Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-01-06 (ITC-9243)
Certification No.	C0232
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	bizhub C253 / bizhub C203 PKI Card System Control Software
Version of TOE	A02E0Y0-0100-GN0-U4
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.
2009-08-17

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

"bizhub C253 / bizhub C203 PKI Card System Control Software" 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 "bizhub C253 / bizhub C203 PKI Card System Control Software, Version : A02E0Y0-0100-GN0-U4" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Konica Minolta Business Technologies, Inc. and provides information to the users and system operators who are interested in this TOE.

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

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

1.1.1 EAL

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

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	bizhub C253 / bizhub C203 PKI Card System Control Software
Version:	A02E0Y0-0100-GN0-U4
Developer:	Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

bizhub C253, bizhub C203 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 "bizhub C253 / bizhub C203 PKI Card System Control Software" 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 function to print the encryption print realized by using a special printer driver and IC card by using exclusive driver (loadable driver) and the IC card that is used generating that encryption print for a printer data transmitted to MFP from client PC among the highly confidential document exchanged between MFP

and client PC. Moreover, TOE can prevent the unauthorized access to the image data written in HDD for the danger of taking HDD, which stores image data temporarily in MFP, out illegally by using the HDD lock function loaded on the HDD or the encryption all the data written in HDD including image data 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
A MFP user who owns IC card. (In general, the employee in the office is assumed.)

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

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

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

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

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

1.2.3.2 Scope of TOE and Overview of Operation

TOE is the software that controls the entire operation of MFP 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, FAX unit, the encryption board and the card reader marked as * are optional parts of MFP. For the environment of TOE operation, the card reader and the encryption board (in case that the encryption function of the stored data in HDD is selected) is installed, and the FAX unit is installed in case that Fax function is used.

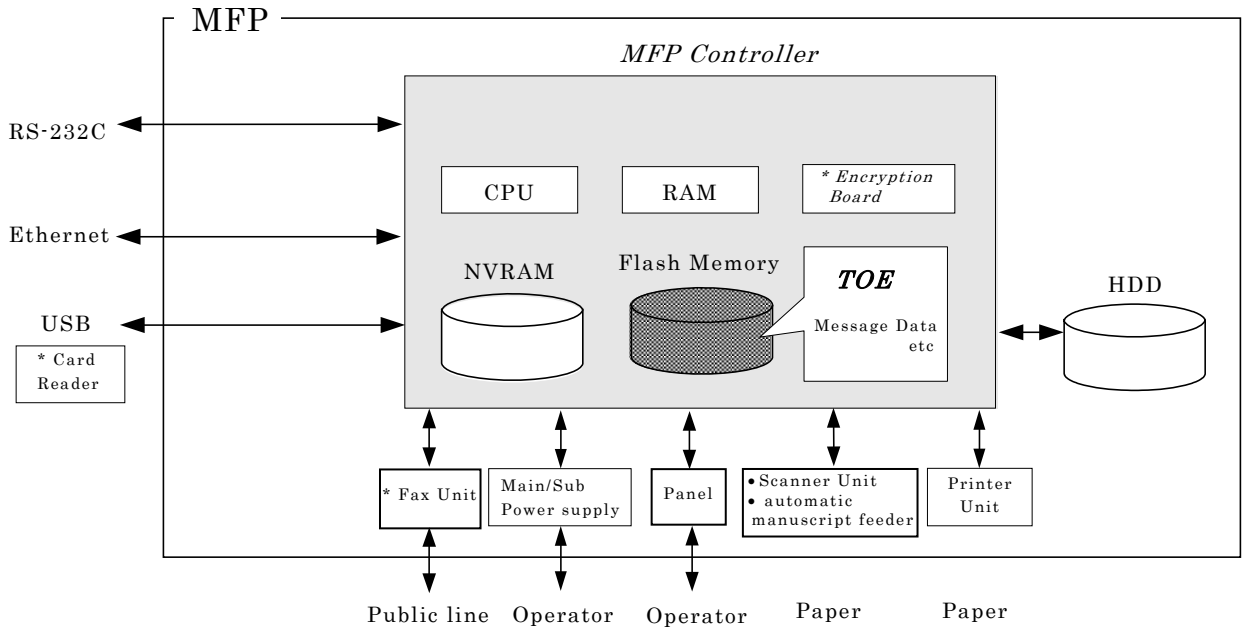

Figure 1-1 Hardware composition relevant to TOE

The components related to TOE are shown as follows.

(1)Flash memory

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

(2)NVRAM

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

(3)Encryption Board (*Option)

An integrated circuit for specific applications which implements an encryption function for enciphering the data written in HDD.
Encryption Board sold as an optional part is necessary to work encryption function.

(4)HDD

A hard disk drive of 60GB in capacity. This is used not only for storing image data as files but also as an area to save image data and destination data temporarily during extension conversion and so on. Also, the exclusive drivers for accessing an IC card are stored here.
The security function (HDD lock function) is installed, being possible to set the 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.

(5)Main/sub power supply

Power switches for activating MFP

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

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

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

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

(10)USB/ Card Reader (*Option)
Besides a printing from a USB memory, it can be connected with a card reader corresponded to IC card. A card reader is not pre-installed in MFP as a standard according to the circumstances in sales, but sold as an optional part. It is an essential component under this ST assumption.

(11)IC Card
An IC card that supports the standard specification of Common Access Card (CAC) and Personal ID Verification (PIV)

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

(13)FAX Unit (*Option)
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.

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. In addition, various functions are realized with IC card.
Operations of copy, print, scan, and fax are managed by the unit of job, so that operation priority can be changed by giving directions from the panel, finishing of print jobs can be changed, and such operations can be aborted.

(2) Encryption Print Function

A print file is stored as standby status remaining encrypted when the encrypted print file, which is generated from the exclusive printer driver of the client PC, is received.

Printing is performed by a print direction from the panel by decrypting an encrypted print file through the PKI processing using IC card.

(3) Scan To Me Function

IC card owner can transmit scan images from MFP to own e-mail address through PKI processing using IC card. Following two functions are usable.

[S/MIME Encryption Function]

Scan image is encrypted as S/MIME mail data file when transmitting an image file scanned by user to mail address.

[Digital Signature Function]

Signature data is added to verify a mail sender and guarantee a mail data as S/MIME mail data file, when transmitting image files scanned by a user to mail address. This function eliminates the possibility to receive a falsified file erroneously on the communication.

(4)Administrator Function

TOE provides the functions such as the management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate from the panel.

(5)Service Engineer Function

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

(7)Encryption Key Generation Function

When the encryption board, an optional product, is installed in MFP controller, encryption/decryption is performed by the encryption board when writing data in HDD or reading data from HDD. (TOE does not process the encryption and description itself.)

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

(7)Remote Diagnostic Function

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

The use of this function is prohibited by the assumptions.

(8)Updating Function of TOE

TOE facilitated with the function to update itself. As for the update means, there are a method that exists as one of items of remote diagnostic function, a method that downloads from FTP server through Ethernet (TOE update function via Internet), and a method that performs the connection of the compact flash memory medium.

The use of TOE update function via Internet is prohibited by the assumptions.

1.2.3.3 Security Functions of TOE

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

- Encrypted print file
  An encrypted image file generated, sent and stored in MFP by using the exclusive printer driver and IC card from client PC.

- Scanned image file
  An image file scanned on the spot by MFP.

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

- Encrypted print file

- Scanned image file

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

- Stored Image File
  Stored image files other than encrypted print file

- HDD 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).

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

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

Firstly, TOE uses the lock function for HDD and the encryption function of image data written in HDD by the encryption board outside of TOE, and provides the verification function the correct HDD at the MFP power ON, all area overwrite deletion function of HDD and the initialization function of set values for NVRAM in order to prevent the leakage of information from HDD and NVRAM where the protected assets are stored in MFP.

Secondly, TOE provides the function to encrypt and transmit image files transmitted from MFP to client PC in order to protect securely the image file (scanned image file) transmitted from MFP to client PC. Moreover, TOE provides the function to add signature, using IC card outside of TOE, on transmitted image files from MFP to client PC and transmit them.

Thirdly, TOE provides the function that only user who made transmitted image files can decrypt and print them, using IC card outside of TOE, in order to prevent unauthorized user from printing the image file (encrypted print file) transmitted from client PC to MFP.

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

1.3 Conduct of Evaluation

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

Scope of the evaluation is as follow;

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

More specific, the evaluation facility examined "bizhub C253 / bizhub C203 PKI Card System Control Software" 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 C253 / bizhub C203 PKI Card System Control Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Evaluation is completed with the Evaluation Technical Report dated 2009-08 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.

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, encrypted print files, scanned image files, on-memory image files, stored image files, HDD remaining image files, image-related files, and highly confidential information such as the setup various passwords 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)	-Encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up can leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP. -A person or a user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files such as encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so that such image files will leak.

2.1.2 Organizational Security Policy

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

Table 2-2 Organizational Security Policy

Identifier	Organizational Security Policy
P.COMMUNICATION-CRYPTO (Encryption communication of image file)	Highly confidential image file (encrypted print files, scanned image files) which transmitted or received between IT equipment must be encrypted.
P.COMMUNICATION-SIGN	Digital signature must be added to a mail

(Signature of image file)	including highly confidential image files (scanned image files).
P.DECRYPT-PRINT (Decryption of image file)	Highly confidential image files (encrypted print file) are permitted to print only to a user who generated that files.

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

2.1.3 Assumptions for Operational Environment

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

Table 2-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN (Personnel conditions to be an administrator)	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.SERVICE (Personnel conditions to be a service engineer)	Service engineers, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.NETWORK (Network connection conditions for MFP)	When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET (Operating condition about secret information)	Each password and encryption passphrase does not leak from each user in the use of TOE.
A.IC-CARD (Operational condition about IC card)	IC card is owned by rightful user in the use of TOE.
A.SETTING (Operational setting condition about security)	- Prohibit administrator authentication operation when failing the input of administrator password consecutively constant frequency. - Disable the use of the remote diagnostic function - Disable the use of the TOE update function via an internet. - Disable the use of the maintenance function. - Activate login authentication of service engineer. - Activate the encryption function or HDD lock function. - Disable the setting of administrator function excluding panel.

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 C253 / bizhub C203 for PKI Card System User's Guide [Security Operations] Ver.101

<Documents for service engineer>
- bizhub C253 / bizhub C203 for PKI Card System SERVICE MANUAL [SECURITY FUNCTION] Ver.101

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 C253 or bizhub C203, digital MFP provided by Konica Minolta Business Technologies, Inc, equipped with the options such as FAX unit, encryption board and card reader.

- Active Directory, the directory service provided by Windows Server 2000 (or later), is connected to Office LAN to authenticate IC card of user.

- The configuration that the client PC installed exclusive printer driver and connected a card reader. And SMTP server and DNS server are available.

2.2 Security Objectives

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

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

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

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

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

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

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 form 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.
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.

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.

(3)Security function to satisfy the organizational security policy [P.COMMUNICATION-CRYPTO (Encryption communication of image file)]

This organizational security policy prescribes that image file which flows on network are encrypted to ensure the confidentiality. As this corresponds as one's request, it does not need to encrypt all image data. It needs to encrypt data between MFP and user's client PC on handling encrypted print file or scan image file.

In this TOE, by supporting the function encrypting scan image file which is transmitted to user's client PC from MFP by e-mail (referred as "S/MIME encryption processing function") and encrypting Encrypted print file which is transmitted to MFP from client PC with IC card and exclusive driver outside of TOE, image data which flows on network can be transmitted and received confidentially.

(4)Security function to satisfy the organizational security policy [P.COMMUNICATION-SIGN (Signature of image file)]

This organizational security policy prescribes that signature is added to ensure the integrity of image file which flows using e-mail. As this corresponds as one's request, it does not need to add signature all image data. It needs to add signature on handling scan image file.

In this TOE, by supporting the function transmitting scan image file to client PC from MFP by e-mail with IC card outside of TOE (referred as "IC card operation support function") and the function that TOE add signature using IC card (referred as "S/MIME signature function"), image data which flows using e-mail can be ensured the integrity and transmitted.

(5)Security function to satisfy the organizational security policy [P.DECRYPT-PRINT (Decryption of image file)]

This organizational security policy prescribes that only the user who generated encrypted print files can decrypt and print encrypted print files concerned.

In this TOE, by supporting the function that the encrypted print files are with IC

card outside of TOE (referred as "IC card operation support function") and the function that encrypted print files can be accepted to decrypt and print when IC card which generated the encrypted print files is used (referred as "encrypted print file decryption function"), only the user who generated the encrypted print files can decrypt and print the encrypted print files concerned.

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 2009-03 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-03.

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

3.3 Product Testing

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

3.3.1 Developer Testing

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

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1 Configuration of Developer Testing.

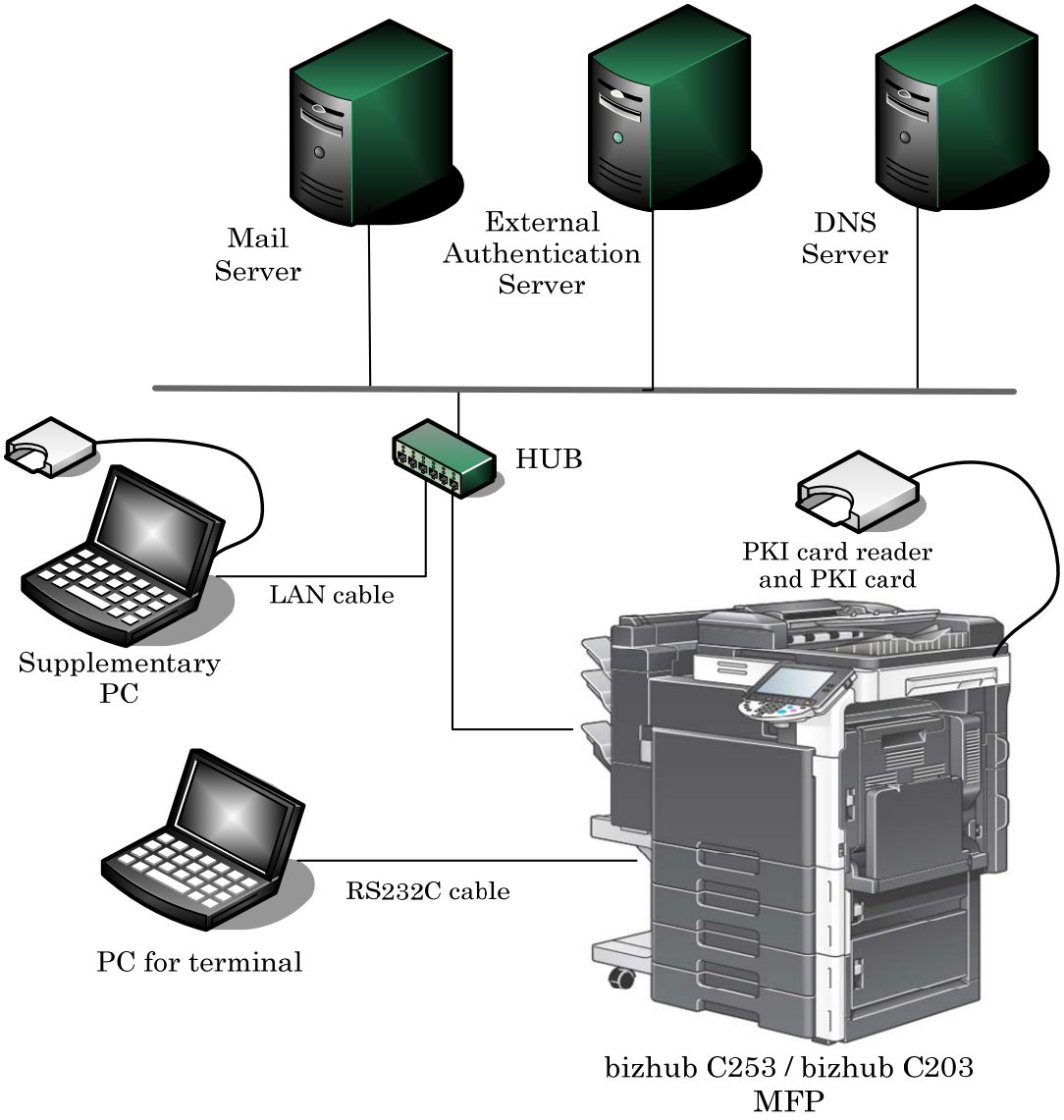

Figure 3-1 Configuration of Developer Testing

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

2) Outlining of Developer Testing

The tests performed by the developer are as follows;

a. Test outline

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
KONICA MINOLTA C353 Series PCL Driver Ver.6.3.0.BT21_00	Exclusive printer driver software included in the bundled CD of bizhub C253 / bizhub C203. Use for encrypted print.
ActiveClient 6.1	Driver software for smart card. Used as driver for PKI card in the supplementary PC.
SCR3310 USB Smart Card Reader Driver V4.41	Driver software for PKI card reader. Installed to the supplementary PC and used.
WireShark Ver. 0.99.5	Tool for monitoring and analyzing of the communication on the LAN. Used to get communication log and confirm data.
Mozilla ThunderBird Ver. 2.0.0.17	General purpose mailer software. Used as the confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver.0.98i 15 Sep 2008	Tool software for hash and encryption/decryption function. Used to confirm S/MIME signature.
Tera Term Pro Ver. 4.29	Terminal software executed in the terminal PC. Used to connect with MFP and to operate the terminal software installed in the MFP to monitor the state of TOE.
Disk dump editor Ver. 1.33	Tool software to display the contents in the HDD. Used to confirm the contents in the HDD.
Stirling Ver.1.3.1.0	Tool software of binary editor. Used to confirm the contents of decode S/MIME message.
MIME Base64 Encode/Decode v1.0	Tool software to Encode/Decode of MIME Base64. Used to decode of S/MIME message.
Blank Jumbo Dog Ver. 4.2.2	Simple server software for intranet. Used as the Web and mailer server function at the S/MIME tests.

b. Scope of Testing Performed

Testing is performed about 40 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. Result

The evaluator confirmed consistencies between the expected test results and the

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

3.3.2 Evaluator Independent Testing

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

1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.
Test configuration performed by the evaluator is showed in the Figure 3-1.
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 TSI for the test of the probabilistic and permutable mechanism.
(4)Based on the complexity of interfaces, test the necessary variations.
(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. And it was done to get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that evaluator can use.

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

<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 administrator.
(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 with considering the complexity of S/MIME encryption function to confirm the action at encrypting scan image data and transmitting by e-mail.
(5) Viewpoint	Tests were performed with judging the functions being innovative and unusual character to confirm the action of encryption key generation function of HDD encryption and encryption print 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 be bypassed the security functions by access through network.

(4)Possibility to affect the security functions by the power ON/OFF.
(5)Possibility to be wiretapped data transferred between card reader, MFP and external authentication server.

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.

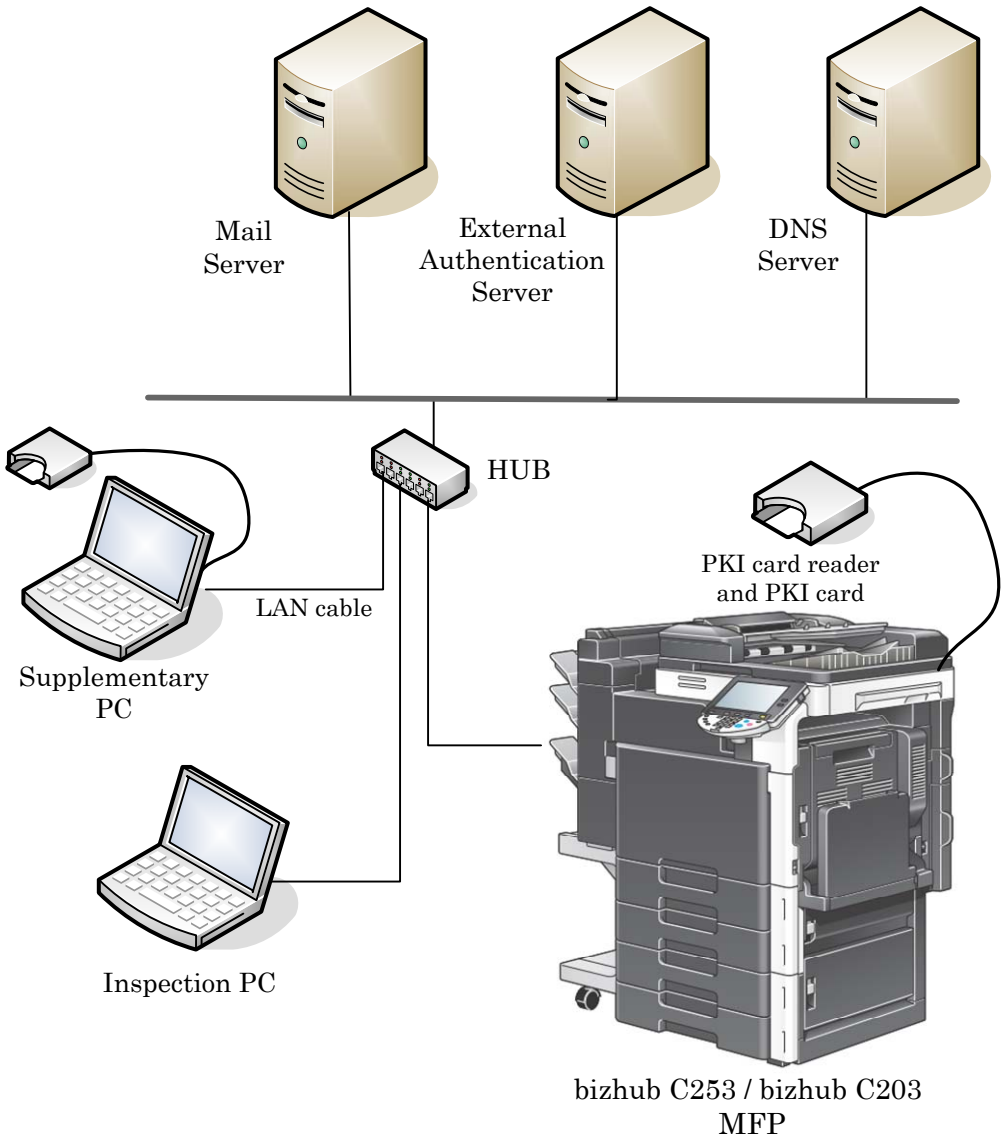

Figure 3-2 Configuration of Penetration Testing

<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 the behavior with test tool by using test tool, method to check authentication operation by using IC card, method to check data transferred between IC card and TOE in authentication process, 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 was installed in bizhub C253 / bizhub C203 (Version: A02E0Y0-0100-GN0-U4) - Network configuration Penetration Tests were done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP SP2. - Using the tools shown in table 3-1 (Thunderbird, Disk dump editor etc.) and software for USB analyzer (made by CATC) - Connect the MFP by using printer driver, IC card etc. and it is possible to use the encryption print function.
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.(The operation check of the following tool is finished in network environment in Mizuho Information & Research Institute, Inc. Plug in and the vulnerability database apply the latest version on March 20, 2009.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8d encryption tool of SSL and hash function (3)Nesuss 3.2.1.1 build 2G299_Q (Use plug in of March 20, 2009.) 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(Use plug in of March 20, 2009.) 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 commands 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 that information to affect security function from data transferred between the card reader and the external authentication servers does not leak out.

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 to set HDD lock function, the encryption function of HDD or both. When only the setting of HDD lock 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 each 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

- The information to authenticate IC card by Active Directory server is registered with Active Directory by the enterprise which publishes IC card when it is published.

- If FAX 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.

CAC:	Common Access Card
FTP:	File Transfer Protocol
HDD:	Hard Disk Drive
MFP:	Multiple Function Peripheral
MIB:	Management Information Base
NVRAM:	Non-Volatile Random Access Memory
PIV:	Personal ID Verification
RAM:	Random Access Memory
SNMP:	Simple Network Management Protocol
SSL:	Secure Socket Layer
S/MIME:	Secure Multipurpose Internet Mainl Extensions
USB:	Universal Serial Bus

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

CAC:	IC card which is issued by the certification organization in the Department of Defense.
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.

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.

PIV: Personal ID verification method to carry out with a certificate published by a federal office or a related information.

SNMP: Protocol to manage various devices through network.

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

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

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

intra-office LAN:
Network connected TOE and being securely connected to the external network through firewall.

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

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

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

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

7. Bibliography

[1] bizhub C253 / bizhub C203 PKI Card System Control Software Security Target Version 1.07 (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 C253 / bizhub C203 PKI Card System Control Software Evaluation Technical Report Version 2, Aug 11, 2009, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security