Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-12-28 (ITC-9283)
Certification No.	C0265
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japanese : bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Zentai Seigyo Software English : bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software
Version of TOE	A1UD0Y0-0100-GM0-00
PP Conformance	None
Assurance Package	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.
2010-08-31

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 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Zentai Seigyo Software, English: bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software Version A1UD0Y0-0100-GM0-00" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Japanese: bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Zentai Seigyo Software, English: bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software Version A1UD0Y0-0100-GM0-00" (hereinafter referred to as "the TOE") developed by Konica Minolta Business Technologies, Inc., and evaluation of the TOE was finished on 2010-07 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). 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 Security Target (hereinafter referred to as "the ST") that is the appendix of this book together. Especially, the TOE security functional requirements, the assurance requirements for TOE and rationale of sufficiency about those 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 Product Overview

The Overview of functions and operation conditions of this TOE is described bellow. Refer to after Chapter 2 for the details

1.1.1 Assurance Package

The Assurance Package of this TOE is EAL3.

1.1.2 TOE and Security Functionality

bizhub 423, bizhub 363, bizhub 283, bizhub 223, bizhub 7828, ineo 423, ineo 363, ineo 283 and ineo 223, 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 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223" 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.

About these security functionalities, the validity of the design policy and the accuracy

of the implementation were evaluated in the range of the assurance package. Threats and operational environment that this TOE assumes is described in the next clause.

1.1.2.1 Threats and Security Objectives

This TOE counters each threat by the following security functions.

- It is assumed as threat that information leaks from MFP after lease return or discard of MFP. To counter this threat, TOE has the function to delete the information in storage medium.

- It is assumed as threat that HDD is stolen from MFP and information is leaked from stolen HDD. To counter this threat, TOE encrypts and writes information in HDD by using the encryption function of ASIC outside of TOE.

- It is assumed as threat that the access not permitted is done to the box file stored in the private box, the public user box or the group user box. To counter this threat, TOE identifies and authenticates user and measures the right or wrong of access based on the information of users and box file.

- It is assumed as threat that the access not permitted is done to the secure print file or ID & print file. To counter this threat, TOE identifies and authenticates user and permits only the person who stored the operation of the secure print file and ID & print file.

- It is assumed as threat that information leaks by the following causes.

  > Transmitting the box file to the different address which user does not intend when transmitted it from TOE.

  > Pretending TOE and exploiting the secure print file and ID & print file.

  > Storing the box file to the different box which user does not intend when TOE receives it.

  To counter this threat, TOE confirms whether it is an administrator by identification and authentication and permits only the administrator the operation of setting about the address, setting to pretend to be TOE and setting about the destination.

- It is assumed as threat that the leak of information cannot prevent because the setting of enhanced security function is changed. To counter this threat, TOE confirms whether it is an administrator or a service engineer by identification and authentication and permits only the administrator or the service engineer to change the setting of enhanced security function.

- It is assumed as threat that backup function or restore function is abused and a result, a leak of information or a change of setting value, is caused. To counter this threat, TOE confirms whether it is an administrator by identification and authentication and permits only the administrator to use the backup function or the restore function.

(Supplement)
TOE has user authentication function and it can use, it can use Active Directory that is outside of TOE.

1.1.2.2 Configuration and Assumptions

It assumes that the product of target of evaluation is operated in the following configuration and assumptions.

It assumes that the MFP including this TOE is installed in the office which is managed by organizations such as a company or the section, and is connected to the intra-office LAN.

In this environment, the MFP is managed so that is not accessed from an external network when LAN is connected to an external network which is outside of the organization such as the Internet, and the communication through the LAN is managed so that is not wiretapped.

It assumes that an administrator and a service engineer are reliable and the other users can keep the secret about his own password.

It assumes that this TOE is used in the condition that the setting of enhanced security function is enabled.

1.1.3 Disclaimers

- The function of Active Directory in case that use external authentication server for user authentication function is not assured in this evaluation.

- The encryption function by ASIC installed in MFP is not assured in this evaluation.

- Fax unit control function is valid only when the Fax unit which is an option part is installed.

1.2 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"[1], "IT Security Certification Procedure"[2] and "Evaluation Facility Approval Procedure"[3]. Evaluation was completed on 2010-07.

1.3 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.
The Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]).
The Certification Body prepared this Certification Report and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	Japanese :	bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Zentai Seigyo Software
	English :	bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software
Version of TOE:	A1UD0Y0-0100-GM0-00	
Developer:	Konica Minolta Business Technologies, Inc.	

At the time of TOE installation or others, a user can ask a service engineer to confirm that the product is this TOE evaluated and certified.

TOE version and checksum are displayed by panel operation of service engineer. A user can confirm that the installed product is this TOE evaluated and certified, by confirming TOE version and confirming that checksum is same as it in a service manual.

3. Security Policies

This chapter describes whether this TOE realizes functions as security service under what kind of policy or rule.

This TOE operates the following data.

- Secure Print file
- ID & print file
- User Box file

To protect these data from unintended leak, TOE identifies and authenticates a person who accesses these data or related data and controls access. Moreover, TOE provides an encryption function with ASIC and a data deletion function to prevent leaking from storage medium that stores these data or related data.

This TOE realizes following functions for customer's demand.

- A function to prevent the leak from the communication line of these data
- Structure not to permit access from an FAX public line port of MFP to an internal network

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 that manages the maintenance of MFP. Assigns service engineers who manage the maintenance of MFP.

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

3.2 Security Function Policies

TOE prepares security functions to counter threats shown in 3.2.1 and to fulfill the organizational security policies shown in 3.2.2.

3.2.1 Threats and Security Function Policies

3.2.1.1 Threats

This TOE assumes such threats presented in Table 3-1 and provides functions for countermeasure to them.

Table 3-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and discard 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 (Unauthorized bringing out 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.

Identifier	Threat
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.

Identifier	Threat
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.

3.2.1.2 Security Function Policies against Threats

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

(1) Security function to counter the threat [T.DISCARD-MFP (Lease return and discard 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 bringing out 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.

3.2.2 Organizational Security Policies and Security Function Policies

3.2.2.1 Organizational Security Policies

Organizational security policy required in use of the TOE is presented in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational 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.

3.2.2.2 Security Function Policies to Organizational Security Policies

TOE prepares the functions to fulfill the organizational security policies shown in Table 3-2.

(1) 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.

(2) 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.

4. Assumptions and Clarification of Scope

This chapter describes assumptions and operational environment to operate this TOE, as the information that is useful for an assumed reader to judge the use of this TOE.

4.1 Usage Assumptions

Assumptions when this TOE is operated present in the Table 4-1.

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

Table 4-1 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.

4.2 Environment Assumptions

This TOE is installed in any one of bizhub 423, bizhub 363, bizhub 283, bizhub 223, bizhub 7828, ineo 423, ineo 363, ineo 283, ineo 223, which is MFP provided by Konica Minolta Business Technologies, Inc.

It assumes that the MFP including this TOE is installed in the office which is managed by organizations such as a company or the section, and is connected to the intra-office LAN.

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.

The reliability of hardware and software to cooperate is outside the scope of this evaluation. (Regarded as reliable enough)

4.3 Clarification of scope

The reliability of ASIC and Active Directory in the below is not the scope of this evaluation.

- TOE has the function to encrypt and write information in HDD. The operation of the encryption is a function done by ASIC which is a part of MFP, so that it is the outside of TOE and is not the scope of this evaluation.

- TOE has the function to authenticate user. If the external server authentication method is selected as for the user identification and authentication, it uses Active Directory, the directory service of an external server to operate authentication.
  If the external server authentication method is selected, this TOE provides the user identification and authentication function by asking authentication information to an external server and receiving the information from it. The authentication function done by Active Directory is the outside of TOE and is not the scope of this evaluation.

5. Architectural Information

This chapter explains a purpose and a relation about the scope of TOE and the main configuration (sub systems).

5.1 TOE boundary and component

TOE is the MFP control software and is installed in the SSD 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 5-1.

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.

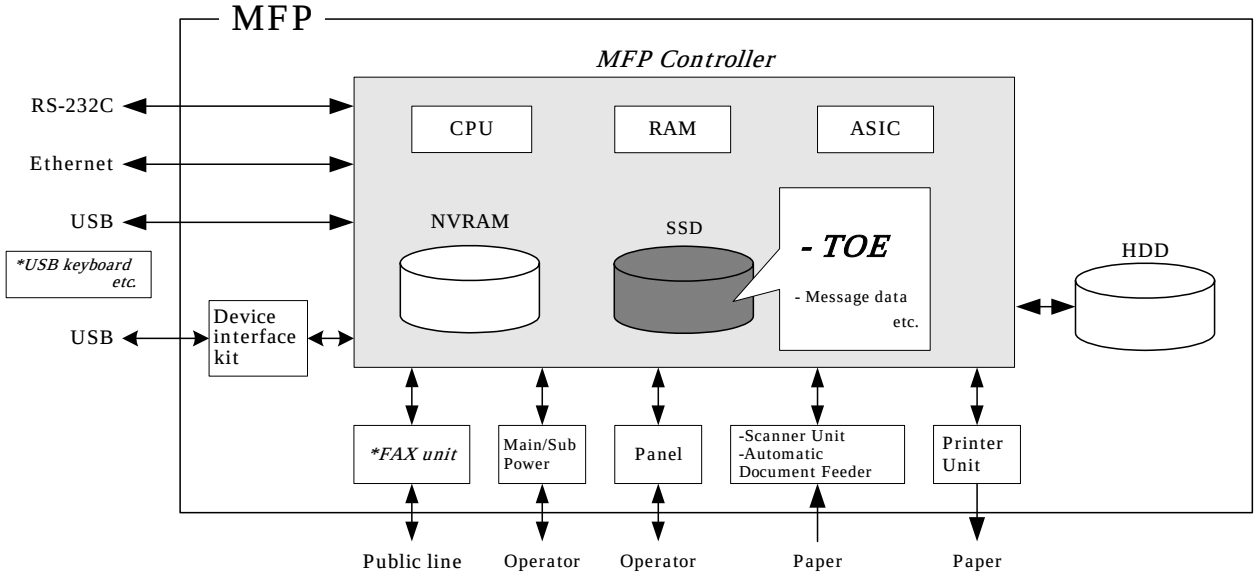

Figure 5-1 Hardware configuration relevant to TOE

TOE is composed of OS part and application part which controls MFP. The application part which controls MFP is composed of the following parts further.

- The part which provides interface through the network
  It controls ethernet and provides communication function of TCP/IP base.
  The encryption communication function is provided in this part.

- The part which provides interface via the panel
  It has the function which receives the input from the panel and the function which draws the screen of the panel.

- The part which controls job
  Job means the unit managing an execution control and operation order, of copy, print, scan, Fax, box file operation and so on.
  When "the part which controls each device" receives the operation from "the part which provides interface through the network" or "the part which provides interface via the panel" and the reception from the Fax unit, the job is made and registered.
  The execution of the actual job is realized using a following "the part which executes common management", "the part which handles HDD" and "the part which controls each device".

- The part which executes common management
  This part manages every kind of setting value and provides a measure which another part of TOE accesses to the setting value. Every kind of setting value includes information used to execute security function, like the authentication information.
  This part provides the function executing identification and authentication and the function of access control.

- The part which handles HDD
  This part provides the handling of image data and input/output function to the HDD. In input/output function to the HDD, an encryption at the time of writing and a decryption at the time of reading are done by ASIC.

- The part which controls each device
  This part controls scanner unit, printer unit and Fax unit and realizes the actual work of Copy, Print, Scan and Fax.
  Moreover, the mechanism does not let to access an internal network from Fax unit.

- The part which provides support function
  This part provides a function used for support of MFP, the function for diagnostics of MFP and the function for updating TOE.

5.2 IT Environment

The configuration of IT environment of this TOE in Figure 5-1 is shown as follows.

(1) SSD
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. These setting values are managed in "the part which executes common management."

(3) ASIC
An integrated circuit for specific applications which implements an encryption function for enciphering the data written in HDD. ASIC is used from "the part which handles 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. It is read and written from "the part which handles HDD."

(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. It is controlled by "the part which provides interface via the panel."

(7) Scanner unit/ automatic document feeder
A device that scans images and photos from paper and converts them into digital data. It is controlled by "the part which controls each device."

(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. It is controlled by "the part which controls each device."

(9) Ethernet
Supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet. It is controlled by "the part which provides interface through the network."

(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 by connecting with the public line via a modem. It is controlled by "the part which provides support function."

(12) FAX Unit
A device that has a port of Fax public line and is used for communications for FAX-data transmission and remote diagnostic via the public line. It is controlled by "the part which controls each device."
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.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required fully understanding and complying with the following documents in order to satisfy the assumptions.

< For administrators and users >

- bizhub 423 / 363 / 283 / 223 User's Guide Security Functions (Japanese) Ver.1.00
- bizhub 423 / 363 / 283 / 223 User's Guide [Security Operations] Ver.1.00
- bizhub 7828 User's Guide [Security Operations] Ver.1.00
- ineo 423 / 363 / 283 / 223 User's Guide [Security Operations] Ver.1.00

< For service engineers >

- bizhub 423 / 363 / 283 / 223 Service Manual Security Functions (Japanese) Ver.1.01
- bizhub 423 / 363 / 283 / 223 / 7828 SERVICE MANUAL SECURITY FUNCTION Ver.1.01
- ineo 423 / 363 / 283 / 223 SERVICE MANUAL SECURITY FUNCTION Ver.1.01

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

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. In this report, it explains the summery of this TOE, the content of the evaluation of each work unit, and the judgment result.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows; Evaluation has started on 2009-12 and concluded by completion the Evaluation Technical Report dated 2010-07. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by the 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 2010-05 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 the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-05.

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

7.3 IT 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.

7.3.1 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 7-1.

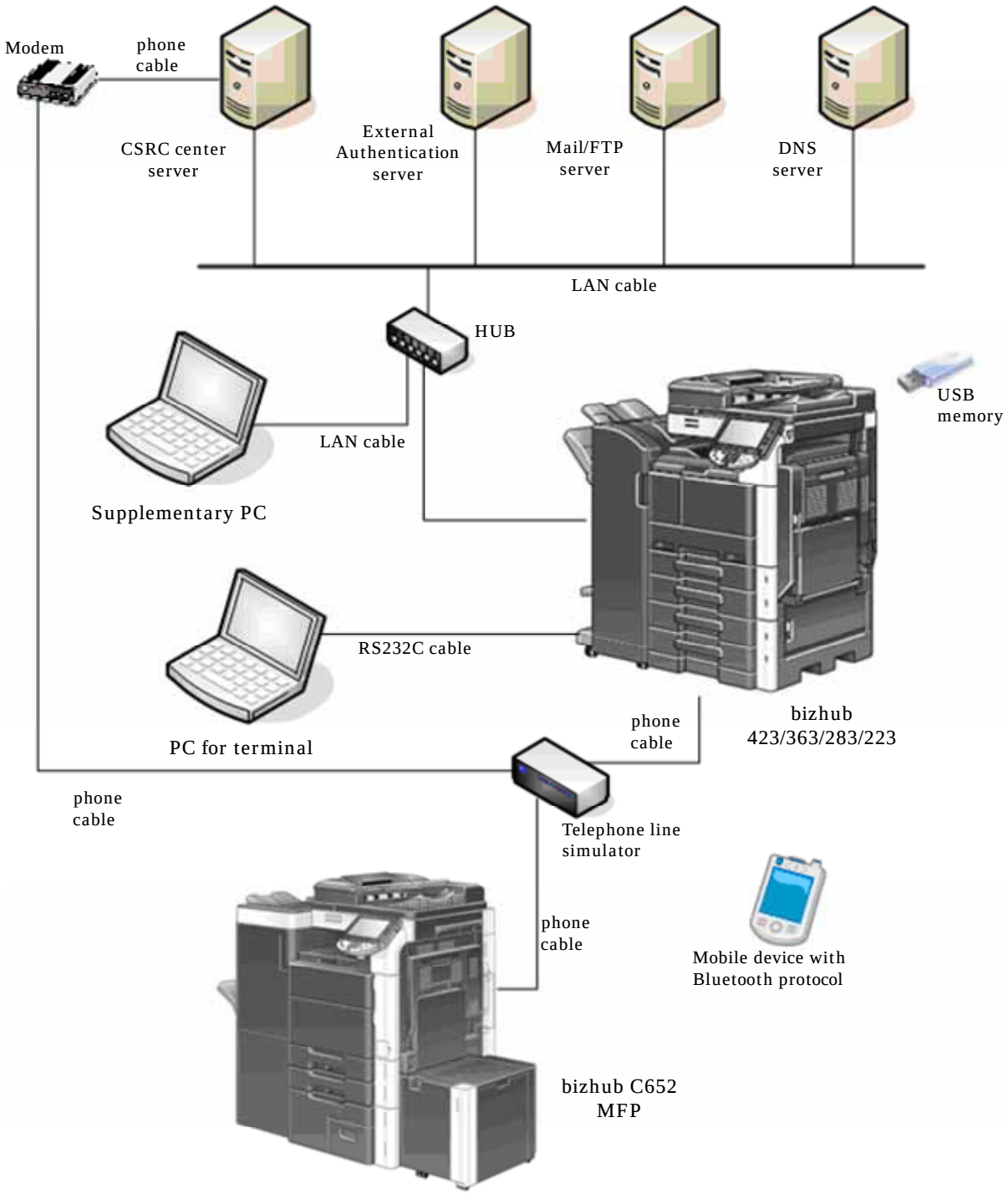

Figure 7-1 Configuration of Developer Testing

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

2) Outlining of Developer Testing

The tests performed by the developer are as follows;

a. Test outline

Outline of the tests performed by the developers are 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 7-1 Tools and others used in developer testing

Name of hardware and software	Outline and Purpose of use
KONICA MINOLTA 423 Series PCL Ver.1.1.2.0 XPS Ver.1.1.1.0	Exclusive printer driver software included in the bundled CD of bizhub 423 / 363 / 283 / 223.
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.
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.

Name of hardware and software	Outline and Purpose of use
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. 1.0.03300.12081	Device management tool software for administrator of plural MFPs. (Activation of the following plug-in software is possible.)
HDD Backup Utility (Plug-in) Ver. 1.3.04000 465	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. 3.2.04000	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. 4.2.2	Simple server software for intranet. Used as mailer server and FTP server function.
CSRC center software Ver. 2.4.0	Server software for CSRC center. CSRC is maintenance service to manage the state of MFP which Konica Minolta business technologies, Inc. offers by remote.

b. Scope of Testing Performed

Testing is performed about 216 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.

7.3.2 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 follows;

1) Evaluator Independent Test Environment

Configuration of test performed by the evaluator shall be the same configuration with developer testing.
Configuration of test performed by the evaluator shall be the same configuration with TOE configuration identified in ST.
Only bizhub423 / bizhub363 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.

- bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 are the products for OEM or the different destination of bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223.

- It was confirmed by a document offered from developer that a difference of bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 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 7-2.

Table 7-2 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 unusual behavior of bluetooth device.

c. Result

Evaluator independent tests conducted were completes correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the expected behavior.

7.3.3 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 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 setting of the enhanced security function by change of HDD.

b. Scope of Test Performed

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

<Testing Environment>
Figure 7-2 shows the penetration test configuration used by evaluator.

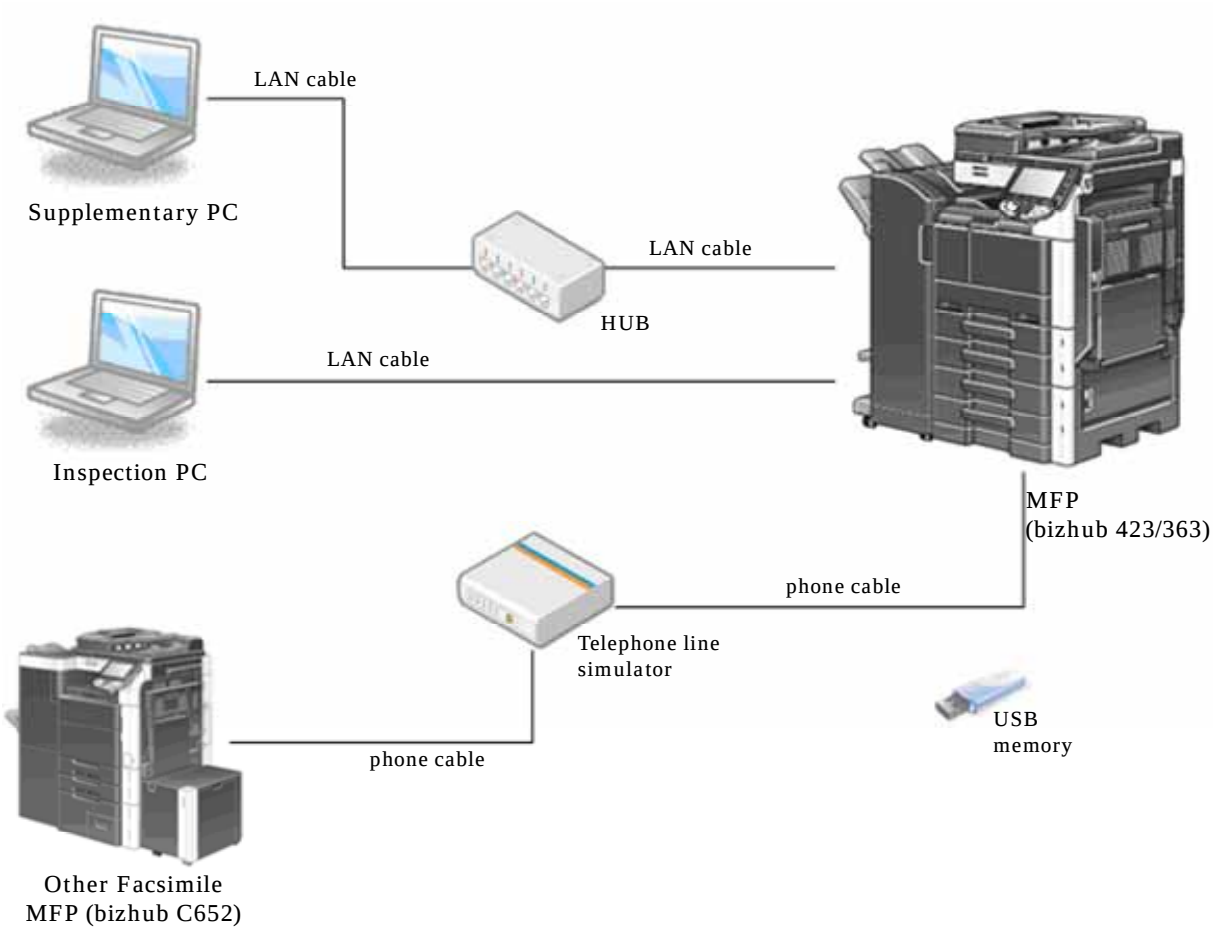

Figure 7-2 Configuration of Penetration Testing

<Penetration 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 bizhub443 / bizhub363 (Version: A1UD0Y0-0100-GM0-00) - 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) or Windows2000 (SP4). - 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.
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 0.9.8n encryption too of SSL and hash function (3)Nessus 4.2.1.(build 9119) 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 2.2.9.1 Web debugger to monitor HTTP operation (7)Wireshark 1.2.4 Packet analyzer software that can parse protocols more than 800. (8)Nikto Version 2.1.1 CGI and publicly known vulnerability inspection tool

<Concerned vulnerabilities and Test outline>
The concerned vulnerabilities and the corresponding tests outline are shown in Table 7-3.

Table 7-3 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.

Concerned vulnerabilities	Overview of Testing
(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.
(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 change of HDD does not affect the setting of the enhanced security function.

c. Result

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

7.4 Evaluated Configuration

(1) Operating model
It is assumed that this TOE is installed in any one of bizhub 423, bizhub 363, bizhub 283, bizhub 223, bizhub 7828, ineo 423, ineo 363, ineo 283, ineo 223, which is MFP provided by Konica Minolta Business Technologies, Inc.
Because of the reason shown in 7.3.2, the evaluation is considered to have been done in all models though the evaluation was not done in these all models.

(2) Setting of TOE
The evaluation was done in the following setting.

- The enhanced security function is "valid"
- The user authentication method is the following either
  > "Machine authentication"
  > "External server authentication" with Active Directory use

These setting are as the setting shown in ST.

7.5 Evaluation Results

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

As a result of the evaluation, the following assurance components were judged, "Passed".

- All assurance components of EAL3 package

In the evaluation, the following were confirmed.

- PP Conformance: none
- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

The result of the evaluation is applied to the composed by corresponding TOE to the identification described in the chapter 2.

7.6 Evaluator Comments/Recommendations

There is no evaluator recommendation that attention should be called to consumer.

8. 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.

8.1 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.

8.2 Recommendations

- This TOE depends on the following functions to counter threats. (Refer to 4.3)

  > ASIC installed in MFP

  > Active Directory (In case that the external server authentication method is selected as for the user authentication function)

  The reliability of these functions is not assured in this evaluation, it depends on operator's judgment.

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

9. Annexes

There is no Annex.

10. Security Target

Security target of the TOE [12] is published as follow, separately from this report.

bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software A1UD0Y0-0100-GM0-00 Security Target Version 1.02, April 16, 2010, Konica Minolta Business Technologies, Inc.

11. 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 Functionality

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
SSD	Solid State Drive
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.

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

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

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

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

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

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

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

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

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

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

[12] bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software A1UD0Y0-0100-GM0-00 Security Target Version 1.02, April 16, 2010, Konica Minolta Business Technologies, Inc.

[13] bizhub 423 / bizhub 363 / bizhub 283 / bizhub 223 / bizhub 7828 / ineo 423 / ineo 363 / ineo 283 / ineo 223 Control Software Evaluation Technical Report Version 2, July 27, 2010, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security