HITACHI
Inspire the Next

Hitachi Virtual Storage Platform
Security Target

Issue date:	August 19, 2011
Revision:	1.17
Prepared by:	Hitachi Ltd.

This document is a translation of the evaluated and certified security target written in Japanese.

- Table of Contents -

List of tables

List of figures

1 ST overview

This chapter describes Security Target (hereinafter referred to as “ST”) reference, TOE reference, TOE overview and TOE description.

1.1 ST reference

This section describes ST identification information.

Title	: Hitachi Virtual Storage Platform Security Target
Version	: 1.17
Issue date	: August 19, 2011
Created by	: Hitachi Ltd.

1.2 TOE reference

This section describes TOE identification information.

TOE	: Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform for VP9500 Control program
TOE version	: 70-02-05-00/00(R7-02-06A) It consists of the following programs - DKCMAIN micro-program 70-02-05-00/00 - SVP micro-program 70-02-03/00 (Including Storage Navigator program)
Keyword	: Storage, SAN, RAID, Virtualization, Role-base access control
Developed by	: Hitachi Ltd.,

1.3 TOE overview

1.3.1 TOE type

TOE, namely the control program of version 70-03-05-00/00 (R7-02-06A) for Hitachi Virtual Storage Platform (It is also marketed under the name of Hitachi Virtual Storage Platform VP9500. Those are both called VSP hereinafter) is the software program operating on VSP, the storage products of Hitachi Ltd.

1.3.2 Relevant personnel

The ST intends for the following users as relevant personnel to storage systems.

- Security administrator:

  The security administrator can register, modify and delete administrator accounts using Storage Navigator program (see 1.4). Also, the administrator can create and delete resource groups, migrate resources between resource groups, and register resource groups to user groups. In addition to the above, authentication setting of host and fibre channel switch and encryption operation of stored data are enabled.

- Storage administrator:

  The storage administrator can manage resources assigned to the storage administrator (such as port, parity group, external volume group, host group and LDEV) by using Storage Navigator program.

- Audit log administrator:

  The audit log administrator can manage audit logs obtained in storage systems. The administrator can refer and download the audit logs and make setting related to syslog.

- Maintenance personnel

  The maintenance personnel belong to an entity specialized in maintenance with whom customers who use the storage system sign contracts concerning maintenance. They are responsible for initial startup process in installing the storage system, changing settings required in maintenance activities such as parts replacement or addition, and disaster recovery.

  Maintenance personnel access SVP PC from a PC for maintenance person (maintenance PC) (see 1.4.2) to perform maintenance operations. Only maintenance personnel can directly contact parts inside the storage system and operate devices connected to the internal LAN. All resources of the storage system are assigned to the maintenance personnel and they can perform operations allowed by maintenance role (see Table 1-2). The TOE recognizes person who uses an interface to access SVP PC from the maintenance PC as “the maintenance personnel” role.

- Storage user:

  It is a user of storage system (represents a host) who uses data stored in the storage system through the host connected to the storage system.

The security administrator, storage administrator and the audit log administrator are hereinafter

collectively called the Storage Navigator user.

1.3.3 How to use TOE and major security feature

VSP is a storage system for companies that require multi-platform, high performance, high response and large capacity. It provides expandable connectivity, virtualization of external storages, logical resource partitioning, remote copy function and expandable disk capacity in environment of different system.

Many hosts of variety types of platforms connect to a storage system via the SAN environment or the IP network environment. If an unauthorized operation is performed to this storage system, it may result in unintended accesses to user data in the storage system. In order prevent the situation, the access control is required for the user data in storage system.

Under the condition that multiple storage administrators manage resources in a disk subsystem (such as port, cache memory and disk) a configuration change beyond the administrator's responsibility might be made. The TOE therefore divides the port, disk (parity group) and cache memory into multiple resource groups, and the multiple resource groups are assigned to each administrator. The assignment of authority for resource management allows each administrator to access the resource without affecting other administrators' resources. The control program for VSP, the TOE, consists of DKCMAIN micro-program, SVP program and Storage Navigator program. The DKCMAIN micro-program controls resources in the storage system and the SVP program controls the authorities for administrators of storage system. The Storage Navigator program is contained in the SVP program and is downloaded from SVP PC to a management PC when it is used. Hereinafter the Storage Navigator program is called Storage Navigator.

This ST describes the security features to protect confidentiality and integrity of user data on VSP by providing functions to prevent unauthorized access to storage resources assigned to specific storage users from other storage users, and to encrypt and shred the user data in hard disks.

VSP equipped with the TOE is manufactured and shipped by Disk Array Systems Division Hitachi Ltd.,

The security features provided by the TOE is as follows.

[Security features TOE provides]

Access control of Storage Navigator users (See 1.3.2) and maintenance personnel:

Users who access the TOE belong to groups. One or more roles and one or more resource groups are assigned to a group. Entire storage resources are divided into several groups as resource groups. Each user has only access to the resource groups assigned to itself with the roles.

LUN Manager:

It controls host access to logical devices in storage system.

Authentication of host:

It authenticates hosts and fibre channel switches to prevent accesses from an unauthorized host to the storage system.

Identification and authentication of Storage Navigator user and maintenance personnel:

It controls users who access the TOE, and identifies and authenticates each user. It also can identify and authenticate users by using an externally connected authentication server.

Encrypted communication between Storage Navigator and SVP PC, and between SVP PC and external authentication server:

It encrypts the communication between Storage Navigator and SVP PC, and between SVP PC and external authentication server.

Encryption of stored data:

It encrypts user data to be stored in the storage system.

Shredding:

It shreds user data in the storage system.

Audit log:

It collects logs of configuration change and update of the storage system and enable administrators to see and manage the logs.

1.3.4 Environment for usage of TOE

1.3.4.1 Environment for usage of TOE

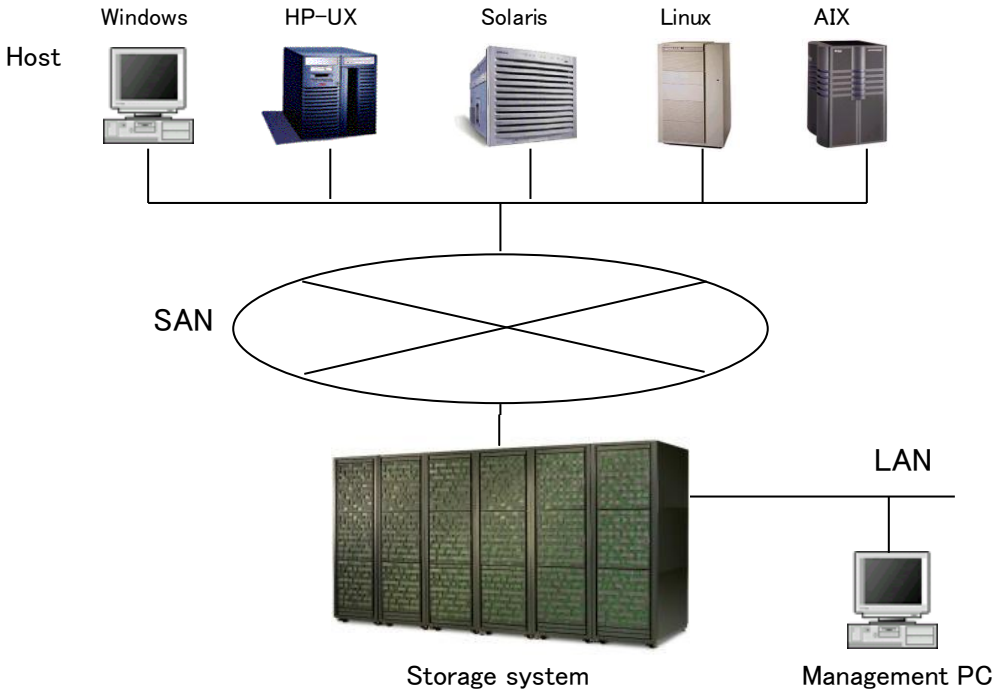


Figure 1-1 General system configuration including storage system

Figure 1-1 illustrates the general system configuration including storage system. Components of the system configuration are as follows.

(1) Storage system

Normally, the storage system with TOE is installed in a secure area where entering and leaving the area is controlled.

(2) SAN and host

Each Open server such as Windows, HP-UX and Solaris (collectively called “host” in this document) and storage systems are connected via SAN (Storage Area Network). SAN is the dedicated network for storage system to connect hosts and storage systems via the fibre channel.

To connect a host to SAN, fibre channel connection adapter (hardware and software) needs to be installed on the host. The storage system identifies the host using the identification information in the fibre channel connection adaptor. The identification information in the fibre channel connection adapter is set by the storage administrator when connecting the host to the storage system.

Since customers performs the host access control configuration, the ST does not have any countermeasure against sophisticated attack capability like unauthorized access to user data in the storage system by altering the identification information of the host. However, if customer policy requires, the TOE can authenticate the host (including fibre channel switch) connected with the storage system.

(3) Management PC

The management PC is the PC for setting up configuration information of storage system via network. The program for the administrator of storage system to set up the configuration information runs on the management PC. The management PC and storage system are connected via LAN (Local Area Network).

1.3.4.2 TOE and other configuration components

This section describes configuration components of hardware and software, and shows which one is included in the TOE and operating environment respectively. The hardware and software built in the storage system are installed at the factory shipment, and Storage Navigator users at customer site and storage users (see 1.3.2) are not required to prepare or change them.

1.3.4.2.1 Hardware components

The table below shows necessary hardware components and whether each component is included in the TOE. The environment means that items are the component of other than TOE.

TOE/environment	**Configuration component**	**Description**
Environment	Hitachi Virtual Storage Platform Hitachi Virtual Storage Platform VP9500	VSP hardware. It includes SVP PC. The difference between the models is branding of external rack. The TOE is installed on the hardware.
Environment	Host	Computers that access the disk subsystem. Windows, HP-UX, Solaris, Linux and AIX are expected as host OS.
Environment	Fibre channel connection adapter	An adapter equipped in computer to connect to SAN.
Environment	Fibre channel connection adapter	A switch to connect host with storage system, which constitutes the SAN.
Environment	Management PC	Computers to administer the TOE. Requirements for the computer are; ・ CPU: Pentium 4 640 3.2GHz and higher Recommended: Core 2 Duo E6540 2.33GHz and higher ・ RAM: 2GB or larger Recommended: 3GB ・ Available HDD capacity: 500 MB and larger ・ Monitor: True Color 32 bit and higher; Resolution: 1280x1024 and higher ・ LAN card: 100Base-T
Environment	SAN	High speed network connecting storage system and computers by using fibre channel.
Environment	Other storage system	Other storage system connected with the storage system equipped with TOE. The other storage is limited to the one equipped with TOE.
Environment	Maintenance PC	A computer used by maintenance personnel at maintenance, which is prepared by maintenance personnel.
Environment	External authentication server	A server that identifies and authenticates users, such as LDAP server and RADIUS server.
Environment	External LAN	LAN to connect storage system, management PC and external authentication server.
Environment	Internal LAN	LAN to connect package in the storage system and maintenance PC.

1.3.4.2.2 Software component

The table below shows necessary software components and whether each component is included in the TOE.

TOE/environment	Configuration component	Description
TOE	DKCMAIN micro-program Version 70-02-05-00/00	It operates on MP PCB. The TOE is embedded in the storage system at factory shipment.
TOE	SVP program Version 70-02-03/00	It runs on SVP PC and Storage Navigator runs on management PC. The TOE is embedded in the storage system at factory shipment.
Environment	SVP PC OS	SVP PC OS。 • Windows Vista Business US version (64bit version) SP2
Environment	Web server	It operates on SVP PC and uses the software below. • Apache Tomcat 6.0.16
Environment	Management PC OS	Os of management PC. • Windows XP (SP3 and later)
Environment	OS of maintenance PC	OS of maintenance PC. • Windows XP (SP3 and later)
Environment	Web browser	Web browser works on management PC. The following browser is supported. • Internet Explorer 8.0
Environment	Flash Player	It operates on management PC as a plug-in of web browser. The following version is used. • Flash Player 10.1
Environment	Java runtime environment	Java runtime environment operates on management PC. • JRE 6.0 Update 20(1.6.0_20)

1.4 TOE description

The TOE consists of DKCMAIN micro-program, SVP program, and Storage Navigator.

The DKCMAIN micro-program is installed on multiple MP PCBs in a storage system and has a role of controlling data transfer between the storage system and a host connected with the storage system. The SVP program is a program to execute operations and maintenances of the storage system. Storage Navigator provides a user interface function of SVP program.

Figure 1-2 illustrates hardware components constituting the storage system and shows that on which components the identified TOE sub set works.

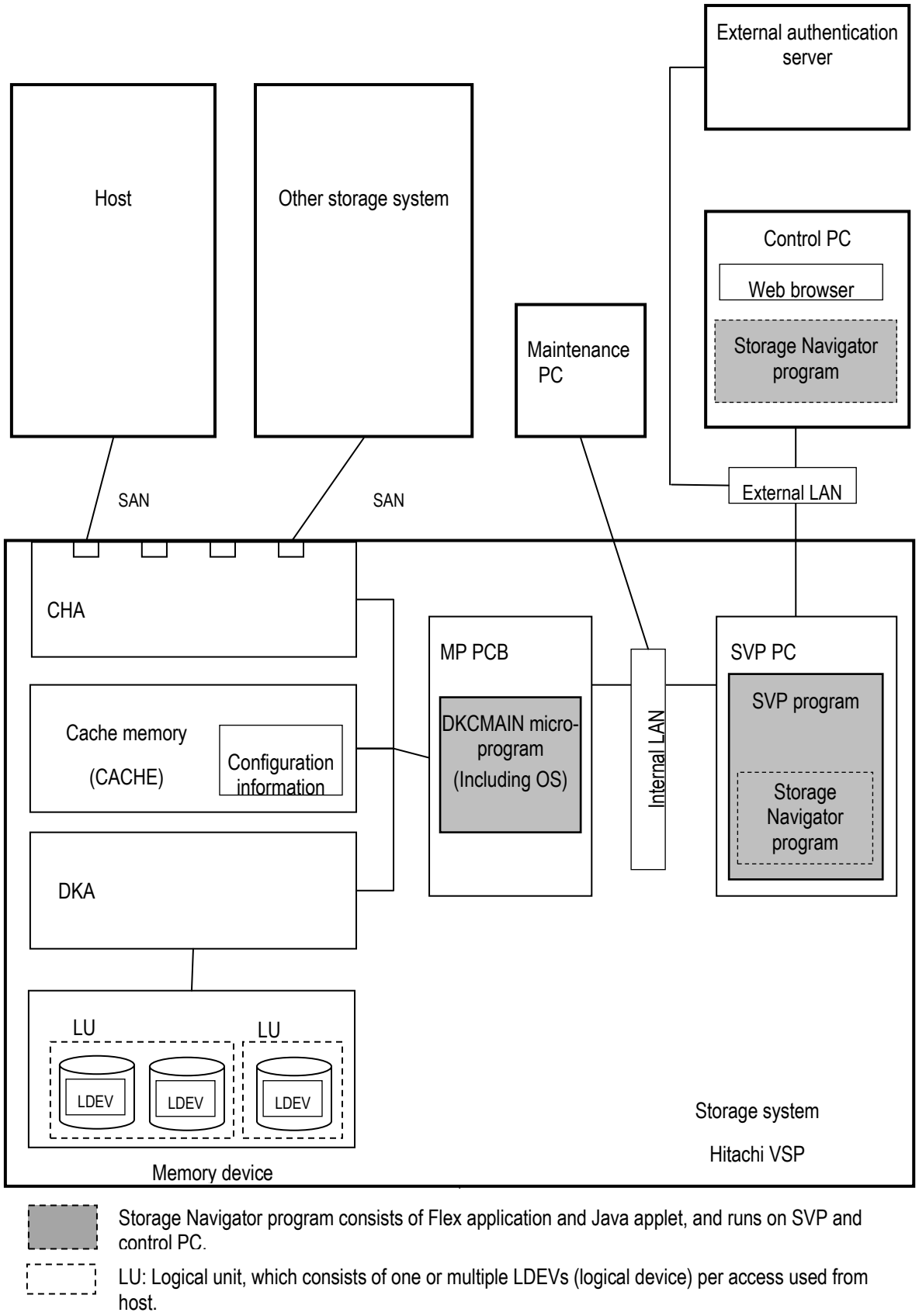


Figure 1-2 Storage system configuration

The storage system consists of control system and storage management system. The control system includes channel adapter (CHA), cache memory (CACHE), disk adapter (DKA), micro processor (MP), and memory device. The storage management system includes SVP (service processor) PC. The control system controls data input and output to and from memory device while the storage management system performs storage maintenance and management operations. The configuration components are as follows.

The control network (CHA, CACHE, DKA, and MP PCB together connected by high speed crossbar switch) and administration network (internal LAN and external LAN) are completely independent each other. This configuration does not allow direct access from SVP PC, management PC, and maintenance PC connected either to the internal LAN or external LAN, to the cache and memory device.

1.4.1 Control system

(1) Channel adapter

Channel adapter (CHA) processes a command from a host or other storage system to a local storage system and controls data transfer. The host and other storage system are connected to a fibre port on the CHA via the fibre channel.

(2) Disk adapter

Disk adapter (DKA) controls data transfer between the cache and memory device. The DKA is equipped with LSI to encrypt and decrypt the stored data as encryption function.

(3) Cache memory

Cache memory (CACHE) is located between CHA and DKA and is commonly accessible from DKCMAIN micro-program. The configuration information to access the data through CHA and DKA is stored in it to be used for data reading and writing. The configuration information on the memory can be accessed only through the DKCMAIN micro-program.

(4) MP PCB

One quad core CPU is equipped in one PCB for DKCMAIN micro-program to work.

(5) Memory device

Memory device consists of multiple hard disks and is used to store user data. In the memory device, an LDEV (logical device) which is a volume to store user data is created. Access to the user data is controlled per LDEV, and done via DKCMAIN micro-program. A part of or all data in the LDEV can be allocated to cache memory so as to enable high speed data access.
An LU (logical unit), which is an access unit from a host, is mapped to one or more LDEV.

LDEVs are created on a parity group in the memory device. The parity group is a series of hard disk drives handled as one data group, and composes RAID by storing the user data and parity information. This RAID configuration enables accesses to the user data even when one or more drive in the parity group is unavailable, which improves the reliability.

CHA, CACHE, DKA and MP PCB are connected with each other by the high-speed crossbar switch.

1.4.2 Storage management system

(1) SVP PC

The SVP is a service processor embedded in the storage system to manage the entire storage system, and SVP program, which is a part of TOE, runs on it. The SVP program is the software to manage configuration information and maintenance function of the entire storage system, and has a function to

send DKCMAIN micro-program a command to set configuration information received from Storage Navigator that works on management PC. It also has a function related to operations of security function in the storage system.

(2) Maintenance PC

The maintenance PC is the PC used by maintenance personnel at maintenance. It is connected to the SVP PC by remote desktop function via internal LAN which is the network in the storage system.

(3) Management PC

Management PC is a customer's PC used by Storage Navigator users (See 1.3.2) for storage system operations and maintenance. Storage Navigator, which is a part of TOE, works on it. The management PC and the SVP PC are connected via the external LAN.

(4) External authentication server

The external authentication server identifies and authenticates users by a request from the SVP program when Storage Navigator user (see 1.3.2) at customer site accesses, and returns to the SVP program the authentication result and user group information (see 1.4.4.2.1) that is a basis of approval information when the authentication succeeds. The communication between the SVP PC and the external authentication server is encryption communication.

(5) Storage Navigator

Storage Navigator is software used by Storage Navigator users (See 1.3.2) at customer site to manage configuration information of storage system.

Storage Navigator consists of Flex application and Java applet. The Flex application executes operations specified from Web browser on the management PC on the SVP PC, and displays the result on the Web browser of the management PC Java applet on the other hand downloads programs from the SVP PC to the management PC. The programs run on the management PC. The communication between the SVP PC and Storage Navigator uses SSL. Storage Navigator users handles setting operations of the storage system by interacting with Storage Navigator through the Web browser of the management PC.

In order to prevent unauthorized use of Storage Navigator by any malicious third party (See), Storage Navigator identifies and authenticates users in collaboration with the SVP program.

1.4.3 Other storages

In addition to hosts, external storage systems can be connected to a port of channel adapter mounted on the storage system. Sending and receiving commands to and from another storage system via the channel adapter enables data copy and backup between storages. When data copy is executed on the data sending side, backup is executed on the data receiving side. Copy operations executed from another storage system is executed by a reliable storage administrator. In addition, as the storage system and another one shares their own data each other, storage administrators need to be reliable. Therefore, other storage system connected with the storage system is limited to the one with the TOE installed.

1.4.4 TOE functions

Basic function and security function the TOE provides are as follows.

1.4.4.1 Basic functions TOE provides

Table 1-1 shows a part of the basic functions provided by the TOE.

Table 1-1 Basic functions provided by TOE

Function	Description
Hitachi Virtual LVI/LUN (Customized volume size function)	The customized volume size function can regard multiple LDEVs as free space and create multiple customized volumes in arbitrary size, which enables effective use of disk capacity.
Hitachi Cache Residency Manager (cache memory management function)	Specific data in a logical volume is resident in cache memory. The resident data can always be accessed by memory access function.
Hitachi Performance Monitor (Performance information management function)	Monitoring Resource usage rate in disk subsystem, disk load and port load measurement are enabled.
Hitachi Universal Volume Manager (External storage management function)	The function realizes virtualization of storage. By using Universal Volume Manager, multiple disk subsystems including VSP can be handled as one disk subsystem. It also allows the system administrator to easily manage multiple storage systems in different types.
Hitachi Disaster Recovery (Remote copy function)	In VSP series, replica volumes can be created at remote site without passing through a server. The replica can be used for backup as a measure for not only local/regional but also large-scale disasters. Without passing through a host, by updating the replica volume in synchronization with update at the main site, remote copy between disk subsystems is realized. For the connection between disk subsystems, fibre channel is used.
Hitachi Universal Replicator **(Asynchronous remote copy function)**	Universal Replicator is an asynchronous remote copy function with a new technology. Adapting the technology to accumulate update records (journal) in a disk drive with capacity larger than cache can realize stable copy which is less affected by fluctuations of bandwidth and operation traffic.
Hitachi ShadowImage (Local copy function)	Volume replication to create a replica of logical volume in a disk subsystem without passing through a host is enabled. Using the replica allows obtaining backup in the same database and concurrent processing such as batch processing while continuing online operation for the data base and minimizing the impact on operating performance.
Hitachi Dynamic Provisioning **(Virtual volume management function)**	With Dynamic Provisioning, the data of volume in a pool is accessed via a virtual volume. For the virtual volume and pool volume, thresholds are set to continuously monitor overflow of the area, which eventually brings the following effects. - Reduction of introduction cost by improving volume usage ratio - Prevention of increases in management cost and time period of no operation due to the stop of operation while establishing the system.

1.4.4.2 Security functions TOE provides

1.4.4.2.1 Access control function of Storage Navigator user and maintenance personnel

In an intensive environment with large-scale storage where data of multiple companies, departments, systems and applications exist in a disk subsystem, so-called Multi-tenancy function to manage storage operations individually by assigning storage administrators per company or department is required. The Multi-tenancy function promises cost reduction by effective use of resource and management simplification by dividing.

In Multi-tenancy environment, a security mechanism not to destroy the data of other organization by mistake, not to leak the data to other organization, and not to affect operations by other storage administrator is necessary.

Access control function of Storage Navigator user and maintenance personnel is per user group. A role and a resource group, a group of resources which can be controlled by the role, are assigned to the user group. Figure 1-3 shows the relationship between user (administrator), user group, resource group and role.

This function enables each user to perform flexible resource allocation and realizes the above security.

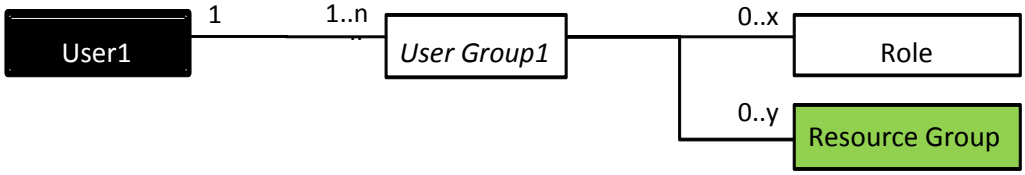


Figure 1-3 Relationship between user, user group, role and resource group

A user belongs to one or more user group. The user group is assigned roles and resource groups and uses them as approved information. The user group information is obtained from SVP PC or external authentication server to be used. Each account can execute management operation allowed by the assigned role for the assigned resource.

(1) Role

The security administrator creates a user account using Storage Navigator and registers it to a user group.

Permission of which operation is assigned to a user is determined based on the role assigned to the user group. The role has categories as follows.

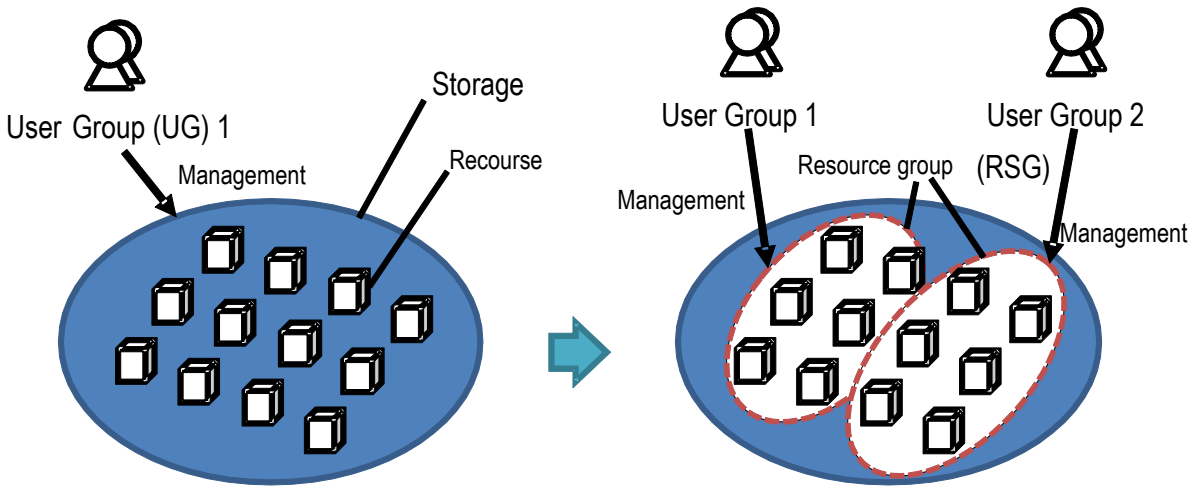
Table 1-2 Role category and operation

Role	Allowed operation
Security administrator role	A role, which is assigned to security administrator and can execute the following operations. ➢ User management ➢ Resource management such as resource group creation and edition. ➢ Authentication setting of host and fibre channel ➢ Encryption of stored data
Audit log administrator role	A role, which is assigned to audit log administrator and can execute the following operation. ➢ Operations related to audit logs
Storage administrator role	A role, which is assigned to storage administrator and can execute the following operations. ➢ Initial setting such as IP address setting ➢ Configuration change such as logical device creation ➢ Device performance information management

Role	Allowed operation
	➢ Local/remote backup of user data ➢ Shredding of user data
Maintenance role	A role, which is assigned to maintenance personnel and can execute the following operations. ➢ Remote desktop connection to SVP PC ➢ Connection setting of authentication server (including connection setting parameter) ➢ Storage system installation ➢ PCB replacement, installation and removal ➢ Volume creation and deletion ➢ Micro-program update ➢ Periodical check ➢ Recovery at failure occurrence

(2) Resource group

Dividing storage resource into multiple groups is called resource group (RSG). Each resource group is assigned a number (RSG number) for identification. Also, each resource group is assigned to a user group and each storage administrator can perform management operation within the range of resource group assigned to the user group the administrator belongs to. As all resource groups are assigned to maintenance personnel, they can perform maintenance for all storage resources.



1.4.4.2.2 LUN Manager

LDEV that stores user data is created by using Storage Navigator. In order to access the LDEV from a host, the LDEV needs to be associated with a port on CHA connected to the host. In particular, LU number is assigned to associate the host and the LDEV to be accessed to set LU path. Data reading and writing for the corresponding LDEV is enabled only from the host with the LU path setting. In other words, data reading and writing from hosts without LU path setting are not allowed.

1.4.4.2.3 Authentication of host

When connecting a host to SAN, the connection management is done in a customer operation to prevent unauthorized host connection. If the prevention of impersonation is required to further ensure safety as a customer policy, authentication by FC-SP function is available for the communication between the host or fibre channel switch and the port of disk subsystem. The port of disk subsystem can authenticate the host and fire channel switch, and the host and fibre channel switch can authenticate the disk subsystem port as well. For the host authentication setting, a security administrator uses LAN manager and sets each host whether to execute host authentication. Also, the security administrator registers host authentication data (WWN, secret) to authenticate. The secret is a password for authentication consists of combination of alphanumeric characters and symbols in 12 to 32 letters.

1.4.4.2.4 Identification and authentication of Storage Navigator user and maintenance personnel

Storage Navigator is used by customers to manage disk subsystem including security setting. The TOE executes user identification and authentication at disk subsystem management (configuration of each function and setting change) using Storage Navigator and remote desktop connection to SVP PC by maintenance personnel. If the identification and authentication fails three times in a row, the identification and authentication of the user is rejected for one minute.

As user authentication, the following 2 methods are supported.

(1) SVP PC internal authentication

ID and password of users are registered in the SVP PC, and the TOE authenticate. The password used for user authentication is 6 to 256 letters with a combination of alphanumeric characters and symbols. (The password of maintenance personnel is 127 letters)

(2) External authentication server

The SVP PC does not manage ID and password but the ID and the password are sent to an external authentication server and the authentication result is sent back. After the success of authentication by the external authentication server, the user group information is obtained from the server and used as approved information. As protocols for user authentication, LDAP (Encryption supports LDAPS, starttls) and RADIUS (authentication protocol is CHAP) are supported.

1.4.4.2.5 Encrypted communication between Storage Navigator and SVP PC, and between SVP PC and external authentication server

To prevent the falsification and leakage of communication data between storage system and the management PC, the communication between Storage Navigator and SVP PC is encrypted by SSL. In addition, LDAPS, starttls or RADIUS (authentication protocol is CHAP) protocols is employed for the communication between the SVP PC and the external authentication server to protect passwords of Storage Navigator user and maintenance personnel.

1.4.4.2.6 Encryption of stored data

The TOE can encrypt the data stored in a volume in the storage system. For encryption and decryption, LSI mounted in DKA is used. Encrypting data can prevent the information from being leaked at replacement of hard disk in the storage system or when the data is stolen. In addition, the following key management functions are available.

- Encryption key creation
- Encryption key deletion

- Encryption key backup and restoring

Only security administrator with user account can operate the encryption of stored data function.

1.4.4.2.7 Shredding

This is a function to disable to restore data by writing dummy data over all the data in a volume, so as to avoid data leakage and unauthorized use at reuse of the volume.

When the Shredding is executed, dummy data is written in the volume containing user data and the user data cannot be restored. The function complies with DoD5220.22-M, recommends writing dummy data at least 3 times. The dummy data is overwritten 3 times in the volume as default setting.

Only storage administrator with user account can operate the Shredding function.

1.4.4.2.8 Audit log

The audit log function is provided by SVP program (including Storage Navigator) and DKCMAIN micro-program. Storage Navigator records events related to the security such as success/fail of login and configuration/setting change.

The maximum number of letters in a line of audit log is 512 (single byte), and up to 250,000 lines information is stored in the SVP HDD. Storage Navigator provides the interface to refer audit logs.

1.4.5 Guidance documentation

Guidance documents for the TOE are as follows.

(1) Users guide for security function

- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 ISO15408 Function of Acquiring Authentication; Instruction manual Ver. 1.6
- Hitachi Virtual Storage Platform Storage Navigator User Guide Ver.5
- Hitachi Virtual Storage Platform Storage Navigator Messages Ver.5
- Hitachi Virtual Storage Platform for Open Systems Ver.4
- Hitachi Virtual Storage Platform Encryption License Key User Guide Ver.3
- Hitachi Virtual Storage Platform Volume Shredder User Guide Ver.3
- Hitachi Virtual Storage Platform Audit Log Reference Guide Ver.3
- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 User Guidance Ver.1.2
- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Manual for Obtaining ISO15408 Certification Ver. 1.6
- Hitachi Virtual Storage Platform Hitachi Storage Navigator User Guide MK-90RD7027-02f
- Hitachi Virtual Storage Platform Hitachi Storage Navigator Messages MK-90RD7028-03a
- Hitachi Virtual Storage Platform Provisioning Guide for Open Systems MK-90RD7022-02e
- Hitachi Virtual Storage Platform Hitachi Encryption License Key User Guide MK-90RD7015-02a

- Hitachi Virtual Storage Platform Hitachi Volume Shredder User Guide MK-90RD7035-02b
- Hitachi Virtual Storage Platform Hitachi Audit Log User Guide MK-90RD7007-02d
- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 User's Guidance Ver.1.2

(2) Disk subsystem maintenance manual

- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 ISO15408 Function of Acquiring Authentication; Maintenance manual Ver. 1.4
- A/H-65AC A-65BC HT-40BC Disk Array System Maintenance ManualREV.3
- TEST PROCEDURE MANUAL for RAID700 CTO Unit
- Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Obtaining ISO15408 Certification Maintenance Manual Ver. 1.4
- DKC710I Maintenance Manual REV.3

  * A/H-65AC, A-65BC, HT-40BC, RAID700 and DKC710I are other names of storage system VSP and VSP VP9500.

  * TEST PROCEDURE MANUAL for RAID700 CTO Unit is a guidance used at factory shipment.

2 Conformance claim

2.1 CC conformance claim

This ST complies with the following standards.

Common Criteria for Information Technology Security Evaluation

Part1: Introduction and general model Version 3.1 Revision 3 Japanese translation version 1.0

Part2: Security functional components Version 3.1 Revision 3 Japanese translation version 1.0

Part3: Security assurance components Version 3.1 Revision 3 Japanese translation version 1.0

Security functional requirements: Part2 Japanese translation version 1.0

Security assurance requirements: Part3 Japanese translation version 1.0

2.2 PP conformance

This ST does not claim compliance with any PP.

2.3 Package name conformant

This ST complies with package: EAL2. There is no additional assurance component.

3 Security Problem Definition

3.1 TOE assets

The most important asset for storage system is the user data of storage user stored in disk drives. In order to maintain integrity and confidentiality of the user data, the user data is protected from unauthorized access by a third party such as host administrator, and from setting change outside authority by Storage Navigator users. In addition, for sniffing of communication data between Storage Navigator and SVP PC and between SVP PC and external authentication server by a third party who can connect to external LAN, TSF data (user ID and password) contained in the communication data must be protected by utilizing high reliable channel.

In the ST, the user data of storage user exists in a resource group is the asset subject to protection in the environment of large-scale storage with data of multiple companies, departments, systems and applications in disk subsystem, and the asset is protected from accesses by unauthorized storage users.

3.2 Threats

The TOE counters threats shown below. A third party in the following description means a person who is none of Storage Navigator user, storage user, and maintenance personnel, and is not authorized to use the storage system.

The degree of attack is assumed to be low.

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 a host that is not allowed to access the LDEV.
T.TSF_COMP	If a third party who can connect to external LAN makes an unauthorized connection on the channel between Storage Navigator and SVP PC, or between SVP PC and external authentication server and obtains the communication data including ID and password of Storage Navigator user, he/she impersonates the Storage Navigator user and changes the storage system setting, eventually may access the LDEV where the user data is stored.
T.LP_LEAK	If a third party entity such as a host administrator access an 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 external LAN change the storage system setting by using Storage Navigator, he/she can access the LDEV where the user data is stored, 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 for the purpose of such as preventive maintenance, 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.

3.3 Organizational security policies

P.MASQ If a customer requests authentication of host, the host is authenticated when connecting the host to the storage system.

3.4 Assumptions

A.NOEVIL Within Storage Navigator users, the security administrator and audit log administrator are assumed to be the qualified person who is capable of operating and managing the entire storage system, executes 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 to the range permitted by the security administrator and 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 host and port on CHA, executes proper maintenance operations as specified by manuals, and never commit any wrongdoing.

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 at a secure area where only persons permitted 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 user is assumed to install and manage the management PC appropriately in accordance with a security policy of organization to protect it from unauthorized use. The security policy of organization to apply to the management PC contains the following.

- Install it in a place where direct administration is enabled, such as standard office area.
- Use it at an area where the direct access from external network to the management (administrator client PC) is disabled.
- Manage user identity authentication and administrator authority to prevent unauthorized access.
- Address malicious codes by restricting software installation, installing antivirus software and applying security patch, and so on.

A.CONNECT_STORAGE Other storage systems connected to TOE are assumed to be limited to those TOE is embedded.

A.EXTERNAL_SERVER	An external authentication server is assumed to be capable of using authentication protocol (LDAPS, starttls and RADIUS (authentication protocol is CHAP)) which can protect communication with SVP PC supported by the TOE, and registering and managing user identification information and user group information while keeping consistency with the TOE.

4 Security objectives

This chapter describes TOE security objective, operational environment security objective, and security objective rationale.

4.1 TOE security objectives

The TOE security objectives are as follows.

O.ADM_AUTH — The TOE must succeed the identity authentication of Storage Navigator user and maintenance personnel before the Storage Navigator user and maintenance personnel execute the management operations of disk subsystem.

O.ADM_ROLE — The TOE must control the management operations done by Storage Navigator user and maintenance personnel as follows.

- Security administrator can perform user management operation, resource management operation, host and fibre channel switch authentication setting, and encryption of stored data.
- Audit log administrator can perform operations related to audit log.
- Storage administrator can perform storage management operation within the permitted resource group.
- Maintenance personnel can perform external authentication server performance management and storage system maintenance operations.

O.SEC_COMM — The TOE must provide the communication function which is secured by the encrypted data on the channel between Storage Navigator and SVP PC, and between SVP PC and external authentication server to protect from sniffing of the data on the communication route.

O.HOST_AUTH — The TOE must identity authentication of the host by FC-SP function if the host requests connection.

O.HOST_ACCESS — The TOE must identify hosts to control that only the host which is allowed to connect to the storage system can access the permitted LDEV.

O.HDD_ENC — The TOE must manage encryption key to encrypt the stored data to prevent the user data from being leaked from the hard disk taken out of the storage system.

O.HDD_SHRED — The TOE must shred the user data to make sure that the user data does not remain in the hard disk when the hard disk in the storage system is replaced or stops to be used.

O.AUD_GEN — The TOE must track events regarding the security such as identity authentication and setting change operation.

4.2 Operational environment security objectives

The operational environment security objectives are as follows.

OE.NOEVIL	The representative of organization must assign person who is capable of managing and operating the entire storage system, executes proper operations as specified by manuals, and never commits any wrongdoing to security administrator and audit log administrator within Storage Navigator user. The storage administrator must be assigned to the qualified person who has been trained to execute proper operations as specified by manuals and never commits any wrongdoing to manage and operate disk subsystem to the range permitted by the security administrator.
OE.NOEVIL-MNT	Maintenance personnel must be assigned to the qualified person who is capable of doing maintenance safely for the entire storage system including connection of host and port on CHA, executes proper maintenance operations as specified by manuals and never commit any wrongdoing.
OE.PHYSICAL_SEC	A storage system, host (including fibre channel connection adapter), fibre channel switch, other storage system and external authentication server must be set at a secure area where only the security administrator, storage administrator, audit log administrator and maintenance personnel are allowed to enter and exit, and the above devices must be completely protected from any unauthorized physical access.
OE.MANAGE_SECRET	The security administrator must control the secret for host authentication set in the host to protect it from the use by unauthorized person.
OE.MANAGEMENT_PC	Storage Navigator user must properly install and manage the management PC in accordance with a security policy of organization to protect it from unauthorized use.
OE.CONNECT_STORAGE	Other storage systems connected to the TOE must be limited to those with TOE embedded
OE.EXTERNAL_SERVER	The security administrator must use protocol (LDAPS, starttls and RADIUS (authentication protocol is CHAP)) which can protect the communication with SVP PC supported by the TOE for external authentication server, and properly register and control the user identification information and user group information while keeping the consistency with TOE.
OE.FC-SP_HBA	When authentication of host is required, a fibre channel connection adapter with FC-SP function must be used. If a fibre channel switch is used in the configuration, the fibre channel switch needs to support FC-SP.

OE.HDD_ENC	In operational environment, a storage system which is capable of encrypting user data by using LSI equipped in DKA must be provided to prevent the user data from being leaked from hard disk.

4.3 Security objective rationale

The security objective must be to address to assumptions stipulated in Security problem definition, to counter threats or to realize organizational security policy. Table 4-1 shows relationships between security objective and corresponding assumption, threats to counter, and organizational security policy.

Table 4-1 Relationship between TOE security problem and security objective

		Security objectives															
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN	O.HDD_ENC	O.HDD_SHRED	OE.NOEVIL	OE.NOEVIL-MNT	OE.PHYSICAL_SEC	OE.MANAGE_SECRET	OE.MANAGEMENT_PC	OE.CONNECT_STORAGE	OE_EXTERNAL_SERVER	OE.FC-SP_HBA	OE.HDD_ENC
TOE security problem	A.NOEVIL									X								
	A.NOEVIL_MNT										X							
	A.PHYSICAL_SEC											X						
	A.MANAGE_SECRET												X					
	A.MANAGEMENT_PC													X				
	A.CONNECT_STORAGE														X			
	A.EXTERNAL_SERVER															X		
	T.ILLEGAL_XCNTL	X	X				X											
	T.TSF_COMP			X												X		
	T.LP_LEAK					X						X						
	T.CHG_CONFIG	X					X											
	T.HDD_THEFT							X										X
	T.HDD_REUSE								X									
	P.MASQ				X												X	

4.3.1 Security objective rational for assumption

Table 4-2 shows that the assumptions are addressed by the security objectives

Table 4-2 Validity of the security objectives for the assumptions

Assumptions	Rationale that assumptions are addressed
A.NOEVIL	A.NOEVIL, as the description of OE. NOEVIL shows, assign a reliable person to the security administrator and audit log administrator respectively for managing or operating the whole storage system. This can be realized by assigning a reliable person to the storage administrator for managing and operating the storage system in the ranged authorized by the administrator who has the authority,
A.NOEVIL_MNT	A.NOEVIL_MNT can be realized by assigning a reliable person to the maintenance personnel as the description of OE.NOEVIL_MNT.
A.PHYSICAL_SEC	A.PHYSICAL_SEC can be realized by ensuring that storage systems, host (including fibre channel connection adapter), fibre channel switch, other storage system and external authentication server are installed in a secure area where only security administrator, storage administrator, audit log administrator and maintenance personnel can access, and protected from unauthorized physical accesses as the description of OE.PHYSICAL_SEC shows.
A.MANAGE_SECRET	A.MANAGE_SECRET can be realized by ensuring that the the secret for host authentication is managed not to be used by a person who is not authorized by the security administrator as the description of OE.MANAGE_SECRET shows.
A.MANAGEMENT_PC	A.MANAGEMENT_PC can be realized by ensuring that the Storage Navigator user correctly installs and manages the management PC (administrator client PC) in accordance with the organizational security policy to prevent unauthorized use as the description of OE.MANAGEMENT_PC shows.
A.CONNECT_STORAGE	A.CONNECT_STORAGE can be realized by limiting that other storage system to be connected with the TOE must be the one consists of TOE as the description of OE.CONNECT_STORAGE shows.
A.EXTERNAL_SERVER	A.EXTERNAL_SERVER can be realized by ensuring that the external authentication server is capable of using authentication protocol that can protect the communication with SVP PC supported by the TOE and registering and managing user identification information and user group information correctly while keeping the consistency with the TOE as the description of OE.EXTERNAL_SERVER shows.

4.3.2 Security objective rationale for threat

Table 4-3 shows that the security objectives can help to cope with threats.

Table 4-3 Validity of the security objectives to cope with threats

Threats	Rationale that threats are being addressed
T.ILLEGAL_XCNTL	T.ILLEGAL_XCNTL is addressed by O.ADM_AUTH, O.ADM_ROLE and O.AUD_GEN as follows. ・ The TOE reduces threats by executing the identity authentication for Storage Navigator user and maintenance personnel by limiting management operations done by the Storage Navigator user and maintenance personnel as follows. ➢ The security administrator can perform user management, resource management, authentication setting for host and fibre channel switch, and encrypting stored data. ➢ The audit log administrator can perform operations related to audit logs. ➢ The storage administrator can perform storage management in the permitted resource group. ➢ The maintenance personnel can manage behavior of external authentication server and perform maintenance for storage system. ・ The requirement for the TOE, which is to trace security issues at setting change related to security, can reduce threats.
T.TSF_COMP	T.TSF_COMP is addressed by O.SEC_COMM and OE.EXTERNAL_SERVER as follows. ・ The encrypted communication is employed for the communication between Storage Navigator and SVP PC, which can reduce the threats, such as sniffing by connecting unauthorized devices. ・ The encrypted communication is employed for the communication between SVP PC and an external authentication server, which can reduce threats such as sniffing by connecting unauthorized devices. ・ LDAPS, starttls or RADIUS (authentication protocol is CHAP) is used for the protocol of communication between SVP PC and an external authentication server to manage the user identity information and group information registered in the external authentication server while keeping consistency with the TOE, which can reduce the threats to leakage of Storage Navigator and maintenance personnel user ID and password, and of group information.
T.LP_LEAK	T.LP_LEAK is addressed by O.HOST_ACCESS and OE.PHYSICAL_SEC as follows. ・ The TOE identifies and controls host so to ensure that the

Threats	Rationale that threats are being addressed
	authorized host only can access the authorized LDEV, which can reduce threats. ・ Storage system, host (including fibre channel connection adapter), fibre channel switch, other storage system and external authentication server are installed in a secure area where only security administrator, storage administrator, audit log administrator and maintenance personnel are allowed to access and are completely protected from unauthorized physical access, which can reduce threats.
T.CHG_CONFIG	T.CHG_CONFIG is addressed by O.ADM_AUTH and O.AUD_GEN as follows. ・ The TOE authenticates Storage Navigator user before management operation of disk subsystem and reject them if the authentication fails, which reduces unauthorized accesses by the third party. ・ The TOE can trace security related issues when the authentication fails, which can reduce unauthorized accesses by the third party.
T.HDD_THEFT	T.HDD_THEFT is addressed by O.HDD_ENC and OE.HDD_ENC as follows. ・ The TOE manages encryption key used to encrypt user data in a hard disk, which can reduce threats such as leakage of user data from the hard disk. ・ The user data is encrypted by using LSI equipped in DKA of storage system, which can reduce threats to user data leakage from the hard disk that is taken out of the storage system by the third party who can access the storage system.
T.HDD_REUSE	T.HDD_REUSE is addressed by O.HDD_SHRED as follows. ・ The TOE shreds the user data in hard disk of storage system when the use of hard disk stops, which can reduce the threat to the user data leakage from the hard disk.

4.3.3 Security objective rationale for organizational security policy

Table 4-4 shows that the organizational security policy is realized by the security objective.

Table 4-4 Validity of the security objectives for organizational security policy

Organizational security policy	Rationale for the fact that organizational security policy is realized
P.MASQ	P.MASQ is realized by O.HOST_AUTH and OE.FC-SP_HBA as follows. ・ The fibre channel connection adapter with FC-SP function is equipped in a host for host authentication. To use the

	fibre channel switch, the one with FC-SP function is used. ・ The TOE execute identity authentication of host by the FC-SP function before the host accesses the corresponding port.

5 Extended components definition

This ST complies with CC Part2 and CC Part3, and does not define any extended components.

6 Security requirement

This section describes security requirements.

6.1 Security functional requirements

Security requirements provided by the TOE are as follows.

All the following components are included in CC Part 2.

Notation system on the operation of functional requirements (selection, assignment and detailed) is described below.

When selecting: [selection: *Description of functional requirements*]: Chosen contents.

When assigning: [assignment: *Description of functional requirements*]: Assigned contents.

When detailed: [refinement: *Description of functional requirements*]: Refined contents.

The letters at the end of duplicated defined functional requirements means as follows.

a: The functional requirement related to access restriction, and identification and authentication of Storage Navigator and maintenance personnel.

b: The functional requirements related to access control and host authentication.

- Security audit (FAU)

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

[selection: choose one of; *minimum, basic, detailed, not specified*]: not specified.

[assignment: *other specifically defined auditable events*]: Auditable event to be described in “Audit Items” on Table 6-1.

[assignment: *other audit relevant information*]: None

Table 6-1 Individually defined items to be audited

Required functions	Audit Items
FAU_GEN.1	None.
FAU_GEN.2	None.
FAU_SAR.1	None.
FAU_STG.1	None.
FAU_STG.3	None.
FAU_STG.4	None.
FCS_CKM.1	・ Record success or failure of the creation of encryption key for data encryption, in the log file.
FCS_CKM.4	・ Record success or failure of the deletion of encryption key for data encryption, in the log file.
FDP_ACC.1	None.
FDP_ACF.1	None.
FDP_RIP.1	・ Record success or failure of start or stop of user data shredding, in the log file.
FIA_AFL.1	None. Reaching threshold of authentication try is not recorded in log file.
FIA_ATD.1a	None.
FIA_ATD.1b	None.
FIA_SOS.1a	None. Unmatched metric is not recorded.
FIA_SOS.1b	None. Unmatched metric is not recorded.
FIA_UAU.1	・ Record the result of host authentication by FC-SP, in the log file.
FIA_UAU.2	・ Record the success or failure of identity authentication of Storage Navigator use and maintenance personnel, in the log file.
FIA_UID.2	・ Record the success or failure of identity authentication of Storage Navigator use and maintenance personnel, in the log file.
FIA_USB.1a	None.
FIA_USB.1b	None.
FMT_MOF.1	・ Record the enabled or disabled setting of stored data encryption function, in the log file. ・ Record the setting change of host authentication by FC-SP, in the log file. ・ Record the start or stop of shredding function, in the log file.
FMT_MSA.1	・ Record LU path information creation and deletion, in the log file. ・ Record that user account is added to or deleted from user group, in the log file. ・ Record that role is added to or deleted from user group, in the log file. ・ Record that resource group is added to or deleted from user group, in the log file.
FMT_MSA.3	None.

Required functions	Audit Items
FMT_MTD.1	• Record creation or deletion of user ID for user account and change of password, in the log file. • Record host WWN, secret creation, change, or deletion, in the log file. • Record creation, deletion, backup or restore of encryption key for data encryption, in the log file. • Record the change of user authentication method, in the log file.
FMT_MTD.3	• Record that encryption key for data encryption is restored, in the log file.
FMT_SMF.1	• Record creation or deletion of user ID for user account, change of password, or change of belonged user group, in the log file. • Record creation, change, or deletion of host WWN or secret.
FMT_SMR.1	• Record change of user group where the user account belongs to, in the log file. • Record that role is added to or deleted from user group, in the log file.
FPT_STM.1	None.
FTP_ITC.1	• Record the success or failure of identity authentication of Storage Navigator use and maintenance personnel, in the log file.
FTP_TRP.1	• Record the success or failure of identity authentication of Storage Navigator use and maintenance personnel, in the log file.

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

[assignment: *authorised users*]: Audit log administrators

[assignment: list of audit information]: It describes in the Audit Information on Table 6-2.

Table 6-2 Audit Information

Audit event	Audit Information

Audit event	Audit Information
Identity authentication of the Storage Navigator user	• Success or failure of the identity authentication of Storage Navigator user, executed date and time of the identity authentication, user ID of the Storage Navigator, IP address of the management PC.
Identity authentication of the maintenance personnel	• Success or failure of the identity authentication of maintenance personnel, executed data and time, user ID of the maintenance personnel, and IP address of maintenance PC.
Creation, modification and deletion of user account of Storage Navigator user and maintenance personnel	• User ID of security administrator who creates or deletes a user ID of user account, executed date and time, user ID of the operation target, authentication method, operation (creation, modification, deletion), operation result (success or failure)
Change of user account password of Storage Navigator user and maintenance personnel	• User ID of the Storage Navigator user and maintenance personnel who change user account password, executed date and time, user ID of operation target and operation result (success or failure).
Change of user group where the user account of Storage Navigator and maintenance personnel belongs to	• User ID of the security administrator who changes user group, executed date and time, name of user group, name of role, name of resource group, operation (role addition, deletion, RSG # addition, and deletion), and operation results (success or failure).
Creation and deletion of LU path information	• User ID of the storage administrator who creates or delete the LU path information, executed date and time, operation (creation or deletion), port number, WWN, LU number, LDEV number and operation result (success or failure).
Addition, modification and deletion of host WWN and secret	• User ID of the storage administrator, security administrator, or maintenance personnel who create, modify or delete the secured (in this case security administrator only) or host WWN, executed date and time, port number, host WWN, operation (creation, modification, deletion) and operation result (success or failure).
Setting change of existence or nonexistence of host identity authentication by FC-SP	• User ID of the security administrator who changes existence or nonexistence of host identity authentication by FC-SP, executed date and time, host WWN, existence of authentication, operation (change), and operation result (success or failure).
Host identity authentication by FC-SP	• WWN of host whose identity is authenticated, executed date and time and authentication result.
Setting for encryption of stored data	• User ID of the administrator who per forms the setting to enable or disable encryption of stored data, executed date and time, parity group number, encryption setting status (enable/disable), operated encryption key number, the number of setting parity groups, and operation result (success or failure).
Generation, deletion, backup and restoring of encryption key for encryption of stored data	• User ID of the security administrator who performs generation, deletion, backup and restoring of encryption key for data encryption, executed date and time, operation (generation, deletion, backup or restoring), encryption key number, the number of operated encryption keys, and operation result (success or failure).

Audit event	Audit Information
Start or stop of shredding	• User ID of the storage administrator who performs volume shredding, executed date and time, operation (start or stop), written data, the number of writing operations, target LDEV number, the execution order of shredding, and operation result (success or failure).

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

[selection: choose one of: *prevent, detect*]: prevent

FAU_STG.3 Action in case of possible audit data loss
Hierarchical to: No other components.
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

[assignment: *actions to be taken in case of possible audit storage failure*]: Give a warning on Storage Navigator screen.

[assignment: *pre-defined limit*]: 175,000 lines

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection: choose one of:*"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]: *overwrite the oldest stored audit records*

[assignment: *other actions to be taken in case of audit storage failure*]: None

- Encryption support (FCS)

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[refinement: *cryptographic key*]: Encryption key for data encryption

[assignment: *list of standards*]: Shown in "Standard" on Table 6-3.

[assignment: *cryptographic key generation algorithm*]: Shown in "Algorithm on Table 6-3.

[assignment: *cryptographic key sizes*]: Shown in "Key size 8bit) on Table 6-3.

Table 6-3 Generation of cryptographic key

Cryptographic key	Standard	Algorithm	Key size(bit)
Encryption key for data encryption	FIPS PUB 197	AES	256

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

[refinement: *cryptographic keys*]: Encryption keys for data encryption

[refinement: *cryptographic key*]: Encryption key for data encryption

[assignment: *list of standards*]: None

[assignment: *cryptographic key destruction method*]: shown in "Encryption destruction method on Table 6-4. Encryption key destruction method.

Table 6-4 Encryption key destruction method

Encryption key	Destruction method

Encryption key	Destruction method
Encryption key for data encryption	According to an instruction of security administrator, destroy the specified encryption key information and release the memory where the information is stored.

- User data protection (FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Subject: Shown in "Subject" on Table 6-5.

Object: Shown in "Object" on Table 6-5.

List of operations between subjects and objects handled by SFP: Shown in "Operations between subjects and objects on Table 6-5.

[assignment: *access control SFP*]: LM access control SFP

Table 6-5 Operations between subjects and objects

Subject	Object	Operation between subject and object
Processing acts for host	LDEV	➢ Access to LDEV
Processing acts for Storage Navigator	LDEV	➢ LDEV creation and deletion
	RSG	➢ RSG creation and deletion

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following

additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]:

Subjects: Processing acts for host, processing acts for Storage Navigator

Objects: LDEV, RSG

The SFP-relevant security attribute or groups with name of SFP-relevant security attribute: Shown in "Security attribute of subject" and "Security attribute of object" on Table 6-6.

Table 6-6 SFP-relevant security attribute

Subject	Security attribute of subject	Security attribute of object
Processing acts for host	WWN, LU number	LU path information (WWN, LU number, LDEV number)
Processing acts for Storage Navigator	User group information (role, RSG number)	Resource group information (RSG number) LU path information (WWN, LU number, LDEV number)

[assignment: *access control SFP*]: LM access control SFP

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]: Rules described in "Rule" on Table 6-7.

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]: None

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]: None

Table 6-7 Rules between subjects and objects

Subjects	Rules	Objects
Processing acts for host	Allow access to objects if the WWN and LU number given from a host to the processing acts for host, and the LU path information that is the security attribute of corresponding objects match each other. Refuse access if the above do not match each other.	LDEV
Processing acts for Storage Navigator	Rule to create or delete the objects by the processing acts for Storage Navigator. 1) In case of security administrator role Creation allows if RSG number is not duplicated, while deletion is allowed if RSG number exists.	RSG

Subjects	Rules	Objects
	Rule to create or delete objects by the processing acts for Storage Navigator. 1) In case of storage administrator role Creation of the LDEV is allowed if a resource group of RSD number allocated to the storage administrator contains the LDEV number to be created. Deletion of the LDEV is allowed if a resource group of RSG number allocated to the storage administrator contains LDEV number to be deleted and the information of LU path associated with the LDEV does not exist.	LDEV

FDP_RIP.1 Subset residual information protection
Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]: *deallocation of the resource from*

[assignment: *list of objects*]: LDEV

- Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*]: 3

[assignment: *list of authentication events*]*:* Authentication by Storage Navigator, or that when connecting to SVP PV via remote desktop.

[refinement: *administrator*]: Security administrator

[selection: *met, surpassed*]:met

[assignment: *list of actions*]: refuse the login of the user for a minute, and then the number of unsuccessful authentication attempts cleared to be 0.

FIA_ATD.1a User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1a The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]: Role, RSG number

FIA_ATD.1b User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1b The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]: WWN, LU number

FIA_SOS.1a Verification of secrets
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1a The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]: at least 6 characters and no more than 256 characters (password for maintenance personnel is 127 characters) containing one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, and any of the following 32 symbols; !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~.

FIA_SOS.1b Verification of secrets
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1b The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]: at least 12 characters and no more than 32 characters containing one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols;.-+@_=:/[],~.

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[refinement: *user*]: host

[assignment: *list of TSF mediated actions*]: Sending DH-CHAP authentication code which is an authentication method of FC-SP function.

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[refinement: *user*]: Storage Navigator user, maintenance personnel

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[refinement: *user*]: Storage Navigator user, maintenance personnel, or host

FIA_USB.1a User-subject binding
Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1a The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2a The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3a The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *list of user security attributes*]: Role, RSG number

[assignment: *rule for the initial association of attributes*]: None

[assignment: r*ule for the changing attributes*]: None

FIA_USB.1b User-subject binding
Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1b The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2b The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3b The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *list of user security attributes*]: WWN, LU number

[assignment: *rule for the initial association of attributes*]: None

[assignment: r*ule for the changing attribute*s]: None

- Management of security (FMT)

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

[assignment: *list of functions*]: Shown in "Function" on Table 6-8.

[selection: *determine the behavior of, disable, enable, modify the behavior of*]: disable, enable

[assignment: *the authorized identified roles*]: Shown in "Role" on Table 6-8.

Table 6-8 List of functions restricting operations for roles

No	Roles	Functions
1	Security administrator	➢ Encryption of stored data function ➢ FC-SP authentication function
2	Storage administrator	➢ Shredding function
3	Maintenance personnel	➢ External authentication server connection function

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised* ***identified roles*****].**

[assignment: *access control SFP(s), information flow control SFP(s)*]: LM access control SFP

[selection: *change_default, query, modify, delete, [assignment: other operations]*]: Operations described in "Operations for LU path information" on Table 6-9, and in "Operations for user group information" on Table 6-10.

[assignment: *list of security attributes*]: LU path information, user group information

[assignment: *the authorized identified roles*]: Described in "Roles" on Table 6-9 and Table 6-10.

Table 6-9 Operations of Storage Navigator user and maintenance personnel for security attributes of processing act for host

Roles	Operations for LU path information					
	RSG number =n			RSG number ≠n		
	WWN	LU number	LDEV number	WWN	LU number	LDEV number
Storage administrator (RSG number = n)	Query, creation, deletion	Query, creation, deletion	Query, creation, deletion	-	-	-
Security administrator	-	-	-	-	-	-
Audit log administrator	-	-	-	-	-	-
Maintenance personnel (All resource groups are assigned to maintenance personnel	Query, creation, deletion	Query, creation, deletion	Query, creation, deletion			

-: No operation

Table 6-10 Operations of Storage Navigator user and maintenance personnel for security attribute (user group information) of processing act for Storage Navigator

Roles	Operations for user group information	
	Roles	RSG number
Security administrator	➢ Addition ➢ Deletion ➢ Query	➢ Addition ➢ Deletion ➢ Query
Storage administrator	➢ (own) Query	➢ (own) Query
Audit log administrator	➢ (own) Query	➢ (own) Query

Roles	Operations for user group information	
	Roles	RSG number
Maintenance personnel	➢ (own) Query	➢ (own) Query

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *access control SFP, information flow control SFP*]: LM access control SFP

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]: restrictive

[assignment: *the authorized identified roles*]: None

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TFS data*]:

User ID and password of Storage Navigator user and maintenance personnel

Host WWN, secret

Encryption key for data encryption

User authentication method

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: Operations for “User account” on Table 6-11, operations for “Host authentication data” on Table 6-12, operations for “Encryption key for data encryption” on Table 6-13, operations for “User authentication method” on Table 6-14.

[assignment: *the authorized identified roles*]: Roles described in “Roles” on Table 6-11, Table 6-12, Table 6-13 and Table 6-14.

Table 6-11 Operations of Storage Navigator and maintenance personnel for user account

Roles	User account of Storage Navigator user and maintenance personnel	
	User ID	Password
Security administrator	Query, creation, deletion	Modification
Storage administrator	(own) Query	(own) Modification
Audit log administrator	(own) Query	(own) Modification
Maintenance personnel	(own) Query	(own) Modification

Table 6-12 Operations of Storage Navigator user and maintenance personnel for host authentication data

Role	Host authentication data	
	Host WWN	Host secret
Security administrator	Query, creation, modification, deletion	Creation, modification, deletion
Storage administrator	Query, creation, modification, deletion	-
Audit log administrator	-	-
Maintenance personnel	Query, creation, modification, deletion	-

-: No operation

Table 6-13 Operations of Storage Navigator user and maintenance personnel for encryption key for data encryption

Roles	Encryption key for data encryption
Security administrator	Creation, deletion, query, modification
Storage administrator	-
Audit log administrator	-

Roles	Encryption key for data encryption
Maintenance personnel	—

-: No operation

Table 6-14 Operations of Storage Navigator user and maintenance personnel for user authentication method

Roles	User authentication method
Security administrator	Query, modification
Storage administrator	-
Audit log administrator	-
Maintenance personnel	-

-: No operation

FMT_MTD.3 Secure TSF data
Hierarchical to: No other components.
Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [assignment: *list of TSF data*].

[assignment: *list of TSF data*]: Encryption key for data encryption

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

[assignment: *list of management functions to be provided by the TSF*]: The following functions are provided.

- Function to manage user ID of user account and host authentication (host WWN)
- Function to manage password for user ID of user account
- Function to manage host authentication data
- Function to manage role of user account
- Function to manage security attribute of processing acting for host
- Function to manage security attribute of processing acting for Storage Navigator
- Function to manage operations by Storage Navigator user and maintenance

personnel for user account

- Function to manage operations by Storage Navigator user and maintenance personnel for host authentication data
- Function to manage operations by Storage Navigator and maintenance personnel for encryption key for data encryption
- Function to stop and activate data encryption function
- Function to stop and activate FC-SP authentication function
- Function to stop and activate shredding function
- Function to stop and activate external authentication server connection function

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

[assignment: *the authorized identified roles*]:
- Security administrator
- Storage administrator
- Audit log administrator
- Maintenance personnel
- Storage user

- Protection of TSF (FPT)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

- Reliable path/channel (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

[refinement: *another trusted IT product*]: External authentication server

[selection: the *TSF, another trusted IT product*]: TSF

[assignment: *list of functions for which a trusted channel is required*]: Sending password and user ID of user account used for identification and authentication (external authentication server method) of Storage Navigator user and maintenance personnel.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*].

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication, [assignment: other services for which trusted path is required]*].

[selection: *remote, local*]: remote

[selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]*:*disclosure

[selection: *the TSF, local users, remote users*]: remote users

[selection: *initial user authentication, [assignment: other services for which trusted path is required]*]:

[*assignment: assignment: other services for which trusted path is required*]: Communication using Storage Navigator

6.2 Security assurance requirements

The TOE security assurance requirements are as follows.

The evaluation assurance level of the TOE is EAL2. All security assurance requirements directly use security assurance components stipulated in CC Part3.

(1) Development (ADV)

ADV_ARC.1 : Security architecture description
ADV_FSP.2 : Security-enforcing functional specification
ADV_TDS.1 : Basic design

(2) Guidance documents (AGD)

AGD_OPE.1 : Operational user guidance
AGD_PRE.1 : Preparative procedures

(3) Life-cycle support (ALC)

ALC_CMC.2 : Use of a CM system
ALC_CMS.2 : Parts of the TOE CM coverage
ALC_DEL.1 : Delivery procedures

(4) Security target evaluation (ASE)

ASE_CCL.1 : Conformance claims
ASE_ECD.1 : Extended components definition
ASE_INT.1 : ST introduction
ASE_OBJ.2 : Security objectives
ASE_REQ.2 : Derived security requirements
ASE_SPD.1 : Security problem definition
ASE_TSS.1 : TOE summary specification

(5) Test (ATE)

ATE_COV.1 : Evidence of coverage ATE_FUN.1 : Functional testing ATE_IND.2 : Independent testing - sample

(6) Vulnerability evaluation (AVA)

AVA_VAN.2 : Vulnerability analysis

6.3 Security requirement rationale

6.3.1 Security requirement rationale

Table 6-15 shows correspondence relation between security function requirements and TOE security objectives. Each security function requirement corresponds to at least one TOE security objective.

Table 6-15 Correspondence between security objectives and security function requirements

		TOE security objectives							
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
TOE security function requirements	FAU_GEN.1								X
	FAU_GEN.2								X
	FAU_SAR.1								X
	FAU_STG.1								X
	FAU_STG.3								X
	FAU_STG.4								X
	FCS_CKM.1						X		
	FCS_CKM.4						X		
	FDP_ACC.1		X			X			
	FDP_ACF.1		X			X			
	FDP_RIP.1							X	
	FIA_AFL.1	X							
	FIA_ATD.1a	X							
	FIA_ATD.1b					X			
	FIA_SOS.1a	X							
	FIA_SOS.1b				X				
	FIA_UAU.1				X				
	FIA_UAU.2	X							
	FIA_UID.2	X				X			
	FIA_USB.1a	X							

	TOE security objectives							
	O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
FIA_USB.1b					X			
FMT_MOF.1		X						
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_MTD.1		X				X		
FMT_MTD.3						X		
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_STM.1								X
FTP_ITC.1			X					
FTP_TRP.1			X					

Table 6-16 shows that the TOE security objectives are realized by the TOE security function requirements.

Table 6-16 Validity of security function requirements for TOE security objectives

TOE security objectives	Rationale that TOE security objectives are realized
O.ADM_AUTH	O.ADM_AUTH requires performing identification and authentication of Storage Navigator user before the Storage Navigator user performs management operation of disk subsystem. The details of necessary measures and required functions for the above request are as follows. a. Maintaining Storage Navigator user The TOE must define user accounts, associate users with the user accounts, and maintain them to identify Storage Navigator users. In other words, it enables identification of Storage Navigator users. The security requirements corresponding to the requirement are FIA_ATD.1a and FIA_USB.1a. b. Identity authentication of Storage Navigator user account before using the TOE Before the TOE is used, the TOE must identify user accounts. Therefore, performing identity authentication of user accounts before execution of any of all Storage Navigator functions is required. The security function requirements corresponding to the

TOE security objectives	Rationale that TOE security objectives are realized
	requirement are FIA_UID.2 and FIA_UAU.2. c. Managing password The password for the TOE to authenticate user accounts must be at least 6 characters and no more than 256 characters (the password for maintenance personnel is 127 characters) consist of combination of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, and any of the following 32 symbols; !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~. If authentication fails 3 times in a row due to entering incorrect password, login of the user ID is refused for a minute, which can decrease the possibility of breaking password. The security function requirements corresponding to the function are FIA_AFL.1 and FIA_SOS.1a. O.ADM_AUTH can be satisfied by achieving all of a, b, and C. And that is, meeting FIA_ATD.1a, FIA_USB.1a, FIA_AFL.1, FIA_SOS.1a, FIA_UAU.2, and FIA_UID.2, which are necessary security requirements, can realize O.ADM_AUTH.
O.ADM_ROLE	O.ADM_ROLE requires be able to restrict management operations by Storage Navigator user and maintenance personnel based on roles of identified and authenticated user ID. The details of necessary measurement and required functions for the above request are as follows. a. Restricting operations of role and RSG number The TOE must restrict addition and deletion of role of user account and RSG number, and creation and deletion of RSG according to the role of user account. The TOE therefore restricts the change for user account based on the rule defined as [LM access control SFP]. The security function requirement corresponding to the requirement is FMT_MSA.1. b. Managing identity authentication information The TOE must restrict change for password and user ID of user account, authentication method, and host WWN and secret according to the role of user account. This can prevent unauthorized change for password and user ID of user account, authentication method, and host WWN and secret. The security function requirement corresponding to the requirement is FMT_MTD.1. c. Holding management function The TOE must have a function to manage Storage Navigator user account, role of user account, host authentication information, WWN identification information, LU path information, and user group information. The TOE must have a function to manage operations by Storage Navigator user and maintenance personnel. Also, it must have a function to stop and activate the data encryption function, the FC-SP authentication function, the shredding function, and the external authentication server connection function. The security function requirement corresponding to the above requirements is FMT_SMF.1. d. Maintaining role The TOE must maintain the roles of security administrator, storage administrator, audit log administrator, maintenance personnel and storage user, and associate them with users. The security function requirement corresponding to the above requirement is

TOE security objectives	Rationale that TOE security objectives are realized
	FMT_SMR.1. e. Managing behavior of security function The TOE must restrict activation and stop of stored data encryption/decryption, host authentication, connection with external authentication server, and shredding function according to roles of user account. It can prevent unauthorized change to use or stop each function. The security function requirement corresponding to the above function is FMT_MOF.1. f. Defining and executing access control The TOE must create and delete RSG and LDEV in accordance with the rule defined as [LM access control SFP] for Storage Navigator user and maintenance personnel. It enables the storage administrator to create and delete LDEVs in the allocated RSG. Also, restrictive default value can be assigned as access attribute at LDEV creation. It means that accesses are limited because LU path information does not exist at the LDEV creation. The security function requirements corresponding to the above requirement are FDP_ACC.1, FDP_ACF.1 and FMT_MSA.3. O.ADM_ROLE is satisfied by achieving the above a, b, c, d, e, and f. And that is, achieving FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FDP_ACC.1, and FDP_ACF.1, which are necessary security function requirements for each measurement, can realize O.ADM_ROLE.
O.SEC_COMM	O.SEC_COMM requires providing a secure communication function by encrypting communication data between Storage Navigator and SVP PC, and between SVP PC and external authentication server to prevent sniffing. The detail of necessary measurement and required function for the above request are as follows. a. Protecting communication data between Storage Navigator and SVP PC Reliable path is used for the communication between Storage Navigator and SVP PC to protect the data from sniffing. The security function requirement corresponding to the function is FTP_TRP.1. b. Protecting communication data between SVP PC and external authentication server When an external authentication server is used for identity authentication (the external authentication server method), reliable channel is used for the communication between SVP PC and the external authentication server. It can protect the communication data from sniffing. The security function requirement corresponding to the function is FTP_ITC.1. O.SEC_COMM can be satisfied by achieving all of the above a and b. And that is, achieving FTP_TRP.1 and FTP_ITC.1, which are the necessary security function requirements for each measurement, cam realize O.SEC_COMM.
O.HOST_AUTH	O.HOST_AUTH requires authenticating a host when the host requests connection. The detail of necessary measurement and required function for the above request are as follows. a. Executing FC-SP function When the TOE receives a command to execute security authentication from a host, it

TOE security objectives	Rationale that TOE security objectives are realized
	generates and returns DH-CHAP authentication code. (FIA_UAU.1) b. Managing secret A secret for the TOE to authenticate a host is at least 12 characters and no more than 32 characters consist of combination of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols; .-+@_=:/[],~. It can decrease the possibility that the password is broken. The security function requirement corresponding to the function is FIA_SOS.1b. O.HOST_AUTH can be satisfied by achieving all of the above a and b. And that is, achieving FIA_UAU.1 and FIA_SOS.1b which are the necessary security function requirements can realize O.HOST_AUTH.
O.HOST_ACCESS	O.HOST_ACCESS requires performing identification of host and access control to allow the host to access only LDEVs allocated to the host when the host accesses the user data of LU that is the protection target property of the TOE. The detail of necessary measurement and required functions for the above request are as follows. a. Maintaining host The TOE must define host attribute information (WWN, LU number), associate the attribute to the host, and maintain them. The security function requirements corresponding to the requirement are FIA_ATD.1b and FIA_USB.1b. b. Identifying host before using TOE Before the TOE is used, the TOE must identify host. The security function requirement corresponding to the request is FIA_UID2. c. Defining and executing access control For each host, the TOE determines access to LDEV according to the rule defined as [LM access control SFP] and must exactly perform the access control so that the host can access user data in allocated LDEVs. The security function requirements corresponding to the request are FDP_ACC.1 and FDP_ACF.1. O.HOST_ACCESS can be satisfied by achieving all of a, b, and c. And that is, achieving FIA_ATD.1b, FIA_USB.1b, FIA_UID2, FDP_ACC.1, and FDP_ACF.1 which are the necessary security function requirements can realize O.HOST_ACCESS.
O.HDD_ENC	O.HDD_ENC requires managing encryption key for data encryption to prevent user data in a hard disk taken out of storage system from being leaked. The detail of necessary measure and required function for the request are as follows. a. Generating and deleting encryption key for data encryption User data stored in a hard disk needs to be encrypted to prevent the user data from being leaked from the hard disk replaced as preventive maintenance. For encryption and decryption, LSI embedded in DKA is used. The TOE generates encryption keys to user for encryption and deletes them after user. The security function requirements corresponding to the above function are FCS_CKM.1, and FCS_CKM.4.

TOE security objectives	Rationale that TOE security objectives are realized
	b. Restricting operations for encryption key for data encryption The TOE needs to restrict operations for encryption keys according to user account roles. In addition, it manages encryption keys so that keys other than those with backup cannot be restored. This prevents unauthorized modification for encryption keys. The security function requirements corresponding to the request are FMT_MTD.1 and FMT_MTD.3. O.HDD_ENC can be satisfied by achieving all of the above a and b. And that is, achieving FCS_CKM.1, FCS_CKM.4 , FMT_MTD.1, FMT_MTD.3 which are necessary security function requirements can realize O.HDD_ENC.
O.HDD_SHRED	O.HDD_ SHRED requires shredding old user data in a hard disk before re-using the hard disk of storage system to prevent the user data from being leaked. The detail of necessary measurement and required function for the request are as follows. a. Protecting user data in hard disk When a hard disk becomes disuse, the user data stored in the hard disk needs to be shred so as to protect the user data from being leaked from the hard disk. The security function requirement corresponding to the above function is FDP_RIP.1. O.HDD_ SHRED can be satisfied by achieving the measurement. And that is, achieving FDP_RIP.1 that is the necessary function requirement for the measurement can realize O.HDD_ SHRED.
O.AUD_GEN	O.AUD_GEN requires observing unauthorized creation, modification and deletion of security related information. The detail of necessary measurement and required function for the above request are as follows. a. Generating audit log of security function related issues If identity authentication by Storage Navigator or falsifications of user account, role, or RSG occurs, SVP PV must generate audit log of the issue for identification from the audit log if such information is incorrectly falsified. The security function requirement corresponding to the request is FAU_GEN.1. Because FAU_GEN.1 obtains audit logs of identity authentication issue, operating issues of setting change, encryption, and user data shredding, the security objective is satisfied. Items without audit item in Table 6-1 of FAU_GEN.1 have no problem if there are no items to be audited since no efficacy is expected from the trace, or they are included in other audit target and can be surely traced. In addition, in the state of no LU path information setting, because a host cannot recognize the corresponding LDEV as a logical device, therefore cannot access the LDEV, not to obtain the audit issue related to the security function requirement of access from host to LDEV does not cause any problem. Because time stamps provided by FPT_STM.1 are those for SVP PC OS and cannot be modified by other than maintenance personnel, logs for issue such as time setting

TOE security objectives	Rationale that TOE security objectives are realized
	change do not need to be obtained. When generating audit log, the date and time the issue occurs and user ID of user who performs the operation need to be put in the audit log so that occurrence date and time and the user who operates can be identified. The security function requirements corresponding to the request are FAU_GEN.2 and FPT_STM.1. b. Restricting reference to audit log To refer audit records, the audit record in SVP PC needs to be downloaded from Storage Navigator. Downloading the audit record is limited to a user account with audit log administrator role to protect the audit logs from unauthorized reference. The security function requirement corresponding to the request is FAU_SAR.1. c. Protecting the audit log from falsification The TOE must prevent deletion and falsification of audit logs by an unauthorized user. Downloading the audit logs is limited to a user account with audit log administrator role. The TOE itself does not have a function to modify the audit logs to protect the audit logs from unauthorized deletion or modification. The security function requirement corresponding to the request is FAU_STG.1. d. Warning risk of loss of audit log Up to 250,000 lines audit logs can be created but when the number of audit logs exceeds the maximum, the oldest audit log is erased. To avoid the loss of audit logs, when the number of audit logs goes over 175,000, a warning to indicate the exceedance is displayed on Storage Navigator window to persuade downloading the audit logs. The security function requirements corresponding to the request are FAU_STG.3 and FAU_STG.4. O.AUD_GEN can be satisfied by achieving all the above measurements a, b, c, and d. And that is, achieving FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1, FAU_STG.3, and FAU_STG.4 which are the security function requirements can realize O.AUD_GEN.

6.3.2 Security requirement internal consistency rationale

Table 6-17 shows dependencies of security requirement components.

Table 6-17 Dependencies of security function requirements

No	TOE/IT environment	Security function requirements	Dependencies defined in CC Part2	Function requirement addressed by this ST
1	TOE	FAU_GEN.1	FPT_STM.1	FPT_STM.1
2	TOE	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
			FIA_UID.1	FIA_UID.2 *1
3	TOE	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
4	TOE	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
5	TOE	FAU_STG.3	FAU_STG.1	FAU_STG.1
6	TOE	FAU_STG.4	FAU_STG.1	FAU_STG.1
7	TOE	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	None *3
			FCS_CKM.4	FCS_CKM.4
8	TOE	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
9	TOE	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
10	TOE	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
			FMT_MSA.3	FMT_MSA.3
11	TOE	FDP_RIP.1	None	-
12	TOE	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 *2
13	TOE	FIA_ATD.1a	None	-
14	TOE	FIA_ATD.1b	None	-
15	TOE	FIA_SOS.1a	None	-
16	TOE	FIA_SOS.1b	None	-
17	TOE	FIA_UAU.1	FIA_UID.1	FIA_UID.2 *1
18	TOE	FIA_UAU.2	FIA_UID.1	FIA_UID.2 *1
19	TOE	FIA_UID.2	None	-
20	TOE	FIA_USB.1a	FIA_ATD.1	FIA_ATD.1a
21	TOE	FIA_USB.1b	FIA_ATD.1	FIA_ATD.1b
22	TOE	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
23	TOE	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1
			FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
24	TOE	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
			FMT_SMR.1	FMT_SMR.1
25	TOE	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
26	TOE	FMT_MTD.3	FMT_MTD.1	FMT_MTD.1
27	TOE	FMT_SMF.1	None	-
28	TOE	FMT_SMR.1	FIA_UID.1	FIA_UID.2 *1
29	TOE	FPT_STM.1	None	-
30	TOE	FTP_ITC.1	None	-
31	TOE	FTP_TRP.1	None	-

*1: Dependency is satisfied by FIA_UID.2 which is the upper hierarchy to FIA_UID.1.

*2: Dependency is satisfied by FIA_UAU.2 which is the upper hierarchy to FIA_UAU.1.

*3: Because the TOE is software, and encryption and decryption are fulfilled by hardware, there is no corresponding function requirement.

Table 6-18 shows the rationale that the definition maintains consistency of function requirements in the same category for each TOE security function requirements.

Table 6-18 Consistency between security function requirements

No	Category	Security function requirements	Rationale of consistency
1	Access control	FDP_ACC.1 FDP_ACF.1 FDP_RIP.1	Access control is defined based on these function requirements. Because they require applying the same SFP to the same object and subject, there is no confliction or inconsistency, but the whole contents are consistent.
2	Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MTD.3 FMT_SMF.1 FMT_SMR.1	Security management is defined based on these function requirements. There is no confliction or inconsistency for target security attribute or action and the whole contents are consistent.
3	Identification and authentication	FIA_AFL.1 FIA_ATD.1a FIA_ATD.1b FIA_SOS.1a FIA_SOS.1b FIA_UAU.1 FIA_UAU.2 FIA_UID.2 FIA_USB.1a FIA_USB.1b	These function requirements realize the identification and authentication. As TSF, (1) Storage Navigator user ID and password, and (2) host WWN and secret are separately defined, and there is no confliction or inconsistency. The whole contents are consistent.
4	Audit	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1 FAU_STG.3 FAU_STG.4	Audit log is defined based on the function requirements, and there is no confliction or inconsistency. The whole contents are consistent.
5	Encryption key management and operation	FCS_CKM.1 FCS_CKM.4	These function requirements define operations of encryption key used to encrypt stored data, and there is no confliction or inconsistency. The whole contents are consistent.
6	Reliable path/channel	FTP_ITC.1 FTP_TRP.1	There function requirements define communication paths and channels between Storage Navigator and SVP, and between SVP PC and external authentication server, and there is no confliction or inconsistency. The whole contents are consistent.

No	Category	Security function requirements	Rationale of consistency
7	Complementary	FPT_STM.1	This function requirement is to complement other function requirements. From the fact that FPT_STM.1 is requirement for time stamp of audit log, it is obvious that there is no confliction or inconsistency between function requirements in this category and the whole contents are consistent.
7	Between categories	#1 - #2	Because requirements for access control defines the control for user data in LU which is protection target property, and the requirement for management is to define the management TSF data, there is no confliction or inconsistency between them.
		#1－#3 #2－#3	There is no confliction or inconsistency between identification requirement and access control or management requirement.
		#1 - #4 #2 - #4 #3 - #4	They are to record audit for requirements of access control, management, identification and authentication, and there is no confliction or inconsistency.
		#1 - #5 #2 - #5 #3 - #5 #4 - #5	There is no confliction or inconsistency between requirements for access control, management, identification and authentication, and audit log.
		#1 - #6 #2 - #6 #3 - #6 #4 - #6 #5 - #6	There is no confliction or inconsistency between requirements for access control, management, identification and authentication, audit log, and encryption key management and operation.
		#1 - #7 #2 - #7 #3 - #7 #4 - #7 #5 - #7 #6 - #7	FPT_STM.1is to provide FAU_GEN.1 with time information and there is no confliction or inconsistency with other requirements.

As stated below, mutual support is established by security function requirements which do not have interdependence.

- For FIA_UID.2 and FIA_UAU.1, FMT_MOF.1 limits operations to start or stop the security function according to roles, and operations can be allowed only from Storage Navigator. The security function cannot be started or stopped by any other method to prevent deactivation.

As aforementioned, IT security requirements described in the ST establish the whole with internal consistency by mutual support in integrated manner.

6.3.3 Security requirement rationale

Storage system including the TOE is installed in a secure area and does not expect other than attack path using LAN. As shown in Section 3.2, attacks from communication path between Storage Navigator or management PC and storage system, and between the storage system and external authentication server. The attack can be “low” level which does not require special knowledge, skill and tool.

Beside, as installation of unauthorized software on the administrator PC where Storage Navigator works is prohibited, potential threat based on the detailed interface to the storage system is excluded from supposition. Evaluating [certain vulnerability] can achieve the balance against the expected threat.

Even though the TOE has a function to encrypt user data stored in a hard disk using LSI embedded in DKA, implementation of encryption key is done by a reliable security administrator at the installation. For this, there is no security characteristic such that not to handle as confidential leads to vulnerability of TOE.

The TOE is software which can ensure to be able to counter expected threats by implementation of security functions based on design documents and evaluation by testing, accordingly classifying it in EAL2 of evaluation assurance level is reasonable.

7 TOE summary specification

This chapter describes summary specification of security functions provided by the TOE.

7.1 TOE Security function

Table 7-1 shows correspondence relation between TOE security functions and security function requirements (SFR). As shown here, security functions explained in this section meet all SFRs described in section 6.1.

Table 7-1 Correspondence relation between TOE security functions and security function requirements

		TOE IT security function					
		SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.HDD**	**SF.AUDIT**
TOE security function requirements	FAU_GEN.1						X
	FAU_GEN.2						X
	FAU_SAR.1						X
	FAU_STG.1						X
	FAU_STG.3						X
	FAU_STG.4						X
	FCS_CKM.1					X	
	FCS_CKM.4					X	
	FDP_ACC.1	X					
	FDP_ACF.1	X					
	FDP_RIP.1					X	
	FIA_AFL.1			X			
	FIA_ATD.1a	X					
	FIA_ATD.1b	X					
	FIA_SOS.1a			X			
	FIA_SOS.1b		X				
	FIA_UAU.1		X				
	FIA_UAU.2			X			
	FIA_UID.2	X		X			

	TOE IT security function					
	SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.HDD**	**SF.AUDIT**
FIA_USB.1a	X					
FIA_USB.1b	X					
FMT_MOF.1				X		
FMT_MSA.1				X		
FMT_MSA.3	X					
FMT_MTD.1				X	X	
FMT_MTD.3					X	
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_STM.1						X
FTP_ITC.1			X			
FTP_TRP.1			X			

The following states each TOE security functions and the specific method to realize SFR corresponding to the security functions.

7.1.1 SF.LM

The TOE is connected with a host via SAN environment. SAN is the dedicated network for storage system that connects hosts and storage systems via the fibre channel. The TOE performs access control by SF.LM while the host accesses LDEVs in the storage system.

[Satisfied Requirements] FIA_ATD.1a, IA_USB.1a, FIA_ATD.1b, FIA_USB.1b, FIA_UID.2, FDP_ACC.1, FDP_ACF.1, and FMT_MSA.3

The TOE maintains user group information (such as role and RSG number) and associates them with processing acting for Storage Navigator (FIA_ATD.1a and FIA_USB.1a).

The TOE maintains the attribute information of host (such as WWN and LU number) and associates them with processing acting for the host (FIA_ATD.1b and FIA_USB.1b).

The TOE identifies the host before an operation of security function related to access from host (FIA_UID.2).

The TOE performs [LM access control SFP] when the processing acting for a host accesses a LDEV or the

processing acting for Storage Navigator creates or delete the LDEV.

[LM access control SFP] consists of the following rules (FDP_ACC.1, FDP_ACF.1, and FMT_MSA.3)

- When WWN and LU number passed over to the processing acting for the host are consistent with LU path that is the security attribute of the corresponding object, the access to the LDEV is allowed while it is rejected if the LU path information is not consistent.
- When the processing acting for Storage Navigator creates or deletes RSG, only the security administrator can create or delete the RSG according to [User group information of Storage Navigator] (such as role and RSG) passed over to the processing acting for Storage Navigator.
- When the processing acting for Storage Navigator creates or delete LDEV, according to [User group information of Storage navigator] (such as role and RSG) passed over to the processing acting for Storage Navigator, the storage administrator can create or delete LDEV in a resource group only when RSG number assigned to the user group where the storage administrator belongs matches with the RSG number of the LDEV.
- Condition when deleting LDEV: Delete a LDEV when there is no LU path associated with the LDEV.
- When storage administrator creates LDEV, a restrictive default value is given as the access attribute. It means that the access from the host is restricted because there is no LU path information at the LDEV creation. (FMT_MSA.3)

7.1.2 SF.FCSP

The TOE executes identity authentication of host if customer security policy requires. DH-CHAP with NULL DH Group authentication is used for this authentication.

[Satisfied requirements] FIA_SOS.1b, FIA_UAU.1

If host authentication is required, the TOE creates DH-CHAP authentication code when a command of security authentication is received from the host, and sends it back to the host (FIA_UAU.1). The connection between the host and storage system is allowed when a secret received from the host matches with a secret that the TOE has (FIA_UAU.1).

The TOE restrict the entry of secret used for host identity authentication by FC-SP to be at least 12 characters and no more than 32 characters consists of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols; .-+@_=:/[],~. (FIA_SOS.1b)

7.1.3 SF.SN

[Satisfied requirements] FIA_AFL.1, FIA_SOS.1a, FIA_UID.2, FIA_UAU.2, FTP_TRP.1, and FTP_ITC.1

The TOE executes identity authentication at remote desktop connection to Storage Navigator and SVP PC using user ID and password before any operations of other security functions. If the identity authentication fails 3 times in a row, the identity authentication of the user is refused for one minute. (FIA_UID.2, FIA_UAU.2, and FIA_AFL.1)

The TOE restricts the entry for password used for Storage Navigator or maintenance personnel internal authentication to be at least 6 characters and no more than 256 characters (127 characters for maintenance personnel) consists of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, any

of the following 32 symbols; !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~. (FIA_SOS.1a)

The TOE employs SVP internal authentication method for identity authentication of Storage Navigator user and maintenance personnel. If the entered user ID does not exist in the TOE, external authentication server method is used.

When identity authentication of Storage Navigator user and maintenance personnel is executed by the external authentication server method, TOE starts communication between SVP PC and external authentication server using LDAPS, starttls or RADIUS (authentication protocol is CHAP) and sends user ID and password of user account to be used for identification and authentication of Storage Navigator user and maintenance personnel. Using LDAPS, starttls, or ADIUS (authentication protocol is CHAP) for the communication between the SVP PC and the external authentication server can prevent TSF data from being sniffed. (FTP_ITC.1)

The TOE allows starting communication when Storage Navigator user activates Storage Navigator on management PC). For the communication between Storage Navigator and SVP PC, SSL is used to prevent the TSF data from being sniffed. (FTP_TRP.1)

The SSL used for the communication between Storage Navigator and SVP PC supports [SSLv3.0] or [TLSv1.0]. Table 7-2 shows Encryption-relevant algorithm used by SSL.

Table 7-2 Encryption-relevant algorithm used by SSL

Standard	Algorithm	Key size (bit)	Encryption operation	How to use
ANSI X9.30 Part1-1997	DSA	1024	Authentication	To be used as certificate to prove SVP PC against management PC (server authentication)
RSA Security Inc. Public-Key Cryptography Standards(PKCS)#1 v2.1	RSA	512 or longer	Authentication	
			Key exchange	To be used at session key exchange.
FIPS PUB 197	AES	256 128	Data encryption and decryption	To select algorithm used for session key by hand-shake protocol in version of [SSLv3.0] and [TLSv1.0]
FIPS PUB 46-3	3DES	168		
FIPS PUB 180-2	SHA-256	256	Hash	To be used at hash value calculation
IEEE P1363 G.7	SHA1PRNG	64	Random digit	To be used as key information at session key creation

7.1.4 SF.ROLE

[Satisfied requirements] FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FMT_MOF.1

The TOE executes [LM access control SFP] for the access from the processing acting for Storage Navigator to SVP PC.

[LM access control SFP] consists of the following rules.

- [LM access control SFP] restricts operations to create, delete and refer LU path information (WWN, LU number, LDEV number) based on roles and RSG numbers. (FMT_MSA.1). Table 6-9 shows operations each role can perform for the LU path information.

- [LM access control SFP] restrict operations to add, delete and refer user group information (role and RSG number) based on roles (FMT_MSA.1). Table 6-10 shows operations each role can perform for the user group information.

The TOE manages the following TSF data. (FMT_MTD.1)

- The account management function of Storage Navigator manages user ID, password, role and RSG number of Storage Navigator user and maintenance personnel. Table 6-10 and Table 6-11 show management operations each role can perform.

- The FC-SP function of Storage Navigator manages WWN and secret which are authentication data of host. Table 6-12 shows management operations each role can perform.

- The access control function of Storage Navigator manages user authentication method. Table 6-14 shows management operations each role can perform.

The TOE has the following management functions (FMT_SMF.1).

- The function to manage user account of Storage Navigator, role of user account, host authentication information, WWN authentication information, LU path information, and user group information.

- The function to manage operations by Storage Navigator user and maintenance personnel.

- The function to manage functions for stored data encryption, FC-SP authentication function, shredding function, management function for starting or stopping connection to external authentication server.

The TOE restricts an operation to set host authentication by FC-SP (With or without authentication) based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts setting operation to use or not to use the stored data encryption function based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts setting operation to user or not to use connecting function of external authentication server (including connection setting parameter) based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts operations to start and stop shredding function based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE maintains and associate roles (security administrator, storage administrator, audit log administrator, maintenance personnel, and storage user). (FMT_SMR.1)

7.1.5 SF.HDD

[Satisfied requirements] FCS_CKM.1, FCS_CKM.4, FMT_MTD.1, FMT_MTD.3, and FDP_RIP.1

The TOE encrypts user data when storing it in a hard disk. For encryption and decryption, LSI embedded in DKA is used. The TOE creates encryption key for data encryption. Table 6-3 shows the algorithm for encryption key generation and Table 6-4 shows method to remove encryption key (FCS_CKM.1, FCS_CKM.4).

The TOE limits administrators who can perform operations for encryption key used for data encryption. Only security administrator can create, delete, backup (inquiry) and restore (inquiry and modification) the encryption keys (FMT_MTD.1).

The TOE can make backup of encryption key for data encryption in management PC. It also can restore the backup encryption key from the management PC to storage system. At the restoring, a hash value set in the backup data at the backup is verifies with a hash value of data to be restored. Only when the hash values are consistent, the encryption key can be restored. As the hash value contains serial number of the storage system, the encryption key can be restored only in the backed up storage system. (FMT_MTD.3)

The TOE shreds user data in LDEV which becomes disuse. (FDP_RIP.1)

7.1.6 SF.AUDIT

[Satisfied requirements] FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1, FAU_STG.3 and FAU_STG.4

The TOE has the following audit functions.

- When an audit issue related to the security function in the TOE occurs, an audit log is generated. The user ID of user account that causes each audit issue is added to the audit log. In addition, for the date used when the audit log is generated, the time managed by OS on SVP PC is used. Table 6-2 describes the audit information.
- There is no role which can modify and delete audit logs.
- Up to 250,000 lines audit logs can be created. When the number of audit logs exceeds the maximum, the oldest audit log is erased by returning to the line where the storing starts (wraparound method). When the number of audit logs goes over 175,000, a warning to indicate the exceedance is displayed on Storage Navigator window to persuade audit administrator to download the audit logs. If the audit logs are downloaded, the number of lines is reset and audit log starts at the first line.
- Only audit log administrator can download audit logs.
- Starting and ending audit function works in conjunction with TOE activation and termination.

The audit logs the TOE obtains consists of basic information and detailed information. Table 7-3 and Table 7-4 show contents of output basic information and detailed information respectively.

Table 7-3 Output content of basic information

<table>
<tr><th>No</th><th>Item</th><th>Description</th></tr>
<tr><td>1</td><td>Date</td><td>Date when issue occurs</td></tr>
<tr><td>2</td><td>Time</td><td>Time when issue occurs</td></tr>
<tr><td>3</td><td>Time zone</td><td>Time difference with GMT (Greenwich Mean Time)</td></tr>
<tr><td>4</td><td>User ID</td><td>Storage Navigator user ID</td></tr>
<tr><td>5</td><td>Function name</td><td>Character string indicates function which executes setting operation<table><tr><th>Function names</th></tr><tr><td>Name of function for identity authentication of Storage</td></tr></table></td></tr>
</table>

No	Item	Description	
			Navigator user and maintenance personnel
			Name of function to create, change and delete user account, to change password, and to change user group.
			Name of function to create and delete LU path information, to create, change and delete WWN and secret of host, and to change setting for host authentication by FC-SP.
			Name of function for host authentication by FC-SP.
			Name of function to enable and disable data encryption, to create, delete, backup and restore encryption keys.
			Name of function for shredding
6	Operation name or issue name	Abbreviation of operation name of each function	
			Operation names
			Identity authentication of Storage Navigator use and maintenance personnel
			User account creation
			User account change
			User account deletion
			User account password change
			Role addition to user group
			Role deletion from user group
			RSG number addition to user group
			RSG number deletion from user group
			Lu path information creation
			LU path information deletion
			Host WWN and secret creation
			Host WWN and secrete change
			Host WWN and secret deletion
			Setting change for host authentication by FC-SP
			Host authentication by FC-SP
			Setting to enable/disable data encryption
			Generation of encryption key for data encryption

No	Item	Description	
			Deletion of encryption key for data encryption
			Backup of encryption key for data encryption
			Restoring encryption key for data encryption
			Starting shredding
			Stopping shredding
7	Parameter	Parameter for executed setting operation	
8	Operation result	Operation result	
9	Identity information of source host	IP address of management PC or maintenance PC In case of host authentication by FC-SP, host WWN is output.	
10	Serial number of log information	Serial number of log information stored	

Table 7-4 Output content of detailed information

No	Audit issue	Detailed information
1	Identity authentication of Storage Navigator user	・ None
2	Identity authentication of maintenance personnel	・ None
3	Creation, modification, deletion of user account of Storage Navigator user and maintenance personnel	・ User ID of operation target, enable/disable setting information, authentication method, user group name, operation result (success or failure)
4	Password change of user account of Storage Navigator user and maintenance personnel	・ User ID of operation target, operation result (success or failure)
5	Change of user group where Storage Navigator user and maintenance personnel belong to	・ User ID of operation target, user group name, role, RSG number, operation result (success or failure)
6	Creation and deletion of LU path information	・ Port number, WWN, LU number, LDEV number
7	Creation, modification, deletion of host WWN and secret	・ Port number, host WWN, the number of hosts
8	Setting change of host authentication by FC-SP	・ Host WWN, whether to execute authentication, operation (change), operation result (success or failure)
9	Host authentication by FC-SP	・ None
10	Setting to enable/disable data encryption	・ Parity group number, setting to enable/disable encryption, operated encryption key number, the number of setting parity group
11	Generation, deletion, backup, and restoring of encryption key for data encryption	・ Encryption key number, the number of operated encryption keys
12	Start of stop shredding	・ Written data , the number of writing, target LDEV number, the number of target LDEVs, execution order or shredding processing

8 Reference

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

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

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

- Common Methodology for Information Technology Security Evaluation
Evaluation methodology July 2009 Version 3.1 Revision 3 Final
CCMB-2009-07-004

- Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model, July 2009, Version 3.1, Revision 3 Final
CCMB-2009-07-001, July 2009, Japanese translated version 1.0, December 2009,
Information-Technology Promotion Agency, Japan

- Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements, July 2009, Version3.1, Revision 3 Final
CCMB-2009-07-002, Japanese translated version 1.0, December 2009 Final
Information-Technology Promotion Agency, Japan

- Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements, July 2009, Version 3.1, Revision 3 Final
CCMB-2009-07-003 Japanese translated version 1.0 Final December 2009,
Information-Technology Promotion Agency, Japan

- Common Methodology for Information Technology Security Evaluation
Evaluation methodology July 2009, Version3.1 Revision 3, Final
CCMB-2009-07-004
Japanese translated version 1.0 Final December 2009
Information-Technology Promotion Agency, Japan

8.1.1 Terms and definitions

For CC terms used commonly, see CC Par1 Section 4.

8.1.1.1 Glossary for ST

Terms	Definition
Disk subsystem	Storage system such as Hitachi Virtual Storage Platform and Hitachi Virtual Storage Platform VP9500
Redundant Array of Independent Disks (RAID)	A technology which can recover damaged data by spreading or duplicating to multiple disk drives, improve the performance, and keep redundancy of data.— There are RAID0 (data striping), RAID 1 (disk mirroring) and RAID5 (data striping with distributed parity added) as commonly used raid types.
Storage Navigator	The program which provides GUI for storage system setting. It consists of Flex application and Java applet, works on SVP PC and management PC. It is used by Storage Navigator user and maintenance personnel.
Parity group	A group of hard disk drives to realize RAID system (see above). A parity group consists of multiple hard disk drives where user data and parity information are stored. The user data can be accessed even if one or more drive in the group becomes unavailable.
Fibre channel	High speed network technology to build Storage Area Network (SAN).
Fibre channel switch	A switch to connect each device of fibre channel interface. Using the fibre channel switch enables to build SAN (Storage Area Network) by connecting multiple host and storage systems in high speed.
LDEV	Abbreviation of logical device and a unit of volume created in a user area in storage system. It is also called as logical volume.
LDEV number	Unique number assigned to logical device at creation.
Logical unit (LU)	The LDEV used from a host of Open system is called LU. On the Open system fibre channel interface, access to LU mapped with one or more LDEV is enabled.
LU path	Data input/output channel connecting Open system host and LU.
LU number (LUN)	LDEV which is associated with fibre channel port and accessible from host. Or it is an address allocated to volume for Open system.
Port	The end of fibre channel. Each port is identified by port number.
Fibre Channel Security Protocol (FC-SP)	A protocol to execute authentication each other at communication between host or fibre channel switch and storage system. DH-CHAP with NULL DH Group authentication is used.

Terms	Definition
Host administrator	An administrator who manages hardware and software of host.
Connection setting parameter for external authentication server	A parameter to be set in SVP PC for identification and authentication by using external authentication server. It contains the following information. Type of external authentication server (LDAP, RADIUS), address of external authentication server, certificate of external authentication server, protocol (LDAPS, starttls, CHAP), and port number and so on.
starttls	A protocol to encrypt TCP session connecting with LDAP.
RADIUS	A protocol to realize authentication and accounting.
CHAP	A protocol to encrypt password to be sent from client to server at authentication.
DH-CHAP	A protocol used for FC-SP. It uses CHAP protocol for key exchange.

8.1.1.2 Abbreviation

In this document, the following abbreviations are used.

CACHE	CACHE memory
CC	Common Criteria
CHA	Channel Adapter
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
DKC	Disk Controller
EAL	Evaluation Assurance Level
FC-SP	Fibre Channel Security Protocol
HDD	Hard disk drive
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
LUN	Logical Unit Number

PC	Personal Computer
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SSL	Secure Sockets Layer
ST	Security Target
SVP	Service Processor
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
VSP	Virtual Storage Platform
WWN	World Wide Name