Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-05-01 (ITC-7148)
Certification No.	C0134
Sponsor	NEC Corporation
Name of TOE	NEC Group Information Leakage Prevention System (Japanese Version)
Version of TOE	V1.0
PP Conformance	None
Conformed Claim	EAL1 Augmented with ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1
Developer	NEC Corporation
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2007-12-26

Hideji Suzuki, 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 1 (Japanese Version 1.2)
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 1 (Japanese Version 1.2)

Evaluation Result: Pass

"NEC Group Information Leakage Prevention System (Japanese Version)" 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 “NEC Group Information Leakage Prevention System (Japanese Version)” (hereinafter referred to as “the TOE”) conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, NEC Corporation.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.8 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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

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

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	NEC Group Information Leakage Prevention System (Japanese Version)
Version:	V1.0
Developer:	NEC Corporation

1.2.2 Product Overview

This TOE is an information leakage prevention system that is deployed throughout the NEC group companies. It is designed to restrict the user’s PC operations relevant to taking information out of a PC. This is implemented by defining the PC control policy by the Administrator in accordance with the privilege assigned to each user and enforcing that policy to each user PC.
The main security features of the TOE include identification and authentication, access control, cryptography and auditing.

・ Identification and Authentication
- A function to identify and authenticate a user

・ Access Control
- A function to control the input/output PC operations from or to its I/O port or a printer
- A function to control the execution of a user program
- A function to control the output of a file to the authorized external media
- A function to control the output of a file to the authorized USB device

- A function to control the creation and modification of the client control information

・ Cryptography

- A function to encrypt and decrypt a file
- A function to create an encryption/decryption key
-A function to encrypt/decrypt a file when inputting/outtputing it from or to the authorized external media or the authorized USB device

・ Auditing

- A function to create and transfer logs to the log server
- A function to view and search logs stored in the log server

1.2.3 Scope of TOE and Overview of Operation

The TOE operates on the log server that stores logs transferred from the administrator and client terminals, on the administrator terminal that is used by the Administrator who implements identification / authentication and access control, and on the client terminal used by general users within the NEC group company. To restrict user's PC operations relevant to taking information out of a client PC , the Administrator (or the administrator terminal) creates the client control information that defines the PC control policy, and distributes it to each general user. Once the general user installs it on its own client terminal, access control based on the client control information is initiated to the associated I/O port, user program, printer and authorized external media. All authorized external media and data are encrypted. When various PC operations such as writing to the external media are executed on the administrator/client terminal, audit logs are created and transferred to the central log server. These audit logs stored in the log server can be viewed and searched on the administrator terminal.

The Figure 1-1 shows the physical scope of the TOE. The area surrounded by the red dashed line represents the software groups running on the log server, the administrator terminal and the client. Details of the TOE software components are shown in Table 1-1.

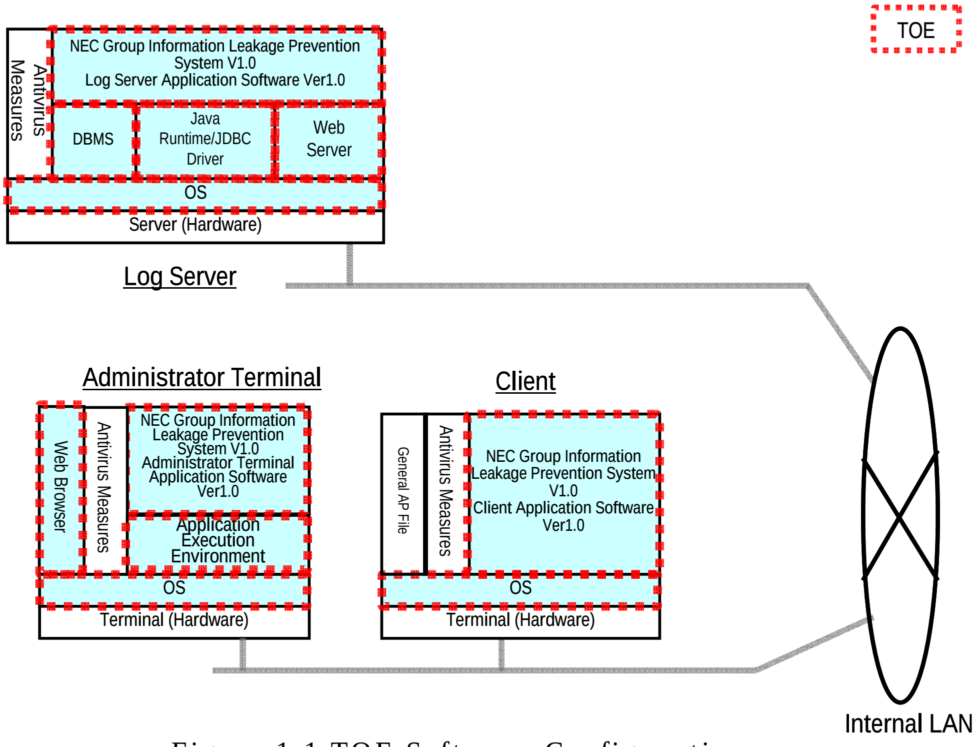
TOE
NEC Group Information Leakage Prevention System V1.0
Log Server Application Software Ver1.0
Antivirus Measures
DBMS
Java Runtime/JDBC Driver
Web Server
OS
Server (Hardware)
Log Server
Administrator Terminal
Web Browser
Antivirus Measures
NEC Group Information Leakage Prevention System V1.0
Administrator Terminal Application Software Ver1.0
Application Execution Environment
OS
Terminal (Hardware)
Client
General AP File
Antivirus Measures
NEC Group Information Leakage Prevention System V1.0
Client Application Software Ver1.0
OS
Terminal (Hardware)
Internal LAN

Figure 1-1 TOE Software Configuration

Table 1-1 TOE Software Components

Product Name	Type	Software Component Name
Log Server	AP	NEC Group Information Leakage Prevention System V1.0 Log Server Application Software Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition (SP1)
	DBMS	Microsoft SQL Server 2005 Standard Edition (SP1)
	JDBC Driver	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Web Server	Apache Tomcat 5.5.17
	Java Runtime	Apache Axis 1.4
Administrator Terminal	AP	NEC Group Information Leakage Prevention System V1.0 Administrator Terminal Application Software Ver1.0
	OS	Microsoft Windows XP Explorer 6.0 (SP2)
	Web Browser	Microsoft Internet Explorer 6.0 (SP2)
	Application Execution Environment	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 Japanese Language Pack
Client	AP	NEC Group Information Leakage Prevention System V1.0 Client Application Software Ver1.0
	OS	Microsoft Windows XP Professional (SP2)

The log server and the administrator terminal can be accessed only by users who have Administrator privileges, on the other hand, the normal client computer can be accessed by any users with privileges other than Administrator privileges.

The TOE hardware specifications are shown in the Table 1-2.

Table 1-2 TOE Hardware Components

Product Name	Type	Description
Log Server	CPU	Pentium 4, 3.0 GHz or higher
	Memory	2 GB or more
	HDD	100 GB or more
	Graphic	1024 x 768 resolution or higher 256 or more colors
Administrator/Client Terminal	CPU	Pentium III, 1.0 GHz or higher
	Memory	512 MB or higher
	HDD	40 GB or higher
	Graphic	1024 x 768 resolution or higher 256 or more colors

1.2.4 TOE Functionality

The TOE provides the following security functions:

(1) Auditing
(Administrator/client terminal)

- Generation and transfer of logs to the log server
- Protection of logs during the transfer

(Log server)

- Viewing and searching logs stored in the log server

(2) Identification/authentication
* The identification/authentication function described in this section refers to that provided by the application programs on the administrator/client terminals and log servers such as Administrator Terminal Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0, Client Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0 and Log Server Application Software Ver1.0 for NEC Group Information Leakage Prevention System V1.0. It is not the identification/authentication function provided by the operating system.
（Administrator Terminal）

- Identification/authentication required for the Administrator to log on to the administrator terminal
- Identification/authentication required to unlock a PC in the locked-out state due to “user inactivity period” setting
- Changing an administrator password

(Client)
Identification/authentication required for the general user or the client administrator to log on to the client terminal
Identification/authentication required to unlock a PC in the locked-out state due to “user inactivity period” setting
Changing a general user password
(Log Server)

- Identification/authentication required for the Administrator to view or search the log data stored in the log server

(3) Access Control
(Administrator terminal)

- Creation and change of the client control information

(Client)

- Reference of the client control information
- Implementation of the following functions based on the client control information:
  - whether to enable or disable I/O ports and a printer
  - Execution of a general AP file and change of a file name
  - File output to the authorized external media
  - File input/output to the authorized USB device

(4) Encryption
(Administrator terminal)

- Creation of a key file to encrypt/decrypt a data file that is obtained or created by a general user who uses a client

(Client)

- Read or delete of a key to encrypt/decrypt a data file that is obtained or created by general users who use a client
- Encryption/decryption of a data file that is obtained or created by a general user

who uses a client

- Encryption/decryption of a file to be output/input to or from an authorized external media

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 “NEC Group Information Leakage Prevention System V1.0 (Japanese Version) Security Target” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1] and evaluation deliverables in relation to development of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B 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 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 “NEC Group Information Leakage Prevention System (Japanese Version) Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [13]. Further, evaluation methodology should comply with the CEM (either of [11] or [12]).

1.4 Certification

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

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of the TOE defined by this ST is EAL1 augmented with assurance components ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1.

1.5.3 Security Functions

For the security functions provided by the TOE, refer to “TOE Functions” in Section 1.2.4.

These security functions satisfy the following security functional requirements:

- Security auditing
- Cryptography
- Access control
- Output data protection
- Input data protection
- Identification and authentication
- Security management
- Security function protection

1.5.4 Threat

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

Table 1-3 Assumed Threats

Identifier	Threat
T.INJUSTICE_LOGON (injustice logon)	A general user or third party may masquerade as an authorized user of the TOE to modify or disclose user or TSF data.
T.UNAUTHORIZED_ACCESS (unauthorized operations)	General users may attempt unauthorized operations including, but not limited to, output to unauthorized printers, execution of unauthorized programs and use of unauthorized I/O ports to disclose the user data that is stored in the client terminals.
T.INJUSTICE_CONNECT (injustice connections)	A third party may connect the external media or the client’s HDD to the unauthorized equipment to disclose the user data that is stored in the external media or the client’s HDD.

1.5.5 Organizational Security Policy

The organisational security policy required for using the TOE is presented in Table 1-4.

Table 1-4 Organisational Security Policy

Identifier	Organisational Security Policy
P.LOG_COLLECT	Log data collected by each administrator/client

(log collection)	terminal is stored in the central log server.
P.RESTRICTED_MEDIA (only authorized external media is allowed)	Only authorized external media can be used to write data from a client terminal.
P.SECURITY_PARAMETER (appropriately configured security parameter settings)	The Administrator shall set the client control information to appropriate values based on the TOE guidance document.

1.5.6 Configuration Requirements

This TOE is configured with a set of software presented in Table 1-1 “TOE Software Components” and operates on a set of hardware presented in Table 1-2 “TOE Hardware Components”.

1.5.7 Assumptions for Operational Environment

Assumptions required in environment using this TOE are presented in Table 1-5. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-5 Assumptions in Use of the TOE

Identifier	Assumptions
A.MANAGE_SAFE_PLACE (safe installation of administrator terminals)	The administrator terminals will be installed inside the Company building where only NEC Group employees and those who are authorized by them are granted the entrance to the building.
A.FACILITIES_IN_SECURE_ROOM (equipment installation at a secure room)	The log servers and the associated log backup media will be installed or placed in rooms with physical entry controls.
A.UNJUST_SOFTWARE (measures against unjust software)	It is necessary to install antivirus software on all log servers (running the TOE) and administrator/client terminals. It is also necessary to appropriately apply the pattern files of antivirus software and the security patches of the operating system that is part of the TOE components.
A.PASSWORD_MANAGEMENT (password management)	The TOE users keep their passwords for accessing the TOE confidential. They also set non-guessable passwords and change them at appropriate intervals.
A.NETWORK	The company LAN is connected to external

(network environments)	networks via security equipment that prevents unauthorized communications from the external networks.　The secure room network is connected via security equipment that permits only the protocols necessary for communication with log servers and administrator/client terminals.
A.OPERATOR_MANAGEMENT (management of administrators)	The Administrator will be a trusty person who never attempts unauthorized operations.
A.LOG_BACKUP (log backup)	It is necessary to take measures for prevention from loss of log data on the log servers.
A.PC_STARTUP_SET (PC startup control setting)	All PCs provided to general users will be configured not to start up in the maintenance mode.

1.5.8 Documents Attached to Product

Documents attached to the TOE are presented in Table 1-6.

Table 1-6 TOE Guidance documents

Type	Guidance Document Name
Installation Guidance	NEC Group Information Leakage Prevention System V1.0 Install Guide
User Operation Guidance	NEC Group Information Leakage Prevention System V1.0 Administrator Guide
	NEC Group Information Leakage Prevention System V1.0 User Guide

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

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

2.2 Overview of Evaluation Conducted

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

Evaluation has started on 2007-05 and concluded by completion the Evaluation Technical Report dated 2007-12. 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. Further, the evaluation facility executed evaluator testing (evaluator independent testing and penetration testing) by using developer testing environment at developer site on 2007-10.

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

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

2.3 Product Testing

Overview of evaluator testing conducted by evaluator is as follows.

2.3.1 Evaluator Testing

(1) Evaluator Test Environment

The Figure 2-1 shows the configuration of the testing system implemented by the evaluator.

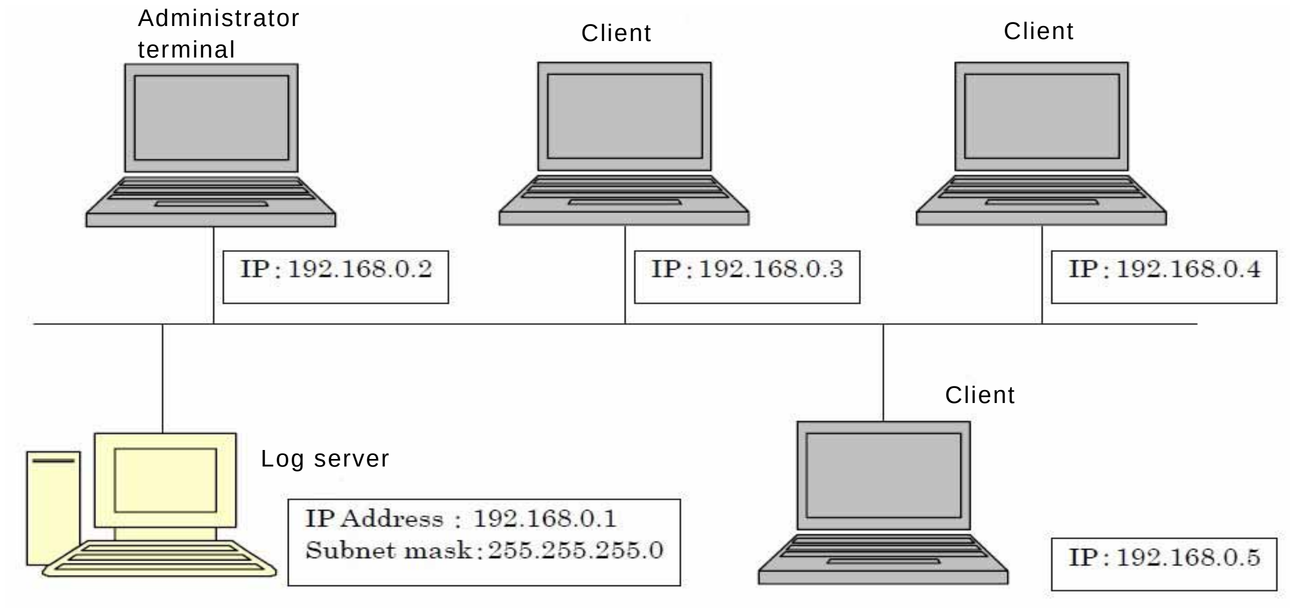

Figure 2-1 TOE configuration of the testing system

The hardware configuration of each equipment is as follows:

(1) Log Server
Express5800/120Re-1(X/3DG(1)) No.44Z01299 NEC Corporation
- CPU Intel(R) Xeon(TM) CPU 3.00GHz
- Memory 2 GB
- HDD 100 GB

(2) Administrator/Client Terminal
VersaPro VY16F/RF-R NEC Corporation
- CPU Intel(R) Pentium(R) M Processor 1.60 GHz
- Memory 496 MB
- HDD 40 GB

The software configuration of each equipment is presented in Table 2-1:

Table 2-1 TOE Software Configuration

Product Name	Type	Model Name
Log Server	AP	NEC Group Information Leakage Prevention System V1.0 Log Server Application Software Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition (SP1)
	DBMS	Microsoft SQL Server 2005 Standard Edition (SP1)
	JDBC Driver	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Web Server	Apache Tomcat 5.5.17 Apache Axis 1.4
	Java Runtime	Sun Java Runtime Environment (JRE) 5.0 Update 11
	Antivirus Software	Networks Associates Technology VirusScan Enterprise 8.0i
Administrator Terminal	AP	NEC Group Information Leakage Prevention System V1.0
	OS	Microsoft Windows XP Professional (SP2)

	Web Browser	Microsoft Internet Explorer 6.0 (SP2)
	Application Execution Environment	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 Japanese Language Pack
	Antivirus Software	Networks Associates Technology VirusScan enterprise 8.0i
Client	AP	NEC Group Information Leakage Prevention System V1.0 Client Application Software Ver1.0
	OS	Microsoft Windows XP Professional (SP2)
	Antivirus Software	Networks Associates Technology VirusScan Enterprise 8.0i

Tools used by the evaluator during the testing are presented in Table 2-2.

Table 2-2 Used tools

Type	Model Name
Register Editor	Microsoft(R) Registry Editor Version 5.1 (Build 2006.xpsp_sp2_gdr..070227 : Service Pack2)
Network Protocol Analyzer	WIRESHARK Version 0.99.6^{a} (SVN Rev 22276)

(2) Outlining of Evaluator Testing

Outlineing of the testing performed by the evaluator is as follows:

a. Test Configuration

The configuration of the testing conducted by the evaluator is shown in the section (1) “Evaluator Test Environment”. The evaluator testing was conducted in the same TOE test envrionement with the TOE configuration identified in ST.

b. Testing Approach

The evaluator used the following approach:

a. A functional test using the TSFI interface provided by the TOE
b. A test for registry change by the registry editor
c. A communication test using a network protocol analyzer

c. Scope of Testing Performed

There are the total number of 47 items for testing, including 39 items for evaluator independent testing created uniquely by the evaluator (12 items for testing on administrator terminal, 22 items for testing on client and 5 items for testing on log server) and 8 items for intrusion testing. Criteria of selecting these test items are as follows:

1) Evaluator Independent Testing

a. A few interfaces relating to identified problems shall be included in the test subsets and tested strictly.
b. The SFR interface shall be included in the test items.

2) Intrusion Testing

Test items were created based on:

a. known vulnerabilities of similar products,
b. reference books and documents (IPA open information), and
c. the results of other tests

d. Results

It was confirmed by the evaluator indepedent testing that the results of all test item are matching the expected results. It was confirmed by the penetration testing that only one test item is not matching the expected result. After reviewing this item on the CEM, it was judged that it cannot be abused on the attacker level assumed by the EAL1 (or it is a residual vulnerability).

2.4 Evaluation Result

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

3. Conduct of Certification

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

1. 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.

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

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

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL1 augmented with assurance components ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1 prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
IT	Information Technology
SFR	Security functional requirement
SAR	Security assurance requirement
TSFI	TOE Security Functionality interface

The TOE specific abbreviations used in this report are listed below:

AP	Application Program
DB	Database
DBMS	Database Management System
GB	Giga Byte
GHz	Gigahertz
HDD	Hard Disk Drive
LAN	Local Area Network
PC	Personal Computer

The terms used in this report are listed below:

Administrator privilege	One of user privileges used in Microsoft operating systems. It permits a user to change the operating system settings.
NEC	NEC Corporation
NEC group	NEC and its subsidiaries

I/O port A port used for data transfer between a PC and its peripheral (e.g. USB ports, IEEE1394 ports, serial ports, parallel ports, infrared ports, PCMCIA ports and printer ports).

Java An object-oriented programming language. Java runtime environment.

JDBC An AP interface for connection between Java and database.

LogViewer An administrative tool for viewing/searching logs that run on the log server application software.

USB device A generic name of peripherals that are connected to the USB port on a PC.

Administrator A generic name of a person who performs the TOE management operations on administrator and client terminals.

External Media Media connected to a client and recognized as a removal media by the operating system (e.g. External HDD, USB memory, PCMCIA memory, etc.).

Administrative Terminal A PC used by an administrator for reading/searching client control information.

Authorized USB Device A USB device authorized by the Administrator.

Authorized External Media Any media (external HDD, USB memory, PCMCIA memory and others) connected to a client terminal and identified as a removal media by the operating system. It stores authorized external media input/output control information written by the Administrator.

Client A PC used within the NEC group.

Client Control Information A PC control policy created by the Administrator and defined to each client PC or the definition information used to control the behavior of each client PC.

Printer Port A port for outputting client’s print data to a printer.

Maintenance mode A mode to be specified when starting Windows to maintain the Microsoft Windows operating system.

User A generic name of Administrators, client administrators and general users.

Log Audit information stored in the audit trail.

6. Bibliography

[1] NEC Group Information Leakage Prevention System V1.0 (Japanese Version) Security Target Version 1.12 (December 12th, 2007) NEC Corporation.

[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 Part1: Introduction and general model Version 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 1 September 2006 CCMB-2006-09-003

[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 (Japanese Version 1.2 March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 1 September 2006 CCMB-2006-09-002 (Japanese Version 1.2 March 2007)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 1 September 2006 CCMB-2006-09-003 (Japanese Version 1.2 March 2007)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 1 September 2006 CCMB-2006-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 1 September 2006 CCMB-2006-09-004 (Japanese Version 1.2 March 2007)

[13] NEC Group Information Leakage Prevention System (Japanese Version) V1.0 Evaluation Technical Report Version 1.3, December 13th, 2007, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center