Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-01-26 (ITC-9245)
Certification No.	C0233
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japanese : bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software English : bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software
Version of TOE	A11U-0100-G10-06
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.
2009-08-21

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

Evaluation Result: Pass

"Japanese：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software, English：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software, Version：A11U-0100-G10-06" 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 "Japanese：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software, English：bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software, Version：A11U-0100-G10-06" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security(hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Konica Minolta Business Technologies, Inc. and provides information to the users and system operators who are interested in this TOE.

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

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

1.1.1 EAL

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

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	Japanese：	bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221
	English：	bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221
Version:	A11U-0100-G10-06	
Developer:	Konica Minolta Business Technologies, Inc.	

1.2.2 Product Overview

bizhub 350, bizhub 250, bizhub 200, bizhub 362, bizhub 282, bizhub 222, ineo 362, ineo 282, ineo 222, VarioLink 3621, VarioLink 2821, VarioLink 2221, which this TOE is installed, are digital multi-function products provided by Konica Minolta Business

Technologies, Inc., composed by selecting and combining copy, print, scan and FAX functions. (Hereinafter all the products are referred to as "MFP".)
TOE is the "control software for bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network. TOE supports the protection function from exposure of the highly confidential documents stored in the MFP. Moreover, for the danger of illegally bringing out HDD, which stores image data in MFP, TOE can prevent the unauthorized access by using the protection function to overwrite at once the data that became unnecessary, HDD lock function installed in HDD, and the encryption function using the encryption board. Besides, TOE has a deletion method compliant with various overwrite deletion standards. It deletes all the data of HDD completely.

1.2.3 Scope of TOE and Security Functions

1.2.3.1 Roles related TOE

The roles related to this TOE are defined as follows.

(1) User
An MPF user who copies, scans, etc. with MFP. In general, the employee in the office is assumed.

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

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

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

(5) Responsible person of the organization that manages the maintenance of the MFP
A responsible person of the organization that manages the maintenance of MFP. Assigns service engineers who manages the maintenance of MFP.

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

1.2.3.2 Scope of TOE and Overview of Operation

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

In Figure 1-1, HDD, FAX Unit, the Encryption board, Local Connecting Unit and Remote Diagnostic Communication Relay Unit marked as * are optional parts of MFP. For the environment of TOE operation, it operates in the state that optional parts are

installed with except the remote diagnostic communication relay unit that cannot be used due to assumptions even if connected.

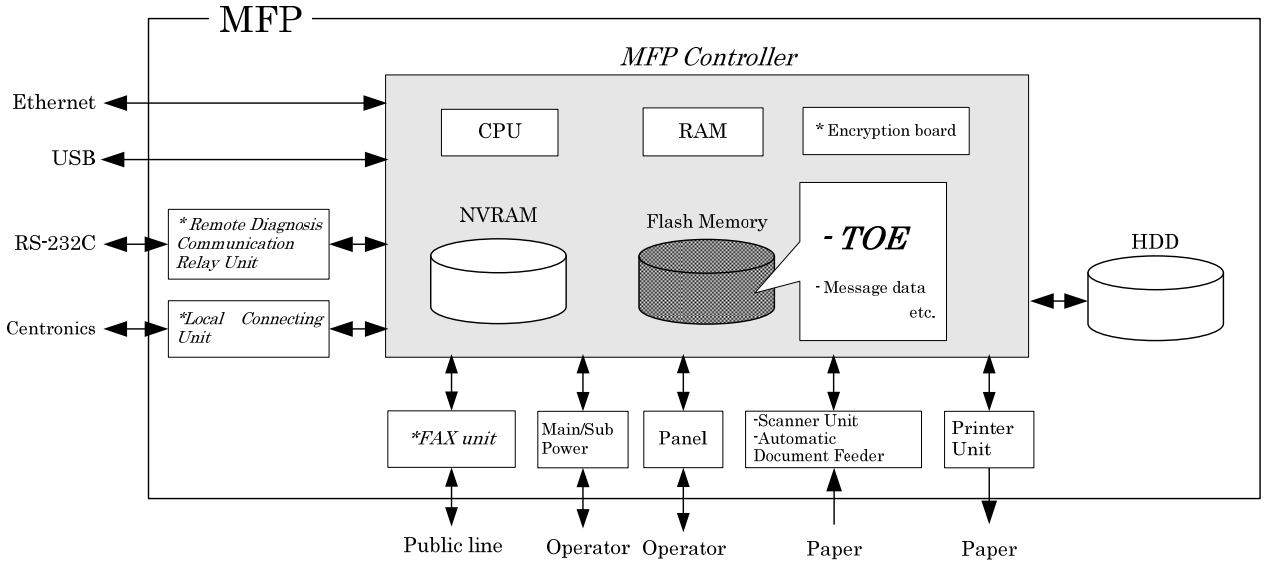

Figure 1-1 Hardware composition relevant to TOE

The components related to TOE are shown as follows.

(1)Flash memory

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

(2)RAM

A volatile memory. This memory medium stores image data.

(3)NVRAM

A nonvolatile memory. This memory medium stores various settings that MFP needs for the operation. (administrator password, transmission address data, etc)

(4)Encryption board (*optional part)

Implemented the encryption function for enciphering all data written in HDD. An integrated circuit for encryption. Encryption Board sold as an optional part is necessary to use security function (encryption function) which encrypts the image data written in HDD.

(5)HDD (*optional part)

Hard disk drive. This is used not only for storing image data as files but also as an area to swap image data that exceeds RAM processing capacity. A security function (HDD lock function) is installed, being possible to set a password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.

HDD sold as an optional part is necessary to use HDD lock function or user box function (described later.)

(6)Panel
An exclusive control device for the operation of the MFP, equipped with a touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

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

(8)USB
Port for the print by local connection

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

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

(11)Printer unit
A device to actually print the image data which were converted for printing when receives a print request from the MFP controller.

(12)FAX Unit (*optional part)
A device used for communications for FAX-data transmission and remote diagnostic (described later) via the public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. However, if this optional part is not installed, it does not affect the operation of security functions.

(13)Local Connecting Unit (*optional part)
Unit for using the printer function with local connection by connecting the client PC and MFP by centronics interface (parallel port). Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. However, if this optional part is not installed, it does not affect the operation of security functions.

(14)Remote Diagnostic Communication Relay Unit (*optional part)
It enables to connect serially via RS-232C. By connecting to the modem that is connected to the public line, the remote diagnostic function (described later) via this interface can be used when any troubles occurred. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. However, this optional part cannot be used due to assumptions even if installed.

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

(1)Basic Function
In MFP, a series of functions for the office work concerning the image such as copy, print, scan, and fax exists as basic functions, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image files, and registers them in RAM and HDD. (For print image files from client PCs, multiple types of conversion are applied.) These image files are converted into data to be printed or sent, and transmitted to the device outside of the MFP controller concerned.

Operations of copy, print, scan, and fax are managed by the unit of job, so that such operations can be aborted, by giving directions from the panel.

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

(3)User Choice Function
User can freely set, including image quality adjustment (magnification and print density, etc.) which are needed to use the basic function, a standard layout, the power saving shift time, and the auto reset time (function that the display of the operation panel returns to a basic screen if it doesn't operate it during the fixed time).

(4)User Box Function
A directory called a “user box” can be created as an area to store image files in HDD. Two types of user box are usable; the one is the public user box which all users can use and the other is the user box used by setting password which can be used individually or among users with sharing password. TOE processes the operation requests to a user box or image files in the user box at the operation request from the panel or from a client PC through a network.

(5)Administrator Function
TOE provides the functions such as the management of user boxes and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

(6)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.

(7)Overwrite delete function of the remaining information
It performs the overwrite deletion of the unneeded image files made by the job termination, the deleting operation by the job management function, the deletion of image files stored in the user box, and the deletion after a lapse of the storage period of image files.

(8)Remote Diagnostic Function
MFP's equipment information such as operating state, setting information of administrator password and the number of printed sheets is managed by making use of multiple connection methods such as E-mail, FAX Unit, and a modem connection through the RS-232C to communicate with the support center of MFP managed by Konica Minolta Business Technologies, Inc. In addition, if necessary, appropriate services (shipment of additional toner packages, account claim, dispatch of service engineers due to the failure diagnosis, etc.) are provided.

(9)Updating Function of TOE
TOE facilitated with the function to update itself. When it receives command from the remote diagnostic function, there is a method to download from FTP server through Ethernet and can update. Also, there is a method that performs by the connection of the compact flash memory medium.
When enhanced security function (described later) is set valid, this updating function of TOE through Ethernet becomes invalid.

(10)Encryption key generation function

Performs encryption/decryption by encryption board when writing data in HDD or reading data from HDD, if the encryption board which is the optional part is installed in MFP controller. (TOE does not process the encryption and description itself.)

The operational setup of this function is performed by the administrator function. When activated, TOE generates the encryption key by the encryption key passphrase that was entered on the panel.

1.2.3.3 Security Functions of TOE

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

- Secure Print File
  Image files registered by Secure Print.

- User Box file
  Image files stored in user box except Public user box.

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

- All User Box Files
  Image files stored in all types of user boxes including Public user box

- Swap Data Files
  Files to constitute images that are generated by copy and PC print of big size that does not fit into an RAM area. (including secure print file).

- Overlay Image Files
  Background image files

- HDD accumulation image files
  Files stored in an HDD from PC print, and printed by the operation from panel

- Remaining Image files
  Files which remain in the HDD data area that is not deleted only by general deletion operation (deletion of a file management area)
  These files do not exist when the enhanced security function is valid.

- Transmission Address Data File
  Files including an E-mail address, a phone number, etc.

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

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

Secondly, TOE verifies the correct HDD and provides overwrite delete function of the

image data written in HDD when it becomes disused, all area overwrite deletion function of HDD and initialization function of settings for NVRAM in order to prevent the leakage of information from HDD and NVRAM where the protected assets are stored in MFP. Moreover, TOE provides HDD lock function outside the TOE and encryption function of data written in HDD using encryption function by the encryption board outside the TOE.

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

1.3 Conduct of Evaluation

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

Scope of the evaluation is as follow;

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

More specific, the evaluation facility examined "bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software Security Target " as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Evaluation is completed with the Evaluation Technical Report dated 2009-08 submitted by the evaluation facility and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

2. Summary of TOE

2.1 Security Problem and assumptions

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

2.1.1 Threat

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

Table 2-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and disposal of MFP)	When leased MFPs are returned or discarded MFPs are collected, secure print files, user box files, on-memory image files, swap data files, overlay image files, HDD-remaining image files, transmission address data files, and various passwords which were set up can leak by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.
T.BRING-OUT-STORAGE (An unauthorized carrying out of HDD)	- All user box files, swap data files, overlay image files, HDD accumulation image files, and remaining image files can leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP. - A person or a user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files such as user box files, swap data files, overlay image files, HDD accumulation image files, and remaining image files are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so that such image files will leak.
T.ACCESS-BOX (Unauthorized access to the user box which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, SMB transmission).
T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file which used a user function)	Exposure of secure print file when a person or a user with malicious intent prints the secure print files that are not permitted to use.
T.UNEXPECTED-TRANSMISSION (Unauthorized change of network setting)	- Malicious person or user changes the network settings that are related to the transmission of a user box files. Even an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that the user box file is exposed. <The network settings which are related to user box file transmission>

	- Setup related to the SMTP server - Setup related to the DNS server - Malicious person or user changes the network settings which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another unauthorized MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print files are exposed.
T.ACCESS-SETTING (An unauthorized change of a function setting condition related to security)	The possibility of leaking user box files and secure print file rises because those malicious including users changes the settings related to the enhanced security function.

2.1.2 Organizational Security Policy

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

2.1.3 Assumptions for Operational Environment

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

Table 2-2 Assumptions in Use of the TOE

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

2.1.4 Documents Attached to Product

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

<Documents for administrator and user>
- bizhub 350 / 250 / 200 User's Guide [Security Function] Ver.101 (Japanese)
- bizhub 362 / 282 / 222 User's Guide [Security Operations] Ver.101 (English)
- ineo 362 / 282 / 222 User's Guide [Security Operations] Ver.101 (English)
- VarioLink 3621 / 2821 / 2221 User's Guide [Security Operations] Ver.101 (English)

<Documents for service engineer>
- bizhub 350 / 250 / 200 Service Manual [Security Function] Ver.1.01 (Japanese)
- bizhub 362 / 282 / 222 / ineo 362 / 282 / 222 / VarioLink 3621 / 2821 / 2221 SERVICE MANUAL [SECURITY FUNCTION] Ver.1.01 (English)

2.1.5 Configuration Requirements

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

- The configuration of bizhub 350, bizhub 250, bizhub 200, bizhub 362, bizhub 282, bizhub 222, ineo 362, ineo 282, ineo 222, VarioLink 3621, VarioLink 2821 and VarioLink 2221, digital MFP provided by Konica Minolta Business Technologies, Inc, equipped with the options such as HDD, Encryption board, FAX Unit and Local Connecting Unit.

2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions.

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

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

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

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

This threat assumes the possibility that the data in HDD leaks by being stolen from

the operational environment under MFP used or by installing the unauthorized HDD and bringing out with the data accumulated in it.

This TOE provides the overwrite delete function of the image data written in HDD when it becomes disused (referred as "overwrite delete function of the remaining information"), so it prevents the leakage of the data in HDD because there are used minimum data in HDD.

TOE prevents the leakage of the data in HDD by the selected function 1, 2, or both.

1. By using HDD lock function that the HDD outside of TOE is not permitted to write before the authentication of HDD lock password, this TOE offers the function working with HDD with HDD lock function (referred as "HDD lock operation support function"), so that it requests the HDD lock password at reading the information from HDD and it prevents the leakage of the protected assets and the security setting values in HDD connected to the MFP that is illegally brought out and analyzed. Moreover, this TOE offers the verifying function that HDD is correct and has HDD lock function (referred as "HDD verification function"), so that information is stored only in the correct HDD with HDD lock function and it prevents the leakage of image data from HDD connected to MFP by taking out the HDD and replacing another HDD without the HDD lock function.
2. By using the encryption function of the encryption board outside of TOE, this TOE offers the generation function of encryption key to encrypt the data written on HDD (referred as "Encryption key generation function") and supporting function with the encryption board (referred as "Encryption kit operation support function"), so that it makes it difficult to decode the data that is encrypted in HDD.

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

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

TOE provides the authentication function on the access of user box, the access control function for user box, the function that limits the changes in settings of user box to administrators and permitted users (referred as "user box function"), so it prevents unauthorized operation by using user functions because the change in settings of user box and the users is limited only to administrators and the permitted users, and the operation of user box is restricted only to the normal users.

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

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

TOE provides the authentication function with secure print password and the access control function for secure print files (referred as "secure print function"), so that the operation of secure print files is restricted only to the normal users, and it prevents unauthorized operation by using user functions.

(5)Security function to counter the threat [T.UNEXPECTED-TRANSMISSION (Unauthorized change of network setting)]

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

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

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

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

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

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

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

3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2009-01 and concluded by completion the Evaluation Technical Report dated 2009-08. 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 2009-05 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-05.

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

3.3 Product Testing

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

3.3.1 Developer Testing

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

1) Developer Test Environment

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

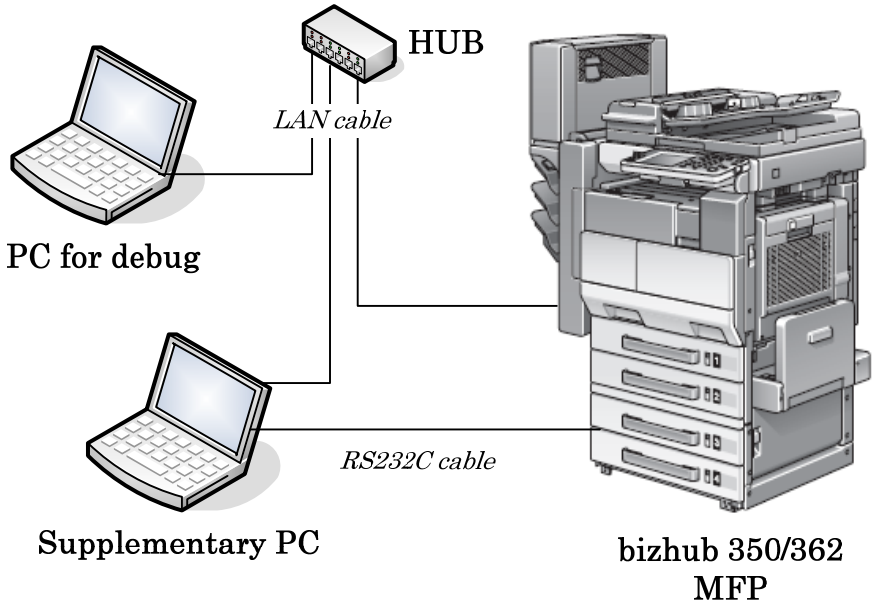

Figure 3-1 Configuration of Developer Testing

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

Only bizhub 350 and bizhub 362 are chosen as MFP which TOE is loaded, however it is judged not to have any problem as a result that the following confirmation was done by evaluator.

- It was confirmed by a document offered from developer that a difference of bizhub 350 and bizhub 250 and bizhub 200 is only copy / print speed and a difference of the durability guarantee value.

- It was confirmed by a document offered from developer that a difference of bizhub 362 and bizhub 282 and bizhub 222 is only copy / print speed and a difference of the durability guarantee value.

- It was confirmed by a document offered from developer that difference of "bizhub 350, bizhub 250, bizhub 200" and "bizhub 362, bizhub 282, bizhub 222" is only a difference of the displayed language.

- The sampling test that picked out the items of developer test performed in bizhub 362 was performed in bizhub 350, and it is confirmed that the results except a difference of the displayed language are same and that security function was not influenced.

2) Outlining of Developer Testing

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

a. Test outline

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

<Testing Approach>
Test was done to execute security functions through external interface when the functions have the external interfaces that developer can use, and was done to

get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that developer can use.

<Tools and others used at Testing>
The tools and others are shown in Table 3-1.

Table 3-1 Tools and others used in developer testing

Name of hardware and software	Outline and Purpose of use
Internet Explorer Ver. 6.0.2800.1106	General purpose browser software. Used to execute PSWC in the supplementary PC.
TORNADO Ver2.1.2	Software to build a develop environment for VxWorks5.x. Boot on PC for debug and enable the executive control of object for debug operating on MFP and debug. Used to gather operation log of MFP.
Tiny FTP Daemon Ver. 0.52d	FTP server software executed in the PC for debug. Used to download executive object from supplementary PC.
Fiddler Ver.1.2.2	Monitor and analyzing tool for Web access of http and etc. Used to analyze communication between MFP and supplementary PC and to perform irregular test.
sslproxy Ver.1.2	SSL-proxy server software executed in the supplementary PC. Used in test using PSWC. By communicating with main body through SSL and with browser software through non-SSL, it makes Fiddler possible to monitor avoiding SSL encryption by sslproxy.
Disk dump editor Ver.1.33	Tool software which boot and can display the contents in the HDD in the supplementary PC. Used to save dumped data with binary format and to analyze it.
Stirling Ver.1.31	Viewer software to view binary format files on the supplementary PC. Used to verify dumped binary data.
Notepad	Text editor attached to Windows2000. Used on supplementary PC to save log data displayed on console of TORNADO as text.
MSG SOFT MIB Browser Professional SNMPv3 Edition Ver. 10.0.0.4044	MIB exclusive browser software executed in the supplementary PC. Used for confirmation test of the write prohibition of the SNMP v1/v2/v3.
Blank Jumbo Dog Ver. 4.1.3	Simple server software for intranet. Used as E-mail and FTP server function in transmission test of user box file.
OPENSSL-0.9.8-Win 32	Encryption tool software for SSL and hash function executed in the supplementary PC. Used to verify of HDD encryption key generation.
Tera Term Pro Ver.4.29	Terminal software executed in the supplementary PC. Used to gather operation log of MFP.
NMAP 4.01	Port scan software executed in the supplementary PC. Used in the test of restricted function after the enhanced security is set.
WireShark	Network packet analyzer software executed in the

Name of hardware and software	Outline and Purpose of use
0.99.5	supplementary PC. Used to record log of restricted function after the enhanced security is set.
PageScope Web Connection (PSWC) Ver. A11U-0100-G10-06	Tool it is had built-in MFP and to perform the state confirmation and the setting of MFP using browser.
KONICA MINOLTA 362/282/222 Driver ver1.01	Used in the test to store in user box and secure print. In case of bizhub 350/250/200, use printer driver for them.

b. Scope of Testing Performed

Testing is performed about 33 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. Result

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

3.3.2 Evaluator Independent Testing

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

1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.
Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

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

<Viewpoints of Test>
(1)Based on the situation of developer test, test as many security functions as possible.
(2)Test targets are all probabilistic and permutable mechanism.
(3)Test the behavior depending on the differences of password input methods to TSFI for the test of the probabilistic and permutable mechanism.
(4)Test the security functions available regardless of installing optional part or not.
(5)For the interfaces with innovative and unusual character, test the necessary variations.

b. Outlining of Evaluator Independent Testing

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

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

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

<Test viewpoints and testing outline>
Test outline for each independent test viewpoint is shown in Table 3-2.

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

Viewpoints of Independent Test	Overview of Testing
(1) Viewpoint	Tests were performed that were judged to be necessary in addition to developer tests.
(2) Viewpoint	Tests were performed with changing the number of letters and the types of letters by paying attention to the probabilistic and permutable mechanism at identification and authentication or etc. by the user.
(3) Viewpoint	Tests were performed with considering the operated interfaces to confirm the behavior depending on the difference of password input method.
(4) Viewpoint	Tests were performed to confirm the action of the secure print function in the different condition that HDD is installed or not.
(5) Viewpoint	Tests were performed with judging the functions being innovative and unusual character to confirm the action of the encryption key generation function and the encryption board operation support function.

c. Result

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

3.3.3 Evaluator Penetration Testing

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

1) Outlining of Evaluator Penetration Testing

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

a. Vulnerability of concern

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

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

b. Scope of Test Performed

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

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

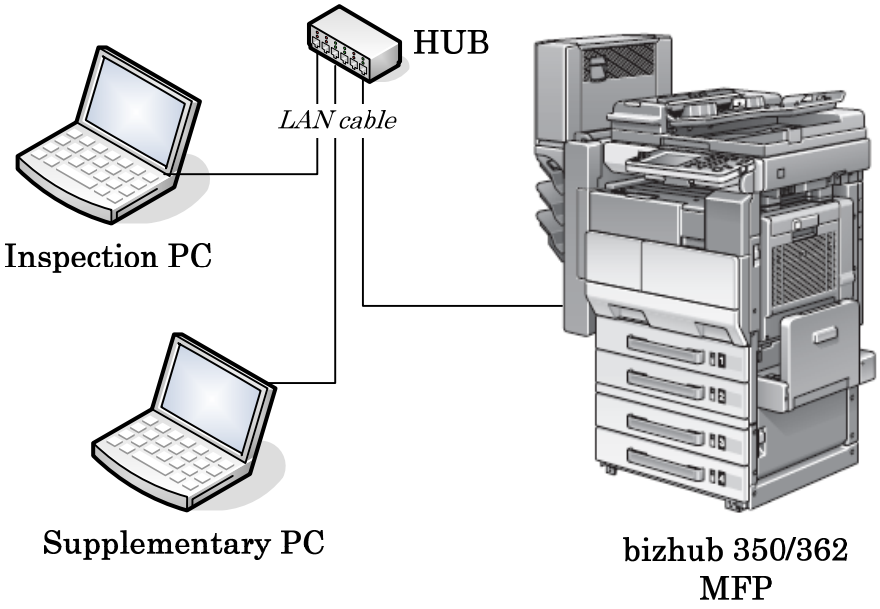

Figure 3-2 Configuration of Penetration Testing

<Testing Approach>
Tests were done to use the following methods; method to check by the visual observation of the behavior after stimulating TOE with operating from the operational panel, method to check by the visual observation of the behavior after accessing TOE through network with operating the supplementary PC, method to check by the test tool of the behavior after tampering parameters by using test tool, method to scan the publicly known vulnerability by the vulnerability checking tool with operating the inspection PC.

<Tools and others used at Testing>
The tools etc. used at tests are shown in Table 3-3

Table 3-3 Tools and others used at Penetration Testing

Test Configuration Environment	Details
Inspection object (TOE)	- TOE installed in bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 (Version: A11U-0100-G10-06) - Network configuration Penetration Tests were done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows 2000 (SP4). - Using the tools shown in table 3-1. (Fiddler, TamperIE etc.) - Access the MFP by using PSWC (abbreviation of "PageScope Web Connection"), HTTPS etc. and it can setup the network etc. Furthermore possible to use TamperIE.
Inspection PC	- Inspection PC is a PC with network terminal operated on Windows XP SP2, and is connected to

	MFP with cross-cable to perform penetration tests. - Explanation of test tools. (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8d encryption too of SSL and hash function (3)Nesuss 3.2.1 build 2G299_Q Security scanner to inspect the vulnerability existing on the System (4)TamperIE 1.0.1.13 Web proxy tool to tamper the transmitted data from general Web browser such as Internet Explorer to arbitrary data. (5)sslproxy Version 2.0 SSL proxy server software (6)Fiddler 2.2.0.7 Web debugger to monitor HTTP operation provided by Microsoft Corporation. (7)Wireshark 1.06 Packet analyzer software that can parse protocols more than 800. (8)Nikto Version 2.03 CGI and publicly known vulnerability inspection tool

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

Table 3-4 Concerned vulnerabilities and Overview of Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and behavior inspection.
(2) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and result analysis.
(3) Vulnerability	Tests were performed to confirm that there is no influence on the security behavior by transmitting of edited parameters through network.
(4) Vulnerability	Tests were performed to confirm that the forced power ON/OFF does not affect the security function of initialization process, screen display and etc.
(5) Vulnerability	Tests were performed to confirm the exclusive control being done by the access from operational panel and network simultaneously.
(6) Vulnerability	Tests were performed to confirm that the setting state of encryption key passphrase does not affect the behavior of the security function.

c. Result

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

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

To counter the threat [T.BRING-OUT-STORAGE (Unauthorized bring-out of HDD)], user can select HDD lock operation support function + HDD verification function, encryption board operation support function + encryption key generation function or both. When only HDD lock operation support function + HDD verification function is selected, pay attention to the following points.

- The analysis for direct reading of lock password from HDD is judged to be a residual vulnerability because it needs to use the specific devices. But it's quite possible of lock password to be easily analyzed because the specific devices and decoding services are provided at a low-price and abused. Therefore for the consumers who take this issue as a threat, it's preferable to consider the encryption of image data using optional encryption function

4. Conduct of Certification

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

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

5. Conclusion

5.1 Certification Result

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

5.2 Recommendations

- If FAX Unit or Local Connecting Unit which is option is not installed, it does not affect the operation of security functions.

6. Glossary

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

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

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

DNS:	Domain Name System
FTP:	File Transfer Protocol
HDD:	Hard Disk Drive
HTTPS:	HyperText Transfer Protocol Security
MFP:	Multiple Function Peripheral
MIB:	Management Information Base
NVRAM:	Non-Volatile Random Access Memory
RAM:	Random Access Memory
SMB:	Server Message Block
SMTP:	Simple Mail Transfer Protocol
SNMP:	Simple Network Management Protocol
SSL:	Secure Socket Layer

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

DNS:	Protocol to manage the relationship of the domain name and IP address in the internet.
FTP:	File Transfer Protocol used at TCP/IP network.

HDD lock function:
Function that the password other than coinciding with the password set in HDD stops to read and write.

HDD lock password:
Password that releases the forbidden state to read and write on HDD.

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

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

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

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

Public Box: User box which all users can use.

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

SMTP: Protocol to transfer e-mail in TCP/IP.

SNMP: Protocol to manage various devices through network.

SSL/TLS: Protocol to transmit encrypted data through the Internet.

Encryption key passphrase:
Original information to generate the encryption key to encrypt and decrypt on the encryption board.

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

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

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

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

Secure Print file:
Image file registered by secure print.

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

allowed only when that password is authenticated.

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

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

User Box file: Image file stored in the user box except “public”.

7. Bibliography

[1] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software Security Target Version 1.03 (Aug 5, 2009)
Konica Minolta Business Technologies, Inc.

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

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

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

[5] Common Criteria for Information Technology Security Evaluation Part 1:
Introduction and general model Version 3.1 Revision 1, September 2006,
CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2:
Security functional requirements Version 3.1 Revision 2, September 2007,
CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3:
Security assurance requirements Version 3.1 Revision 2, September 2007,
CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1:
Introduction and general model Version 3.1 Revision 1, September 2006,
CCMB-2006-09-001 (Translation Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2:
Security functional requirements Version 3.1 Revision 2, September 2007,
CCMB-2007-09-002 (Translation Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3:
Security assurance requirements Version 3.1 Revision 2, September 2007,
CCMB-2007-09-003 (Translation Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation:
Evaluation Methodology Version 3.1 Revision 2, September 2007,
CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation:
Evaluation Methodology Version 3.1 Revision 2, September 2007,
CCMB-2007-09-004 (Translation Version 2.0, March 2008)

[13] bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software Evaluation Technical Report Version 2, Aug 12, 2009
Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security