CRP-C0315-01

Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-10-26 (ITC-0313)
Certification No.	C0315
Sponsor	Hitachi Ltd.
Name of the TOE	Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 Control Program
Version of the TOE	70-02-05-00/00(R7-02-06A)
PP Conformance	None
Assurance Package	EAL2
Developer	Hitachi Ltd.
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.
2011-09-30

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

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 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 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

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 Control Program, Version 70-02-05-00/00(R7-02-06A)" (hereinafter referred to as the "TOE") developed by Hitachi Ltd., and the evaluation of the TOE was finished on 2011-08-31 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Hitachi Ltd. and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This certification report assumes "general consumers" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions is as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL2.

1.1.2 TOE and Security Functionality

This TOE is a program dedicated to run a large-scale storage system, "Hitachi Virtual Storage Platform (also known as "Hitachi Virtual Storage Platform VP9500"). This TOE has functions that identify and authenticate the host computer (hereinafter referred to as "host") when it connects with Hitachi Virtual Storage Platform (hereinafter referred to as "storage system") to read/write data and control reading/writing to the designated storage area from the host computer. This TOE has a function that safely manages the encryption key, which is used when the storage system encrypts data and stores it in the storage area, and a function that safely erases the data from the storage area.

The TOE also identifies and authenticates TOE users (storage administrators, maintenance personnel) and safely provides the following functions to operate the storage system within their given authority. Storage administrators use the functions to set various information for the TOE to identify and authenticate the host and the functions to set the corresponding storage area and set the rule for controlling access to the area. Maintenance personnel who perform maintenance operations use the functions to make various settings when installing the storage system, replacing hardware, or recovering from failures, and the setting functions to connect the TOE to the network and connect external authentication servers and remote desktop client.

To prevent these security functions from being exploited, the TOE identifies and authenticates users to permit only the following TOE users (security administrators, audit log administrators) to use the functions to manage the TOE. Security administrators use the function to manage users' accounts, the function to manage resources such as users' groups and storage areas, and the functions to set security functions, such as the functions to identify and authenticate hosts and fibre channel switches and the encryption-related functions. Audit log administrators use the function to view audit logs. The TOE and the program required for the TOE operation identify and authenticate each other and use encrypted communication.

Regarding these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the assurance package. Assumed threats and assumptions are as described in the following section.

1.1.2.1 Threats and Security Objectives

This TOE counters each threat by using the security functions as follows.

To prevent unauthorized hosts that are not allowed to connect to the storage system from accessing and falsifying the user data of the storage users stored in the storage device of the storage system, the TOE allows host connections, establishes secure communication between the host and the TOE, and controls access to the host to permits only hosts that are permitted to connect the storage system to access the user data.

To prevent the settings of the TOE security functions from being changed by attackers who connect the TOE management interface and prevent user data of the storage users stored in the storage device of the storage system from being illegally accessed and falsified, the TOE performs identification and authentication of TOE users (security administrators, storage administrators, audit log administrators), controls user access, performs SSL communications between the Storage Navigator program and the SVP program, and manages security functions. Thus, it prevents the settings of the TOE security functions from being illegally changed.

In addition, to prevent the remaining data in the storage device of the storage system from being leaked, it performs the encryption key management function that supports encryption of user data stored in the storage device and the shredding function that erases the remaining data by overwriting the used area of the storage device with dummy data. The TOE logs events related to security functions to prevent and reduce improper operations.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

The storage system that contains the TOE, the host (including fibre channel connection adapter), fibre channel switch, other storage system, and external authentication server should be installed in a secure area where only authorized people can enter and exit. To avoid illegal use of the storage system described above, the security administrator needs to properly operate and manage users, configurations, and security measures, etc., of the storage system.

The management PC should be installed in a location where it can be monitored directly to avoid unauthorized use while it is connected to the network in which direct access from external network is restricted. The following should also be performed; to identity and authenticate the users and administrators of the management PC, to manage their accounts, to install antivirus software, to apply the security patches, and to restrict installation of dangerous software, etc.

For communications between the TOE and the external authentication servers, one of the following protocols should be used; LDAPS, starttls, or RADIUS (CHAP authentication). When using the RADIUS protocol, the CHAP secret should be used to perform CHAP authentication because the external authentication server supports the RADIUS protocol that can use the CHAP authentication using the CHAP secret.

Security administrators, audit log administrators, and maintenance personnel must not engage in inappropriate actions.

1.1.3 Disclaimers

The TOE does not counter the following threats. In addition, the TOE cannot assure safety in information security if the TOE is used as follows.

- The TOE cannot counter such a threat if an attacker gains control of the host, which is connected to the storage area network or the TOE, sets or changes WWN or secret used by the TOE to identify/authenticate the host, and impersonates the host to connect to the TOE. When an attacker gains control of the host connected to the TOE, safety is not assured.

- Maintenance personnel must not log into the TOE from the external LAN.

- If syslog transfer of audit log is performed, the security of the audit log in the target is not assured.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation and completed on 2011-08 based on functional requirements and assurance requirements of the TOE, according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] and Observation Reports prepared by Evaluation Facility as well as evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 Control Program
Version of the TOE:	70-02-05-00/00(R7-02-06A)
Developer:	Hitachi Ltd.

The TOE consists of the following two programs.

Name of the TOE:	DKCMAIN micro-program
Version of the TOE:	70-02-05-00/00
Developer:	Hitachi Ltd.

Name of the TOE:	SVP program (Including the Storage Navigator program)
Version of the TOE:	70-02-03/00
Developer:	Hitachi Ltd.

In addition to the programs described above, additional programs exist for the connected host types, but the TOE does not include those options.

Users are able to confirm that the product is the TOE that has been evaluated and certified by using the following method. In accordance with the procedure described in the maintenance manual for maintenance personnel, the versions of the DKCMAIN micro-program and the SVP (Service Processor) program from the menu of the Storage Navigator program or the SVP program are displayed. By comparing the name and the version with the descriptions in the user's manual for users with those in the maintenance manual for maintenance personnel, users can confirm that the installed product is the evaluated TOE.

3. Security Policy

This chapter describes the security function policy that is adopted for the TOE to counter threats and the organizational security policy.

The TOE is a program that controls access from the host connected with the storage system to the protected user data stored in the storage system and provides a function to manage the settings.

The security functions of the TOE prevent user data from being falsified and leaked via the host by identifying the host and controlling accesses, securely manage the encryption key used by the storage system for the encryption processing of user data, and prevent user data from being leaked from the removed hard disks by completely erasing the user data.

The TOE identifies and authenticates TOE users and permits the use of the functions to operate the storage system and to manage the TOE within the authority of the users to avoid inappropriate use of the functions. For the communication between the TOE and the external server or the Storage Navigator program via the external LAN, mutual identification/authentication and encrypted communication are used to prevent the impersonation of TOE users. The TOE also records the events related to the security functions, and prevents and reduces improper operations.

The TOE has the mechanism to protect implementation of these functionalities.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1. and to meet the organisational security policy shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3.1-1 and provides the functions for countermeasure against them.

Table 3.1-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_XCNTL	If Storage Navigator user or maintenance personnel wrongly uses a function outside own authority, an LDEV storing user data may be accessed by the host that is not allowed to access the LDEV, and eventually the user data may be leaked.

Identifier	Threat
T.TSF_COMP	If a third party who can connect to the external LAN makes an unauthorized connection on the channel between the Storage Navigator program and the SVP PC, or between the SVP PC and the external authentication server and obtains the communication data including user ID and password of a Storage Navigator user, he/she impersonates the Storage Navigator user and changes the storage system setting, and eventually may access the LDEV where the user data are stored.
T.LP_LEAK	If a third party, such as host administrator, who is allowed to use the host, accesses any LDEV other than those allocated to the host, the user data may be leaked or falsified.
T.CHG_CONFIG	If a third party, who can access the external LAN, changes the storage system setting by taking advantage of the Storage Navigator program, he/she can access the LDEV, where the user data are stored, and eventually the user data may be leaked, falsified and deleted.
T.HDD_THEFT	From a hard disk which maintenance personnel takes out from the storage system, the user data may wrongly be leaked.
T.HDD_REUSE	If a storage administrator reuses the storage system or hard disk, the user data remained in it may be leaked to users of the storage system.

Note that this TOE does not counter the following threats.

- When an attacker takes control of the host, or the following threats that occur in this case:
  > The host that is taken over accesses user data on the LDEV assigned to the host, and leaks, falsifies, and deletes them.
  > The host that is taken over impersonates another host and accesses the user data on the LDEV assigned to another host, and leaks, falsifies, and deletes them.

- When the storage administrator restores or synchronizes user data to the local storage system from the target storage system, the user data in the storage system may be falsified, and the user data in the local storage may also be falsified.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3.1-1 by the following security function policies.

(1) Countermeasure to the threat “T.ILLEGAL_XCNTL”

If Storage Navigator user or maintenance personnel wrongly uses a function outside own authority, an LDEV storing user data may be accessed by the host that is not allowed to access the LDEV, and eventually the user data may be leaked.

To counter the threat, the TOE identifies and authenticates Storage Navigator users and maintenance personnel, and limits the functions that can be used by Storage Navigator users and maintenance personnel to those within the authority. In addition, since the TOE records the events related to security to logs, it can discover and track improper operations. Thus, the TOE counters the above threat.

(2) Countermeasure to the threat “T.TSF_COMP”

If a third party who can connect to the external LAN makes an unauthorized connection on the channel between the Storage Navigator program and the SVP PC, or between the SVP PC and the external authentication server and obtains the communication data including user ID and password of a Storage Navigator user, he/she impersonates the Storage Navigator user and changes the storage system setting, and eventually may access the LDEV where the user data are stored.

The TOE counters the threat of wiretapping on the external LAN by using encrypted communication for communications between the Storage Navigator program and the SVP PC as well as between the SVP PC and the external authentication server. Therefore, a third party who can connect to the external LAN is unable to obtain the user ID and the password of the Storage Navigator user to impersonate the Storage Navigator user. In addition, the user ID, the password, and the group information of the Storage Navigator users registered in the external authentication server are managed properly, so it is impossible to register a user ID and a password of an invalid Storage Navigator user to the external authentication server to impersonate a normal Storage Navigator user and log in.

(3) Countermeasure to the threat “T.LP_LEAK”

If a third party, such as host administrator, who is allowed to use the host, accesses any LDEV other than those allocated to the host, the user data may be leaked or falsified.

The TOE identifies and authenticates the host and permits only access to the permitted LDEV from the host, based on the security attribute of the identified host. Storage systems, hosts, and fibre channel switches are installed in a physically protected secure area where entrance and exit are managed properly. Therefore, a physical connection between the host fibre channel connection adapter and the fibre channel switch port as well as one between the channel adapter port of the TOE and the fibre channel switch port are protected. In addition, as for fibre channel switches, the communication path between the host and the fibre channel switch, between the fibre channel switch and the TOE, and the communication path from the host to the TOE on the fibre channel switch are properly set and maintained. Thus, it counters the threat except for the case where an attacker gains control of the host.

(4) Countermeasure to the threat “T.CHG_CONFIG”

If a third party, who can access the external LAN, changes the storage system setting by taking advantage of the Storage Navigator program, he/she can access the LDEV where the user data are stored, and eventually the user data may be leaked, falsified and deleted.

The TOE identifies and authenticates Storage Navigator users and maintenance personnel and rejects login for one minute if login fails three times in a row. Therefore, invalid login to the Storage Navigator program by a third party who can connect to the external LAN is reduced. In addition, the TOE records events related to security to logs, so it can discover attempts to login to the Storage Navigator program by a third party and suspicious TOE setting changes and reduce the threat by taking appropriate actions.

(5) Countermeasure to the threat “T.HDD_THEFT”

From a hard disk which maintenance personnel takes out from the storage system, the user data may wrongly be leaked.

The storage system encrypts user data by using the installed encryption device (LSI for encryption processing) and stores them in a hard disk or decrypts them to send to the host. The TOE safely creates or discards the encryption key to be used at the time. User data on hard disks are always encrypted, and the TOE manages the encryption key securely so that the encrypted user data would not be decrypted even if the hard disks are removed. Thus, it counters the above threat.

(6) Countermeasure to the threat “T.HDD_REUSE”

If a storage administrator reuses the storage system or hard disk, the user data remained in it may be leaked to users of the storage system.

The TOE overwrites the user data in the storage area when stopping the use of the storage area on the hard disk assigned to the host or when replacing the hard disk in the storage system to counter the threat of leakage of user data from the removed hard disk.

3.1.2 Organisational Security Policy and Security Function Policy

3.1.2.1 Organisational Security Policy

Organisational security policy required in use of the TOE is shown in Table 3.1-2.

Table 3.1-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.MASQ	If a storage user requests authentication of the host, the host is authenticated when connecting the host to the storage system.

Customers whose storage users pay for the use of storage system may request authentication of the host connected to the storage system to improve the security of user data.

3.1.2.2 Security Function Policy to Organisational Security Policy

The TOE provides the security functions to fulfill the Organisational Security Policy shown in Table 3.1-2.

(1) Means to support the organizational security policy “P.MASQ”

The TOE uses FC-SP (Fibre Channel Security Protocol) to authenticate the host. Therefore, the host installs the FC-SP compliant fibre channel connection adapter and sets the driver that supports FC-SP. Storage area network (hereinafter referred to as “SAN”) consists of the FC-SP compliant fibre channel switches.

The fibre channel switch uses FC-SP to connect with the host and identifies and authenticates the host. The fibre channel switch uses FC-SP to connect with the TOE and identifies and authenticates the channel adapter (CHA) of the TOE. After that, the host requests connection to the TOE via the fibre channel switch, the TOE identifies the host, and the connection between the host and the TOE is established. Since the host and the TOE are connected using FCP (Fibre Channel Protocol) instead of FC-SP, the TOE cannot directly authenticate the host.

Note that since the host, fibre channel switch, and the storage system are installed in a physically protected secure area and managed properly, these physical port connections are protected. Attackers cannot connect fake hosts, either. In addition, the fibre channel switch identifies and authenticates the fibre channel switch port as well as the host and the TOE that are connected with the port to maintain the unique combination, and assures the unique connection status from the fibre channel connection adapter port of the host to the fibre channel connection adapter port of the TOE via the fibre channel switch port. Therefore, the connection between the host and the TOE is considered as the state in which the TOE authenticates the host.

Consequently, it is considered that the TOE satisfies the organizational security policy.

4. Assumptions and Clarification of Scope

In this chapter, it describes the assumptions and the operational environment to operate the TOE as useful information for the judgment before the assumed reader uses the TOE.

4.1 Usage Assumptions

Table 4.1-1 shows assumptions to operate the TOE. The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4.1-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.NOEVIL	Among Storage Navigator users, the security administrator and audit log administrator are assumed to be the qualified persons who are capable of operating and managing the entire storage system, execute proper operations as specified by manuals, and never commit any wrongdoing. The storage administrator is assumed to be the qualified person who is capable of managing and operating a disk subsystem within the range permitted by the security administrator, executes proper operations as specified by manuals, and never commits any wrongdoing.
A.NOEVIL_MNT	Maintenance personnel is assumed to be the qualified person who is capable of doing maintenance safely for the entire storage system, including connection of the host and a port on CHA, executes proper maintenance operations as specified by manuals, and never commits any wrongdoing.

Identifier	Assumptions
A.PHYSICAL_SEC	A storage system, host (including fibre channel connection adapter), fibre channel switch, other storage system and external authentication server are assumed to be set in a secure area where only permitted persons can enter and exit under the security administrator's responsibility, and observed properly to protect from unauthorized use.
A.MANAGE_SECRET	The secret for host authentication set in the host is assumed to be controlled under the security administrator's responsibility to protect from use by unauthorized person.
A.MANAGEMENT_PC	Storage Navigator users are assumed to properly set and manage the management PC, so that it would not be used inappropriately. The following shows examples of assumptions applied to the management PC. - The management PC shall be set in an office area etc., where it can be managed directly. - The management PC must not be accessed directly from external network. - The management PC identifies and authenticates users. - The administrator authority of the management PC shall be managed. - The countermeasures for malicious codes shall be implemented by restricting software installation, installing anti-virus software, and applying security patches.
A.CONNECT_STORAGE	The TOE is assumed to connect other storage system installed with the TOE.
A.EXTERNAL_SERVER	For communications between the TOE and external authentication servers, one of the following protocols is assumed to be used: LDAPS, starttls, or RADIUS (CHAP authentication). The user identification information and the user group information on the TOE and those on the external authentication server are assumed to be properly registered and managed and to be consistent with each other.

The detailed conditions etc., are added to the above assumptions as follows.

- A.EXTERNAL_SERVER

  When the RADIUS protocol is used, it is assumed that CHAP authentication is performed by using the CHAP secret. Therefore, when the RADIUS protocol is used, the external authentication server is assumed to support the RADIUS protocol that can use the CHAP authentication with the CHAP secret.

4.2 Environment Assumptions

The storage system installed with the TOE, SAN (including fibre channel switch), host (including fibre channel connection adapter), other storage system, external authentication server, and maintenance PC are installed in a physically protected secure area where entrance and exit are controlled and managed properly. The management PC is set in an area where the security administrator can manage directly. The storage system installed with the TOE, the external authentication server, and the management PC are connected to the external LAN. Figure 4-1 shows the general operational environment of the TOE.

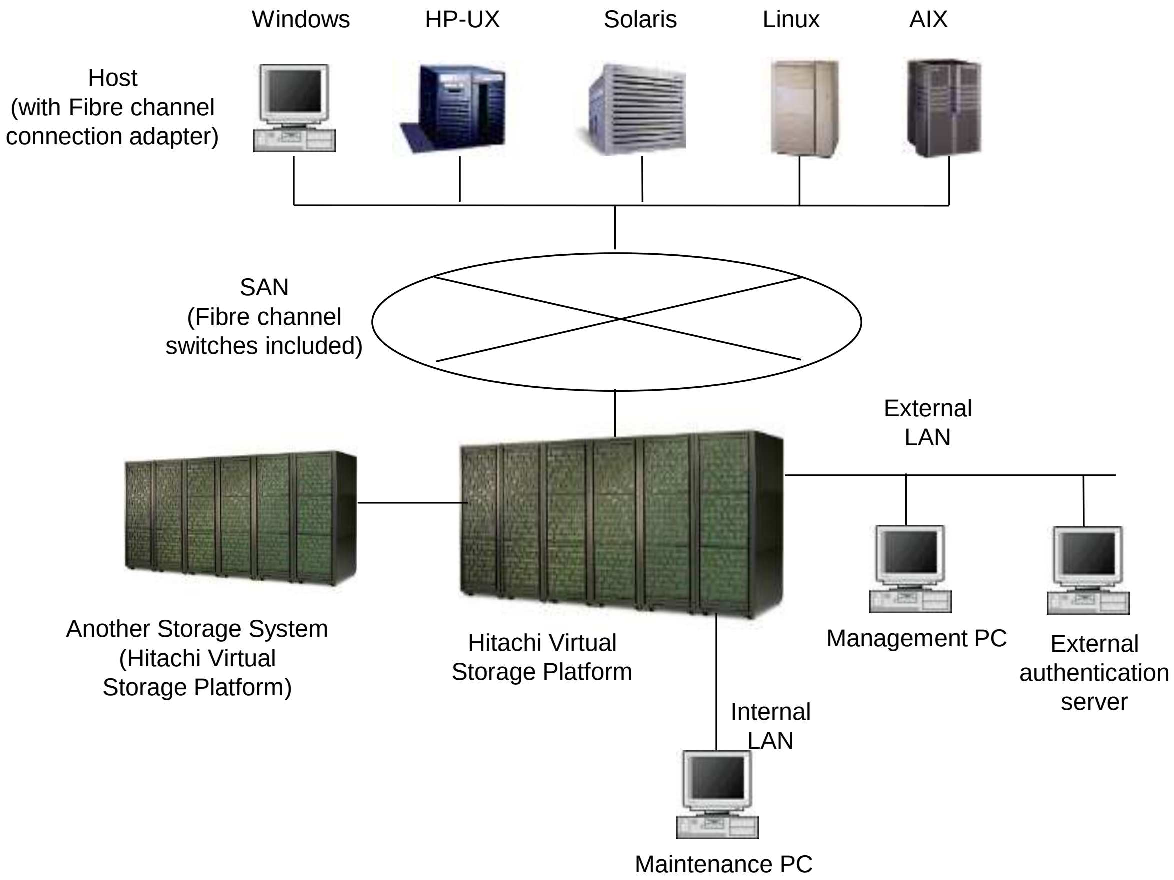

Figure 4-1 Operational environment of the TOE

The storage system installed with the TOE and the host (including the fibre channel connection adapter) connect to the SAN (including fibre channel switch) and communicate each other. SAN should not be connected to other network. The storage system installed with the TOE is connected with other storage system directly without SAN. The external LAN should not be connected directly to external network, such as the Internet, and the management PC cannot be accessed directly from outside.

For the management PC, the security administrator manages the authority of users of the management PC and requires identification and authentication of users. In addition, the anti-virus software needs to be installed, the security patch needs to be applied, and security measures, such as restricting installation of unnecessary software, need to be taken in the management PC.

In the storage system installed with the TOE, the encryption device (LSI for encryption processing) to encrypt/decrypt user data is installed. The storage system, fibre channel switch, and the fibre channel connection adapter shown in this configuration are not covered in this evaluation, but they should be sufficiently reliable.

The TOE uses FC-SP to connect with hosts (Windows, HP-UX, Solaris, Linux, AIX) installed with fibre channel connection adapter that complies with the commercially available FC-SP. Note that the developer has not confirmed the provision of drivers for fibre channel connection adapters that support FC-SP. When the host connects with the port of the channel adapter of the TOE via a port of the fibre channel switch, it is assumed that the security that is equivalent to the state in which the TOE identifies/authenticates the host using FC-SP is assured, according to the FC-SP connection between the fibre channel switch and the TOE and the operations and management status of SAN and fibre channel switch.

4.3 Clarification of Scope

The TOE has a security function that controls access from the host to LDEV by identifying/authenticating hosts connected with the TOE and a security function that controls the function to manipulate TOE settings by identifying/authenticating the TOE users. Since it is assumed that the TOE trusts TOE users and devices connected to the TOE, it does not counter the following threats that are not included in the scope of the TOE and the assumptions.

- The TOE has the basic function “Hitachi Universal Volume Manager (External storage management function)” that is used to connect multiple storage systems of different models with the storage system installed with the TOE. However, the configuration in which multiple storage systems of different models are connected with the storage system installed with the TOE is not assumed in this evaluation. To use this configuration, the security administrator and the storage administrator need to take responsibility.
- The TOE has the function to back up the backup file of the encryption key, the TOE setting information, and the TOE user information outside the TOE, such as the management PC. The TOE cannot counter the leakage and falsification of the TOE setting information and the TOE user information that are backed up outside the TOE. The security administrator needs to take responsibility for security measures of IT environment and operation management. (Because the backup file of the encryption key is encrypted, it counters the leakage and falsification.)
- In case of the connection configuration, in which user data are backed up from the other storage system installed with the TOE to the storage system installed with the TOE, the storage system installed with the TOE cannot trust the storage administrator of the other storage system installed with the TOE. Therefore, if the storage administrator of the other storage system installed with the TOE executes a command to read/write the user data in the storage system installed with the TOE, the user data may be leaked or falsified.

If the functions described above are used or the operational environment of the TOE is configured, they are not covered in this evaluation, and the security administrator and the storage administrator need to take responsibility.

5. Architectural Information

This chapter explains the scope of the TOE and the main components (subsystems).

5.1 TOE boundary and component

Figure 5-1 shows the configuration of the TOE. The TOE that is installed in the storage system is classified into the DKCMAIN micro-program (including OS) and the SVP program including the Storage Navigator program. The hardware of the storage system in which the TOE runs and the OS on the SVP PC that runs the SVP program are not covered in the TOE.

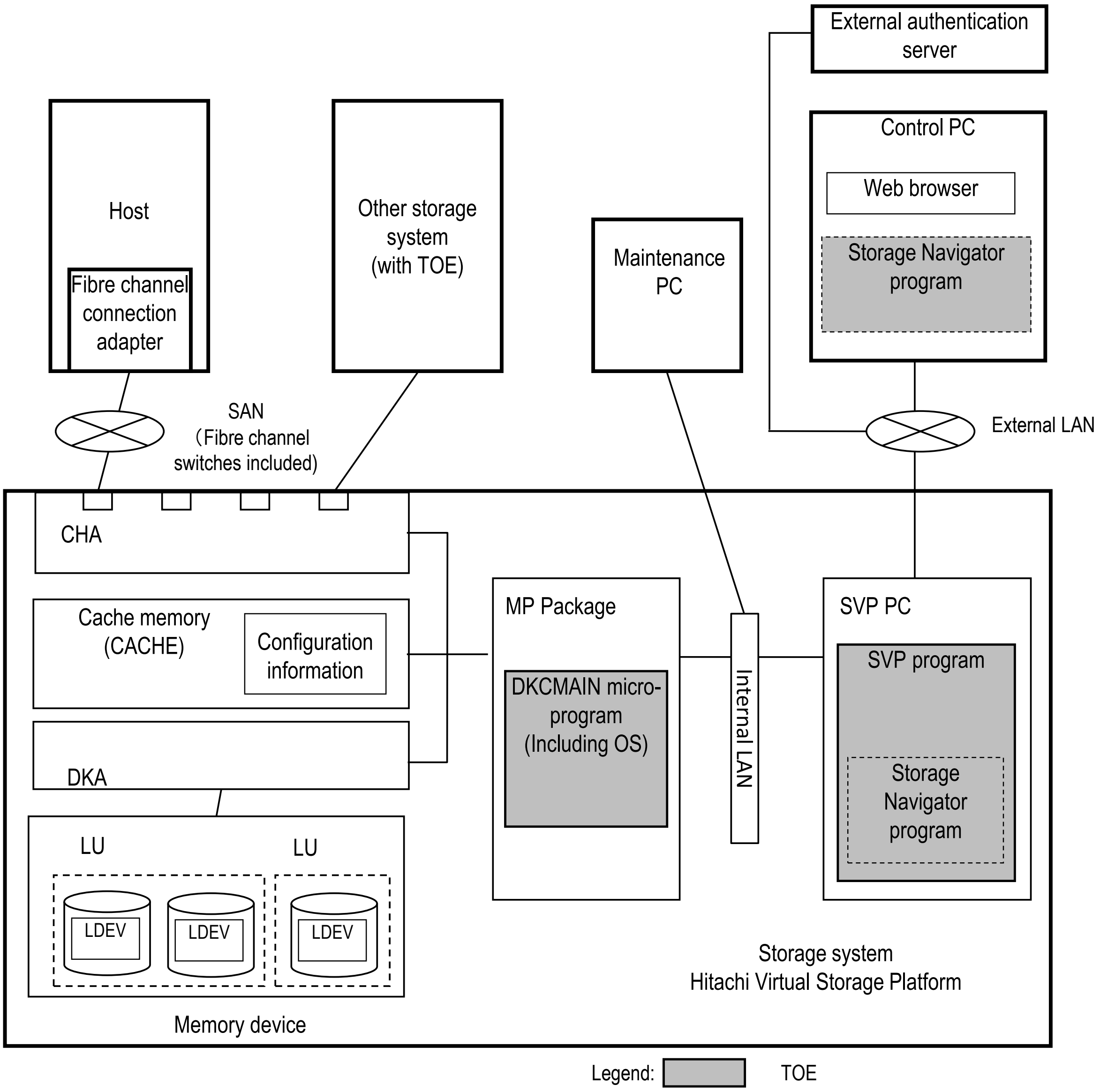
External authentication server
Control PC
Web browser
Storage Navigator program
Host
Fibre channel connection adapter
Other storage system (with TOE)
Maintenance PC
SAN (Fibre channel switches included)
External LAN
CHA
Cache memory (CACHE)
Configuration information
DKA
LU
LU
LDEV
LDEV
LDEV
Memory device
MP Package
DKCMAIN micro-program (Including OS)
Internal LAN
SVP PC
SVP program
Storage Navigator program
Storage system
Hitachi Virtual Storage Platform
Legend:
TOE

Figure 5.1 TOE boundary

The following describes the DKCMAIN micro-program (including OS) and the SVP program including the Storage Navigator program that constitute the TOE.

(1) DKCMAIN micro-program

The DKCMAIN micro-program is a control program of the storage system that controls host connections, data transfer between the host and the storage system, and data input/output to storage devices; manages encryption keys and security function data; and provides the shredding function. It is installed and runs in the MP package in the storage system. The following shows the major security functions of the DKCMAIN micro-program.

- Connection control of host/fibre channel switch (FC-SP/FCP connection)
  > Identification and authentication of host/fibre channel switch (DH-CARP authentication (Response verification including secret))
  > Host access control to logical units (LU)

- Role-based access control for security function data

- Encryption key management (to create and delete)

- Shredding function

- Settings to run/stop security functions
  > Setting of the FC-SP authentication function
  > Setting of the stored data encryption function

- Management of security function data (to create, modify, and delete)
  > WWN, secret management
  > Management of resource group information, LU path information, LDEV information
  > Management of users' role information
  > Backing up/restoring encryption keys (Encryption/decryption of the encryption key using the protection key, hash verification of the encryption key)

(2) SVP program

The SVP program is management software that performs operations and maintenance of the storage system and manages the configuration information by establishing remote desktop connection with the Storage Navigator program, performing identification and authentication of the TOE users, providing the interface to set the TOE, and requesting settings to the DKCMAIN micro-program. The SVP program is installed and runs in the OS (Windows Vista Business) on the SVP PC. The following shows the major security functions of the SVP program.

- Identification and authentication of SVP program users
  > Identification and authentication of users (security administrators, storage administrators, audit log administrators, maintenance personnel)
  > Rejecting access when authentication fails in a row
  > Internal authentication function, external authentication function, communication with external authentication server (authentication, encryption)

- Management of accounts and host information (to create, change, and delete)
  > Management of user information (User ID/password) and user group information
  > Quality verification of passwords and secret

- SSL connection of the Storage Navigator program and remote desktop connection

- The window control function of the SVP program

- Role-based control of setting requests for the DKCMAIN micro-program
  > Control of setting requests of security functions
  > Control of requests to run/stop security functions
  > Control of requests to manage data of security functions

- Settings of security functions
  > Setting of the internal authentication method/external authentication method
  > Connection setting of the external authentication server

- Input/output of setting file
  > Reading/writing backup file of encryption key
  > Reading/writing the configuration information file (CFL: Configuration File Loader)
  > Checking the configuration information file format

- Audit log function
  > Recording and storing audit logs (Wrap-around method)
  > Outputting audit logs

(3) Storage Navigator program

The Storage Navigator program is a client program that connects to the SVP program and provides the graphical user interface to operate the SVP program. The Storage Navigator program runs on the Web browser of the management PC. SSL communication is used between the Storage Navigator program and the SVP program.

5.2 IT Environment

The DKCMAIN micro-program and the SVP program that constitute the TOE run on the separate hardware, but they are connected via the internal LAN that is protected by the assumptions to communicate each other. The maintenance PC is also connected to the internal LAN and establishes the remote desktop connection to the SVP PC to use the SVP program.

The SVP program, the Storage Navigator program, and the external authentication server are connected via the external LAN. Because the external LAN is not protected by the assumptions etc., authenticated and encrypted communication is used between the SVP program and the Storage Navigator program and between the SVP program and the external authentication server. It is described in the guidance that the firewall needs to be set in the boundary between the SVP program and the external LAN.

The DKCMAIN micro-program and the host are connected via SAN that consists of a fibre channel switch. SAN and the fibre channel switch are physically protected, based on the assumptions, so that no third party would change the physical configuration of SAN. The fibre channel switch has secure settings to avoid inappropriate use.

This storage system uses the security functions of the TOE, such as SSL communication of the Storage Navigator program and the access control, and physically separates the DKCMAIN micro-program and the SVP program to protect user data on CHA, CACHE, DKA, and storage devices to be protected from invalid access from attackers who connect to the external LAN.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions. English versions of documents are English translations of the Japanese versions of documents. Contents of the English versions are the same as those of the Japanese versions except some parts. "Table 5.2-3 Disk subsystem maintenance manual" and "Table 5.2-4 Disk subsystem maintenance manual (English version)" show guidance documents for maintenance personnel.

Table 5.2-1 Users guide

No	Name of document attached to the product (Users guide)	Version
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500　ISO15408 Function of Acquiring Authentication; Instruction manual	1.6
2	Hitachi Virtual Storage Platform Storage Navigator User Guide	5
3	Hitachi Virtual Storage Platform Storage Navigator Messages	5
4	Hitachi Virtual Storage Platform for Open Systems	4
5	Hitachi Virtual Storage Platform Encryption License Key User Guide	3
6	Hitachi Virtual Storage Platform Volume Shredder User Guide	3
7	Hitachi Virtual Storage Platform Audit Log Reference Guide	3
8	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 User Guidance	1.2

Table 5.2-2 Users guide (English version)

No	Name of document attached to the product (Users guide)	Version
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Manual for Obtaining ISO15408 Certification	1.6
2	Hitachi Virtual Storage Platform Hitachi Storage Navigator User Guide	MK-90RD7 027-02f
3	Hitachi Virtual Storage Platform Hitachi Storage Navigator Messages	MK-90RD7 028-03a
4	Hitachi Virtual Storage Platform Provisioning Guide for Open Systems	MK-90RD7 022-02e
5	Hitachi Virtual Storage Platform Hitachi Encryption License Key User Guide	MK-90RD7 015-02a
6	Hitachi Virtual Storage Platform Hitachi Volume Shredder User Guide	MK-90RD7 035-02b
7	Hitachi Virtual Storage Platform Hitachi Audit Log User Guide	MK-90RD7 007-02d
8	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 User’s Guidance	1.2

Table 5.2-3 Disk subsystem maintenance manual

No	Name of document attached to the product (Disk subsystem maintenance manual)	Version
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500　ISO15408 Function of Acquiring Authentication; Maintenance manual	1.4
2	A/H-65AC A-65BC HT-40BC Disk Array System Maintenance Manual	REV.3
3	TEST PROCEDURE MANUAL for RAID700 CTO Unit	REV.2

Table 5.2-4 Disk subsystem maintenance manual (English version)

No	English version of disk subsystem maintenance manual	Version
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Obtaining ISO15408 Certification Maintenance Manual	1.4
2	DKC710I Maintenance Manual	REV.3

- "A/H-65AC", "A-65BC", "HT-40BC", "RAID700" and "DKC710I" are aliases of "Hitachi Virtual Storage Platform".
- There are some differences in delivery method and maintenance system between Japan and foreign countries. Therefore, the English version of No.2 of the maintenance manual slightly differs from the Japanese version of it. The description of "INSTALLATION SECTION" of the "DKC710I Maintenance Manual" is not written in the Japanese version of the manual. However, an equivalent description is written in the "TEST PROCEDURE MANUAL for RAID700 CTO Unit", which is No.3 of "Table 5.2-3 Disk subsystem maintenance manual"
- There is no English version of the "TEST PROCEDURE MANUAL for RAID700 CTO Unit", which is No.3 of "Table 5.2-3 Disk subsystem maintenance manual". This manual is used for installing the TOE by the person in charge of delivery when the TOE is delivered in Japan.

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-10 and concluded by completing the Evaluation Technical Report dated 2011-08. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-04 and examined procedural status conducted in relation to each work unit for configuration management and delivery and operation by investigating records and staff interview. Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-04 and 2011-05.

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

Concerns that the Certification Body found about the evaluation process was described as a certification oversight reviews, and they were sent to Evaluation Facility.

After Evaluation Facility and the developer examined it, these concerns were reflected in the evaluation report.

7.3 IT Product Testing

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

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual testing results. It explains the content of the developer testing evaluated by the evaluator as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration executed by the developer.

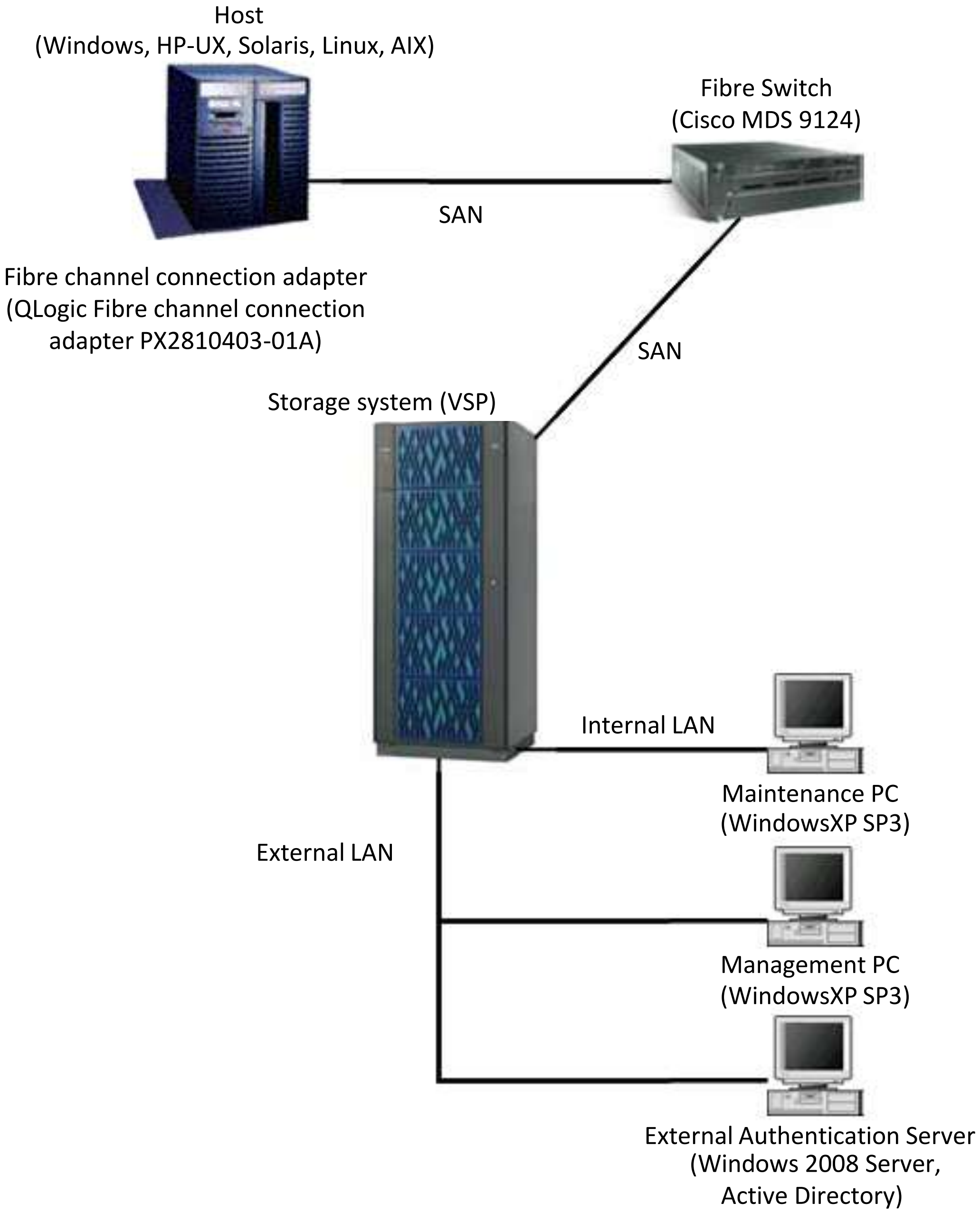

Figure 7-1 Configuration of the Developer Testing

In the developer testing, "Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 control program version 70-02-00-00/11 (DKCMAIN micro-program version 70-02-00-00/11, SVP program version 70-02-00/10)" was used. This is different from the TOE version described in the ST. The difference in the versions described above is caused by the modification of the RAID function, and it does not affect the security functions. The TOE has some options, but they are not covered by the TOE, so the TOE itself excluding options was evaluated.

The operational environment of the TOE assumes that the storage system to be evaluated is connected directly with other storage system installed with the TOE. The TOE has the function to internally reproduce the state that the storage system to be evaluated is connected with the other storage system installed with the TOE. When the function is used, the TOE behaves in the same way as the case in which other storage system is physically connected. Therefore, the tests related to the storage system to be evaluated and other storage system were conducted by using this function.

Table 7.3-1 Developer testing configuration

Terminal/ Device name	Product
Storage system (SVP PC)	OS: Windows Vista Business SP2 Web server: Apache Tomcat 6.0.16
Host	OS: Windows Server 2003 SP2, HP-UX, Solaris, Linux, AIX Fibre channel connection adapter: QLogic Fibre Channel Adapter PX2810403-01A
Fibre channel switch	Cisco MDS 9124 (4G/2G/1Gbps 24 ports)
Management PC	OS: Windows XP SP3 Browser etc.: Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
Maintenance PC	OS: Windows XP SP3 Browser etc.: Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
External authentication server	OS: Windows 2008 Server Authentication server: Active Directory

As described above, the developer testing was conducted in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of Developer Testing

Summary of the developer testing is as follows.

a. Developer Testing Outline

Outline of the developer testing is as follows.

<Developer Testing Approach>

From the Storage Navigator program and the maintenance PC, combinations of values that can be entered in the screen were tested for the external interface of the TOE. From the screen display and messages of the Storage Navigator program, the behavior of the TOE for input and the behavior related to the TOE and the external authentication server were confirmed indirectly.

The developer accessed the storage system by operating the host and confirmed the behavior from the TOE logs.

<Tools for the Developer Testing>

No tool was used in the developer testing except for the configuration described in Figure 7-1.

<Content of execution of the developer testing>

From the Storage Navigator program and the maintenance PC, the developer input data by directly manipulating the following available external interfaces (1) and (2) below and compared the window output with the expected testing results. Security functions, such as identification and authentication of Storage Navigator users and maintenance personnel and access control of setting data, were checked.

Regarding the interface with the host as shown in (3) below, the developer accessed the storage system by manipulating the host and compared the TOE logs with the expected testing results. Security functions, such as identification and authentication of hosts and access control of storage areas, were checked.

As for the external interface (4) below, the developer made related settings for the TOE from the Storage Navigator program and compared the messages etc., displayed in the Storage Navigator program with the expected testing results to check the TOE behavior indirectly. Security functions, such as identification/authentication and encryption of communication between the TOE and the external server, were checked.

(1) Interface between the TOE and Storage Navigator users (Management PC)

(2) Interface between the TOE and the maintenance PC

(3) Interface between the TOE and the host

(4) Interface between the TOE and the external authentication server

b. Scope of Execution of the Developer Testing

The developer testing is executed on 119 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested enough.

c. Result

The evaluator confirmed an approach of the executing developer testing and legitimacy of tested items, and confirmed consistencies between testing approach described in the testing plan and actual testing approach. The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results executed by the developer.

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by the test items extracted from the developer testing. The evaluator executed the evaluator independent testing (hereinafter referred to as "independent testing") to reconfirm that security functions are certainly implemented from the evidence shown by the process of the evaluation. It explains the independent testing executed by the evaluator as follows.

1) Independent Testing Environment

Table 7.3-2 and Figure 7-2 show the configuration of the independent testing executed by the evaluator. In the evaluator independent testing, only the configuration that uses the host installed with Windows Server 2003 was tested. In the developer testing, it was verified that OS (Windows, HP-UX, Solaris, Linux, AIX) on each host and the driver for the fibre channel connection adapter can be connected with the TOE using WWN and FCP, and the storage system can be operated normally. From the result of the developer testing, the evaluator determined that the above driver should run by being compliant with FCP and there should be no difference. Therefore, only the configuration of the host installed with Windows Server 2003 was tested in the evaluator independent testing.

Table 7.3-2 Evaluator independent testing configuration

Terminal/Device name	Product
Storage system (SVP PC)	OS: Windows Vista Business SP2 Web server: Apache Tomcat 6.0.16
Host	OS: Windows Server 2003 SP2 Fibre channel connection adapter: QLogic Fibre Channel Adapter PX2810403-01A
Fibre channel switch	Cisco MDS 9124 (4G/2G/1Gbps 24 ports)
Management PC	OS: Windows XP SP3 Browser etc.: Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
Maintenance PC	OS: Windows XP SP3 Browser etc.: Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
External authentication server	OS: Windows 2008 Server Authentication server: Active Directory

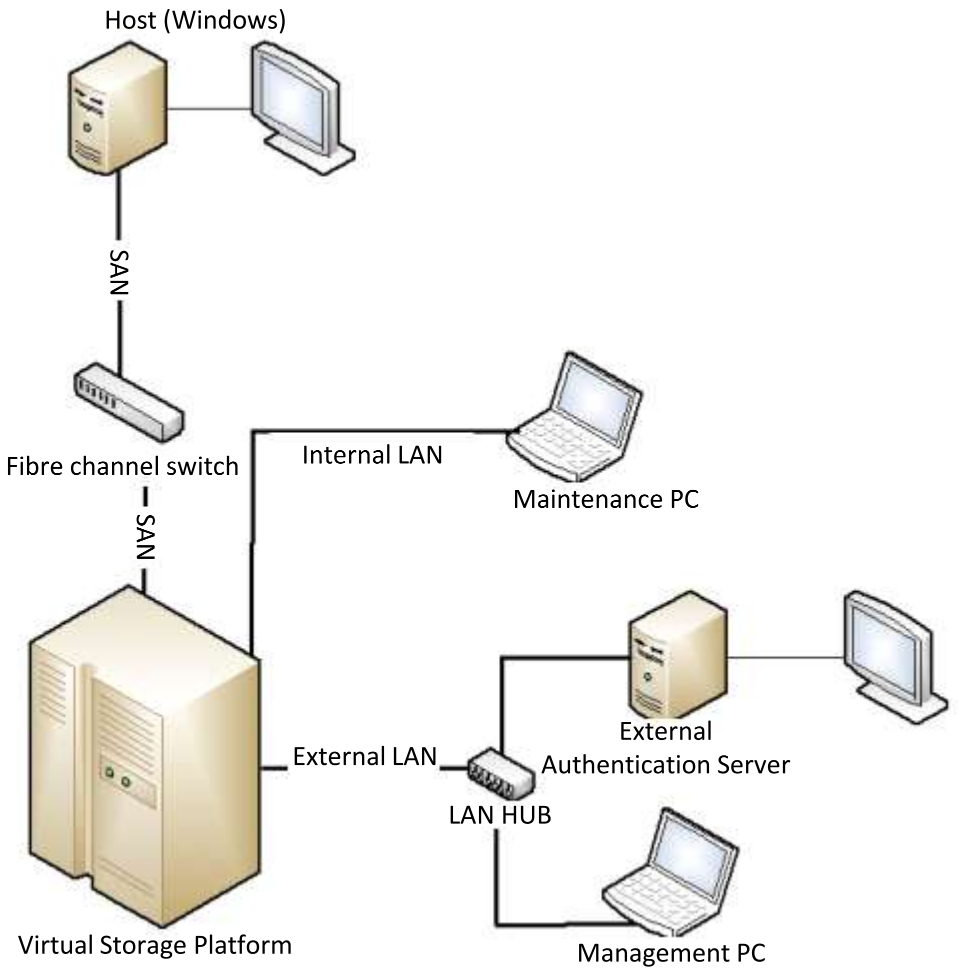

Figure 7-2 Independent Testing Configuration

The independent testing was executed in the same configuration as the TOE identified in the ST, except for the difference in the host OS described above and connection with other storage system.

2) Summary of Independent Testing

Summary of the independent testing performed by the evaluator is as follows.

a. Independent Testing Points of View

The evaluator devised the independent testing from the developer testing and the provided documentation in terms of the following viewpoints.

The evaluator tested at least one sample test for each of all the TOE security function interfaces. Based on the policy that nonbiased testing should be performed for all the four types of the TOE security function interfaces, the evaluator executed at least one independent testing for interfaces that have test items to be added.

<Viewpoints of independent testing>

(1) To confirm the management PC operations, maintenance PC operations, and output audit logs.

(2) To check the operation when a setting is changed while the TOE is running.
(3) To confirm the behavior when the external authentication server is used.

b. Independent Testing Outline

The evaluator executed the sample testing of 56 items from the developer testing and the provided documentation with the following points of view. The evaluator devised the additional independent testing of 10 items from the developer testing and the provided documentation with the following points of view. Outline of the independent testing that the evaluator executed is as follows.

<Independent Testing Approach>

Just like the developer testing method, the evaluator confirmed direct operations and display of interfaces, confirmed host operations and TOE logs, and indirectly confirmed the behavior related to the TOE and the external authentication server.

<Content of Execution of the Independent Testing >

Independent testing was executed on 10 items by the evaluator.

Table 7.3-3 shows the points of view for the independent testing and the content of the testing corresponding to them.

Table 7.3-3 Executed independent testing

No	Outline of testing
IND-1	Access control for role-based operation function (1): when the role of a user is changed from the storage administrator to the security administrator, it is confirmed that it is impossible to access the operation menu of the storage administrator.
IND-2	Access control for role-based operation function (2): it is confirmed that the security administrator cannot access the operation menu of the storage administrator.
IND-3	Host authentication: when the security administrator changes the secret, it is confirmed that the host is authenticated with the changed secret.
IND-4	Login by the deleted user: when deleting one user (storage administrator) registered to the external authentication server, it is confirmed that the user cannot login from the Storage Navigator program.
IND-5	Access from the remote desktop: it is confirmed that the security administrator, storage administrator, and audit log administrator cannot connect from the remote desktop.
IND-6	Consecutive failures of maintenance personnel authentication: after authentication of maintenance personnel ID failed three times in a row in the remote desktop, it is confirmed that it cannot log in for one minute. The authentication method shall be the external authentication method.
IND-7	Password change by maintenance personnel : when the maintenance personnel changes his/her password, it is confirmed that the personnel can log in with the changed password, and also confirmed the check function of password quality (number of characters and character type).
IND-8	Restoring encryption key: when the backup encryption key is falsified, it is confirmed that it cannot be restored to the TOE.
IND-9	Stopping the shredding function: it is confirmed that the storage administrator is able to stop the shredding function, and the warning indicating that the data are not shredded is displayed.

No	Outline of testing
IND-10	WWN change: when WWN registered to the TOE is changed, it is confirmed that the host cannot access the storage system after the TOE updates the host information.

c. Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

The evaluator devised and executed the necessary evaluator penetration testing (hereinafter referred to as "penetration testing") about the possibility of exploitable concern at assumed environment of use and attack level. It explains the penetration testing executed by the evaluator as follows.

1) Summary of the Penetration Testing

Summary of the penetration testing executed by the evaluator is as follows.

a. Vulnerability of concern

The evaluator searched into the provided evidence and the public domain information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing. The following shows the five viewpoints of the identified vulnerabilities.

1. Behavior for inconsistent operation

   When an invalid parameter value or unacceptable value (user name, password, etc.) is entered, vulnerabilities, such as OS command injection or directory traversal, may occur: vulnerabilities of incorrect cable connection to fibre channel switch port and performing unauthorized operations.

2. Falsification of session

   Vulnerabilities of session hijacking and cross-site scripting due to the quality issue of the session ID (Cookie value) used to maintain sessions between the SVP PC and the management PC, unexpected session ID use, and corruption of session ID, etc.

3. Publicly-known vulnerability related to open ports

   Unnecessary ports open in the external LAN or the internal LAN of the SVP PC and the MP package, or publicly-known vulnerabilities exist in services related to open ports, leading to illegal access from the network.

4. Encryption algorithm in communication

   Vulnerabilities in communication due to SSL communication between the SVP PC and the management PC, and due to the LDAPS, starttls, or RADIUS (CHAP) protocol between the SVP PC and the external authentication server.

5. Other concerns

   Vulnerabilities related to LDEV deletion, expiration of the certificate, and exclusive control, which are not confirmed in the developer testing and the evaluator independent testing.

b. Penetration Testing Outline

The evaluator executed the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>

Figure 7-3 shows the penetration testing environment. In this environment, the test PC and test tools are added to “Figure 7-2 Independent testing configuration”.

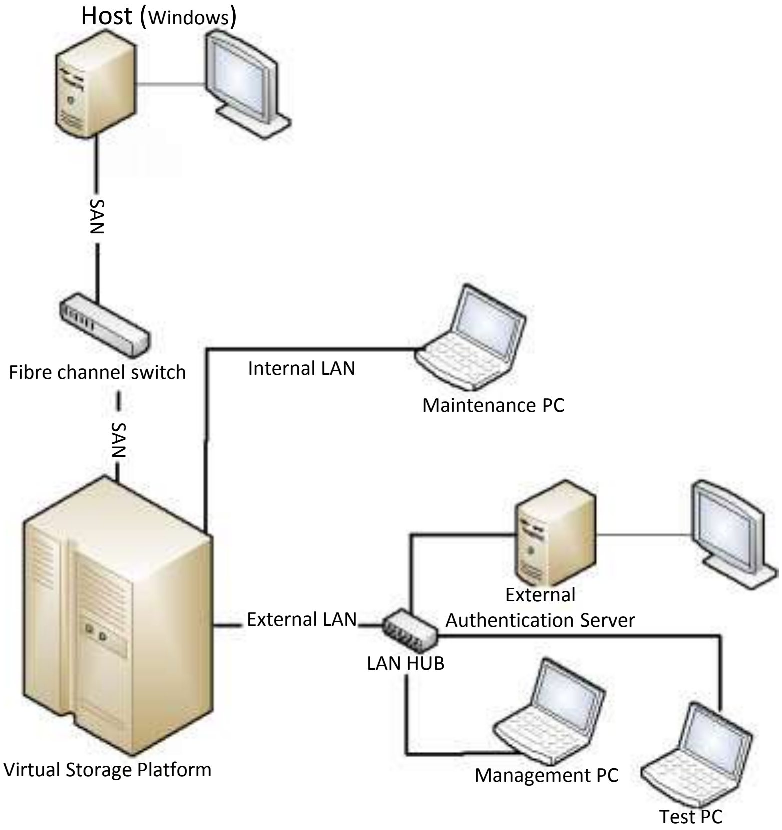

Figure 7-3 Penetration testing environment

Table 7.3-4 shows the details of the test tools on the test PC added to the independent testing environment.

Table 7.3-4 Tools used for the penetration testing

Tool name	Outline/Purpose of use
Nmap Ver 5.51	A tool that detects IP communication port that is opened by the device to be investigated. It investigates the ports open for the external LAN and the internal LAN of the TOE.

Tool name	Outline/Purpose of use
Nessus Ver 4.4.1 (build 15078)	A tool that checks publicly-known vulnerabilities, such as OS and application, based on the communication service and protocols to be used. The plug-in uses the data of April 19, 2011. It investigates the vulnerabilities of communication service open for the external LAN of the TOE.
Nikto Ver 2.1.4	A vulnerability diagnosis tool dedicated for web server. It investigates publicly-known vulnerabilities, such as HTTP protocol and CGI. The plug-in uses the data of April 19, 2011. It investigates the web server of the TOE.
Fiddler	A tool that captures and displays HTTP packet and sends its contents by altering them. It investigates the vulnerabilities by sending an invalid value to the web server of the TOE.
Wireshark Ver 1.4.4	An analysis program of network packets. It collects packets on Ethernetwork and analyses the protocols.

< Penetration Testing Approach >

In the penetration testing related to the TOE interfaces, the value for the penetration testing is entered from the Storage Navigator program to confirm the screen transitions of the TOE, displayed messages, and logs.

For SSL communication between the SVP PC and the management PC as well as communication using the LDAPS, starttls, or RADIUS (CHAP) protocol between the SVP PC and the external authentication server, it is confirmed that the protocol is used by getting the TCP/IP packet of the communication, the communication procedure with vulnerability is not used, and confidential data cannot be accessed as it is an encrypted communication.

<List of Executed Penetration Testing>

Table 7.3-5 shows concerned vulnerabilities and the content of the related penetration testing.

Table 7.3-5 Outline of penetration testing

No	Test name	Outline of testing	Vulnerability of concern
VAN-1-1	Invalid parameter	For the parameter that has a restriction on the input value, an invalid value is set to confirm the behavior.	1
VAN-1-3	Replacing fibre channel switch port cable	The cable connected to the fibre channel switch port is replaced to confirm the behavior.	1
VAN-1-4	Deleting LDEV	It is confirmed that the LDEV deleted by the storage administrator cannot be reused. (*)	5
VAN-2	Checking randomness of session ID	The randomness of session ID used for session management is confirmed.	2
VAN-3-1	Port scan (SVP PC)	Nmap is used to check unnecessary ports open in the SVP PC.	3
VAN-3-2	General-purpose vulnerability scan (SVP PC)	The general-purpose vulnerability scan tool, Nessus, is used to check the publicly-known vulnerability in the SVP PC.	3
VAN-3-3	Web vulnerability scan (SVP PC)	The vulnerability diagnosis tool for the web server, Nikto, is used to check the vulnerability of the web server in the SVP PC.	1

No	Test name	Outline of testing	Vulnerability of concern
VAN-3-4	Port scan (MP package)	Nmap is used to check unnecessary ports open in the MP package.	3
VAN-4	Confirming external authentication	It is confirmed that encrypted communication is used between the SVP PC and the external authentication server. (*)	4
VAN-5-1	Cross-site scripting	It is confirmed that malicious script cannot be included in the user name input interface in the user creation window.	2
VAN-5-2	OS command injection	It is confirmed that malicious OS command cannot be included in the user name input interface in the user creation window.	1
VAN-6	Certificate of expiration	The behavior is confirmed when logging into the web server of the SVP PC whose certificate expired from the Storage Navigator program.	5
VAN-7	Changing cookie	The cookie (session ID) used for session management is changed to confirm the behavior.	2
VAN-8	Exclusive control	It is confirmed that multiple storage administrators cannot edit LDEVs in the same resource group at the same time. (*)	5
VAN-9	Invalid CFL-CLI file	For the function of reading/writing the configuration information file, the behavior is confirmed in the case invalid configuration information file is input.	1

*It is performed in the developer testing or the evaluator independent testing, but since it has a vulnerability of concern, the penetration testing was additionally performed.

c. Result

In the penetration testing conducted by the evaluator, the evaluator could not find any exploitable vulnerability that attackers who have the assumed attack potential could exploit.

7.4 Evaluated Configuration

This evaluation was performed in the configuration described in “7.3.2 Evaluator Independent Testing” and Figure 7-2. The evaluator evaluated the combinations of five types of hosts (Windows, HP-UX, Solaris, Linux, AIX) and the fibre channel connection adapter drivers as well as three types of communication methods (LDAPS, starttls, RADIUS) between the SVP PC and the external authentication server. For the connection between the TOE and other storage system, the function that internally reproduces the above condition in the TOE was used.

The TOE is not used in such a configuration that is significantly different from the above components. Therefore, the evaluator determined that the above evaluation configuration was appropriate.

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2

The result of the evaluation is applied to the composed by the corresponding TOE to the identification described in Chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

The certification body conducted the following certification based on each materials submitted by Evaluation Facility during the 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 oversight reviews and were sent to Evaluation Facility. The Certification Body confirmed such concerns pointed out in Observation Report and certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this certification report.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL2 in the CC part 3.

8.2 Recommendations

- The TOE has a function to identify/authenticate the host and prohibit the host from accessing LDEVs that are not assigned to the host. However, if an attacker takes over the host and accesses the LDEV that is assigned to the host to leak or falsify user data in the LDEV, the TOE cannot counter it. The host administrator needs to take responsibility to implement security measures for the host.

- When backing up user data to the storage system installed with the TOE from other storage system installed with the TOE, the storage system installed with TOE cannot trust the storage administrator of the other storage system installed with the TOE. Therefore, when the storage administrator of the other storage system installed with the TOE executes a command to read/write user data from the storage system installed with the TOE, it could fall into the leakage or falsification of user data.

- It is possible to use by connecting the storage system installed with the TOE to another storage system of a different model, but in such a case, the operations of the security functions of the TOE are not assured. The security administrator and storage administrator need to take responsibility for the operations.

- The security administrator needs to protect the backup file of the encryption key, the TOE setting information file, and the TOE user information that are backed up from the TOE to the management PC or other recording media from being lost, leaked, and falsified.

- According to the assumptions, it is described that the storage system installed with the TOE is directly connected with other storage systems in a physically protected secure area where entrance and exit are controlled. However, other storage systems used for backup and synchronization are generally installed in remote sites. In case of connecting the TOE with other storage systems in a remote site, the security administrator and the storage administrator need to take responsibility for securing physical security in operation between the TOE and the other storage systems in a remote site.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided within a separate document of this certification report.

Hitachi Virtual Storage Platform Security Target, Version 1.17 (August 19, 2011) Hitachi Ltd.

11. Glossary

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

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

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

CFL	Configuration File Loader
CHA	Channel Adapter
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
DKC	Disk Controller
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel Security Protocol
FTP	File Transfer Protocol
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over TLS
LDEV	Logical Device
LSI	Large Scale Integration
LU	Logical Unit
PC	Personal Computer
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks

SAN	Storage Area Network
SSL	Secure Sockets Layer
SVP	Service Processor
TLS	Transport Layer Security
VSP	Virtual Storage Platform
WWN	World Wide Name

The definitions of terms used in this report are listed below.

Audit log administrator
Person who manages reference and download of audit logs and makes syslog related settings by using the Storage Navigator program

CHAP authentication
Method to perform authentication by sending the encrypted password from the client to the server, based on the random character string sent from the server to the client

CHAP secret
Shared password used for mutual CHAP authentication

Cookie
Mechanism that the web server temporarily writes and stores data in the web browser. It is used for user identification and authentication and session management.

Cross-site scripting
A web application problem that dynamically creates a web page: a vulnerability that allows injection of malicious script.

Directory traversal
Attack that enables to access unintended files for which access is not permitted, because access permission is not set properly, or the security of the entered directory or the file name is not verified sufficiently.

Disk subsystem
Storage system, Hitachi Virtual Storage Platform (also known as "Hitachi Virtual Storage Platform VP9500")

DKCMAIN micro-program
Control program of the storage system that is installed in the MP package in the storage system; it controls host connections, data transfer between the host and the storage system, and data input/output to the storage device; manages encryption keys and security function data; and provides the shredding function.

FC-SP
Protocol for secure communication using a fibre channel to authenticate each device when communicating between computers and the peripheral devices, such as storage system, and the fibre channel switch. The DH-CHAP with NULL DH Group authentication is used.

Fibre channel
Data transfer method between computers and the peripheral devices, such as storage system. It is used when connecting the server that requires high performance with the hard disk device.

Fibre channel connection adapter
Network interface device for fibre channel that is installed in the computer

Fibre channel switch	Network device to mutually connect various devices that have the fibre channel interface. Using this fibre channel switch enables to build SAN (Storage Area Network) by connecting multiple hosts and storage systems in high-speed.
Host administrator	Administrator who manages hardware and software configuration of the host.
LDEV	Abbreviation of “Logical Device”. It is a unit of volume to be created in the user area in the storage system.
Logical unit (LU)	Logical unit. The minimum unit of storage area accessed by the host. It consists of one or multiple LDEVs (logical devices).
LU path information	Path information between the host and LU
Maintenance personnel	Person who belongs to the maintenance organization with which the customer who uses the storage system has a maintenance contract. The maintenance personnel is in charge of initial start-up processing performed when installing the storage system, maintenance operations, such as replacement and addition of parts, changing settings due to maintenance operations, and recovery processing in case of error.
Maintenance PC	Terminal that is used by maintenance personnel to connect to the SVP PC at maintenance
Management PC	Terminal that is used by Storage Navigator users to operate the Storage Navigator program
OS command injection	Sending a command to the server from outside to manipulate the server OS and execute it improperly
Resource group	Resource group information
Response verification	In the CHAP authentication, the server compares and verifies the encrypted password sent from the client with the encrypted password created by the server itself.
Secret	Shared password that is used for mutual authentication using DH-CHAP with FC-SP
Security administrator	Person who makes TOE settings by using the Storage Navigator program, such as managing accounts, resource groups, and user groups as well as authentication settings of hosts and fibre channel switches for the TOE.
Session hijacking	Attack technique that a third party takes over the communication session between the server and the client (a group of communications performed among specific users): e.g. web session hijacking in HTTP.
Shredding function	Function to overwrite storage devices, such as hard disks and SSD (Solid State Drive), with dummy data to erase the remaining data
starttls	The extended version of the SMTP protocol. Communication is encrypted using SSL/TLS.
Storage administrator	Person who manages resources of the assigned storage system by using the Storage Navigator program
Storage Area Network (SAN)	The network system that connects servers etc., with hard disk devices etc. It establishes communications using fibre channels and Ethernet.

Storage Navigator program

Program that provides GUI to make settings for the storage system. It consists of the Flex application and the Java applet, and runs in the SVP PC and the management PC. It is used by Storage Navigator users and maintenance personnel.

Storage Navigator users

Users of the Storage Navigator program, including security administrators, storage administrators, and audit log administrators.

Storage user

An entity which uses user data stored in the storage system. The entity is the host or manipulates the user data via the host

SVP PC

PC in the storage system to install the SVP program

SVP program

Management software that is installed in the SVP PC in the storage system. It connects the Storage Navigator program with the remote desktop, performs identification/authentication of TOE users, displays the TOE setting interface, and communicates with the DKCMAIN micro-program to perform operations and maintenance of the storage system and manage the configuration information.

Syslog transfer

Function of which the syslog program that records logs, such as the system operating condition and messages, sends and receives the logs with other computers

User group

User group information

Wrap-around method

When the log file size is limited, and the file becomes full, it is returned to the top of the file to overwrite the logs.

12. Bibliography

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

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

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

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)

[12] Hitachi Virtual Storage Platform Security Target, Version 1.17 (August 19, 2011) Hitachi Ltd.

[13] Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 Control Program Evaluation Technical Report, Version 3, August 31, 2011, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security