Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-08-27 (ITC-7165)
Certification No.	C0200
Sponsor	Hitachi, Ltd.
Name of TOE	Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program
Version of TOE	60-02-32-00/00(R6-02A-14)
PP Conformance	None
Conformed Claim	EAL2
Developer	Hitachi, Ltd.
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.
2008-12-24

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

Evaluation Result: Pass

"Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program " 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 "Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program" (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, Hitachi, Ltd.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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

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

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program
Version:	60-02-32-00/00(R6-02A-14)
Developer:	Hitachi, Ltd.

1.2.2 Product Overview

TOE is a software program operating on the storage devices produced by Hitachi Ltd.: "Hitachi Universal Storage Platform V", "Hitachi Universal Storage Platform H24000", "Hitachi Universal Storage Platform VM", and "Hitachi Universal Storage Platform H20000". The storage devices are connected with many host of wide variety of platforms via SAN or IP network environment.
This TOE provides the function of protecting the storage device, which is allocated for the specific storage user, from the illegal access of the other storage users.

1.2.3 Scope of TOE and Overview of Operation

Storage device including TOE is generally used in the configuration as shown in Figure 1.1.

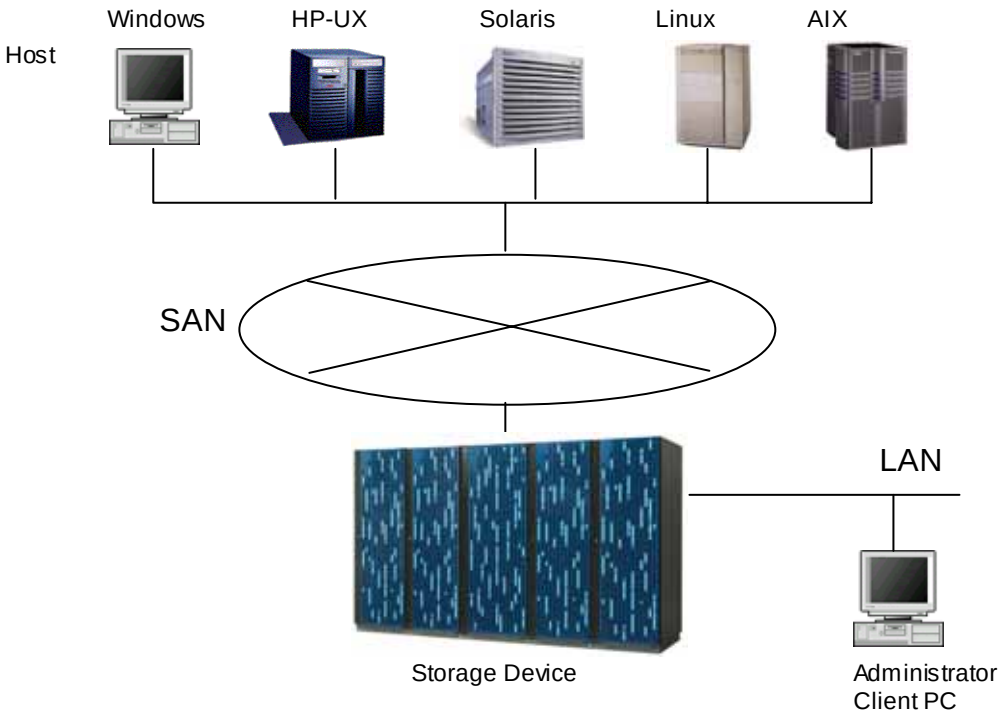

Figure 1.1 System Configuration including the Storage Device

The below explains the system configuration.

(1) Storage device

A storage device is usually installed in a secure area where entrance and exit are controlled.

(2) SAN and Host

Open-system server such as Windows, HP-UX or Solaris (those products are totally called "host" in this document) and storage devices are usually connected via SAN (Storage Area Network). SAN is dedicated network for the storage system that connects the hosts and the storage devices via the Fibre Channel.

(3) Administrator Client PC

The administrator client PC is a PC for setting up device control information of the storage device from remote sites. It operates the program for the storage device administrator to set up the device control information on the administrator client PC. The administrator client PC and the storage device are connected via LAN (Local Area Network).

Figure 1.2 illustrates the relations of storage device configuration and TOE. TOEs are "DKCMAIN Microprogram", "SVP Program" and "Storage Navigator Program".

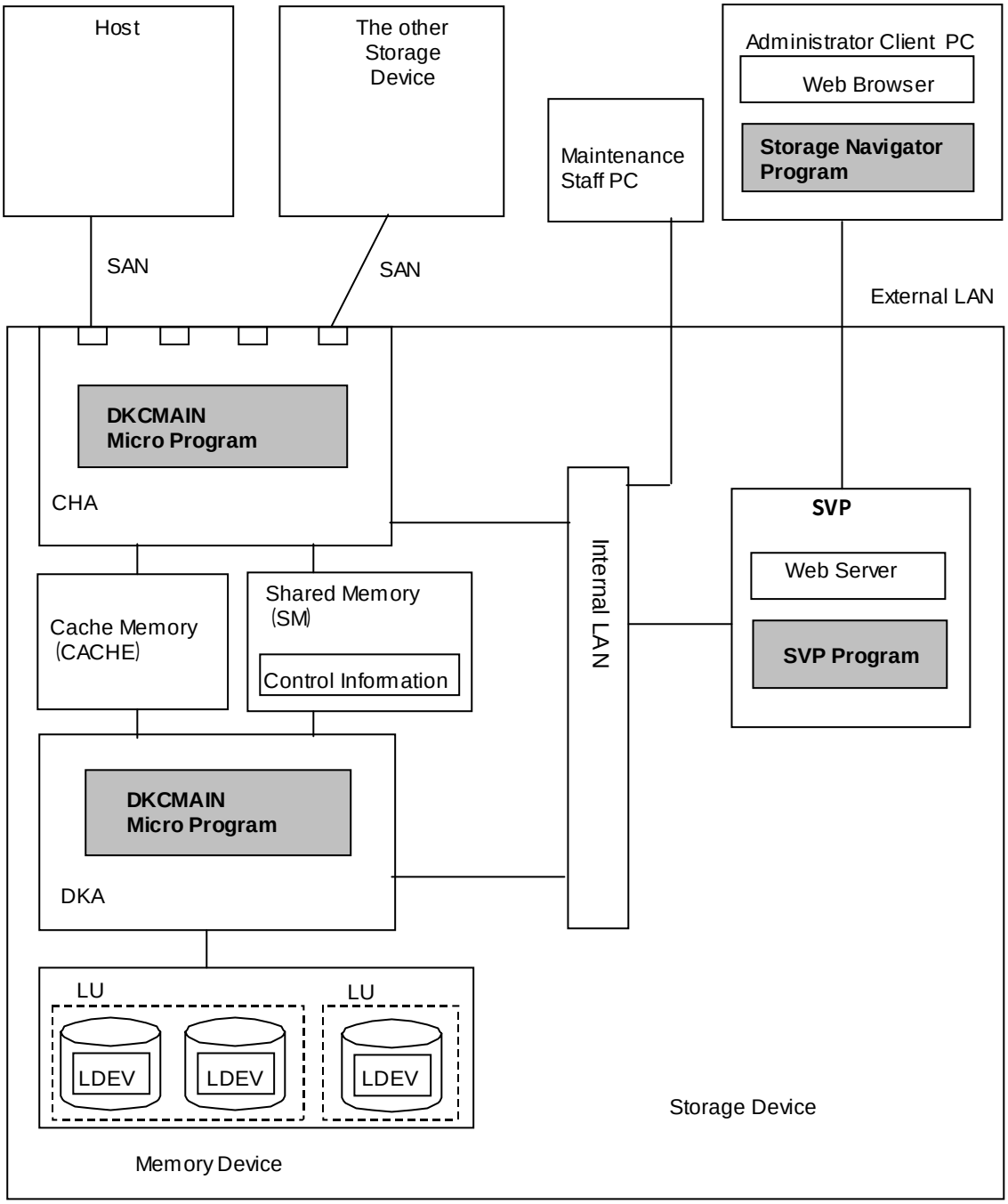

Figure 1.2 Storage Device Configuration and TOE

The below explains the system configurations.

(1) Channel Adapter

Channel adapter (CHA) is an adapter that processes a command from the host to the storage device, and controls data transmission. The host is connected to the fiber port on the CHA via Fibre Channel. On CHA, the DKCMAIN microprogram, which is a part of TOE, operates.

(2) Disk Adapter

Disk Adapter (DKA) is an adapter that controls data transmission between the cache memory (CACHE) and the memory device. On DKA, the DKCMAIN microprogram, which is a part of TOE, operates.

(3) Cache Memory (CACHE)

Cache Memory is a memory located between CHA and DKA, used for data Read/Write.

(4) Shared Memory

Shared Memory (SM) is a memory that is accessible both from the DKCMAIN microprogram on the CHA and DKCMAIN microprogram on the DKA. Control information for accessing data from CHA and DKA is stored in it. This control information includes the setting information required for the security function to operate is included. Control information on shared memory cannot be accessed without through DKCMAIN Microprogram. And the control information is updated by TOE, according to the commands from SVP or Storage Navigator.

(5) Memory Device

Memory Device consists of multiple hard disks, in which user data is recorded. In the memory device, an LDEV (Logical Device), which is the volume to store user data, is created. Access to user data is controlled by the unit of LDEV, and executed via DKCMAIN microprogram.

LU (logical unit) is a unit of accessing from the host, and it mapped to one or multiple LDEV.

(6) SVP (Service Processor)

SVP is a service processor embedded in the storage device to manage the whole storage device, and it works SVP program, which is a part of TOE. SVP program is a software for managing the maintenance function of the storage device and the device control information, and it has the function of transmitting a command received from Storage Navigator program that works on the administrator client PC to DKCMAIN microprogram, to set the device control information. The SVP program has the function to set the operations of the security function in the storage device.

(7) Maintenance Staff PC

The maintenance staff PC is a PC used by a maintenance staff in the maintenance process. They use it by connecting it to the SVP by the remote desktop function, via internal LAN which is the network in the storage Device.

(8) Administrator client PC

Administrator client PC is a customer's PC used by a user of Customer's Storage Navigator for the operation and the maintenance work of the storage device, and it works the Storage Navigator program, which is a part of TOE. The administrator client PC and the SVP is connected via the external LAN.

(9) Storage Navigator Program

Storage Navigator program (hereinafter called "Storage Navigator") is a software to manage the device control information on the storage device. Storage Navigator is a Java applet program, which is downloaded from the SVP to the administrator client PC to work on the Web Browser.

(10) The Other Storage Device

The port of the Storage Device can connect the other storage devices other than the host. To connect the other storage devices, such the data copying or creating backup copy between the devices become available. The copy operation executed from the other storage device is handled by the reliable storage administrator. Thus, the

other storage device connected to the storage device is limited to the one that installed TOE.

1.2.4 TOE User

TOE assumes the following users.

- The account administrator:
  The account administrator can execute registration, modification, and deletion of an account that is related to the operation of Storage Navigator by the Administrator (Storage administrators, storage partition administrators, account administrators, account partition administrators and audit log administrators). This is built in as an initial account when constructing a system.
- The storage administrator:
  The storage administrator has the control competence of the entire storage system. The storage administrator can divide the resources of the storage device (port, cache memory, and LDEV) into logical partitions with the Virtual Partition Manager function, a function of TOE.
- The storage partition administrator:
  The storage partition administrator can manage the resources (port, cache memory, LDEV) in the logical partition assigned by the storage administrator, and associates between WWN, identification information of the host, and LDEV number that permits the access.
- The account partition administrator:
  The account partition administrator can manage the divided logical partition and can execute creation, modification, and deletion of the accounts for the storage partition administrator and the account partition administrator.
- Audit log administrator:
  The Audit log administrator can manage the audit log acquiring from the storage device and can refer or download the audit log or the set related to syslog.
- Maintenance staff:
  Maintenance staff is a staff of the special organization for maintenance with which the customer who uses the storage device has signed a contract concerning maintenance. Manages the initial startup process in installing the storage device, changing the settings required in maintenance operations such as replacement or addition of parts or disaster recovery. Maintenance staff may execute the setting operations of the storage administrator, the storage partition administrator, the account administrator, the account partition administrator and audit log in their place. Maintenance staff access SVP from the maintenance staff PC, and executes maintenance operations.
- Storage User:
  Storage device user (represents Host) who uses the data saved in the storage device through the host connected to the storage device.
  The storage administrator, the storage partition administrator, the account administrator, the account partition administrator, and the audit log administrator are totally called as the users of Storage Navigator.

1.2.5 Property To Be Protected

The most important property for a storage device is the user data of storage users that is stored in disk drives. To maintain the integrity and confidentiality of the user data, it is required to protect it from the unauthorized alteration by the Storage Navigator and the unauthorized accessing from the storage user.

On the environment of existing the logical partitions that are divided into several pieces, the user data of the storage user existed in the LDEV in each partition is the property to be protected. So the property to be protected must be protected from the

unauthorized access by the storage users. And it prevents the deletion of the property to be protected by the storage partition administrator whom does not have an authorization to the area that identified by the logical partition.

1.2.6 TOE Functionality

TOE provides the following functions to make realize the access control not to have any intentional access to the user data existed in the storage device from the various host connected to the storage device:

- Storage Navigator Function (Security function)

  The Virtual Partition Manager function, LUN Manager function, various setting of the audit function (creation, modification, and deletion) are not possible without the identity authentication by the Storage Navigator function. And the setting of a storage navigator user account (creation, modification, deletion) is done by using this function.

  Cryptograph the communication between Storage Navigator and SVP by SSL to prevent the leakage of communication data and the falsification between the storage device and the administrator client PC.

- Virtual Partition Manager Function (Security function)

  It divides the resource of one whole disk subsystem (port, cache memory and LDEV) into the multiple virtual disk subsystems and each one of administrator of the virtual disk subsystem can only access to the respective virtual disk subsystem. This ensures that it is available to protect from breaking volume of other organizations or from leaking the data of one specific organization. Figure 1.3 shows the overview of the Virtual Disk Subsystem.

  CLPR: Cache Logical Partition

  A partition created by dividing the cache memory logically.

  SLPR: Storage Logical Partition:

  A partition created by dividing the cache in the storage device and the hard disk drive logically.

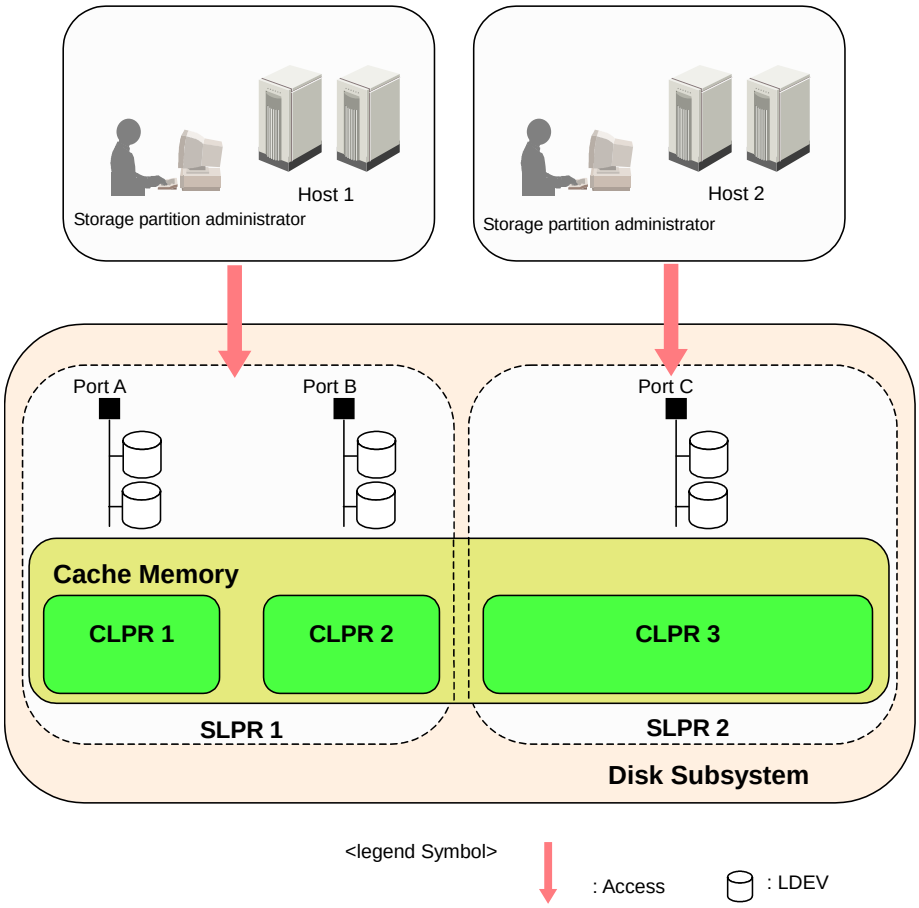

Figure 1.3 Virtual Disk Subsystem

- LUN Manager Function (Security function)

  LDEV that stores the user data is created by using Storage Navigator and associated with SLPR when it created. To access from the Host to LDEV, it associates LDEV and the port on the CHA, which is connected to the host. More in detail, it sets LU path by giving LU number that associates between the host and LDEV that permits accessing. The read and write of the data for the corresponding LDEV is available only from the host that executed LU path setting, and execute the access control to the LDEV for not to authorize read and write of data from the host which is not executed the LU path setting.

- Function of Identifying and Authenticating of the Host (Security function)

  When connecting the host to SAN, the authentication is done by the FC-SP function to prevent the illegal host connection. The storage administrator or the storage partition administrator set to the each host whether to give the authentication of host or not, with the operation of LUN Manager. The host that executes authentication registers the user information (WWN and secret).

- Audit Log Function (Security function)

  The audit log function is provided by the Storage Navigator or DKCMAIN microprogram. Storage Navigator records the event related to the security such as a success/fail of the login, a changing on the configuration or the setting. DKCMAIN microprogram records the event related to the security such as creation, deletion,

and modification of the LU path information.

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 "Hitachi Universal Storage Platform V 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 B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in " Evaluation Technical Report(URE-ETR-0001-02)" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2008-12 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL2 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
This TOE assumes the attack capability that the threatening agent has is "Low". Therefore the level of function strength should be SOF-basic.

1.5.4 Security Functions

The security functions of the TOE are as shown in section "1.2.6 TOE Functionality".

1.5.5 Threat

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

Table 1-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_XCNTL	Within the users of storage Navigator, a storage partition administrator or an account partition administrator might be able to access to LDEV where the host is not authorized, by chaining the setting of the storage device where beyond the own authorization.
T.TSF_COMP	A third person might make illegal connection on the channel between Storage Navigator and SVP on the purpose of sniffing or falsification of the data.
T.LP_LEAK	The leakage or falsification of the data might be done if a third person such as a host device administrator accesses to LDEV by connecting the unauthorized host to SAN.
T.CHG_CONFIG	A third person might change the setting of storage device with using the Storage Navigator.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.MASQ	If the customer requests the identity authentication of the host, the access of corresponding port must be prohibited until the identity authentication is completed.

1.5.7 Configuration Requirements

TOE is included one of the following storage products.
- Hitachi Universal Storage Platform V
- Hitachi Universal Storage Platform H24000
- Hitachi Universal Storage Platform VM
- Hitachi Universal Storage Platform H20000

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.NOEVIL	Within the users of Storage Navigator, the storage administrator, the account administrator and the audit log administrator are assumed to be trusted as the person who have sufficient skills to execute the administration and operation of a whole storage device, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior. The storage partition administrator and the account partition administrator are assumed to be trusted as the person who have sufficient skills to execute the administration and operation within the area where approved by the administrator who has the authorization, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.
A.NOEVIL_MNT	Maintenance staff is assumed to be trusted as the person who has the sufficient skills to safely execute the general maintenance operations of the storage device, including the connecting operations between the host and the port on CHA, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.
A.PHYSICAL_SEC	A storage device is assumed to be set at a secure area where only the storage administrator, the account administrator, the audit log administrator and the maintenance staff are allowed to enter and exit, and the device is completely protected from any unauthorized physical access. Note) This is included the protection related to internal LAN.
A.ILLEGAL_SOFT	The administrator client PC is assumed to be never installed illegal software.
A.CONNECT_STORAGE	TOE has a function that acquiring the data copy or the backup copy of the data between the storage devices by connecting the other storage devices.

	Once this function is used, the modifying or browsing of the user data that is the property to be protected of TOE becomes available. The operations of these functions are assumed to be done by the reliable storage administrator only.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

<Japanese>
- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000 ISO15408 Certification Instructions Manual
- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000 User Guidance

<English>
- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM ISO15408 Certification Instructions Manual
- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM User Guidance

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 2007-08 and concluded by completion the Evaluation Technical Report dated 2008-12. 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. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2008-08 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 2008-08.

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

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

2.3 Product Testing

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

2.3.1 Developer Testing

1) Developer Test Environment

The configuration of the test executed by the developer are shown in Figure 2-1, and Table 2-1.

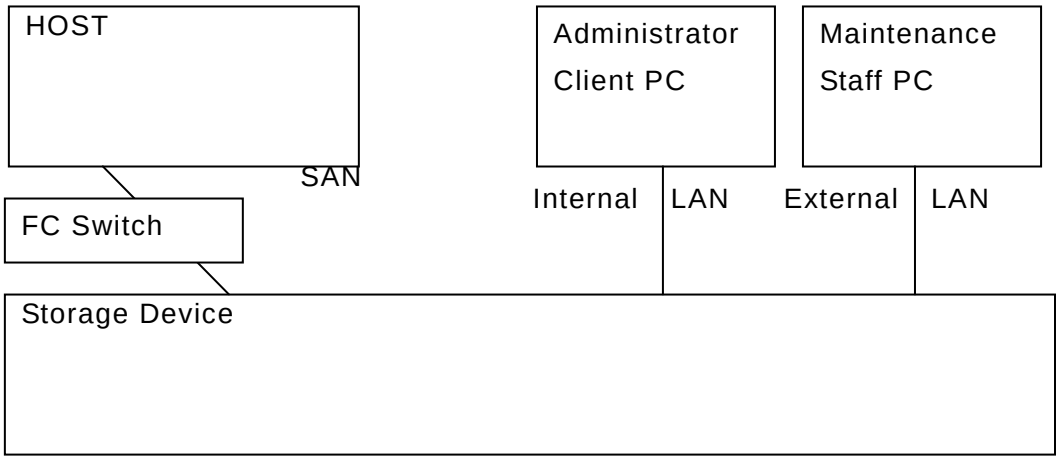

Figure 2-1 Configuration of Developer Testing

Table 2-1 Test Components

Component	Using Equipment / Software
Storage Device (Including TOE, and Maintenance Staff PC)	Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000 [TOE] - DKCMAIN Microprogram Version 60-02-32-00/00 - SVP Program Version 60-02-26/00 (Including Storage Navigator of the maintenance staff PC)
Host	Windows 2000 SP3 CPU: Intel Xeon 2.0 GHz
Administrator Client PC	Windows XP Professional (SP2) -CPU: Pentium 4, Equal to 2.4 GHz or better; Recommended: Pentium 4, 3 GHz or better -RAM: 1GB or more; Recommended: 1 GB or more -Available HDD space: 150 MB or more -Monitor: High-Color 16-bit or better; Resolution: 1024x768 or better -Ethernet LAN card: 100Base-T
FC Storage Network	Cisco Type: MDS 9216i 2Gbps 14 port
Web Server	Apache Version 2.2.4
Web Browser	Internet Explorer 6.0 SP2
Java Runtime	JRE 1.5.0_06

2) Outlining of Developer Testing

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

a. Test configuration

Figure 2-1 shows the structure of the test executed by the developer. The developer's test is done in the same TOE test environment with the TOE configuration identified by the ST.
The same TOE is installed in the Hitachi Universal Storage Platform VM and Hitachi Universal Storage Platform H20000. The differences of each device are just the available disk capacity, the number of fibre channel port, and the bland

name to be presented on the market. Since the hardware and the software related on the TOE are the same, the tests are executed at just one type of storage device.

b. Testing Approach

For the testing, following approach was used.
1. Verify that the parameter input in the Storage Navigator is displayed in the operation result screen.
2. Verify that the audit log is obtained by each operation from the Storage navigator, and the contents of the audit log must be the same with the contents of the audit log reference guide.
3. Verify the access result of host with the test tool by capturing the display when the host accessed to TOE.

c. Scope of Testing Performed

Testing is performed about 134 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.

d. Result

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

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Figure 2-1 shows the structure of the tests executed by the evaluators. The evaluator's tests are done in the same TOE test environment with the TOE configuration identified by the ST.

b. Testing Approach

The tests are done with the same methods of the developer's test.

c. Scope of Testing Performed

Totally 65 items are done in this evaluator's test: 13 independent tests invented by the evaluators, 11 intrusion tests, 41 tests from the sampling of the

developer's test. The selection criteria of the test items are considered the following descriptions.

1. Execute the additional parameter tests from the SOF point of view and different from the developer's test (Independent test).
2. Execute at least one test in each subset of the tests provided by the developer to confirm if the tests executed by the developer are valid (Sampling test).
3. Although there is no logical problem on the rationale of the developer that the vulnerability must not be misused, execute the tests to confirm (disproof) if this vulnerability has a problem on the different methods and conditions (Penetration test).
4. Execute the test to check whether it has an obvious vulnerability on the operating environment elements (JRE: Java Runtime Environment), which is not considered by the developer, in the intended environment by the TOE.

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 EAL2 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

- The storage devices installing TOE are also sold outside Japan, but the subject of this evaluation is for the one manufactured and shipped by Hitachi, Ltd., Disk Array Systems Division.
- The host controlling (protecting SAN information against tampering etc.) is out of concern of the TOE.

5. Glossary

The abbreviations used in this document are described in the following.

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

The abbreviations specific for TOE used in this document are described in the following.

CHA	Channel Adapter
DKA	Disk Adapter
DKC	Disk Controller
LAN	Local Area Network
SAN	Storage Area Network
SVP	Service Processor
WWN	World Wide Name

The terminologies used in this document are described in the following.

Cache Memory	Tentative high-speed storage area of the data that is recently accessed or frequently accessed.
Disk Subsystem	It means Storage Device and represents Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform VM etc.
Fibre Channel	High-speed network technology to build the Storage Area Network (SAN).
Port	The end of the fibre channel. Each port is identified by the port number.
CLPR (Cache Logical Partition)	It is a partition logically created by partitioning the cache memory. More than one parity group is allocated in the CLPR.
FC-SP	Fibre Channel Security Protocol. This is a protocol to authenticate each device when communicating between the host or the fibre channel switch and the storage device.
LDEV	This is short for Logical Device. It is a unit of volume to be created in the user area of the storage device. It is also called as Logical Volume.
LU (Logical Unit)	LDEV to be used from the host is called LU. On the fibre channel interface, It is possible to access to LU which is mapped

	one or more LDEV.
LU Path	Data input/output channel, which connects a host for open system and LU.
LUN (Logical Unit Number)	This is LDEV that can be accessed from a host by associating with a fibre channel port. Or, the address where the volume allocated for the open system.
SLPR	Storage Logical Partition. It is a partition logically created by partitioning the cache and the hard disk drive in the storage device. More than one CLPR and more than one target port are allocated.
WWN (World Wide Name)	A 64bit address used in fibre channel networks to uniquely identity each element.

6. Bibliography

[1] Hitachi Universal Storage Platform V Security Target Version 1.13 (October 8, 2008) Hitachi, Ltd.

[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 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] Evaluation Technical Report (URE-ETR-0001-02) Version 1.2, December 8, 2008,