Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	June 19, 2006 (ITC-6082)
Certification No.	C0095
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	bizhub C252 / ineo+ 251 Control Software
Version of TOE	4038-0100-GN0-09-000
PP Conformance	None
Conformed Claim	EAL3
TOE 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.
May 30, 2007

Haruki Tabuchi, Technical Manager
IT Security Center

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

- Common Criteria for Information Technology Security Evaluation Version 2.3
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"bizhub C252 / ineo+ 251 Control Software version: 4038-0100-GN0-09-000" 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 "bizhub C252 / ineo+ 251 Control Software version: 4038-0100-GN0-09-000" (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.

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

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

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

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:
Name of Product:

Japan   bizhub C252 / ineo+ 251 Zentai Seigyo Software

English   bizhub C252 / ineo+ 251 Control Software

Version: 4038-0100-GN0-09-000
Developer: Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

This TOE is the embedded software that is installed on the Konica Minolta Business Technologies, Inc. digital MFP (bizhub C252 / ineo+ 251   Hereinafter referred to as " MFP" . This TOE is on the flash memory on the MFP controller carried in MFP, and this controls the whole operation of MFP such as the operation control processing and the image data management received from the panel of MFP body or the network.
This TOE offers the protection from exposure of the highly confidential document stored in the MFP, and aims at protecting the data which may be exposed against a user's intention. In order to realize it, this offers the functions such as the function that limits the operation to the specific document only to the authorized user, the function that performs the overwrite deletion of the data domain which became unnecessary and the function that deletes the confidential information including a setting value. Moreover, this has the mechanism using the unauthorized access protection function (HDD Lock Function) with

which HDD is equipped against the risk of taking out HDD unjustly which is a medium for storing image data in MFP. And this offers the encryption key generation function to encrypt the data written to the HDD when the encryption board (option part) is installed on the MFP controller.

1.2.3 Scope of TOE and Overview of Operation

This TOE exists on the flash memory on the MFP controller, which built in the body of the MFP, and is loaded and run on the RAM. Figure1-1 shows the relationship between this TOE and the MFP. Shaded region on the figure1-1 indicates the TOE and "*" shows the option parts of MFP.
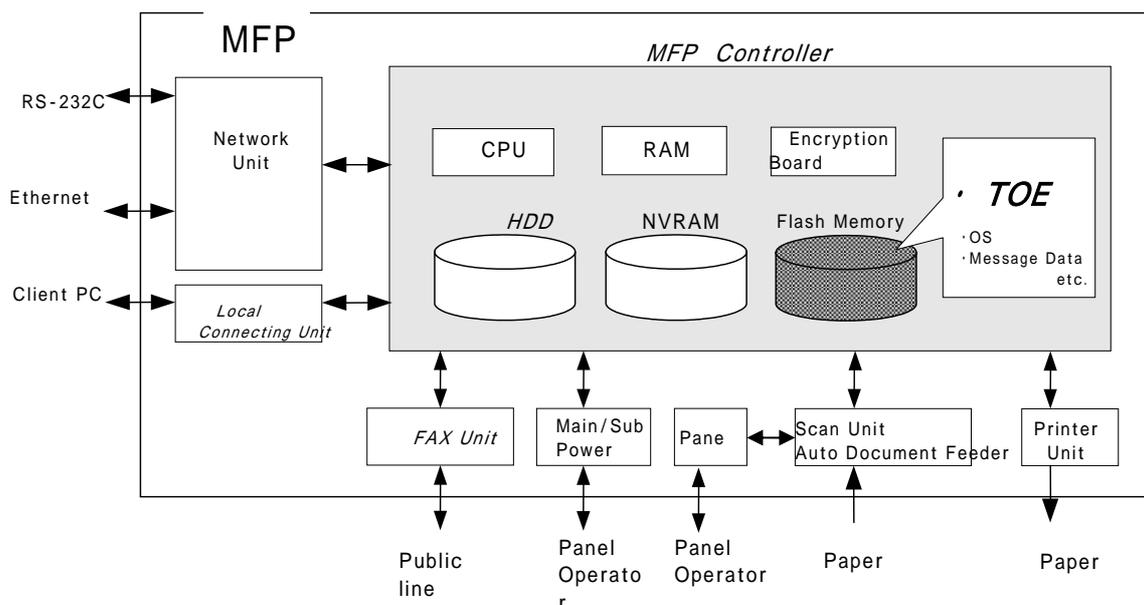
Figure 1-1:   Hardware structure that relates to TOE

Flash memory is the storage medium that stores the object code of this TOE and it also stores the message data of each country's language to display the response accessed through the panel and network, OS, and so on.
NVRAM is the nonvolatile memory and it stores various setting values (administrator password etc).
HDD stores the image data as the file, and is also used for the storage area for swapping the image data which exceeds the capacity of RAM processing area. Also, this TOE has the HDD lock function that can prohibit the unauthorized reading and unauthorized writing to HDD by setting the password in HDD.
The encryption board is provided as option parts. The encryption function is installed on the encryption board to encrypt the data written to the HDD as the hardware-based function.

Next, the logical structure of this TOE is shown. MFP includes the function that is not associated with the security directly such as basic function, and remote diagnosis function other than the function that is indicated in "1.2.4 TOE functionality".
Basic function is a series of function for the office work concerning the image such as copy, print scan and fax and TOE performs the core control in the operation of these functions.
Remote diagnosis function is used for managing the operation status of MFP, setup information, and the device information like the number of prints by using the

methods for the connection, such as the modem connection via RS-232C and the E-Mail, etc, and communicating with the support center run by the subsidiaries of the Konica Minolta Holdings, Inc.

MFP user who can use these functions uses each function that TOE provides, via the panel or the network.
The roles of the personnel that relate to the use of the MFP are defined as follows.

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

2. Administrator
MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user. (In general, it is assumed that the person elected from the employees in the office plays this role.

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

4. Person in charge at the organization that uses the MFP
A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.

5. Person in charge at the organization that manages the maintenance of the MFP
A person in charge at the organization that carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

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

1.2.4 TOE Functionality

This TOE provides the following functions.

1. Secure Print Function
When the secure print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.

2. User Box Function
The directory named a use box can be created as an area to store the image file in HDD. Two types of user box exist; one is the personal user box which a user possesses and the other is the public user box which the registered user making a group within a certain number uses jointly.
TOE offers the functions to the user box and the image file in a user box such as downloading from the client PC, deleting, and setting of the period to keep (delete automatically by the fixed time passed), and also the change of user box name, the change of the password, the deletion of the user box, and the attribute setting of user

box from the panel or the network unit. (Upon request via the network from the client PC.)

3. User Authentication Function
TOE can limit the user who uses MFP. Also, when accessing it via the panel and the network, TOE identifies and authenticates that the user is permitted to use the MFP by applying the user ID and user password. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function, etc. Two types of user authentication methods exist; one is the "Machine Authentication" that registers the user ID and user password into HDD on MFP controller, and another is the "External Server Authentication" that authenticates the user by using the user ID and the user password that are registered on the user information management server which is connected by the intra-office LAN.

4. Administrator Function
TOE provides the functions such as the management of the user boxes, the management of various settings of the network and image quality, and the management of user information at the time of machine authentication in the administrator mode that only authenticated administrator can operate. Also, it offers the operation setting function related to the behavior of the other function.

5. 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.

6. 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.

7. HDD Lock Function
HDD has the HDD lock function as measure against the illegal taking out, when the password is set. The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

8. Encryption Key Generation Function
The encoding and decoding are processed on the encryption board due to the reading and writing data in HDD. However, TOE itself does not process the encryption and decryption. It offers only the function to generate the encryption key.

The protected assets of this TOE are image files (secure print files) that are registered by the secure print and image files (user box files) that are stored in the public user box or personal user box.
Moreover, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of an HDD theft, a user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

  a. On Memory Image File
    Image file of job in the wait state

  b. Stored Image File
    Stored image files other than secure print file and user box file
  c. Remaining Image File
    The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file maintenance area)
  d. File related to the Image
    Temporary data file generated in print image file processing
  e. Transmission Address Data File
    File including E-mail address and telephone numbers that become the destination to transmit an image

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 C252 / ineo+ 251 Control Software Security Target ver.1.05" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "bizhub C252 / ineo+ 251 Control Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated April, 2007 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

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

1.5.3 SOF

This ST claims a minimum strength of function level of "SOF-basic".
This TOE assumes the use in the general office environment protected from the attack of the external network.
Access which went via the panel to TOE, or access which went via the internal network is under management by an administrator, and a complicated attack is not assumed. Therefore, SOF-foundations are enough.

1.5.4 Security Functions

Security functions of the TOE are as follow.

1. Administrator Function (F.ADMIN)
This is a series of security function that administrator operates, such as an administrator identification and authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box.

  a. Administrator Identification and Authentication Function
  It identifies and authenticates the accessing user as the administrator in response to the access request to the administrator mode.

  b. Auto Logoff Function of administrator mode
  It logs off from the administrator mode automatically when any operation was not performed for the panel auto logoff period or more, during the access to the administrator mode from the panel.

  c. Function offered in Administrator Mode
  When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user.
  The following operations and the use of the functions are permitted.

    1) Change of the administrator password
    When a user is re-authenticated as an administrator, and the new password satisfies the quality, the password is changed.
    Administrator password is set with 8-digit by using ASCII code (0x21 to 0x7E, except 0x22 and 0x2B) (A total of 92 characters are selectable.)
    It returns "*" for each character as feedback for the entered administrator

6

password if it's the access from the panel.
Also, it shall not be composed of one kind of character.
It resets the number of authentication failure when the authentication is successful
When the authentication failure that becomes the third times at total in each authentication function by using the administrator password is detected, it locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
Lock of Authentication function is released with F.RESET function operated.

2) User Settings
User is registered by setting the user ID and registering the user password. It verifies whether the user password newly set have been satisfied the following qualities. Also, it changes and deletes a user ID and a user password.
User password is set with 8-digit by using ASCII code 0x21 to 0x7E, except 0x22 and 0x2B　A total of 92 characters are selectable.
Also, it shall not be composed of one kind of character.

3) User Box Password Settings
It registers as Public user box by setting the user attributes to the unregistered user box ID. It sets and changes the user box password and also changes the user attributes of the user box.
User box password is set with 8 or more digits by using ASCII code 0x20 to 0x7E, except 0x22 and 0x2B　A total of 93 characters are selectable.
It can change to the other user's personal user box or to the public user box by specifying the user registered to user attribute of personal user box.
Also, it shall not be composed of one kind of character.

4) Release of Lock
It resets (0 clear) the number of authentication failure for user, all secure prints, all user boxes, and SNMP password.
If a user, secure print, user box or MIB object that access locked exists, the lock is released.

5) Setting of user authentication function
An authentication method in a user authentication function is set to the machine authentication or the external server authentication.

6) Setting of unauthorized access detection threshold
The unauthorized access detection threshold in the authentication operation prohibition function is set in the range for 1-3 times.

7) Setting and execution of all area overwrite deletion function
The deletion method is selected and the overwrite deletion at the all data area is performed. Perform F.OVERWRITE-ALL. The deletion method is as follows.

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers　　Random numbers　　0x00
Mode:3	0x00　　0xFF　　Random numbers　　Verification
Mode:4	Random numbers　　0x00　　0xFF
Mode:5	0x00　　0xFF　　0x00　　0xFF
Mode:6	0x00　　0xFF　　0x00　　0xFF　　0x00　　0xFF　　Random numbers
Mode:7	0x00　　0xFF　　0x00　　0xFF　　0x00　　0xFF　　0xAA
Mode:8	0x00　　0xFF　　0x00　　0xFF　　0x00　　0xFF　　0xAA Verification

7

8) Setting of auto logoff function
The panel auto logoff time is set in the range for 1-9 minutes.

9) Network Settings
A setup operation of the following setting data is performed.
　　A series of setup data that relates to SMTP server IP address, Port Number, etc
　　A series of setup data that relates to DNS server IP address, Port Number, etc
　　A series of setup data that relates to MFP address IP address, NetBIOS Name, AppleTalk Printer Name, etc.

10) Execution of back-up and restoration function
The setting data (except administrator password and CE password) stored in NVRAM and HDD is backed-up (refer) and restored (change).

11) Operation setting function of HDD lock function
When turning HDD lock function ON from OFF, it verifies that the newly set HDD lock password satisfies the following qualities.
Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.
HDD lock password is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D   A total of 83 characters are selectable
It returns "*" for each character as feedback for the entered HDD lock password in verification.
Also, it shall not be composed of one kind of character.

12) Operation setting of encryption function
When turning the encryption function ON from OFF, it verifies that the encryption passphrase newly set satisfies the qualities, and F.CRYPT is performed.
It changes the encryption passphrase. By using the encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality, it is changed and F.CRYPT is performed.
Encryption passphrase is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D   A total of 83 characters are selectable
It returns "*" for each character as feedback for the entered encryption passphrase in verification.
Also, it shall not be composed of one kind of character.

13) Function related to Enhanced Security function
The function that influences the setting of the Enhanced Security function that the administrator operates is as follows.
　　Operation setting of Enhanced security function
　　Function to set valid or invalid of Enhanced Security function.
　　HDD Logical Format Function
　　Function to re-write system file of OS in HDD. Along with the execution of this logical format, the setting of security function is invalidated.
　　Overwrite Deletion Function for all area
　　The settings of enhanced security function are invalidated by executing the overwrite deletion of all area.

14) Change of SNMP password
SNMP password is changed. Verify that SNMP password newly set satisfies the following qualities.
SNMP password is composed of 8 or more digits by using ASCII code (0x20 to 0x7E) that is selectable in total of 95 characters.

15) Setting of SNMP password authentication function
The authentication method in the SNMP password authentication function is set to "Only Authentication password" or the "Authentication password and Privacy password."

2. SNMP Administrator Function F.ADMIN-SNMP
This is a security function, which identifies and authenticates the administrator in the access through the network by SNMP from PC, and then permits the operation of setting function of the network only to the administrator whose identification and authentication was succeeded.

a. Identification and authentication function by SNMP password
It identifies and authenticates by the SNMP password, that the user who accesses the MIB object through the network with the use of SNMP is an administrator.
SNMP password is composed of 8 or more digits by using ASCII code. (0x20 to 0x7E (A total of 95 characters is selectable.)
SNMP password includes "Authentication password" and "Privacy password" and all authentication function to user SNMP password is locked when the authentication failure in total of 1 to 3 times is detected in the authentication function that uses these. Deny the access to MIB object.
The lock of authentication function is released with the operation of the lock release function to MIB object of F.ADMIN or the operation of the F.RESET function.
It resets the authentication failure frequency if it succeeds in authentication. But if both Privacy password and Authentication password is used, both authentications need to succeed to reset the authentication failure frequency.

b. Management function using SNMP
When it is identified and authenticated that the user is an administrator by the SNMP password, the access to the MIB object is permitted, and then the operation of the setting data shown as followings is permitted to be done.
     Network Settings
   Setting operation of the following setting data is performed.
       Setting data that relates to SMTP server (IP address, port number, etc.)
       Setting data that relates to DNS server (IP address, port number, etc.
       A series of setting data that relates to MFP address (IP address, NetBIOS name, AppleTalk printer name, etc.
     Change of SNMP password
   SNMP password (Privacy password, Authentication password) is changed. SNMP password newly set is composed of 8 or more digits using ASCII code. (0x20 to 0x7E)   A total of 95 characters is selectable
     Setting of SNMP password authentication function
   The authentication method in the SNMP password authentication function is set to "Only Authentication password" or the "Authentication password and Privacy password."

3. Service Mode Function (F.SERVICE)
This is a series of security function that the service engineer operates, such as the service engineer identification and authentication function in service mode accessing

from a panel, and a security management function that includes a change in the CE password and the administrator password.

   a. Service Engineer Identification and Authentication Function
It identifies and authenticates the accessing user as the service engineer in response to the access request to the service mode from panel.

   b. Function offered in service mode
The following function is allowed to use when a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the accessing request to the service mode.

   1) Change of CE password
When a user is re-authentication as a service engineer and the new password satisfies the quality, it is changed.
CE password is composed of 8-digits using ASCII code. 0x21 to 0x7E, except 0x22 and 0x2B A total of 92 characters is selectable
It returns "*" for each character as feedback for the entered CE password.
It resets the number of authentication failure when succeeding in the authentication.
It locks all the authentication functions to use the CE password when the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected. Deny the access to service mode.
F.RESET function operates and then the lock of the authentication function is released.
Also, it shall not be composed of one kind of character.

   2) Change of administrator password
It changes the administrator password. Administrator password newly set is composed of 8-digits using ASCII code. (0x21 to 0x7E, except 0x22 and 0x2B) A total of 92 characters is selectable

   3) Function that relates to Enhanced Security function
The functions that influence the setting of the Enhanced Security function that the service engineer operates are as follows.
     HDD logical format function
      The function to re-write system file of OS in HDD. The setting of the Enhanced Security function is invalidated along with the execution of this logical format.
     HDD physical format function
      The function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information. The setting of the Enhanced Security function is invalidated along with the execution of this physical format.
     HDD installation setting function
      The function to make the installed HDD effective. The setting of the Enhanced Security function is invalidated by nullifying this HDD installation setting.
     Initialization function
      Function to reset every setting value written in NVRAM to the factory default. The setting of the Enhanced Security function is invalidated by executing this initialization function.

4. User Function F.USER
It identifies and authenticates the user of the use of MFP various function. To the identified and authentication user, it offers the management functions of the user

password that is managed in the MFP at the time of machine authentication, besides the permission of the use of functions such as F.BOX and F.PRINT.

a. User identification and authentication
It identifies and authenticates to be a user for the access request to the user box and the registration request of secure print file. The use of F.BOX and F.PRINT is permitted to the user who is identified and authenticated.
User password is composed of 8 or more digits using ASCII code. 0x21 to 0x7E, except 0x22 and 0x2B   A total of 92 characters is selectable
It uses the session information more than 10^{10} for the access from the network.
It returns "*" for each character as feedback for the entered user password.
Also, it shall not be composed of one kind of character.
It resets the number of authentication failure when succeeding in the authentication.
It locks all the authentication functions to the user when the authentication failure that becomes 1-3 times at total for the concerned use is detected.
The lock of authentication function is released with the operation of the lock release function to the user authentication of F.ADMIN or the operation of the F.RESET function.
In the case of the "External server authentication" has been selected as the user authentication method, when the user who is identified and authenticated with the above-mentioned function is not registered in the MFP, this user ID is registered.

b. Auto logoff function in user identification and authentication domain
While the user who is identified and authenticated is accessing from a panel, if it does not accept any operations for more than the "panel automatic logoff time," it logs off from a user identification and authentication domain automatically.

c. Modification function of user password
When the identification and authentication are succeeded, and the access to the user identification and authentication domain is permitted, the user is permitted to change its own password. When the external server authentication is effective, this function cannot be applied.

5. User Box Function (F.BOX)
This is a series of security function related to the user box to the user who is identified and authenticated that you are the registered user, such as the permission of the operation and management of the personal user box of the user, the authentication to the user who is permitted the utilization of the user box in the access to the pubic box, and the access control function to permit various operations of the concerned user box and the user box file after the authentication.

a. Registration of user box
By selecting the user attribute to the non-registration user box ID selected, this registers a personal user box or a pubic user box.
In the case of the personal user box, the arbitrary user ID registered is specified
In addition, the personal user box that has the user ID of user who operates the concerned job is registered to user attributes, when the specified user box is unregistered on the user box storage operation of the copy job and the print job.
In the case of the pubic use box, verify that a user box password registered satisfies the qualities.
Public user box password is composed of 8-digits using ASCII code. 0x20 to 0x7E, except 0x22 and 0x2B   A total of 93 characters is selectable
Also, it shall not be composed of one kind of character.

b. Personal User Box Function

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the personal user box which has a corresponding user attribute with this user attribute.

When the user box to operate is selected, "User Box ID" of the user box is related to the task as a user box attribute in addition to the user attribute. This task is permitted, to the user box file with the user attribute and the user box attribute corresponding to the user attribute and the user box attribute of itself , the printing, the E-mail transmission, the FTP transmission, the FAX transmission, the SMB transmission, download, the removing to other user boxes, and the copy operations to other user boxes.

The user attribute of a personal user box can be changed. If another registered user is specified, it becomes a personal user box that another user manages. If public is specified, it becomes a public user box. In this case, it is necessary to register the public user box password.

c. Public User Box Function

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the public user box which is set the public as the user attribute.

For the access request to each public user box, it authenticates that a user is permitted to use each concerned user box.

It utilizes the 10^{10} session information or more for the access from the network.

It returns "*" for each character as feedback for the entered user box password.

It resets the number of authentication failure when succeeding in the authentication.

In case of the access from the panel, when it fails in the authentication, an input from the panel is not accepted for five seconds.

When the authentication failure that becomes the 1-3 times in total is detected for the public user box concerned, the authentication function to the public user box concerned is locked.

The lock of the authentication function is released with the operation of the lock release function to the public user box of F.ADMIN or the operation of F.RESET function.

The task to act for the user is related the "User Box ID" of the user box as a user box attribute in addition to the user attribute. This task is permitted the user box file, which have been set the public to the user attribute and have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, the E-mail transmission, the FTP transmission, the FAX transmission, the SMB transmission, download, the movement to other user boxes, and the copy operations to other user boxes.

The user attribute of the public user box can be changed. Specify the registered user and change to a personal user box for the registered user.

It changes the public user box password.

6. Secure Print Function (F.PRINT)

This is a series of security function related to the secure print such as the access control function that allows the printing the secure print file after authenticating if a user is the authorized user to use the secure print file for the access to the secure print file from the panel to the identified and authenticated user as a registered user.

a. Authentication function by the secure print password

When the user is identified and authenticated as the registered user, it authenticates that the accessing user is a user to whom the user of the secure print file concerned is permitted, in response to the access request to each secure print file.

Secure print password is composed of 8-digits using ASCII code. 0x20 to 0x7E, except 0x22 and 0x2B A total of 93 characters is selectable
The access from the panel is not accepted for five seconds when the authentication is failed.
It returns "*" for each character as feedback for the entered secure print password.
When the authentication failure that becomes the 1-3 times in total for the secure print file concerned is detected, the authentication function to the secure print file is locked.
The lock status is released with the operation of the lock release function to secure print file of F.ADMIN or the operation of F.RESET function.

b. Access control function to secure print file
The secure print file access control operates when it is authenticated.
The task to act for the user who is identified and authenticated has the secure print internal control ID of the authenticated secure print file for the file attribute.
This task is permitted the printing to the secure print file with a corresponding file attribute to the file attribute of this task.

c. Registration function of a secure print file
    Registration of the secure print password
   For the registration request of secure print file, the registered secure print password is verified to satisfy the following requirements.
    User box password is composed of 8-digits using ASCII code. 0x20 to 0x7E, except 0x22 and 0x2B A total of 93 characters is selectable
    Also, it shall not be composed of one kind of character.
    Giving of the secure print internal control ID
   For the registration request of secure print file, when the verification of the secure print password is completed, the secure print internal control ID uniquely identified is set to the concerned secure print file.

7. All area overwrite deletion function (F.OVERWRITE-ALL)
This executes the overwrite deletion in the data area of HDD and initializes the setting value of the password that is set to NVRAM as well. The object for the deletion or the initialization is as follows.
     Object for the deletion   HDD
    Secure print file
    User box file
    On memory image file
    Stored image file
    Remaining image file
    Transmission address data file
    User ID
    User password
    User box password
    Secure print password
    Remaining TSF data
     Object for the initialization   NVRAM
    Administrator password
    SNMP password
    Operation setting of HDD lock function OFF
    Operation setting of Encryption function OFF
The deletion methods such as the data written in HDD and the written frequency is executed according to the deletion method of all area overwrite deletion function set in F.ADMIN. The HDD lock password and the encryption Passphrase cannot be used for

being turned off the operation setting of the HDD lock function and the encryption function.
The setting of the Enhanced Security function becomes invalid in the execution of this function.

8. Encryption key generation function F.CRYPT
This generates the encryption key to encrypt all data written in HDD by using KonicaMinolta HDD encryption key generation algorithm (SHA-1) that is regulated by the KonicaMinolta encryption specification standard. KonicaMinolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-1.

9. HDD verification function F.HDD
This is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD.
When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. As a result of status check, when the HDD lock password certainly being set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

10. Authentication Failure Frequency Reset Function (F.RESET
This is a function to reset the number of authentication failure counted in each authentication function including the administrator authentication. (Do not relate to the lock is valid or not.)
This function operates by activating TOE such that the main power supply is turned on, or it returns from the power failure. When it starts, the following numbers of authentication failure are reset. The object account locked is released.

    The number of failure to authentication of administrator
    The number of failure to authentication using SNMP password
    The number of failure to authentication of service engineer
    The number of failure to authentication of each user
    The number of failure to authentication of each public user box
    The number of failure to authentication to each secure print

1.5.5 Threat

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

Table 1-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP	- When the leaser returned or the discarded MFP were collected, secure print file, a user box file, on memory image file, the stored image file, the remaining image file, the image-related file, the transmission address data file, and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD in MFP.
T.BRING-OUT-STORAGE	- A secure print file, a user box file, a on-memory image file, a stored image file, a remaining image file, an image-related file, a transmission address data file, and the set-up various passwords can leak by a person or a

	user with malicious intent illegally taking out and analyzing an HDD in MFP. - A person or a user with malicious intent illegally replaces an HDD in MFP. In the replaced HDD, new files of the secure print file, a user box file, on-memory image file, a stored image file, a remaining image file, an image related file, a transmission address data file and set various passwords are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.
T.ACCESS-PRIVATE-BOX	- Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, fax transmission, and SMB transmission).
T.ACCESS-PUBLIC-BOX	- Exposure of the user box file when a person or the user with malicious intent accesses the public user box which is not permitted to use, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission and SMB transmission) and removes and copies to the other user box the user box file.
T.ACCESS-SECURE-PRINT	- Exposure of the secure print file when a person or the user with malicious intent prints the secure print file which is not permitted to use.
T.ACCESS-NET-SETTING	- Malicious person or user changes the network settings that is related to the transmission of a user box file. 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 a user box file is exposed. The network setting which is related to user box file transmission - Setting related to the SMTP server - Setting related to the DNS server - Malicious person or user changes the network setting which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another illegal MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print file is exposed.
T.ACCESS-SETTING	- The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.
T.BACKUP-RESTORE	- The user box file and the secure print file can leak by malicious person or user using the backup function and the restoration function illegally. Also highly confidential data such as password can be exposed and each setting values are falsified.

1.5.6 Organisational Security Policy

There are no organisational security policies required for using the TOE.

1.5.7 Configuration Requirements

The TOE operates on the bizhub C252 / ineo⁺ 251 which is the digital MFP provided by the Konica Minolta Business Technologies, Inc. HDD and the encryption board are option parts and are not equipped as a standard. When option parts HDD and the encryption board are not installed, the function that requires the each of them cannot be used.

1.5.8 Assumptions for Operational Environment

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

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	- 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	- Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.
A.NETWORK	- 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	- Each password and encryption passphrase does not leak from each user in the use of TOE.
A.SETTING	- MFP with the TOE is used after enabling the enhanced security function.
A.SERVER	- When the external server authentication is used for the user authentication method, the user information management server that is connected with the intra-official LAN installing MFP with TOE are performed appropriately the management of the account, access control and patch application, etc.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

<Document for administrator/general user>
1)bizhub C252 User s Guide Security Operations   Ver. 1.01 (Japanese)
2)bizhub C252 User s Guide [Security Operations]   Ver.1.01 (English)
3)ineo⁺ 251 User s Guide [Security Operations]   Ver.1.01 (English)

<Document for service engineer>
1)bizhub C252 Service Manual Security Function (Ver. 1.01) (Japanese)
2)bizhub C252 ineo⁺ 251 Service Manual Security Function (Ver. 1.01) (English)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

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

2.2 Overview of Evaluation Conducted

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

Evaluation has started on Jury, 2006 and concluded by completion the Evaluation Technical Report dated April, 2007. 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 June, September, and November, 2006 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. About that the same process is carried out also in this TOE, and difference, the evaluation facility directly visited the development and manufacturing sites on February, 2007, and conducted the investigation. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on October, and February, 2007.

No concerns were found in evaluation activities for each work unit. Therefore no Observation Report was reported to developer.

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

2.3 Product Testing

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

2.3.1 Developer Testing

1. Developer Test Environment

Figure 2-1 shows the test configurations used by the developer.

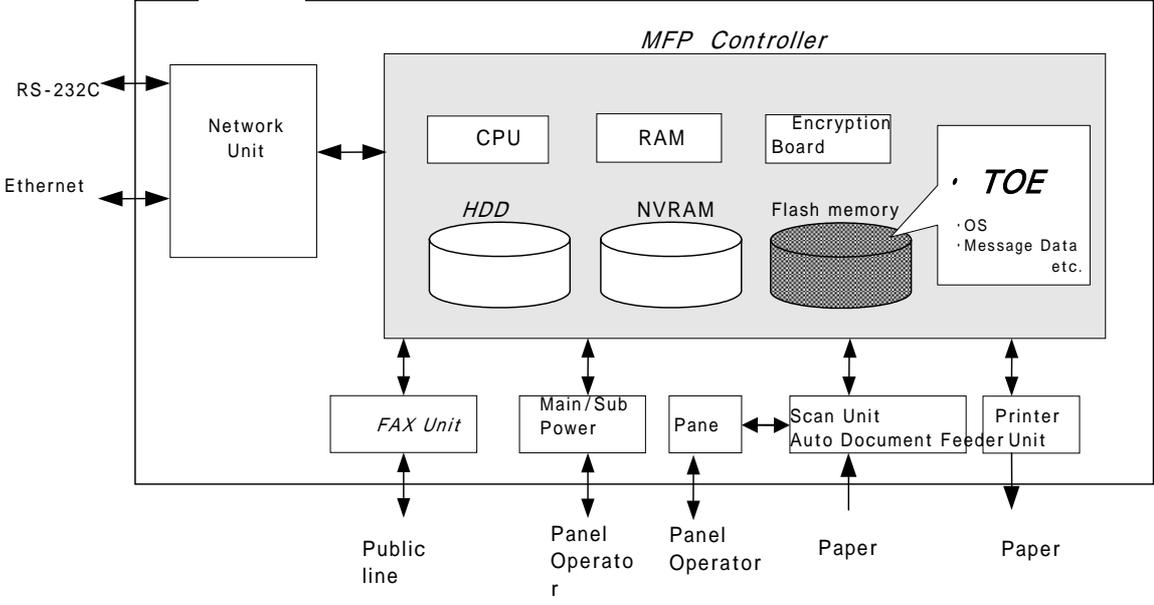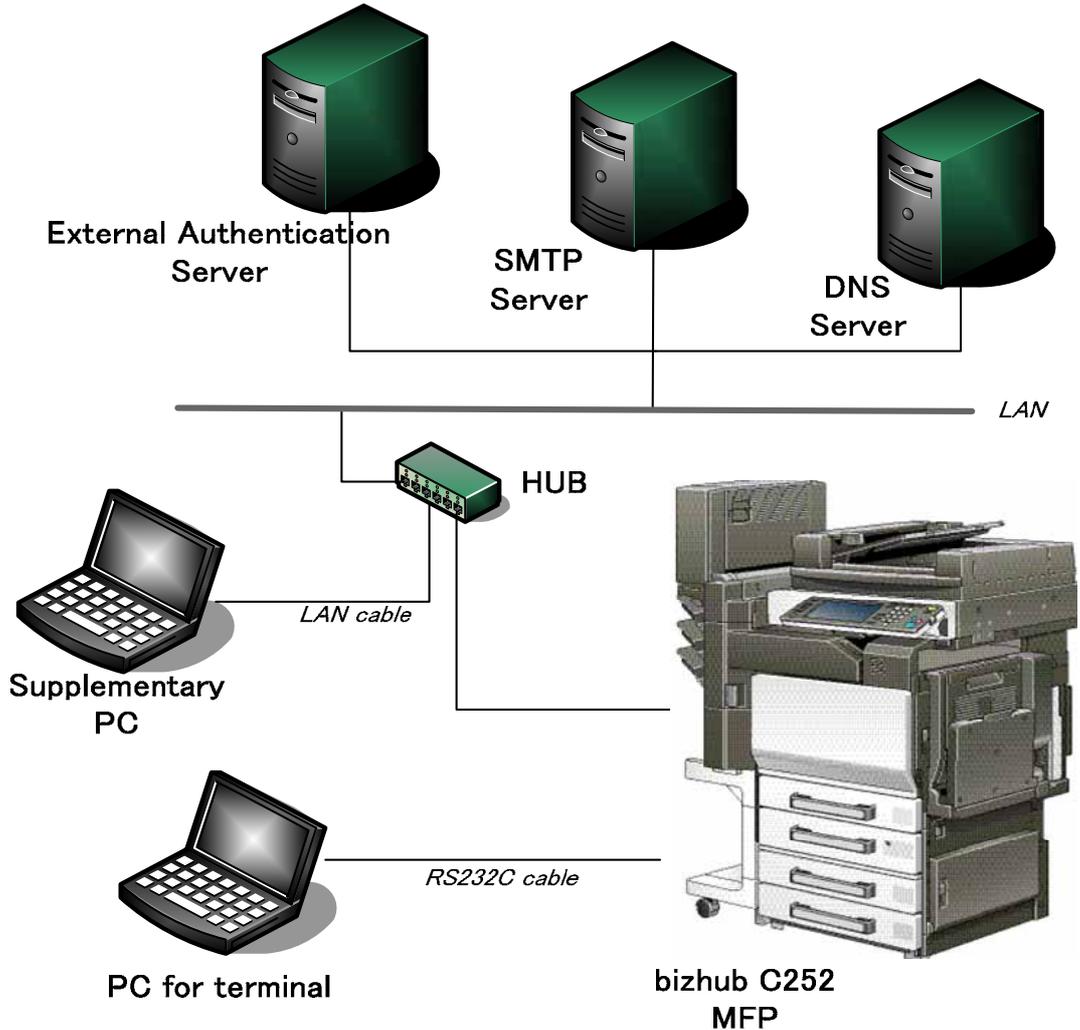Figure 2-1 Developer test configuration

2. Outlining of Developer Testing

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

a. Test configuration

The configurations of the tests performed by the developer are shown in Figures 2-1. Developer testing is performed at the same TOE testing environment with the TOE configuration identified in ST. However, local connection unit (option parts) is eliminated from the configuration of MFP.

b. Testing Approach

For the testing, following approach was used.
1) Check the change of setting values, the authentication method and the check of access control, by using the external interface (panel, network, and power supply OFF/ON) and check the change of output message and its operation, and the behavior of them. In network, it can access using HTTPS protocol, TCP Socket (API of TCP base using for the access from application), Open API (API of XML base using for the access from application) and SNMP (operate MIB) used by PageScope Web Connection (PSWC). About each protocol it can observe the behavior of security function by sending and receiving the test data of each protocol using test tool. Also, it can check by using the test tool that the session information of when using HTTPS protocol or when using OpenAPI, is generated correctly.

2) For the security function that cannot verify by using the interface of 1), it performs the test procedure for each and checks the adequacy of the behavior. Outlining of the concerned test is as follows.
    To check that all area overwrite deletion function operates correctly   HDD is deleted by "0x00 0xFF 0x00 0xFF 0x00 0xFF 0xAA verify," area of use for administrator is initialized, it accepts the method to check by using the tool to dump display of the HDD contents and to edit.
    To check that the encryption key is appropriately generated, it accepts the method to refer directly the data on the memory on the terminal screen connected directly to the machine.
    To check that HDD lock password functions effectively, it accepts the method to check the error occurrence status by exchanging with other HDD that is not set the HDD lock password.

c. Scope of Testing Performed

Testing is performed about 129 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 high-level design and the subsystem interfaces.

d. Result

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

and the actual test results.

2.3.2 Evaluator Testing

1. Evaluator Test Environment

   The evaluator used test configuration that are identical to those used by the developer.
   For the intrusion tests, it was performed by adding two inspection PC instead of terminal PC and using two same MFP (bizhub C252) to perform the test more effectively. Figure 2-2 shows its schematic.
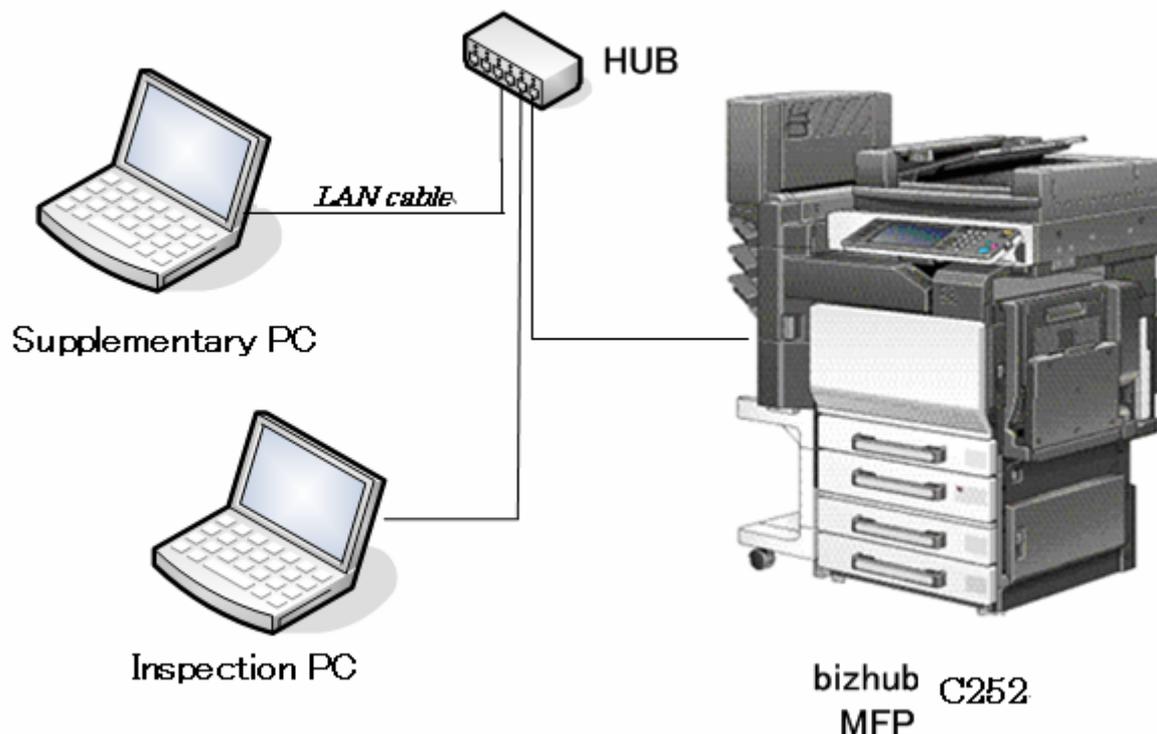

   Figure2 2 Developer test Intrusion test configuration

2. Outlining of Evaluator Testing

   Outlining of testing performed by the evaluator is as follow.

   a. Test configuration

      The configurations of the tests performed by the evaluator are shown in figures 2-1 and 2-2. The evaluator tests were performed in TOE test environments identical to the TOE configuration identified by ST.

   b. Testing Approach

      For evaluator testing, same approach with the developer test was used.

   c. Scope of Testing Performed

      The evaluator performed 62 tests in total: 30 independent tests and 32 sampled developer tests. As the selection criteria of the test, followings take into account.

20

1) Security function that is suspected to operate along the specifications by the developer test.
2) More important security function than other security function
3) Security function set as the object of strength of function.
4) Function that is used from different interface.

Also, intrusion tests performed by evaluator are conducted as follows.
TOE can perform three kinds of operations such as the operation by the panel, the operation through the network by HTTPS protocol, TCP Socket, OpenAPI and SNMP, and the operation by power supply OFF/ON of MFP. The operation by the panel and by power supply OFF/ON of MFP can be considered impossible to perform unauthorized operations such as operation other than assumed usage because of the physical restriction of MFP and operation panel. On the other hand, the operation via the network has broad option and is easy to perform the operation other than expected input.
With a focus on the items related to the network, 8 intrusion tests were invented in consideration of the following 3 points.
1) Verify the truth of insistence based on the vulnerability analysis of developer.
2) Verify the response to the clear vulnerability, that evaluator thinks.
3) Verify the truth of insistence of the strength of function of developer.

Table 2-2 shows the intrusion test item list.

Table 2-2: Intrusion Test Item List

Test No.	Intrusion Testing name for vulnerability test based on [VLA]	Intrusion Test Perspective of idea
VLA-T1	Security objective situation assurance test of network I/F (1)	Perspective 1)
VLA-T2	Security objective situation assurance test of network I/F (2)	Perspective 1)
VLA-T3	Assurance test of official vulnerability	Perspective 1)
VLA-T4	Assurance test of official vulnerability OpenSSL	Perspective 1)
VLA-T5	Security function assurance test against HTTP request	Perspective 2)
VLA-T6	Assurance test of Web server function	Perspective 2)
VLA-T7	Assurance test related to the strength of function	Perspective 3)
VLA-T8	Assurance test for random nature of cookie	Perspective 3)

d. Result

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

2.4 Evaluation Result

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

3. Conduct of Certification

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

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

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

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

4. Conclusion

4.1 Certification Result

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

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
MFP	Multiple Function Peripheral
HDD	Hard Disk Drive
LAN	Local Area Network
IP	Internet Protocol
FTP	File Transfer Protocol
SNMP	Simple Network Management Protocol
NVRAM	Non-Volatile Random Access Memory

The glossaries used in this report are listed below.

MFP Controller	Controller that controls all the operation of MFP including the operation control process received from the network or the MFP panel and the management of image data. TOE is the software that operates on that controller.
Flash Memory	Memory device that performs the high speed and high integration of EEPROM and carried the batch deletion mechanism
PC Print	Send the print data of file desired to print to MFP by using the printer driver from PC. MPF converts the data into image file and prints that image data.

Secure Print	This is the 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	Directory that is created in the HDD area in order to store the image files in the MFP.
Service Engineer	A user who performs the management of maintenance for the MFP. Performs the repair and adjustment of MFP. In general, it is the person in charge at the sales companies or agencies that performs the maintenance service of MFP and that is in cooperation with Konica Minolta Business Technologies, Inc.
Service Mode	Operation panel screen area which can operate MFP function that is prepared for the service engineer.
CE password	Kind of password collating when entering the service mode
Remaining Image File	File that remains in the HDD data area. It is the image file that cannot be deleted by general deletion operation.
Transmission Address Data File	File including address transmitting an image, such as an E-mail address and a phone number etc.
Account Lock	Unable to perform continuous password authentication when the operation of password authentication is failed consecutively, or its situation.

6. Bibliography

[1]   bizhub C252 / ineo+ 251 Control Software Version 1.05 (April 16, 2007) Konica Minolta Business Technologies, Inc

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

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

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

[5]   Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

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

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

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

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

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

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

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

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

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

[15]   Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

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

[17]   bizhub C252 / ineo+ 251 Control Software Evaluation Technical Report ,April 26, 2007, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security