CRP-C0189-01

Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2008-02-12 (ITC-8195)
Certification No.	C0189
Sponsor	Panasonic Communications Co., Ltd.
Name of TOE	Japanese Name: Data Security Kit DA-SC06 English Name: Data Security Kit DA-SC06
Version of TOE	V1.01
PP Conformance	None
Conformed Claim	EAL2
Developer	Panasonic Communications Co., Ltd.
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.
2008-10-30

Hideji Suzuki, 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 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"Data Security Kit DA-SC06" 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-SC06" (hereinafter referred to as "the TOE") conducted by 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:	Japanese Name: Data Security Kit DA-SC06 English Name: Data Security Kit DA-SC06
Version:	V1.01
Developer:	Panasonic Communications Co., Ltd.

1.2.2 Product Overview

The TOE is a software product, Data Security Kit DA-SC06 installed in the Digital 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 Imaging System DP-8032P / 8025P, DP-8032V / 8025V, DP-8032VA / 8025VA for Japan (DP-8032 / 8025 for Overseas), and provides the security functions by replacing the standard bundled software of the Digital Imaging System.

(*) All models require the installation of optional Hard Disk Unit.

1.2.3 Scope of TOE and Overview of Operation

1) Usage Environment of TOE

The TOE is a software product installed in the Digital 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. The TOE installed in the Digital Imaging System is used in an environment shown in Figure 1-1. Two Digital Imaging Systems are shown in Figure 1-1 to use tandem copy / remote copy function. The Digital Imaging System can be operated with single system when the tandem copy / remote copy function is not used.

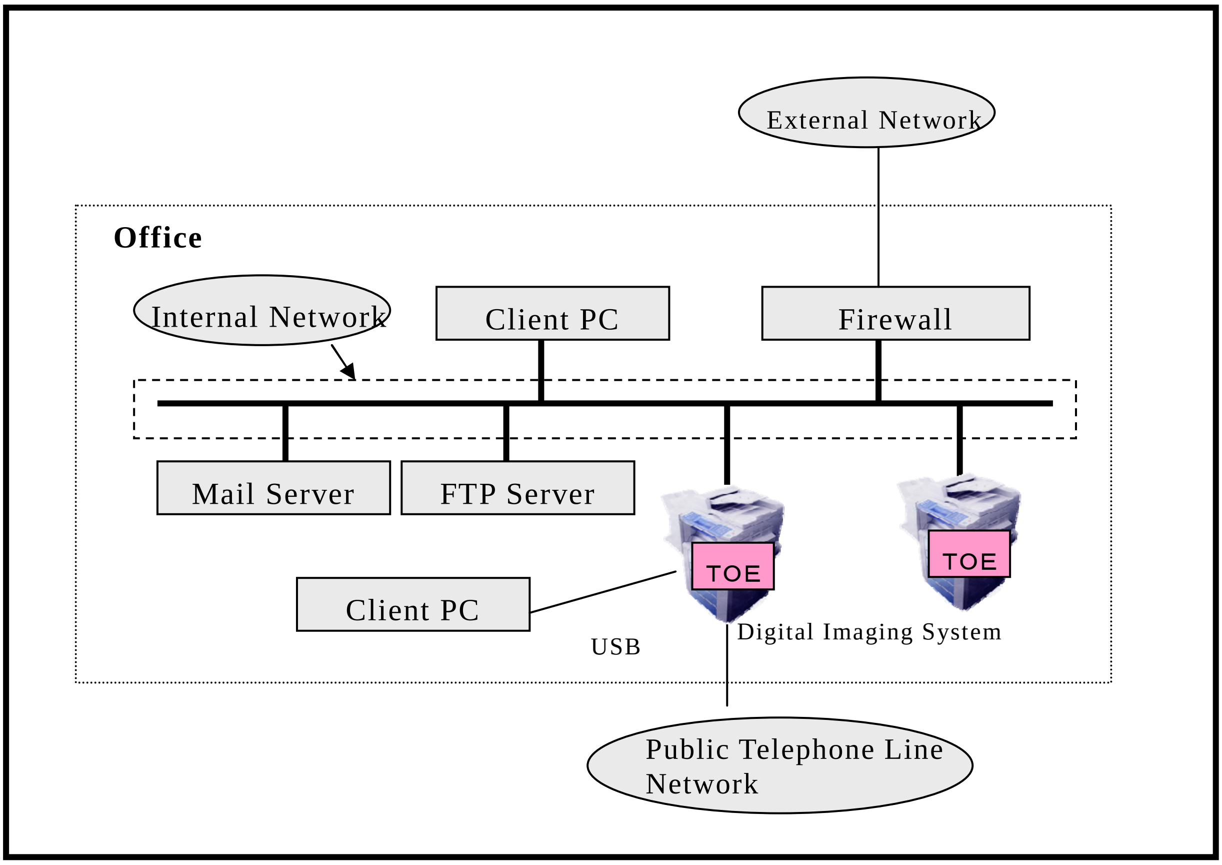

Figure 1-1 Assumed Usage Environment

2) Scope of TOE

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

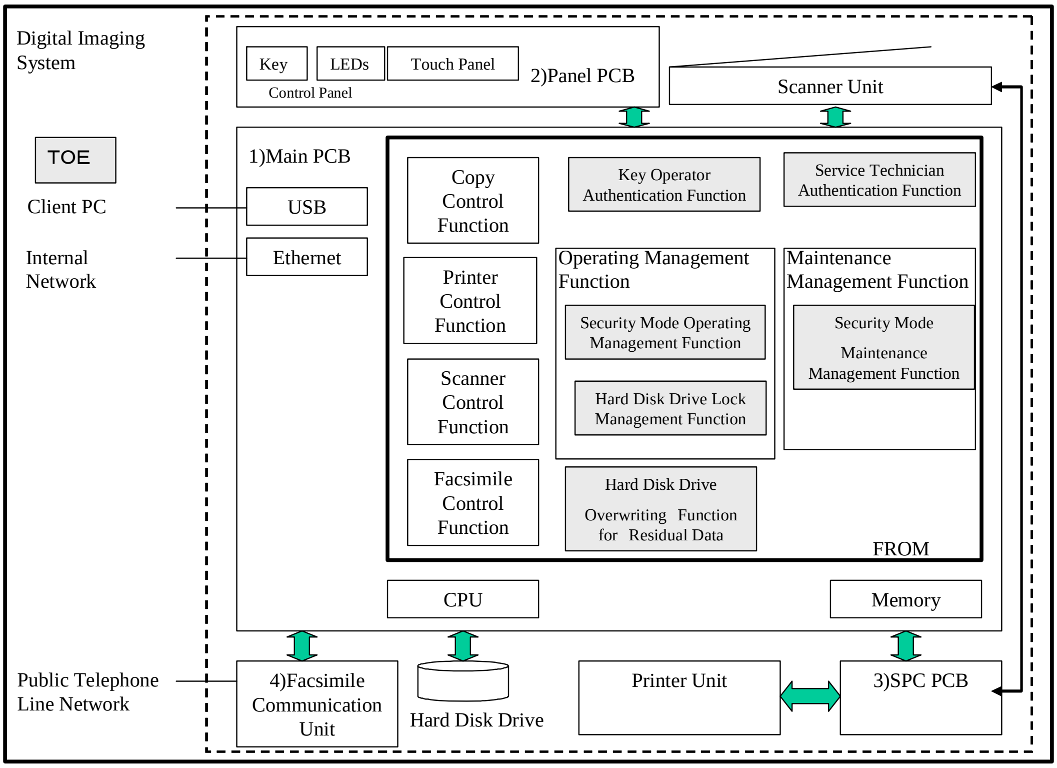
Digital Imaging System
TOE
Client PC
Internal Network
Public Telephone Line Network
Key
LEDs
Touch Panel
Control Panel
2)Panel PCB
Scanner Unit
1)Main PCB
USB
Ethernet
Copy Control Function
Printer Control Function
Scanner Control Function
Facsimile Control Function
Key Operator Authentication Function
Service Technician Authentication Function
Operating Management Function
Security Mode Operating Management Function
Hard Disk Drive Lock Management Function
Maintenance Management Function
Security Mode Maintenance Management Function
Hard Disk Drive Overwriting Function for Residual Data
FROM
CPU
Memory
4)Facsimile Communication Unit
Hard Disk Drive
Printer Unit
3)SPC PCB

Figure 1-2 Physical Configuration

Software that controls the Digital Imaging System is stored in FROM on Main PCB in Figure 1-2. The TOE is a group of software parts 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

The hard disk drive unit attached to the Digital Imaging System has a drive lock function 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. TOE provides "Hard Disk Drive Lock Management Function" to manage the password. The drive lock function of the hard disk drive is outside the TOE scope.

3) Persons Related to TOE

Following are the persons related to Digital Imaging System with TOE installed.

- General user
  General users are the ones who use the general functions of Digital Imaging System, such as copy, printer, scanner and facsimile.

- Key operator
  The machine administrator called key operator is to perform operating

management using the operating management functions offered by Digital Imaging System. Key operator is appointed by the person in charge of Digital Imaging System.

- Person in charge
  Person in charge is the one who is in charge of introducing Digital Imaging System, and appoints and manages the key operator.

- Service technician
  The service technician provides installation, maintenance and repair services, using the maintenance and management functions offered by Digital Imaging System. Service technicians belong to the company which undertakes the maintenance of Digital Imaging System.

4) Overview of Operation

The TOE is used as follows.

- General user
  When a general user uses copy function / printer function / scanner function of the Digital Imaging System, the document data is stored temporarily in the hard disk drive. This temporary document data becomes used document data when each function finishes its usage. "Hard Disk Drive Overwriting Function for Residual Data" of the TOE is executed automatically at the time of generation of the used document data, and the document data area is overwritten and erased without any awareness of the general user.

- Key operator
  The key operator operates the control panel to use "Hard Disk Drive Lock Management Function" and "Security Mode Operating Management Function" of the TOE after the identification and the authentication by "Key Operator Authentication Function" of the TOE. "Security Mode Operating Management Function" includes the function to command the execution of "Hard Disk Drive Overwriting Function for Residual Data" of the TOE.

- Service technician
  The service technician operates the control panel to use "Security Mode Maintenance Management Function" of the TOE after the identification and the authentication by "Service Technician Authentication Function" of the TOE.

1.2.4 TOE Functionality

The TOE has the security functions described below.

(1) Hard Disk Drive Overwriting Function for Residual Data

This function overwrites and erases the data area of the used document data. There are following three overwriting and erasing methods, and set by "Security Mode Operating Management Function".

- 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 function is executed at the following timing.

- When used document data is generated in the hard disk drive, after the document data is processed by copy control function, printer control function or scanner control function.
- When the key operator directs it from the control panel by "Hard disk initialization" in "Security Mode Operating Management Function".

(2) Key Operator Authentication Function

This function identifies and authorizes the key operator, by means of the input to the control panel and the entered dedicated password for key operator. Only the identified and authorized key operator can perform operations in "Hard Disk Drive Lock Management Function" and "Security Mode Operating Management Function".

(3) Hard Disk Drive Lock Management Function

This function is for the key operator to manage the hard disk drive lock. Only the identified and authorized key operator can set up and change the password for the memory inside the Digital 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

This function is the management function for key operator to conduct operations. Only the identified and authorized 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 overwriting and erasing mode of "Hard Disk Drive Overwriting Function for Residual Data". (Except "Hard Disk Initialization")
  It can set up three types of overwriting and erasing, Basic (initial setting), Medium and High.

- "Hard Disk Initialization"
  This function enables the key operator to direct "Hard Disk Drive Overwriting Function for Residual Data" to overwrite and erase all document data stored on the hard disk drive. As the ways to overwrite and erase, there are two types, Medium and High.

- "Key Operator Password"
  This function is to set up and change the key operator password.

(5) Service Technician Authentication Function

This function identifies and authenticates the service technician by the operations of service mode setting procedure from the control panel as well as the entered password. Only the identified and authorized service technician is allowed for operations in "Security Mode Maintenance Management Function".

(6) Security Mode Maintenance Management Function

This function is for service technician to carry out the management functions for maintenance tasks. Only the identified and authorized 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"
  This function is to set up and change the service technician password.

- "System Initialization"
  Under the direction from the service technician, this function initializes setup data such as "Hard Disk Drive Lock Password" in "Hard Disk Drive Lock Management Function", "Hard Disk Data Erasure Level" and "Key Operator Password" in "Security Mode Operating Management Function", "Service Technician Password" in "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 follows.

- 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 "Data Security Kit DA-SC06 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 B 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-SC06 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. 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 2008-10-15 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 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

The security functions of the TOE are as shown in "1.2.4 TOE Functionality".

1.5.5 Threat

This TOE assumes such threats 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 Organisational Security Policy

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

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.OWMETHOD	- Overwriting and erasing the used document data The data area of used document data remaining on the hard disk drive must be overwritten and erased.

1.5.7 Configuration Requirements

The TOE is used installed in the Panasonic Communications Co., Ltd. Digital Imaging System DP-8032P / 8025P, DP-8032V / 8025V, DP-8032VA / 8025VA for Japan (DP-8032 / 8025 for Overseas).

(*) In All models, the hard disk drive is not installed in the standard configuration, and requires the installation of optional Hard Disk Unit.

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.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
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 below.

(1) For Japan
- Operating Instructions Data Security Kit DA-SC06 (in Japanese) C0808-0(04)
- Installation Instructions for Service Technicians Data Security Kit DA-SC06 (in Japanese) C0808-0(03)

(2) For Overseas
- Operating Instructions Data Security Kit DA-SC06 C0808-0 (04)
- Installation Instructions for Service Technicians Data Security Kit DA-SC06 C0808-0 (03)

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 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started in February 2008 and concluded by completion the Evaluation Technical Report in October 2008. 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 directly visited the development and manufacturing sites in May 2008 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site in May 2008.

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.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

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

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is shown in the Figure 2-1 and 2-2.

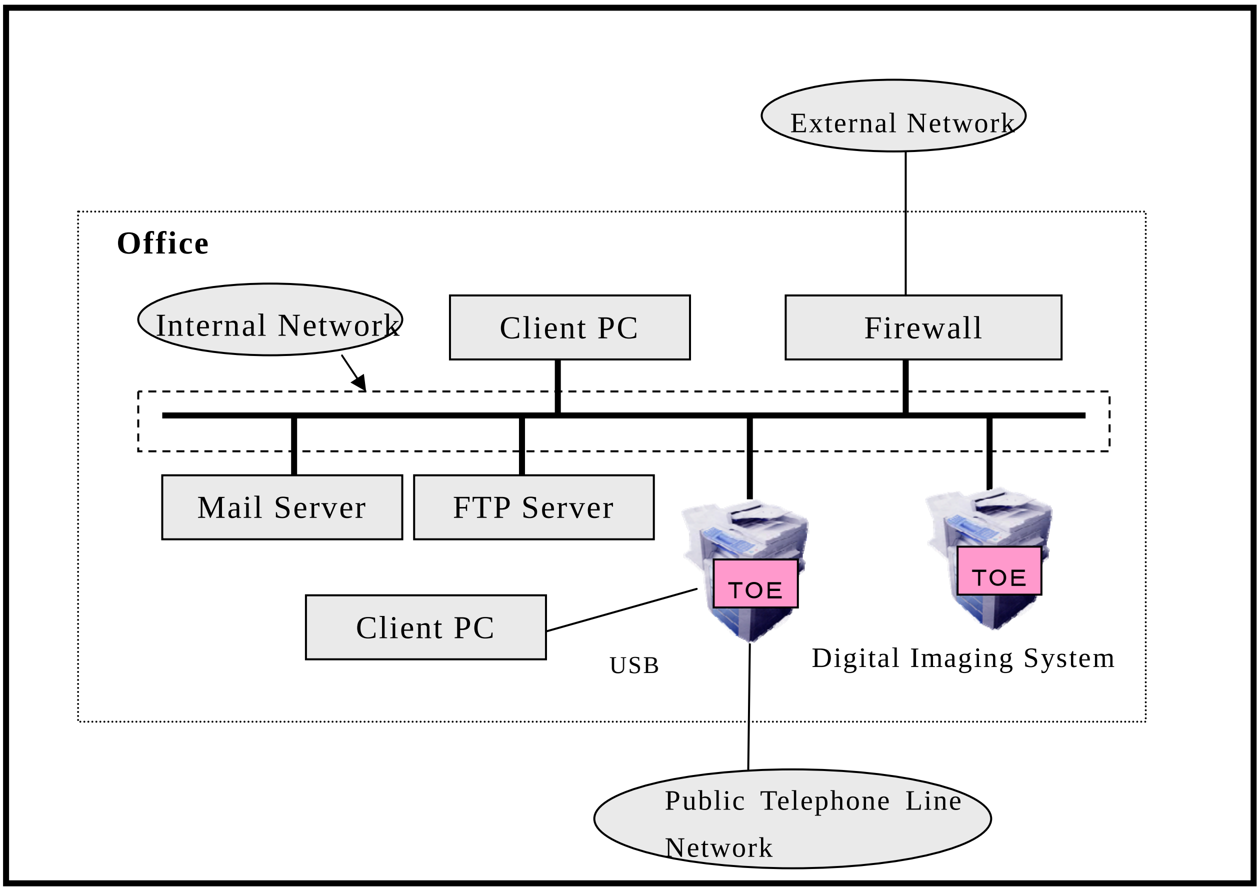

Figure 2-1 Configuration of Developer Testing

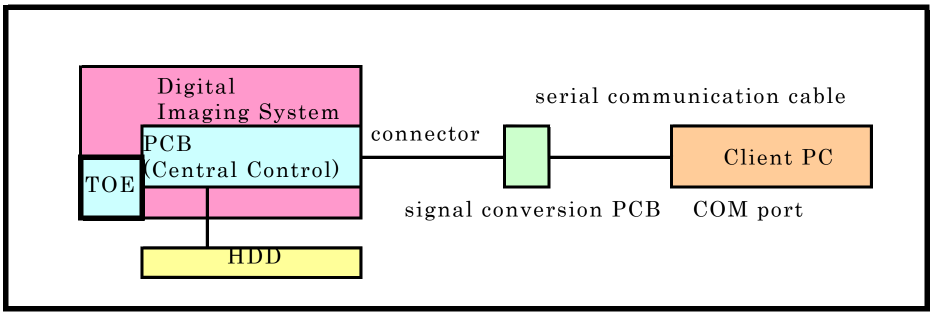

Figure 2-2 Test Configuration of testing for "Hard Disk Drive Overwriting Function for Residual Data"

2) Outlining of Developer Testing

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

a. Test configuration

Test configuration performed by the developer is shown in the Figure 2-1 and 2-2. Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

The Digital Imaging System that was used for test is DP-8032VA for Japan and DP-8032 for Overseas. Each model has an optional Hard Disk Unit DA-HD31.

The TOE supports multiple models. The difference between the models is the installable function (Facsimile Function), installation of the optional unit (double side printing unit) and print speed in the standard configuration. The evaluator confirmed that the difference has no effect on the TOE security functions, and the testing using the representative model is sufficient for multiple models.

b. Testing Approach

For the testing, following approach was used.

1. The TOE is operated from the control panel and from the client PC (internal network connection and USB connection), and the display status and processing results are confirmed.
2. To confirm the operation of "Hard Disk Drive Overwriting Function for Residual Data", the TOE is operated from the control panel and from the client PC. The result of the operation is confirmed from the log data which is output by the debugging client PC 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 performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

2.3.2 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 follows.

a. Test configuration

Test configuration performed by the evaluator is shown in the Figure 2-1 and 2-2. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

However, the Mail Server, the FTP Server and the public telephone line network are not used because the tests that utilize these functions are not executed. The Digital Imaging System which is used in testing is the same as the developer testing.

b. Testing Approach

For the testing, following approach was used.

1. The security function is stimulated by the use of the control panel, and the display and process of the security function is observed.
2. The security function is stimulated by the use of the control panel and client PC (USB connection), and observed by the use of the log data which is output from the debugging client PC as shown in Figure 2-2.
3. The possibility of an illegal intrusion is searched by the use of a client PC (internal network connection).

c. Scope of Testing Performed

Total of 92 items of testing; namely 33 items from independent testing devised by the evaluator, 4 items from penetration testing devised by the evaluator, and 55 items from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. Security function that the evaluator doubts it operates as specified.
2. Further significant security function than the other security function.
3. Security function subjected for strength of function.
4. Function used by 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.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM 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.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

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

4. Conclusion

4.1 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.

4.2 Recommendations

The reader is advised to notice the following.

The countermeasure for the threat T.RECOVER directly is the drive lock function of the hard disk drive which is one of the IT environments. The TOE provides the management function for the password of the drive lock function to support the countermeasure.

The assets of the TOE are protected by two functions. One function is the drive lock function of the hard disk drive to counter the threat. Another function is "Hard Disk Drive Overwriting Function for Residual Data" to satisfy the organisational security policy. The user of the TOE is advised to use both function properly according to the documents attached to the TOE.

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 Imaging System
Peripheral which integrates functions such as copy, printer, scanner and facsimile into one machine. In this report, the term "Digital Imaging System" is used to generically refer to the models DP-8032P / 8025P, DP-8032V / 8025V, DP-8032VA / 8025VA (for Japan) and DP-8032 / 8025 (for Overseas) manufactured by Panasonic Communications Co., Ltd.

Internal Network
The LAN used in the organization where the Digital Imaging System is introduced.

External Network
The networks other than the Internal Network, such as the Internet.

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 Imaging System.

Key Operator
One who manages Digital Imaging System.

Service Technician
A technician who belongs to the service provider company to provide installation, maintenance and repair services of Digital Imaging System.

Service Mode
A set of maintenance functions that the service technician uses for installation, maintenance and repair services of Digital Imaging System.

Service Mode Setting Procedure
The setting procedure that a service technician uses to switch the mode to Service Mode.

Control Panel
Operation Panel with keys, LEDs and a touch panel display required for operating the functions of Digital Imaging System.

SPC PCB
PCB to control the mechanical function of scanner and printer unit.

FROM
Nonvolatile memory allowing electrical block erasure and reprogramming of arbitrary portion.(Flush Read Only Memory)

Document Data
Collective name for all digitized image data handled inside Digital Imaging System when copy, print, scanner or facsimile functions are used in Digital Imaging System.

- Image data captured from scanner unit.
- Image data that can be printed on printer unit.
- Image data which has been received from the FAX Communication Unit and transformed 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 Imaging System and had already been used.

Tandem Copy
A printing function whereby half of the specified number of copies for the data captured from the scanner are printed by the Digital Imaging System that captured the data, and the other half are printed on the other Digital Imaging System that is connected in the Internal Network.

Remote Copy
A printing function whereby all the data captured from the scanner are printed on some other Digital Imaging System.

6. Bibliography

[1] Data Security Kit DA-SC06 Security Target Version 1.01 (May 21, 2008) Panasonic Communications Co., Ltd.

[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 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[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 (Translation Version 1.0 December 2005)

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

[17] Data Security Kit DA-SC06 Evaluation Technical Report Version 1.4, October 15, 2008, Information Technology Security Center