Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-08-31 (ITC-7168)
Certification No.	C0156
Sponsor	NEC Corporation
Name of TOE	NEC Group Secure Information Exchange Site
Version of TOE	1.0
PP Conformance	None
Conformed Claim	EAL1 Augmented with ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1
Developer	NEC Corporation
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.
2008-04-25

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 Secure Information Exchange Site" 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 Secure Information Exchange Site Version 1.0” (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, 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 Secure Information Exchange Site
Version:	1.0
Developer:	NEC Corporation

1.2.2 Product Overview

The TOE is the business data exchange system that provides services for preventing the miss-delivery of business data and the information leakage in communications between internal users of NEC Group and their customers.

The basic operation of the TOE is as follows: An employee of NEC Group first creates an Area that is an administered data storage area, and then creates a folder in that Area. An internal user or a customer uploads business data to that folder. The uploaded data is then downloaded by internal users or customers for their business use.

As service functions, the TOE provides the Upload function, the Download function, Area Maintenance function, the User Maintenance function, the Set Personal Information function and the Administration function.

As security functions, the TOE protects the business data to be exchanged by the TOE from unauthorized access, miss-delivery and information leakage. It also collects audit logs. The overview of security functions provided by the TOE is as follows:

- Identification and Authentication
  A function to identify and authenticate the users of the TOE

- Access Control
  A function to control access to the business data based on the user roles of the TOE

- Auditing
  A function to generate and view the audit trail of the TOE

- Cryptography
  A function to encrypt and decrypt the communication data between the TOE and a user of the TOE

1.2.3 Scope of TOE and Overview of Operation

1) Scope and Operational Environment of TOE

The TOE is the system used by the NEC Group employees and their customers. The operational environment of the TOE is shown in Figure 1-1.

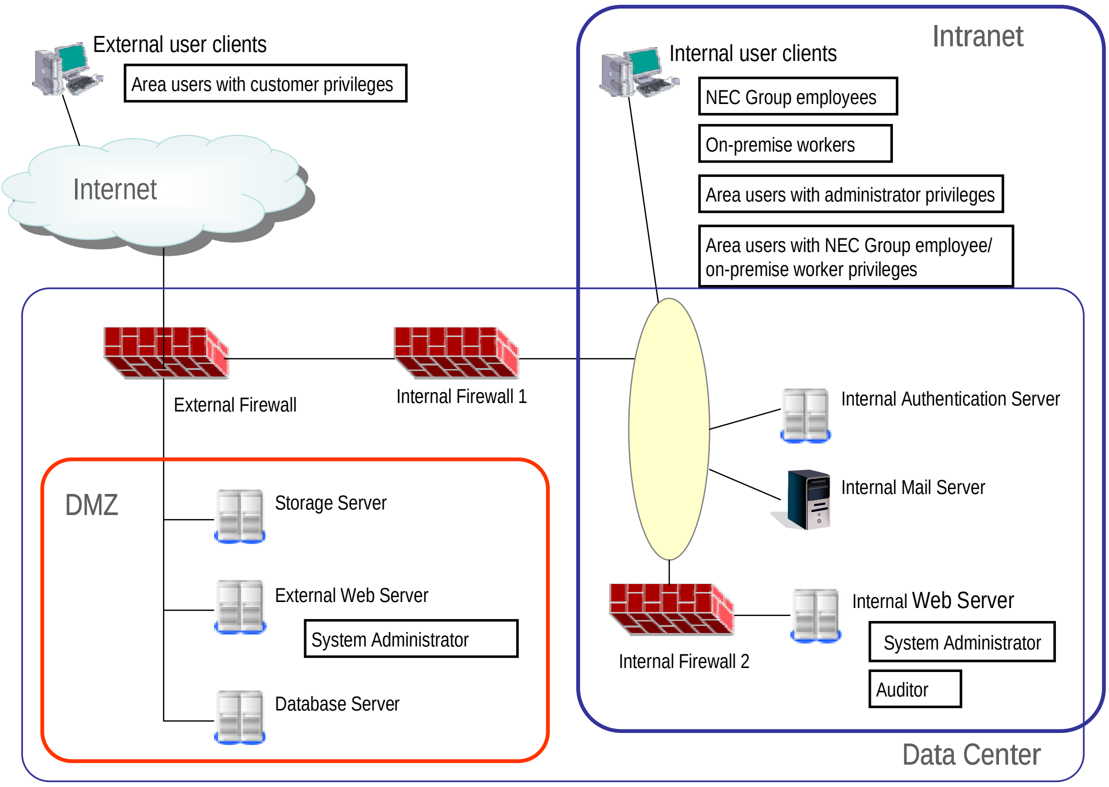

Figure 1-1 Operational Environment of the TOE

The scope of the TOE is defined as a software family running on Internal Web Server, External Web Server, internal user clients and external user clients. The software configuration of the TOE is shown in Table 1-1.

Table 1-1 Software Configuration of the TOE (Scope of the TOE)

Equipment Name			
	Vendor Name	Product Name	Type
Internal Web Server			
	NEC	NEC Group Secure Information Exchange Site V1.0 Internal Server Application Software V1.0	Application software
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	.NET Framework 3.0	Application execution environment
	Microsoft	Internet Information Server 6.0	Web server
External Web Server			
	NEC	NEC Group Secure Information Exchange Site V1.0 External Server Application Software V1.0	Application software
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	.NET Framework 3.0	Application execution environment
	Microsoft	Internet Information Server 6.0	Web server
Internal User Client			
	NEC	NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	OS Cryptographic Processing Library	OS library
External User Client			
	NEC	NEC Group Secure Information Exchange Site V1.0 Web Browser Library V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web browser
	Microsoft	OS Cryptographic Processing Library	OS library

2) Overview of TOE Operation

Traditionally, e-mail services have been used as a means of exchanging business data. However, it is at increased risk for misdelivery or information leakage. The TOE is the information leakage prevention system that restricts those internal users allowed to exchange business data with customers, prevents misdelivery by providing a URL and a PIN to the customer separately, and protects data from information leakage by cryptographic means.

The business data to be exchanged and its related information are stored in the Storage Server and the Database Server outside the TOE respectively (see Figure 1-1). The NEC Group users use the internal user client to access the business data via the Internal Web server. The customers use the external user client to access the business data via the External Web server.

The business data exchange is carried out as follows:

a) It is first required to create "areas" and "folders" for storing the business data to be exchanged. For each folder the person who has created an associated area will register internal users and the customers who can access to that folder.

b) These internal users and customers are permitted to upload their business data to the predefined folder. At this time it is required to specify the internal users and customers who are permitted to download that data. Selection of these downloaders is made from among the preregistered internal users and customers.

c) The TOE generates a one-time URL for downloading and a PIN for enabling the customers to use the URL. The one-time URL generated is sent to the downloaders (internal users and customers) via an email. Such emails are sent via the internal mail server outside the TOE while the PIN is sent to the customers by means other than that used for sending one-time URL.

d) To use a one-time URL each internal user must be authenticated by the internal authentication system outside the TOE, and each customer by the PIN authentication. This allows the predefined downloaders (internal users and customers) to download the business data stored in the folder.

3) Roles of TOE-Related Users

Roles of TOE-related users are as follows.

Users of the TOE-provided services are System Administrator, Auditor, NEC Group employees, on-premise workers and customers. User roles of the NEC Group employees are categorised into NEC Group employee, area-user with administrator privileges and area-user with NEC Group employee/on-premise worker privileges. User-roles of the on-premise workers are categorised into on-premise worker and area-user with NEC Group employee/on-premise worker privileges. User roles of the customer are area-user with customer privileges only.

a) NEC Group employee
NEC Group employees are authorised to create, update and delete areas and view areas and folders using an internal user client.

b) On-premise worker
On-premise workers are authorised to view areas and folders using an internal user client.

c) Area-user with administrator privileges
Any NEC Group employees who have created areas are referred to as area-users with administrator privileges in that area. They are authorised to perform the following business data related operations and controls using an internal user client.

- Create, update and delete folders.
- Register, update and delete the internal workers and the customers who are authorised to use folders.
- Assign operational privileges to area-users with NEC group employee/on-premise worker privileges.
- Assign area-user with administrator privileges to any NEC Group employees registered as folder-users.

d) Area-user with NEC Group employee/on-premise worker privileges
All NEC Group employees and on-premise workers registered as folder-users by the area-user with administrator privileges are defined as area-users with NEC

Group employee/on-premise worker privileges in the associated folder. They are authorised to perform the business data related operations using an internal user client.
Any on-premise workers cannot be defined as area-users with administrator privileges.

e) Area-user with customer privileges
Any customers registered as folder-users by the area-user with administrator privileges are defined as area-users with customer privileges in the associated folder. They are authorised to perform the business data related operations using an internal user client.
Any customers cannot be defined as area-users with administrator privileges.

f) System Administrator
The System Administrator is authorised to perform the following TOE-related operational controls using the Internal Web server or the External Web server.
- Initial settings of the TOE
- Start and stop the TOE operation

g) Auditor
The Auditor is authorised to view the TOE audit trail data using the Internal Web server.

1.2.4 TOE Functionality

The TOE provides the following service functions.

[Area Maintenance]
The Area Maintenance function is used to create, update and delete areas and folders, delete files in a folder, and display and output area logs.

[User Maintenance]
The User Maintenance function is used to register, update and delete internal users and customers.

[Upload Request]
The Upload Request function enables area-users with customer privileges to upload their business data. The upload request process flow is as follows:
a) An area-user with customer privileges makes an upload request to an appropriate area-user with NEC Group employee/on-premise worker privileges.
b) The area-user with NEC Group employee/on-premise worker privileges determines the upload destination area and folder and specifies authorised download-users.
c) An upload request mail is sent to the area-user with customer privileges.

[Upload]
The Upload function is used to upload the business data. When upload of business data is completed, a download request mail is generated.

[Download]
The Download function is used to download the business data. The downloading is allowed only one time. When all associated authorised users complete the downloading, the business data stored in the folder is automatically deleted.

[Set Personal Information]
The Set Personal Information function is used to change the e-mail address of a

specific user.

[Administration]

The Administration function is used to start and stop the TOE operation, register and delete Auditors, initialise Auditor's password, and display and output all area logs.

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 follows.

- 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;
- The 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 Secure Information Exchange Site Version 1.0 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 "NEC Group Secure Information Exchange Site 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 and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2008-04-04 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

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

1.5.3 Security Functions

Security functions of the TOE are as follow.

[Identification and Authentication]

The TOE provides the identification and authentication function to permit each user to access the TOE.

- Area-user with customer privileges
  Identification by one-time URL and authentication by PIN must be succeeded. When the user enters an invalid PIN for the same one-time URL, the TOE counts the number of such failed PIN attempts. When the number of failed PIN attempts exceeds the predetermined threshold, the TOE disables the issued one-time URL.

- Area-user with NEC Group employee/on-premise worker privileges
  Identification by one-time URL must be succeeded. The user attempts access to the TOE via one-time URL and needs to be authenticated by the internal authentication system outside the TOE. When the user fails in the authentication, the TOE counts the number of such failed authentication attempts. When the number of failed authentication attempts exceeds the predetermined threshold, the TOE disables the issued one-time URL.

- NEC Group employee and on-premise worker
  Identification by user ID must be succeeded.

- System Administrator
  Identification by URL must be succeeded.

- Auditor
  Identification by URL must be succeeded.

[Auditing]

The TOE generates an audit record when an auditable event occurs. The Auditor uses this function to view and search audit records.

[Access Control]

Based on the defined user privileges the TOE determines whether to permit each TOE user to access the business data and the associated area and folder storing that data.

[Encryption]

The TOE provides all TOE users with the function to protect the communication data between Web servers and Web browsers by means of SSL encryption and decryption.

1.5.4 Threat

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

Table 1-2 Assumed Threats

Identifier	Threat
T.SPOOFING (spoofing)	A third party not having any specialised knowledge may maliciously access the TOE via the Internet or a TOE user may masquerade as an authorised user and access the TOE via the NEC Intranet to destroy or disclose the business data.
T.ILLEGAL_ACCESS (illegal access)	An authorised TOE user, who is an NEC group employee, on-premise worker, area-user with administrator privileges, area-user with NEC employee/on-premise worker privileges and area-user with customer privileges may destroy or disclose the business data, upload area information or area-user information by performing the following operations that are not authorised for each user role. - Creating, updating or deleting areas by TOE users other than the NEC Group employees. - Creating, updating or deleting folders by TOE users other than area-users with administrator privileges. - Registering, updating or deleting folder-users (NEC Group employees, on-premise workers and customers) by TOE users other than area-users with administrator privileges. - Downloading, uploading or deleting business data by TOE users other than area-users with NEC Group employee/on-premise worker privileges or those with customer privileges.
T. LISTEN-IN_NW_ DATA(listen-in network data)	A third party not having any specialized knowledge may maliciously listen in or tamper business data that are exchanged between Web servers and networks to disclose, destroy or tamper that data.
T.MISDELIVERY (misdelivery)	An authorised TOE user may accidentally send a URL to an unintended customer, resulting in disclosure of business data.

1.5.5 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-3.

Table 1-3 Organisational Security Policy

Identifier	Organisational Security Policy
P. ADMIN_IDENTIFY (identification of administrator)	The System Administrator and the Auditor who use the TOE are subject to the TOE identification to keep a record of TOE access logs.
P. AUDIT_LOG (audit logs)	To track unauthorised operations on the TOE assets to be protected, the ability to access the TOE audit logs must be restricted to the Auditor only.

1.5.6 Configuration Requirements

Table 1-4 shows the required hardware configuration in the operational environments of the TOE. The TOE operates correctly and reliably in the operational environments as shown in that table.

Table 1-5 shows the required software configuration in the operational environments of the TOE. The TOE operates correctly in the software configuration identified in that table.

Table 1-4 Hardware Configuration in the TOE Operational Environments

Equipment Name	Type	Description
Storage Server		
Main Unit	Vendor Name	NEC
	Product Name	iStorage NS460
	Model Name	NF8100-145A
	CPU	Dual Core Intel Xeon Processor 3GHz
	Memory	3GB(2GB+1GB)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(standard)
	Expansion Disk	Physical capacity: 2100GB(300GB×7)RAID5
Internal Web Server		
Main Unit	Vendor Name	NEC
	Product Name	Express5800/120Ri-2 (XD2/3G(4))
	Model Name	N8100-1318
	CPU	Dual Core Intel Xeon Processor 3GHz × 2CPU
	Memory	4GB(2GB×2)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(standard)
External Web Server		
Main Unit	Vendor Name	NEC
	Product Name	Express5800/120Ri-2 (XD2/3G(4))
	Model Name	N8100-1318
	CPU	Dual Core Intel Xeon Processor 3GHz × 2CPU

Equipment Name		Type	Description
		Memory	4GB(2GB×2)
		HDD	73GB×2(15000rpm, RAID1)
		LAN	1000BASE-T×2(standard)
Database Server			
	Main Unit	Vendor Name	NEC
		Product Name	Express5800/140Re-4(XMPD/3.40G(16))
		Model Name	N8100-1276
		CPU	Dual Core Intel Xeon Processor 3.40GHz×4
		Memory	4GB(2GB×2)
		LAN	1000BASE-T×2(standard)
		External Storage	1148GB
Internal User Client			
	Main Unit	The client that is capable of running the OS defined in the Internal User Client column in Table 1-5	
External User Client			
	Main Unit	The client that is capable of running the OS defined in the External User Client column in Table 1-5	

Table 1-5 Software Configuration in the TOE Operational Environments

Equipment Name			
	Vendor Name	Product Name	Type
Storage Server			
	Microsoft	Windows Storage Server 2003 R2	OS
Internal Web Server			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
External Web Server			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
Database Server			
	Microsoft	Windows Server 2003 R2_Standard Edition	OS
	Oracle	Oracle Database 10g Standard Edition 1 Processor	DBMS
Internal User Client			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS
External User Client			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS

1.5.7 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-6. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-6 Assumptions in Use of the TOE

Identifier	Assumptions
A. DATACENTER (data center)	It is assumed that Internal Web Server, External Web Server, Database Server, Storage Server, Internal Authentication Server and Internal Mail Server are all placed in the data center which is protected by appropriate physical entry controls to ensure that only authorised personnel are allowed access.
A.NETWORK (network)	It is assumed that access to the Internal Web server from the Intranet is restricted by Internal Firewall 2 that is appropriately configured. It is assumed that access to the External Web server from the Internet is restricted by External Firewall that is appropriately configured.
A.SYSTEM_ADMIN (restrictions on TOE access by System Administrator)	It is assumed that the System Administrator accesses the Internal Web server or External Web server directly.
A.AUDIT_ADMIN (restrictions on TOE access by Auditor)	It is assumed that the Auditor accesses the Internal Web server directly.
A.ADMINISTRATOR (trusty administrator)	It is assumed that Operations Manager, System Administrator, Auditor, Storage Administrator and Database Administrator perform actions that are assigned to their roles, and never perform malicious actions.

1.5.8 Documents Attached to Product

Documents attached to the TOE are listed below.

- NEC Group Secure Information Exchange Site Version 1.0 Operational Manual V1.04, January 8, 2008 (Japanese version)

- NEC Group Secure Information Exchange Site Version 1.0 User Manual V1.03, February 28, 2008 (Japanese version)

- NEC Group Secure Information Exchange Site Version 1.0 User Manual (for NEC Group users) V1.03, February 28, 2008 (Japanese version)

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 in September 2007 and concluded by completion the Evaluation Technical Report in April 2008. 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, including evaluator independent testing and penetration testing, by using developer testing environment at developer site in December 2007.

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

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

2.3 Product Testing

Overview of evaluator testing conducted by evaluator is as follows.

2.3.1 Evaluator Testing

1) Evaluator Test Environment

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

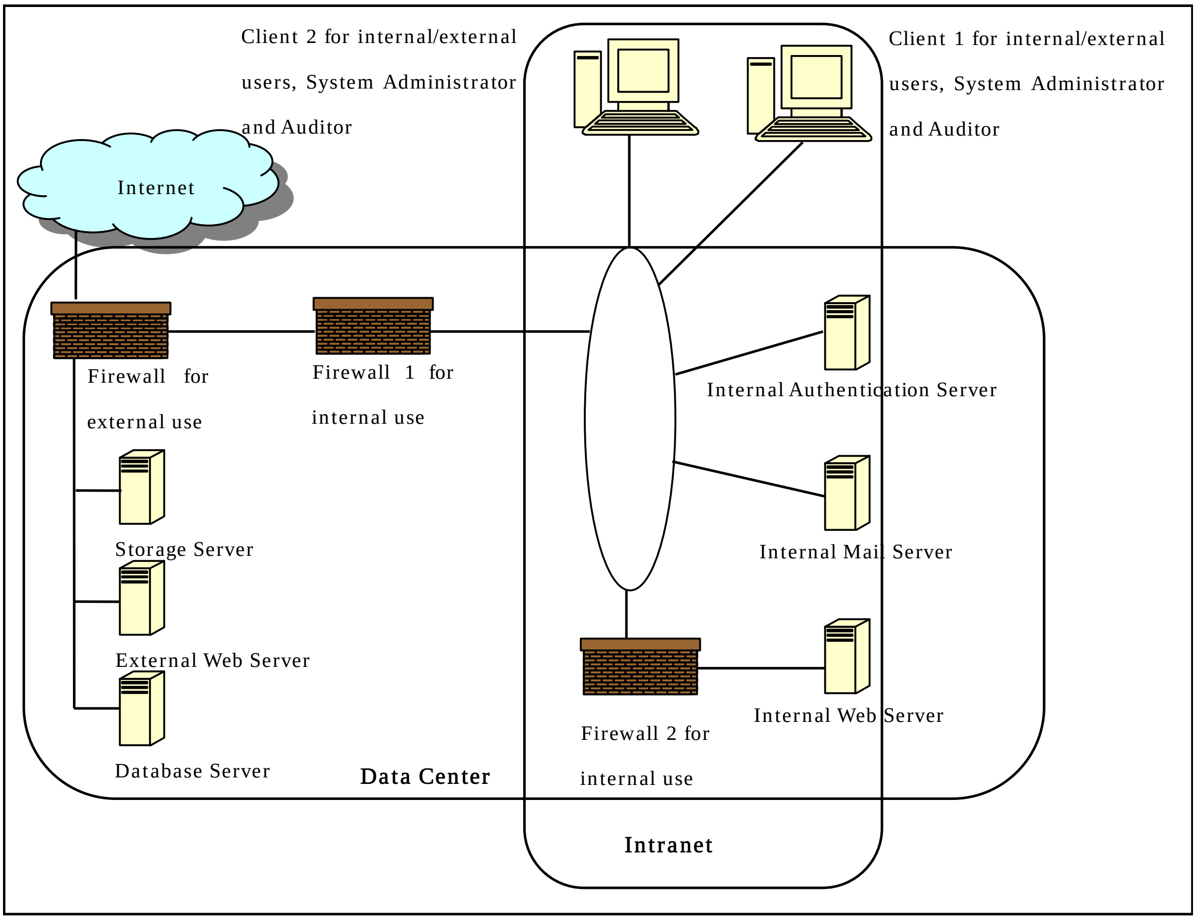
Client 2 for internal/external users, System Administrator and Auditor
Client 1 for internal/external users, System Administrator and Auditor
Internet
Firewall for external use
Firewall 1 for internal use
Internal Authentication Server
Storage Server
Internal Mail Server
External Web Server
Internal Web Server
Firewall 2 for internal use
Database Server
Data Center
Intranet

Figure 2-1 Configuration of Evaluator Testing

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is showed in the Figure 2-1. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in the ST.

Although the connection configuration of the external user, System Administrator and Auditor terminals differs from that in the actual environment, the evaluator confirmed that it was substantially comparable to that in the actual environment for use in the testing.

b. Testing Approach

For the testing, following approach was used.

1. The evaluator operated the terminal for each user role and examined the screen and log information.
2. The evaluator collected the transmitted and received data to examine the content of data and the response to invalid input values.

3. The evaluator examined the known vulnerabilities of the OS and the Web server using a vulnerability testing tool.

c. Scope of Testing Performed

Total of 49 items of testing; namely 30 items from evaluator independent testing and 19 items from penetration testing devised by the evaluator. As for selection of the test subset, the following factors are considered.

1. Security functions that play prominent roles.
2. Security function that contains innovative or unusual features.
3. Function used by different interface.
4. Security functions that are suspected to have vulnerabilities similar to those publicly known.

d. Result

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

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 ASE_OBJ.2, ASE_REQ.2 and ASE_SPD.1 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SAR:	Security Assurance Requirement
SFR:	Security Functional Requirement
ST:	Security Target
TOE:	Target of Evaluation
TSFI:	TOE Security Functionality Interface

The glossaries used in this report are listed below.

Area
The basic unit of business data management. Multiple folders are present under the area. Multiple areas can be created.

Area-user
A person who is authorised to use folders in the specific area (NEC Group employee, on-premise worker and customer).

Customer
An employee of business partners who are not authorised to use the NEC Intranet.

On-premise Worker
An employee of contractors who are authorised to use the NEC Intranet.

Internal Authentication Server
A server running the internal authentication service.

Internal Authentication Service
A service to centrally manage internal user IDs and passwords and provide authentication information to the various systems used by NEC Group.

Internal User
An NEC Group employee or an on-premise worker.

Folder
The basic business data unit to be stored in the area. Multiple folders can be created.

One-Time URL
A URL that is available for a specified period of time. It shows the destination folder. One-time URL contains identification information.

6. Bibliography

[1] NEC Group Secure Information Exchange Site Version 1.0 Security Target Version 1.14 (April 3, 2008) 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 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 components Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components 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 components 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 components 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 Secure Information Exchange Site Evaluation Technical Report Version 2, April 4, 2008, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security