Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-10-29 (ITC-9275)
Certification No.	C0260
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japanese: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Zentai Seigyo Software English: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software
Version of TOE	A0P00Y0-0100-GM0-22
PP Conformance	None
Conformed Claim	EAL3
Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2010-06-29

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

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

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

Evaluation Result: Pass

"Japanese: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Zentai Seigyo Software, English: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software Version A0P00Y0-0100-GM0-22" 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.

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 "Japanese: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Zentai Seigyo Software, English: bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software Version A0P00Y0-0100-GM0-22" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Konica Minolta Business Technologies, Inc. and provides information to the users and system operators who are interested in this TOE.

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

This certification report assumes "general consumer" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

1.1.1 EAL

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

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	Japanese:	bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Zentai Seigyo Software
	English:	bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software
Version:	A0P00Y0-0100-GM0-22	
Developer:	Konica Minolta Business Technologies, Inc.	

1.2.2 Product Overview

bizhub C652, bizhub C652DS, bizhub C552, bizhub C552DS, bizhub C452, ineo+ 652, ineo+ 652DS, ineo+ 552, ineo+ 452, VarioLink 6522c, VarioLink 5522c, VarioLink 4522c, which this TOE is installed, are digital multi-function products provided by Konica Minolta Business Technologies, Inc., composed by selecting and combining copy, print, scan and FAX functions. (Hereinafter all the products are referred to as "MFP".)
TOE is the "control software for bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network. TOE supports the protection function from exposure of the highly confidential documents stored in the MFP. Moreover, for the danger of illegally bringing out HDD, which stores image data in MFP, TOE can encrypt all the data written in HDD including image data using ASIC (Application Specific Integrated Circuit). Besides, TOE provides the function that deletes all the data of HDD completely by deletion method compliant with various overwrite deletion standards and the function that controls the access from the public line against the danger using Fax function as a steppingstone to access internal network.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Roles related TOE

The roles related to this TOE are defined as follows.

(1) User
An MFP user who is registered into MFP. In general, the employee in the office is assumed.

(2) Administrator
An MFP user who manages the operations of MFP. Manages MFP's mechanical operations and users. In general, it is assumed that the person elected from the employees in the office plays this role.

(3) Service engineer
A user who manages the maintenance of MFP. Performs the repair and adjustment of MFP. In general, the person-in-charge of the sales companies that performs the maintenance service of MFP in cooperation with Konica Minolta Business Technologies, Inc. is assumed.

(4) Responsible person of the organization that uses the MFP
A responsible person of the organization that manages the office where the MFP is installed. Assigns an administrator who manages the operation of MFP.

(5) Responsible person of the organization that manages the maintenance of the MFP
A responsible person of the organization (In general, the sales companies that performs the maintenance service of MFP) that manages the maintenance of MFP. Assigns service engineers who manage the maintenance for MFP.

Besides this, though not a user of TOE, those who go in and out the office are assumed as accessible person to TOE.

1.2.3.2 Scope of TOE and Environment of Operation

TOE is the MFP control software and is installed in the flash memory on the MFP controller in the main body of MFP. It is loaded and run on the RAM when main power is switched ON. The relation between TOE and MFP is shown in Figure 1-1.

FAX unit and device interface kit are optional parts of MFP. For the environment of TOE operation, it assumes that the device interface kit is installed when user uses bluetooth device and FAX unit is installed when user uses FAX function.

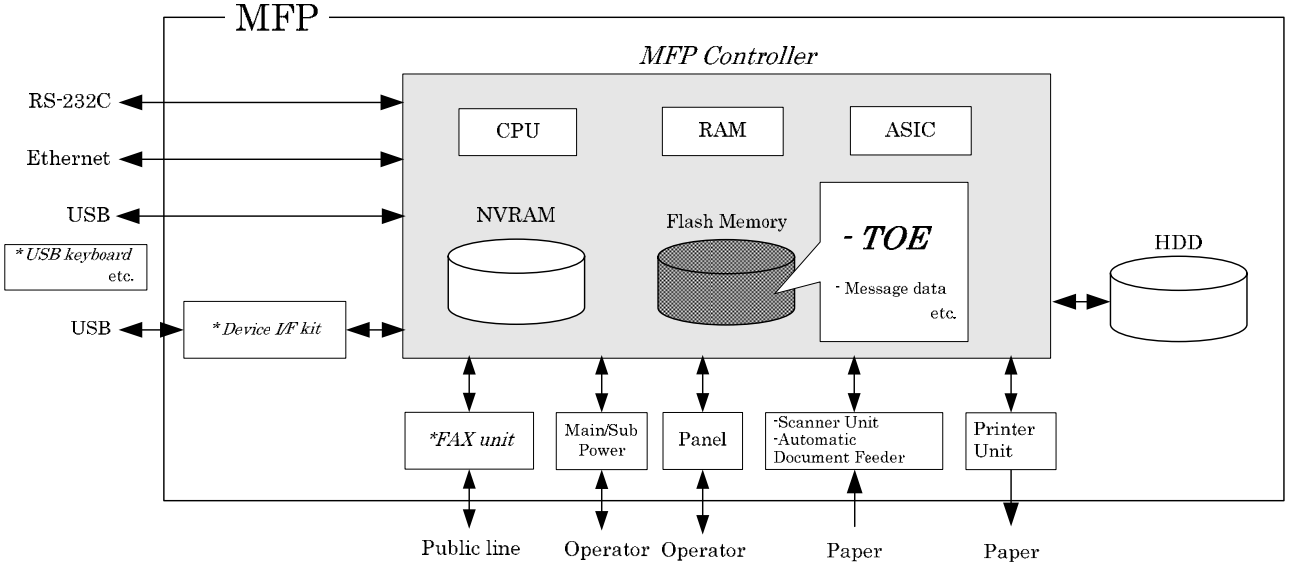

Figure 1-1 Hardware composition relevant to TOE

The composition of TOE are shown as follows.

(1)Flash memory
A storage medium that stores the object code of the "MFP Control Software," which is the TOE. Additionally, stores the message data expressed in each country's language to display the response to access through the panel and network.

(2)NVRAM
A nonvolatile memory. This memory medium stores various settings that MFP needs for the processing of TOE.

(3)ASIC
An integrated circuit for specific applications which implements an encryption function for enciphering the data written in HDD.

(4)HDD
A hard disk drive of 250GB in capacity. This is used not only for storing image data as files but also as an area to save image data and destination data temporarily during extension conversion and so on.

(5)Main/sub power supply
Power switches for activating MFP

(6)Panel
An exclusive control device for the operation of the MFP, equipped with a touch

panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

(7)Scanner unit/ automatic document feeder
A device that scans images and photos from paper and converts them into digital data

(8)Printer unit
A device that actually prints the image data which were converted for printing when receives a print request by the MFP controller

(9)Ethernet
Supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet

(10)USB
Copying image file to an external memory, copying or printing image file from an external memory, update of TOE, and so on can be performed through this interface. It is usable as connection interface of the optional parts. There are the device interface kit which is need for copy or print from bluetooth device and the USB keyboard to complement key entry from the panel. Including an external memory, it is necessary to be able to use them.

(11)RS-232C
Serial connection using D-sub 9 pins connectors is usable. The maintenance function is usable through this interface in the case of failure. It is also possible to use the remote diagnostic function (described later) by connecting with the public line via a modem.

(12) FAX Unit (*Option)
A device that has a port of Fax public line and is used for communications for FAX-data transmission and remote diagnostic (described later) via the public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. Fax unit is purchased when the organization needs it, and the installation is not indispensable.

Users of TOE (users, administrators, service engineers) use a variety of functions of TOE from the panel and a client PC via the network. The Overview of TOE functions are shown as follows.

(1)Basic Function
In MFP, a series of functions for the office work concerning the image such as copy, print, scan, and fax exists as basic functions, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image files, and stores them in RAM and HDD. (For print image files from client PCs, multiple types of conversion are applied.) These image files are converted into data to be printed or sent, and transmitted to the device outside of the MFP controller concerned.
Operations of copy, print, scan, and fax are managed by the unit of job, so that operation priority can be changed by giving directions from the panel, finishing of print jobs can be changed, and such operations can be aborted.

(2)Secure Print Function
When a Secure Print password is received together with printing data, the image file is stored as standby status. Then, printing is performed by a print direction and password entry from the panel.

(3)ID & Print Function

When this function is set up, usual print data are saved in the print waiting state, and printed by the user authentication processing from the panel. Even when this function is not set up, if it is specified on the print data to activate this function, the system will operate in the same manner as this function is set up by a user.

(4)User Box Function

A directory called "user box" can be created as an area to store image files in HDD. Three types of user box are usable; the first is the personal user box which a user possesses, the second is the public user box which is shared by registered users who made a certain number of groups, and the third is the group box which is shared by the users belonging to same account. As for the personal user box, the operation is limited only for the user who owns it, the public user box performs access control by sharing a password set to the user box among users, and group box limits operations only for the users of the account that are permitted to use it. TOE processes the following operation requests to a user box or image files in the user box that is transmitted from the panel or the network unit through a network from a client PC.

(5)User Authentication Function

TOE can limit the user who uses MFP. For access through the panel or the network, TOE identifies and authenticates that the user is permitted to use the MFP by applying the user password and user ID. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function etc.

The following are supported in the method of the user authentication.

[Machine authentication]

A method to authenticate user at MFP by registering a user ID and a user password into HDD on the MFP controller.

[External server authentication]

A method to authenticate user at MFP by using the user ID and the user password that are registered on the user information management server which is connected with the intra-office LAN without managing the user ID and user password on the MFP side.

In this evaluation, machine authentication and external server authentication using Active Directory are the targets for evaluation.

(6)Account Authentication Function

TOE can manage the MFP users by grouping them into Account unit. The methods of Account Authentication are as follows.

[Method synchronized with User Authentication]

Set an Account ID on a user beforehand, and the user with the account ID of the user's account when he/she is authenticated.

[Method not synchronized with User Authentication]

Associate a user with his/her account ID when the user is authenticated by the account password set for each account ID.

(7)Administrator Function

TOE provides the functions such as the management of user boxes, management of user information at the time of MFP authentication and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

(8)Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate.

(9)Encryption Key Generation Function

Performs encryption/decryption by ASIC when writing data in HDD or reading data from HDD. (TOE does not process the encryption and description itself.)
The operational setup of this function is performed by the administrator function. When it operates, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

(10)Remote Diagnostic Function

MFP's equipment information such as operating state and the number of printed sheets is managed by making use of the connection by a port of FAX public line, by a modem through RS-232C or by E-mail or WebDAV to communicate with the support center of MFP produced by Konica Minolta Business Technologies, Inc. In addition, if necessary, appropriate service (shipment of additional toner packages, account claim, dispatch of the service engineers due to the failure diagnosis, etc.) are provided.
When enhanced security function (described later) is set valid, the setting function in the function concerned becomes invalid.

(11)Updating Function of TOE

TOE facilitated with the function to update itself. As for the update means, there are a method that exists as one of items of remote diagnostic function, a method that downloads from FTP server through Ethernet (TOE update function via Internet), and a method that performs the connection of an external memory.
When enhanced security function (described later) is set valid, this updating function of TOE through Ethernet including the request from the remote diagnostic function becomes invalid.

(12)Encryption Communication Function

TOE can encrypt the data transmitted from client PC to MFP, and the data received by download from MFP by using SSL/TLS. The operational setup of this function is performed by the administrator function.

(13)S/MIME certificate automatic registration Function

It is the function to register the certificate for S/MIME (conforms to ITU-T X.509) with each transmission address automatically. When a certificate is attached in received e-mail, MFP recognizes user ID according to the information of e-mail header, and registers the certificate as certificate of the same user ID.

(14) Fax unit control function

TOE prohibits access to the internal network, where MFP was connected to, from a port of Fax public line through Fax unit.

(15)Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, there is the reset function of the network setting and the update function of TOE through the network, but the use of these functions is prohibited.

1.2.3.3 Security Functions of TOE

The protected assets are the following image files which are produced as MFP is generally used.

- Secure Print File
  An image file registered by Secure Print.

- ID & Print File
  An image file stored as ID & print file when print data is registered by using ID & print function

- User Box file
  An image file stored in the personal user box, public user box and group user box.

Furthermore, when the stored data have physically gone away from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of a theft of HDD, the user has concerns about leak possibility of every remaining data in HDD and NVRAM. Therefore, in this case, the following data files become protected assets.

- Secure Print File

- ID & Print File

- User Box File

- On-memory Image File
  Image file of job in the wait state on memory.

- Stored Image File
  Stored image files other than secure print file, ID & print file and user box file.

- HDD remaining Image File
  The file which remains in the HDD data area that is not deleted only by general operation (deletion of a file maintenance area).

- Image-related File
  Temporary data file generated in print image file processing.

- Transmission Address Data File
  File including E-mail address and telephone numbers that become the destination to transmit an image.

TOE has the following security functions to protect the above mentioned protected assets.

Firstly, TOE provides the identification authentication function to confirm that the user is permitted and the access control function to limit the access to protected assets for each user, in order to prevent the illegal operation to secure print file, ID & print file and user box file of the protected assets.

Secondly, TOE provides encryption function of data written in HDD by using all area overwrite deletion function of HDD, initialization function of settings for NVRAM and encryption function by ASIC outside the TOE in order to prevent the leakage of information from HDD and NVRAM where the protected assets are stored in MFP.

Thirdly, TOE provides trusted channel function used for the communication to correct destination and the encrypting and transmitting function of image file sent from MFP to client PC by using S/MIME in order to protect securely the image file transmitted between TOE and client PC used by user or administrator.

Fourthly, TOE provides the identification and authentication function to confirm users are an administrator or a service engineer and management function to limit the access such as the change of setting files for each user in order to prevent the illegal operation against the various set files that decide operations of MFP and TOE.

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 "bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software A0P00Y0-0100-GM0-22 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 A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Evaluation is completed with the Evaluation Technical Report dated 2010-06 submitted by the evaluation facility and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

2. Summary of TOE

2.1 Security Problem and assumptions

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

2.1.1 Threat

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

Table 2-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and disposal of MFP)	When leased MFPs are returned or discarded MFPs are collected, secure print files, user box files, ID & print files, on-memory image files, stored image files, HDD-remaining image files, image-related file, transmission address data files, and various passwords which were set up can leak by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.
T.BRING-OUT-STORAGE (An unauthorized carrying out of HDD)	- Secure print files, user box files, ID & print files, on-memory image files, stored image files, HDD-remaining image files, image-related files, transmission address data files, and various passwords which were set up can leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP. - A person or a user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files such as secure print files, user box files, ID & print files, on-memory image files, stored image files, HDD-remaining image files, image-related files, transmission address data files and various passwords which were set up are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so that such image files will leak.
T.ACCESS-PRIVATE-BOX (Unauthorized access to the personal user box which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and operates the user box file, such as copies, moves, downloads, prints, transmits, and so on.
T.ACCESS-PUBLIC-BOX (Unauthorized access to public box which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the public user box which is not permitted to use, and operates the user box file, such as copies, moves, downloads, prints, transmits, and so on.
T.ACCESS-GROUP-BOX (Unauthorized access to the group user box which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the group user box which the account where a user does not belong to owns, and operates the user box file, such as

	copies, moves, downloads, prints, transmits, and so on.
T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file or ID & print file by utilizing the user function)	- Secure print files are exposed by those malicious including users when he/she operates, such as prints, ones to which access is not allowed. - ID & print files are exposed by those malicious including users when he/she operates, such as prints, ones which were stored by other users.
T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)	- Malicious person or user changes the network settings that are related to the transmission of a user box files. Even an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that the user box file is exposed. <The network settings which are related to user box file transmission> - Setup related to the SMTP server - Setup related to the DNS server - Malicious person or user changes the network settings which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another unauthorized MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print files or ID & print files are exposed. - Malicious person or user changes the TSI receiving settings. A user box file is stored to the entity which a user does not intend to, so that a user box file is exposed. - Malicious person or user changes the PC-FAX reception settings. By changing the setting of the storing for the public user box to store to common area for all users, a user box file is stored to the entity which a user does not intend to, so that a user box file is exposed. *This threat exists only in the case that the setting of PC-FAX reception is meant to work as the operation setting for box storing.
T.ACCESS-SETTING (An unauthorized change of a function setting condition related to security)	The possibility of leaking user box files, secure print files, or ID & print files rises because those malicious including users change the settings related to the enhanced security function.
T.BACKUP-RESTORE (Unauthorized use of Backup function and restoration function)	User box files, secure print files, or ID & print files can leak by those malicious including users using the backup function and the restoration function illegally. Also highly confidential data such as passwords can be exposed, so that settings might be falsified.

2.1.2 Organisational Security Policy

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

Table 2-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.COMMUNICATION-DATA (secure communication of image file)	Highly confidential image file (secure print files, user box files, and ID & print files) which transmitted or received between IT equipment must be communicated via a trusted pass to the correct destination, or encrypted when the organization or the user expects to be protected.
P.REJECT-LINE (Access prohibition from public line)	An access to internal network from public line via the port of Fax public line must be prohibited.

The term "between IT equipment" here indicates between client PC and MFP that the user uses.

2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 2-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN (Personnel conditions to be an administrator)	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.SERVICE (Personnel conditions to be a service engineer)	Service engineers, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.NETWORK (Network connection conditions for MFP)	- The intra-office LAN where the MFP with the TOE will be installed is not intercepted. - When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET (Operating condition about secret information)	Each password and encryption passphrase does not leak from each user in the use of TOE.
A.SETTING (Operational setting condition enhanced security function)	MFP with the TOE is used after enabling the enhanced security function.

2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions in order to fulfill the assumptions.

<Documents for administrator and user>

- bizhub C652 / C652DS / C552 / C552DS / C452 User's Guide [Security Functions] (Japanese) Ver.102
- bizhub C652 / C652DS / C552 / C552DS / C452 User's Guide [Security Operations] Ver.102
- ineo+ 652 / 652DS / 552 / 452 User's Guide [Security Operations] Ver.102
- VarioLink 6522c / 5522c / 4522c User's Guide [Security Operations] Ver.102

<Documents for service engineer>

- bizhub C652 / C652DS / C552 / C552DS / C452 SERVICE MANUAL [SECURITY FUNCTION] (Japanese) Ver.102
- bizhub C652 / C652DS / C552 / C552DS / C452 SERVICE MANUAL [SECURITY FUNCTION] Ver.102
- ineo+ 652 / 652DS / 552 / 452 SERVICE MANUAL [SECURITY FUNCTION] Ver.102
- VarioLink 6522c / 5522c / 4522c SERVICE MANUAL [SECURITY FUNCTION] Ver.102

2.1.5 Configuration Requirements

The TOE is software. This evaluation targets at the behavior on the following hardware and software. However the reliability of hardware and software described in the configuration is outside the scope of this evaluation.

- If the external server authentication method is selected as for the user identification and authentication, Active Directory, the directory service provided by Windows Server 2000 (or later), is needed to consolidate the user's information under the Windows platform network environment as the external server.

2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions and fulfills the organisational security policies in 2.1.2.

(1)Security function to counter the threat [T.DISCARD-MFP (Lease return and disposal of MFP)]

This threat assumes the possibility of leaking information from MFP collected from the user.

TOE provides the function to overwrite data for the deletion of all area of HDD and initializes the settings like passwords that is set in NVRAM (referred as "All area overwrite deletion function"), so it prevents the leakage of the protected assets and

the security settings in HDD and NVRAM connected to leased MFPs that were returned or discarded MFPs

(2)Security function to counter the threat [T.BRING-OUT-STORAGE (Unauthorized bring-out of HDD)]

This threat assumes the possibility that the data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorized HDD and bringing out with the data accumulated in it.

This TOE provides the generation function of encryption key to encrypt the data written in the HDD (referred as "encryption key generation function") and supporting function with the ASIC (referred as "ASIC operation support function") by using the encryption function of ASIC outside of TOE, so that the encrypted data is stored in HDD and it makes it difficult to decode the data even if the information is read out from HDD.

(3)Security function to counter the threat [T.ACCESS-PRIVATE-BOX (Unauthorized access to personal user box using user function)]

This threat assumes the possibility that an unauthorized operation is done by using the user function for the personal user box which each user uses to store the image file.

When you use various functions of MFP with this TOE, the change in settings of users and personal user boxes is limited only to administrator and the permitted users, and the operation of personal user box is restricted only to the normal users, and it prevents unauthorized operation by using user functions by maintaining functions such as the identification and authentication function of users and administrators (referred as "user function" and "administrator function"), the access control function for personal user box (referred as "user box function") and the function that limits the changes in settings of users and personal user box to administrators and users (referred as "administrator function", "user function" and "user box function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

(4)Security function to counter the threat [T.ACCESS-PUBLIC-BOX (Unauthorized access to public user box using user function)]

This threat assumes the possibility that an unauthorized operation is done by using the user function for the public user box which each user shares to store the image file.

When you use various functions of MFP with this TOE, the change in settings of public user box and the users is limited only to administrators and the permitted users, and the operation of public user box is restricted only to the normal users, and it prevents unauthorized operation by using user functions, by maintaining functions such as the identification and authentication function of users and administrators (referred as "user function" and "administrator function"), the authentication function on the access of public user box, access control function for public user box, the function that limits the changes in settings of public user box to administrators and permitted users (referred as "user box function") and the

functions that limits the changes in settings of users to administrators and users (referred as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

(5)Security function to counter the treat [T.ACCESS-GROUP-BOX (Unauthorized access to a group user box using user function)]

This threat assumes the possibility that an unauthorized operation is performed by using the user function for the group user box that is a storage area of image file used by user who is permitted the use of the account, or the user box file in it.

When you use various functions of MFP with this TOE, the change in settings of group user box and the users is limited only to administrators and the permitted users, and the operation of group user box is restricted only to the normal users, and it prevents unauthorized operation by using user functions, by maintaining functions such as the identification and authentication function of users and administrators (referred as "user function" and "administrator function"), the access control function for group user box, the function that limits the changes in settings of group user box to administrators and users (referred as "user box function") and the functions that limits the changes in settings of users to administrators and users (referred as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

(6)Security function to counter the threat [T.ACCESS-SECURE-PRINT (Unauthorized access to a secure print file using user function)]

This threat assumes the possibility that an unauthorized operation is done to the secure print and ID & print using user function.

When you use various functions of MFP with this TOE, the changes in settings of secure print are limited to administrators and the changes of user settings are limited only to administrators and the permitted users, and the operation of secure print and ID & print files are restricted only to the normal users, and it prevents unauthorized operation by using user functions, by maintaining functions such as the identification and authentication function of users and administrators (referred as "user function" and "administrator function"), the authentication function with secure print password and identification and authentication function of user registered ID & print file, access control function for secure print and ID & print files, the function that limits the changes in settings of secure print and ID & print files to administrators (referred as "secure print function") and the functions that limits the changes in settings of users to administrators and permitted users (referred as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

(7)Security function to counter the threat [T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)]

This threat assumes the possibility of sending the information to the address that isn't intended, when the network setting related to the transmission or the network setting related to MFP address, PC-FAX operational setting or TSI receiving setting is illegally changed.

This TOE provides the identification and authentication function of administrator and functions to limit the changes of settings such as network installation, PC-FAX operation setting and TSI receiving setting only to administrator (referred as "administrator function"), so that the change of network installation, PC-FAX operation setting and TSI receiving setting is restricted only to administrator, and it prevents the possibility of transmission to the address that isn't intended.

(8)Security function to counter the threat [T.ACCESS-SETTING (Unauthorized change of function setting condition related to security)]

This threat assumes the possibility of developing consequentially into the leakage of the user box files, the secure print files and ID & print files by having been changed the specific function setting which relates to security.

This TOE provides the identification and authentication function of administrator (referred as "administrator function" and "SNMP manager function"), the identification and authentication function of service engineer (referred as "service mode function", and restricting function for setting the specific function related to security only to administrator and service engineer (referred as "administrator function", "SNMP manager function" and "service mode function"), so that the change of the specific function related to security only to administrator and service engineer, and as a result, it prevents the possibility of leakage of the user box file, the secure print file or ID & print file.

(9)Security function to counter the threat [T.BACKUP-RESTORE (Unauthorized use of back-up function and restoration function)]

This threat assumes a possibility that user box files, secure print files, and ID & print files may leak since the back-up function or the restoration function is illegally used. Moreover, this assumes that confidential data such as the passwords might leak or various settings are falsified, so that user box files, secure print files, or ID & print files may leak.

This TOE provides the identification and authentication function of administrator and restricting function for the use of back-up function and restore function only to administrator (referred as "administrator function"), so that the use of back-up function and restore function is restricted only to administrator, and as a result, it prevents the possibility of leakage of user box files, secure print files, ID & print files and confidential data such as passwords.

(10)Security function to satisfy the organizational security policy [P.COMMUNICATION-DATA (secure communication of image file)]

This organizational security policy prescribes carrying out processing via trusted pass to a correct destination or encrypting to ensure the confidentiality about the image file which flows on a network in the case of the organization or the user

expect to be protected. As this corresponds as one's request, there is no need to provide secure communication function for all communication. At least one secure communication method between MFP and client PC needs to be provided when transmitting the secure print file, ID & print file or the user box file.

This TOE provides the functions such as the function to support the trusted channel to correct destination in the transmission and reception of images between MFP and client PC, for the user box file, the secure print file, and ID & print file (referred as "trusted channel function"), the encryption key generation function to transmit the user box file by S/MIME, the encryption function of user box file, the encryption function of encrypted key for S/MIME transmission (referred as "S/MIME encryption processing function"), the identification and authentication function of administrator, and the function to limit the change in settings related to the trusted channel and S/MIME only to administrator (referred as "administrator function"), so that it realizes to transmit to correct destination by transmitting image data confidentially in the network and restricting the change of settings only to the administrator.

(11)Security function to satisfy the organizational security policy [P.REJECT-LINE (Access prohibition from public line)]

This organizational security policy prohibits being accessed to internal network via the port of Fax public line on Fax unit installed to MFP. This function is provided when Fax unit is installed to MFP.

This TOE provides the function prohibits the access to the data existing in internal network from public line via the port of Fax public line (referred as "Fax unit control function"), so that it realizes to prohibit the access to the internal network via the port of Fax public line.

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

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

3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2009-11 and concluded by completion the Evaluation Technical Report dated 2010-06. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2010-03 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 2010-03.

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

3.3 Product Testing

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

3.3.1 Developer Testing

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

1) Developer Test Environment

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

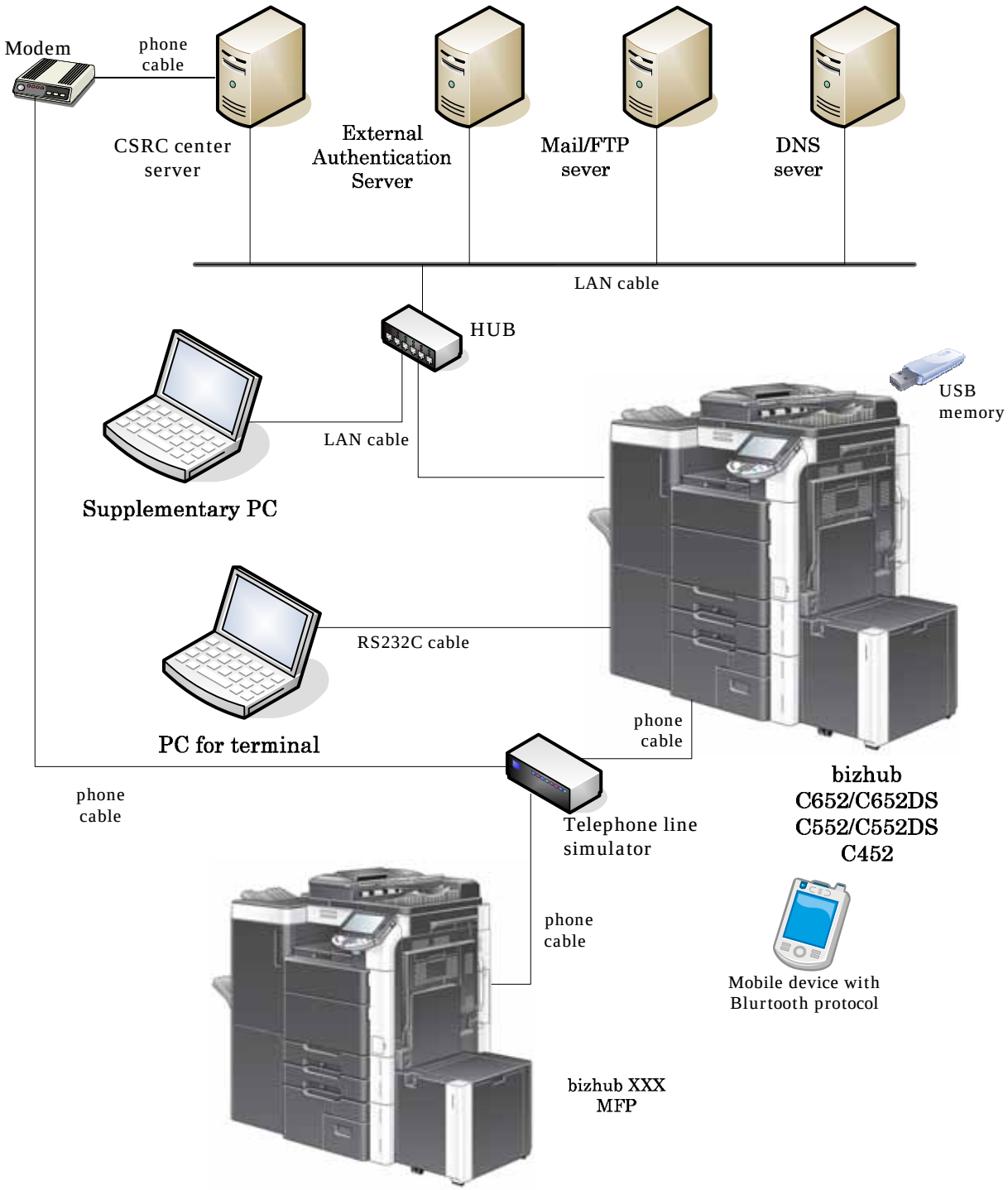

Figure 3-1 Configuration of Developer Testing

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

2) Outlining of Developer Testing

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

a. Test outline

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

<Testing Approach>
Test was done to execute security functions through external interface when the functions have the external interfaces that developer can use. And it was done to get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that developer can use.

<Tools and others used at Testing>

Table 3-1 Tools and others used in developer testing

Name of hardware and software	Outline and Purpose of use
KONICA MINOLTA C652 Series PCL/XPS Ver. 3.0.16.0	Exclusive printer driver software included in the bundled CD of bizhub C652 / C652DS / C552 / C552DS / C452.
Internet Explorer Ver. 6.0.2800.1106 (Win2000) Ver. 6.0.2900.2180 (WinXP)	General purpose browser software. Used to execute PSWC in the supplementary PC. Also used as SSL/TLS confirmation tool.
Fiddler Ver. 2.2.2.0	Monitor and analyzing tool software for Web access of http and etc. Used to test HTTP protocol between MFP and supplementary PC.
Open API test tool Ver. 7.2.0.5	Exclusive test tool software for the Open API evaluation. Most of the tests for Open API are confirmed the functions at the message level by this tool.
SocketDebugger Ver. 1.12	Used as the test tool for TCP-Socket.
WireShark Ver. 1.2.2	Tool software for monitoring and analyzing of the communication on the LAN. Used to get communication log.
Mozilla ThunderBird Ver. 2.0.0.21	General purpose mailer software. Used as the confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver.0.9.8k (25-May-2009)	Encryption tool software for SSL and hash function.

Name of hardware and software	Outline and Purpose of use
MG-SOFT MIB Browser Professional SNMPv3 Edition (Hereinafter it is omitted with MIB Browser) Ver. 10.0.0.4044	MIB exclusive browser software. Used for tests related to SNMP.
Tera Term Pro Ver. 4.29	Terminal software executed in the terminal PC. Used to connect with MFP and to operate the terminal software installed in the MFP to monitor the state of TOE.
Disk dump editor Ver. 1.4.3	Tool software to display the contents in the HDD.
Stirling Ver. 1.31	Binary editor software. Used to confirm the contents of the encryption key and decode S/MIME message and to edit the print file.
FFFTP Ver. 1.92a	Used as FTP client software.
MIME Base64 Encode/Decode Ver. 1.0	Tool software to encode/decode of MIME Base64. used as tool to confirm encode/decode of S/MIME message.
Pagescope Data Administrator with Device Set-Up and Utilities Ver. 1.0.03200.10051	Device management tool software for administrator of plural MFPs. (Activation of the following plug-in software is possible.)
HDD Backup Utility (Plug-in) Ver. 1.3.03000 781	HDD Backup Utility is the utility to backup and restore the recorded media installed in the MFP on the network
PageScope Box Operator (PSBO) Ver. 3.2.03000	Tool to acquire and print the image document stored in the HDD. Used as the confirmation tool of trusted channel.
Sslproxy Ver. 1.2	Proxy software in the supplementary PC operating between MFP main body and the browser software of the supplementary PC. By communicating with main body through SSL and with browser software through non-SSL, it makes Fiddler and Socket Debugger possible to monitor avoiding SSL encryption by sslproxy.
Blank Jumbo Dog Ver. 4.1.3	Simple server software for intranet. Used as mailer server and FTP server function.
CSRC center software Ver. 2.4.0	Server softare for CSRC center.

b. Scope of Testing Performed

Testing is performed 223 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. Result

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

3.3.2 Evaluator Independent Testing

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

1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.
Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.
Only bizhub C652 and C552 are chosen as MFP which TOE is loaded, however it is judged not to have any problem as a result that the following confirmation was done by evaluator.

- ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 and VarioLink 6522c / VarioLink 5522c / VarioLink 4522c are OEM of bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C452.

- It was confirmed by a document offered from developer that bizhub C652DS / bizhub C552DS are different from C652 / bizhub C552 in the type of auto document feeder which is not TOE.

- It was confirmed by a document offered from developer that a difference of bizhub C652 / bizhub C552 / bizhub C452 is only copy / print speed and a difference of the durability guarantee value.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

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

<Viewpoints of Test>
(1)Based on the situation of developer test, test targets are all security functions.
(2)Test targets are all probabilistic and permutable mechanism.
(3)Test the behavior depending on the differences of password input methods to TSI for the test of the probabilistic and permutable mechanism.

(4)Based on the strictness of the developer test, test the necessary variations.
(5)Based on the complexity of interfaces, test the necessary variations.
(6)For the interfaces with innovative and unusual character, test the necessary variations.

b. Outlining of Evaluator Independent Testing

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

<Testing Approach>
Test was done to execute security functions through external interface when the functions have the external interfaces that evaluator can use. And it was done to get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that evaluator can use.

<Tools and others used at Testing>
The tools and others are the same as used ones at the developer test.

<Outline of each Test viewpoint>
Test outline for each independent test viewpoint is shown in Table 3-2.

Table 3-2 Viewpoints of Independent Test and Overview of Testing

Viewpoints of Independent Test	Overview of Testing
(1) Viewpoint	Tests were performed that were judged to be necessary in addition to developer tests.
(2) Viewpoint	Tests were performed with changing the number of letters and the types of letters by paying attention to the probabilistic and permutable mechanism at identification and authentication or etc. by the user.
(3) Viewpoint	Tests were performed with considering the operated interfaces to confirm the behavior depending on the difference of password input method.
(4) Viewpoint	Tests were performed to confirm the WebDAV server password modification function, based on the closeness of the test done by the developer.
(5) Viewpoint	Tests were performed with considering the complexity of various user boxes combination to confirm the action at changing the types of user boxes.
(6) Viewpoint	Tests were performed with judging the function being innovative and unusual character to confirm the action of the Fax unit control function and the unsual behavior of bluetooth device.

c. Result

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

3.3.3 Evaluator Penetration Testing

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

1) Outlining of Evaluator Penetration Testing

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

a. Vulnerability of concern

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

<Vulnerability requiring the penetration tests>
(1)Possibility to be activated the unexpected service.
(2)Possibility to be detected the public vulnerability by the vulnerability checking tool.
(3)Possibility to affect the behavior of the TOE through the variation of input data.
(4)Possibility of the easy speculation of session information.
(5)Possibility to affect the security functions by the power ON/OFF.
(6)Possibility of the inappropriate exclusive access control.
(7)Possibility to affect the security functions through the setting status of encryption passphrase.

b. Scope of Test Performed

Evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

<Testing Environment>
Figure 3-2 shows the penetration test configuration used by evaluator.

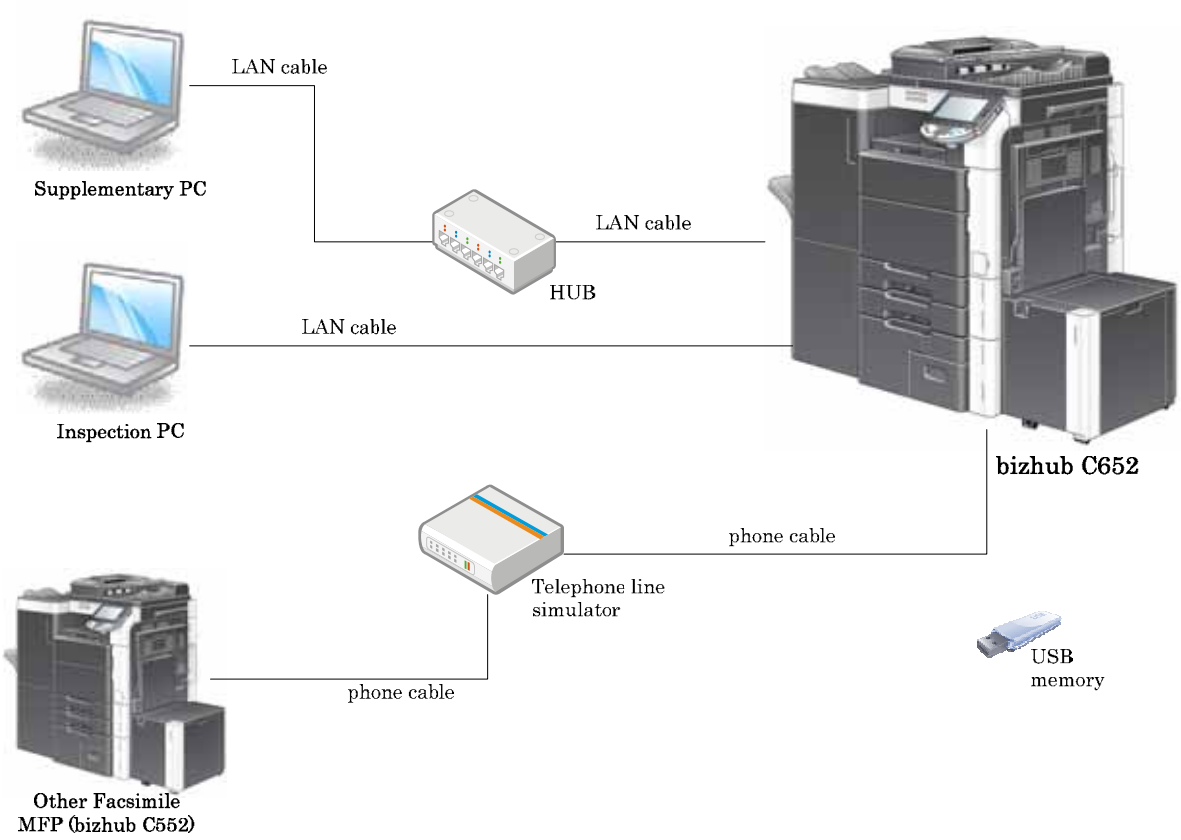

Figure 3-2 Configuration of Penetration Testing

<Testing Approach>
Penetration tests were done by the following methods.

- Method to check by the visual observation of the behavior after stimulating TOE with operating from the operational panel.
- Method to check by the visual observation of the behavior after accessing TOE through network with operating the supplementary PC.
- Method to check by the test tool of the behavior after tampering parameters by using test tool.
- Method to scan the publicly known vulnerability by the vulnerability checking tool with operating the inspection PC.

<Tools and others used at Testing>

Test Configuration Environment	Details
Inspection object (TOE)	- TOE installed in bizhub C652/C552 (Version: A0P00Y0-0100-GM0-22) - Network configuration Penetration Tests were done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP (SP2). - Using the tools shown in table 3-1. (Fiddler, OpenAPI test tool, SocketDebugger etc.) - Access the MFP by using PSWC (abbreviation of "PageScope Web Connection"), HTTPS, TCPSocket, OpenAPI, SNMP etc. and it can setup the network etc. Furthermore possible to use TamperIE.

Test Configuration Environment	Details
Inspection PC	- Inspection PC is a PC with network terminal operated on Windows XP SP2, and is connected to MFP with cross-cable to perform penetration tests. - Explanation of test tools. (Plug-in and vulnerability database are applied the latest version on Mar. 19, 2010.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8m (25-Feb-2010) encryption too of SSL and hash function (3)Nessus 4.0.1 build 4G1046-Q Security scanner to inspect the vulnerability existing on the System (4)TamperIE 1.0.1.13 Web proxy tool to tamper the transmitted data from general Web browser such as Internet Explorer to arbitrary data. (5)sslproxy v 1.2 2000/01/29 SSL proxy server software (6)Fiddler 2.2.8.6 Web debugger to monitor HTTP operation (7)Wireshark 1.2.4 Packet analyzer software that can parse protocols more than 800. (8)Nikto Version 2.03 CGI and publicly known vulnerability inspection tool

<Concerned vulnerabilities and Test outline>
The concerned vulnerabilities and the corresponding tests outline are shown in Table 3-4.

Table 3-4 Concerned vulnerabilities and Overview of Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and behavior inspection.
(2) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and result analysis.
(3) Vulnerability	Tests were performed to confirm that there is no influence on the security behavior (domain separation, by-pass, interference and etc.) by transmitting of edited parameters through network.
(4) Vulnerability	Tests were performed to confirm that the mechanism for holding session has a unique identification.
(5) Vulnerability	Tests were performed to confirm that the forced power ON/OFF does not affect the security function of initialization process, screen display and etc.

Concerned vulnerabilities	Overview of Testing
(6) Vulnerability	Tests were performed to confirm the exclusive control being done by the access from operational panel and network simultaneously.
(7) Vulnerability	Tests were performed to confirm that the setting state of encryption passphrase does not affect the behavior of the security function.

c. Result

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

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

Especially, none comments.

4. Conduct of Certification

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

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

5. Conclusion

5.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body determined the TOE is satisfied the assurance requirements of EAL3 components prescribed in CC Part 3.

5.2 Recommendations

- If the external server authentication method is selected as for the user authentication function, the external server authentication method using Active Directory is required and TOE accepts the identification and authentication information managed with Active Directory that is outside of TOE with assuming that it is correct and, operates.

- If FAX unit which is option is not installed, FAX unit control function that is security function is unnecessary, but it does not affect the operation of other security functions.

6. Glossary

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

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

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

API	Application Programming Interface
DNS	Domain Name System
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HTTPS	HyperText Transfer Protocol Security
MFP	Multiple Function Peripheral
MIB	Management Information Base
NVRAM	Non-Volatile Random Access Memory
RAM	Random Access memory
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL/TLS	Secure Socket Layer/Transport Layer Security
S/MIME	Secure Multipurpose Internet Mail Extensions
TSI	Transmitting Subscriber Identification
USB	Universal Serial Bus
WebDAV	Web-based Distributed Authoring and Versioning

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

Bluetooth	One of the short distance wireless communication technology used for connection between the devices, such as mobile device, in several meters

DNS — Protocol to manage the relationship of the domain name and IP address in the internet

FTP — File Transfer Protocol used at TCP/IP network.

HTTPS — Protocol adding with the encryption function of SSL to hold a secure communication between Web server and client PC

MIB — Various setting information that the various devices managed using SNMP opened publicly

NVRAM — Random access memory that has a non-volatile and memory keeping character at the power OFF

PageScope Web Connection
Tool installed in the MFP to confirm and set the MFP state by using browser

PC-FAX operation
Operation to process sorting the received image data into storage user boxes based on the information specified at the FAX receiving

SMB — Protocol to realize the sharing of files and printers on Windows

SMTP — Protocol to transfer e-mail in TCP/IP

SNMP — Protocol to manage various devices through network

SNMP password
Generic term of password (Privacy password, Authentication password) to confirm the user at the use of SNMP v3 in TOE

SSL/TLS — Protocol to transmit encrypted data through the Internet

S/MIME — Standard of e-mail encryption method
Transmitting the encrypted message using RSA public key cryptosystem and needs electric certificate published from certification organization

TSI reception — Function to designate the storing user box for each sender

WebDAV — Protocol to manage files on the Web server with expanded specification of HTTP1.1

Encryption passphrase
Original information to generate the encryption key to encrypt and decrypt on ASIC

Intra-office LAN
Network connected TOE and being secured by using switching hub and eavesdropping detection device in the office environment, also being securely connected to the external network through firewall

Administrator mode
State possible for administrator to conduct the permitted operation to the MFP

External network
: Access restricted Network from TOE connected intra-office LAN by firewall or other

Service Mode
: State possible for service engineer to conduct the permitted operation to the MFP

Secure Print password
: Password to confirm whether permitted user or not before the operation to the secure print file

Secure Print file
: Image file registered by secure print

Secure Print
: Printing method that restricts by the password authentication. Specify the password by the printer driver and printing by MFP is allowed only when that password is authenticated.

Flash Memory
: Memory device that performs the high speed and high integration of EEPROM and carries the batch deletion mechanism

User Box file
: Image file stored in the user box, public box and group box.

7. Bibliography

[1] bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software A0P00Y0-0100-GM0-22 Security Target Version 1.06 (April 7, 2010) Konica Minolta Business Technologies, Inc.

[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 Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

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

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

[8] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001 (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002 (Japanese Version 1.0, December 2009)

[10] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003 (Japanese Version 1.0, December 2009)

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

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

[13] bizhub C652 / bizhub C652DS / bizhub C552 / bizhub C552DS / bizhub C452 / ineo+ 652 / ineo+ 652DS / ineo+ 552 / ineo+ 452 / VarioLink 6522c / VarioLink 5522c / VarioLink 4522c Control Software Evaluation Technical Report Version 1, May 27, 2010, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security