Hitachi Unified Storage110 Microprogram Security Target

Revision 1.2

September 25, 2013

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

HITACHI
Inspire the Next

Contents

1 ST overview

1.1 ST identification

Title:	Hitachi Unified Storage 110 Microprogram Security Target
Revision:	1.2
Issued on:	September 25, 2013
Prepared by:	Hitachi, Ltd.
Keywords:	disk array, shared disk array, storage, SAN

1.2 TOE identification

TOE identification:	Hitachi Unified Storage110 Microprogram
Version:	0917/A
Developed by:	Hitachi, Ltd.

1.3 TOE description

1.3.1 TOE type

This TOE is a control program (software) operating in the disk array subsystem. The disk array subsystem means Hitachi Unified Storage 110, developed by Hitachi, Ltd. This disk array subsystem is henceforth called HUS. The TOE constitutes a part of HUS and controls access to its storage areas from multiple host computers connected. HUS is a product family, and its variants are distinguished by digits accompanying the product name. In this ST, HUS means the specific product that is followed by the digits “110”.

1.3.2 TOE use and key security features

(1) TOE use and configuration

[HUS Description]

TOE is software that constitutes HUS. First, description of HUS that includes the TOE is described here.

HUS is a storage product of disk array subsystem for the midrange, provided by Hitachi, Ltd. Satisfying the customers' requirements, scalable disk array subsystem can be configured, with up to 960 drives mounted (one drive can accommodate 3TB) in the top-end configuration. To address multiple failures of disk drives, it supports redundant configuration using RAID (RAID0/RAID1/RAID1+0/RAID5/RAID6), however, features related to the RAID configuration are not included in TOE security features.

Figure 1-1 shows an IT environment configuration where HUS is used. TOE is software stored in the HUS; not shown in the figure.

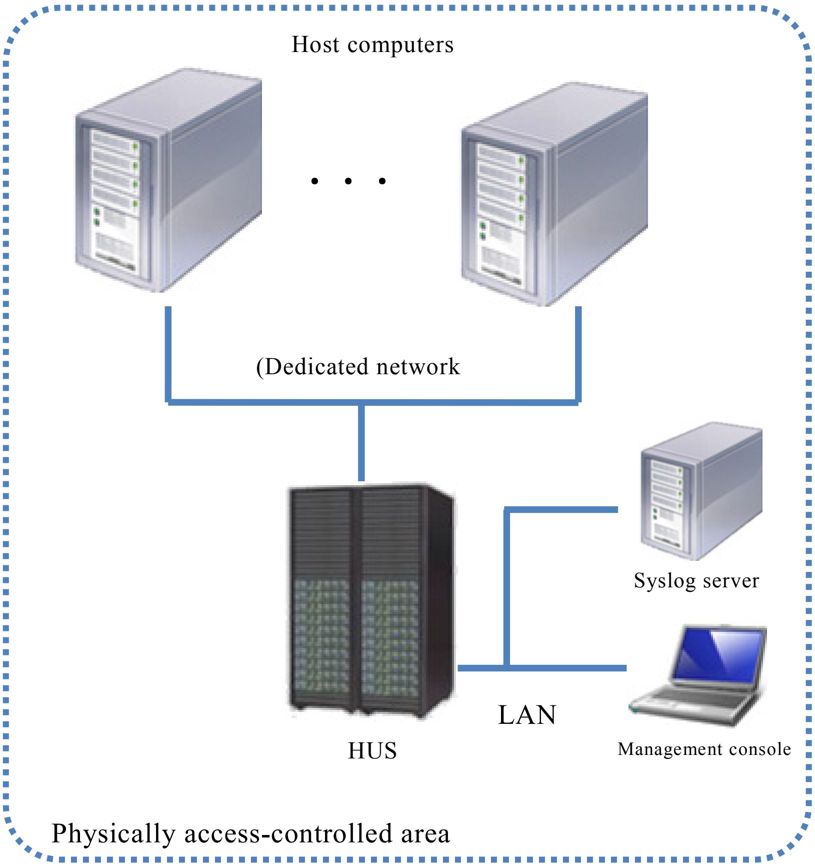

Figure 1-1 HUS and IT environment

HUS is connected with multiple host computers via a dedicated network and serves as high-capacity disk array subsystem that supports RAID configuration. It is assumed that host computers, HUS, and dedicated network that interconnect them are used in a physically and logically access-controlled secure environment.

FC-SAN and IP-SAN are available for a dedicated network. FC-SAN (Fibre Channel Storage Area Network) utilizes optical fiber cable and IP-SAN (IP Storage Area Network) uses SCSI protocol on IP network such as Ethernet.

HUS has 8 to 16 connecting ports for dedicated network. Multiple host computers can be connected to each port in both FC-SAN and IP-SAN. Users are encouraged to select the appropriate network configuration for its use because the number of host computers connectable to the network and the amount of data transmission capacity differs depending on the type of network.

In FC-SAN, one port accommodates up to 128 host groups and one host group accommodates up to 128 host computers (accurately, network interfaces). Host group means a group that consists of multiple host computers running on the same OS. In IP-SAN, one port accommodates up to 255 host computers. These figures are theoretical maximum value, not guaranteeing the number of devices that can be used simultaneously. Regardless of the type of network, appropriate network must be configured considering transmission rate and data transmission amount required for host computers. The guidance that comes with HUS discusses the details.

Host computers that use HUS are not limited to any specific models or types. HUS can accommodate host computers running on the various OSs including Windows, HP-UX, and Solaris.

Each host computer is assigned a dedicated storage area in the disk array. This storage area is a logical storage area that is configured in the physical disk array and recognized as one volume by host computers. Logical storage area assigned to one host computer is logically separated from storage areas of other host computers, preventing mutual interference. Host computers cannot access storage areas other than those assigned. FC-SAN and IP-SAN are respectively evaluated by the configuration that uses 2 host computers.

In Figure 1-1, management console is connected with HUS via the LAN. The LAN is configured with Ethernet and used within a physically and logically access-controlled area. In the figure, only one HUS is used as disk array subsystem, however, multiple disk array subsystems and other peripheral devices share the LAN in an actual operational environment. Also not shown in the figure are servers that may be connected, commonly managing audit log data of HUS and other devices etc. These devices are not users of the TOE, not affecting the TOE security features.

HUS provides the interface for maintenance personnel (not shown in Figure 1-1). Maintenance personnel play role of maintaining HUS parts. In maintenance work, part of the TOE functionality is used to read information about HUS parts. The TOE does not identify or authenticate users who use this function but recognize them as unknown users. (See (2) (b) in [TOE description] later) It makes it possible to perform maintenance to change TOE setting and/or configuration by the defined procedure, however, it is excluded from the assurance since such maintenance and the resulting environment are out of the evaluation configuration of ISO/IEC15408 certification.(Defined procedure*: Refer to Section 3.1 of Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide. (For Maintenance personnel Version))

HUS provides functions for collecting trace information via management console. Trace information contains hardware status of the devices and versions and status of internal software including TOE, and is output to management console. Trace information is collected by maintenance personnel when a failure (malfunction) occurs in a device and used for analyzing its cause.

[TOE description]

Next, the TOE, which operates in HUS, is described here. HUS, as disk array subsystem, provides dedicated data storage areas to multiple host computers. A large number of physical disk drives in HUS are integrated into one logical storage area and it is divided into dedicated storage areas for each host computer and assigned. This control is performed by the TOE. Host computers correspond to users who use the TOE service. Administrators described later are also the TOE users.

The TOE assigns prepared logical storage area for each host computer on physical disk drive storage media in HUS. Host computers can use assigned storage areas exclusively, but the TOE prohibits them from accessing storage areas for other host computers. To manage and control storage areas securely, the TOE provides security functionality, with Organizational security policies considered.

Integrating a large number of host computer storage devices into disk arrays to build shared resources enables not only efficient use of storage devices but also integrated operation and maintenance work, and security operations. This provides many benefits that make overall system economical, efficient and reliable, and so on.

(2) Key security features

HUS containing the TOE is used in a secure operational environment where all the connected host computers, the dedicated network and the management consoles where host computers are connected, and the LAN where management consoles are connected, are physically and logically access-controlled (Users must prepare such operational environment). In this operational environment, physical and logical attacks are prohibited to the TOE and its key IT environment. TOE security features alleviate the security risks to the TOE caused by operation and maintenance Key security features of the TOE are shown in the following (a) to (c).

(a) Exclusive control of storage areas

This generates logical storage areas controlled by the TOE in physical storage areas provided by disk drive storage media (included in HUS, but is not the TOE), and assigns the exclusive logical storage areas to each host computer, which corresponds to a TOE user.

(b) User management

TOE users are divided into two groups: host computers and HUS users (also TOE administrators in this ST and maintenance personnel). This user management function deals with the administrators. By identifying and authenticating administrators, and assigning those permissions corresponding to their roles, it realizes secure operational administrations of the TOE resources. The TOE provides three types of administrators' roles: Account Administrator, Storage Administrator, and Audit Log Administrator. Each role is further divided into two groups: those who can only view the setting data and those who can view and modify the setting data. This means that the TOE has six types of administrators' roles in total.

In this regard, however, the use of readout permission by Account Administrators and Storage Administrators is a basic function; thus, it is not a target of this function.

Also, a TOE function is utilized when HUS users read HUS configuration parts information. TOE treats HUS users as anonymous users since the TOE does not manage HUS users individually. HUS users can read only the limited information without being identified and authenticated by the TOE.

(c) Audit

The TOE records operations of the TOE by users (administrators) in the audit trail as audit log data. Audit log data can be read from the TOE and transferred to an external Syslog server.

1.3.3 Hardware/software/firmware other than TOE

Hardware/software/firmware that are required for the TOE are described here.

[HUS]

The TOE is software operating in HUS, which is a disk array system. The TOE requires low-level hardware for the operational environment of the TOE. Disk drives are used as storage media resources for HUS to serve as disk array system. Users in Japan do not need to prepare these additional TOE operational environments as they are included in HUS, which is a unified disk array subsystem. For international users, files that contain the TOE and its OS, manuals, and hardware including disk drives are provided (shipped). They should prepare TOE operational environments according to the preparation procedures and the user's guidance.

HUS is a product family including “Hitachi Unified Storage 100” as described in 1.3.1. Table 1-1 shows key IT environment configuration elements used in the TOE.

Table 1-1 Key IT environment used in TOE

Component	Description
Control hardware	HT-4017-XSS/XSL/XSSA/XSLA(DF850XS)※
Disk drive unit	HT-F4017-DBS/L (Drive units that accommodate 24 units of 2.5-inch drives/12 units of 3.5-inch drives/48 units of 3.5-inch drives)

※ XSS/XSSA accommodates 24 units of 2.5-inch drives. XSL/XSLA accommodates 24 units of 3.5-inch drives. This means that you do not necessarily connect disk arrays. Also note that XSS/XSL supports (only) Fibre Channel for host connection interface. XSSA/XSLA supports (only) iSCSI for host connection interface.

[Management console]

PC is used for managing the TOE. This PC is a general product in which Windows XP SP3 is used as OS and the WEB browser (IE ver.8.0) runs, but it features the dedicated utility program (Hitachi Storage Navigator Modular 2), which is used by administrators to use the TOE services. This utility program is provided for users with HUS, as it is essential software to utilize the services (management functions) that the TOE provides. Details of management console are described in the guidance that comes with HUS.

The version of the dedicated utility program (Hitachi Storage Navigator Modular 2) for using services of the TOE is shown below. It is necessary to use the utility program shown as below (Hitachi Storage Navigator Modular 2) to uniform the operational environment and the evaluation configuration.

Name:	Hitachi Storage Navigator Modular 2
Version:	21.70
Developer:	Hitachi, Ltd.

[Host computers]

Host computers that use HUS services correspond to the TOE users. Host computers use disk array function that is provided by HUS via the connection control process of the TOE. HUS can support various OSs of host computers, such as Windows, HP-UX, Solaris, Linux, and AIX, but they are independent from the TOE security functionality. Details of host computers are described in the guidance that comes with HUS.

[Details of IT environment]

To use HUS including the TOE, the configuration of dedicated network and disk drives, etc., needs to be designed appropriately. Details of these IT environments are described in the guidance that comes with HUS.

1.4 TOE description

1.4.1 TOE and its IT environment

First, the relationship between HUS, which is a unified IT product, and the TOE, which operates in it, is described.

The TOE is software that operates in HUS. Figure 1-2 is a diagram showing the TOE and its IT environment. The TOE builds logical storage areas on the disk drives mounted on HUS, divides logical storage areas for each host computer connected to HUS and assigns them, and controls host computers to exclusively use their storage areas.

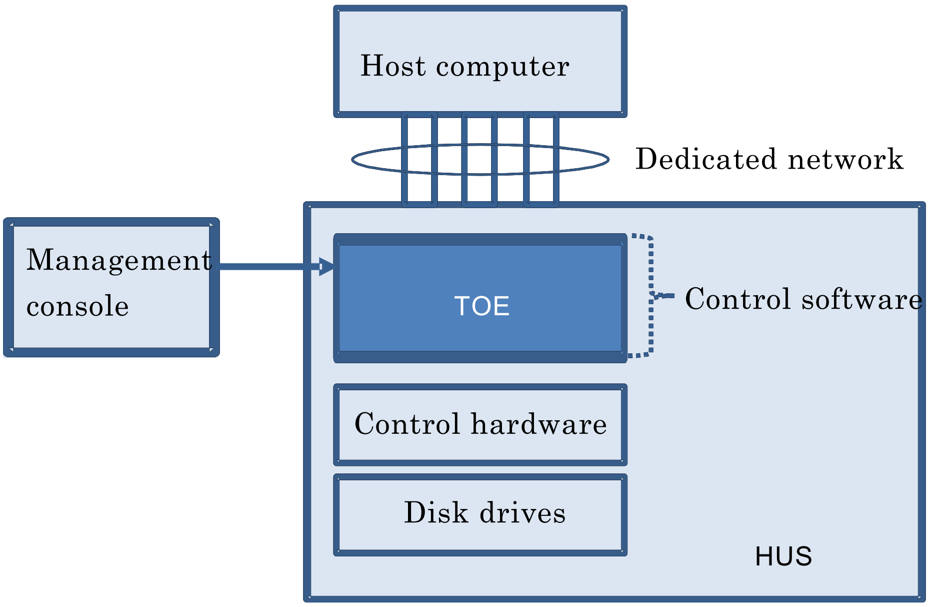

Figure 1-2 TOE and its IT environment

In Figure 1-2, multiple host computers are collectively shown as "host computers". Each host computer is connected to HUS via a dedicated network, one of the two types: FC-SAN or IP-SAN, which are described in 1.3.2 (1), and uses logical storage areas built on disk drives, being controlled by the TOE.

The TOE is called the control software. The control software operates on the control hardware. Disk drives are managed by these control software and control hardware to make the assigned storage area resources available to host computers.

Next, the connection control between host computers and logical storage areas built on disk drives is described using Figure 1-3.

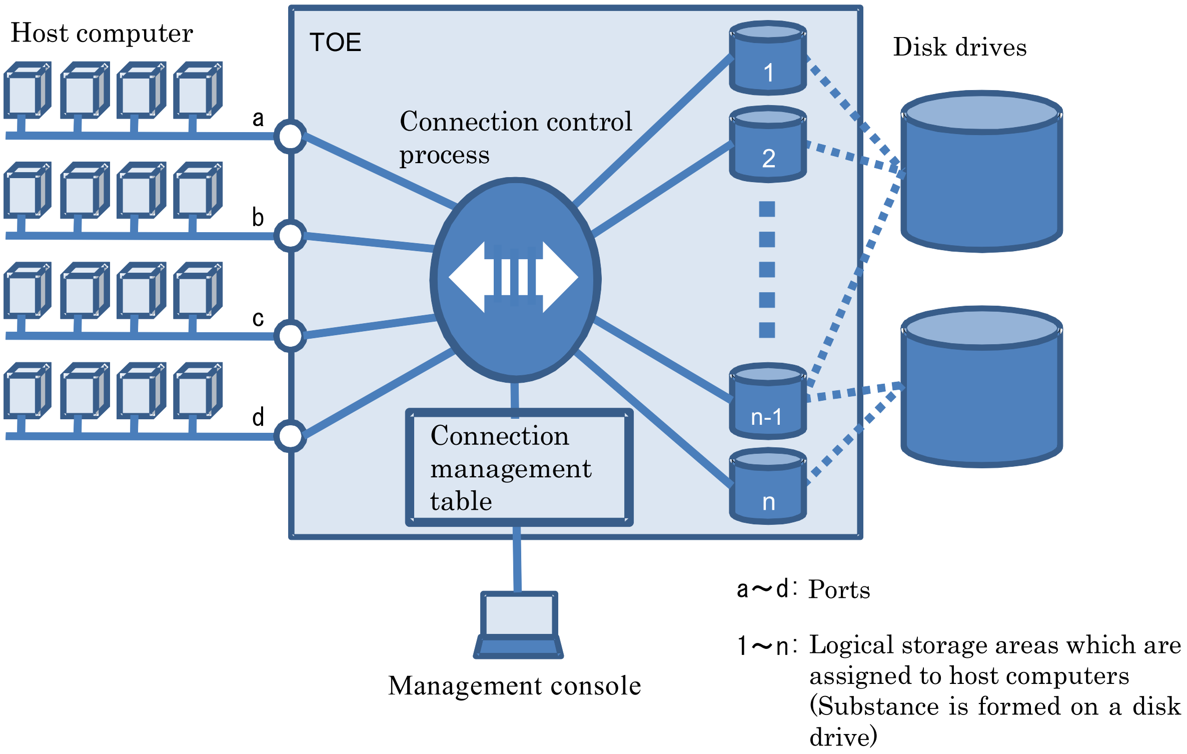
Host computer
TOE
Disk drives
a
b
c
d
Connection control process
1
2
n-1
n
Connection management table
Management console
a～d: Ports
1～n: Logical storage areas which are assigned to host computers (Substance is formed on a disk drive)

Figure 1-3 Connection control between host computers and logical storage areas

In Figure 1-3, ports (a - d) of the TOE accommodate host computers via a dedicated network. In the TOE, the connection control process receives requests from each host computer and accesses logical storage areas (1 - n) assigned exclusively to each host computer based on the requests. The connection control process is the subject (active entity) in the TOE, and logical storage areas (1 - n) are the objects (passive entities) in the TOE. These logical storage areas are built on physical storage areas on disk drive storage media and associated with host computers by the TOE Security Functionality (TSF).

Host computers send requests towrite/read data to the connection control process. Upon receiving requests, the connection control process refer to the connection management table to associate host computers with logical storage areas, accesses logical storage areas assigned to host computers to write/read data, and returns its result to the host computers. Multiprocessing is performed for these operations by the connection control process and multiple host computers' requests are processed simultaneously. Host computers can use the assigned storage areas exclusively, but accessing to other storage areas is prohibited by the TSF.

The correspondence between host computers and logical storage areas can be changed by modifying the connection management table by administrators (Storage Administrators). The connection management table is modified using the management console.

1.4.2 Physical boundaries

The physical TOE consists of the following (a) and (b).

(a) Hitachi Unified Storage 110 Microprogram

(b) User's guidance: detailed in Table 1-2

Table 1-2 User's guidance

Type	Document	Edition number
Program Product User's guide	Hitachi Unified Storage 100 Account Authentication User's Guide (Japanese: Account Authenticationユーザーズガイド（HUS100 シリーズ）)	5th
	Hitachi Unified Storage 100 Audit Logging User's Guide (Japanese: Audit Loggingユーザーズガイド　(HUS100 シリーズ）)	5th
	Hitachi Unified Storage 100 LUN Manager User's Guide (Japanese: LUN Managerユーザーズガイド　（HUS100 シリーズ）)	4th
Disk array User's guide (with maintenance)	Hitachi Unified Storage 100 Series Disk Array System User’s Guide (Japanese: HUS100シリーズディスクアレイ ユーザーズガイド)	6th
	Hitachi Unified Storage 100 Series Disk Array System Service Guide (Japanese: HUS100シリーズディスクアレイ サービスガイド)	6th
Disk array User's guide (without maintenance)	Hitachi Unified Storage 110 Disk Array System User’s Guide (Japanese: Hitachi Unified Storage 110 ディスクアレイ ユーザーズ ガイド)	6th
Hitachi Storage Navigator Modular 2 User's Guide	Hitachi Storage Navigator Modular 2（for GUI）User's Guide (Japanese: Hitachi Storage Navigator Modular 2（for GUI）　ユーザーズガイド)	54th
	Hitachi Storage Navigator Modular 2（for CLI）　User's Guide (Japanese: Hitachi Storage Navigator Modular 2（for CLI）　ユーザーズガイド)	58th
Host Installation Guide	Hitachi Unified Storage 100Series Host Installation Guide for Fibre Channel Connection (Japanese: Hitachi Unified Storage 100シリーズ Fibre Channel接続用 ホストインストールガイド)	3rd
	Hitachi Unified Storage 100 Series Host Installation Guide for iSCSI Connection (Japanese: Hitachi Unified Storage 100シリーズ	2nd

	iSCSI接続用　ホストインストールガイド)	
Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide	Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Administrators/Users) (Japanese: Hitachi Unified Storage 100 ISO/IEC15408認証取得機能取扱説明書(管理者/利用者編))	2nd
	Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Maintenance) (Japanese: Hitachi Unified Storage 100 ISO/IEC15408認証取得機能取扱説明書(保守員編))	1st

The above (a) corresponds to the TOE in Figure 1-2. In Figure 1-2, components other than the TOE are IT environments of the TOE.

The above (b) are guidance documents that come with HUS. Operations and managements of the TOE and its IT environments are covered in these documents.

1.4.3 Logical boundaries

The following (a) to (c) are security functions provided by the TOE.

(a) Exclusive control of storage area

The TOE manages physical storage areas provided by disk drive storage media (outside of the TOE) as logical storage areas in the TOE. It assigns logical storage areas to each host computer and controls access to disk drives by host computers so that assigned storage areas can be used as exclusive volumes for each host computer.

Access control between host computers and disk drives is performed based on the information of the connection management table in the TOE. The information of the connection management table is managed by administrators who have the Storage Administrator role. This role includes generating a logical storage area for each host computer and setting initial values of access permission.

(b) User management

TOE users who are targets of the user management function are administrators with the following divided six roles (permission group). Host computers are also TOE users, but they are not administrators and not targets of this function. User management function 1) identifies and authenticates users, and 2) grants authorized users permissions to use the TOE resources according to the permission group.

The roles of users (administrators) management by the TOE are divided into the following three groups, and each group is further divided into two groups: those who have View permission and those who have View and Modify permissions. Thus, there are six administrator's roles in total.

- Account Administrator administrates accounts of all the administrators
- Storage Administrator administrates storage area assignment of host computers
- Audit Log Administrator administrates settings of the audit trail related to TOE security functionality

However, the use of View permission by Account Administrators and Storage Administrators is a basic function, and it is not included in this function.

The TOE functions are used when HUS users read HUS configuration part information. HUS users, when they read HUS configuration part information are not included in the user management of the TOE, and are treated as anonymous users. The TOE allows them to read only the limited information without identifying and authenticating them.

(c) Audit

The TOE records operations of the TOE by users (administrators) in the audit trail as audit log data. If the size of the audit trail exceeds a prescribed size, the oldest data is overwritten by new data. Recorded audit log data can only be accessed by Audit Log Administrators. Audit log data can be not only read directly from the TOE but also automatically transferred to an external Syslog server (outside of the TOE) according to the TOE settings. If it is transferred to a Syslog server, it is stored in both the TOE and a Syslog server. A Syslog server has more data storage areas to accommodate more data that would be deleted automatically in the TOE by overwriting, enabling it to be stored in a Syslog server for a long time.

2 Conformance claims

2.1 CC conformance claims

This ST and the TOE conform to the CC version 3.1, Revision 3.

The CC that is used in developing the ST is the Japanese version provided by JISEC. They claim conformance as follows:

- Part 2: Security functional components Version 3.1 Revision 3 [Japanese Version 1.0]
- Part 3: Security assurance components Version 3.1 Revision 3 [Japanese Version 1.0]

2.2 PP claims

This ST does not claim conformance to other PPs.

2.3 Package claims

This ST contains the assurance requirements for the TOE from the EAL2 assurance package.

2.4 Rationale

No rationale is provided because this ST does not claim conformance to other PPs.

3 Security problem definition

This section defines security problems related to the TOE. Threats, organizational security policies, and assumptions are given identification name of [T.xxxx], [P.xxxx], and [A.xxxx] respectively.

3.1 Assets

HUS where the TOE is included provides data storage areas exclusively used by host computers connected. The storage areas can be accessed only by the host computers that are registered in HUS to associate with the areas.

The key asset protected by the TOE is the data storage area provision service by HUS. This service provides host computers with the secure use environment for assigned data storage areas. The data storage areas that are used by host computers are protected against other host computers' interferences. The TOE Security Functionality (TSF) and/or data used by TSF (TSF data) are required for the key asset to be kept secure.

3.2 Threats

There is no threat to be countered with regard to this TOE.

3.3 Organizational security policies

P.Exclusive_assign A logical storage area for each host computer is assigned exclusively to each host computer. In other words, the logical storage area used by a host computer does not allow access by other host computers.

P.Audit The TOE records the following event based on operation results by users (administrators) as audit data. Only authorized users can access the audit data. If the audit data storage area becomes full, the oldest data is overwritten by the newest data to prevent loss of new audit data.

- Successful and/or failure events on identification and authentication of users (administrators)
- Successful events on the setting of enabling/disabling audit log data transfer to the Syslog server.

- Successful events for the modified operation against the session timeout value.
- Successful and/or failure events on performing the forced logout procedure of login users (administrators).
- Successful and/or failure events on the operation of either change default, modification, or deletion of information associating host computers with logical storage areas (connection management table)

P.User_role

The TOE distinguishes the following roles of users

- Account Administrator (View and Modify)
- Account Administrator (View Only) (Basic functions are provided.)
- Storage Administrator (View and Modify)
- Storage Administrator (View Only) (Basic functions are provided.)
- Audit Log Administrator (View and Modify)
- Audit Log Administrator (View Only)

Also, the following TOE operations are allowed only for the users who have their permission

- Account Administrator (View and Modify): Settings of accounts for all the administrators, the forced logout for login users
- Account Administrator (View and Modify): Setting the session timeout value
- Storage Administrator (View and Modify): Setting of the access control for disk drive storage media
- Audit Log Administrator (View and Modify): Readout of the audit trail, Setting of enabling/disabling audit log data transfer to the Syslog server
- Audit Log Administrator (View Only): Readout of the audit trails

P.Session_timeout

The TOE forcibly terminates the session of an administrator if the session timeout value specified by Account Administrator (View and Modify) is exceeded during the operation of the TOE by the administrator.

3.4 Assumptions

A.Environment

The TOE and HUS where the TOE resides, will be located in physically and logically access-controlled secure environment, * along with the connected host computers, dedicated network where the host computers are connected, management console, and LAN connected to the management console.

If audit log data of the TOE is transferred to a Syslog server connected to HUS, the transferred audit log data of the TOE will be managed securely so that the security policy of the TOE will not be compromised.

* Physically and logically access-controlled secure environment means a secure area where only Storage Administrators, Account Administrators, Audit Log Administrators, and Maintenance personnel are allowed to enter and leave, and where each network is set directly inaccessible from the external network by firewall, etc.

A.Administrator

The administrators who are TOE users will not perform malicious operations that may compromise the security of the TOE and will follow the instructions provided by the TOE guides to change settings or build configurations.

A.Configuration

The settings related to security functionality of the TOE will be set by administrators for each function to the appropriate settings. In the appropriate settings, all of the following conditions are met.

- Audit functions and identification and authentication function for users (administrators) set up to be enabled.
- Exclusive control of storage area is run

4 Security objectives

This chapter defines the security objectives for the security problems specified in Chapter 3 that are addressed by the TOE or its environment. The security objectives to be addressed by the TOE are described in 4.1, and the security objectives to be addressed by its environment are described in 4.2. Rationale of the appropriateness for these security objectives against security problems is described in 4.3.

The security objectives for the TOE and for the operational environment are shown with identifiers beginning with “O.” or “OE.” respectively.

4.1 Security Objectives for the TOE

This section defines the security objectives to be addressed by the TOE regarding the organizational security policies defined as security problems.

O.Exclusive_access

The TOE will ensure that only designated host computers can access to the exclusively assigned logical storage areas so that it prevents accesses from other host computers.

O.Audit

The TOE must record the following events based on operation results by users (administrators) as audit data. Audit data must be protected from unauthorized access by unauthorized users. The loss of new audit data must be prevented by overwriting the oldest data with new data when the recorded area becomes full.

- Successful and/or failure events on identification and authentication of users (administrators)
- Successful events on the setting of enabling/disabling audit log data transfer to the Syslog server
- Successful events for the modified operation against the session timeout value.
- Successful and/or failure events on the forced logout procedure of login users (administrators).
- Successful and/or failure events on the operation of either change default, modification, or deletion of information associating host computers with logical storage areas (connection management table)

O.User_role

The TOE will maintain the following user roles. To prevent inconsistency in controlling operations, multiple users who have the same role must be prohibited from setting the TOE simultaneously.

- Account Administrator (View and Modify)
- Account Administrator (View and Modify) (Basic functions are provided.)
- Storage Administrator (View and Modify)
- Storage Administrator (View Only) (Basic functions are provided.)
- Audit Log Administrator (View and Modify)
- Audit Log Administrator (View Only)

Also, the following TOE operations are allowed only for the users who have their permissions

- Account Administrator (View and Modify): Setting of accounts for all the administrators, and performing the forced logout for login users
- Account Administrator (View and Modify): Setting of the session timeout value
- Storage Administrator (View and Modify): Setting of the access control for disk drive storage media
- Audit Log Administrator (View and Modify): Readout of the audit trail, and Setting of enabling/disabling audit log data transfer to the Syslog server
- Audit Log Administrator (View Only): Readout of the audit trails

O.Session_timeout The TOE will forcibly terminate the session of an administrator if the session timeout value specified by Account Administrator (View and Modify) is exceeded during the operation of the TOE by the administrator.

4.2 Security objectives for the operational environment

This section defines the security objectives to be addressed by the operational environment of the TOE regarding organizational security policies, which are defined as security problems, and assumptions.

OE.Environment

The TOE and HUS where the TOE resides will be located in physically and logically access-controlled secure environment, * along with the connected host computers, dedicated network where host computers are connected, management console, and LAN connected to the management console.

If audit log data of the TOE is transferred to a Syslog server connected to HUS, the transferred audit log data of the TOE will be managed securely so that the security policy of the TOE will not be compromised.

* Physically and logically access-controlled secure environment means secure area whereonly Storage Administrators, Account Administrators, Audit Log Administrators, and Maintenance personnel are allowed to enter and leave, and where each network is set directly inaccessible from the external network by firewall, etc.

OE.Administrator

To ensure that the administrators who are TOE users do not perform malicious operations that may compromise the security of the TOE, consumers who deploy HUS will assign reliable administrators to change settings or build configurations according to the TOE guidance.

OE.Configuration

The settings related to security functionality of the TOE will be set by administrators for each function to the appropriate settings. In the appropriate settings, all of the following conditions are met.

- Audit function and identification and authentication function for users (administrators) are set up to be enabled.
- LUN Manager is enabled. (=Exclusive control of storage area is run)

4.3 Security objectives rationale

This section provides rationale supporting the effectiveness of the above security objectives against each item of the security problem definitions. In 4.3.1, tracing between each security objective and any of the security problems is described, while4.3.2 explains that, each security problem is effectively addressed by the corresponding security objectives.

4.3.1 Tracing between security problem definition and security objectives

Table 4-1 shows tracing between security problem definitions and security objectives. As shown in this table, all the security objectives trace to one security problems.

Table4-1 Tracing between security problem definition and security objectives

Security Objectives Security problem definition	O.Exclusive_access	O.Audit	O.User_role	O.Session_timeout	OE.Environment	OE.Administrator	OE.Configuration
P.Exclusive_assign	x						
P.Audit		x					
P.User_role			x				
P.Session_timeout				x			
A.Environment					x		
A.Administrator						x	
A.Configuration							x

4.3.2 Security objectives rationale

This subsection provides rationale that security objectives for the TOE and operational environment successfully enforce the organizational security policies, and properly meet the assumptions.

P.Exclusive_assign

O.Exclusive_access covers all the organizational security policies defined in P.Exclusive_assign and properly enforces P.Exclusive_assign.

P.Audit

O.Audit directly supports the organizational security policies defined in P.Audit and properly enforces P.Audit.

P.User_role

O.User_role supports the organizational security policies defined in P.User_role and defines countermeasures to prevent conflicts over users' roles against users' roles to function properly. This security objective properly enforces P.User_role.

P.Session_timeout O.Session_timeout directly supports the organizational security policies defined in P.Session_timeout and properly enforces P.Session_timeout.

A.Environment OE.Environment directly supports the organizational security polices defined in A.Environment and properly addresses A.Environment.

A.Administrator OE.Administrator directly supports the organizational security policies defined in A.Environment and properly addresses A.Environment.

A.Configuration OE.Configuration directly supports the organizational security policies defined in A.Configuration and properly addresses A.Configuration.

5 Extended components definition

This ST does not define extended components definition.

6 Security requirements

6.1 Security functional requirements

The SFRs specified in this ST have been drawn from components described in the CC part 2. Table 6-1 lists the SFRs.

Table 6-1 SFR

6.1.1	FAU_GEN.1	Audit data generation
6.1.2	FAU_GEN.2	User identity association
6.1.3	FAU_SAR.1	Audit review
6.1.4	FAU_SAR.2	Restricted audit review
6.1.5	FAU_STG.1	Protected audit trail storage
6.1.6	FAU_STG.4	Prevention of audit data loss
6.1.7	FDP_ACC.1	Subset access control
6.1.8	FDP_ACF.1	Security attribute based access control
6.1.9	FIA_ATD.1	User attribute definition
6.1.10	FIA_SOS.1	Verification of secrets
6.1.11	FIA_UAU.1	Timing of authentication
6.1.12	FIA_UAU.2	User authentication before any action
6.1.13	FIA_UAU.5	Multiple authentication mechanisms
6.1.14	FIA_UID.1	Timing of identification
6.1.15	FIA_UID.2	User identification before any action
6.1.16	FIA_USB.1	User-subject binding
6.1.17	FMT_MOF.1	Management of security functions behavior
6.1.18	FMT_MSA.1	Management of security attributes
6.1.19	FMT_MSA.3	Static attribute initialization
6.1.20	FMT_MTD.1	Management of TSF data
6.1.21	FMT_REV.1	Revocation
6.1.22	FMT_SMF.1	Specification of Management Functions
6.1.23	FMT_SMR.1	Security roles
6.1.24	FPT_STM.1	Reliable time stamps
6.1.25	FRU_RSA.1	Maximum quotas
6.1.26	FTA_SSL.3	TSF-initiated termination

The SFRs are defined by performing necessary operations to each security functional component. The following conventions are used to describe operations in each SFR.

- Assignment and selection are identified in [assignment: *XXX*(Italics)] and [selection: *XXX*(Italics)] respectively.
- In selectable operations, items not selectable are identified in ~~strike through~~ (strike through).
- In refinement operations, refined parts are identified in ***Italics & Bold***.

The following are SFRs defined in this ST.

6.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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 in Table 6-2*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *none*].

Table 6-2

Auditable event
Successful and/or failure events on identification and authentication of users (administrators)
Successful events on the setting of (enabling/disabling) audit log data transfer to the Syslog server
Successful and/or failure events on the operation of either change default, modification, or deletion of information associating host computers with logical storage areas (connection management table)
Successful events of the operations of delete modifying the following TSF data. • *Session timeout value*
Successful and/or failure events on the forced logout of login users (administrators)

6.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *Audit Log Administrator (View and Modify) and Audit Log Administrator (View Only)*] with the capability to read [assignment: *all the recorded information*] from the audit records.

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

6.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

6.1.6 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: ~~*"ignore audited events"*~~, ~~*"prevent audited events, except those taken by the authorized user with special rights"*~~, *"overwrite the oldest stored audit records"*] and [assignment: *none*] if the audit trail is full.

6.1.7 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *HUS access control SFP*] on [assignment: *list of subject :< connection control process*[*1]*>, objects :< logical storage areas*[*2]*>, and operations :< data write and/or read> among subjects and objects covered by SFP*]

[*1] A process operating in the TOE. Upon receiving requests for data write and read to disk array from each host computer, it executes the requests to TSF-controlled logical storage areas assigned to the host computer and return its result to the host computer. Only one instance is generated in the TOE. It operates consistently while the TOE is in operation and handles all the requests from host computers simultaneously.

[*2] Logical storage areas are controlled by the TSF and built on the storage media of disk drives (outside of the TOE). (One or more) objects corresponding to these are generated for each host computer.

6.1.8 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: *HUS access control SFP*] to objects based on the following: [assignment: *list:<in Table 6-3> 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:<in Table 6-3>*].

Table 6-3

Entity	*Security attribute*
Subject: *Connection control process*	*・ID of the host computer that sent request to the subject* *・Object ID (contained in the request from host computer)*
Object: *Logical storage areas*	*・Object ID* *・Host computer ID*

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: *If an object ID contained in the subject and object match and "ID of the host computer that sent request to the subject" match "host computer ID" contained in the security attributes of the object identified as access target, the subject can perform the* *operation to the object requested by the host computer*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *none].*

6.1.9 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes shown in Table 6-4*].

Table 6-4

User	*Security attribute*
Host computers	・ *Host computer ID* ・ *Object ID (One or more objects are assigned to host computer and their information is maintained being associated with objects.)*
Administrators	・ *ID (Information that can identifies individuals)* ・ *Roles (One of the six roles shown in Table 6-9.; multiple roles can be allowed)* ・ *Authentication status (Information that indicates whether authenticated or not)*

6.1.10 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *six or more characters*].

6.1.11 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *read of HUS configuration information (configuration part type, quantity, status, trace information)*] on behalf of the user to be performed before the user ***who corresponds to the administrator*** 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.

6.1.12 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

6.1.13 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms shown in Table 6-5*] to support 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 shown in Table 6-5*].

Table 6-5

Authentication mechanism	*Authentication target*
By password	*Users who correspond to administrators*
By WWN (World Wide Name), which is the unique number of Fibre Channel HBA (Host Bus Adaptor) in host computer	*Users that correspond to host computers*
By iSCSI NAME, which is the unique information of iSCSI HBA in host computer	*Users that correspond to host computers*
None	*Access via HUS web port (Only specific data defined in FIA_UAU.1/FIA_UID.1 can be read by anonymous users.)*

6.1.14 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *the readout of HUS configuration information (configuration part type, quantity, status, trace information)*] on behalf of the user to be performed before the user ***who corresponds to the administrator*** is identified.

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

6.1.15 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

6.1.16 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attributes definition

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *If the subject receive a write or read request to a disk drive from a host computer, the subject associates the host computer ID with the security attribute of the subject*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *If the subject receives a new request from a host computer, the subject replaces the security attribute associated with the subject by host computer ID associated with the new request after completing the process in progress. A host computer to be associated with the new request can be identical to or different from the previous host computer*].

6.1.17 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: ~~*determine the behavior of*~~, *disable*, *enable*, ~~*modify the behavior of*~~] the functions [assignment: *transferring audit log data to a Syslog server*] to [assignment: *Audit Log Administrator (View and Modify)*].

6.1.18 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *HUS access control SFP*] to restrict the ability to [selection: *see Table 6-6*] the security attributes [assignment: *object ID*, *host computer ID associated with objects*, *information defining logical storage areas of objects*] to [assignment: *administrators in Table 6-6*].

Table 6-6

Administrator	*Selection*
Storage Administrator (View and Modify)	~~*change default, query,*~~ *modify, delete,* ~~*[assignment: other operations]*~~

6.1.19 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

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

FMT_MSA.3.2 The TSF shall allow the [assignment: *Storage Administrator (View and Modify)*] to specify alternative initial values to override the default values when an object or information is generated.

6.1.20 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: ~~change_default, query, modify, delete, clear~~, [assignment: *operations in Table 6-7*]] the [assignment: *list of TSF data in Table 6-7*] to [assignment: *the authorized identified roles in Table 6-7*].

Table 6-7

Role	*TSF data*	*Operation*
Account Administrator (View and Modify)	*User ID*	*Change default, delete*
	User password (All users)	*Change default, modify*
	User roles	*Change default, modify*
	Session timeout	*Modify*
Account Administrator (View Only)	*Own password*	*Modify*
Audit Log Administrator (View and Modify)	*Audit trail*	*Query*
	Own password	*Modify*
Audit Log Administrator (View Only)	*Audit trail*	*Query*
	Own password	*Modify*
Storage Administrator (View and Modify)	*Host computer ID*	*Change default, modify, delete*
	Own password	*Modify*
Storage Administrator (View Only)	*Own password*	*Modify*

6.1.21 FMT_REV.1 Revocation

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_REV.1.1 The TSF shall restrict the ability to revoke [assignment: *security attribute indicating that authentication status is logged-in*] associated with the [selection: *users* ***who correspond to administrators***, ~~*subjects, objects, [assignment: other additional resources]*~~] under the control of the TSF to [assignment: *Account Administrator (View and Modify)*].

FMT_REV.1.2 The TSF shall enforce the rules [assignment: *immediately change the authentication status from logged-in to logged-out to stop TSF-mediated actions on behalf of the user*].

6.1.22 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF in Table 6-8*].

Table 6-8

Management function	*Note: Corresponding FMT class*
Setting of enabling/disabling audit log data transfer to the Syslog server	*FMT_MOF.1*
Management of security attributes associating host computer with logical storage areas (objects)	*FMT_MSA.1*
Setting of security attributes when generating objects	*FMT_MSA.3*
Management of TSF data shown in Table 6-7	*FMT_MTD.1*

6.1.23 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorized identified roles in Table 6-9*].

Table 6-9

Role
Account Administrator (View and Modify)
Account Administrator (View Only)
Storage Administrator (View and Modify)
Storage Administrator (View Only)
Audit Log Administrator (View and Modify)
Audit Log Administrator (View Only)

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

6.1.24 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.25 FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas<***login count "1"***> of the following resources: [assignment: *login count of the same set of user roles*] that [selection: ~~*individual user*~~, *defined group of users*, ~~*subjects*~~] can use [selection: *simultaneously*, ~~*over a specified period of time*~~].

6.1.26 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of the management console inactivity defined by Account Administrator (View and Modify)*].

6.2 Security assurance requirements

The security assurance requirements for this TOE are defined by the assurance components shown in Table 6-10. All of these are included in Part 3 of the CC.

This ST applies no operations to all of the assurance components shown in Table 6-10.

Table 6-10 Assurance components

Assurance class	Assurance component
Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2

	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.2

6.3 Security requirement rationale

6.3.1 Security functional requirements rationale

This subsection provides rationale that the defined SFRs properly address the TOE security objectives. In 6.3.1.1, a tracing that shows SFRs address which security objectives for the TOE is described. In 6.3.1.2, a set of justifications that shows all security objectives for the TOE are effectively addressed by SFRs is described.

6.3.1.1 Relation between security objectives and security functional requirements

The SFRs corresponding to the TOE security objectives are shown in Table 6-11. This table shows rationale that all the SFRs can trace back to at least one TOE security objective.

Table 6-11 Relation between TOE security objectives and SFRs

SFR TOE security objective	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.5	FIA_UID.1	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_REV.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FRU_RSA.1	FTA_SSL.3
O.Exclusive_access							x	x	x			x	x		x	x										
O.Audit	x	x	x	x	x	x														x		x		x		
O.User_role									x	x	x		x	x			x	x	x	x	x	x	x		x	
O.Session_timeout																										x

6.3.1.2 Justification for the tracing

Rational that shows all security objectives for the TOE are met by the corresponding SFRs is described here. Effectiveness of each SFR to meet security objectives for the TOE is also described.

O.Exclusive_access

Logical storage areas of the TOE are assigned on a host computer basis. This assignment is performed by the connection control process i.e., subject in the TOE), receiving access requests to disk drives from host computers and executing the requests to the corresponding logical storage areas (i.e., objects in the TOE).

The TOE identifies and authenticates the host computer to determine the host computer that sent access requests and verify that the host computer is valid one registered in the TOE. This is defined in FIA_UAU.2, FIA_UAU.5 and FIA_UID.2. Upon receiving the request, the TOE subject associates the security attribute of the verified host computer with that of subject. This requirement is defined in FIA_USB.1. Security attribute for each host computer is defined in FIA_ATD.1. The access to disk drive storage areas from host computers is controlled based on the security attributes associated with subjects and objects respectively. This access control requirement is defined in FDP_ACC.1 and FDP_ACF.1.

O.Exclusive_access is properly enforced by these SFRs.

O.Audit

O.Audit defines audit data items to be collected and requires protection of audit data. The requirements of audit log data items to be collected correspond to FAU_GEN.1 and FAU_GEN.2. FAU_GEN.2 requires that user ID be included in audit data. FPT_STM.1 is defined for the requirement for time stamps provided for audit data. FAU_SAR.1 and FAU_SAR.2 are applied to the requirement for allowing only specific users (i.e., Audit Log Administrators) to read audit data. To protect audit data, FAU_STG.1 defines prevention of unauthorized deletion and modification, and FAU_STG.4 defines the prevention of loss when the storage area becomes full. FMT_MTD.1/FMT_SMF.1 defines audit data management by administrator. O.Audit is properly enforced by these SFRs.

O.User_role

FMT_SMR.1 defines requirements for managing six types of user roles by the TOE. Identification and authentication corresponding to roles are required and defined in FIA_UAU.1, FIA_UAU.5, and FIA_UID.1. FIA_SOS.1 is used for test requirements for user authentication. The security attributes of users include roles, the requirements of which are defined in FIA_ATD.1.

The user's operations associated with each role include operations of the TSF data, the requirement of which are defined in FMT_MTD.1/FMT_SMF.1. Account Administrator (View and Modify), one of the roles, administrates authentication status of login users. FMT_REV.1 defines the requirements of discarding security attributes of users whose authentication status is login. Storage Administrator (View and Modify), one of the roles, administrate security attributes related to access control, the requirements of which are defined in FMT_MSA.1, FMT_MSA.3, and FMT_SMF.1. Audit Log Administrators (View and Modify), one of the roles, enables/disables audit log transfer to Syslog server. The requirements are defined in FMT_MOF.1/FMT_SMF.1.

If administrators who have the same role perform administrative operations to the same resources simultaneously, its results become inconsistent. To prevent this, assignment of users to the resources needs to be limited. This requirement is defined in FRU_RSA.1.

O.User_role is properly enforced by these SFRs.

O.Session_timeout

FTA_SSL.3 requires that the interactive session of the administrator account using it be forcibly terminated when the session timeout period of the management console exceeds the predetermined period of time defined by Account Administrator (View and Modify). This covers all the objectives of O.Session_timeout, properly enforcing O.Session_timeout.

6.3.1.3 Security functional requirement dependencies

Table 6-12 shows dependencies defined in each SFR and the satisfaction of them.

In Table 6-12, "Dependent requirement" shows dependencies defined in SFR and "Satisfied by" shows which SFRs meet the defined dependencies. All the requirements on which each SFR depends are satisfied.

Table 6-12 SFR dependencies

SFR	Dependent	Satisfied by

	requirement	
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 and FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FIA_ATD.1	none	–
FIA_SOS.1	none	–
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	–
FIA_UID.1	none	–
FIA_UID.2	none	–
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, and FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_REV.1	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	none	–
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	none	–
FRU_RSA.1	none	–
FTA_SSL.3	none	–

6.3.2 Security assurance requirements rationale

The TOE is operated in secure areas. Host computers that use the TOE services and network that connects the TOE and host computers are also placed in the same environment. The environment where the TOE resides is relatively undisturbed, lowering necessity for considering the probability of being attacked for a long period of time. The external interface of the TOE is limited, lowering probability of internal structure vulnerability being exploited. Furthermore, attacks against the TOE development environment are considered to be limited.

Given these characteristics of the TOE, EAL2 is suitable for security assurance requirement.

7 TOE summary specification

7.1 Summary of measures for security functional requirements

This section provides summary the measures for security functional requirements for the TOE. These measures are described by each SFR listed in 6.1.

7.1.1 FAU_GEN.1/FAU_GEN.2

Date and time of start-up and shutdown of the audit functions are recorded. Furthermore, the following information is recorded when the events shown in Table 7-1 occur due to triggered security functions to be audited.

[Information contained in audit data]

- Event date & time
- Event type
- User (administrator) ID
- Event results (success or failure)

Table 7-1 Audit events to be recorded

SFR	Audit event
FIA_UAU.1/FIA_UID.1	Successful and/or failure events on triggered mechanisms of identification and authentication of users (Target users are administrators)
FMT_MOF.1	Successful events on the settings of (enabling/disabling) audit log data transfer to the Syslog server
FMT_MSA.1/FMT_MSA.3	Successful and/or /failure events on the operation of either change default, modification, or deletion of information associating host computers with logical storage areas (connection management table)
FMT_MTD.1	*Successful events of the operations of modifying the following TSF data.* - Session timeout value
*FM*T_REV.1	Successful and/or /failure events on the forced logout of login users (administrators)

7.1.2 FAU_SAR.1/FAU_SAR.2

The TOE shall identify and authenticate users (administrators) at login to provide only users who have Audit Log Administrator role with the capability to read audit data. Users access audit data in the TOE by using the management console in which the utility program for HUS is installed. Audit data can be read directly from the TOE and transferred to a Syslog server outside of the TOE. Anyone other than Audit Log Administrators reading audit log sent to a Syslog server violates security objectives for the TOE. A Syslog server is outside of the TOE, but its operation and management should be performed so as not to violate security objectives for the TOE.

7.1.3 FAU_STG.1/FAU_STG.4

Up to 2,048 entries of the audit trail (1 entry: 1,024 byte) shall be stored and the oldest data shall be overwritten by new data when the capacity is exceeded.

Audit records (audit data) stored in the audit trail can be collectively read by Audit Log Administrators. The audit function is in operation while the TOE is in operation, prohibiting deletion (initialization) and modification of the audit trail.

7.1.4 FDP_ACC.1/FDP_ACF.1

Access requests (write/read) to the disk array from host computers are processed by the connection control process constantly operating in the TOE. The connection control process receives requests from host computers, compares host computer ID information with the connection control table in the TOE, and executes operations requested to logical storage areas. If the IDs of the host computers are not registered, the request is denied.

7.1.5 FIA_ATD.1

Users who have security attributes are divided into two types: host computers and administrators. Each user has attributes shown in Table 7-2.

Table 7-2 User security attributes

User	Security attribute
Host computer	・ Host computer ID ・ Object ID assigned to a host computer (One or more objects are assigned and its information is managed associated with objects. Requests sent by host computer contain ID of object to be accessed. One object is specified.)
Administrator	・ ID (Information that can identify individual) ・ Roles (Account Administrator [Modify/View], Storage Administrator [Modify/View], Audit Log Administrator [Modify/View]: 6 roles in total); more than one roles can be assigned to individual who has one ID information ・ Authentication status (indicating whether authenticated or not)

7.1.6 FIA_SOS.1

The number of characters is checked when a password is registered by administrators. If the password fails to meet the condition [6 characters], the registration of password is denied.

7.1.7 FIA_UAU.1/FIA_UAU.2/FIA_UAU.5/FIA_UID.1/FIA_UID.2

FIA_UAU.1 and FIA_UID.1 are requirements for identifying and authenticating users corresponding to administrators, FIA_UAU.2 and FIA_UID.2 for identifying and authenticating host computers. FIA_UAU.5 is a requirement for defining the multiple authentication mechanisms for both of the authentications.

[FIA_UAU.1/FIA_UAU.5/FIA_UID.1]

Administrators are identified and authenticated on an individual basis by ID and password. The TOE services are provided for administrators via the management console where the dedicated HUS utility program "Hitachi Storage Navigator Modular 2" is installed. Management consoles are connected to HUS via LAN. The command sent from the management console to the TOE contains user's ID and password, which is allowed to be executed if identification and authentication succeed.

HUS users can read information related to HUS configuration parts (configuration part type, quantity, status, trace information) without being identified and authenticated. It is out of the user management by the TOE if HUS users read HUS configuration parts related information.

[FIA_UAU.2/FIA_UAU.5/FIA_UID.2]

In identification and authentication of host computers, different sets of data are used depending on the HBAs (Host Bus Adaptors) that are mounted on the host computers. Fibre Channel HBA has WWN (World Wide Name), which is a unique number of it and iSCSI HBA has iSCSI Name, which is its unique information. These sets of data are read by the TOE when host computers are registered. If WWN or iSCSI Name contained in the requested data matches the data registered in the TOE, identification and authentication of host computer by the TOE succeeds, and the request from the host computer is accepted.

7.1.8 FIA_USB.1

One connection control process operates constantly in the TOE. If the connection control process receives a request from a host computer and identifies and authenticates the host computer by WWN or iSCSI Name contained in the request, it associates the identification information with its own security attribute and performs the requested operation to a logical storage area.

Every time a request is issued from a host computer, the security attribute associated with the connection control process is replaced by new information (host computer ID).

7.1.9 FMT_MOF.1

As one of the TOE audit functions, enabling/disabling audit log data transfer to a Syslog server (outside of the TOE) can be performed by Audit Log Administrators (View and Modify). Audit log data is recorded in the TOE as the audit trail regardless of the setting of Syslog server transfer. These operations of changing the setting is performed via the dedicated interface installed in the management console (a utility program called “Hitachi Storage Navigator Modular 2”.

7.1.10 FMT_MSA.1

The association between requests from host computers and logical storage areas managed by the TOE is maintained based on the information of the connection control table. This information in the connection control table is managed by Storage Administrators via the management console.

7.1.11 FMT_MSA.3

Storage Administrators set logical storage areas (objects) on a host computer basis and initial settings of allowed operations. Default value before not being changed initially is "no access allowed to any storage areas".

7.1.12 FMT_MTD.1

Table 7-3 shows permitted operations of TSF data for each administrator.

Table 7-3 Administrator roles and permitted operations of TSF data

Role	TSF data	Operation
Account Administrator (View and Modify)	User ID	Change default, modify, delete
	User password (All users))	Change default, modify
	User roles	Change default, modify
	Session timeout	Modify
Account Administrator (View Only)	Own password	Modify
Audit Log Administrator (View and Modify)	Audit trail	Query
	Own password	Modify
Audit Log Administrator (View Only)	Audit trail	Query
	Own password	Modify
Storage Administrator (View and Modify)	Host computer ID	Change default, modify, delete
	Own password	Modify

Storage Administrator (View Only)	Own password	Modify

7.1.13 FMT_REV.1

This requirement describes the function addressing the condition where the authentication status is incorrectly fixed to “logged in” due to a failure in the TOE or its IT environments, etc. Account Administrator (View and Modify) can forcibly change the authentication status of the administrator to “logged out”.

7.1.14 FMT_SMF.1

Table 7-4 shows security management function mechanisms to be implemented for the related SFRs.

Table 7-4 Security management function mechanisms

SFR	Management function mechanism
FMT_MOF.1	Administrators who belong to the Audit Log Administrator (View and Modify) group among identified and authenticated administrators can enable/disable audit log data transfer to the Syslog server.
FMT_MSA.1	Administrators who belong to the Storage Administrator group among identified and authenticated administrators can use the connection control table to manage associations between each object (logical storage area) and host computers. (The management function in FMT_MSA.3 applies only when objects are generated.) ・ Storage Administrator (View and Modify) can modify the above setting.
FMT_MSA.3	Administrators who belong to the Storage Administrator (View and Modify) group among identified and authenticated administrators can populate the connection control table with the information between an object and host computers and that defining logical storage area of the object when objects are generated.
FMT_MTD.1	Administrators who have been identified and authenticated can perform operations of the TSF data according to the assigned roles defined in Table 7-3. No operations other than predetermined one are allowed.

7.1.15 FMT_SMR.1

The TOE provides six role groups as roles of administrators: Account Administrator (View and Modify), Account Administrator (View Only), Storage Administrator (View and Modify), Storage Administrator (View Only), Audit Log Administrator (View and Modify) and Audit Log Administrator (View Only). All the administrators are registered in one or more groups.

7.1.16 FPT_STM.1

Time stamps are obtained from a low-level OS and added to audit data.

7.1.17 FRU_RSA.1

Three user roles are assigned Modify roles: Account Administrator (View and Modify), Audit Log Administrator (View and Modify), and Storage Administrator (View and Modify). The number of simultaneous logged-in administrators for each of these roles is limited to “1”. The number of simultaneous logged-in administrators who have not the Modify permission is not limited.

7.1.18 FTA_SSL.3

Each session of the logged-in administrator is managed to monitor how much period of time operations are not performed via the management console. If the session timeout value exceeds the upper limit the session of the user (administrator) is forcibly terminated. The session timeout value can be initially set and/or changed by Account Administrators (View and Modify).

8 Terms and definitions

8.1 CC-related

PP

Protection Profile: A set of security requirements that is defined as common specifications by procurement personnel or developer industries of the TOE.

CC

Common Criteria for Information Technology Security Evaluation. The same contents of CC are also defined as ISO/IEC 15408.

ST

Security Target: A set of security requirements for each IT product.

TOE

Target of Evaluation; a product to be evaluated. The TOE can be an entire IT product or part of the IT product. The scope of the TOE is strictly defined in the ST.

8.2 TOE-related

Disk array

A logical disk drive that consists of multiple disk drives (generally, hard disks). Furthermore, some disk array systems are able to divide a combined disk drive into logical disk drives and assign them to different host computers. The TOE in this ST is one of them.

Most of disk arrays are provided as devices independent of host computers. Implementing RAID (Redundant Array of Independent Disks) in the configuration improves the reliability related to hardware failures. A very high capacity disk drive can be realized by combining a large number of disk drives. Managing host computers separately from disk drives contributes to a higher maintainability.

SAN

An acronym for Storage Area Network. A dedicated network for connecting storage devices such as disk arrays to host computers. It is recognized by host computers (OS that runs on it) as local storage device directly connected it. It enables high speed block level data transfer independent of OS on host computers. The SCSI protocol is used for communicating between host computers and storage devices. The conventional SCSI specifications have a restriction of 320Mbps of bandwidth and 25m of transmission length. Using FC (Fibre Channel), which is applied to SAN, high-speed and long-length transmission can be attained where bandwidth is 8Gbps and transmission length is 100km (or more). Alternatively, Ethernet and IP protocol are used instead of FC to configure SAN. iSCSI (SCSI on IP network) is used as protocol in this case.

Host computer

In this ST, users of disk array service provided by HUS are called host computers. Interfaces with which HUS provides host computers are independent of file systems, enabling various OSs such as Windows, HP-UX, and Solaris to use disk array resources of HUS. The same logical storage area (volume) can be shared by host multiple computers that run on the same OS.