Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2008-03-07 (ITC-8206)			
Certification No.	C0239			
Sponsor	RICOH COMPANY, LTD.			
Name of TOE	Japan: Ricoh imagio MP 4000/5000 series Overseas: Ricoh Aficio MP 4000/5000 series Savin 9040/9050 series Lanier MP 4000/5000 series Gestetner MP 4000/5000 series Nashuatec MP 4000/5000 series Rex-Rotary MP 4000/5000 series Infotec MP 4000/5000 series			
Version of TOE	Following software and hardware			
	System/Copy:	1.09	Web Support:	1.57
	Network Support:	7.23	Web Uapl:	1.13.1
	Scanner:	01.23	Network Doc Box:	1.09.3C
	Printer:	1.09	Ic Key:	1100
	Fax:	03.00.00	Ic Hdd:	01
PP Conformance	None			
Conformed Claim	EAL3			
Developer	RICOH COMPANY, 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.
2009-11-13

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

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

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

Evaluation Result: Pass

"Japan:Ricoh imagio MP 4000/5000 series, Overseas:Ricoh Aficio MP 4000/5000 series, Savin 9040/9050 series, Lanier MP 4000/5000 series, Gestetner MP 4000/5000 series, Nashuatec MP 4000/5000 series, Rex-Rotary MP 4000/5000 series, Infotec MP 4000/5000 series Version System/Copy:1.09, Network Support:7.23, Scanner:01.23, Printer:1.09, Fax:03.00.00, Web Support:1.57, Web Uapl:1.13.1, Network Doc Box:1.09.3C, Ic Key:1100, Ic Hdd:01" 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 "Japan:Ricoh imagio MP 4000/5000 series, Overseas:Ricoh Aficio MP 4000/5000 series, Savin 9040/9050 series, Lanier MP 4000/5000 series, Gestetner MP 4000/5000 series, Nashuatec MP 4000/5000 series, Rex-Rotary MP 4000/5000 series, Infotec MP 4000/5000 series Version System/Copy:1.09, Network Support:7.23, Scanner:01.23, Printer:1.09, Fax:03.00.00, Web Support:1.57, Web Uapl:1.13.1, Network Doc Box:1.09.3C, Ic Key:1100, Ic Hdd:01" (hereinafter referred to as "the TOE") conducted by Information Technology Security Center Evaluation Department (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, RICOH COMPANY, 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:	Japan:	Ricoh imagio MP 4000/5000 series
	Overseas:	Ricoh Aficio MP 4000/5000 series
		Savin 9040/9050 series
		Lanier MP 4000/5000 series
		Gestetner MP 4000/5000 series
		Nashuatec MP 4000/5000 series
		Rex-Rotary MP 4000/5000 series
		Infotec MP 4000/5000 series

Version:	System/Copy:	1.09
	Network Support:	7.23
	Scanner:	01.23
	Printer:	1.09
	Fax:	03.00.00
	Web Support:	1.57
	Web Uapl:	1.13.1
	Network Doc Box:	1.09.3C
	Ic Key:	1100
	Ic Hdd:	01

Developer: RICOH COMPANY, LTD.

The "~ series" in the product names is the generic name for multiple products. The following are the specific product/model names for each "~ series". Some of these products have the Fax Function, and some of these do not. When an "F" is suffixed to the product name, it indicates that the product has the Fax Function, and when an "F" is not suffixed, the product does not have the Fax Function.

Japan:
Ricoh imagio MP 4000SP
Ricoh imagio MP 4000SPF
Ricoh imagio MP 5000SP
Ricoh imagio MP 5000SPF

Overseas:
Ricoh Aficio MP 4000SP
Ricoh Aficio MP 4000SPF
Ricoh Aficio MP 5000SP
Ricoh Aficio MP 5000SPF
Savin 9040SP
Savin 9040SPF
Savin 9050SP
Savin 9050SPF
Lanier LD040SP
Lanier LD040SPF
Lanier LD050SP
Lanier LD050SPF
Lanier MP 4000SP
Lanier MP 4000SPF
Lanier MP 5000SP
Lanier MP 5000SPF
Gestetner MP 4000SP
Gestetner MP 4000SPF
Gestetner MP 5000SP
Gestetner MP 5000SPF
Nashuatec MP 4000SP
Nashuatec MP 4000SPF
Nashuatec MP 5000SP
Nashuatec MP 5000SPF
Rex-Rotary MP 4000SP
Rex-Rotary MP 4000SPF
Rex-Rotary MP 5000SP
Rex-Rotary MP 5000SPF
Infotec MP 4000SP
Infotec MP 4000SPF
Infotec MP 5000SP
Infotec MP 5000SPF

1.2.2 Product Overview

The product of this certification is a digital MFP (hereafter called MFP), made by Ricoh COMPANY, Ltd., that provides the functions of copier, scanner, printer and fax (optional). Those functions are for digitising the paper document files, managing the document files and printing the document files.
This product is an I/O device that incorporates the functionality of copier, scanner, fax and printer. In general, this product is connected to an office LAN and is used to input, store and output the Document Data. This product protects Document Data from the unintentional disclosure and operation when stored internally, and prevents Document Data from leakage when sent and received between the MFP and a client.

1.2.3 Scope of TOE and Overview of Operation

1.2.3.1 Scope of TOE

The TOE is the product of this certification and it is configured as it satisfies the following. If the configuration of the product does not satisfy some of the following, it means that the product is not the TOE. Once its Service Mode Lock is cancelled and its Maintenance Function is used, it leaves the possibility that the product is no longer the TOE (since there might be a possibility that the Maintenance Function changes the product itself).

- Do not set Service Mode Lock to "Off".
- Use IPv4 protocol (do not use IPv6 protocol).
- Do not use IP-Fax and Internet Fax Function.
- Use Basic Authentication for Identification and Authentication Function (do not use the authentication except for Basic Authentication).

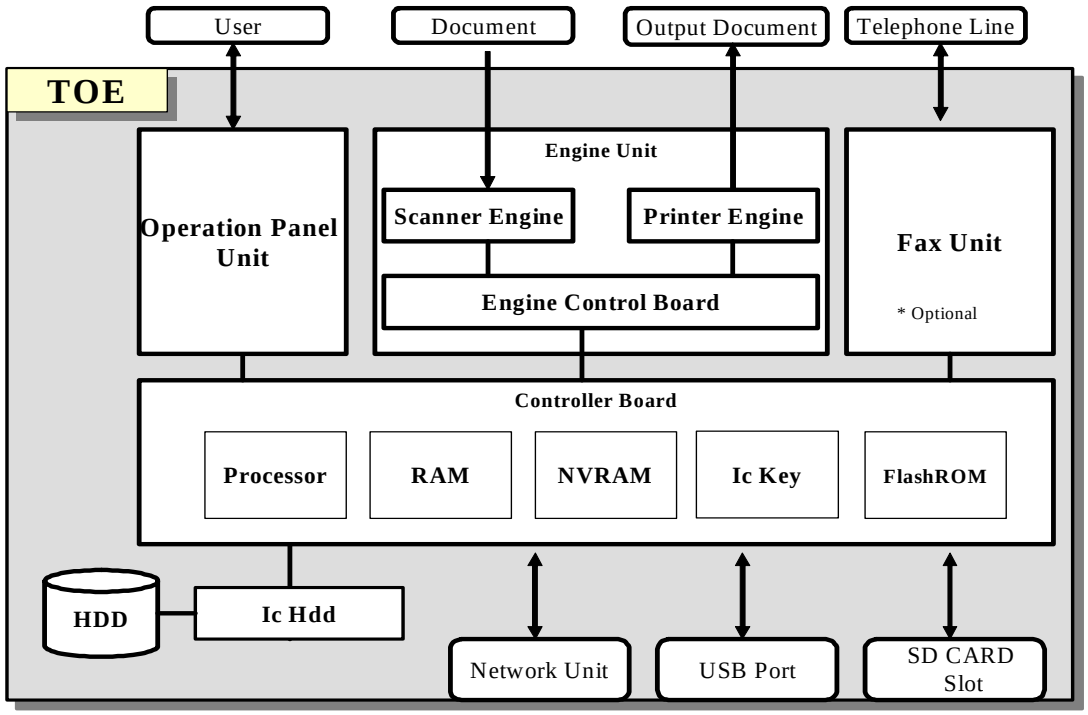

Fig. 1-1 TOE Configuration

Figure 1-1 shows the physical configuration items of the TOE. The brief description of each item is as follows:

- Operation Panel Unit (hereafter called Operation Panel)
  The Operation Panel is an interface device that is equipped on the TOE and is used by TOE users for TOE operation. It is configured with key switches, LED indicators, touch screen LCD, and the Operation Panel Control Board.

- Engine Unit
  The Engine Unit consists of a Scanner Engine, Printer Engine and Engine Control Board. The Scanner Engine is an input device to read the paper documents. The Printer Engine is the output device to print and output the paper documents.

- Fax Unit (Optional)
  The Fax Unit is a device that has a modem function to send and receive fax data when connected to a telephone line.

- Controller Board
  The Controller Board contains Processors, RAM, NVRAM, Ic Key and FlashROM. The brief description of each item is as follows:
  [Processor] A processor that carries out the processing such as arithmetic processing according to software.
  [RAM] A volatile memory that is used for an image processing memory.
  [NVRAM] A non-volatile memory in which MFP Control Data to configure the MFP operation is stored.
  [Ic Key] A security chip that provides the functions of random number generation and encryption key generation, and is used to detect the tampering of MFP Control Software.
  [FlashROM] A memory in which MFP Control Software is installed. MFP Control Software is installed in the TOE and has the elements that identify the TOE such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box.

- Ic Hdd
  Ic Hdd is a security chip that provides the functions to encrypt the information to be stored on HDD and decrypt the information to be read from HDD.

- HDD
  HDD is a hard disk drive in which image data and user information for identification and authentication are stored. The area where image data are stored as Document Data is called D-BOX.

- Network Unit
  The Network Unit is an interface board for Ethernet (100BASE-TX/10BASE-T) networks.

- USB Port
  The USB Port is used to connect a client PC to the TOE, and is used for printing or faxing from that client PC.

- SD CARD Slot
  SD CARD Slot is an interface that is used to enable the Stored Data Protection Function when installing the TOE, and is used for the maintenance work. However, since the maintenance work is not assumed for this certification, this is used only when installing the TOE.

1.2.3.2 Operation Overview of TOE

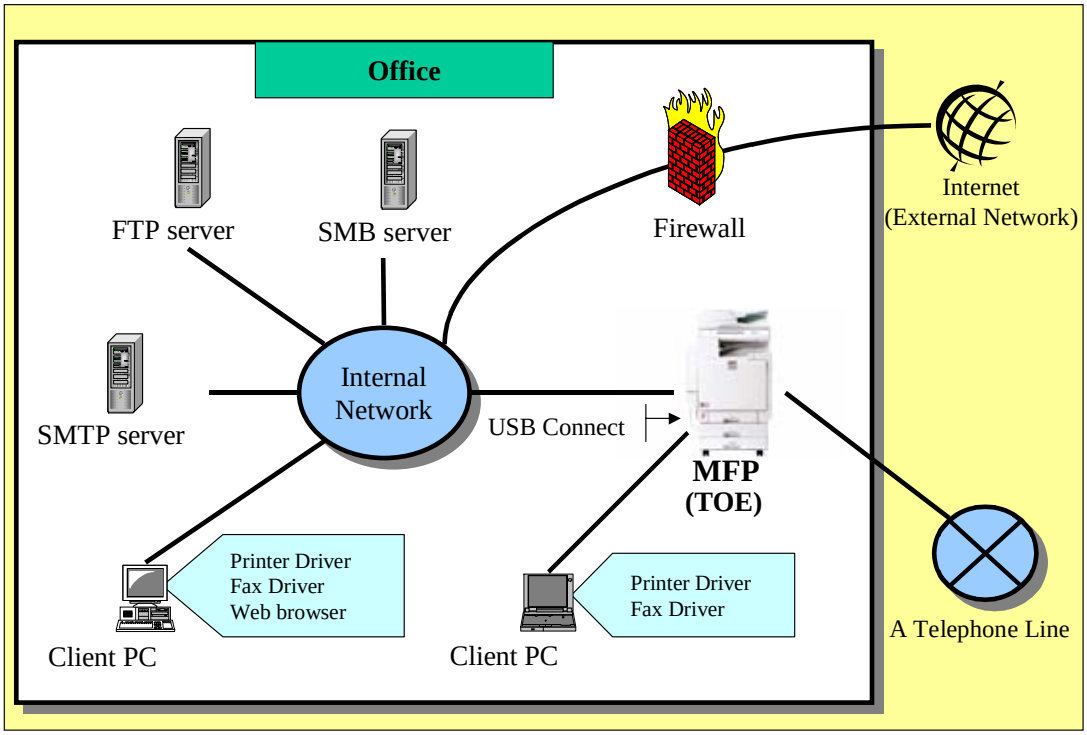

Fig. 1-2 Example of Environment for usage of TOE

The TOE is used in the environment as shown in the example in Figure 1-2, and its main purpose is to input, output, and store image data. The following are the methods to input and output image data. The TOE can simply output the data that were put into the TOE, and also can store the data.

- How to input image data to the TOE
  > Scan the original optically using Scanner Engine.
  > Receive the data from the client PC via Network Unit or USB Port.
  > Receive the data from a telephone line via Fax Unit.

- How to output image data from the TOE
  > Print image data using Printer Engine.
  > Transfer image data from Network Unit.
  > Send image data attached to e-mail from Network Unit.
  > Send image data either to an FTP Server using FTP protocol, or to an SMB Server using SMB protocol.
  > Fax image data from Fax Unit via a telephone line.

1.2.4 TOE Functionality

The TOE has Copy Function, Printer Function, Fax Function, Scanner Function, Document Server Function, Management Function and Web Service Function. The following are the descriptions of each function.

1.2.4.1 Copy Function

The Copy Function is used to scan the original as image data using Scanner Engine and print out the image data in accordance with the specified Print Settings using

Printer Engine.
The scanned image data can be stored in D-BOX as Document Data (except for the Scanner Function).

1.2.4.2 Printer Function

The Printer Function is used to receive the print data from a client PC via Network Unit or USB Port sent from a client PC and to print out the data using Direct Print Function or Store and Print Function.
Direct Print Function simply prints out the received print data using Printer Engine.
Store and Print Function stores (does not print out immediately) the print data in D-BOX as Document Data (except for the Scanner Function). The actual print out is performed using "1.2.4.8 Document Server Function (Management)", which is described later.

1.2.4.3 Fax Function (Reception)

The Fax Function (Reception) is used to receive fax data from Fax Unit and either print or store the fax data.
When printing the fax data, it simply prints out the received fax data using Printer Engine.
When storing the fax data, it converts the received fax data into the Fax Reception Data and then stores it in D-BOX (does not print out immediately). The actual print out is performed using "1.2.4.8 Document Server Function (Management)", which is described later.

*Note: The received fax data by the TOE is not intended for the target of this certification. (Refer to "4.2.1 Notes for Protected Assets")

1.2.4.4 Fax Function (Immediate Transmission/Memory Transmission)

The Fax Function (Immediate Transmission/Memory Transmission) is used to scan the original as image data using Scanner Engine and send the image data from Fax Unit using Immediate Transmission or Memory Transmission.
Immediate Transmission sends the generated image data to the destination fax sequentially while scanning the original, after connecting to the destination fax.
Memory Transmission scans the original before connecting to the destination fax. After scanning the original, it connects to the destination fax and sends the image data.

1.2.4.5 Fax Function (Stored Documents Fax Transmission)

The Fax Function (Stored Documents Fax Transmission) is used to send "the specified Document Data stored in D-BOX" from Fax Unit.

1.2.4.6 Fax Function (Fax Transmission from PC)

The Fax Function (Fax Transmission from PC) is used to receive print data from the client PC via Network Unit or USB Port, and send the print data from Fax Unit.

1.2.4.7 Document Server Function (Scan)

The Document Server Function (Scan) is used to scan the original using Scanner Engine as image data, and store the scanned data in D-BOX as Document Data (except for the Scanner Function).

1.2.4.8 Document Server Function (Management)

The Document Server Function (Management) is used to carry out the specified process (described below) either to the "stored Document Data in D-BOX (except for the Scanner Function) or the specified Fax Reception Data".
- Print (Print using Printer Engine)
- Deletion (Delete the stored data in D-BOX)
- Downloading (Transfer the data to the client PC via Network Unit)

*Note: The Document Data generated using the "Scanner Function (Scan)" cannot be managed using "Document Server Function (Management)", but can be managed using "Scanner Function (Management)".

1.2.4.9 Scanner Function (Scan)

The Scanner Function (Scan) is used to scan the original as image data using Scanner Engine, and then send it by e-mail, deliver to folder or store.
For sending by e-mail, this function sends the image data attached to e-mail to the specified e-mail address from Network Unit.
For Deliver to Folder, this function transfers the image data to the specified folder from Network Unit using the FTP protocol or SMB protocol.
For storing, this function stores image data in D-BOX as Document Data (for Scanner Function use only).

*Note: The management of the Document Data generated using this function differs from the management of the Document Data generated using other functions. The Document Data generated using this function is managed using the "Scanner Function (Management)", and the Document Data generated using other functions are managed using the "Document Server Function (Management)".

1.2.4.10 Scanner Function (Management)

The Scanner Function (Management) is used to carry out the specified process (described as follows) to the "specified Document Data (for Scanner Function use only) in D-BOX".
- Sending (Send by e-mail or Deliver to Folder of the "Scanner Function (Scan)"
- Deletion (Delete Document Data in D-BOX)
- Downloading (Transfer Document Data to a client PC via Network Unit)

*Note: This function only manages the Document Data that is stored using the "Scanner Function (Scan)". The "Document Server Function (Management)" manages other Document Data that is stored using other functions.

1.2.4.11 Management Function

The Management Function is used to configure the following settings: the TOE machine settings, settings for network connection, settings for authorized user information and settings for the information to restrict the use of the Document Data. A user's ability to manage this information is determined in accordance with that user's authorized role (General User, Administrators, or Supervisor).

1.2.4.12 Web Service Function

The Web Service Function is used to operate the TOE remotely from the web browser of a client PC by authorized TOE users (General Users, Administrators or Supervisor).

Although the Web Service Function is available for the functions described above in "1.2.4.1 Copy Function" - "1.2.4.11 Management Function", there are some functions that are not available using this Web Service Function.

1.3 Conduct of Evaluation

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

Scope of the evaluation is as follow.

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

More specific, the evaluation facility examined "imagio MP 4000/5000 series, Aficio MP 4000/5000 series Security Target" as the basic 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 "RICOH COMPANY, LTD. imagio MP 4000/5000 series, Aficio MP 4000/5000 series 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 2009-10 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 EAL3 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
This TOE is assumed to be placed on the premises for organizations such as offices in which the risk of its assumed threats is low, and to be operated with it connected to the Internal Networks of the organization. Therefore SOF-basic is selected.

1.5.4 Security Functions

The TOE counters the threats with its functions as described below, and satisfies the organizational security policy.

1.5.4.1 Countermeasure to T.ILLEGAL_USE, T.UNAUTH_ACCESS, T.ABUSE_SEC_MNG

These threats are countered with a sequence of countermeasure, identification/authentication and the access control.
For users (operators) who attempt to use the TOE, the TOE requires them to enter their user ID and the authentication information (password). Then it verifies the integrity of the entered user ID and authentication information.
The TOE has the following functions to counter the impersonation when entering the user ID and authentication information.

- According to the Lockout Policy, if the number of consecutive unsuccessful attempts to identify and authenticate a particular user ID meets the Number of Attempts before Lockout, the TOE lockouts this user ID (prevents this user ID from using the TOE).
- When allowing users to set or change their passwords, the TOE allows them to register only the passwords as the authentication information that satisfy the conditions of Minimum Password Length and Complexity Setting for Password.

After the TOE verifies the user ID and authentication information, it selects either (1) or (2).

(1) If the user ID and authentication information cannot be verified, the TOE does not allow the operator to use the TOE functions.

Since the users who are not allowed to use the TOE do not have the valid user ID and authentication information, (1) indicates the unauthorized TOE users cannot use the TOE functions. This is the countermeasure to T.ILLEGAL_USE.

(2) If the user ID and authentication information are verified, the TOE identifies the operator by the user ID, and then identifies the user's User Role by the user ID. After the TOE identifies these, the TOE allows the user to use the TOE functions. The following are the roles that are identified by the TOE.
- General User
- Administrator
- Supervisor

For Administrators, the user can also be identified by the any of the following roles. The following roles are not exclusive. More than one role can be assigned to one Administrator user ID.
- User Administration
- Machine Administration

- Network Administration
- File Administration

After the TOE carries out (2), the operator gives the instruction to the TOE of what he/she wants to operate. The instruction may include the "operation on Document Data" or "use of the Management Function". Either (3) or (4) is processed, depending on which instruction you select.

(3) For the instruction including the "operation on Document Data", the TOE determines if the instructed operation is authorized for the user or not, based on the user ID and operator's role, identified in (2). The TOE follows the instruction and performs the operation only if it is authorized. The TOE determines the instructed operation based on the following criteria.
- When the operator's role is the General User
  Each Document Data has the information (Document Data ACL) that determines who to allow the operation and what kind of operation to allow (there are some phases, such as to allow only to read, and also to change Print Setting, and also to delete, and also to operate on the Document Data ACL). The TOE determines if the instructed operation is authorized or not, based on the user ID that is identified in (2) and the Document Data ACL.
- When the operator's role is not the General User
  If the operator's role identified in (2) is the Administrator, and has the role of File Administrator, it is allowed for the operator to delete the arbitrary data. If not, no operations on Document Data are allowed.

Since (3) limits the operation on Document Data by the authorized TOE user according to the access control (if the user is the General User who are authorized with the Document Data ACL or not, OR if the user is the authorized Administrator or not), the TOE counters T.UNAUTH_ACCESS.

(4) For the instruction including "use of the Management Function", the TOE applies to the "Security Management Function", based on the user ID and the operator's role identified in (2).
The Security Management Function is the operations on the following data the TOE has.
- Document Data ACL
- Registration Information about Users
- Lockout Policy (Number of Attempts before Lockout, whether or not to release Lockout base on the elapsed time, Lockout Release Timer)
- System date, time
- HDD Encryption Key
- Audit Log
- Service Mode Lock Function
- Password Policy (Minimum Password Length, and the minimum of combination of character types for password)

The TOE allows the operations on these data provided that the operator's role is the Administrator or Supervisor*1. However, the TOE also allows General Users to perform the operations on Document Data provided that the operator can leaves the security maintained as described below.
- It is allowed for the document file owners and the General Users, who are set for each Document Data, to perform the operations on Document Data ACL (except

*1 Some operations may not be allowed for the Administrators or Supervisor. There is a rule that determines which operation is allowed for the detailed Administrator (User Administration, Machine Administration, Network Administration and File Administration) and Supervisor. The detail of this rule is beyond the scope of this document.

for changing the document file owners).
- It is allowed for the General Users to change their own "authentication information", "Document Data Default ACL (except for field of the document file owner)" and "S/MIME User Information".

Since (4) limits the use of the Security Management Function to the "authorized person to use the Security Management Function", the TOE counters T.ABUSE_SEC_MNG.

1.5.4.2 Countermeasure to T.SALVAGE

The TOE protects Document Data from leakage by making it difficult to understand unless the Document Data is accessed in the normal way (using the function described in "1.2.4 TOE Function" from the Operation Panel or Client PC) to counter T.SALVAGE.
(Stored Data Protection Function)
This function is realized by encrypting the data just before writing it on HDD with the following cryptographic algorithm and cryptographic key size, and by decrypting the data just after reading it from HDD.
- Cryptographic algorithm: AES
- Key size: 256 bits

1.5.4.3 Countermeasure to T.TRANSIT

The TOE protects the Document Data and image data that are sent or received by the TOE via the Internal Networks from interceptions and tampering to counter T.TRANSIT.
The mechanism, SSL, IPSec or S/MIME, varies depending on the type of data to be protected. Although S/MIME is realized by the TOE functions, the communication path for SSL is established by the cooperation of the TOE and client PCs, and the communication path for IPSec is established by the cooperation of TOE and either SMB Server or FTP Server.
The protected scope depends on the mechanism used for the data protection. The following Tables, 1-1(1)-(3), show the specific scopes.

Table 1-1 (1) Specific data, mechanism and scope

Target data
Print data that are sent to Network Unit from client PC via Internal Networks using the "Printer Function" (except for via USB Ports)
Protection mechanism and protected scope
The Internal Network between client PC and Network Unit is protected by SSL mechanism

Table 1-1 (2) Specific data, mechanism and scope

Target data
Print data that are sent to Network Unit from client PC via Internal Networks using the "Fax Function (Fax Transmission from PC)" (except for via USB Ports)
Protection mechanism and protected scope
The Internal Networks between client PC and Network Unit is protected by SSL mechanism

Table 1-1 (3) Specific data, mechanism and scope

Target data
Document Data that are output from Network Unit using the "Scanner Function (Scan)" or "Scanner Function (Management)"
Protection mechanism and protected scope
When delivering to folders: The Internal Networks between Network Unit and the "SMB Server or FTP Server of the specified folders" is protected by IPSec mechanism. When sending to an e-mail address: The networks (including the Internal Networks) between Network Unit and the "e-mail client of the destination address" are protected by S/MIME mechanism. When downloading: The Internal Networks between Network Unit and client PC is protected by SSL mechanism.

1.5.4.4 Countermeasure to T.FAX_LINE

The TOE does not have the active mechanism to counter T.FAX_LINE.
The TOE counters T.FAX_LINE by not performing any operations via a telephone line except for sending and receiving faxes.

1.5.4.5 Realization of P.SOFTWARE

The TOE has the function that checks the executable code of MFP Control Software, which is installed in FlashROM, is in the same condition as the ones that are provided by RICOH in order to realize P.SOFTWARE.
This function is realized by checking the electronic signature added to the executable code.
Along with this function and checking of the version for each element that the TOE outputs, the "correct version for the software is provided by RICOH with the regular method".
Although it is not possible to specifically assume the threats to the executable code of MFP Control Software by the description in the ST, it is defined in Organizational Security Policy in order to specify the consumers that it is possible to check the integrity of MFP Control Software.

1.5.4.6 Support for Other Security Functions

The TOE has the Audit Function that is used to detect the security invasion, and this function does not directly counter to the threats.
This function records the audit logs when the events that are used to detect the security invasion occur.

1.5.5 Threat

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

Table 1-2 Assumed Threats

Identifier	Threat
T.ILLEGAL_USE	Attackers may read or delete the Document Data by gaining unauthorized access to the TOE from the TOE external interfaces (Operation Panel, Network Interface, USB Interface or SD CARD interface).
T.UNAUTH_ACCESS	Authorized TOE users may go beyond the bounds of the authorized usage and access to Document Data from the TOE external interfaces (Operation Panel, Network Interface or USB Interface) that are provided to the authorized TOE users.
T.ABUSE_SEC_MNG	Persons who are not authorized to use Security Management Function may abuse the Security Management Function.
T.SALVAGE	Attackers may take HDD out of the TOE and disclose Document Data.
T.TRANSIT	Attackers may illegally obtain, leak, or tamper Document Data and Print Data that are sent or received by the TOE via the Internal Networks.
T.FAX_LINE	Attackers may gain unauthorized access to the TOE from telephone lines.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-3.

Table 1-3 Organisational Security Policy

Identifier	Organisational Security Policy
P.SOFTWARE	Measures are provided for verifying the integrity of MFP Control Software, which is installed in FlashROM in the TOE. *Note: The "integrity" means that the software is provided by RICOH with the regular method and is the correct version.

1.5.7 Configuration Requirements

The TOE is connected to the following external environment as Figure 1-2 shows. The entire following external environment is not required but it depends on how to use the TOE.

- Client PC connected to the TOE via a USB Port
- Client PC connected to the TOE via Ethernet
- SMTP Server connected to the TOE via Ethernet
- FTP Server connected to the TOE via Ethernet
  (An FTP Server has to support the IPSec communication)

- SMB Server connected to the TOE via Ethernet
  (An SMB Server has to support the IPSec communication)
- Public telephone line or equivalent line

The following drivers or later version of these drivers are required when using the TOE from the client PC with drivers.
- RPCS Driver V7.68 for domestic machines
- RPCS Driver V7.66 for overseas machines
- PC Fax Driver V1.59 for domestic machines
- LAN Fax Driver V1.60 for overseas machines

Internet Explorer 6.0 or later is required for the "client PC connected to the TOE via Ethernet" when using the TOE from the browser.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-4.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 1-4 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Administrators will have adequate knowledge to operate the TOE securely in the roles assigned to them, and guide General Users operate the TOE securely. Additionally, Administrators will not carry out any malicious acts using Administrator permissions. *Note: The "adequate knowledge to operate the TOE securely" includes the following: - Do not use the following function. > Back up/Restore Address Book - Use the TOE with the following settings maintained > Set Service Mode Lock Function to Off > Use the IPv4 protocol (Do not use the IPV6 protocol) > Do not use IP-Fax and Internet Fax > Use Basic Authentication for Identification and Authentication Function (Do not use the authentications other than Basic Authentication)
A.SUPERVISOR	The Supervisor will have adequate knowledge to operate the TOE securely in the role assigned to him/her, and will not carry out any malicious acts using Supervisor permissions.
A.NETWORK	The Internal Networks will be protected from the External Networks when the TOE-connected networks are connected to the External Networks such as the Internet.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

For Japan (Japanese version)

- Printed documents

  > imagio MP 4000/5000 series Operating Instructions <Security Reference>
  (D012-7950)

  > Notes for Security Functions
  (D011-7750A)

  > Notes for Users Back Up/Restore Address Book
  (D015-7103)

  > Notes for Administrators: Using this Machine in a CC-Certified Environment
  (D011-7781)

  > imagio MP 4000/5000 series Operating Instructions <About This Machine>
  (D012-7750)

  > imagio MP 4000/5000 series Operating Instructions <Troubleshooting>
  (D012-7800)

  > imagio MP 4000/5000 series supplied Operation Instructions
  (D012-7501)

  > imagio MP 4000/5000 series Quick Guide
  (D012-7658)

- Documents in CD-ROM

  > Operating Instructions, Drivers&Utilities imagio MP 5000/4000
  (D0097500A)

For North America (English version)

- Printed documents

  > Notes for Users Back Up/Restore Address Book
  (D015-7108, D015-7105(for GSA))

  > Notes for Administrators: Using this Machine in a CC-Certified Environment
  (D011-7782, D011-7784(for GSA))

  > 9040 / 9040b / 9050 / 9050b
  MP 4000 / MP 4000B / MP 5000 / MP 5000B
  LD040 / LD040B / LD050 / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  Operating Instructions About This Machine
  (D012-7753, D012-7757 (for GSA))

  > 9040 / 9040b / 9050 / 9050b
  MP 4000 / MP 4000B / MP 5000 / MP 5000B
  LD040 / LD040B / LD050 / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  Operating Instructions Troubleshooting
  (D012-7803, D012-7807 (for GSA))

- Documents in CD-ROM

  > Manuals 9040 / 9040b / 9050 / 9050b
  MP 4000 / 5000 / 4000B / 5000B
  LD040 / LD050 / LD040B / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  (D009-7502A)

  > Manuals for Administrators Security Reference
  9040 / 9040b / 9050 / 9050b
  MP 4000 / 5000 / 4000B / 5000B
  LD040 / LD050 / LD040B / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  (D009-7504A)

  > Manuals for Administrators Security Reference Supplement
  9040 / 9040b / 9050 / 9050b
  MP 4000 / 5000 / 4000B / 5000B
  LD040 / LD050 / LD040B / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  (D011-7790A)

For Europe (English version)

- Printed documents

  > Notes for Users Back Up/Restore Address Book
  (D015-7109)

  > Notes for Administrators: Using this Machine in a CC-Certified Environment
  (D011-7782, D011-7784(for GSA))

- Documents in CD-ROM

  > Manuals General Setting Manuals
  MP 4000 / 5000 / 4000B / 5000B
  Aficio MP 4000 / 5000 / 4000B / 5000B
  (D009-7510)

  > Manuals Functions and Network Manuals
  MP 4000 / 5000 / 4000B / 5000B
  Aficio MP 4000 / 5000 / 4000B / 5000B
  (D009-7514A)

  > Manuals for Administrators Security Reference
  MP 4000 / 5000 / 4000B / 5000B
  Aficio MP 4000 / 5000 / 4000B / 5000B
  (D009-7512A)

  > Manuals for Administrators Security Reference Supplement
  9040 / 9040b / 9050 / 9050b
  MP 4000 / 5000 / 4000B / 5000B
  LD040 / LD050 / LD040B / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  (D011-7790A)

For Asia (English version)

- Printed documents

  > Notes for Users Back Up/Restore Address Book
  (D015-7107)

  > Notes for Administrators: Using this Machine in a CC-Certified Environment
  (D011-7782, D011-7784 for GSA))

  > 9040 / 9040b / 9050 / 9050b
  MP 4000 / MP 4000B / MP 5000 / MP 5000B
  LD040 / LD040B / LD050 / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  Operating Instructions About This Machine
  (D012-7755)

  > 9040 / 9040b / 9050 / 9050b
  MP 4000 / MP 4000B / MP 5000 / MP 5000B
  LD040 / LD040B / LD050 / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  Operating Instructions Troubleshooting
  (D012-7805)

- Documents in CD-ROM

  > Manuals
  MP 4000 / 5000 / 4000B / 5000B
  Aficio MP 4000 / 5000 / 4000B / 5000B
  (D009-7506A)

  > Manuals for Administrators Security Reference
  MP 4000 / 5000 / 4000B / 5000B
  Aficio MP 4000 / 5000 / 4000B / 5000B
  (D009-7508A)

  > Manuals for Administrators Security Reference Supplement
  9040 / 9040b / 9050 / 9050b
  MP 4000 / 5000 / 4000B / 5000B
  LD040 / LD050 / LD040B / LD050B
  Aficio MP / 4000 / 4000B / 5000 / 5000B
  (D011-7790A)

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 on 2008-03 and concluded by completion the Evaluation Technical Report dated 2009-10. 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 on 2008-10, 2008-12, 2009-01, 2009-06 and 2009-10 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 on 2009-06 and 2009-07.

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 reviews were 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.

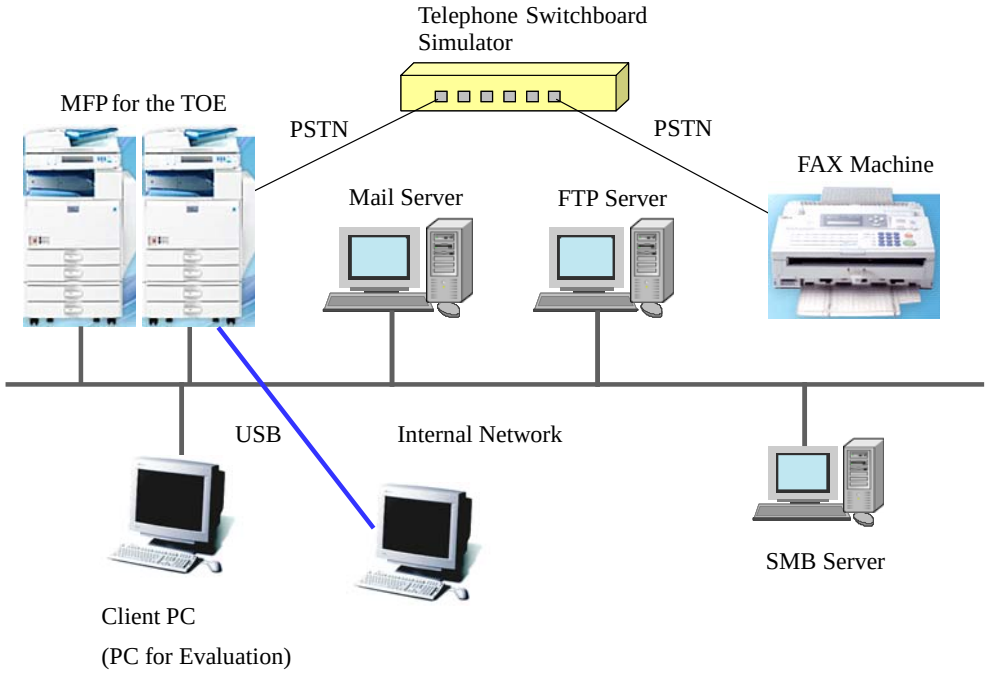

Figure 2-1 Configuration of Developer Testing

The following outlines show the elements of the test configuration.

- MFP for the TOE
  The following machines were intended for testing:
  Japan: Ricoh imagio MP 4000SP
  Ricoh imagio MP 4000SPF
  Ricoh imagio MP 5000SPF
  Overseas: Ricoh Aficio MP 4000SP
  Ricoh Aficio MP 4000SPF
  Ricoh Aficio MP 5000SP

- Client PC
  The followings were used as Web browser:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0

  Drivers were used as follows:
  > RPCS Driver V7.68, V7.69 for domestic machines
  > RPCS Driver V7.66 for overseas machines
  > PC Fax Driver V1.59 for domestic machines
  > LAN Fax Driver V1.60 for overseas machines

- Mail Server
  Windows Server 2003 SP2 was used for Software with SMTP server function.

- FTP Server
  Windows XP Pro Sp2 was used for Software with FTP server function.

- SMB Server
  Windows XP Pro Sp2 was used for Software with SMB server function.

- Fax machines

Ricoh imagio MP 5000SPF, Ricoh Aficio MP 4000SPF were used for machines with Fax function.

- Telephone Switchboard Simulator
  TLE-101III (manufactured by LSI JAPAN CO., LTD.) was used for machines to be considered equivalent to public lines.

The configuration of the developer testing covers the TOE configuration which is identified in this ST except for MFP as the TOE. Since the configuration of the developer testing also covers the properties (print speed, domestic or overseas machines, with/without Fax Function) of each MFP identified in this ST, it is considered as covering each MFP for the TOE identified in ST.

2) Outlining of Developer Testing

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

a. Test configuration

The test configuration which the developers implemented is shown in Figure 2-1. The developer testing is implemented in the environment to be considered as covering the TOE configuration identified in ST.

b. Testing Approach

Testing, mainly from the usage of the desired TOE (operate the Operation Panel, internal network or client PC which is connected with USB, operate Fax machines), stimulated an external interface to the TOE and performed in a way to eye-check and observe the results. Sometimes it is inappropriate to use such ways. In that case, the following approach was used:

1. To ensure that the communication over the internal network is SSL, IPSec protocol, capture the communication over the internal network using WireShark, and then check it.
2. To ensure the operation which is inside of the TOE, replace MFP control software with the embedded code to output the debug information and then check the output debug information.
3. To ensure the function of checking the integrity for MFP control software, replace the MFP control software with the code, "which is embedded to output the debug information and in which the integrity is damaged", and then check the output debug information.

c. Scope of Testing Performed

This testing is implemented by the developers for approximately 642 items.
It detected that the coverage analysis was implemented and all of the security functions and external interfaces described in the function specifications were completely tested. Also, it detected that the depth analysis was implemented and that all of the subsystems and subsystem interfaces described in the upper-level design were fully tested.

d. Result

The test results by the developers verified that the expected test results and the actual test results met. The evaluators confirmed the implementation methods

of the developer testing and the validity of the implementation items, and then verified that the implementation methods and results met the ones shown in the test plans.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The configuration of testing which the evaluators implemented is the same as the one of the developer testing. The configuration is shown in Fig. 2-1.

- MFP for the TOE
  The following machines were intended for testing:
  Japan: Ricoh imagio MP 4000SP
  Ricoh imagio MP 4000SPF
  Ricoh imagio MP 5000SPF
  Overseas: Ricoh Aficio MP 4000SPF

- Client PC
  The followings were used as Web browser:
  > Internet Explorer 6.0
  > Internet Explorer 7.0
  > Internet Explorer 8.0

  Drivers were used as follows:
  > RPCS Driver V7.69 for domestic machines
  > RPCS Driver V7.66 for overseas machines
  > PC Fax Driver V1.59 for domestic machines
  > LAN Fax Driver V1.60 for overseas machines

- Mail Server
  Windows Server 2003 Pro was used for Software with SMTP server function.

- FTP Server
  Windows Server 2003 Pro was used for Software with FTP server function.

- SMB Server
  Windows Server 2003 Pro was used for Software with SMB server function.

- Fax machines
  Ricoh imagio MP 2550 was used for machines with Fax function.

- Telephone Switchboard Simulator
  TLE-101III (manufactured by LSI JAPAN CO., LTD.) was used for machines to be considered equivalent to public lines.

The configuration of the evaluator testing covers the TOE configuration which is identified in this ST except for MFP as the TOE. Since the configuration of the developer testing also covers the properties (print speed, domestic or overseas machines, with/without Fax Function) of each MFP identified in this ST, it is considered as covering each MFP for the TOE identified in ST. For drivers, it is considered as covering each driver identified in ST because it was performed by identifying the equality of the different version.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follows:

a. Test configuration

The test configuration which the evaluators implemented is shown in Figure 2-1. The evaluator testing is implemented in the environment to be considered as covering the TOE configuration identified in ST.

b. Testing Approach

The testing was implemented in the same way as the developer testing.

c. Scope of Testing Performed

The testing which the evaluators independently created was created by 40 items from the following perspectives:

- For the purpose of increasing the testing strictness, conduct the testing which the developers implemented to change the parameters and the conditions.
- Considering SSL, IPSec, S/MIME which is the function to protect the communications as the characteristic security functions, complement the testing to ensure that there are no conditions to disable these functions.

Sampling of the developer testing was selected by 192 items after covering the security functions and interfaces for testing and considering the following perspectives:

- Regarding as the important behaviors to ensure that the following security functions correctly operate, the followings must be selected clearly:
  > Combination of each condition in the access control function to stored documents
  > Combination of the authorized operator and the authorized operation in the security management function
  > Combination of each condition in the action for authentication failure
  > Checking of operating the functions to verify software validity
  > Function of checking password strength
  > Encryption function for stored documents
  > Self-Test function for encrypting the TOE initiation
  > Protection function for network communication data
- It is intended to include the completeness of audit log event and the testing to check the contents of the obtained audit log records.
- It is intended to include all types of the interface (Classification of the Operation Panel, Web interface, etc.).

The evaluators searched for the potential vulnerability from the provided evidence materials and the public-known information, and they identified the following vulnerabilities needed for the intrusion testing.

1. The existing unintentional network port interface makes it possible to access the TOE.
2. Direct access to the designated URL from Web interface makes it possible to bypass the Identification and Authentication function and the access control function.
3. There is the possibility of the existing measures to bypass the Identification and Authentication function in the Operation Panel and Web interface and to operate the TOE.
4. The vulnerability which the diagnostic tool cannot detect for Web application used by the developer testing could exist in Web interface.

The evaluators implemented the following intrusion tests to determine if the potential vulnerability can be misused.

1. Use the tool for port scan and the command to access the network port (Rlogin, Telnet, SSH, Rsh, FTP) and investigate the network port which can use TOE.
2. Investigate the potential URL which can bypass the Identification and Authentication function and the access control function, and then enter in the browser the URL which was found by the result to try to access.
3. Attempt all the possible operations except for the login operation from the Operation Panel or Web interface.
4. Use the different vulnerability tool from the one used in the developer testing, and implement the vulnerability diagnosis for Web interface

d. Result

All of the implemented "tests which the evaluators independently created" and "sampled developer testing" correctly completed and could confirm the behaviour of the TOE. The evaluators confirmed that all of the test results met the expected behaviors.
All of the implemented evaluator intrusion tests indicated that there was no vulnerability which attacker who has the assumed attack potential can exploit.

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 reviews, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Reports and certification reviews 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 EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

4.2.1 Notes for the Protected Assets

The following data is not intended for protection in this certification.
- Data which the TOE received by Fax function
- Print Settings

4.2.2 Notes for the Settings and the Functions to Restrict the Usage

The certified configuration of the TOE is restricted to some designated settings. If the TOE is not configured using the designated settings, then the TOE is not in the certified configuration. For the specific setting items and the restrictions, see "1.2.3.1 Scope of TOE".
The certified configuration also restricts some functions of the TOE. If the administrator uses those functions, then the TOE is not in the certified configuration. For the specific restricted functions, see A.ADMIN in "1.5.8 Assumptions for Operational Environment".
If a consumer expects to use restricted settings or functions, the consumer should consider this when determining if it is appropriate for the product to be introduced in its own environment.

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.

Address Book	A database containing General User Information for each General User.
Administrator	An authorized TOE user who manages the TOE. Administrators are given Administrator Roles and perform administrative operations accordingly. Up to four (4) Administrators can be registered, and each Administrator is given one (1) or more Administrator Roles.
Administrator Role	Management functions given to Administrators. There are four types of Administrator Roles: User Administration, Machine Administration, Network Administration and File Administration. Each Administrator Role is assigned to at least one of the registered Administrators.
Complexity Setting for Password	The minimum combination of character types that can be registered for passwords. There are four (4) character types: upper-case letters, lower-case letters, numbers, and symbols. There are two complexity setting levels for Complexity Setting for Password, Level 1 and Level 2. Level 1 requires passwords with a combination of more than two character types. Level 2 requires passwords with a combination of more than three character types.
D-BOX	A storage area for Document Data on the HDD.
Deliver to Folder	A function that sends the Document Data to folders in SMB Server or FTP Server from the TOE via networks.

Document Data	Electronic data that are loaded into MFP by authorized MFP users using either of the following operations. 1. Electronic data that are scanned from paper-based original and digitized by authorized MFP users' operation. 2. Electronic data that are sent to the MFP by authorized MFP users and converted by the MFP from received Print Data into a format that can be processed by the MFP.
Document Data ACL	An access control list of General Users that is set for each Document Data.
Document Data Default ACL	One of the data items of General User Information. The default value that is set for the Document Data ACL of a new Document Data to be stored.
External Networks	Networks that are not managed by the organization that manages the MFP. Generally, indicates the Internet.
Fax Transmission from PC	A function that faxes Document Data from a client PC via the TOE when connecting client PC to networks or with USB Ports.
File Administration	The Administrator Role that manages the D-BOX, which stores the Document Data stored in the TOE, and manages the Document Data ACL, which controls the access to the Document Data. The File Administrator is a person who has the role of File Administration.
FTP Server	A server for sending files to client PC and receiving files from client PC using File Transfer Protocol.
General User	An authorized TOE user who uses the basic functions of the TOE.
General User Information	A record containing information about a General User. Data items include the General User IDs, General User authentication information, Document Data Default ACL, and S/MIME User Information.
GSA	The government agency in North America. General Service Administration.
HDD	An abbreviation for Hard Disk Drive. Indicates the HDD installed in the TOE.
Ic Hdd	A hardware device that encrypts the data to be written on HDD and decrypts the data to be read from HDD.
Ic Key	A chip that contains a microprocessor for encryption processing and EEPROM that stores a private encryption key for secure communication. It keeps the keys for validity authentication and encryption processing and the random number generator.
Immediate Transmission	A function that dials first, then faxes data while scanning the original.
Internal Networks	Networks managed by an organization that has MFP. Normally indicates the office LAN environment established as the intranet.

Internet Fax	A function that converts scanned document images to e-mail format and transit the data over the Internet, and a machine that has an e-mail address can receive the e-mail sent using this function.
IP-Fax	A function that sends and receives document files between two faxes directly via a TCP/IP network. It is also possible to send document files to a fax that is connected to a telephone line using this function.
Lockout	A function that prohibits the access for the specific user IDs to the TOE.
Machine Administration	The Administrator Role that manages machines and plays the role of performing the audit. The Machine Administrator is a person who has the machine management role.
Memory Transmission	A function that stores the scanned data of the original in memory, and then dials and faxes the data.
MFP	An abbreviation for digital multi function product.
MFP Control Data	A generic term for a set of parameters that control the operation of MFP.
MFP Control Software	Software installed in the TOE and has the elements that identify the TOE such as System/Copy, Network Support, Scanner, Printer, Fax, Web Support, Web Uapl and Network Doc Box. It manages the resources for units and devices that comprise the MFP and controls their operation.
Minimum Password Length	The minimum number of digits that can be registered for passwords.
Operation Panel	A display-input device that consists of a touch screen LCD, key switches, and LED indicators, and is used for MFP operation by users. Operation Panel Unit.
Print Data	The document files in client PC that are sent to the TOE from a client PC to be printed or faxed. It is necessary to install drivers into client PC in advance - printer driver for printing and fax driver for faxing. Print Data is taken into the TOE from Network Units or USB Ports.
Print Setting	Print Settings for printed output, including paper size, printing magnification and customized information (such as duplex and layout).
PSTN	An abbreviation for Public Switched Telephone Networks.
Responsible Manager for MFP	A person in an organization in which MFPs are placed and who has the authority to assign MFP Administrators and a Supervisor (or the person who is responsible for the organization). E.g., MFP purchasers, MFP owners, a manager of the department in which MFPs are placed, a person who is in charge of IT department.

Sending by E-mail	A function that sends e-mail with the attached Document Data from the TOE.
SMB Server	A server for sharing files with client PC using Server Message Block protocol.
S/MIME User Information	Information about each General User that is required for using S/MIME. Includes E-mail address, user certificates and specified value for S/MIME use.
SMTP Server	A server for sending E-mail using Simple Mail Transfer Protocol.
Store and Print Function	A function that converts Print Data received by the TOE into Document Data and stores it in D-BOX. Document Data stored in D-BOX can be printed out according to users' instruction.
Stored Data Protection Function	A function that protects the Document Data stored on HDD from leakage.
Stored Documents Fax Transmission	A function that faxes Document Data previously stored in D-BOX.
Supervisor	The authorized TOE user who manages the passwords of Administrators.
User Administration	The Administrator Role that manages General Users. The User Administrator is a person who has the user management role.

6. Bibliography

[1] imagio MP 4000/5000 series, Aficio MP 4000/5000 series Security Target Version 1.13 (October 30, 2009) RICOH COMPANY, 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] RICOH COMPANY, LTD. imagio MP 4000/5000 series, Aficio MP 4000/5000 series Evaluation Technical Report Version 1.8, October 30, 2009, Information Technology Security Center Evaluation Department