Hitachi Universal Storage Platform V
Security Target
Version 1.13

October 8, 2008

Hitachi, Ltd.

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

External Trademarks

Microsoft **and Windows are trademarks or registered trademarks of Microsoft Corporation, United States, in the** United States and/or other countries.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc, in the U.S. and other countries.

HP-UX is a registered trademark of Hewlett-Packard, United States.

RedHat is a trademark or registered trademark of RedHat, Inc., in the U.S. and other countries.

Linux **is a trademark or** registered trademark of Linus Torvalds in the U.S. and other countries.

AIX **is a trademark or** registered trademark of IBM Corporation.

All other product names and/or products names mentioned herein are the trademarks or registered trademarks of their respective owners.

- Contents -

List of Tables

List of Figures

1 ST Introduction

This chapter describes the Security Target (hereinafter referred to as “ST”), TOE, conformity for CC, configuration of ST, glossary, and the overview of this product.

1.1 ST Identification

TOE Identification:	Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program Version 60-02-32-00/00(R6-02A-14)
ST Identification:	Hitachi Universal Storage Platform V Security Target
ST Version:	1.13
ST Issued Date:	October 8, 2008
ST Development:	Hitachi, Ltd.
CC Identification:	Applied for Common Criteria for Information Technology Security Evaluation Version 2.3 Annex-0512

1.2 ST Overview

Hitachi Universal Storage Platform V (Hereinafter referred to as “USP V”. This product has another brand name for sale as “Hitachi Universal Storage Platform H24000”.) is an enterprise storage device of the large storage capacity, which realizes a multi-platform, high performance, high-speed response, with providing the performance of extensible connectivity, virtualization of the external storage, partitioning of the logical resources, disaster recovery function, and extendable disk capacity in an environment of different systems. Hitachi Universal Storage Platform VM (Hereinafter referred to as “USP VM”. This product has another brand name for sale as “Hitachi Universal Storage Platform H20000”.) is a rack-mounted type device which has the same functions of USP V except the extensibility of the disk capacity.

To a storage device, many hosts of various platforms will be connected via the SAN environment or the IP Network environment. If an incorrect operation is done in this storage device connection, it might have an unintended access for user data existing in the storage device. Therefore, the access control is required for the user data in the Storage device.

There is another concern if the setting might be done which exceeds one’s authorization in the condition of multiple storage administrators exist in the resource of the disk subsystem (Port, cache memory, disk etc.). Therefore, Hitachi Virtual Partition Manager function divide the port, cache memory, and disk (Parity group) into the multiple disk subsystems logically, and make it possible to arrange one administrator par partition. By giving one authorization to manage the allocated resource to one partition’s administrator, the each administrator can access the resource that managing without any influence to the other partition.

This ST describes the security functions to protect the integrity and confidentiality of user data on USP V and USP VM.

USP V and USP VM, evaluated with this ST version are manufactured and shipped by Disk Array Systems Division, Hitachi Ltd.

1.3 CC Conformance

Conformities of this ST are listed below.

- CC version 2.3[1] part 2
- CC version 2.3 part 3
- Package and EAL 2
- There is no conformable PP.

[1] Common Criteria (CC) August 2005, version 2.3, CCMB-2005-08-001, CCMB-2005-08-002, CCMB-2005-08-003.

1.4 Glossary

The definition of the CC terms, which is used commonly, are described in the CC part 1, section 2.3 of a following document.

- Common Criteria for Information Technology Security Evaluation

Part 1:Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

1.4.1 ST Technical Term

Terms	Explanations
Disk Subsystem	It means Storage Device and represents Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform VM etc.
Storage Logical Partition (SLPR)	It is a partition created by logically partitioned the cache and the hard disk drive in the storage device. More than one CLPR and more than one target port are allocated.
Cache Logical Partition (CLPR)	It is a partition created by logically partitioned the cache memory. More than one parity group is allocated in the CLPR.
Redundant Array of Independent Disks (RAID)	This is a way, to recover data quickly from the disk broken, to have good performance, and to keep redundancy of the data, by diffusing or duplicating the data to multiple disk drives. There are RAID 0 (Data striping), RAID 1 (DISK Mirroring), and RAID 5 (The striping which is added distributed parity) in the commonly used RAID type.
Parity Group (PG)	A group of hard disk drives to realize the RAID (see above). Parity group is consisted of the multiple hard disk drives where store user data and the parity information. It is possible to access to user data even if one or multiple hard disk drives in the group cannot use.
FC Storage Network	Network of the storage device using fibre channel.
Fibre Channel	High-speed network technology to build the Storage Area Network (SAN).
Fibre Channel Switch	A switch to connect various devices of the fibre channel interface mutually. Using this fibre channel switch enables to build SAN (Storage Area Network) by connecting multiple storage devices and hosts in high-speed.
LDEV	This is short for Logical Device. It is a unit of volume to be created in the user area in the storage device. It is also called as Logical Volume.

Terms	Explanations
Logical Unit (LU)	LDEV to be used from the host of open system is called LU. On the open system fibre channel interface, It is possible to access to LU which is mapped one or more than one LDEV.
LU Path	Data input/output channel, which connects a host for open system and LU.
Logical Unit Number (LUN)	This is LDEV that can be accessed from a host by associating with the fibre channel port. Or the address where the volume for the open system is allocated.
Port	The end of the fibre channel. Each port is identified by the port number.
Cache Memory	Tentative high-speed storage area of the data that is recently accessed or frequently accessed.
Fibre Channel Security Protocol (FC-SP)	This is a protocol to authenticate each device when communicating between the host or the fibre channel switch and the storage device. It uses the DH-CHAP with NULL DH Group for this authentication.

1.4.2 Reference

Here are abbreviations of the documents that are referred in this document.

[Abbreviation] Document Title

[SSLv3.0] “The SSL Protocol Version 3.0”,http://wp.netscape.com/eng/ssl3/draft302.txt

[TLSv1.0] “The TLS Protocol Version 1.0”,ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

1.4.3 Abbreviation

The following abbreviations are used in this document.

CC	Common Criteria
CHA	Channel Adapter
CLPR	Cache Logical Partition
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
DKC	Disk Controller
EAL	Evaluation Assurance Level
FC-SP	Fibre Channel Security Protocols

HDD	Hard disk drive
JRE	Java Runtime Environment
LAN	Local Area Network
LDEV	Logical Device
LU	Logical unit
LUN	Logical Unit Number
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SLPR	Storage Logical Partition
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
SVP	Service Processor
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
USP V	Universal Storage Platform V
USP VM	Universal Storage Platform VM
VPM	Virtual Partition Manager
WWN	World Wide Name

2 TOE Description

This chapter defines the classification, the range and the boundary of TOE, and provides the general information of TOE.

2.1 TOE Classification

TOE, namely the control program for USP V and USP VM, version 60-02-32-00/00(R6-02A-14) is the software program operating on the storage devices produced by Hitach Ltd., “Hitachi Universal Storage Platform V”, “Hitachi Universal Storage Platform H24000”, “Hitachi Universal Storage Platform VM”, and “Hitachi Universal Storage Platform H20000”. The above-described storage devices are, though they are different in scale as hardware, all use the same control program.

The control program is consisted of “DKCMAIN Micro program”, “SVP program” and “Storage Navigator program”.

DKCMAIN Micro program is loaded on multiple boards in the storage device, and has the role of controlling data transmission between the host connected to the storage device and the storage device. SVP program is a program to execute the operation and maintenance of the storage device, and the Storage Navigator Program provides the user interface function of the SVP program.

This TOE provides the function of protecting the storage device which is allocated for the specific storage user from the illegal access of the other storage user.

2.2 General Configuration of the System including the Storage Device

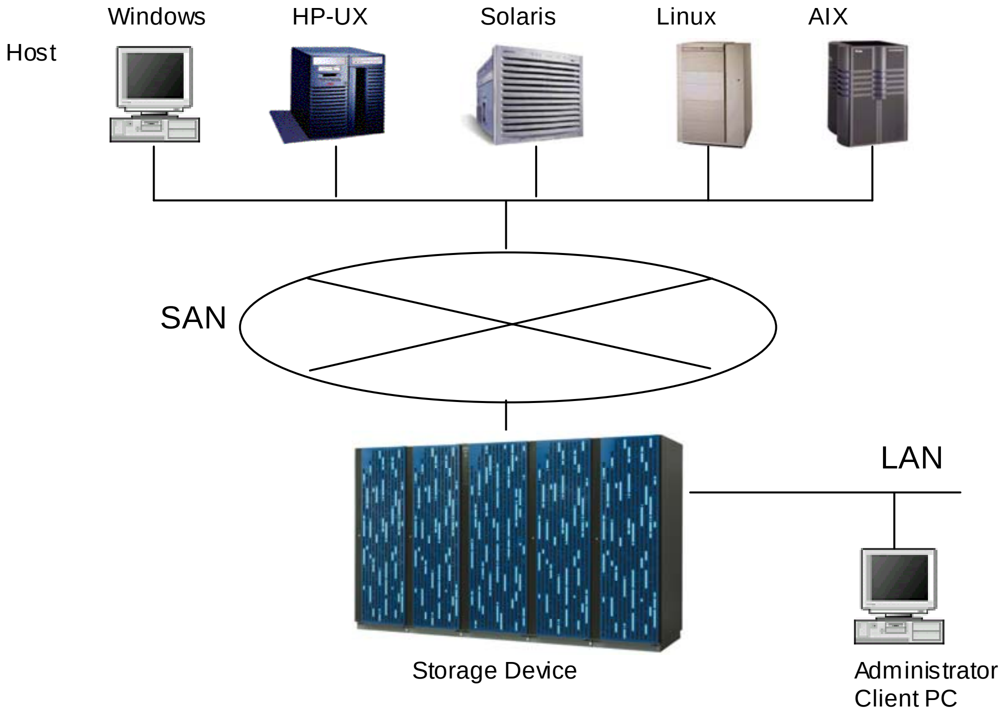

Figure 2.1 General Configuration of the System including the Storage Device

Figure 2.1 illustrates the general configuration of the system including the storage device, and the descriptions are in the following.

(1) Storage device

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

(2) SAN and Host

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

To connect a host to SAN, it is required to install the Fibre Channel Connection Adapter (hardware and software) to the host. The storage device identifies the host with the identification information in the Fibre Channel Connection Adapter.

Since the connection control is executed in the host on the operation of the customers, this ST does not have any countermeasure against a high-assault capability such as accessing to the unauthorized user data in the storage device by re-organizing the identification information of the host. However, if the customer requests to have a function of a storage device, to prevent the re-organization of host identification information, as their policy, TOE can execute authentication process on the host or the fibre channel switch which are connected to the storage device.

(3) Administrator Client PC

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

2.3 TOE and Storage Device

Figure 2.2 illustrates the hardware members which consist of storage device, and shows that where in the component part the identified TOE subset works.

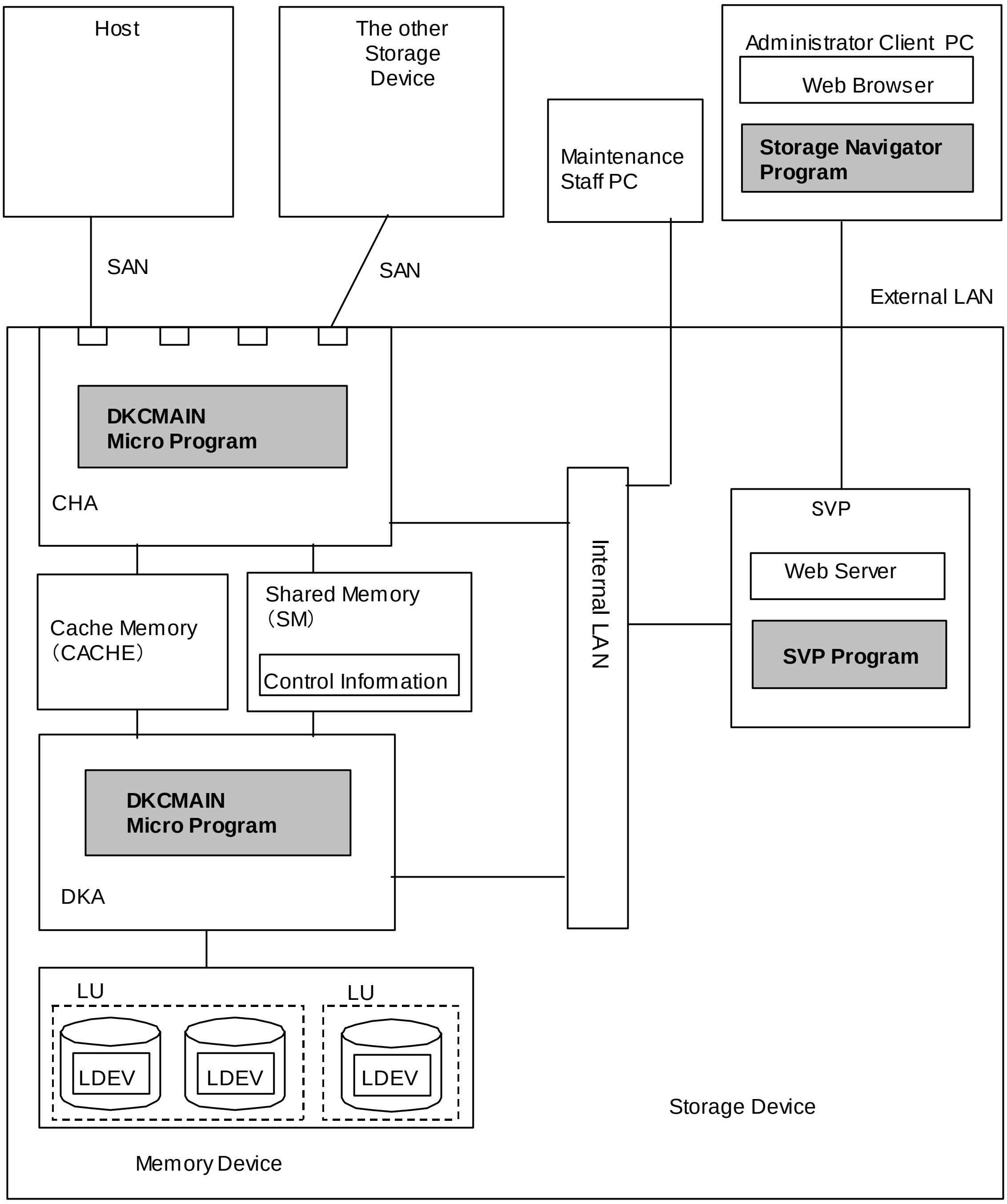

Figure 2.2 Storage Device Configuration

A storage device can be divided into the control system that includes Channel Adapter (CHA), Shared Memory (SM), Cache Memory (CACHE), Disk Adapter (DKA) and Memory Device, and the administration system that includes SVP (Service Processor). The control system controls data input and output to and from the disk, and the administration system maintains and manages the storage device. Each of these components is described below:

2.3.1 Control System

(1) Channel Adapter

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

(2) Disk Adapter

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

(3) Cache Memory

Cache Memory (CACHE) is located between CHA and DKA, used for data Read/Write.

(4) Shared Memory

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

(5) Memory Device

Memory Device consists of multiple hard disks, in which user data is recorded. In the memory device, an LDEV (Logical Device) which is the volume to store user data is created. Access to user data is controlled by the unit of LDEV, and executed via DKCMAIN microprogram. A part of or the entire of data in the LDEV can be given out to the cache Memory. By giving it to the cache memory, the high-speed accessing of data becomes available.
LU (logical unit) is a unit of accessing from the host, and It mapped to one or more than one multiple LDEV.

LDEV is created on the parity group which is composed in the memory device. The parity group is a series of hard disk drives which is handled as one data group, and composes RAID by storing the user data and the parity information. With this configuration of RAID, it can access to the user data even if one or more than one drive in the parity group is not available to operate, and improves the reliability.

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

2.3.2 Administration System

(1) SVP

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

(2) Maintenance Staff PC

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

(3) Administrator client PC

Administrator client PC is a customer’s PC used by a user of Customer’s Storage Navigator (see section 2.4) for the operation and the maintenance work of the storage device, and it works the Storage Navigator program, which is a part of TOE. The administrator client PC and the SVP is connected via the external LAN.

(4) Storage Navigator Program

Storage Navigator program is software used by a user of customer’s Storage Navigator (see section 2.4) to manage the device control information on the storage device. Hereinafter, Storage Navigator program is called just “Storage Navigator”.

Storage Navigator is a Java applet program, which is downloaded from the SVP to the administrator client PC to work on the Web Browser. The communication between SVP and Storage Navigator uses SSL. Storage Navigator user handles the setting operation of the storage device by interacting with Storage Navigator through the Web browser of the Administrator client PC.

And, to prevent illegal use of Storage Navigator by any malicious third person (see section 3.2), Storage Navigator executes the identity authentication in cooperation with the SVP program.

(5) The Other Storage Device

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

The control series network (CHA, SM, CACHE and DKA connected together by the high-speed crossbar switch) and the administration network (internal LAN and external LAN) are completely independent of each other. This configuration does not allow direct access from the SVP, Administrator client PC and Maintenance Staff PC connected either to the internal LAN or the external LAN, to SM, CACHE and Memory Device. Thus the user data is completely protected from attack via the administration series network.

Note that the equipments embedded in the storage device are factory-installed, and a customer of Storage Navigator or a Storage user (see section 2.4) will not prepare or change any of them by themselves.

2.3.3 TOE Range

2.3.3.1 Logical Boundary

This section describes the component of product's hardware and software, and shows which one is included in TOE or the operating environment respectively.

2.3.3.1.1 Hardware's Component

The following table lists the component of the necessary hardware and shows if the each one of them is included in the TOE.

TOE or Environment	**Components**	**Descriptions**
Environment	Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000	USP V hardware. This includes the SVP hardware. The difference between these models is branding of the external racks. The numbers of HDDs and the number of racks required can vary depending on the specific configuration ordered by customers.
Environment	Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H20000	USP VM Hardware. This includes the SVP hardware. The difference between these models is branding of the external racks. The numbers of HDDs and the number of racks required can vary depending on the specific configuration ordered by customers.
Environment	Host computers	Computers accessing the storage array.
Environment	Administrator Client PC	Computers used to administer the TOE. Requirements of computers for running are: • CPU: Pentium 4, Equal to 2.4 GHz or better; Recommended: Pentium 4, 3 GHz or better • RAM: 512 MB or more; Recommended: 1 GB or more • Available HDD space: 150 MB or more • Monitor: High-Color 16-bit or better; Resolution: 1024x768 or better • Ethernet LAN card: 100Base-T
Environment	FC storage network	Network of the storage device using fibre channel.

2.3.3.1.2 Software's Component

This table identifies the required software components and indicates whether or not each component is in the TOE.

TOE or Environment	**Components**	**Explanations**
TOE	DKCMAIN microprogram version 60-02-32-00/00	It works with CHA and DKA.
TOE	SVP software Version 60-02-26/00	It includes the SVP software running on the SVP and the Storage Navigator running on the administrator client PC.
Environment	Web Server	It running on the SVP. It uses the following software. • Apache 2.2.4
Environment	Administrator Client computer(s) OS	The computer must be running on the following OS. • Windows XP (SP2 or later version)
Environment	Web Browser	Web browser running on the administrator client PC. Supported browser • Internet Explorer 6.0 SP2
Environment	Java Runtime Environment	Java runtime environment running on the administrator client PC. JRE 1.5.0_06

2.4 Storage Device User

This ST assumes the following users as those concerned with the storage device. When building the system, the initial account is built in the TOE. The initial account has the authorization of “The Account Administrator” described in the following. There is no other administrator other than this.

- The account administrator:

  The account administrator can execute registration, modification, and deletion of an account which is related to the operation of Storage Navigator by the Administrator (Storage administrators, storage partition administrators, account administrators, account partition administrators and audit log administrators).

- The storage administrator:

  The storage administrator has the control competence of the entire storage system.

  The storage administrator can divide the resources of the storage device (port, cache memory, and LDEV) into logical partitions with the Virtual Partition Manager function (see section 2.6.1 for more details).

  On the divided logical partition, the managing of the virtual disk subsystem (see section 2.6.1 for more details), which will not have any influence from the existing of the other logical partition, becomes available by registering the storage partition administrator and account partition administrator whom controls LU that are visible from the host.

  In the virtual disk subsystem, an account partition administrator is set to operate the account management operations from the Storage Navigator in the range of logical partition, when the storage partition administrator wants to set the other storage administrator, or to delete that administrative authority.

- The storage partition administrator:

  The storage partition administrator is the administrator who can manage the resources (port, cache memory, LDEV) in the logical partition assigned by the storage administrator, and associates between WWN, an identification information of the host, and LDEV number that permits the access.

- The account partition administrator:

  The account partition administrator is an administrator who can manage the divided logical partition.

  The account partition administrator can execute registration, modification, and deletion of the accounts for the storage partition administrator and the account partition administrator with the Storage Navigator.

- Audit log administrator:

  The Audit log administrator is an administrator who can manage the audit log acquiring from the storage device. The Audit log administrator can refer or download the audit log or the set related to syslog, with the Storage Navigator on the administrator client PC.

- Maintenance staff

  Maintenance staff is the staff of the special organization for maintenance with whom the customer who uses the storage device has signed a contract concerning maintenance. Manages the initial startup process in installing the storage device, changing the settings required in maintenance operations such as replacement or addition of parts or disaster recovery. Maintenance staff may execute the setting operations of the storage administrator, the storage partition administrator, the account administrator, the account partition administrator and audit log in their place. Maintenance staff access SVP from the maintenance staff PC, and executes maintenance operations. Only maintenance staff can directly contact the equipments inside the storage device and manipulate the equipments connected to internal LAN. TOE recognizes that the maintenance staff uses the interface to access SVP with the maintenance staff PC as his/her role.

- Storage User:

  Storage device user (represents Host) who uses the data saved in the storage device through the host connected to the storage device.

Hereinafter, the storage administrator, the storage partition administrator, the account administrator, the account partition administrator, and the audit log administrator are totally called as the users of Storage Navigator.

2.5 Property To Be Protected

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

In this ST, on the environment of existing the logical partitions that are divided into several pieces, the user data of the storage user existed in the LDEV in each partition is the property to be protected. So the property to be protected must be protected from the unauthorized access by the storage user. And it prevents the deletion of the property to be protected by the storage partition administrator whom does not have an authorization to the area that identified by the logical partition.

2.6 TOE Functions

The overview of IT functions provided by TOE and the overview of the data security function of the storage device are described below:

2.6.1 The Outline of Virtual Partition Manager Functions

USP V and USP VM disk subsystem can share in the multiple organizations (i.e. multiple enterprises or multiple departments within one enterprise). Therefore, some administrators from the different organizations may exist in one disk subsystem. In such circumstance, it may have a concern that the whole of disk subsystem becomes complicate and difficult to manage if an administrator broke the volume of the other organization, or executed inappropriate operation influenced to the other organization.

The storage control split function of the Virtual Partition Manager (VPM function) divides the resource of one whole disk subsystem (port, cache memory and LDEV) into the multiple virtual disk subsystems and each one of administrator of the virtual disk subsystem can only access to the respective virtual disk subsystem. Therefore, it is available to protect from breaking volume of other organization or from leaking the data of one specific organization. Figure 2.3 shows the Overview of the Virtual Disk Subsystem. In the Figure 2.3, the resource is allocated by dividing one disk subsystem into 2 virtual disk subsystems.

The virtual disk subsystem created by dividing the disk subsystem is called as Storage Logical partition (SLPR). SLPR is identified by numbering the SLPR number. SLPR number is given to the SLPR to identify the divided resource for allocating the divided resource of TOE to a specific virtual disk subsystem. The storage partition administrator allocated in each virtual disk subsystem has the operation authorization for the allocated resource of the SLPR which is specified by the SLPR number to be managed.

And the VPM function can divide the cache memory in the disk subsystem into the multiple virtual cache memories. With this operation, the usable cache capacity can be allocated in the host in advance, and enables to prevent the much occupation of the cache memory by the specific host. This divided virtual cache memory is called “CLPR (Cache Logical Partition)”.

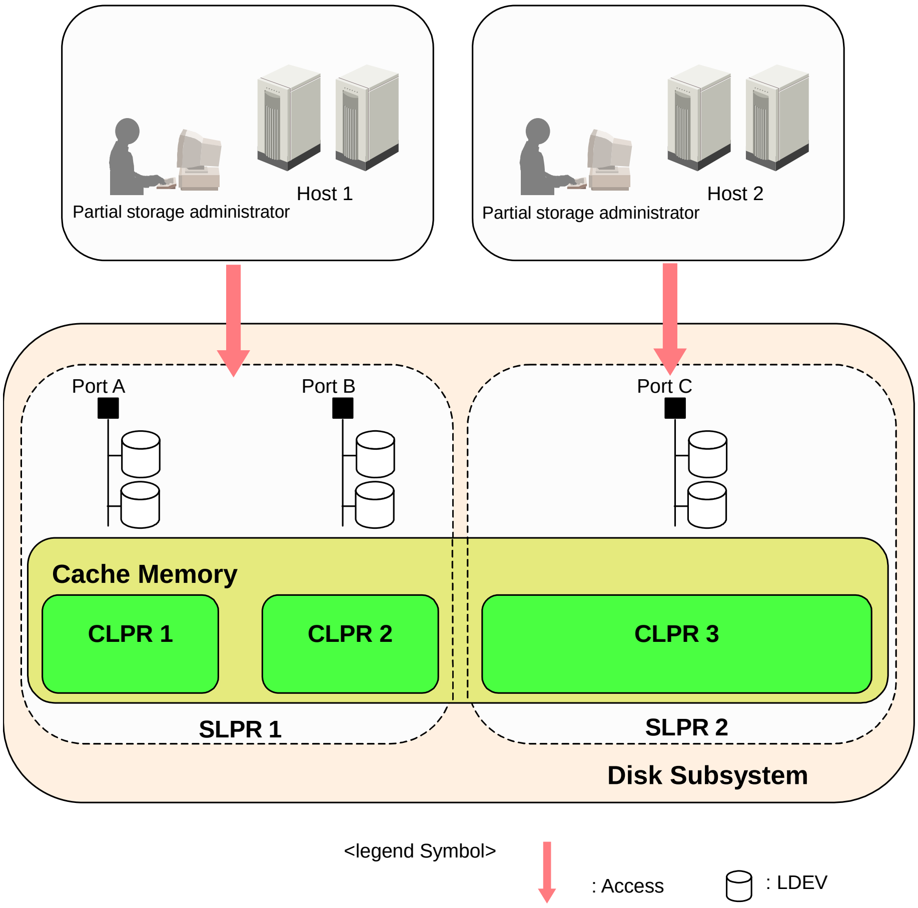

Figure 2.3 Overview of the Virtual Disk Subsystem

2.6.2 Security Function provided by TOE

2.6.2.1 Access Control for LDEV

2.6.2.1.1 LUN Manager Function

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

2.6.2.1.2 Virtual Partition Manager Function

A storage partition administrator of the virtual disk subsystem cannot access to the virtual disk subsystem other than the one own controlled. Therefore, it enables to protect the data broken or data leakage by a storage partition administrator of the other virtual disk subsystem.

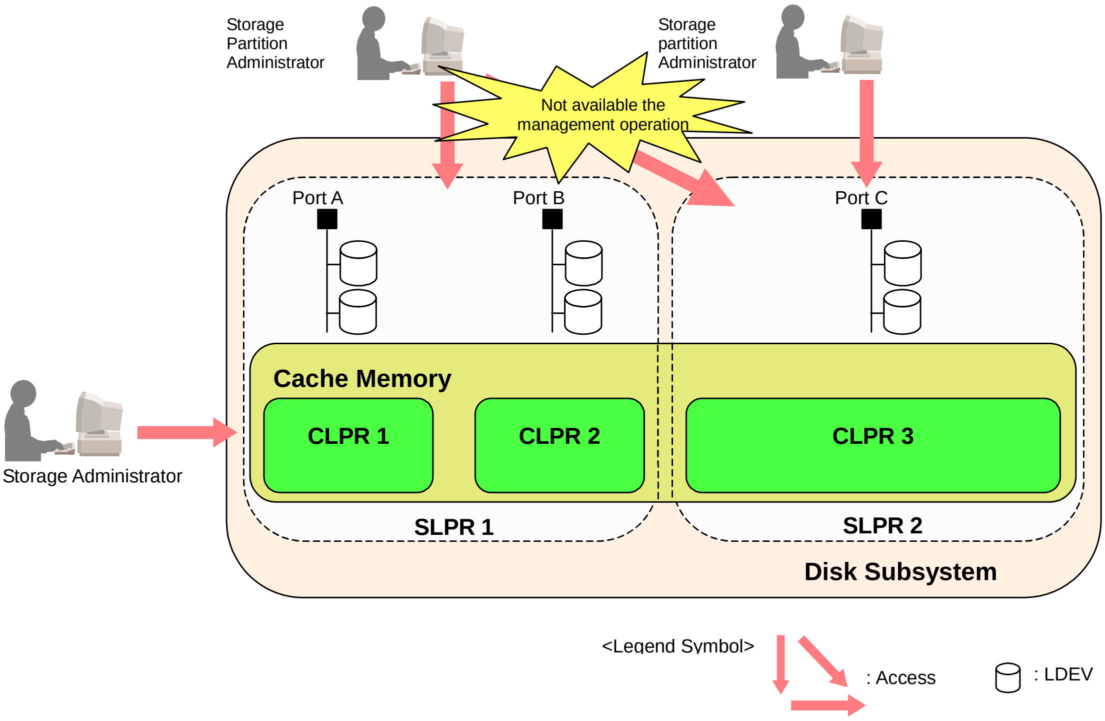

Figure 2.4 Operation Range of the Storage Administrator and the Storage Partition Administrator

2.6.2.2 Function of Identifying and authenticating of the Host

When connecting the host to SAN, the connection control is done in the customer side's operation to prevent the illegal host connection. If the customer requests the countermeasure to prevent the impersonation of the illegal host, ensuring more of safety as their policy, the authentication by the FC-SP function can be done on the connection between the host or the fibre channel switch and the port of disk subsystem. The port of disk subsystem can authenticate the fibre channel switch or the host, and can give the authentication of the port of disk subsystem to these switch hosts. The storage administrator or the storage partition administrator set to the each host whether to give the authentication of host or not, with the operation of LUN Manager. The host that executes authentication registers the user information (WWN and secret). The secret is a password for the authentication and available to mix the alphanumeric characters and symbols from 12 to 32 letters.

2.6.2.3 Function of Authentication of User by the Storage Navigator

Storage Navigator is used to manage the disk subsystem including the security function setting by the user of customer's Storage Navigator. When managing the disk subsystem (the configuration of each function or the setting change etc.), the user identification and authentication are done by the TOE. When using the Storage Navigator, the identity authentication is done with the user ID and password.

The password entry is available from 6 to 256 letters, mixed in alphanumeric characters and symbols, and the entered password displays in "*". If more than 3 times identity authentication are failed, the authentication of that user is denied for one minute.

2.6.2.4 Storage Navigator - Encrypted Communication with SVP

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

2.6.2.5 Authorization Control of the Administrator

User account, which is used at the authentication on the Storage Navigator, includes the information of the type of user and the operating authorization.

There are 2 types in the user: the administrator and the partition administrator. The administrator is a kind that can manage the whole USP V/USP VM. And the partition administrator is a kind that can manage the allocated logical partition (the logical partition is identified by the SLPR number.)

The operating authorization is also called as "Role", and there are 3 types in the role: the account administrator role, the audit log administrator role, and the storage administrator role. The account administrator role can display, create, modify or delete the user account with the account managing function. When creating an account, the account administrator role gives the type of user, Operating Authorization and SLPR number to that account. When the administrator creates the user account of a partition administrator, the administrator make an account by specifying the SLPR number to be allocated to the partition administrator. The partition administrator cannot change the allocated SLPR number.

The audit log administrator role is an operating authorization that can give a type of user to the administrator, and it enables to refer or download the audit log and to set related to the syslog.

Storage administrator role can set and manage the storage resource.

The definition of the operating authorization defines which role is given in each user account. The account administrator role and the audit log administrator role enables to define the disable, view, and modify authorization. And the storage administrator role enables to define the disable and enable authorization in each function of program product.

The administrator and the partition administrator are assigned the following roles.

- Newly creation, modification and deletion of a user account as an account administrator's role.
- The account administrator can determine the authorization of the storage administrator.
- There are 2 kind of account administrator existing by the type of user: the account administrator, and the account partition administrator who can manage an account in the operable range (logical partition).
- The account administrator can determine the operable range of the storage administrator.
- The account administrator and the storage administrator who are set by the account partition administrator are inherited the operable range.
- The storage administrator can manage the disk subsystem with using Storage Navigator as one of his/her role.
- There are 2 kinds of storage administrator: the storage administrator, and the storage partition administrator who can execute storage management in its operable range.

- The storage administrator can set the creation and deletion of LDEV, and set the LU path information in a whole of the storage device.
- The storage partition administrator can set the creation and deletion of LDEV, and set the LU path information in his/her operable range.
- The audit log administrator can download and refer the audit log as a role of Audit log administrator.

2.6.2.6 Audit log

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

The maximum number of letters in 1 line of Audit log is 512 (single byte), and maximum 250,000 lines information is stored in the SVP's HDD. Storage Navigator provides the interface that referring the audit log.

3 TOE Security Environment

This chapter defines the use environment and usages of TOE that are intended by this ST, the properties to be protected and the threats against them, and the security policy of the organization that TOE should follow.

3.1 Assumptions

A.NOEVIL Within the users of Storage Navigator, the storage administrator, the account administrator and the audit log administrator are assumed to be trusted as the person who have sufficient skills to execute the administration and operation of a whole storage device, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.

The storage partition administrator and the account partition administrator are assumed to be trusted as the person who have sufficient skills to execute the administration and operation within the area where approved by the administrator who has the authorization, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.

A.NOEVIL_MNT Maintenance staff is assumed to be trusted as the person who has the sufficient skills to safely execute the general maintenance operations of the storage device, including the connecting operations between the host and the port on CHA, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.

A.PHYSICAL_SEC A storage device is assumed to be set at a secure area where only the storage administrator, the account administrator, the audit log administrator and the maintenance staff are allowed to enter and exit, and the device is completely protected from any unauthorized physical access.

A.ILLEGAL_SOFT The administrator client PC is assumed to be never installed illegal software.

A.CONNECT_STORAGE

TOE has a function that acquiring the data copy or the backup copy of the data between the storage devices by connecting the other storage devices. Once this function is used, the modifying or browsing of the user data which is the property to be protected of TOE becomes available. The operations of these functions are assumed to be done by the reliable storage administrator only.

3.2 Threats

TOE or IT environment pits against the following threats listed below. Note that “a third person” in the following description indicates the person who is not a storage navigator user, a storage user nor a maintenance staff, and is not authorized to use the storage device.

In addition, the attack capability of the attacker is assumed to be “Low”.

T.ILLEGAL_XCNTL Within the users of storage Navigator, a storage partition administrator or an account partition administrator might be able to access to LDEV where the host is not authorized, by chaining the setting of the storage device where beyond the own authorization.

T.TSF_COMP A third person might make illegal connection on the channel between Storage Navigator and SVP on the purpose of sniffing or falsification of the data.

T.LP_LEAK The leakage or falsification of the data might be done if a third person such as a host device administrator accesses to LDEV by connecting the unauthorized host to SAN.

T.CHG_CONFIG A third person might change the setting of storage device with using the Storage Navigator.

3.3 Organizational Security Policies

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

4 Security Objectives

This chapter defines the security policy related to TOE and its operating environment.

4.1 Security Objectives for the TOE

The security policy of TOE is described below.

O.ADM_AUTH

The TOE must succeed the identity authentication of a user of Storage Navigator before the user executes the management operations of the disk subsystem.

O.ADM_ROLE

The TOE must control the management operations which are done by the user of Storage Navigator as the following.

- The account administrator enables to execute the account management operations for the whole device.
- The storage administrator enables to execute the storage management operations for the whole device.
- The storage partition administrator enables to execute the storage management operations within the authorized logical partition.
- The account partition administrator enables to execute the account management operations within the authorized logical partition.

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, to protect from sniffing or falsification of the data on the communication route.

O.HOST_AUTH

The TOE must execute identity authentication of the host if the host requests the connection.

O.HOST_ACCESS

TOE must control the identified host to access only to the authorized LDEV.

O.AUD_GEN

TOE must able to track the event regarding the security such as identity authentication or the setting change operation.

4.2 Security Objectives for the Environment

The security objectives for the environment are described below.

OE.NOEVIL Within the users of Storage Navigator, the storage administrator, the account administrator and the audit log administrator must be allocated the person who are trusted to have the sufficient ability to execute the administration and operation of a whole storage device, to execute the proper operations as specified by the manual, and never commits any inappropriate behavior.

The storage partition administrator and the account partition administrator must be allocated the person who are trusted to have the sufficient ability to execute the administration and operation of the storage device within the authorized area by the person who has that authorization, to execute the operations exactly as specified by the manual by gaining the on-the-job training, and never to commit any inappropriate behavior.

OE.NOEVIL-MNT A maintenance staff must be allocated the person who is trusted to have the sufficient skills to safely execute the general maintenance operations of the storage device, including the connecting operations between the host and the port on CHA, to execute the proper operations as specified by the manual, and never to commit any inappropriate behavior.

OE.PHYSICAL_SEC A storage device must be set at a secure area where only the storage administrator, the account administrator, the audit log administrator and the maintenance staff are allowed to enter and exit, and the device must be completely protected from any unauthorized physical access.

OE.ILLEGAL_SOFT The administrator client PC shall not be installed any illegal software.

OE.CONNECT_STORAGE

The other storage devices connected to TOE must be the one that is constructed with TOE so that only the reliable storage administrator can execute the operation of remote copy to the other storage device and of backup.

5 IT Security Requirements

The security requirements that are levied on the TOE are specified in this section. The security functional requirements are defined in section 5.1. There are no security functional requirements levied on the IT environment.

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

All the following components are included in CC Part 2.

Notation system on the operation of functional requirements (Selection, Assignment, detailed) is described below.

When choosing: [selection: *Description of functional requirements*]: Chosen contents.
When assigning: [assignment: *Description of functional requirements*]: Assigned contents.
When detailing: [detailed: Description of functional requirements]: Detailed contents.

And the letters on the last of duplicated defined functional securities specify the following contents.

a: Authentication function of Storage Navigator.

b: Access control function of LUN Manager.

FIA_ATD.1a User attribute definition

Hierarchical to: No other components.

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*]. User type, operating authority, SLPR number

Dependencies: No dependencies.

FIA_USB.1a User-subject binding

Hierarchical to: No other components.

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*]: User type, operating authority, SLPR number [assignment: *rules for the initial association of attributes*]: None

[assignment: *rules for the changing of attributes*]: None

Dependencies: FIA_ATD.1 User attribute definition

FIA_ATD.1b User attribute definition

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FIA_USB.1b User-subject binding

Hierarchical to: No other components.

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: *rules for the initial association of attributes*]: None

[assignment: *rules for the changing of attributes*]: None

Dependencies: FIA_ATD.1 User attribute definition

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

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 met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of authentication events*]: Authentication by Storage Navigator

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

[assignment: *list of actions*]: Deny the corresponding user’s login for one minute. Then, reset the number of unsuccessful authentication attempts.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1a Verification of secrets

Hierarchical to: No other components.

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*]: From 6 to 256 single byte uppercase and lowercase English letters, Single byte numeric values, and the following 32 kinds of symbolic codes: !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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.

[Detailed: User]: Users of Storage Navigator, Maintenance staffs

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]: Display the numbers of [*] for entered characters.

[Detailed: User]: Users of Storage Navigator

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

[Detailed: User]: Users of Storage Navigator, Maintenance staffs, hosts

Dependencies: No dependencies.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FIA_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, Information flow control SFP*] 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 authorized identified roles*].

[assignment: *list of security attributes*]: LU path information, Logical partition information, user authority information.

[selection: *change_default, query, modify, delete, [assignment: other operations]*]:
"Operation for the LU Path information " on Table 5.1and 5.2,
"Operation for the Logical partition Information" on Table 5.3,
"Operation for the User authority information" on Table 5.4 and 5.5.

[assignment: *the authorized identified roles*]: Roles described in the "Role" on Table 5.1, 5.2, 5.3, 5.4, and 5.5.

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

Table 5.1 Operation of the Administrators for the Security Attributes of the Process on behalf of the Host

Roles	Operations for the LU path information		
	WWN	LU number	LDEV number
Storage administrators	query, modify, create, delete	query, create, delete	query, create, delete
Account administrators	–	–	–
Audit log administrators	–	–	–

–: No operation

Table 5.2 Operation of the Partition Administrator for the Security Attribute of the Process on behalf of the Host

Roles	Operations for the LU path information					
	SLPR number of the logical partition=n			SLPR number of the logical partition≠n		
	WWN	LU number	LDEV number	WWN	LU number	LDEV number
Storage partition administrators (Own SLPR number = n)	query, modify, create, delete	query, create, delete	query, create, delete	–	–	–
Account partition Administrators (Own SLPR number = n)	–	–	–	–	–	–

–: No operation

Table 5.3 Operation for the Security Attribute (Logical Partition Information) of the Process on behalf of Storage Navigator

Roles	Operations for the logical partition information
	SLPR number
Storage administrators	Query, create, delete
Account administrators	–
Audit log administrators	–
Storage partition administrators	Query for the SLPR number of the logical partition that matches with the SLPR number of own account.
Account partition administrators	–

–: No operation

Table 5.4 Operation of the Administrator for the Security Attribute (user authority information) of the Process on behalf of Storage Navigator

Roles	Operations for the user authority information		
	User type	Operation authority	SLPR number
Account administrators	Setup, query	Setup, query, modify	Setup, query
Storage administrators	Query (to own)	Query (to own)	Query (to own)
Audit log administrators	Query (to own)	Query (to own)	Query (to own)

Table 5.5 Operation of the Partition Administrator for the Security Attribute (User Authority Information) of the Process on behalf of Storage Navigator

Roles	Operations for the user authority information					
	SLPR number of the operating target account =n			SLPR number of the operating target account ≠n		
	User type	Operating authority	SPLR number	User type	Operating authority	SPLR number
Account partition administrators (Own SLPR number = n)	Setup, query	Setup, query, modification	Setup, query	–	–	–
Storage partition administrators (Own SLPR number = n)	Query (to own)	Query (to own)	Query (to own)	–	–	–

–: No operation

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security management roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FIA_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.

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

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

[Assignment*: other property*]: None

[assignment: *access control SFP, Information flow control SFP*]: LM access control SFP.

[assignment: *the authorized identified roles*]: It describes in “Role” on Table 5.6.

Table 5.6 Initial Value Specified Range of the Storage Administrator and Storage Partition Administrator

Roles	Available range of initial values
Storage administrators	LU path information can be set for all the LDEVs in the storage device, when they are created.
Storage partition administrators (Own SLPR number = n)	LU path information can be set for LDEVs that are associated with SLPR number =n of the logical partition in the storage device, when LDEVs are created.

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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 authorized identified roles*].

[assignment: *list of TSF data*]: User ID of Storage Navigator user, password, WWN of the host, secret

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: Operation for the “User account” on Table 5.7 and Table 5.8, Operation for the user name and password of the remote desktop connection on Table 5.9, Operation for the “Host identity authentication data” on Table 5.10 and Table 5.11.

[assignment: *the authorized identified roles*]: Roles described in “Role” on Table 5.7, 5.8, 5.9, 5.10, and 5.11.

Table 5.7 Operation of the Administrators for the User Account

Roles	User accounts	
	Storage Navigator User ID	Storage Navigator password
Account administrators	Query, create, delete	Modify
Storage administrators	Query (to own)	Modify (own)
Audit log administrators	Query (to own)	Modify (own)

Table 5.8 Operation of the Partition Administrator for the User Account

Roles	User accounts			
	SLPR number of the operating target account =n		SLPR number of the operating target account ≠n	
	Storage Navigator User ID	Storage Navigator password	Storage Navigator User ID	Storage Navigator password
Account Partition Administrators (Own SLPR number = n)	Query, create, delete	Modify	–	–
Storage partition Administrators (Own SLPR number = n)	Query (to own)	Modify (own)	–	–

–: No operation

Table 5.9 Operation for the User ID and Password of the Remote Desktop Connection

Roles	Remote Desktop connections	
	User name	Password
Maintenance staffs	Query, modify	Modify

–: No operation

Table 5.10 Operation of the Administrators for the Host Identity Authentication Data

Role	User accounts	
	WWN of the host	Secret of the host
Storage administrators	Query, create, modify, delete	Create, modify, delete
Account administrators	–	–
Audit log administrators	–	–

–: No operation

Table 5.11 Operation of the Partition Administrator for the Host Identity Authentication Data

Role	Host identity authentication data			
	SLPR number of the logical partition =n		SLPR number of the logical partition ≠n	
	WWN of the host	Secret of the host	WWN of the host	Secret of the host
Storage Partition Administrators (Own SLPR number = n)	Query, create, modify, delete	Create, modify, delete	–	–
Account Partition Administrators (Own SLPR number = n)	–	–	–	–

–: No operation

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

[assignment: *list of security management functions to be provided by the TSF*]: The security management function describes in “management function” on Table 5.12.

Table 5.12 List of Security Management Functions Provided by the TSF

Required Functions	Management functions	Items to be managed
FIA_ATD.1a	a) If so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	a) None.
FIA_USB.1a	a) An authorized administrator can define default subject security attributes. b) An authorized administrator can change subject security attributes.	a) None. User types, operating authorizations, and SLPR numbers are always fixed. b) None. User types, operating authorizations, and SLPR numbers are always fixed.
FIA_ATD.1b	a) If so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	a) None.
FIA_USB.1b	a) An authorized administrator can define default subject security attributes. b) An authorized administrator can change subject security attributes.	a) None. WWN and LU numbers are always fixed. b) None. WWN and LU numbers are always fixed.
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.	a) None. The threshold values are always fixed. b) None. The actions are always fixed.
FIA_SOS.1a	a) The management of the metric used to verify the secrets.	a) None. The metric is always fixed.
FIA_UAU.2	a) Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	a) Manage the password for the user account’s user ID. Manage the password for the user account’s user ID of the remote desktop.
FIA_UAU.7	–	–

Required Functions	Management functions	Items to be managed
FIA_UID.2	a) The management of user identities.	a) Manage the user account's User ID, the user name of the Remote desktop connection, and the Host identity (WWN of the host).
FMT_MSA.1	a) Managing the group of roles that can interact with the security attributes.	a) None. Roles area always fixed.
FMT_MSA.3	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP.	a) None. Roles are always fixed. b) None. Always fixed.
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	a) None. Roles area always fixed.
FMT_SMF.1	–	–
FMT_SMR.1	a) Managing the group of users that are part of a role.	a) Manage the user account's user type and the operating authority.
FCS_COP.1	–	–
FCS_CKM.1	a) The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	a) None.
FCS_CKM.2	a) The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	a) None.

Required Functions	Management functions	Items to be managed
FCS_CKM.4	a) The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	a) None.
FIA_SOS.1b	a) The management of the metric used to verify the secrets.	a) None. The metric is always fixed.
FIA_UAU.1	a) Management of authentication data by an administrator; b) Management of the authentication data by the associated user; Managing the list of actions that can be taken before the user is authenticated.	a) Manage the authentication data of the host with the FC-SP function of Storage Navigator. b) None.
FIA_UAU.5	a) The management of authentication mechanisms; b) The management of rules for authentication.	a) None. The mechanisms are always fixed. b) None. Rules are always fixed.
FMT_MOF.1	a) Managing the group of roles that can interact with the functions in the TSF;	a) None. Roles are always fixed.
FDP_ACC.1	–	–
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	a) None. There is no explicit access or deny.
FAU_GEN.1	–	–
FAU_GEN.2	–	–
FPT_STM.1	a) Management of the time.	a) None. (The time is not managed as TOE, but as the OS.)

Required Functions	Management functions	Items to be managed
FAU_SAR.1	a) Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	a) None. Roles are always fixed.
FAU_STG.1	–	–
FAU_STG.3	a) Maintenance of the threshold; b) Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.	a) None. The values of threshold are always fixed. b) None. The actions are always fixed.
FPT_RVM.1	–	–
FPT_SEP.1	–	–

–: No operation

Dependencies: No dependencies.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

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

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

[assignment: Allowed identified role]:
- The account administrator
- The storage administrator
- The account partition administrator
- The storage partition administrator
- Audit log administrator
- Maintenance staff
- Storage user

Dependencies: FIA_UID.1 Timing of identification

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and the cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of* *standards*].

[assignment: *list of standards*]: It describes in “Standard” on Table 5.13.

[assignment: *cryptographic algorithm*]: It describes in “Algorithm” on Table 5.13.

[assignment: *cryptographic key sizes*]: It describes in “Key size (bit)” on Table 5.13.

[assignment: *list of cryptographic operations*]: It describes in “Cryptographic operation” on Table 5.13.

Table 5.13 Cryptographic Operation

Standard	Algorithm	Key size (bit)	Cryptographic operation	How to use
ANSI X9.30 part 1-1997	DSA	1024	Authentication	Server authentication
RSA Security Inc. Public-Key Cryptography Standards(PKCS)#1 V2.1	RSA	512 or more	Authentication	Server authentication
			Key replacing	Session key replacing
FIPS PUB 197	AES	256 128	Cryptograph or double sign of data	Select the algorithm to be used for the session key by the handshake protocol of [SSLv3.0] and [TLSv1.0]
FIPS PUB 46-3	3DES	168		
FIPS PUB 180-2	SHA-1	160	Hash	Hash function
IEEE P1363 G.7 compliant	SHA1PRNG	64	Random number	Use as a key information when creating a session key.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attribute, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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*].

[Detail: Cryptographic key]: session key

[assignment: *list of standards*]: it describes in “Standard” on Table 5.14.

[assignment: *cryptographic key generation algorithm*]: It describes in “Algorithm” on Table 5.14.

[Assignment: *cryptographic key sizes*]: it describes in “key sizes (bit)” on Table 5.14.

Table 5.14 Cryptographic Operation

Standards	Algorithm	Key sizes (bit)
[SSLv3.0] and [TLSv1.0]	Generate a session key by the handshake protocol	128, 160

Dependencies: [FCS_CKM.2 cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No the components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

[Detail: Cryptographic key]: session key

[Assignment: Standard list]: PKCS#1

[Assignment: *Cryptographic key distribution method*]: Cryptograph a key with RSA and distribute it.

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 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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*].

[Detail: Cryptographic key]: Session key

[assignment: *list of standards*]: None

[assignment: *cryptographic key destruction method*]: Delete from the memory when the user of Storage Navigator releases SSL session with logging off the Storage Navigator.

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]
FMT_MSA.2 Secure security attributes

FIA_SOS.1b Verification of secrets

Hierarchical to: No other components.

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*]: From 12 to 32 single byte uppercase and lowercase English letters, single byte numeric values, single byte space, and the following 12 kinds of symbolic codes: .-+@_=:/[],~

Dependencies: No dependencies.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

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.

[Detailed: User]: Host

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support the user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

[assignment: *list of multiple authentication mechanisms*]: It describes in the “Authentication mechanisms” on Table 5.15.

[assignment: *rules describing how the multiple authentication mechanisms provide authentication*]: It describes in the “Rules” on Table 5.15.

Table 5.15 Authentication Mechanisms and Rules

Subjects of authentication	Authentication Mechanisms	Rules
Storage Navigator user	Password mechanism	Check if the entered password by the user meets the password that TOE holds.
Maintenance Staff	Password mechanism	Check if the entered password by the maintenance staff via remote desktop connection meets the password that TOE holds.
Host (while working FC-SP authentication.)	FC-SP authentication mechanism	Check if the secret received from the host meets the secret that TOE holds.

Dependencies: No dependencies.

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

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

[assignment: *list of functions*]: It describes in the “Functions” on Table 5.16.

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

[assignment: *the authorized identified roles*]: It describes in the “Roles” on Table 5.16.

Table 5.16 List of Functions Restricting the Operation for the Roles

No.	Roles	Functions
1	Storage Administrator	FC-SP Identity authentication function.
2	Storage Partition Administrator	FC-SP Identity authentication function in a range of matching SLPR number which of the security attribute of the storage partition administrator him/herself with the SLPR number of the logical partition.
3	Maintenance Staff	FC-SP identity authentication function.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FDP_ACC.1 Subset access control

Hierarchical to: No other component.

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: Process acting on behalf of the host, process acting on behalf of the Storage Navigator.

Object: LDEV, SLPR

List of operations among subjects and objects covered by the SFP: accessing LDEV, Creating and deleting LDEV, creating and deleting SLPR

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other component.

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [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*]:

Subject: Process acting on behalf of the host, process acting on behalf of the Storage Navigator.

Object: LDEV, SLPR

The SFP-relevant security attributes, or named groups of SFP-relevant security attributes: It describes in “Security attributes of Subject” and “Security attributes of Object” on Table 5.17.

Table 5.17 SFP Related Security Attribute

Subjects	Security Attributes of Subject	Security Attribute of Objects
Process acting on behalf of the Host	WWN, LU number	LU path information (WWN, LU number, LDEV number)
Process acting on behalf of the Storage Navigator	User authority information (User type, Operation authority, SLPR number)	LDEV creation: logical partition information (SLPR number) LDEV number: LU path information (WWN, LU number, LDEV number) and Logical partition information (SLPR 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 that describes in “Rules” on Table 5.18.

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

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

Table 5.18 Rules among Subjects and Objects

Subjects	Rules	Objects
Process acting on behalf of the Host	Authorize the access to objects if the WWM and LU number provided by the process acting on behalf of the Host meets the LU path information, the security attributes of the corresponding object. Deny the access if the LU path information does not meet.	LDEV
Process acting on behalf of the Storage Navigator	Rules to create or delete the objects by the process acting on behalf of the Storage navigator. 1) When the user type is the administrator, and the operation authority is the storage administrator: Authorize the creation or deletion of SLPR.	SLPR
	Rules to create or delete the objects by the process acting on behalf of the Storage navigator. 1) When the user type is the administrator, and the operation authority is the storage administrator: Authorize all of the LDEV creation. When there is no LDEV relevant LU path information, the deletion of the corresponding LDEV is authorized. 2) When the user type is the partition administrator, and the operation authority is the storage administrator: Authorize the LDEV creation when the SLPR number of the storage partition administrator meets the SLPR number of the logical partition to be associated with LDEV. Authorize the LDEV deletion when the SLPR number of the storage partition administrator meets the SLPR number associated with LDEV, but there is no LU path information associated with LDEV.	LDEV

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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, 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*]: It describes in “Audit Items” on Table 5.19.

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

Table 5.19 Items to be Audited Defined Individually

Required Functions	Audit Items
FIA_ATD.1a	None.
FIA_USB.1a	None.
FIA_ATD.1b	None.
FIA_USB.1b	None.
FIA_AFL.1	None. Logs are not recorded when the authentication trial reaches the threshold.
FIA_SOS.1a	None. Unmatched metric is not recorded.
FIA_UAU.2	- Record the success or failure of identity authentication of the user of Storage navigator in the log files.
FIA_UAU.7	None.
FIA_UID.2	- Record the success or failure of identity authentication of the Storage navigator in the log files.

Required Functions	Audit Items
FMT_MSA.1	- Record the creation, deletion, and modification of the LU path information in the log files. - Record the changing of operating authority the user account in the log files.
FMT_MSA.3	None.
FMT_MTD.1	- Record the creation and deletion of User ID of the user account, and the password changing in the log files. - Record the WWN of host, and creation, modification, and deletion of the secret in the log file.
FMT_SMF.1	- Record the creation and deletion of user ID of the user account, the password changing, and the operating authority changing in the log files. - Record the WWN of host, and creation, modification, and deletion of the secret, in the log file.
FMT_SMR.1	- Record the changing of the operating authority of user account in the log file.
FCS_COP.1	None.
FCS_CKM.1	None.
FCS_CKM.2	None.
FCS_CKM.4	None.
FIA_SOS.1b	None. Unmatched metric is not recorded.
FIA_UAU.1	- Record the result of the identity authentication of host executed by FC-SP, in the log file.
FIA_UAU.5	- Record the success or failure of identity authentication of the user of Storage navigator in the log file.
FMT_MOF.1	- Record the setting change of the existing/ not existing of identity authentication of the host executed by FC-SP, in the log file.
FDP_ACC.1	None.
FDP_ACF.1	None.

Required Functions	Audit Items
FAU_GEN.1	None.
FAU_GEN.2	None.
FPT_STM.1	None.
FAU_SAR.1	None.
FAU_STG.1	None.
FAU_STG.3	None.
FPT_RVM.1	None.
FPT_SEP.1	None.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that cased the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] form 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: *authorized users*]: Audit log administrator [assignment: *list of audit information*]: it describes in the “Audit Information” on Table 5.20.

Table 5.20 Audit Information

Audit events	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 Storage Navigator running PC.
Creation modification, and deletion of user account of Storage Navigator user	Creation and deletion of user ID of the user account, user ID of the Storage Navigator where its password is changed, User ID to be operated, Operation contents (creation, modification, deletion), results of the operation (success, failure).
Changing the operation authority of user account of Storage Navigator user	User ID of the Storage Navigator where the operation authority of user account is changed, target User ID for the operation, Operating authority, operating contents (modification), results of the operation (success, failure)
Creation, deletion, and modification of LU path information	User ID of the Storage Navigator where the creation, deletion, modification of LU path information is executed, operating contents (Creation, deletion, modification), WWN, LU number, LDEV number, results of the operation (success, failure).
Addition, modification, deletion of the WWN of the host and the secret	WWN of host, User ID of the Storage Navigator where the creation, deletion, modification of secrets is executed, operating contents (creation, modification, deletion), results of the operation (success, failure)
Setting change of the existing/ not existing of the identity authentication of the host	User ID of the Storage Navigator where the FC-SP executes the changing of existing/ not existing identity authentication of host, WWN of host, existing or not existing of identity authentication, operating contents (modification), results of the operation (success, failure)

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trial storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

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

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

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

[assignment: *actions to be taken in case of possible audit storage failure*]: Warning message will be shown on the Storage navigator screen.

Dependencies: FAU_STG.1 Protected audit trial storage

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.2 Minimum Level of Function Strength

The minimum level of function strength of this TOE is SOF-Basic.

The TOE security function requirements that use the stochastically or permutable mechanisms are above mentioned: FIA_SOS.1a, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FCS_COP.1, FCS_CKM.1, FIA_SOS.1b, FIA_UAU.1, and FIA_UAU.5.

5.1.3 TOE Security Assurance Requirements

The TOE security assurance requirements are the following items which are included in EAL2.

Table 5.21 TOE Security Assurance Requirements

Security Assurance Requirements	
ACM_CAP.2	Component
ADO_DEL.1	Distribution procedure
ADO_IGS.1	Installation, creation, and startup procedure
ADV_FSP.1	Informal function specification
ADV_HLD.1	Descriptive design of the upper level
ADV_RCR.1	Demonstration of the informal response
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Proof of the coverage
ATE_FUN.1	Function test
ATE_IND.2	Independency test-sample
AVA_SOF.1	Evaluation of the TOE security function strength
AVA_VLA.1	Developer’s analysis of vulnerability

5.2 Security Requirements for the IT Environment

There are no security requirements for TOE to depend on the IT environment.

6 TOE Summary Specification

This section describes TOE security functions that satisfy TOE security requirements and the assurance measures.

6.1 TOE Security Functions

Table 6.1 shows that the corresponding table between the TOE security function and the security function requirements.

Table 6.1 TOE Security Functions and the Corresponding Security Function Requirements

		IT Security Functions of TOE				
		SF.LM	SF.FCSP	SF.SN	SF.ROLE	SF.AUDIT
TOE Security Function Requirements	FIA_ATD.1a	X				
	FIA_USB.1a	X				
	FIA_ATD.1b	X				
	FIA_USB.1b	X				
	FIA_AFL.1			X		
	FIA_SOS.1a			X		
	FIA_UAU.2			X	X	
	FIA_UAU.7			X		
	FIA_UID.2		X	X	X	
	FMT_MSA.1				X	
	FMT_MSA.3	X				
	FMT_MTD.1				X	
	FMT_SMF.1				X	
	FMT_SMR.1				X	
	FCS_COP.1			X		
	FCS_CKM.1			X		
	FCS_CKM.2			X		
	FCS_CKM.4			X		
	FIA_SOS.1b		X			
	FIA_UAU.1		X			
	FIA_UAU.5		X	X	X	
	FMT_MOF.1				X	
	FDP_ACC.1	X				
	FDP_ACF.1	X				
	FAU_GEN.1					X
	FAU_GEN.2					X
	FPT_STM.1					X
	FAU_SAR.1					X
	FAU_STG.1					X
	FAU_STG.3					X
	FPT_RVM.1	X	X	X	X	X
	FPT_SEP.1	X	X	X	X	X

6.1.1 SF.LM

TOE is connected with the host via SAN environment. SAN is a storage-dedicated network that connects with the fibre channel between the host and storage device. By the SF.LM, TOE executes the access control while the host access to the LDEV in the storage device.

[Satisfied requirements] FIA_ATD.1a, FIA_USB.1a, FIA_ATD.1b, FIA_USB.1b, FDP_ACC.1, FDP_ACF.1, FPT_RVM.1, FPT\SEP.1

TOE maintains the Storage Navigator attribution information (User type, operating authority, SLPR number) and associates those attributes with the user account of Storage Navigator. (FIA_ATD.1a, FIA_USB, 1a)

TOE keeps the attribute information of host (WWN, LU number), and associates that attributes with the host. (FIA_ATD.1b, FIA_USB.1b)

TOE executes "LM access control SFP" when the process acting on behalf of the host access the LDEV, and when the process acting on behalf of the host creates or deletes the LDEV.

"LM Access Control SFP" consists of the following rules: (FDP_ACC.1, FDP_ACF.1, FMT_MSA.3)

- The access is authorized for the LDEV, when the WWN and LU number passed over to the process acting on behalf of the host meets the LU path information which is the security attributes of the corresponding object. The access is denied when the LU path information are unmatched.
- When the process acting on behalf of the Storage Navigator creates or deletes SLPR, only the storage administrator can create or delete SPLR by the "User authority information of the Storage Navigator (User type, Operating authority, SLPR number) that is passed from the process acting on behalf of the Storage Navigator.
- When the process acting on behalf of the Storage Navigator creates or deletes LDEV, the storage administrator can create or delete all the LDEVs by the "user authority information of the Storage Navigator (User type, Operating authority, SLPR number) that is passed from the process acting on behalf of the Storage Navigator. The storage partition administrator can create or delete LDEVs in the corresponding logical partition, when the SLPR number, which is the security attribute of the storage partition administrator, meets the SLPR number of the logical partition.
- Conditions when deleting LDEV: Delete the corresponding LDEV when there is no associated LU path information with the subject LDEV to be deleted.
- When creating LDEV, a restricted default value is given as the access attribute. It represents that the access from the host is restricted, because there is no LU path information when creating LDEV (FMT_MSA.3)

TOE ensures that the "LM access control SFP" is applied surely when executing the function of TOE. TOE also ensures that the TSF that relevant to SF.LM protects the own, and not to occur the interference and the falsification from the unreliable subject (FPT_RVM.1, FPT_SEP.1)

6.1.2 SF.FCSP

TOE executes the identity authentication of the host by the FC-SP, when it is required by the security policy of the customer. DH-CHAP with NULL DH Group authentication is used for this authentication.

[Satisfied requirements] FIA_UID.2, FIA_SOS.1b, FIA_UAU.1, FIA_UAU.5, FPT_RVM.1, FPT_SEP.1.

TOE executes the identity authentication of the host from FC-SP with WWN and the secret before the operations of other security functions that are related accessing from the host (FIA_UID.2, FIA_UAU.1).

When there is the Host identity authentication, TOE creates the DH-CHAP authentication code when a command of security authentication is received from the host, and sends back to the host (FIA_UAU.1). The connection between the host and the storage device is authorized when the secret received from the host meets the secret that TOE holds (FIA_UAU.5).

TOE restricts the entry when a secret to be used for the identity authentication of the host by FC-SP is setting: From 12 to 32 of single byte uppercase and lowercase English letters, single byte numeric values, single byte space, and the single byte symbols of 12 kinds: .-+@_=:/[],~ (FIA_SOS.1b).

TOE ensures that it calls SF.FCSP and executes the host identity authentication when the host identity authentication is done and when the host connects to the storage device. TOE also ensures that the TSF that relevant to SF.FCSP protects the own, and not to occur the interference and the falsification from the unreliable subject (FPT_RVM.1, FPT_SEP.1).

6.1.3 SF.SN

[Satisfied requirements] FIA_AFL.1, FIA_SOS.1a, FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FPT_RVM.1, FPT_SEP.1

TOE executes the identity authentication at the Storage Navigator with the user ID and the password before the operations of other security functions. If the identity authentication failed 3 times continuously, the subject user’s identity authentication is denied for one minute (FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FIA_AFL.1).

TOE restricts the entry of password to be used for the identity authentication of the Storage Navigator as follows: From 6 to 256 of single byte uppercase and lowercase English letters, single byte numeric values, and the single byte symbols of 32 kinds: !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~ (FIA_SOS.1a, FIA_UAU.7).

TOL uses SSL on the communication between the Storage Navigator and the SVP, and protect TSF-data from the sniffing and the falsification with the cryptography processing. SSL provides the public key cryptosystem method server, authentication system between the clients, data cryptography system by the common key cryptosystem, and the securement of coincidence of the data by the hash function. Table 5.1.3 shows the cryptography operation to be used at SSL. The cryptography algorithm and the key size are determined by the negotiation between the Storage navigator and the SVP, and the key will be erased from the memory when it is used. The supported SSL versions are: SSL version 3.0 and TLS version 1.0 (FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4).

TOE calls SF.SN before the Storage Navigator user executes the management operation of the storage device by using the Storage Navigator, and ensures that the cryptographic communication by the SSL and the identity authentication of the user of Storage Navigator are executed. TOE also ensures that the TSF that relevant to SF.SN protects the own, and not to occur the interference and the falsification from the unreliable subject (FPT_RVM.1, FPT_SEP.1).

6.1.4 SF.ROLE

[Satisfied requirements] FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FPT_RVM.1, FPT_SEP.1

TOE executes the “LM access control SFP” for the access to the SVP which is the process acting on behalf of the Storage Navigator user.

The “LM access control SFP” consists of the following rules:

- “LM Access control SFP” restricts the operation of creation, modification, deletion, reference of the LU path information (WWN, LU number, LDEV number), based on the user type, operating authority, and SLPR number (FMT_MSA.1). Table 5.1 and Table 5.2 show the operation where each role can execute for the LU path information.
- “LM Access control SFP” restricts the operation of creation, deletion, reference of the Logical partition information (SLPR number) based on the user type, operating authority, and SLPR number (FMT_MSA.1). Table 5.3 shows the operation where each role can execute for the Logical partition information.
- “LM Access control SFP” restricts the operation of setting, modification, reference of the User authority information (user type, operating authority, SLPR number) of the Storage Navigator, based on the user type and the operating authority (FMT_MSA.1). Table 5.4 and Table 5.5 show the operation where each role can execute for the User authority information.

TOE has the following managing functions. (FMT_MTD.1, FMT_SMF.1)

- TOE manages the user account’s user ID, password, user type, operating authority, and SLPR number by the account managing function of the Storage Navigator. Table 5.7 and Table 5.8 show the operation that can be managed by each role, and Table 5.12 shows its management items.
- TOE manages the user name and the password when the maintenance staff executes the remote desktop connection. Table 5.9 shows the operation to the user name and the password at the remote desktop connection, and Table 5.12 shows its management items.
- TOE manages the WWN and the secret, which are the authentication data of the host at the FC-SP function of the Storage navigator. Table 5.10 and Table 5.11 show the operation that can be managed by each role, and Table 5.12 shows its management items.

TOE restricts the setup operation of the host identity authentication (existing or not existing authentication) based on the user type and the operating authority. Table 5.16 shows the operation that can be operated by each role (FMT_MOF.1).

TOE maintains the roles (the account administrator, the storage administrator, the account partition administrator, the storage partition administrator, the audit log administrator, the maintenance staff, and the storage user.) (FMT_SMR.1).

TOE executes the identity authentication for the maintenance staff when they make a connection to the SVP with the user name and password of the remote desktop connection.

TOE calls SF.ROLE when the user of Storage navigator executes the management operation, and ensures that the unauthorized management operation shall not be executed by the user type and the operating authority of the user of Storage Navigator. TOE also ensures that the TSF that relevant to SF.ROLE protects the own, and not to occur the interference and the falsification from the unreliable subject (FPT_RVM.1, FPT_SEP.1).

6.1.5 SF.AUDIT

[Satisfied requirements] FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1, FAU_STG.3, FPT_RVM.1, FPT_SEP.1

TOE has the following audit functions:

- The audit log is generated when the auditing issues related on the security function in the TOE occur. User account's user ID which is the cause of this auditing issue is given to the audit log to be generated. On the date and time to be used for the generating audit log, the time and date controlled by the OS on the SVP is used. Table 5.20 shows the audit information.
- There are no roles that are available to execute unauthorized modification or deletion of the audit log.
- The audit log can save up to 250,000 lines. When the audit log reaches the maximum line, the new record will be overwritten from the first line. Therefore, the old information will be deleted (Wraparound method). When the audit logs reach 175,000 lines, a message shows on the Storage Navigator screen, that the audit log reaches 175,000 lines and persuade the user to download the audit log. Once the audit log is downloaded, the audit log lines are reset, and the new logs are recorded from the first line.
- The audit log administrator only can download the audit log.

When a security related issue occurs, TOE calls the SF.AUDIT and ensures the creation of audit log. TOE also ensures that the TSF that relevant to SF.AUDIT protects the own, and not to occur the interference and the falsification from the unreliable subject (FPT_RVM.1, FPT_SEP.1).

The audit log that TOE acquires consists of the basic and detailed information. Table 6.2 shows the output contents of the basic information, and Table 6.3 shows the output contents of the detailed information.

Table 6.2 Output Contents of the Basic Information

No.	Items	Acquisition contents
1	Log in User ID	Output the user ID of the Storage Navigator.
2	SLPR Number	Output the SLPR number of the login user.
3	Date	Output the date of issue occurred.
4	Time	Output the time of issue occurred.
5	Time zone	Output the time difference with GMT (Greenwich mean Time)
6	Name of function	Output the name of executed function
7	Name of operation or issue	Output the short operation name of each function.
8	Parameter	Output the parameter of the executed setting operation.
9	Result of operation	Output the result of the operation.
10	Sequential number of the log information	Output the sequential number of the saved log information.

Table 6.3 Output Contents of the Detailed Information

No.	Items	Acquisition contents
1	Identity authentication of the Storage Navigator User	IP address of the Storage Navigator operating PC.
2	Creation, modification, deletion of Storage Navigator user’s user account	User ID of the operational subject, operating contents (creation, modification, deletion), and the result of the operation (Success, failure).
3	Changing the operating authority of Storage navigator user’s user account	User ID of the operational subject, operating authority, operating contents (modification), and the result of the operation (Success, failure).
4	Creation, modification, and deletion of LU path information	Operating contents (creation, modification, deletion), WWN, LU number, LDEV number, the result of the operation (Success, failure).
5	Addition, modification, and deletion of Host’s WWN and Secret	WWN of the host, operating contents (creation, modification, deletion), and the result of the operation (Success, failure).
6	Setting change of the existence or not existence of the identity authentication of the Host by FC-SP	WWN of the host, existence or not existence of identity authentication, operating contents (modification), and the result of the operation (Success, failure).

6.2 Level of Security Function Strength

In this TOE, the security functions that have sequential and stochastic mechanisms, which are the target of security function strength, are SF.FCSP and SF.SN. The functions related to the password and the secret of those security functions, and the functions related to the SSL session key generation have the security strength level: SOF-basic.

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

6.3 Assurance Measures

The assurance measures are defined below by showing the reference to the documents that satisfy the security assurance requirements.

The document names in the following table will be revised to the new titles and the versions in the process of evaluation.

Table 6.4 Security Assurance and Assurance Measures

Security Assurance Requirements		Assurance measures
ACM_CAP.2	Components	• Hitachi USP V Microprogram Configuration Administration List • Method of Adding the DKCMAIN/SVP Version
ADO_DEL.1	Distribution procedure	• HITACHI USP V Distribution Method
ADO_IGS.1	Installation, creation and startup procedure	[Hitachi Universal Storage Platform V/ Hitachi Universal Storage Platform H24000] • A/H-65AA, A-65BA, HT-40BA Disk Subsystem Maintenance Manual Rev.1.3 [Hitachi Universal Storage Platform VM/ Hitachi Universal Storage Platform H20000] • A/H-65AA, A-65BA, HT-40BA Disk Subsystem Maintenance Manual [Hitachi Universal Storage Platform V] • DKC610I Maintenance Manual Rev.1.3 [Hitachi Universal Storage Platform VM] • DKC615I Maintenance Manual
ADV_FSP.1	Informal function specification	• Hitachi Universal Storage Platform V Function Specification
ADV_HLD.1	Descriptive design of the upper level	• Hitachi Universal Storage Platform V Higher Level Specification
ADV.RCR.1	Demonstration of the informal response	• Hitachi Universal Storage Platform V Representation Correspondence Analysis

Security Assurance Requirements		Assurance measures
AGD_ADM.1	Administrator guidance	• Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM/ Hitachi Universal Storage Platform H24000/ Hitachi Universal Storage Platform H20000 ISO15408 Function of Acquiring Authentication; Instruction Manual • Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM/ ISO15408 Certification Instruction Manual
AGD_USR.1	User guidance	• Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM/ Hitachi Universal Storage Platform H24000/ Hitachi Universal Storage Platform H20000 User Guidance • Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM/ User Guidance
ATE_COV.1	Proof of the coverage	• Hitachi Universal Storage Platform V Test Analysis
ATE_FUN.1	Function test	• Hitachi Universal Storage Platform V Test Specification
ATE_IND.2	Independency test - sample	• TOE
AVA_SOF.1	Evaluation of the TOE security function strength	• Hitachi Universal Storage Platform V Function Specification Analysis
AVA_VLA.1	Developer’s analysis of vulnerability	• Hitachi Universal Storage Platform V Analysis of Vulnerability

7 PP Claims

This ST does not claim for any PP.

8 Rationale

This section provides the rationale used for mainly evaluating ST.

8.1 Security Objectives Rationale

This section explains that the security objectives are fit for covering all the phases that have been identified in the TOE security environment.

Table 8.1 shows that the security objectives described in this ST can be traced to assumptions, treats or the security policy of the organization.

Table 8.1 Correspondences of the TOE Security Environments to the Security Objectives

		Security Objectives										
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN	OE.NOEVIL	OE.NOEVIL-MNT	OE.PHYSICAL_SEC	OE.ILLEGAL_SOFT	OE.CONNECT_STORAGE
TOE security environments	A.NOEVIL							X				
	A.NOEVIL_MNT								X			
	A.PHYSICAL_SEC									X		
	A.ILLEGAL_SOFT										X	
	A.CONNECT_STORAGE											X
	T.ILLEGAL_XCNTL	X	X				X					
	T.TSF_COMP			X								
	T.LP_LEAK					X						
	T.CHG_CONFIG	X					X					
	P.MASQ				X							

8.1.1 Security Objectives Rationale for the Prerequisite

Table 8.2 shows that the prerequisites are covered by the security objectives.

Table 8.2 Validity of the Security Objective for the Prerequisite

Prerequisite	Rationale that the prerequisite are covered
A.NOEVIL	A.NOEVIL assigns a reliable person to the storage administrator, the account administrator, the audit log administrator respectively for the managing or operating of the whole storage device, as described in OE. NOEVIL. And this can be realized by assigning a reliable person to the storage partition administrator and the account partition administrator respectively for the managing or operating of the storage system in the range 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 staff, as described in OE.NOEVIL_MNT.
A.PHYSICAL_SEC	A.PHYSICAL_SEC can be realized by, that the storage device is installed in the secure area where only authorized personnel: the storage administrator, the account administrator, the audit log administrator, and the maintenance staffs have access rights, and protected fully from the unauthorized physical access, as described in OE.PHYSICAL_SEC.
A.ILLEGAL_SOFT	A.ILLEGAL_SOFT can be realized by not installed illegal software to the administrator client PC, as described in OE.ILLEGAL_SOFT.
A.CONNECT_STORAGE	A.CONNECT_STORAGE can be realized by restricting the storage device connected from the other to the one that consisted of TOE, as described in OE.CONNECT_STORAGE. Because the protection property of TOE can be modified or browsed by the operation of remote copy or the backup operation to the other storage devices, and this can authorize only the reliable storage administrator to operate remote copying or the backup operation to satisfy the operation that meet the prerequisite.

8.1.2 Security Objectives Rationale to cope with Threats

Table 8.3 shows that the security objectives help to cope with the treats.

Table 8.3 Validity of the Seculity objectives to cope with Threats

Treats	Rationale that threats are being coped with
T.ILLEGAL_XCNTL	T.ILLEGAL_XCNTL is coped with treats by the O.ADM_AUTH, O.ADM_ROLE and O.AUD_GEN, as described below: • TOE reduces threats by executing the identity authentication for the use of Storage Navigator and restricting the management operations executed by the user of Storage Navigator as follows. - The account administrator can execute the account

Treats	Rationale that threats are being coped with
	managing operation for the whole device. - The whole storage administrator can execute the storage managing operation for the whole device. - The storage partition administrator can execute the storage managing operation in the authorized logical partition. - The account partition administrator can execute the account managing operation in the authorized logical partition. • The treats can be reduced, because TOE can trace the issues related to security if the unauthorized operation is done or not, at the setting change operation.
T.TSF_COMP	T.TSF_COMP is coped with treats by the O.SEC_COMM as described in the following: • Between the Storage Navigator and the SVP use the cryptography communication because it can reduce treats of sniffing or falsification by connecting unauthorized devices.
T.LP_LEAK	T.LP_LEAK is coped with treats by the O.HOST_ACCESS as described in the following: • TOE controls by the LU path information that the authorized identified host only can access to the authorized LDEV. This results in removing threats.
T.CHG_CONFIG	T.CHG_CONFIG is coped with treats by the O.ADM_AUTH and O.AUD_GEN as described in the following: • TOE authenticates the identity of Storage Navigator user before the management operating of the virtual storage device, and if the authentication process fails, the operation is denied. Therefore, illegal access from the third party is reduced. • Because TOE can trace the issues related to the security when the identity authentication is failed, illegal access from the third party can be reduced.

8.1.3 Security Objectives Rationale for the Security Policy of the Organization

Table 8.4 shows that the security policy of the organization is realized by the security objectives.

Table 8.4 Validity of the Security Objectives for the Security Policy of the Organization

Security policy of the Organization	Rationale that the security policy of organization is realized
P.MASQ	P.MASQ is realized by O.HOST_AUTH, as described below. • TOE executes the identity authentication of the host by the FC-SP, before the host accesses to the corresponding port.

8.2 Security Requirements Rationale

This section explains that the set of security requirements are fit for satisfying the security objectives.

8.2.1 Rationale for the Security Function Requirements

Table 8.5 shows that the sedulity function requirements described by this ST can be traced to the security objectives.

Table 8.5 Correspondences of the Security Function Requirements to the Security Objectives

		TOE Security Objectives					
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN
TOE Security Function Requirements	FIA_ATD.1a	X					
	FIA_USB.1a	X					
	FIA_ATD.1b					X	
	FIA_USB.1b					X	
	FIA_AFL.1	X					
	FIA_SOS.1a	X					
	FIA_UAU.2	X					
	FIA_UAU.7	X					
	FIA_UID.2	X			X		
	FMT_MSA.1		X				
	FMT_MSA.3		X				
	FMT_MTD.1		X				
	FMT_SMF.1		X				
	FMT_SMR.1		X				
	FCS_COP.1			X			
	FCS_CKM.1			X			
	FCS_CKM.2			X			
	FCS_CKM.4			X			

		TOE Security Objectives					
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN
TOE Security Function Requirements	FIA_SOS.1b				X		
	FIA_UAU.1				X		
	FIA_UAU.5	X			X		
	FMT_MOF.1		X				
	FDP_ACC.1		X			X	
	FDP_ACF.1		X			X	
	FAU_GEN.1						X
	FAU_GEN.2						X
	FPT_STM.1						X
	FAU_SAR.1						X
	FAU_STG.1						X
	FAU_STG.3						X
	FPT_RVM.1	X	X	X	X	X	X
	FPT_SEP.1	X	X	X	X	X	X

Table 8.6 shows that the TOE security objectives realized by the TOE security function requirements.

Table 8.6 Validity of the Security Function Requirements for TOE Security Objectives

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
O.ADM_AUTH	O.ADM_AUTH requires that, for identifying and authenticating the user of the Storage Navigator prior to executing the management operations of storage device. The details of the necessary measurement and the required functions for this request are the following: a. Maintaining the user of Storage Navigator. TOE must define the user account to identify the user of Storage

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	Navigator and maintain the account by associating with the user. With this operation, the identification of Storage Navigator user becomes available. The security function requirements that correspond to this requirement are: FIA_ATD.1a and FIA_USB.1a. b. Executing the identity authentication of the user account of the Storage navigator before using TOE. TOE must identify the user account before the TOE is used. Therefore, executing the identity authentication of the user account must be done before the operation of all the storage navigator functions. The security function requirements that correspond to this requirement are: FIA_UID.2, FIA_UAU.2, and FIA_UAU.5. c. Managing password. The password that TOE to identify the user account is available to combine from 6 to 256 single byte uppercase and lowercase English letters, single byte numeric values, and single byte symbols, and the entered value is displayed as * (asterisk) in the screen, in place of the actual password. If the authentication is failed 3 times continuously because of entering the incorrect password, the login of the corresponding user is denied for 1 minute, to reduce the possibility of cracking password. The security function requirements that correspond to this requirement are: FIA_AFL.1, FIA\SOS.1a, and FIA_UAU.7. d. Executing the identity authentication certainly. To execute the identity authentication of the Security Navigator, the identity authentication function must be called before the user of Storage Navigator starts the operation. And it must be protected its mechanism from the interruption or falsification. In addition, TSF is required to protect defensively from the interruption or falsification by the unreliable subjects. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.ADM_AUTH can be satisfied by achieving all of the a, b, c and d procedures above. And achieving the security function requirements that correspond to the respective measurements: FIA_ATD.1a, FIA_USB.1a, FIA_AFL.1, FIA_SOS.1a, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2, FPT_RVM.1, and FPT_SEP.1, O.ADM_AUTH can be realized.
O.ADM_ROLE	O.ADM_ROLE requires that, for restricting the managing operation of the user of Storage Navigator, based on the user type and the operating authority of the authorized user ID. The details of the necessary measurement and the required functions for this request are the following: a. Restricting the operation of user type, operating authority, and SLPR number. TOE must control the user type of the user account, operating authority, setting or changing of SLPR number, and creating or deleting of SLPR by the user type and the operating authority of the user account.

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	Therefore, TOE must control any change to the user account in accordance with the rules defined as the “LM access control SFP”. The security function requirement that correspond to this requirement is: FMT_MSA.1. b. Managing the identity authentication information. TOE is required to control the user ID of the user account, password, WWN of host, secret changing in accordance with the user type and the operating authority of the user account. With this operation, it prevents the illegal change of the user ID of the user account, password, WWN of host, and secret. The security function requirement that correspond to this requirement is: FMT_MTD.1. c. Holding the managing function. TOE is required that it must have a function to manage the user account of Storage Navigator, Identity authentication information of the host, and the identity information of WWN. The security function requirement that correspond to this requirement is: FMT_SMF.1. d. Maintaining the roles. TOE is required that it must maintain the roles of the account administrator, the storage administrator, the account partition administrator, the storage partition administrator, the audit log administrator, the maintenance staff, and the storage user, and then associate them with the users. The security function requirement that correspond to this requirement is: FMT_SMR.1. However, the maintenance staff does not have to execute identity authentication, because the storage device is installed in the secure area and a reliable person is assigned for the maintenance staff. e. Managing the identity authentication operation of the host. TOE is required that it must control the changing of existing or not existing of the host identity authentication in accordance with the user type and the operating authority of the user account. With this operation, it prevents the illegal change of the existing or not existing of the host identity authentication. The security function requirement that correspond to this requirement is: FMT_MOF.1. f. Defining and executing the access control. TOE is required that it must execute creating or deleting of SLPR and LDEV in accordance with the rules defined as “LM access control SFP”. With this operation, the storage partition administrator can control the creation and deletion of LDEV in the allocated SLPR. And creating LDEV is giving the limited default value as the access attribute. This means that the accessing from host is limited because there is no LU path information when the LDEV is created. The security function requirements that correspond to this requirement are: FDP_ACC.1, FDP_ACF.1. and FMT_MSA.3. g. Executing LM access control SFP certainly. To execute the operating of the operating authority of the user account

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	of Storage Navigator, the operating of SLPR, and the managing of the identity authentication data surely, LM access control SFP must be executed certainly when the subjects operate the objects. It must be protected its mechanism from the interruption or falsification. And, TSF is required to protect defensively from the interruption or falsification by the unreliable subjects. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.ADM_ROLE can be satisfied by achieving all of a, b, c, d, e, f and g procedures above. And achieving the security function requirements that correspond to the respective measurements: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT.SMF.1, FMT_SMR.1, FMT_MOF.1, FDP_ACC.1, FDP_ACF.1, FPT_RVM.1, and FPT_SEP.1, O.ADM_ROLE can be realized.
O.SEC_COMM	O.SEC_COMM requires that, for providing the secure communication function by the cryptography data between the Storage Navigator and the SVP, to protect the data between the Storage Navigator and the SVP from sniffing or falsification. The details of the necessary measurement and the required functions for this request are the following: a. Protecting the communication data. It is required to cryptograph the communication data between the Storage Navigator and the SVP. With this operation, it protects the communication data from the sniffing or falsification. Use the SSL for the cryptography, and the cryptographic algorithm and the key size are determined by the negotiation between the Storage Navigator and the SVP. The Key will be erased from the memory once it is used. The security function requirements that corresponds to this requirement are: FCS_COP.1, FCS_CKM.1, FCS_CKM.2 and FCS_CKM.4. b. Executing cryptography certainly. The cryptography operation must be executed certainly to protect the communication data between the Storage Navigator and the SVP from the sniffing and falsification. And, it must be protect its mechanism from the interruption and falsification. In addition, TSF is required to protect defensively from the interruption or falsification by the unreliable subjects. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.SEC_COMM can be satisfied by achieving all of a and b procedures above. And achieving the security function requirements that correspond to the respective measurements: FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS.CKM.4, FPT_RVM.1, and FPT_SEP.1, O.SEC_COMM can be realized.
O.HOST_AUTH	O.HOST_AUTH requires that, for executing the identity authentication of the host if there is a connection request from the host. The details of the necessary measurement and the required functions for

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	this request are the following: a. Authenticating the host before using TOE. TOE is required that the host is able to access the user data in the LU when the authentication of the host is succeeded. The security function requirements that correspond to this requirement are: FIA_UID2, FIA_UAU.1 and FIA_UAU.5. b. Executing FC-SP function. When a command of executing the security authentication is received from the host, TOE creates the DH-CHAP authentication code and sends it to the Host (FIA_UAU.1). c. Managing the secret. The secret for the authentication of the host by TOE is available to combine from 12 to 32 single byte uppercase and lowercase English letters, single byte numeric values, and single byte space, and the single byte symbols of 12 kinds: .-+@_=:/[],~, to reduce the possibility of cracking password. The security function requirement that correspond to this requirement is: FIA_SOS.1b. d. Executing the identity authentication certainly. TOE is required to execute the identity authentication of the host when the host connects to LU. Therefore, the identity authentication function is called certainly when the host connects to LU. And, it must be protect its mechanism from the interruption and falsification. In addition, TSF is required to protect defensively from the interruption or falsification by the unreliable subjects. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.HOST_AUTH can be satisfied by achieving all of a, b, c and d procedures above. And achieving the security function requirements that correspond to the respective measurements: FIA_UID.2, FIA_UAU.1, FIA_UAU.5, FIA_SOS.1b, FPT_RVM.1, and FPT_SEP.1, O.HOST_AUTH can be realized.
O.HOST_ACCESS	O.HOST_ACCESS requires that, for executing the access control to be able to access in the assigned partition for the own host, when the host accesses to the user data of LU, which is the subject to be protected property of this TOE. The details of the necessary measurement and the required functions for this request are the following: a. Maintain the host. TOE must define the host attribute information (WWN and LU number) and maintain the host by associating the attribute to the host, for the identification of the host. The host identification becomes available with this function. The security function requirements that correspond to this requirement are: FIA_ATD.1b and FIA_USB.1b.

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	b. Defining and executing the access control. TOE is required that it determines the access to the LDEV in accordance with the rules defined as “LM access control SFP”, and needs to execute the access control as it defined. With this function, the host can be controlled to access only to the user data in the assigned LDEV. The security function requirements that correspond to this requirement are: FDP_ACC.1 and FDP_ACF.1. c. Executing LM access control SFP certainly. To execute the access control of the host surely, LM access control SFP must be executed certainly when the subjects operate the objects. It must be protected its mechanism from the interruption or falsification. In addition, TSF is required to protect defensively from the interruption or falsification by the unreliable subjects. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.HOST_ACCESS can be satisfied by achieving all of a, b, and c procedures above. And achieving the security function requirements that correspond to the respective measurements: FIA_ATD.1b, FIA_USB.1b, FDP_ACC.1, FDP_ACF.1, FPT_RVM.1, and FPT_SEP.1, O.HOST_ACCESS can be realized.
O.AUD_GEN	O.AUD_GEN requires that, for managing if the information related security is created or modified, or deleted illegally. The details of the necessary measurement and the required functions for this request are the following: a. Generating the audit log for the subject related to the security function. SVP is required to create audit log of the subjects when the identity authentication at the Storage Navigator or falsification of the user account or the SLPR are occurred. With this operation, it becomes available to identify from the audit log in case the falsification for the information is done illegally. The security function requirement that correspond to this requirement is: FAU_GEN.1. Since FAU_GEN.1 acquires the audit log on the subject of identity authentication and subject of setting change operation, it satisfies the security objectives. The items written as “None” in the table of FAU_GEN.1, Table 5.19, have no problem if there are no items to be audit since there is no effectiveness on the trace of the security issue, or the trace is possible because it is included in the other audits that subject to execute certainly. In addition, in the state of no setting of the LU path information, the host cannot be recognized the corresponding LDEV as a logical device, and not available to access LDEV. Therefore, there is no problem if it does not acquire the audit issue related to the security function requirements that accessing from the host to LDEV. The timestamp provided by FPT_STM.1 is the timestamp of the SVP OS. Because it cannot be changed by the other people except the

TOE Security Objectives	Rationale for the Realization of TOE Security Objectives
	maintenance staff, the audit log is not required such for the setting change of the time. When creating the audit log, the issued date and time of the subject and the user ID of the user who operated must be added in the audit log. With this operation, the issued date and time of the subject and the operated user can be identified. The security function requirements that correspond to this requirement are: FAU_GEN.2 and FPT_STM.1. b. Restricting the referencing of audit log. Referring to the audit log, it is required to download the audit log in the SVP from the Storage Navigator. The downloading of audit log is limited to the user account who has the operation authority of the audit log administrator. This can protect the log from the illegal referencing. The security function requirement that correspond to this requirement is: FAU_SAR.1. c. Protecting the audit log from the falsification TOE is required to protect the deletion or the falsification of the audit log by an unauthorized user. The downloading of audit log is limited to the user account who has the operation authority of the audit log administrator. In addition, TOE does not have any function to modify the audit log. This can protect the log from the illegal deletion or the falsification. The security function requirement that correspond to this requirement is: FAU_STG.1. d. Warning the risk of loss of the audit log. The audit log is available to create up to 250,000 lines. However, when the audit log exceeds the maximum, the record is overwritten from the first line and erased the oldest audit log. Therefore, a warning message is shown on the display of Storage Navigator, when the logs exceed the175,000 lines, and persuade the downloading of the audit log. This relieves the risk of audit log loss. The security function requirement that correspond to this requirement is: FAU_STG.3. e. Creating audit log certainly. TOE must create audit log certainly when a subject related to the security is occurred to audit if there is illegal creation, modification, or deletion in the security related information. And, it must be protect its mechanism from the interruption and falsification. In addition, TSF is required to protect defensively from the interruption or falsification by the unreliable subject. The security function requirements that correspond to this requirement are: FPT_RVM.1 and FPT_SEP.1. O.AUD_GEN can be satisfied by achieving all of a, b, c, d, and e procedures above. And achieving the security function requirements that correspond to the respective measurements: FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1. FAU_STG.3, FPT_RVM.1, and FPT_SEP.1, O.AUD_GEN can be realized.

8.2.2 Rationale for the Internal Consistency of the Security Requirements

Table 8.7 describes the dependency of the security function requirements.

Table 8.7 Dependencies of Security Function Requirements

Item number	TOE or IT Environment	Security Function Requirements	Dependency Defined by CC part 2	Function Requirements handled in this ST
1	TOE	FIA_ATD.1a	None	–
2	TOE	FIA_USB.1a	FIA_ATD.1	FIA_ATD.1a
3	TOE	FIA_ATD.1b	None	–
4	TOE	FIA_USB.1b	FIA_ATD.1	FIA_ATD.1b
5	TOE	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 *2
6	TOE	FIA_SOS.1a	None	–
7	TOE	FIA_UAU.2	FIA_UID.1	FIA_UID.2 *1
8	TOE	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 *2
9	TOE	FIA_UID.2	None	–
10	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
11	TOE	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
			FMT_SMR.1	FMT_SMR.1
12	TOE	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
13	TOE	FMT_SMF.1	None	–
14	TOE	FMT_SMR.1	FIA_UID.1	FIA_UID.2 *1
15	TOE	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FCS_CKM.4	FCS_CKM.4
			FMT_MSA.2	None *3
16	TOE	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
			FCS_CKM.4	FCS_CMK.4
			FMT_MSA.2	None *3
17	TOE	FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FCS_CKM.4	FCS_CKM.4
			FMT_MSA.2	None *3
18	TOE	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FMT_MSA.2	None *3
19	TOE	FIA_SOS.1b	None	–
20	TOE	FIA_UAU.1	FIA_UID.1	FIA_UID.2 *1
21		FIA_UAU.5	None	–
22	TOE	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
23	TOE	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1

Item number	TOE or IT Environment	Security Function Requirements	Dependency Defined by CC part 2	Function Requirements handled in this ST
24	TOE	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
			FMT_MSA.3	FMT_MSA.3
25	TOE	FAU_GEN.1	FPT_STM.1	FPT_STM.1
26	TOE	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
			FIA_UID.1	FIA_UID.2 *1
27	TOE	FPT_STM.1	None	–
28	TOE	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
29	TOE	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
30	TOE	FAU_STG.3	FAU_STG.1	FAU_STG.1
31	TOE	FPT_RVM.1	None	–
32	TOE	FPT_SEP.1	None	–

*1: Dependency is achieved by FIA_UID.2 which is the upper hierarchy component of FIA_UID.1.

*2: Dependency is achieved by FIA_UAU.2 which is the upper hierarchy component of FIA_UAU.1.

*3: The security attribute handled at FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1 are the one related to the each cryptographic key. Since each one has defined the secured attribute according to the standardized algorithm, no setting and modifying is done from the Storage navigator or the SVP. Therefore, there is no problem if the dependency for the security function requirement: FMT_MSA.2, which is related to accepting the secured security attribute, does not satisfy the dependency relations.

For each TOE security function requirement, rationale is shown on Table 8.8 for consistency that the definition has through the function requirement of the same category.

Table 8.8 Consistencies among Security Function Requirements

Item Number	Category	Security Function Requirement	Rationale for Consistency
1	Access Control	FDP_ACC.1 FDP_ACF.1	Definitions related to access control are made based on these function requirements. It is required that the same SFP be applied to the same subject or object and there are no competitions or inconsistencies. The whole contents are consistent.
2	Administration	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Definitions related to security management are made based on these function requirements. There are no competitions or inconsistencies in any targeted security attributes or actions. The whole contents are consistent.

Item Number	Category	Security Function Requirement	Rationale for Consistency
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_UAU.5 FIA_UAU.7 FIA_UID.2 FIA_USB.1a FIA_USB.1b	These function requirements realizes the identification and authentication, As TSF, definitions are made separately as described below, and there are no competitions or inconsistencies. The whole contents are consistent. I) User ID and password of the Storage Navigator. II) WWN and secret of host.
4	Audit	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1 FAU_STG.3	Definitions related to audit log are made based on these function requirements. There are no competitions or inconsistencies and the whole contents are consistent.
5	Management and operation of cryptography key	FCS_COP.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	Definitions related to the management and operation of the cryptography key to be used in SSL communication between the Storage Navigator and the SVP. There are no competitions or inconsistencies and the whole contents are consistent.
6	Complementation	FPT_STM.1 FPT_RVM.1 FPT_SEP.1	The function requirements are for complementing the other function requirements. Since FPT_STM.1 is the one for the timestamp of the audit log, FPT_RVM.1 is the one for preventing bypass, and FPT_SEP.1 is the one for separating the security domain, it is obvious that there are no competitions or inconsistencies among the function requirements in this category, and that the whole contents are consistent.

Item Number	Category	Security Function Requirement	Rationale for Consistency
7	Among categories	#1 to #2	The requirements concerning access control define the control over the user data in LU that is the property to be protected, and the requirements concerning management define the management of TSF data. Therefore, there is no competitions or inconsistencies with each other.
		#1 to #3 #2 to #3	The requirement concerning identification and the one concerning access control or management have no competitions or inconsistencies with each other.
		#1 to #4 #2 to #4 #3 to #4	Since they are for recording the result of audit for the requirements concerning access control, management, identification and authentication, there are no competitions or inconsistencies with each other.
		#1 to #5 #2 to #5 #3 to #5 #4 to #5	Among the requirement concerning access control, management, identification and authentication, and audit log have no competitions or inconsistencies with each other.
		#1 to #6 #2 to #6 #3 to #6 #4 to #6 #5 to #6	As described in the above, it is obvious that FPT_RVM.1 and FPT_SEP.1 cause no competitions or inconsistencies with the other requirements. In addition, since FPT_STM.1 is for providing time information for FAU_GEN.1, where there is no competitions or inconsistency with the other requirements.

Furthermore, mutual assistance is being made by the security requirements that have no dependent relations, as described below.

- FIA_UID.2 and FIA_UAU.1 are restricting the run and stop of identity authentication function of FC-SP to the operation from the Storage Navigator executed by the storage administrator and the storage partition administrator only. Since the operation cannot be stopped by the other ways, it prevents the deactivation. And since the other requirements concerning the security functions cannot change the function stopping and behalf by the operation, deactivation does not have to be considered.

As described in the above, the IT security requirements described in this ST work together, mutually assist each other and form the whole which is internally consistent.

8.2.3 Rationale for the Minimum Level of Function Strength

Section 3.2 assumes the attack capability of the threatening agent to be “low”.

Therefore, TOE has to be prepared to deal with the low level of threatening agent, and the valid minimum level of function strength should be SOF-based. In addition, section 5.1.2 requires TOE for the SOF-based as the minimum level of function strength, and the attack capability and the minimum level of function strength are consistent.

8.2.4 Rational for the Evaluation Assurance Level

The Storage device including this TOE is installed in a secure area and it assumed no other way of attacking except the way of using San or LAN. Section 3.2 assumes the attacks from the route of communication between an administrator client PC and a storage device, and the route of connecting unauthorized host to SAN, and these can be taken as “low” level attacks without requiring of special knowledge, technique, or tools.

In addition, the administrator client PC where the Storage Navigator runs is controlled to prohibit installation of unauthorized software. Therefore, evaluating for the “explicit vulnerability” balances with the assumption of threat, by removing the assumption of potential threat based on the detailed interfacing with the storage device.

Although TOE has the cryptography function, the actual implementation of cryptography key is done at the installation. Therefore, there is no security policy of TOE that leads the vulnerability of TOE if it is not handled as “sensitive”.

Furthermore, as TOE is software, the installing of security function based on the designing documents and evaluating it by test can counter from the possible threat assumed by the security function.

Therefore, the evaluation assurance level 2 should be valid.

8.3 TOE Summary Specification Rationale

This section explains that the TOE security function and the assurance measures are fit for satisfying the TOE security requirements.

8.3.1 Rationale for the TOE Security Functions

Table 8.9 shows that the IT security functions described in this ST can be traced to TOE security function requirements.

Table 8.9 Mapping of TOE Security Function to SFR

		IT Security Functions of TOE				
		SF.LM	SF.FCSP	SF.SN	SF.ROLE	SF.AUDIT
TOE Security Function Requirements	FIA_ATD.1a	X				
	FIA_USB.1a	X				
	FIA_ATD.1b	X				
	FIA_USB.1b	X				
	FIA_AFL.1			X		
	FIA_SOS.1a			X		
	FIA_UAU.2			X	X	
	FIA_UAU.7			X		
	FIA_UID.2		X	X	X	
	FMT_MSA.1				X	
	FMT_MSA.3	X				
	FMT_MTD.1				X	
	FMT_SMF.1				X	
	FMT_SMR.1				X	
	FCS_COP.1			X		
	FCS_CKM.1			X		
	FCS_CKM.2			X		
	FCS_CKM.4			X		
	FIA_SOS.1b		X			
	FIA_UAU.1		X			
	FIA_UAU.5		X	X	X	
	FMT_MOF.1				X	
	FDP_ACC.1	X				
	FDP_ACF.1	X				
	FAU_GEN.1					X
	FAU_GEN.2					X
	FPT_STM.1					X
	FAU_SAR.1					X
	FAU_STG.1					X
	FAU_STG.3					X
	FPT_RVM.1	X	X	X	X	X
	FPT_SEP.1	X	X	X	X	X

Table 8.10 shows the IT security functions satisfy the TOE security function requirements, complement each other and work as the whole.

Table 8.10 Validity of IT Security Functions to TOE Security Function Requirements

TOE Security Function Requirements	IT Security Functions
FIA_ATD.1a	FIA_ATD.1a is described in regard to SF.LM as follows, which has been realized accordingly. “TOE maintains the attribute information of Storage Navigator (user type, operating authority, SLPR number), and…”
FIA_USB.1a	FIA_USB.1a is described in regard to SF.LM as follows, which has been realized accordingly. “TOE maintains the attribute information of Storage Navigator (user type, operating authority, SLPR number) and associate its attribute with the user account of Storage navigator.”
FIA_ATD.1b	FIA_ATD.1b is described in regard to SF.LM as follows, which has been realized accordingly. “TOE maintains the attribute information of the host (WWN and LU number), and…”
FIA_USB.1b	FIA_USB.1b is described in regard to SF.LM as follows, which has been realized accordingly. “TOE maintains the attribute information of the host (WWN and LU number), and associate its attribute with the host.”
FIA_AFL.1	FIA_AFL.1 is described in regard to SF.SN as follows, which has been realized accordingly. “TOE executes the identity authentication of Storage Navigator with User ID and Password prior to the operation of the other security functions. When the identity authentication failed 3 times continuously, the identity authentication of the corresponding user is denied for 1 minutes.”
FIA_SOS.1a	FIA_SOS.1a is described in regard to SF.SN as follows, which has been realized accordingly. “TOE restricts the password to be entered for the identity authentication of Storage Navigator as: from 6 to 256 single byte uppercase and lowercase English letters, single byte numeric values, and single byte symbols of 32kinds: !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~, and…”
FIA_UAU.2	FIA_UAU.2 is described in regard to SF.SN and SF.ROLE as follows, which has been realized accordingly. • SF.SN “TOE executes the identity authentication of Storage Navigator with User ID and Password prior to the operation of the other security functions. And…” • SF.ROLE “TOE executes the identity authentication with the user ID and the password of the remote desktop connection, when the maintenance staff connects to the SVP.”

TOE Security Function Requirements	IT Security Functions
FIA_UAU.7	FIA_UAU.7 is described in regard to SF.SN as follows, which has been realized accordingly. “TOE restricts the password to be entered for the identity authentication of Storage Navigator as: from 6 to 256 single byte uppercase and lowercase English letters, single byte numeric values, and single byte symbols of 32kinds: !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~, and then displays as “*” on the screen in place of the actual password.”
FIA_UID.2	FIA_UID.2 is described in regard to SF.FCSP, SF.SN, and SF.ROLE as follows, which has been realized accordingly. • SF.FCSP “TOE executes the identity authentication of the host by FC-SP with the WWN and the secret prior to the operation of the other security functions that are related to the access from the host. And…” • SF.SN “TOE executes the identity authentication of Storage Navigator with User ID and Password prior to the operation of the other security functions. And…” • SF.ROLE “TOE executes the identity authentication with the user ID and the password of the remote desktop connection, when the maintenance staff connects to the SVP.”
FMT_MSA.1	FMT_MSA.1 is described in regard to SF.ROLE as follows, which has been realized accordingly. “LM Access Control SFP” consists of the following rules: • LM Access Control SFP” restricts the operation of creating, modifying, deleting, and referring of LU path information (WWN, LU number, LDEV number), based on the user type and the operating authority.” • LM Access Control SFP” restricts the operation of creating, deleting, referring of logical partition information (SLPR number), based on the user type, the operation authority, and the SLPR number.” • LM Access Control SFP” restricts the operation of setting, modifying, referring of user authority information of the Storage Navigator (User type, Operating authority, SLPR number), based on the user type and the operation authority.”

TOE Security Function Requirements	IT Security Functions
FMT_MSA.3	FMT_MSA.3 is described in regard to SF.LM as follows, which has been realized accordingly. “LM Access Control SFP” consists of the following rule: • When and LDEV is created, “LM Access Control SFP” gives a limited default value as the access attribute. It means that the access from the host is limited because there is no LU path information when an LDEV is created.”
FMT_MTD.1	FMT_SMF.1 is described in regard to SF.ROLE as follows, which has been realized accordingly. “TOE has the following control functions: • TOE manages user ID, password, user type, operating authority, and SLPR number of the user account by the Storage Navigator account managing function. And… • TOE manages the user ID and the password when the maintenance staff connects the remote desktop. And… • TOE manages WWN and the secret, which is the authentication data of the host, by the FC-SP functions of Storage Navigator. And…”
FMT_SMF.1	FMT_SMF.1 is described in regard to SF.ROLE as follows, which has been realized accordingly. “TOE has the following control functions: • TOE manages user ID, password, user type, operating authority, and SLPR number of the user account by the Storage Navigator account managing function… • TOE manages the user ID and the password when the maintenance staff connects the remote desktop. And… • TOE manages WWN and Secret, which is the authentication data of the host, by the FC-SP functions of Storage Navigator. And…”
FMT_SMR.1	FMT_SMR.1 is described in regard to SF.ROLE as follows, which has been realized accordingly. “TOE maintains the roles (the account administrator, the storage administrator, the account partition administrator, the storage partition administrator, the audit log administrator, the maintenance staff, and the storage user).”

TOE Security Function Requirements	IT Security Functions
FCS_COP.1	FCS_COP.1 is described in regard to SF.SN as follows, which has been realized accordingly. “SSL provides the server by the public key cryptographic method, the authentication between clients, the cryptography data by the common key cryptographic method, the identity securement of the data by hash function.”
FCS_CKM.1	FCS_CKM.1 is described in regard to SF.SN as follows, which has been realized accordingly. “SSL provides the server by the public key cryptographic method, the authentication between clients, the cryptography data by the common key cryptographic method, the identity securement of the data by hash function. The cryptography operation to be used at SSL is listed on Table 5.13. The cryptography algorithm and the key size are determined by the negotiation between the Storage navigator and the SVP, and…”
FCS_CKM.2	FCS_CKM.2 is described in regard to SF.SN as follows, which has been realized accordingly. “SSL provides the server by the public key cryptographical method, the authentication between clients, the cryptography data by the common key cryptographic method, the identity securement of the data by hash function. The cryptography algorithm and the key size are determined by the negotiation between the Storage navigator and the SVP, and…”
FCS_CKM.4	FCS_CKM.4 is described in regard to SF.SN as follows, which has been realized accordingly. “The cryptography algorithm and the key size are determined by the negotiation between the Storage navigator and the SVP, and the key is erased from the memory once it is used.”
FIA_SOS.1b	FIA_SOS.1b is described in regard to SF.FCSP as follows, which has been realized accordingly. “TOE restricts the entry of secret setting to be used for the identity authentication of the host by FC-SP as: from 12 to 32 of single byte uppercase and lowercase English letters, single byte numeric values, single byte spaces, and single byte symbols of 12 kinds: .-+@_=:/[],~.”
FIA_UAU.1	FIA_UAU.1 is described in regard to SF.FCSP as follows, which has been realized accordingly. “TOE, when the host identity authentication is existed, creates the DH-CHAP authentication code when it received the security authentication executing command from the host, and then send it back to the host.”

TOE Security Function Requirements	IT Security Functions
FIA_UAU.5	FIA_UAU.5 is described in regard to SF.FCSP, SF.SN, and SF.ROLE as follows, which has been realized accordingly. • SF.FCSP "The connection between the host and the storage device is permitted when the secret received from the host meets the secret that TOE holds." • SF.SN "TOE executes the identity authentication of Storage Navigator with User ID and Password prior to the operation of the other security functions. And…" • SF.ROLE "TOE executes the identity authentication with the user ID and the password of the remote desktop connection, when the maintenance staff connects to the SVP."
FMT_MOF.1	FMT_MOF.1 is described in regard to SF.ROLE as follows, which has been realized accordingly. "TOE restricts the setting operation, which is existing or not existing of the host identity authentication, by FC-SP, based on the user type and the operating authority."
FDP_ACC.1	FDP_ACC.1 is described in regard to SF.LM as follows, which has been realized accordingly. ""LM Access Control SFP" consists of the following rules: • Accessing LDEV is authorized if the WWN and the LU number meet the LU path information which is the security attribute of the corresponding object. If the LU path information does not meet, the access is denied. • When the process acting on behalf of the Storage Navigator creates or deletes a SLPR, only the storage administrator can create or delete a SLPR in accordance with the "Storage Navigator user authority information" (user type, operating authority, SLPR number of the Storage Navigator) which is passed to the process acting on behalf of the Storage Navigator. • When the process acting on behalf of the Storage Navigator create or delete an LDEV, the storage administrator can create or delete the all of LDEVs in accordance with the "Storage Navigator user authority information" (user type, Operating authority, SLPR number of the Storage Navigator) which is passed to the process acting on behalf of the Storage Navigator. The storage partition administrator can create or delete an LDEV in the logical partition where meets the SLPR number assigned for the storage partition administrator."

TOE Security Function Requirements	IT Security Functions
FDP_ACF.1	FDP_ACF.1 is described in regard to SF.LM as follows, which has been realized accordingly. ““LM Access Control SFP” consists of the following rules: • Accessing LDEV is authorized if the WWN and the LU number meet the LU path information which is the security attribute of the corresponding object. If the LU path information does not meet, the access is denied. • When the process acting on behalf of the Storage Navigator creates or deletes a SLPR, only the storage administrator can create or delete a SLPR in accordance with the “Storage Navigator user authority information” (user type, operating authority, SLPR number of the Storage Navigator) which is passed to the process acting on behalf of the Storage Navigator. • When the process acting on behalf of the Storage Navigator create or delete an LDEV, the storage administrator can create or delete the all of LDEVs in accordance with the “Storage Navigator user authority information” (user type, Operating authority, SLPR number of the Storage Navigator) which is passed to the process acting on behalf of the Storage Navigator. The storage partition administrator can create or delete an LDEV in the logical partition where meets the SLPR number assigned for the storage partition administrator.”
FAU_GEN.1	FAU_GEN.1 is described in regard to SF.AUDIT as follows, which has been realized accordingly. “TOE has the following audit function. • Creating the audit logs when the auditable event related on the security function of TOE occurs. And…”
FAU_GEN.2	FAU_GEN.2 is described in regard to SF.AUDIT as follows, which has been realized accordingly. “TOE has the following audit function. • Creating the audit logs when the auditable event related on the security function of TOE occurs. In the audit log to be created, add the user ID of the user account which made the cause of this auditable event. And…”

TOE Security Function Requirements	IT Security Functions
FPT_STM.1	FPT_STM.1 is described in regard to SF.AUDIT as follows, which has been realized accordingly. "TOE has the following audit function. • Creating the audit logs when the auditable event related on the security function of TOE occurs. In the audit log to be created, add the user ID of the user account which made the cause of this auditable event. In addition, the date and time used at the time of creating audit log is based on the one managed by the OS on the SVP."
FAU_SAR.1	FAU_SAR.1 is described in regard to SF.AUDIT as follows, which has been realized accordingly. "TOE has the following audit function. • The person who are able to download the audit log is only the audit log administrator."
FAU_STG.1	FAU_STG.1 is described in regard to SF.AUDIT as follows, which has been realized accordingly. "TOE has the following audit function. • There is no role who are able to modify or delete the audit log illegally."
FAU_STG.3	FAU_STG.3 is described in regard to SF.AUDIT as follows, which has been realized accordingly. "TOE has the following audit function. • Display a message that the audit log exceeds the line of 175,000 at the point of audit log exceeds the 175,000 lines on the Storage Navigator, and persuade the user to download the audit log."

TOE Security Function Requirements	IT Security Functions
FPT_RVM.1	FPT_RVM.1 is described in regard to SF.LM, SF.FCSP, SF.SN, and SF.ROLE as follows, which has been realized accordingly. • SF.LM “TOE assures that the “LM access control SFP” is applied when the functions of TOE are executed.” • SF.FCSP “TOE assures that, it calls SF.FCSP when the host connects to the storage device and executes the identity authentication of the host.” • SF.SN “TOE assures that, it calls SF.SN before the management operations of the storage device using Storage Navigator by the user of Storage Navigator, and executes the cryptography communication by the SSL and the identity authentication for the user of Storage Navigator.“ • SF.ROLE “TOE assures that, it calls SF.ROLE when the user of Storage Navigator executes the management operation, and do not execute the out of authorized managing operations by the user type and the operating authority of Storage Navigator.” • SF.AUDIT “TOE assures that, it calls SF.AUDIT when an auditable event occurs, and the audit log is to be generated.”
FPT_SEP.1	FPT_SEP.1 is described in regard to SF.LM, SF.FCSP, SF.SN, SF.ROLE, and SF.AUDIT as follows, which has been realized accordingly. “TSF, which is related to the SF.XXXX, protects the own and assures that the interruption or falsification executed by the unreliable subject will not happen.”

8.3.2 Rationale for the Level of TOE Function Strength

In this TOE, the security functions based on the stochastically or permutating mechanism are SF.FCSP and SF.SN. The security function strength of the SF.FCSP and SF.SN are specified “SOF-Basic” on the section 6.2. On the other hand, the minimum function strength level of the TOE is specified “SOF-Basic” on the section 5.1.2. Therefore, the both are consistent.

8.3.3 Rationale for Assurance Measures

The assurance measures described in Table 6.4 are the names of the documents that imply they satisfy the equivalent security assurance requirements, and the security assurance requirements and the assurance measures correspond to each other. The additional remarks are described below, regarding the assurance measures.

- ADO_IGS.1 describes four manuals, whose only difference is that the below two manuals are English version that corresponds to the above two Japanese version manuals, and their contents are the same.
- AGD_ADM.1 describes two manuals, whose only difference is that one is in Japanese and the other in English, and their contents are the same.
- AGD_USR.1 describes two manuals, whose only difference is that one is in Japanese and the other in English, and their contents are the same.

As described above, those documents show that each assurance measure can be traced to TOE security assurance requirements, and that all the TOE security assurance requirements can be satisfied by implementing all the assurance that have been described.

8.4 PP Claims Rationale

This ST does not claim for any PP.

9 Reference

- Common Criteria for Information Technology Security Evaluation
  Part 1: introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements, Version2.3, August 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003
- Common Criteria for Information Technology Security Evaluation
  Part 1: introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001
  Japanese translated version 1.0, December 2005, Information-Technology Promotion Agency, Japan
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements, Version2.3, August 2005, CCMB-2005-08-002
  Japanese translated version 1.0, December 2005, Information-Technology Promotion Agency, Japan
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003
  Japanese translated version 1.0, December 2005, Information-Technology Promotion Agency, Japan
- Interpretations-0512, December 2005, Information-Technology Promotion Agency, Japan