Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2006-6-19 (ITC-6081)
Certification No.	C105
Sponsor	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.
Name of TOE	Japan：bizhub C250P / ineo+ 250P / magicolor 7460CK Zentai Seigyo Software Overseas：bizhub C250P / ineo+ 250P / magicolor 7460CK Control Software
Version of TOE	4038-0100-GM0-11-000
PP Conformance	None
Conformed Claim	EAL3
Developer	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2007-6-27

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center

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

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

Evaluation Result: Pass

“Japan:bizhub C250P / ineo+ 250P / magicolor 7460CK Zentai Seigyo Software

English:bizhub C250P / ineo+ 250P / magicolor 7460CK Control Software version: 4038-0100-GM0-11-000 ” 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.

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

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Japan：bizhub C250P / ineo+ 250P / magicolor 7460CK Zentai Seigyo Software English：bizhub C250P / ineo+ 250P / magicolor 7460CK Control Software” (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 C250P / ineo+ 250P / magicolor 7460CK Zentai Seigyo Software
English：bizhub C250P / ineo+ 250P / magicolor 7460CK Control Software
Version: 4038-0100-GM0-11-000
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. network Printer (bizhub C250P / ineo+ 250P / magicolor 7460CK) (Hereinafter referred to as “Printer”). This TOE is on the flash memory on the Printer controller carried in Printer, and this controls the whole operation of Printer such as the operation control processing and the image data management received from the panel of Printer body or the network.
This TOE offers the protection from exposure of the highly confidential document stored in the Printer, 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 Printer. 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 Printer controller.

1.2.3 Scope of TOE and Overview of Operation

This TOE exists on the flash memory on the Printer controller, which built in the body of the Printer, and is loaded on the RAM. Figure 1-1 shows the relationship between this TOE and the Printer. Shaded region on the figure 1-1 indicates the TOE and "*" shows the option parts of Printer.

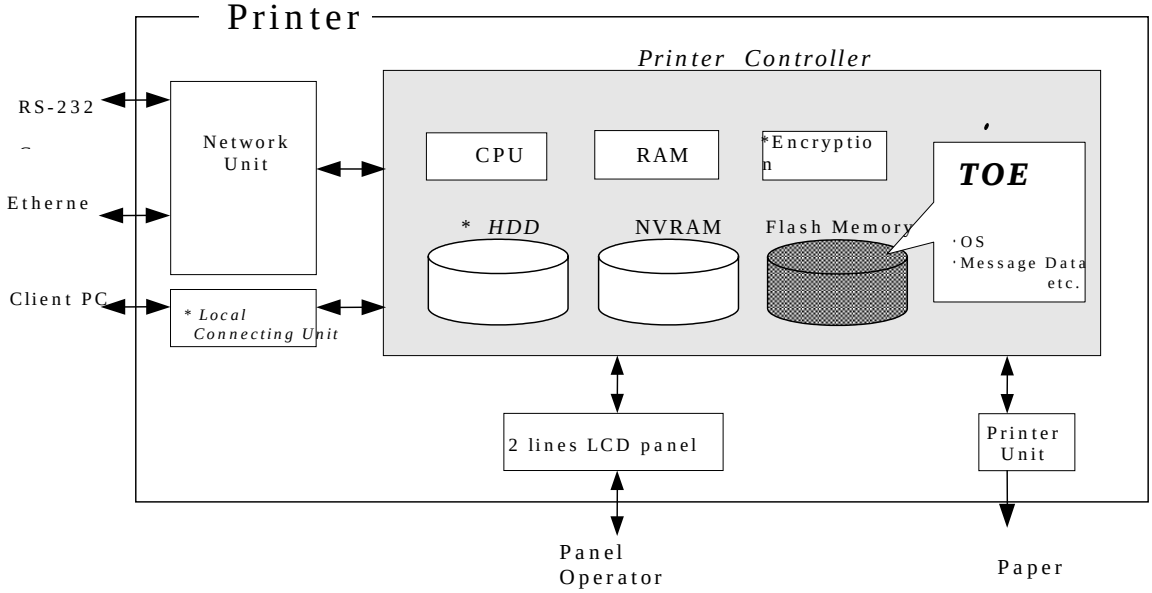


Figure 1-1：Hardware structure that relates to TOE

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, encryption passphrase, etc).

HDD, offered as the option parts, 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 all data including image data written to the HDD as the hardware-based function.

Next, the logical structure of this TOE is shown. Printer includes the function that is not associated with the security directly such as basic function, remote diagnosis function, and setup function other than the function that is indicated in "1.2.4 TOE

functionality".

Basic function performs the core control in the operation of functions acquired print from PC.

Remote diagnosis function is used for managing the operation status of Printer, 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 printer support center run by the subsidiaries of the Konica Minolta Business Technologies, Inc.

Setup function offers the function to setup by using the special installing software operating on the PC by connecting with client PC via RS-232C. Special installing software is the one used only by service engineer and it does not be provided to user. Also, this function is prohibited to use when enhanced security function is active.

Printer 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 Printer are defined as follows.

1) User

Printer's user who prints from PC by using printer (In general, the employee in the office is assumed.)

2) Administrator

Printer's user who carries out the management of the operation of Printer. An administrator performs the operation management of Printer 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 Printer. Service Engineer performs the repair and adjustment of Printer. (In general, the person in charge at the sales companies that performs the maintenance service of Printer and is in cooperation with Konica Minolta Business Technologies Inc. is assumed.)

4) Person in charge at the Organization that uses the Printer

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

5) Person in charge at the Organization that manages the Maintenance of the Printer

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

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. The access of user is controlled by using the password set to the user box.

TOE offers the functions to the user box and the image file in a user box such as printing of image file in the user box, moving or copying to the other user box, 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, from the panel or the network unit. (Upon request via the network from the client PC.)

3) 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 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.

4) Service Engineer Function

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

5) 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.

6) 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 and as for the starting operation of Printer, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the Printer. (Even if HDD is taken out, it is impossible to use it excluding the Printer that the concerned HDD installed.)

7) 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 user box.

Moreover, when the stored data have physically been separated from the jurisdiction of a user, such as the use of Printer 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.

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 Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in bizhub C250P / ineo+ 250P / magicolor 7460CK Zentai Seigyo 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 issued on June 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 “SOF-basic” as its minimum strength of function.
This TOE assumes the use in the general office environment that is protected from the attack of the external network. The access via the panel or the internal network to TOE is under the management by the administrator and does not assume the complex attack. Therefore, it is reasonable to assume the attacking ability to attacker is “low-level.”

Thus, it is adequate with the SOF-Basic.

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 to the administrator mode.

b. 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. And 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 satisfied 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 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 one to three 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 Box Settings

It registers a user box by setting the user password to the unregistered user box ID. It changes the user box password.

User box password is set with 8 digits by using ASCII code（0x20 to 0x7E, except 0x22 and 0x2B）(A total of 93 characters are selectable.)

Also, it shall not be composed of one kind of character.

③ Release of Lock

It resets (0 clear) the number of authentication failure for all secure prints, all user boxes, and SNMP password.

If a secure print, user box or MIB object that access locked exists, the lock is released.

④Setting 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.

⑤Setting and execution of all area overwrite deletion function

The HDD 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

⑥Network Settings

A setup operation of the following setting data is performed.

- A series of setup data that relates to Printer address（IP address, NetBIOS Name, AppleTalk Printer Name, etc.）

⑦Execution 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).

⑧Operation 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）

Return "*" for each character as feedback for the entered HDD lock password in verification.

Also, it shall not be composed of one kind of character.

⑨Operation 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.

Change 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）

Return "*" for each character as feedback for the entered encryption passphrase in verification.

Also, it shall not be composed of one kind of character.

⑩Function 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.

⑪Change 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.

⑫Setting 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.

Reset 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.

①Network Settings

Setting operation of the following setting data is performed.

- A series of setting data that relates to Printer address (IP address, NetBIOS name, AppleTalk printer name, etc.

②Change 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）

③Setting 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 authentication function in service mode accessing from the panel, and a security management function that includes a change in the CE password and the administrator password.

a. Service engineer identification authentication function

It identifies and authenticates the accessing user as the service engineer in

response to the access request to the service mode from the panel.

b. Function offered in service mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the following functions is permitted.

①Change 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）

Return “*” for each character as feedback for the entered CE password.

When the access is from panel, if the authentication is failed, the input from the panel does not be accepted for 5 seconds.

Reset 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.

②Change of administrator password

Change 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）

③Function 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.

④Function to set the operation of setup function

Set whether or not to use (start) the setup function.

⑤Function that relates to password initialization function

The function that relates to the initialization of the password that the service engineer operates is as follows.

- Initialization function

  Function to reset various setting values written in NVRAM to the factory default. The administrator password and the SNMP password are set to an initial value of the factory shipment by executing this initialization function. Both of the operation settings of the HDD lock function and the encryption function are turned OFF. (The HDD lock password and the encryption passphrase have been set cannot be used again by turning OFF the setting operation.)

- HDD physical format function

  The function to rewrite the entire disk to a regulated pattern in HDD including the signal rows such as the track and sector information. The HDD lock function is turned OFF along with the execution of this physical format. (The HDD lock password that is set cannot be used again by turning OFF the operation setting.)

4)User Box Function (F.BOX)

This is a series of security function related to the user box such as the access control function to permit various operations of the concerned user box and the user box file after the authenticating a user as the permitted user to use the user box for the access to the user box

a. Registration of user box

Set the user box password to the non-registration user box ID selected, and register a user box.

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. Authentication function for the access to User Box

For the access request to 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.

Return “*” for each character as feedback for the entered user box password.

Reset 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 user box concerned, the authentication function to the user box concerned is locked.

The lock of the authentication function is released with the operation of F.RESET function.

c. Access Control tot eh user box file in the user box

The task to act for the permitted user to use the user box is related to the user box ID of the user box as the user box attribute.

The task is permitted the printing, the moving to the other user box and copying to other user box, for the user box file which has corresponding user box attributes with the user box attributes of the task.

d. Change of User Box Password

Change if the quality of the user box password of the user box is satisfied.

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.

5) 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.

Return “*” 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 task to act for the user who is permitted to use the secure print file 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

① Verification 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.

- 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）
- Also, it shall not be composed of one kind of character.

② 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.

6) 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
- Image related file
- 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.

7) Encryption key generation function（F.CRYPT）

This generates the encryption key to encrypt all data written in HDD by using Konica Minolta HDD encryption key generation algorithm (SHA-1) that is regulated by the Konica Minolta encryption specification standard. Konica Minolta 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.

8) 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.

9) 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 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-PRINTER	･When the leaser returned or the discarded Printer 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, and the set various passwords (administrator password, SNMP password, HDD lock password, encryption passphrase password, secure print password, user box password) can leak by the person with malicious intent taking out and analyzing an HDD in Printer.
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 and the set-up various passwords (secure print password, user box password) can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in Printer. ･A person or a user with malicious intent illegally replaces as HDD in Printer. 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 and set various passwords (secure print password, user box password) are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.

T.ACCESS-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 prints 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 setting which set in Printer to identify Printer itself where TOE installed, by setting to the value of the entity such as another illegal Printer from the value of Printer (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 is no organizational security policy assumed to be applied to this TOE.

1.5.7 Configuration Requirements

The TOE operates on the bizhub C250P / ineo+ 250P / magicolor 7460CK which is the network printer provided by the Konica Minolta Business Technologies, Inc. The Encryption board is the option and so is not equipped as a standard. When the encryption board is not installed, the function that relates to the encryption 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 the series

	of permitted operations given to them.
A.NETWORK	･The intra-office LAN where the Printer with the TOE will be installed is not intercepted. ･When the intra-office LAN where the Printer with the TOE will be installed is connected to an external network, access from the external network to the Printer is not allowed.
A.SECRET	･Each password and encryption passphrase do not leak from each user in the use of TOE.
A.SETTING	･The Printer with the TOE is used after enabling the enhanced security function.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Documents attached to the TOE are listed below.

＜Document for administrator / general user＞

1)bizhub C250P User's Guide Security Operations （Ver.：1.02）(Japanese)

2)bizhub C250P User's Guide [Security Operations] （Ver.1.02）(English)

3)ineo+ 250P User's Guide [Security Operations] （Ver.1.02）(English)

＜Document for service engineer＞

1)bizhub C250P Service Manual Security Function (Ver. 1.02) (Japanese)

2)bizhub C250P / ineo+ 250P / magicolor 7460CK
Service Manual Security Function (Ver. 1.02) (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 June,2006 and concluded by completion the Evaluation Technical Report issued on June 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 October in 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. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on March 2007 and development environment checking at a development corporation companion May 2007.

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

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

2.3 Product Testing

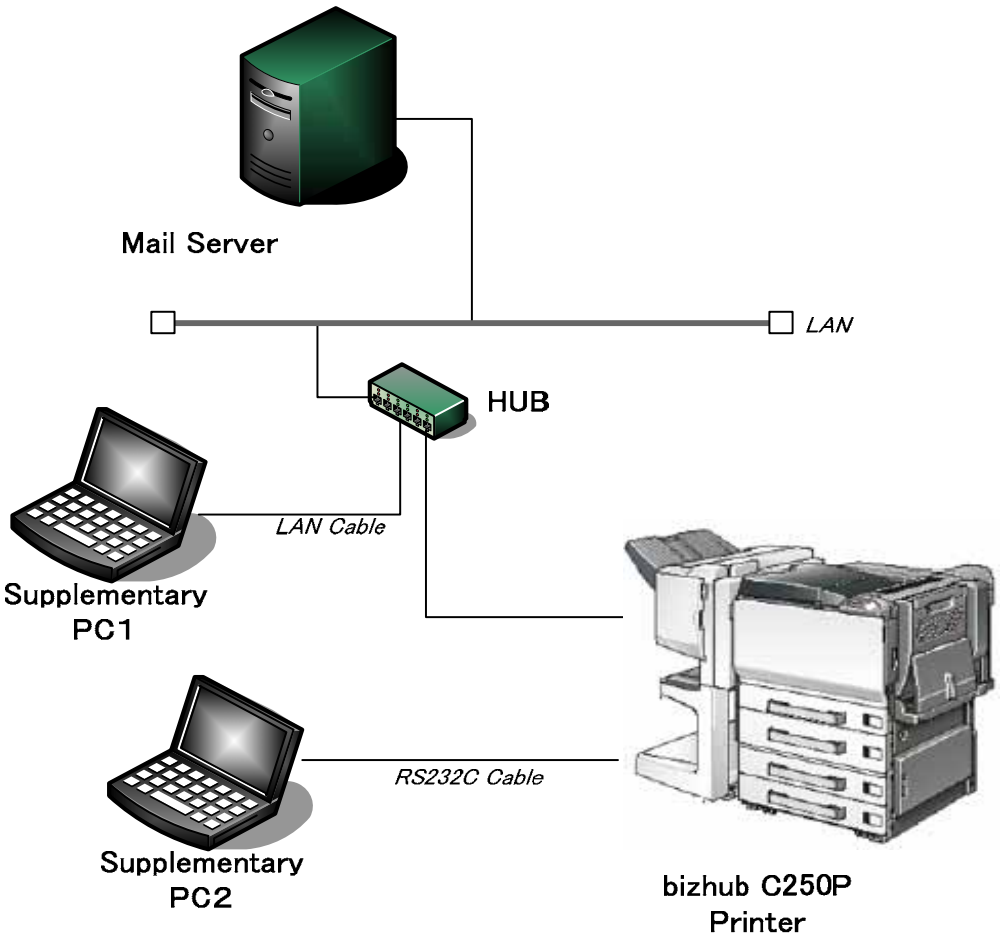
Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

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

<insert Figure>



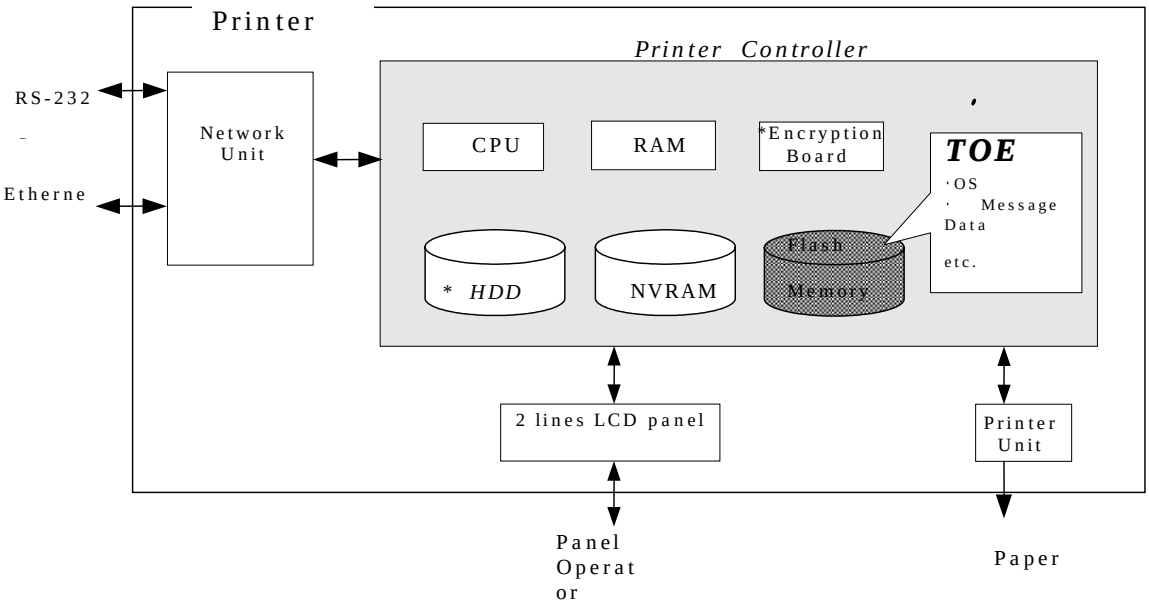


Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

a. Test Configuration

The configurations of the tests performed by the developer are shown in Figure 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 Printer. Also, two types of products that embedded the TOE exist including bizhub C250P (bizhub C250P/ ineo+ 250P/ magicolor 7460CK), but the printer which was used for the test is bizhub C250P. ineo+ 250P is the OEM product of bizhub C250P and magicolor 7460CK is same as bizhub C250P except paper unit and desk (stand), and so these can be seen as the same environment. The test is performed only by the bizhub C250P.

b. Testing Approach

For the testing, following approach was used.

① Check the change of setting values, the authentication method and the 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). Each protocol can observe the behavior of security function by sending and receiving the test data of each protocol using test tool and Web browser. 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.

②For 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 76 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 with the same configuration. Figure 2-2 shows its schematic.

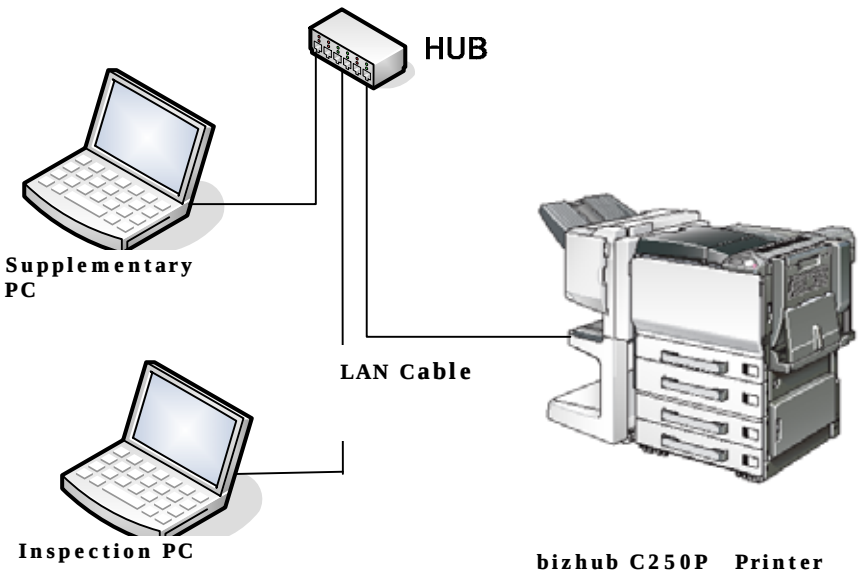


Figure2-2 Developer test （Intrusion test）configuration

2) Outlining of Evaluator Testing

a. Test configuration

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

b. Testing Approach

For the evaluator testing, the approach that is same as the developer test was used.

c. Scope of Testing Performed

The evaluator performed 46 tests in total: 18 independent test and 28 sampled developer tests. As the selection criteria of the test, followings take into account.

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 Printer. The operation by the panel and the power supply OFF/ON of Printer can be considered impossible to perform the unauthorized operations such as operation other than assumed usage because of the physical restriction of Printer and the 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, 9 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.

Table2-2 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	Perspective①
VLA-T4	Assurance test of official vulnerability (OpenSSL)	Perspective①
VLA-T5	Security function assurance test against HTTP request	Perspective②
VLA-T6	Assurance test of Web server function	Perspective②
VLA-T7	Assurance test related to the strength of function	Perspective③
VLA-T8	Assurance test for random nature of cookie	Perspective③
VLA-T9	Setting Assurance test of setup function	Perspective①

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.

No concerns were found in certification process.

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
HDD	Hard Disk Drive
LAN	Local Area Network
IP	Internet Protocol
SNMP	Simple Network Management Protocol
NVRAM	Non-Volatile Random Access Memory

The glossaries used in this report are listed below.

Printer Controller	Controller that controls all the operation of Printer including the operation control process received from the network or the Printer 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.
Secure Print	This is the printing method that restricts by the password authentication. Print data of file which is desired to print by using the printer driver from PC is sent and a printer driver exchanges that data into image file by the printer. To print that image data, specify the password by the printer driver and printing by printer 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 Printer.
Service Engineer	A user who performs the management of maintenance for the Printer. Performs the repair and adjustment of Printer. In general, it is the person in charge at the sales companies or agencies that performs the maintenance service of Printer and that is in cooperation with Konica Minolta Business Technologies, Inc.
Service Mode	Operation panel screen area which can operate Printer 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.
Account Lock	Unable to perform continuous password authentication when the operation of password authentication is failed consecutively, or its situation.

6. Bibliography

[1] bizhub C250P / ineo+ 250P / magicolor 7460CK Control Software Security Target Version1.04 (June 1st, 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 C250P / ineo+ 250P / magicolor 7460CK Control Software Evaluation Technical Report Version 2, June 4th, 2007, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security