Version of TOE	Version V1.00
PP Conformance	None
Conformed Claim	EAL2
TOE Developer	Panasonic Communications Co., Ltd
Evaluation Facility	Japan Electronics and Information Technology Industries Association, Information Technology Security Center (JEITA ITSC)

This is to report that the evaluation result for the above TOE is certified as follows.
October 31, 2006

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-technology Promotion Agency, Japan

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 2.3 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"DATA SECURITY KIT DA-SC02 Version V1.00" 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 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “DATA SECURITY KIT DA-SC02 Version V1.00” (hereinafter referred to as “the TOE”) conducted by Japan Electronics and Information Technology Industries Association, Information Technology Security Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Panasonic Communications Co., Ltd.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of product: Data Security Kit DA-SC02

Version: V1.00

Developer: Panasonic Communications Co., Ltd.

1.2.2 Product Overview

The TOE is a software product, Data Security Kit DA-SC02 installed in the digital color imaging system, to protect the used document data which had been already stored on the hard

disk drive after being processed by the digital imaging system from being disclosed illicitly.
The TOE is offered as an optional product of Panasonic Communications Co., Ltd. Digital Color Imaging System DP-C2635 / C2626 / C2121 for Japan (DP-C354 / C264 / C323 / C263 / C213 for Overseas), and provides the security functions by replacing with the standard bundled software of the digital imaging system.

1.2.3 Scope of TOE and Overview of Operation

The TOE is Data Security Kit DA-SC02 installed on the Digital Color Imaging System to protect the used document data which had been already stored on the hard disk drive after being processed by digital imaging systems from being disclosed illicitly.
TOE is used in an environment shown in Figure 1-1.

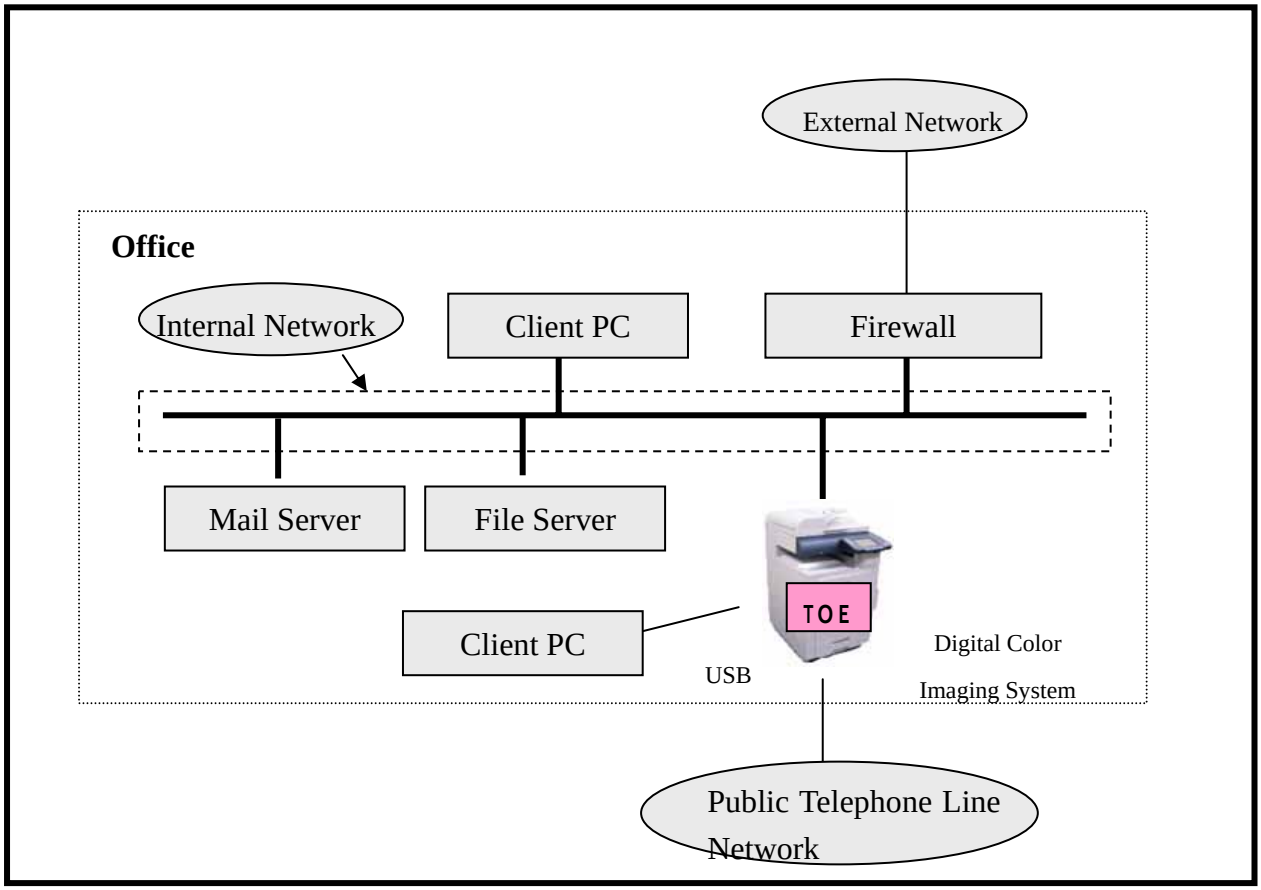

Figure 1-1 Assumed Usage Environment

The physical configuration of Digital Imaging System with TOE installed is shown in Figure 1-2.

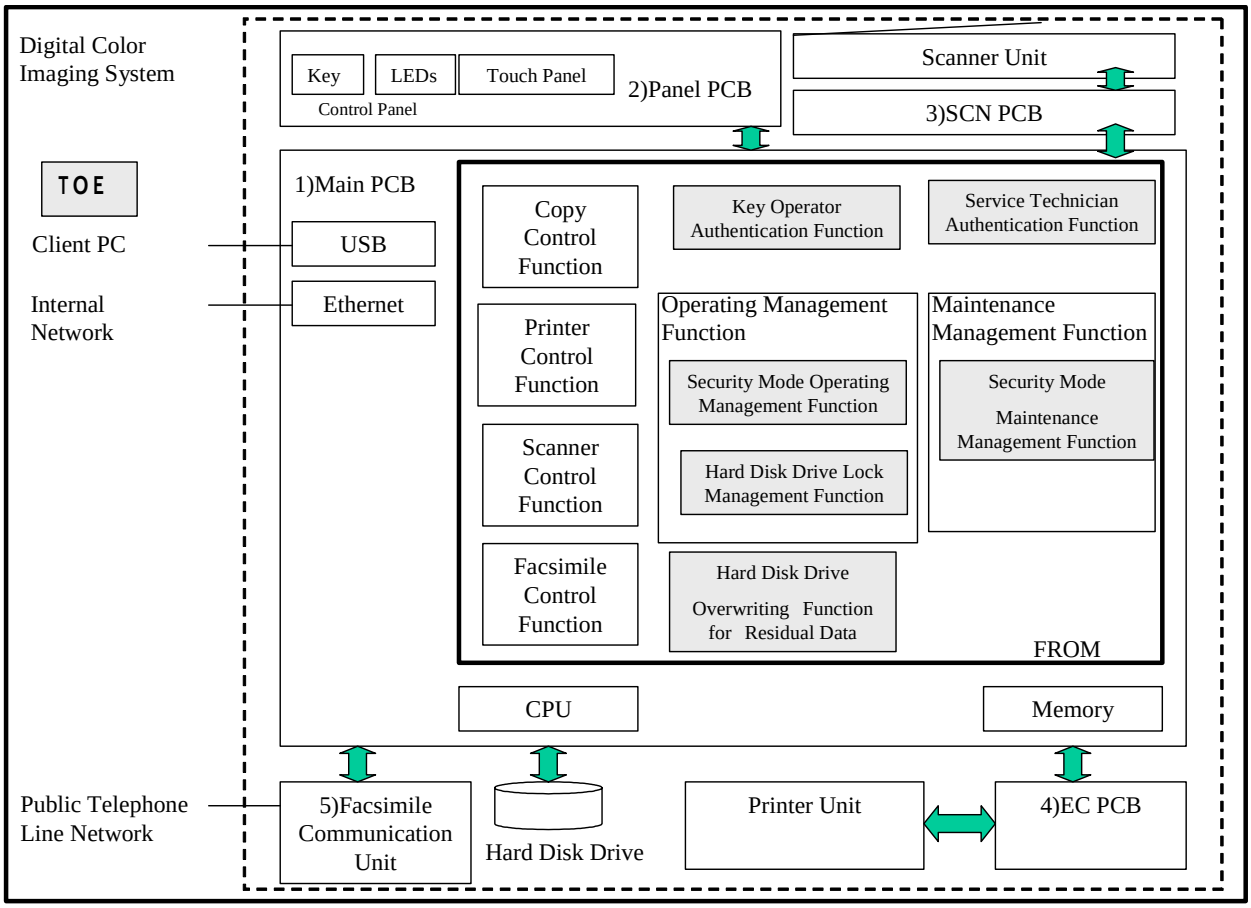

Figure 1-2 Physical Configuration

Digital Color Imaging System DP-C2635 / C2626 / C2121 for Japan (DP-C354 / C264 / C323 / C263 / C213 for Overseas) comprises of five PCBs, which are: 1) Main PCB to control the entire digital imaging system, 2) Panel control PCB that controls the control panel where all the necessary keys, LEDs and a touch panel for operations of digital imaging system are laid out, 3) SCN PCB that controls the mechanical operations of scanner unit, 4) EC PCB that controls the mechanical operations of printer unit and 5) PCB for facsimile communication unit.

1) Main PCB and 2) Panel PCB are connected by Internal Interface for communicating the control data.

1) Main PCB and 3) SCN PCB, 4) EC PCB are connected by Internal Interface for communicating the control data and the document data.

3) SCN PCB performs the communication of control data with scanner unit to control the mechanical motion of scanner. The document data captured from the scanner are sent directly to 1) Main PCB. Also 4) EC PCB exchanges the control data and document data with printer unit, and prints document data while executing the mechanical controls of the printer.

1) Main PCB and 5) Facsimile Communication Unit are connected to each other by Internal

Interface, and 5) Facsimile Communication Unit is further connected to Public Telephone Line Network to send/receive facsimile data.

Furthermore, 1) Main PCB has the Ethernet and USB interface to connect to Client PCs and Mail/File servers. Also, the hard disk drive unit to store the document data is connected to 1) Main PCB.

1) Main PCB comprises of CPU, FROM that stores software, Memory that stores data and other electronic circuits to control the entire digital imaging system.

The TOE is a group of software recorded on FROM that is mounted on Main PCB and is shown in the shaded portion of Figure 1-2, namely:

- Key Operator Authentication Function
- Service Technician Authentication Function
- Security Mode Operating Management Function
- Security Mode Maintenance Management Function
- Hard Disk Drive Lock Management Function
- Hard Disk Drive Overwriting Function for Residual Data

This TOE protects the used document data which had been already stored on the hard disk drive after being processed by copy, printer, scanner functions, from being disclosed illicitly.

1.2.4 TOE Functionality

The TOE has the security functions described bellow.

(1) Hard Disk Drive Overwriting Function for Residual Data

When the document data is processed by copy control function, printer control function or scanner control function, and becomes used document data, this function immediately and automatically overwrites and erases the entire area of the document data.

There are following three overwriting and erasing methods.

- Basic: Only the management information for the document data is deleted.
- Medium: Over the entire area of the document data, the data of all 0's are overwritten three times for erasure.
- High: Over the entire area of the document data, random values are overwritten twice and then all 0's are overwritten once for erasure.

This overwriting and erasing method is specified in the "Hard Disk Data Erasure Level" described in (4) Security Mode Operating Management Function.

Since "Basic: Only the management information for the document data is deleted" is the initial setting, the key operator normally selects Medium or High to operate the Digital Color Imaging System DP-C2635 / C2626 / C2121 for Japan (DP-C354 / C264 / C323 / C263 / C213 for Overseas).

Note that only the key operator can use the "Hard Disk Initialization" function which is described in (4) Security Mode Operating Management Function, to overwrite and erase the residual document data on the hard disk drive by either Medium or High, in such cases as the drives are discarded.

(2) Key Operator Authentication Function

This function is key operator identification and authentication, by means of the input to the control panel and the entered dedicated password for key operator (hereinafter called key operator password). Only the key operator can perform operations described in (3) Hard Disk Drive Lock Management Function and (4) Security Mode Operating Management Function.

(3)Hard Disk Drive Lock Management Function

The hard disk drive unit has the drive lock function attached whereby the password can directly be assigned to the hard disk drive so that the hard disk drive cannot be recognized unless the correct password is entered. Only the key operator can set up and change the password for the memory inside the digital color imaging system controlling the "Hard Disk Drive Lock Password" and the hard disk drive, and also reset the drive lock setting the password to "unsetup" condition. At its startup time, the digital imaging system sends the password stored in the memory inside the system to the hard disk drive, requesting the data access to it.

(4) Security Mode Operating Management Function

Only the key operator can direct following setup and change of setting data and processing regarding the security.

- "Hard Disk Data Erasure Level"

  This function specifies the erasing mode of overwriting data for residual data stored on the hard disk drive, which is automatically executed at the instant when the copy control function, printer control function or scanner control function is completed and the used document data develops.

  It can set up three types of overwriting and erasing, Basic (initial setting), Medium and High.

- "Hard Disk Initialization"

  Upon the direction from key operator, this function overwrites and erases all document data stored on the hard disk drive. As the ways to overwrite and erase, there are two types, Medium and High.

- "Delete All Image Files"

  This function when invoked by the key operator, overwrites and erases all document data stored in the image box which is inside the hard disk drive by the method specified by “Hard Disk Data Erasure Level” setting.

- "Key Operator Password"

  This function is to set up and change the key operator password.

(5) Service Technician Authentication Function

This function is identification and authentication for service technician by the operations of service mode setup procedure from the control panel as well as the entered password.

Only the service technician is allowed for operations described in (6) Security Mode Maintenance Management Function.

(6) Security Mode Maintenance Management Function

Only the service technician can direct the setup, change and initialization (returning to the initial setting) for the following setup data regarding the security.

- "Service Technician Password"

  Sets up and changes the service technician password.

- "System Initialization"

  Under the direction from the service technician, this function is to initialize such setup data as "Hard Disk Drive Lock Password" described in (3) Hard Disk Drive Lock Management Function, "Hard Disk Data Erasure Level" and "Key Operator Password" described in (4) Security Mode Operating Management Function, "Service Technician Password" described in (6) Security Mode Maintenance Management Function, to the initial setting.

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.

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

More specific, the evaluation facility examined “DATA SECURITY KIT DA-SC02 Security Target” 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 C of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in “DATA SECURITY KIT DA-SC02 Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [18]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

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. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated August, 2006 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.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL2 conformance.

1.5.3 SOF

This ST claims “SOF-Basic” as its minimum strength of security function.

This TOE is a product which assumes low attack capabilities. So, “SOF-Basic” is enough level as its minimum strength of security function.

1.5.4 Security Functions

Security Functions of the TOE are as follow.

-Hard Disk Drive Overwriting Function for Residual Data (SF.OVWRT)
The purpose of this function is to overwrite and erase the data area of the residual document data stored on the hard disk drive.

-Key Operator Authentication Function (SF.ADM_IA)
This function restricts such operations as the setting data of "Hard Disk Drive Lock Password", "key Operator Password", "Hard Disk Data Erasure Level" that are provided by Hard Disk Drive Lock Management Function (SF.HDMNG) as well as Security Mode Operating Management Function (SF.ADMMNG), and also the instruction of "Hard Disk Initialization" to be performed only by the key operator.
Before allowing any operation or instruction, it checks the key operator password entered from the control panel and identifies and authenticates that the operator is the key operator.

-Hard Disk Drive Lock Management Function (SF.HDMNG)
This function is for the key operator to manage the hard disk drive lock, and it authorizes and executes the setup and modification of "Hard Disk Drive Lock Password" and the release of drive lock, only when the key operator is identified and authorized by SF.ADM_IA.

-Security Mode Operating Management Function (SF.ADMMNG)
This function is the management function for key operator to conduct operations, and it authorizes and executes the setup/modification of "Key Operator Password", the setup/modification of "Hard Disk Data Erasure Level" and the instruction of "Hard Disk Initialization", "Delete All Image Files" only when the key operator is identified and authenticated by SF.ADM_IA.

-Service Technician Authentication Function (SF.SE_IA)
This function enables only the authenticated service technician to manipulate the setup data of "Service Technician Password" that is offered by Security Mode Maintenance Management Function (SF.SEMNG) and also to instruct "System Initialization".

-Security Mode Maintenance Management Function (SF.SEMNG)
This function is for service technician to carry out the management functions for maintenance works, and it authorizes and executes the setup/modification of "Service Technician Password" as well as the instruction of "System Initialization" only when an operator is identified and authenticated as service technician by SF.SE_IA.

1.5.5 Threat

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

Table 1-1 Assumed Threat

Identifier	Threat
T.RECOVER	-Illicit recovery of used document data General users or the non-related persons to TOE having malicious intention may attempt to recover the used document data by connecting PC or other tools to hard disk drive.

1.5.6 Organizational Security Policy

Organizational security policy required in use of the TOE is presented in Table 1-2.

Table1-2 Organizational security policy

Identifier	Organizational security policy
P.OWMETHOD	- The used document data remaining on the hard disk drive to be overwritten and erased. The data area of used document data remaining on the hard disk drive must be overwritten and erased.

1.5.7 Configuration Requirements

This Security Target offered as an optional product of Digital Color Imaging System DP-C2635 / C2626 / C2121 for Japan (DP-C354 / C264 / C323 / C263 / C213 for Overseas) manufactured by Panasonic Communications Co., Ltd.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The Effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table1-3 Assumptions in Use of the TOE

Identifier	Assumption Description
A.SETSEC	- Security Mode setting Key operator enables following TOE functions before operations. "Hard Disk Drive Lock Password" is set up.
A.ADMIN	- Credibility of key operator Key operator is a person who commits no illicit acts.
A.SE	- Credibility of service technician Service technician is a person who commits no illicit acts.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed bellow.

Manuals (Japanese version)		Corresponding English manual
1	Operating Instructions(For Basic Operations) Digital Color Imaging Systems DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F(in Japanese)	Operating Instructions(For Basic Operations) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
2	Operating Instructions(For Setting Up) Digital Color Imaging Systems DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F(in Japanese)	Operating Instructions(For Setting Up) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
3	Operating Instructions(For Copier) Digital Color Imaging Systems DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F(in Japanese)	Operating Instructions(For Copier) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
4	Operating Instructions (For Scanner and Email) Digital Color Imaging Systems DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F(in Japanese)	Operating Instructions (For Scanner and Email) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
5	Operating Instructions (For Function Parameters) Digital Color Imaging Systems DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F(in Japanese)	Operating Instructions (For Function Parameters) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
6	Operating Instructions Data Security Kit DA-SC02(in Japanese)	Operating Instructions Data Security Kit DA-SC02
7	Installation Instructions for Service Technicians Data Security Kit DA-SC02(in Japanese)	Installation Instructions for Service Technicians Data Security Kit DA-SC02

8	Service Manual Digital Color Imaging Systems DP-C2635 / C2626 / C2121 DP-C322 / C262(in Japanese)	Service Manual Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213 DP-C322 / C262

NOTE: Manuals（Japanese version) were translated from the original Japanese titles.

2 Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report 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 Part 2

2.2 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.2.1 Developer Testing

1）Developer Test Environment

Test Configurations performed by the developer are showed in the Figure 2-1 and 2-2.

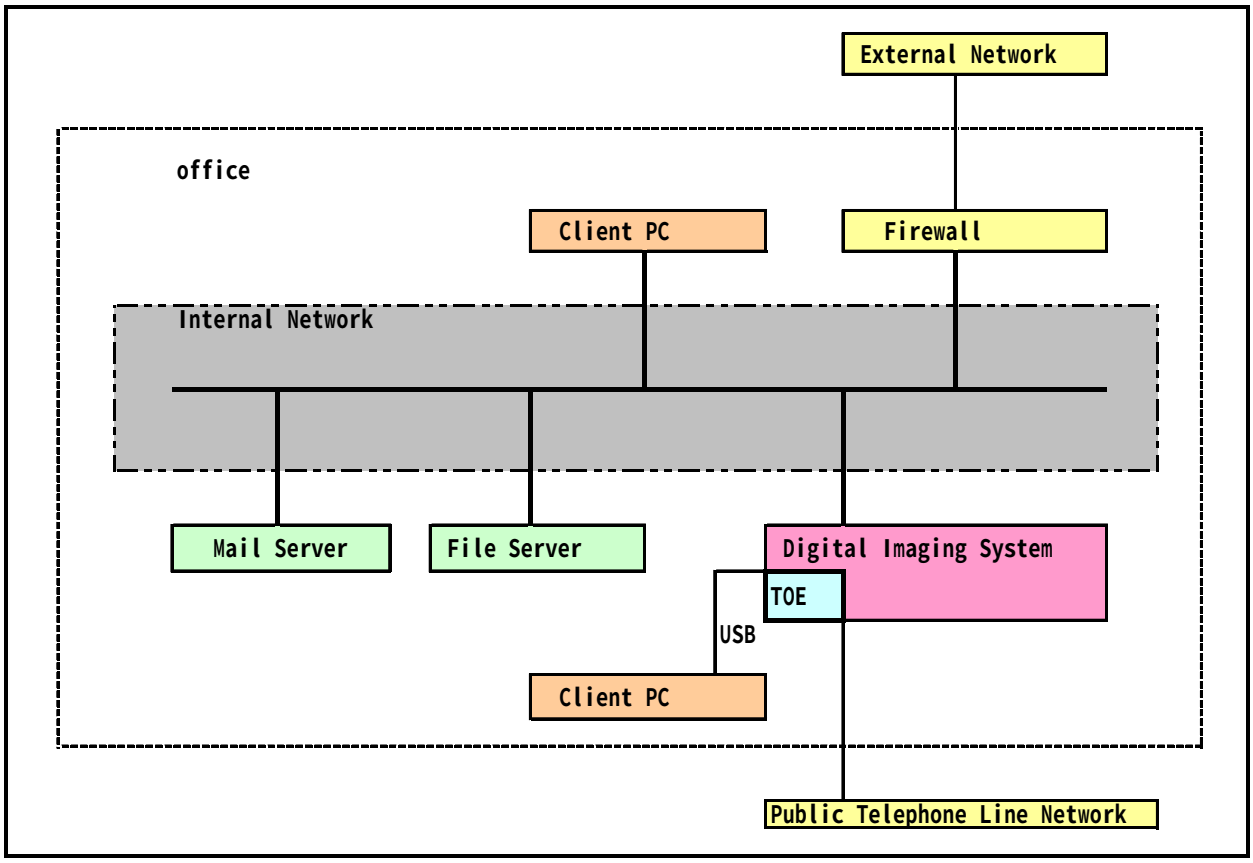

Figure 2-1 Configuration of Developer Testing

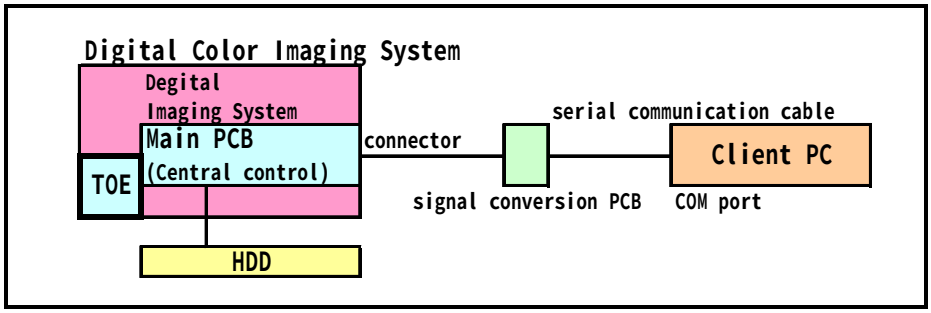

Fig. 2-2 Test Configuration of Hard Disk Drive Overwriting Function for Residual Data testing

2) Outlining of Developer Testing

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

a) Test configuration

Test configurations performed by the developer are showed in the Figure 2-1 and 2-2. The developer testing had been performed in the TOE testing environment equivalent to the TOE configuration identified in the ST.

b) Testing Approach

For the testing, following approach was used.

① Operating from the operation panel and monitoring status of the program processing.

Operating to the TOE from the operation panel and confirming the processing results.

② Operating from the remote PC and monitoring status of the program processing.

Operating from the equipment (client PC for general user, the Mail server, the FTP server or client PC for debugging etc.) that should be connected with the digital imaging system TOE installed, and confirming the processing results.

③ Confirmed the processing of Hard Disk Drive Overwriting Function for Residual Data, of the digital imaging system which was connected with the serial communications cable via client PC and the signal conversion PCB as shown in Figure 2-2.

c) Scope of Testing Performed

Testing is performed 171 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.

d) 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 and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

2.2.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator is the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a) Test configuration

Test configurations performed by the evaluator are showed in the Figure

2-1 and 2-2. The evaluator testing had been performed in the TOE testing environment equivalent to the TOE configuration identified in the ST.

b) Testing Approach

For testing, following approach was used.

① The security function is stimulated and observed the use of the operation panel that is an external interface of the digital color imaging system.

② Tests of detaching HDD which was installed in digital color imaging system, and exchange already prepared HDD of the other digital imaging system, etc.

③ Function Test that connects the serial connector which is internal interface of developer for digital color imaging system, to the debugging environment.

c) Scope of Testing Performed

Evaluator conducted total 98 items test (36 items created uniquely by evaluator, 62 items conducted by sampling from developer testing).

The following are considered as a test selecting items.

① A security function that might be doubted the operation to satisfy the specification which was done by developer testing.

② A security function that is more important than other security functions

③ Security function of target for function strength

④ Functions used from different interface

d) Result

All evaluator 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.

2.3 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report

3 Conduct of Certification

The following certification was conducted 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.

No concerns found in certification process were prepared as certification review.
The Certification Body confirmed such concerns pointed out in Observation Report were solved in the ST and the Evaluation Technical Report.

4 Conclusion

1) Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL2 assurance requirements prescribed in CC Part 3.

2) Recommendations

None

5 Glossary

The abbreviations 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 glossaries used in this report are listed below.

Digital Color Imaging System	Peripheral which integrates functions such as copy, printer, scanner and facsimile into one machine. In this document, the term “Digital Color Imaging System” is used to generically refer to the models DP-C2635 / C2626 / C2121 (for Japan) and DP-C354 / C264 / C323 / C263 / C213 (for Overseas) manufactured by Panasonic Communications Co., Ltd.
Internal Network	The LAN used in the organization where the Digital Color Imaging System is introduced.
External Network	The networks other than the Internal Network, such as internet.
Remote Operation Panel	A function that can instruct and operate a subset of copy, scanner, printer and facsimile functions of the Digital Color Imaging System from a general user‘s client PC connected to the internal network.

USB	A data transmission standard which connects peripherals to a personal computer.
General User	One who uses copy, printer, scanner or facsimile functions of Digital Color Imaging System.
Key operator	One who manages a Digital Color Imaging System.
Service Technician	A technician who belongs to the service provider company to provide installation, maintenance and repair services of Digital Color Imaging System.
Service Mode	A set of maintenance functions that the service technician uses for installation, maintenance and repair services of Digital Color Imaging System.
Service Mode Setting Procedure	The setting procedure that a service technician uses to switch the mode to Service Mode.
Initialization	Operation to go back to the initial setting, activated by a Maintenance Management function "System Initialization".
Control Panel	Operation Panel with keys, LEDs and a touch panel display required for operating the functions of Digital Color Imaging System.
SCN	PCB to control the mechanical function of scanner unit.
EC	PCB to control the mechanical function of printer unit.
FROM	Nonvolatile memory allowing electrical block erasure and reprogramming of arbitrary portion.
Document Data	Collective name for all digitized image data handled inside digital color imaging system when copy, print, scanner or facsimile functions are used in Digital Color Imaging System. - Image data captured from scanner unit. - Image data that can be printed on printer unit. - Image data that have been transformed from the raw data by image processing technology. - Image data received from client PCs or the received data

	to be transformed to image data.
Used Document Data	Document Data that is stored on the hard disk drive of the Digital Color Imaging System and had already been used.
Image box function	One of the scanner functions that stores the document data captured from the scanner unit on the hard disk drive, and allows the inspection and deletion of the document data from Web browser of general user's client PC.
Web browser	PC application software to browse a Web page. The application software downloads files such as the HTML file and the image file from the Internet and then analyzes the layout, and displays/replays these files.
Job	A unit of operations comprising of a series of functions in copy, printer, scanner or facsimile functions of Digital Color Imaging System.
Job Cancellation	Canceling function issued from Control Panel to cancel some of the jobs that have not been started with printing yet on the printer unit, after multiple jobs have been assigned to Digital Color Imaging System that is being used for copying or printing.
Accepting Sound	Panel touch tone peep sounding notifying that the input characters or operations from control panel have been accepted correctly in Digital Color Imaging System.

6 Bibliography

The abbreviations used in this report are listed below.

[1] Data Security Kit DA-SC02 Security Target version 1.02（November.9th 2006 ） Panasonic Communications Co., Ltd.

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 （Japanese translated version）

[9] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 （Japanese translated version）

[10] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 （Japanese translated version）

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 Japanese translated version）

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] Data Security Kit DA-SC02 Evaluation Technical Report version1.3 December

10th ,2006 Japan Electronics and Information Technology Industries Association, Information Technology Security Center