HITACHI
Inspire the Next

Hitachi Adaptable Modular Storage ~~2300~~ Microprogram Security Target

~~Revision.11~~Revision.12

This document is the English version of security target written in Japanese for changed TOE related to Assurance Continuity.

~~April 13, 2009~~August 17, 2010

Hitachi, Ltd.

Trademarks

- AIX and IBM are registered trademarks of International Business Machines Corporation.
- HP and HP-UX are registered trademarks of Hewlett-Packard Company.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and/or other countries.
- Linux is a registered trademark of Linus Torvalds in the United States and/or other countries.
- Microsoft, Windows, and the Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Microsoft Internet Explorer is a product name of Microsoft Corp.
- Mozilla is a trademark of Mozilla Foundation in the United States and/or other countries.
- Red Hat is a registered trademark or trademark of Red Hat, Inc. in the United States and/or other countries.
- Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.
- IRIX and SGI are registered trademark of Silicon Graphics, Inc. in the United States.
- VxWorks and Wind River are registered trademark of Wind River Systems, Inc. in the United States and /or other countries.
- All other brand or product names are or may be registered trademarks, trademarks or service marks of and are used to identify products or services of their respective owners.

– Contents –

1. ST Introduction

This chapter describes the ST and TOE identification information, ST overview, CC conformance, and glossary to be used.

1.1. ST Identification

The ST and TOE identification information targeted by ST are shown below.

(1)ST Identification

ST Name	Hitachi Adaptable Modular Storage ~~2300~~ Microprogram Security Target
Revision.	~~1~~12
Development	Hitachi, Ltd.
Issued Date	~~April 13, 2009~~August 17, 2010

(2)TOE Identification

TOE Identification	Hitachi Adaptable Modular Storage ~~2300~~ Microprogram
Version.	0862/A~~-M~~
Development	Hitachi, Ltd.

(3)CC version of applied

CC Identification	Common Criteria for Information Technology Security Evaluation Version 2.3 Interpretations-0512

1.2. ST Overview

The Hitachi disk array subsystem “Hitachi Adaptable Modular Storage ~~2300~~” (hereinafter referred to as “Hitachi AMS~~2300~~”) is a disk array subsystem for the midrange which realized the flexible system extension by the large capacity, high reliability, and modular structure.
The disk array subsystem stores important data for host users. Therefore, the settable operation by each administrator must be limited to prevent setting changes of the disk array subsystem which may lose security and confidentiality of the data.
This ST describes the security functions provided by the microprogram for Hitachi AMS~~2300~~ as the target of evaluation (TOE).
The microprogram of Hitachi ~~AMS2300~~ (TOE) and its hardware (Hitachi AMS~~2300~~) evaluated by this ST 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 part 2
- CC version 2.3 part 3
- Package and EAL 2
- There is no conformable PP.

1.4. 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, Version 2.3, 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
- Interpretations-0512, December 2005, Information-Technology Promotion Agency, Japan
- 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, Version 2.3, 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

1.5. Terminology

The terms used in this ST are shown in the table below.

Table 1 Terminology

Terms	Explanations
FC	An abbreviation of Fibre Channel. A high-speed data transfer technology (protocol) for connecting computers and peripherals. Optical fibers and copper wires are used for the connection.
FC-SAN	An abbreviation of Fibre Channel – Storage Area Network. A form of SAN using Fibre Channel as a network.
Hitachi AMS 2100	An abbreviation of Hitachi Adaptable Modular Storage 2100. A disk array subsystem where TOE treated by this ST operates.
Hitachi AMS 2300	An abbreviation of Hitachi Adaptable Modular Storage 2300. A disk array subsystem where TOE treated by this ST operates.
Hitachi AMS 2500	An abbreviation of Hitachi Adaptable Modular Storage 2500. A disk array subsystem where TOE treated by this ST operates.
Hitachi AMS	A general term of Hitachi AMS 2100, Hitachi AMS 2300,Hitachi and AMS 2500
Hitachi Storage Navigator Modular 2	Software for the disk array subsystem management setting. In the text, “for CLI” and “for GUI” may be totally called as “Hitachi Storage Navigator Modular 2” or “HSNM2” (abbreviation).
Hitachi Storage Navigator Modular 2 (for CLI)	Hitachi Storage Navigator Modular 2 operated by a command line interface.
Hitachi Storage Navigator Modular 2 (for GUI)	Hitachi Storage Navigator Modular 2 operated by GUI. A Web-based application having the computer in which Hitachi Storage Navigator Modular 2 (for GUI) is installed as a server and operated by a Web browser of the same or different computer.
HSNM2 (for CLI)	An abbreviation of Hitachi Storage Navigator Modular 2 for CLI.
HSNM2 (for GUI)	An abbreviation of Hitachi Storage Navigator Modular 2 for GUI.
IP-SAN	An abbreviation of Internet Protocol - Storage Area Network. A form of SAN using Ethernet that can be constructed at low cost as a network and TCP/IP operated on Ethernet, and using iSCSI for communication control.
iSCSI	An abbreviation of Internet Small Computer System Interface. A standard of using the SCSI protocol on the TCP/IP network.
LU	An abbreviation of Local Unit. Logically divided disk spaces. A given address to identify these two or more logical units is called LUN (Logical Unit Number).
RAID	An abbreviation of Redundant Arrays of Inexpensive (or Independent) Disks. A technology of realizing high-speed, large-capacity, and highly-reliable disk subsystem by distributing accesses using two or more storage devices such as hard disks.
RAID Manager	Software for the disk array subsystem management setting. RAID Manager operates in the host and issues the setting command for the disk array subsystem via SAN.
SAN	An abbreviation of Storage Area Network. A dedicated network to connect a storage device such as a disk subsystem and tape device with a server.
SCSI	An abbreviation of Small Computer System Interface. An interface to mainly connect a computer and peripherals such as storages, etc. and to send/receive data.
Priced option	An option function of the disk array subsystem provided onerously. Setting of Enabled/Disabled of the function is possible.

Terms	Explanations
Resource operation authority	An authority assigned to the administrator who logged in by the Account Authentication function. This authority is to prevent two or more users perform setting changes at the same time and the array subsystem becomes an unexpected status (setting). The authority has “Update Mode” and “Reference Mode”, and either is determined when logging in the account. When another account having the same role with the account to login has already logged in, the reference mode is given (the update mode when another account having the same role has not logged in). In case of the update mode, the management operation according to the role becomes possible. In case of the reference mode, only the reference of the management information becomes possible regardless of the role assignment.

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

The microprogram version 0862/A-~~M~~ for Hitachi AMS~~2300~~, which is TOE, is a control program (software) operated in Hitachi disk array subsystem "Hitachi Adaptable Modular Storage ~~AMS2300~~" and has roles to control the operation of the disk array subsystem such as data transfer control between the disk array subsystem and the host connected to the disk array subsystem.

This TOE provides a function to permit the management operation of the disk array subsystem only to the previously authorized administrator and an audit log function to record the event of the management operation as security functions.

2.2. General Configuration of the System including the Storage Device

General configurations of the systems including the disk array subsystem are shown in the figure below.

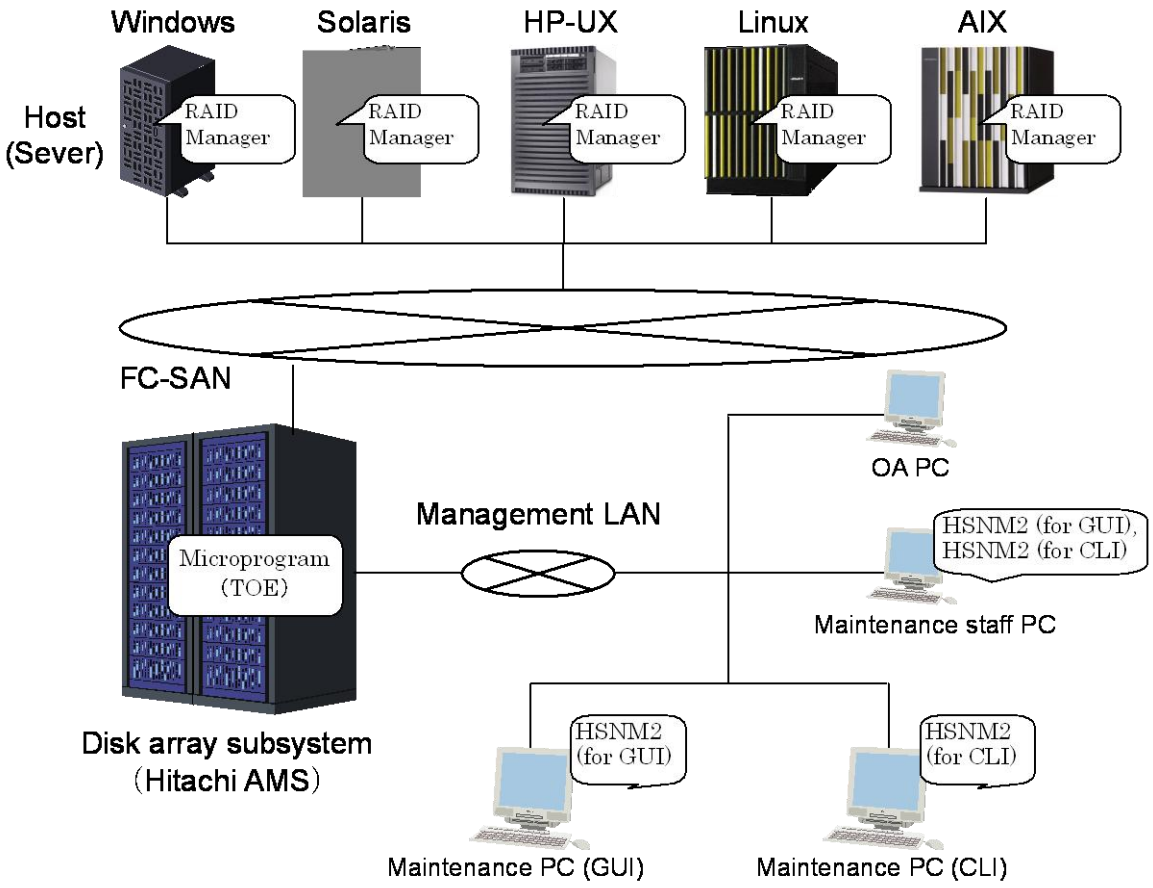

Figure 1 General Configuration of the System including the Storage Device

(1) Host

Hosts are various open-system servers such as Windows, Solaris and HP-UX connecting with and using the disk array subsystem. These devices are totally called as “Host” in this ST. The host users described later use this device. The host enables to install RAID Manager which is software for managing the subsystem control information of the disk array subsystem. This ST targets the subsystem configuration not using RAID Manager. (To use RAID Manager, the setting by Hitachi Storage Navigator Modular 2 is required for the disk array subsystem in advance, but this ST assumes the environment that such setting is not done.)

(2) FC-SAN (Fibre Channel - Storage Area Network)

FC-SAN is a dedicated network for the storage system connecting the host and disk array subsystem using Fibre Channel. This network is not used for any purposes other than the storage system.

(3) Disk array subsystem

The Disk array subsystem is Hitachi AMS~~2300~~. This is a subsystem where TOE operates and connected with the host via FC-SAN. The disk array subsystem in the evaluation configuration is the evaluation configuration uses Fibre Channel (FC-SAN) as a connection interface with the host. Hitachi AMS~~2300~~ can use either FC-SAN or IP-SAN exclusively, but the evaluation configuration uses FC-SAN.

(4) Management LAN

The management LAN is an Ethernet network connecting the disk array subsystem and a management PC. This network is not limited to an independent network because an OA PC may be connected sharing with a network of another company, but it is protected by a firewall, etc. not to be accessed directly from external networks such as Internet.

(5) Management PC (GUI)

The management PC (GUI) is a computer used for setting, operating, and managing the disk array subsystem, and Hitachi Storage Navigator Modular 2 (for GUI), which is a disk array subsystem setting program, is installed. Furthermore, JRE is installed in this subsystem because HSNM2 (for GUI) uses Java in a part of the window display. The administrators (disk array administrators, account administrators, and audit log administrators) to be described later or maintenance staff operates this subsystem. This subsystem and the disk array subsystem are connected via management LAN.

This PC accesses Hitachi Storage Navigator Modular 2 (for GUI) in this subsystem using the HTTP protocol. Therefore, it uses the Web browser, starts HSNM2 (for GUI), and accesses TOE of the disk array subsystem (it may start JRE in HSNM2 (for GUI) depending on the display window).

(6) Management PC (CLI)

The management PC (CLI) is a computer used for setting, operating, and managing the disk array subsystem, and Hitachi Storage Navigator Modular 2 (for CLI), which is a disk array subsystem setting program, is installed. This subsystem and the disk array subsystem are connected via the management LAN. The administrators (disk array administrators, account administrators, and audit log administrators) to be described later or the maintenance staff operates this subsystem. The computer starts HSNM2 (for CLI) of this subsystem and accesses TOE of the disk array subsystem.

(7) Maintenance staff PC

The maintenance staff PC is a computer used by the maintenance staff for performing the maintenance work of the disk array subsystem. Hitachi Storage Navigator Modular 2 (for GUI) or (for CLI) necessary for performing the maintenance work is installed (JRE is also installed in case of HSNM2 (for GUI)). Furthermore, the computer may access TOE of the disk array subsystem using the Web maintenance window from the Web browser for the maintenance work (the Web maintenance window is a Web page displayed if an IP address of the disk array subsystem is entered in the Web browser). This subsystem and the disk array subsystem are connected to the management LAN only when performing the maintenance work.

In this ST, the above-mentioned computers from (5) to (7) may be totally called as “Management PC”. Furthermore, the management PC (GUI) and the management PC (CLI) can be shared in the same hardware.

(8) Hitachi Storage Navigator Modular 2

Hitachi Storage Navigator Modular 2 is a program used for setting and displaying the disk array subsystem configuration, displaying the information, and monitoring failures, and installed and used in the management PC. There are two types; Hitachi Storage Navigator Modular 2 (for GUI) which is the Web-based GUI and Hitachi Storage Navigator Modular 2 (for CLI) which is a command line interface.

The computers shown in (5), (6), and (7) above can co-exist HSNM2 (for GUI) and (for CLI) in each computer if the conditions of the hardware configuration factors to be described later are satisfied.

Among the devices mentioned above, it is assumed that the host, the disk array subsystem and FC-SAN connecting them are placed in the environment where only the limited person can access, and others are set in offices of ordinary companies.

2.2.1. General Configuration of Hardware

The general configuration of hardware is shown in the table below.

Table 2 General Configuration of Hardware

Components	Description or Operating Condition
Disk array subsystem	This is Hitachi Adaptable Modular Storage ~~2300~~ (Hitachi AMS2100, Hitachi AMS2300 or Hitachi AMS2500). The number of HDDs and ports differs depending on the configurations ordered by customers.
Host	This is a computer to access the disk array subsystem.
Management PC (GUI)	The operating conditions are shown below. ■Windows ▪OS: Windows2000 (SP3,SP4)/XP (SP2)/Vista, Windows Server 2003 (SP1,SP2) Windows Server 2003 (R2)(32/64bit) Windows Server 200 8 (32/64bit)(32/64bit) ▪CPU: 1 GHz or more (2 GHz or more is recommended) ▪Memory: 1 GB or more (2 GB or more is recommended) ▪Browser: Internet Explorer6.0 (SP1), Internet Explorer 7.0 ▪Java (JRE): Java6.0 Update10 (1.6.0_10) ▪Disk capacity: Free capacity of 1.5 GB or more ▪Monitor resolution: 1024 × 768 or more is recommended (256 colors or more)
	■Sun (SPARC) ▪OS: Solaris 8,9,10 ▪CPU:SPARC 1 GHz or more (2 GHz or more is recommended) ▪Memory: 1 GB or more (2 GB or more is recommended) ▪Browser: Mozilla1.7 ▪Java (JRE): Java6.0 Update10 (1.6.0_10) ▪Disk capacity: Free capacity of 1.5 GB or more ▪Monitor resolution: 1024 × 768 or more is recommended (256 colors or more)
	■RedHatLinux (x86) ▪OS: Red Hat Enterprise Linux AS4.0 Update1/Update5 (32 bits for both) ▪CPU: 1 GHz or more (2 GHz or more is recommended) ▪Memory: 1 GB or more (2 GB or more is recommended) ▪Browser: Mozilla1.7 ▪Java (JRE): Java6.0 Update10 (1.6.0_10) ▪Disk capacity: Free capacity of 1.5 GB or more ▪Monitor resolution: 1024 × 768 or more is recommended (256 colors or more)
Management PC (CLI)	The operating conditions are shown below. ■Windows ▪OS: Windows2000/XP/Vista, Windows Server2003 (SP1, SP2) Windows Server 2003 (R2)(32/64bit) Windows Server 2008 (32/64bit) ▪CPU: 233 MHz or more ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 30 MB or more
	■Sun (SPARC) ▪OS: Solaris 8, 9, 10 ▪CPU: SPARC or more (Frequency is no object) ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 54 MB or more ▪Kanji character code: EUC-JP

Components	Description or Operating Condition
	■Sun (x86, 32bit) ▪OS: Solaris 10 ▪CPU: 256 MHz or more ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 54 MB or more ▪Kanji character code: EUC-JP
	■SGI ▪OS: IRIX 6.5 ▪CPU: R10000 or more (Frequency is no object) ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 90.5 MB or more ▪Kanji character code: EUC-JP
	■HP ▪OS: HP-UX 11.0, 11i, 11i v2.0 ▪CPU: PA8000 or more, 11iv2.0 is Itanium 2 (Frequency is no object) ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 65 MB or more ▪Kanji character code: SJIS/EUC-JP
	■IBM ▪OS: AIX 5L v5.1, 5.2 ▪CPU: PowerPC/RS64IIor more (Frequency is no object) ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 46.5 MB or more ▪Kanji character code: SJIS ▪Prerequisite program: VisualAge C++ Runtime 6.0.0.0 or more. IY33524 patch is required.
	■Red Hat Linux (x86) ▪OS: Red Hat Enterprise Linux AS4 Update1 (32 bit) ▪CPU: 233 MHz or more ▪Memory: 256 MB or more ▪Disk capacity: Free capacity of 35 MB or more ▪Kanji character code: SJIS/EUC-JP
Maintenance staff PC	The management PC can be used as a maintenance staff PC. Therefore, either operation condition of the management PC (GUI) or (CLI) should be satisfied.

2.2.2. General Configuration of Software

The general configuration of Software is shown in the table below.

Table 3 General Configuration Software

Components	Descriptions
Microprogram	This is TOE and microprogram operating in the controller of the disk array subsystem. Version: 0862/A~~-M~~ (In detail, microprogram used 0862/A-S for operating environment Hitachi AMS2100 0862/A-M for operating environment Hitachi AMS2300 0862/A-H for operating environment Hitachi AMS2500)
Real-time OS	This is a real-time OS operating in the disk array subsystem. Package name: WindRiver Platform for Network Equipment, Vxworks Edition 3.5 (Old: Tornado) OS: VxWorks 6.5 Web: Wind River CLI, Web, MIBway 4.6 (Old:WindManageWeb) Security: WindRiver Security Library 1.3 SSL: Wind River SSL 1.3 (OpenSSL: version 0.9.8a)
Hitachi Storage Navigator Modular 2 (for GUI)	This is a program to manage the disk array subsystem operating in the management PC (GUI). Version: 6.20
Hitachi Storage Navigator Modular 2 (for CLI)	This is a program to manage the disk array subsystem operating in the management PC (CLI). Version: 6.20
This is an OS of the management PC (GUI)	Refer to Table 2 “Management PC (GUI)” for the details.
This is an OS of the management PC (CLI)	Refer to Table 2 “Management PC (CLI)” for the details.
Web browser (HSNM2)	This is a Web browser accessible to Hitachi Storage Navigator Modular 2 from the management PC (GUI). ● Internet Explorer6.0 (SP1) ● Internet Explorer7.0 ● Mozilla 1.7
Web browser (Web maintenance window)	This is a Web browser accessible to the Web maintenance window of the disk array subsystem from the maintenance staff PC. ● Internet Explorer6.0 (SP1) ● Internet Explorer7.0 ● Mozilla 1.7
Java run-time environment	This is a Java run-time environment to be necessary when starting the Java applet of Hitachi Storage Navigator Modular 2 for GUI by the management PC (GUI). ● Java6.0 Update10 (1.6.0_10)

2.3. Physical range of TOE

The physical configuration of this TOE is shown below.

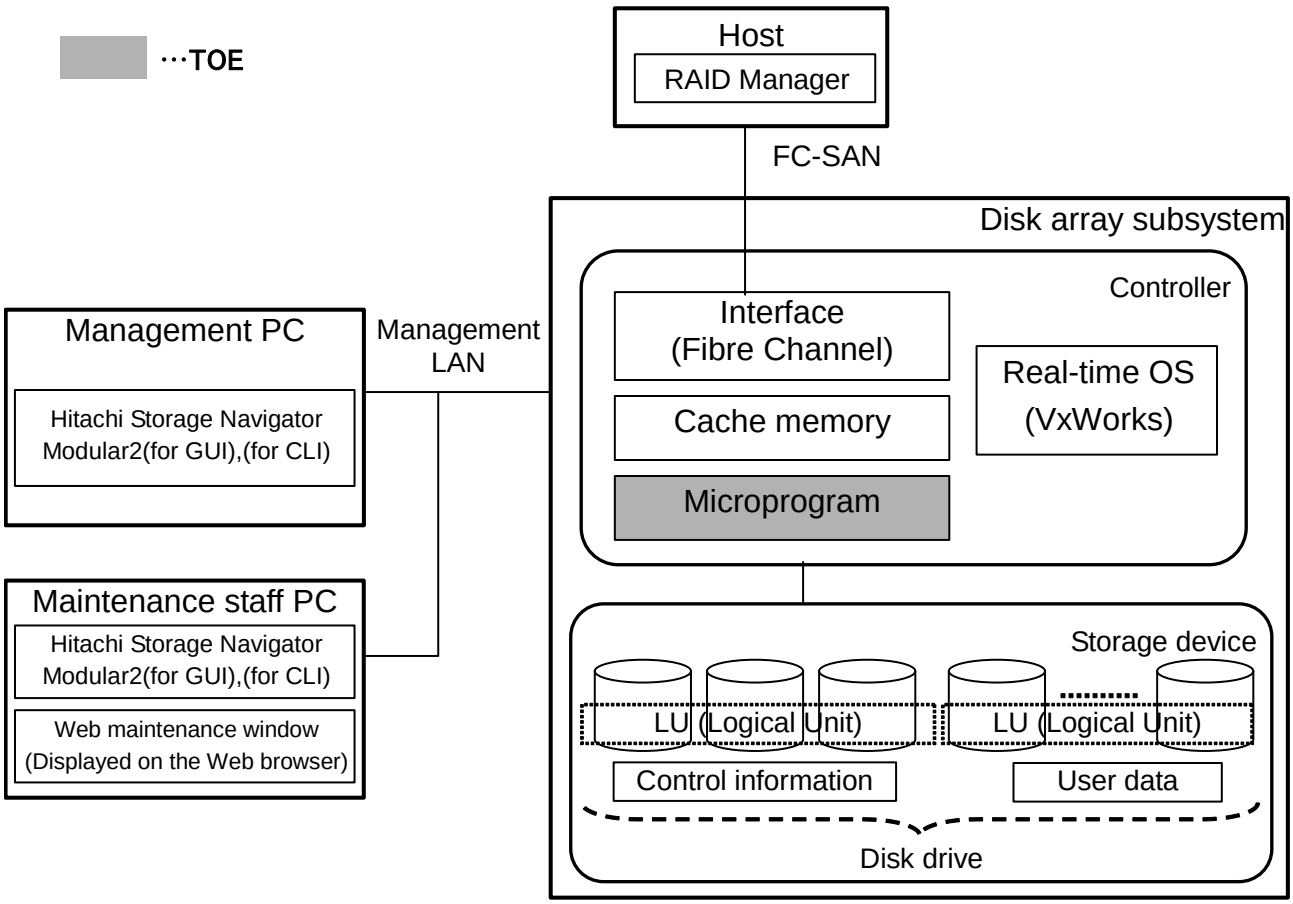

Figure 2 TOE Logical Configuration

The disk array subsystem is composed of a controller to control the operation of the disk array subsystem and a storage device to record the user data. Furthermore, a management PC and a maintenance staff PC are used for the operation-related setting and the operation maintenance of the subsystem. The description of each component is shown below.
The devices to be embedded in the disk array subsystem and software are factory-installed.

(1) Controller

The controller is a part to control the operation of the disk array subsystem. The controller includes an interface for LAN to connect with the management PC, an interface for Fibre Channel to connect with the host, an interface to connect with the disk drives, a cache memory to temporarily store the data sending/receiving to/from the host, etc. Furthermore, the microprogram, which is TOE, operates in the controller.
The structure of the management LAN, FC-SAN, and storage device is completely independent. Therefore, any devices connected to the management LAN cannot access the FC-SAN, cache memory, and storage device.

(2) Interface for Fibre Channel

The interface for Fibre Channel is a part of which the disk array subsystem receives communication from the host, and the interface for Fibre Channel (used for FC-SAN) is installed.

Two or more interfaces of the same type may be installed due to fault tolerance.

(3) Cache memory

The cash memory stores data temporarily when reading/writing user data from the host to the storage device, and uses it for accelerating the processing.

(4) Microprogram

The microprogram is TOE treated by this ST. This program controls the operation of the disk array subsystem. The microprogram can provide the additional option functions (hereinafter referred to as “priced options”) onerously. In the configuration of this TOE, among the priced options, only Account Authentication and Audit Logging, which are the security functions, are provided, and other priced options are not provided.

(5) Storage device

The storage device comprises two or more disk drives and stores the user data and the control information which is the setting information of the disk array subsystem. The storage device improves reliability by the RAID configuration. The storage device is identified by the host in units of LUs (Logical Units), and the user data is stored in the LUs.

(6) Management PC

The management PC a computer where Hitachi Storage Navigator Modular 2, which is the program for setting the disk array subsystem, is installed. This device combines both the management PC (GUI) and the management PC (CLI). Furthermore, in this device, Hitachi Storage Navigator Modular 2 (for GUI) and (for CLI) co-exist (if HSNM2 (for GUI) is installed, JRE is also installed). The administrators (disk array administrator, account administrator, and audit log administrator) to be described later or the maintenance staff operates this device.

(7) Maintenance staff PC

This maintenance staff PC is a computer used for performing the maintenance work. Hitachi Storage Navigator Modular 2, which is the program for setting the disk array subsystem, is installed, and uses this program for the maintenance work. In this device, Hitachi Storage Navigator Modular 2 (for GUI) and (for CLI) co-exist. Furthermore, it accesses the Web maintenance window of the disk array subsystem by the Web browser. The maintenance staff operates this device and is connected to the management LAN only when performing the maintenance work.

(8) Hitachi Storage Navigator Modular 2

Hitachi Storage Navigator Modular 2 is a program for setting the disk array subsystem, and used for setting and displaying the configuration of the disk array subsystem, displaying the information, and monitoring failures. The two types, Hitachi Storage Navigator Modular 2 (for GUI) which is Web-based GUI and Hitachi Storage Navigator Modular 2 (for CLI) which is a command line interface are totally called as “Hitachi Storage Navigator Modular 2”. The setting operation of this TOE is enabled only in the version 6.20 or more.
This program is not included in TOE.

(9) Host

The host is an open-system server connecting with the disk array subsystem and using the user data area of the disk array subsystem. The host users to be described later use this device. RAID Manager can be installed.
This device cannot access, except for RAID Manager, the control information (protection target asset to be described later) of the disk array subsystem.

(10) RAID Manager

RAID Manager is software used for managing the subsystem control information of the disk array subsystem and operates in the host. This ST targets the subsystem configuration not using RAID Manager. (To use RAID Manager, the setting by Hitachi Storage Navigator Modular 2 is required for the disk array subsystem in advance, but this ST assumes the environment where such setting is not done.)
This program is not included in TOE.

2.3.1. Hardware Configuration of TOE

The hardware configuration of TOE verified by this evaluation is shown in the table below.

Table 4 Hardware Configuration

Components	Descriptions
Disk array subsystem	Hitachi Adaptable Modular Storage 2300
Host	■Windows ▪OS: Windows Server 2003 (R2) ▪CPU: Xeon 2.8GHz ▪Memory: 1 GB ▪Host Bus Adapter (For connecting a Fibre Channel)
Management PC	This device combines the management PC (GUI) and (CLI). Therefore, the configuration should satisfy all these operation environments. Refer to the following. ■Windows ▪OS: Windows Vista ▪CPU: AMD Opteron 2 GHz ▪Memory: 2 GB ▪Disk capacity: 200 GB or more
Maintenance staff PC	The same as the above-mentioned “Management PC”.

2.3.2. Software Component

The software configuration of TOE verified by this evaluation is shown in the table below.

Table 5 Software Conmonent

Components	Descriptions
Microprogram	Version: 0862/A~~-M~~ (Because the operating environment is Hitachi AMS2300, 0862/A-M is used. and only Account Authentication and Audit Logging are provided as priced options)
Real-time OS	Package name: WindRiver Platform for Network Equipment, Vxworks Edition 3.5 (Old: Tornado) OS: VxWorks 6.5 Web: Wind River CLI, Web, MIBway 4.6 (Old: WindManageWeb) Security: WindRiver Security Library 1.3 SSL: Wind River SSL 1.3 (OpenSSL version: version 0.9.8a)
Hitachi Storage Navigator Modular 2 (for GUI)	Version: 6.20
Hitachi Storage Navigator Modular 2 (for CLI)	Version: 6.20
This is an OS of the management PC	Refer to Table 4 “Management PC” for the details.
Web browser (HSNM2)	Internet Explorer 7.0
Web browser (Web maintenance window)	Internet Explorer 7.0
Java run-time environment	Java6.0 Update10 (1.6.0_10)

2.4. Participants of TOE

The people shown below relate to this TOE.

(1) Disk array administrator

The disk array administrator is a person who operates Hitachi Storage Navigator Modular 2 in the management PC and manages the disk array subsystem.
At least the role of Storage Administrator (View and Modify) is assigned to the disk array administrator.

(2) Account administrator

The account administrator is a person who operates Hitachi Storage Navigator Modular 2 in the management PC and manages the accounts of the disk array administrator, account administrator, and audit log administrator. The account administrator can create, change, and delete the accounts using the Account Authentication function which is the TOE function.
At least the role of Storage Administrator (View and Modify) is assigned to the disk array administrator.

(3) Audit log administrator

The audit log administrator is a person who operates Hitachi Storage Navigator Modular 2 in the management PC and manages the audit log acquired by the disk array subsystem. The audit log administrator can make the audit log setting (Enabled/Disabled of log acquisition) and the settings for erasing by using the Audit Logging function which is the TOE function.
At least the role of Storage Administrator (View and Modify) is assigned to the disk array administrator.

(4) Maintenance staff

The maintenance staff is a staff belonging to the organization for maintenance where the customer using the disk array subsystem has signed a maintenance contract. The maintenance staff uses a manual for the maintenance staff and takes charge of the maintenance work (initialization when setting the disk array subsystem, setting changes associated with replacement and addition of parts, etc., and restoration processing at trouble.) Furthermore, the maintenance staff may take care of the setting work which should be performed by the above-mentioned administrators according to the requests from the customers. Hitachi Storage Navigator Modular 2 and the Web maintenance window (a window displayed when an IP address of the disk array subsystem is entered in the Web browser) are used when performing the maintenance work. When using Hitachi Storage Navigator Modular 2, the maintenance staff receives some administrator roles given by the account administrator of the customer and performs the management operation within the authorized range. When using the Web maintenance window, the authority of the administrator role is not required because only the maintenance staff performs the operation, and the identity authentication and audit log to be described later are not acquired.

In this ST, the above-mentioned people from (1) to (4) may be totally called “administrators”.

(5) Host user

The host user is a person who uses the host connecting to the disk array subsystem. The data is read/written from the host to the storage area of the disk array subsystem. This person does not manage the disk array subsystem.

2.5. Property to be Protected

The disk array subsystem stores important data for host users. Therefore, the settable operation must be limited to each administrator for preventing setting changes of the disk array subsystem which may lose security and confidentiality of the data. Therefore, this ST specifies the general function setting parameters of the microprogram as the property to be protected so that unauthorized settings which affect the security and confidentiality of the data of the host users to be recorded in the disk array subsystem are not performed, and controls it so that the specified administrator can change the settings within the limited range.

The settable items as general functions are shown below.

- Creation, deletion, and reference of RAID groups and LUs
- Assignment of LUs to the host (setting of host access control)
- Setting the configuration information (IP address, port number, operation setting at the time of drive restoration, etc.) of the disk array subsystem
- Setting the priced options other than the Audit Logging function and Account Authentication function (Unlocked/Locked, Enabled/Disabled).

2.6. Logical Range of TOE

The overview of the general IT functions and security functions provided by TOE are shown below.

2.6.1. TOE general functions

The microprogram is software to control the operation of the disk array subsystem, and controls the data transfer between the host and the disk array subsystem and the data transfer between the cache memory and the storage device.

2.6.2. TOE Security Functions

In TOE, the administrator role is assigned to a person who operates the disk array subsystem. There are six types of administrator roles; Account Administrator (View and Modify), Account Administrator (View Only), Audit Log Administrator (View and Modify), Audit Log Administrator (View Only), Storage Administrator (View and Modify), and Storage Administrator (View Only), and at least one role of these is assigned to the operator of Hitachi Storage Navigator Modular 2.
This ST treats the operator whom Account Administrator (View and Modify) is assigned as the account administrator, whom Audit Log Administrator (View and Modify) is assigned as the audit log administrator, and whom Storage Administrator (View and Modify) is assigned as the disk array administrator. These operators may combine two or more roles. The difference between “View and Modify” and “View Only” of each is whether to be able to execute the setting operations or only to be able to view the setting information (table storing the setting parameters of the disk array subsystem) within the authorized range.

TOE provides the following functions as the security functions.

(1) Account Authentication function
This function comprises the following functions.

[Identity/Authentication]
The microprogram compares the registered account information (user ID, password) with the input value once accepting the identity/authentication requests from the operators when the operators set the disk array subsystem. When they match and “Account Disabled” attribute is not set for the account concerned, the identity/authentication is successful.
Furthermore, when the identity/authentication is successful, the microprogram issues a session ID corresponding to the account concerned and distributes it to Hitachi Storage Navigator Modular 2. When managing the disk array subsystem, Hitachi Storage Navigator Modular 2 combines the operation command and session ID and transmits it to the disk array subsystem. When the session ID matches with the one issued, the microprogram determines the account concerned as the operator related to the session ID, and performs the execution control by the following roles.

[Execution control by roles]
When the session ID checking is successful, the command concerned is executed only if the role given to the account concerned permits the execution of the received command. If the role given to the account does not permit the command execution, it is not executed.

[Time-out function]
If the operation is not performed for a certain period of time, the session ID concerned becomes disabled.

[Account management]
The microprogram manages the user ID, password, account disabled attribute, and role response per account as the account information. Furthermore, the microprogram provides the measures of managing the account information settings.

(2) Audit Logging function.
The function concerned comprises the following functions.

[Audit log acquisition]
The microprogram acquires (creates/stores) the audit log of the event when an audit event related to the security function in TOE such as login success/failure of the administrator occurs. Furthermore, the microprogram provides the measures of Enabled/Disabled settings of the audit log acquisition.

[Audit log erasing]
The microprogram provides the measures of erasing the audit log (batch erasing of all audit logs).

(3) Setting function
The microprogram provides the measures of enabling or disabling the Account Authentication function and the Audit Logging function.

The relation of the setting items of the administrator and the security functions is shown below.

Table 6 Setting Items of the Security Functions

Security Functions		Setting Items of the Security Functions	Executable Administrator
Account Authentication Function	Account management	▪Account creation (user ID, password, role assignment), change, deletion, reference	Account management
Audit Logging Function	Audit log creation	▪Enabled/Disabled setting of audit log acquisition	Audit log administrator
	Audit log erasing (batch erasing of all audit logs)	▪Audit log erasing setting	Audit log administrator
Setting Function		▪Enabled/Disabled of Account Authentication function	Account management
		▪Enabled/Disabled of Audit Logging	Audit log administrator

3. TOE Security Environment

This Chapter defines the TOE security environment.

3.1. Prerequisite conditions

This TOE assumes to be used under the prerequisite conditions shown below.

A.Administrator

The disk array administrator, account administrator, and audit log administrator are assumed to be the reliable people who have sufficient ability to perform the management operation of the disk array subsystem, and not to perform the operation/setting which interferes with the security of the disk array subsystem intentionally.

A.CustomerEngineer

The maintenance staffs are assumed to be the reliable people who have the sufficient ability and knowledge to performing overall maintenance work of the disk array subsystem safely, to perform correct maintenance work as stated in the procedure manual, and not to commit a fraud.

A.Environment

The following conditions are assumed as the environment for the usage of this TOE.

- FC-SAN to connect the disk array subsystem, host, or both of them must be set in the secured area where only the disk array administrator, account administrator, audit log administrator, and maintenance staff are authorized for entering/leaving, and must be completely protected from the unauthorized physical access.
- FC-SAN must be used only for the purpose of connecting the disk array subsystem and the host, and must not be connected to other networks or used for other purposes.
- The account management of the host must be performed appropriately, and the third person other than the host user must not use the host illegally.
- The management LAN must have the configuration not accessed directly from external networks such as Internet by the firewall, etc..
- The management PC and the maintenance staff PC must be managed appropriately so that unauthorized programs (malwares such as keylogger) are not installed or they are not infected by computer viruses.
- RAID Manager must not be used in the disk array subsystem where TOE operates.
- The password of the account of the Account Authentication function must be the character string combining a number, the alphabet, and a sign (either of !" # $ % & ' () * + , - . / : ; <=> ? @ [¥] ^ _ ` {|} ~) among the half-width characters.
- When accessing the disk array subsystem via the management LAN, the administrator must use Hitachi Storage Navigator Modular only and not to be accessed by irregular packet such as not creating Hitachi Storage Navigator Modular 2 (however, the maintenance staff is authorized to access the Web maintenance window via the Web browser).
- For the maintenance work, the procedure of the setting operation (time setting of the subsystem, etc.) must be the secured work provided only to the maintenance staff in the Web maintenance window accessed from the Web browser. Furthermore, the administrators other that the maintenance staff must not perform the setting operation in the Web maintenance window.

- The maintenance staff PC is connected to the management LAN only when performing the maintenance work, and in other cases, the maintenance staff must manage the PC to be protected from the unauthorized physical access.

A.SSL

The communication path between Hitachi Storage Navigator Modular 2 and the disk array subsystem is assumed to be protected from the falsification and disclosure.

3.2. Threats

The third person described below is assumed to be a person who is not any of the disk array administrator, account administrator, audit log administrator, maintenance staff, and host user, and does not have the operation authority of the disk array subsystem. Furthermore, the attack capability of the attacker is assumed to be “Low”.

T.MaliciousClient

A third person may use the unmanaged PC (OA PC), access Hitachi Storage Navigator Modular 2 (for GUI) of the management PC (GUI), log in the disk array subsystem, and change the TOE setting value (management information setting parameter of microprogram).

T.MaliciousApplication

A third person may acquire Hitachi Storage Navigator Modular 2 illegally, install it in the unmanaged PC (OA PC), connect to the management LAN, log in illegally, and change the TOE setting value (management information setting parameter of microprogram) of the disk array subsystem.

3.3. Organizational Security Policies

The organizational security policies applied to this TOE are the following items.

P.Role

For the setting operation of the disk array subsystem, the management operation that the operator can perform must be limited based on the role set to the account of the operator. In that case, the event of the management operation must be recorded.

4. Security Objectives

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

4.1. Security Objectives for the TOE

The TOE security objectives are shown below.

O.I&A

TOE must identify/authenticate the operator before the operator performs the management operation of the disk array subsystem.

O.Log

TOE must record the event related to the general function setting parameter change or disk array subsystem status change occurred by the event of the identity authentication of the operator and the management operation. Furthermore, TOE must provide the function to erase the audit log only to the audit log administrator.

O.Role

TOE must be able to restrict the management operation that the operator can perform based on the role set in the account of the operator.

4.2. Security Objectives for the Environment

This section shows the objectives required for the TOE environment.

4.2.1. Security Objectives for the IT Environment

The security objectives required for the IT environment are shown below.

OE.SSL

The communication path between Hitachi Storage Navigator Modular 2 and the disk array subsystem must be protected from the falsification and disclosure using the SSL function provided by the IT environment.

4.2.2. Security Objectives for the Non-IT Environment

The security objectives required for the Non-IT environment are shown below.

OE.Administrator

The reliable people must be assigned to the disk array administrator, account administrator, and audit log administrator. Furthermore, they must take the appropriate education and strengthen that they must not operate/set which interferes the work.

OE.CustomerEngineer

The maintenance staff must be the reliable people who have the sufficient ability and knowledge to perform overall maintenance work of the disk array subsystem safely, to perform correct maintenance work as stated in the procedure manual, and not to commit a fraud.

OE.Environment

This TOE must be used in the environment meeting the following conditions.

- FC-SAN to connect the disk array subsystem, host, or both of them must be set in the secured area where only the disk array administrator, account administrator, audit log administrator, and maintenance staff are authorized for entering/leaving, and must be completely protected from the unauthorized physical access.
- FC-SAN must be used only for the purpose of connecting the disk array subsystem and the host, and must not be connected to other networks or used for other purposes.
- The account management of the host must be performed appropriately, and the third person other than the host user cannot use the host illegally.
- The direct access from the external network must be prevented by the firewall, etc. when connecting the management LAN with the external network such as Internet.
- The management PC and the maintenance staff PC must be managed appropriately so that unauthorized programs (malwares such as keylogger) are not installed or they are not infected by computer viruses.
- RAID Manager must not be used in the disk array subsystem where TOE operates
- The password of the account of the Account Authentication function must be the character string combining a number, the alphabet, and a sign (either of !" # $ % & ' () * + , - . / : ; <=> ? @ [¥] ^ _ ` {|} ~) among the half-width characters.
- When accessing the disk array subsystem via the management LAN, the administrator must use Hitachi Storage Navigator Modular only and not to be accessed by irregular packet such as not creating Hitachi Storage Navigator Modular 2.
- In the maintenance work, the setting operation (time setting of the subsystem, etc.) in the Web maintenance window must not be performed without the operation of the hardware switch on the disk array subsystem in advance. Furthermore, the operation method of the hardware switch must be provided only to the maintenance staff so that any administrators other than the maintenance staff cannot perform the setting operation in the Web maintenance window.
- The maintenance staff PC is connected to the management LAN only when performing the maintenance work, and in other cases, the maintenance staff must manage the PC to be protected from the unauthorized physical access.

5. IT Security Requirements

This Chapter defines the IT security requirements that TOE or other environments must satisfy.
When getting into details for the security requirements, bracket ([ ]) off and underline the place.

5.1. TOE Security Requirements

This Chapter describes the TOE security requirements.

5.1.1. TOE Security functional Requirements

All the functional requirement components used in this section are those specified in CC part2.

(1) Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 TSF must create the audit log of the following auditable events:

a) Starting/completing the audit function;
b) All auditable events for the [Selection: choose one of: minimum, basic, detailed, not specified] level of audit;
c) [Assignment: Other specifically defined auditable events]

FAU_GEN.1.2 TSF must record at least the following information in each audit log:

a) Date and time of the event, type of the event, subject identification information, and the result (success or failure) of the event;
b) For each auditable event type, [Assignment: other audit related information] based on the auditable event definitions of the functional components included in PP/ST

Dependencies: FPT_STM.1 Highly-reliable time stamp

[Selection: choose one of: minimum, basic, detailed, not specified]
Not specified.
[Assignment: other audit related information]
Items shown in the table below

Table 7 Auditable Events

Functional requirement	Foreseen auditable event	Audit record item
FAU_GEN.1	None	-
FAU_GEN.2	None	-
FAU_STG.1	None	-
FAU_STG.4	a) Basic: Action to be taken in case of an audit storage failure.	None
FDP_ACC.1	None	-

FDP_ACF.1	a) Minimum: Successful requirement for executing the operation for the object treated by SFP. b) Basic: All requirements for executing the operation for the object treated by SFP. c) Detailed: Specified security attribute used at the time of the access check.	When changing the general function parameter produced by the management operation or the disk array subsystem status (parameter stored in each table of the object shown in Table 8), the execution result (success or failure) and the operation event are recorded.
FIA_ATD.1	There is no foreseen auditable event.	-
FIA_SOS.1	a) Minimum: Rejection of the tested secret by TSF;; b) Basic: Rejection or acceptance of the tested secret by TSF; c) Detailed: Identification of the change for the defined quality measure.	None
FIA_UAU.2	Minimum: Use that the authentication mechanism was unsuccessful; Basic: All use of the authentication mechanism.	Basic: At the time of attempting the identity authentication, only the execution result (success or failure) and the attempt of the identity authentication are recorded.
FIA_UID.2	a) Minimum: Unsuccessful use of the operator identification mechanisms including the provided operator identification information; b) Basic: All use of the operator identification mechanism including the provided operator identification information.	b) At the time of attempting the identity authentication, only the execution result (success or failure) and the attempt of the identity authentication are recorded.
FIA_USB.1	a) Minimum: Unsuccessful connection (e.g. creating subjects) for the subjects of the user security attribute. b) Success or failure of the connection for the subjects of the user security attribute (e.g. success or failure of creating subjects).	None
FMT_MOF.1	a) Basic: All modifications of the behavior of the TSF function.	At the time of executing the following operation, the execution result (success, failure) and the operation event are recorded. ▪Unlocking, locking, enabling (only for the success), and disabling (only for the success) of the Account Authentication function ▪Unlocking (only for the success), locking, enabling (only for the success), and disabling (only for the success) of the Audit Logging function
FMT_MSA.1	a) Basic: All modifications of the values of the security attribute.	At the time of executing the following operation, the execution result (success 0, failure) and the operation event are recorded. ▪Modification of the role (assignment) (however, this is recorded as an operation event of “account setting”)

FMT_MTD.1	a) Basic: All modifications of the values of the TSF data.	At the time of executing the following operation, the execution result (success 0, failure) and the operation event are recorded. ▪Deletion/creation of the user ID, modification/deletion/creation of all passwords, modification of own password (however, these are recorded as operation events of "account setting") ▪Modification of time zone ▪Deletion of session ID (forcible logout) ▪Modification of the account disabled attribute (account enabled, disabled (however, these are recorded as operation events of "account setting")
FMT_SMF.1	a) Minimum:Using the management function	Events (refer to the followings) corresponding to the function requirements of the other FMT class are recorded. ▪Unlocking, locking, enabling (only for the success), and disabling (only for the success) of the Account Authentication function ▪Unlocking (only for the success), locking, enabling (only for the success), and disabling (only for the success) of the Audit Logging function ▪Modification of the role (assignment) (however, this is recorded as an operation event of "account setting") ▪Deletion/creation of the user ID, modification/deletion/creation of all passwords, modification of own password (however, these are recorded as operation events of "account setting") ▪Modification of time zone ▪Deletion of session ID (forcible logout) ▪Modification of the account disabled attribute (account enabled, disabled (however, these are recorded as operation events of "account setting")
FMT_SMR.1	a) Minimum: Modification for the group with the operator who takes a part of the roles: b) Detailed: All use of the authority of the roles.	None
FPT_RVM.1	None	-
FPT_SEP.1	None	-
FPT_STM.1	a) Minimum: Changing the time; b) Detailed: Providing the time stamp.	None
FTA_SSL.3	a) Minimum: Completing the conversational session by the session lock mechanism.	Recording the completion of the session at the time of the session time-out.

FTA_TSE.1	a) Minimum: Rejecting the session establishment by the session establishment mechanism. b) Basic: All attempts for establishing the operator session. c) Detailed: Acquiring the values of the selected access parameters (e.g. access place, access data).	a) At the time of attempting the identity authentication, the execution result (success or failure) and the attempt of the session establishment are recorded.

[Assignment: other audit related information]
None

FAU_GEN.2 **Relating to the operator identification information**
Hierarchical to: No other components.

FAU_GEN.2.1 TSF must be able to relate each auditable event to the identification information of the operator who caused the event.

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

FAU_STG.1 **Protected audit trial storage**
Hierarchical to: No other components.

FAU_STG.1.1 TSF must protect the stored audit log from the unauthorized deletion.

FAU_STG.1.2 TSF must [Selection: choose one of: prevent, detect] unauthorized modifications to the stored audit log in the audit trial.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.4 Preventing audit data loss
Hierarchical to: FAU_STG.3

FAU_STG.4.1 TSF, when the audit trial becomes full, must perform [Selection: choose one of: ignore auditable events, prevent auditable events other than those related to the authorized operators who have privileges, overwrite to the oldest stored audit log] and [Assignment: other actions to be taken in case of audit storage failures].

Dependencies: FAU_STG.1 Protected audit trial storage

[Selection: choose one of: ignore auditable events, prevent auditable events other than those related to the authorized operators who have privileges, overwrite to the oldest stored audit log]
Overwriting to the oldest stored audit log
[assignment: other actions to be taken in case of audit storage failures]
None

(2) Class FDP: User data protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.

FDP_ACC.1.1 TSF must perform [assignment: access control SFP] for [assignment: list of operations between subjects and objects treated among subjects, objects, and SFP].

Dependencies: FDP_ACF.1 Security attribute based access control

[assignment: list of operations between subjects and objects treated among subjects, objects, and SFP]
Subject:Process on behalf of the operator (microprogram control operation)
Object:
RAID group/LU information table, LU assignment information table, configuration information table, priced option information table (except for Audit Logging function and Account Authentication function)
Operation: Reference, change
[assignment: access control SFP]
Disk array subsystem SFP

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 TSF must perform [Assignment: access control SFP] based on the following [Assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP related security attributes, or named groups of SFP related security attributes].

FDP_ACF.1.2 TSF must perform the following rules to determine if an operation among controlled subjects and controlled objects: [Assignment: rules managing access among controlled subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 TSF must explicitly authorize the 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 TSF must explicitly deny the access of subjects to objects based on the [Assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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

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

Subject:Process on behalf of the operator (microprogram control operation)

Object:

RAID group/LU information table, LU assignment information table, configuration information table, priced option information table (except for Audit Logging function and Account Authentication function)

Subject attribute: Role

Object attribute: None

[assignment: Access control SFP]

Disk array subsystem SFP

[assignment: rules managing access among controlled subjects and controlled objects using controlled operations on controlled objects]

The subject controls the access to the objects, as shown in the table below, based on its attribute (role).

Table 8 Relation of Attribute between the Object and Subject

Object / Attribute of the subject (role)	RAID group/LU information table	LU assignment information table	Configuration information	Priced option information table (except for Audit Logging function and Account Authentication function)
Account Administrator (View and Modify)	C	C	C	B
Account Administrator (View Only)	C	C	C	B
Audit Log Administrator (View and Modify)	C	C	C	B
Audit Log Administrator (View Only)	C	C	C	B
Storage Administrator (View and Modify)	A	A	A	A
Storage Administrator (View Only)	B	B	B	B
Description of the setting operation related to the object	Setting the configuration of the disk array subsystem shown below. •RAID group/LU information table: Creation/deletion/reference of RAID groups, and creation/deletion/reference of LUs •LU assignment information table: Assignment of LUs to the host (setting of host access control) •Configuration information table: Configuration information of the disk array subsystem (operation setting at drive restoration, verify, LU format mode, etc.)			Settings shown below. •Priced option information table: Setting priced options other than the Audit Logging function and Account Authentication function (unlocking, locking, enabled, disabled)

A: Reference and change are possible

B: Reference only

C: No authority

[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

(3) Class FIA: Identity and authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

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

Dependencies: No dependencies

[assignment: list of security attributes]
User ID, session ID, role, account disabled

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

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

Dependencies: No dependencies

[assignment: defined quality metric]
Number of characters: Six characters or more

FIA_UAU.2 User authentication before any action (Authentication by password)

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 TSF must request each user to authenticate itself before permitting any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action (Identity by user)

Hierarchical to: FIA_UID.1

FIA_UID.2.1 TSF must request each user to authenticate itself before permitting any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FIA_USB.1 **User-subject binding**

Hierarchical to: No other components.

FIA_USB.1.1 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.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of user: [assignment: rules for the initial association of attributes].

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 user: [assignment: rules for the changing of attributes].

Dependencies: FIA_ATD.1 User attribute definition

[assignment: list of user security attributes]

User ID, session ID, role,

[assignment: rules for the initial association of attributes]

None

[assignment: rules for the changing of attributes]

None

(4) Class FMT: Security management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 TSF must restrict the ability to [selection: determine, stop, operate, modify the behavior of] the functions [assignment: list of functions] to [Assignment: the authorized identified roles].

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

Assignments and selections of this function requirement are shown in the following table.

Table 9 Operation related to FMT_MOF

List of functions	determine, stop, operate, modify the behavior of	Authorized identified roles
Account Authentication Function	•Account Authentication function is stopped •Account Authentication function is operated	Account Administrator (View and Modify)
Audit Logging Function	•Account Authentication function is stopped •Account Authentication function is operated	Audit Log Administrator (View and Modify)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP, Information flow control SFP] to restrict the ability to [selection: change_defaule, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

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

Assignment and selection of this functional requirement are shown in the table below.

Table 10 Operation related to FMT_MSA.1

List of security attribute	Change_default, query, modify, delete, other operations	Authorized identified roles	Access control SFP, information flow control SFP
Roles	Query, modify	Account Administrator (View and Modify)	Disk array subsystem SFP
	Query	Account Administrator (View Only)	

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].

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

Assignment and selection of these functional requirements are shown in the table below.

Table 11 Operation related to FMT_MTD.1

List of TSF data	Change_default, query, modify, delete, erase, other operations	Authorized identified roles
User ID	Query, delete, other operation: Create	Account Administrator (View and Modify)
	Query	Account Administrator (View Only)
All passwords	Modify, delete, other operations: Create	Account Administrator (View and Modify)
own password	Modify	Account Administrator (View Only) Audit Log Administrator (View and Modify) Audit Log Administrator (View Only) Storage Administrator (View and Modify) Storage Administrator (View Only)
Log	Erasing	Audit Log Administrator(View and Modify)
Session ID	Delete	Account Administrator(View and Modify)
Account disabled	Query, modify	Account Administrator(View and Modify)
	Query	Account Administrator(View Only)

Among the events in Table 11 above, the audit log is not recorded for the event of “Log erasing”. This is because the specification that “Log erasing” is executable only when the storage setting of the audit log to the inside of the disk array subsystem is “Disabled” (that is, the setting not recording the audit log for any events occurred).

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].

Dependencies: No dependencies.

Assignment of this functional requirement is shown in the table below.

Table 12 Operation related to FMT_SMF.1

Required Function	Foreseen management activity	Items to be managed
FAU_GEN.1	None	-
FAU_GEN.2	None	-
FAU_STG.1	None	-
FAU_STG.4	a) Maintenance of actions to be taken at the time of the audit storage failure (delete, modify, add).	a) None. Actions are fixed.
FDP_ACC.1	None	-
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.	a) None. There is no explicit authorization or rule to deny.
FIA_MTD.1	a) If so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	a) None. Security attribute is fixed
FIA_SOS.1	a) The management of the metric used to verify the secrets.	a) None. Scale is fixed.
FIA_UAU.2	Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	▪Creation, modification, and deletion of the password by Account Administrator (View and Modify). ▪Modification of own password by each user.
FIA_UID.2	a) Management of the operator identification information.	a) ▪Creation, deletion, and query of the user ID by Account Administrator (View and Modify). ▪Query of the user ID by Account Administrator (View Only).
FMT_MOF.1	a) Managing the group of roles that can interact with the functions in TSF;	a) None. The group of roles is fixed.
FMT_MSA.1	a) Managing the group of roles that can interact with the security attributes.	a) None. The group of roles is fixed.
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	a) None. The group of roles is fixed.
FMT_SMF.1	None	-
FMT_SMR.1	a) Managing the group of operators who are a part of role.	a) The group of operators who are a part of role is fixed.
FPT_RVM.1	None	-
FPT_SEP.1	None	-
FPT_STM.1	a) Management of the time.	a)None. Providing only the modification of the time information by the maintenance staff as the maintenance work.
FTA_SSL.3	a) Specifying the time that the operator who terminates a dialog session for each operator is inactive; b) Specifying the default time that the operator who terminates a dialog session.	a) None. b) None. The default time is fixed.
FTA_TSE.1	a) Managing the session establishment conditions by the authorized administrator.	a) None. The session establishment conditions are fixed.

The following management functions exist other than the above-mentioned functions.

- Enabled/disabled Account Authentication function
- Enabled/disabled Audit Logging function
- Deletion of session ID
- Query and modification of the account disabled attribute
- Query and modification of roles
- Erasing of audit log

FMT_SMR.1 Security roles
Hierarchical to: No other components.

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

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

Dependencies: FIA_UID.1 Timing of identification

[assignment: authorized identified roles]
Account Administrator (View and Modify)
Account Administrator (View Only)
Audit Log Administrator (View and Modify)
Audit Log Administrator (View Only)
Storage Administrator (View and Modify)
Storage Administrator (View Only)

(5) Class FPT: TSF protection

FPT_RVM.1 **Non-bypassability of the TSP**
Hierarchical to: No other components.

FPT_RVM.1.1 TSF must ensure that TSP performance functions are invoked and successful before each function in TSC is permitted to proceed.

Dependencies: No dependencies.

FPT_SEP.1 **TSF domain separation**
Hierarchical to: No other components.

FPT_SEP.1.1 TSF must maintain a security domain for its own execution that protects it from the interference and falsification by the unreliable subjects.

FPT_SEP.1.2 TSF must perform separation between the security domains of the subjects in TSC.

Dependencies: No dependencies.

FPT_STM.1 **Highly-reliable time stamp**
Hierarchical to: No other components.

FPT_STM.1.1 TSF must be able to provide highly-reliable time stamps for its own use.

Dependencies: No dependencies.

(6) Class FTA: TOE access

FTA_SSL.3 **Termination by TSF start-up**
Hierarchical to: No other components.

FTA_SSL.3.1 TSF must terminate the dialog session after [assignment: time interval in which the operator is inactive].

Dependencies: No dependencies.

[assignment: time interval in which the operator is inactive]
Time specified by Account Administrator (View and Modify).
It must be any of 20, 25, 30, 35, 40, 45, 50, 55, 60, 70, 80, 90, 100, 110 and 120 minutes and 24 hours.

FTA_TSE.1 TOE session establishment
Hierarchical to: No other components.

FTA_TSE.1.1 TSF must be able to deny the session establishment based on [assignment: attribute].

Dependencies: No dependencies.

[assignment: attribute]
Account disabled

5.1.2. Minimum of Function Strength

The minimum level of function strength of this TOE is SOF-basic. The security function requirement based on the stochastic or permutable mechanism is FIA_UAU.2.

5.1.3. TOE Security Assurance Requirements

The evaluation assurance level is EAL2. All assurance requirement components use the EAL2 components specified in CC part3 directly. The security assurance requirements applied to this TOE are shown in the table below.

Table 13 TOE Security Assurance Requirements

Assurance class	Assurance component	
Configuration management (ACM)	ACM_CAP.2	Component
Distribution and operation (ADO)	ADO_DEL.1	Distribution procedure
	ADO_IGS.1	Installation, creation, and startup procedure
Development (ADV)	ADV_FSP.1	Informal function specification
	ADV_HLD.1	Descriptive design of the upper level
	ADV_RCR.1	Demonstration of the informal response
Guidance document (AGD)	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Test (ATE)	ATE_COV.1	Proof of the coverage
	ATE_FUN.1	Function Test
	ATE_IND.2	Independency test-sample
Vulnerability evaluation (AVA)	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

This section describes the security function requirements provided by the IT environment. All the function requirement components used in this section are specified in CC part2.

FTP_ITC.1	Highly-reliable channel between TSF
Hierarchical to:	No other components.
FTP_ITC.1.1	TSF must provide the communication channel which is logically separated from other communication channels, assured identification of its endpoint, and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	TSF must permit that [selection: TSF, remote highly-reliable IT products] start the communication via the highly-reliable channel.
FTP_ITC.1.3	TSF must start the communication via the highly-reliable channel for [assignment: list of functions that the highly-reliable channel is required].
Dependencies:	No dependencies.

[selection: TSF, remote highly-reliable IT products]
Remote highly-reliable IT products

[assignment: list of functions that the highly-reliable channel is required]
All accesses to the disk array subsystem via Hitachi Storage Navigator Modular 2

6. TOE Summary Specification

This chapter describes the TOE security functions, security function strength, and security assurance measures.

6.1. TOE Security Functions

This section describes the TOE security functions. As shown in Table 14, the security functions described in this section satisfy the TOE security function requirements described in "5.1.1. TOE Security Function Requirements".

Table 14 TOE Security Functions and the Corresponding Security Function Requirements

Security Function / Security Function Requirements	FAU_GEN.1	FAU_GEN.2	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_SOS.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FTA_SSL.3	FTA_TSE.1
SF.Account_Authentication			X		X	X	X	X	X	X	X		X	X	X	X	X	X		X	X
SF.Audit_Logging	X	X		X										X	X		X	X	X		
SF.Configuration												X		X	X		X	X			

6.1.1. SF.Account_Authentication

SF.Account_Authentication maintains the identity/authentication of the operator when the operator sets the disk array subsystem by Hitachi Storage Navigator Modular 2, or provides the function related to the account management. Furthermore, TSF related to SF.Account_Authentication protects the own, and assured not to occur the interference and falsification by the unreliable subjects.

(1) Identity/authentication

SF.Account_Authentication compares the registered account information (user ID and password) and the input value once the operator receives the identity/authentication requests of the operator by the user ID and password from Hitachi Storage Navigator Modular 2 when the operator sets the disk array subsystem.

If the user ID and password match the input value and only if "Account disabled" attribute is not set for the account concerned, it determines the identity/authentication successful, creates the session ID corresponding to the account concerned, and relates it to the user ID and role. The created session ID is distributed to Hitachi Storage Navigator Modular 2.

When managing the disk array subsystem, Hitachi Storage Navigator Modular 2 combines the operation command and the session ID and transmits to the disk array subsystem. TSF, if the session ID matches the issued one, determines the operator as the one related to the session ID of the account concerned, and relates the process (microprogram control operation) on behalf of the operator to the provided session ID, user ID and role.

SF.Account_Authentication assures that SF.Account_Authentication is definitely performed when receiving the identity/authentication request of the operator from Hitachi Storage Navigator Modular 2.

(2) Account management

SF.Account_Authentication manages the correspondence of the user ID, password, account disabled attribute, and role per account as the account information.

SF.Account_Authentication provides the measures of operating the query, creation, and deletion of the user ID, creation, modification, and deletion (as entire account), query and modification of the account disabled attribute and role, and deletion (forced logout) of the session ID.

SF.Account_Authentication permits all the above-mentioned operations for the operator who has the role of Account Administrator (View and Modify), and only permits the query of the above-mentioned attributes for the operator who has the role of Account Administrator (View Only). For other operators, it permits only the operation of the modification of own password.

SF.Account_Authentication, when creating or modifying a password, checks whether the number of letters satisfies the quality measure which should be six letters or more, and does not permit the password not satisfying the quality measure.

SF.Account_Authentication maintains each attribute of the security attributes such as the user ID, session ID, role, and account disabled.

(3) Session time-out function

SF.Account_Authentication times out the session when there is no operation for a certain period of time, that is, the session ID is not checked for a certain period of time after logging in Hitachi Storage Navigator Modular 2, and requests the identity/authentication again. The value that can be specified as the session time-out time is any of 20, 25, 30, 35, 40, 45, 50, 55, 60, 70, 80, 90, 100, 110 and 120 minutes and 24 hours.

(4) Execution control by the role

SF.Account_Authentication permits the execution of the command concerned and accesses the general function setting parameter of the related microprogram only when the role given to the account related to the session ID permits the execution of the received command. The relation between the table and the role is shown in the Table 8.

(5) Access restriction to audit log

SF.Account_Authentication permits erasing the audit log (batch deletion of all audit logs) only to the operator who has the role of Audit Log Administrator (View and Modify). This assures that the audit log is protected from the unauthorized modification and deletion.

6.1.2. SF.Audit_Logging

SF.Audit_Logging includes the following audit functions. TSF related to SF.Audit_Logging protects its own and assures that the interference or falsification executed by the unreliable subject does not occur.

(1) Creation of audit log

SF.Audit_Logging creates the audit log when the auditable event related to the security function in TOE occurs. The auditable events to be the log target are shown in "Table 7 Auditable Events". The user ID of the account which has caused each auditable event is given to the audit log to be created. Furthermore, for the date and time used at the time of creating the audit log, the audit log is created based on the time managed by the OS of the disk array subsystem.

SF.Audit_Logging assures that SF.Audit_Logging is definitely performed when the auditable events occur.

(2) Storage of the audit log

SF.Audit_Logging stores up to 2,048 audit logs inside the disk array subsystem. If the number of audit logs exceeds 2,048, it erases the oldest audit log and overwritten by the newly occurred audit log.

6.1.3. SF.Configuration

SF.Configuration provides the measures of enabling or disabling the Account Authentication function (all functions of SF.Account_Authentication) and the Audit Logging function (all functions of SF.Audit_Logging). TSF related to SF.Configuration protects its own and assures that the interference or falsification executed by the unreliable subject does not occur.

The enabled/disabled setting of the Account Authentication function is only allowed to Account Administrator (View and Modify) and the enabled/disabled setting of the Audit Logging function is only allowed to Audit Log Administrator (View and Modify).

SF.Configuration assures that SF.Configuration is definitely performed when the request related the above-mentioned setting is received.

6.2. Level of Security Function Strength

In this TOE, the security function including the stochastic or permutable mechanism to be the target of the security function strength is SF.Account_Authentication.

The security related to the password of the security function has the function strength level of SOF-basic.

6.3. Assurance Measures

Table 15 shows the correspondence of the security assurance requirements and security assurance measures applied to this TOE.

Table 15 TOE Security Assurance Measures

Security Assurance Requirements		Security Assurance Measures
ACM_CAP.2	Components	▪Hitachi Adaptable Modular Storage2100 Configuration Administration List ▪Hitachi Adaptable Modular Storage2300 Configuration Administration List ▪Hitachi Adaptable Modular Storage2500 Configuration Administration List ▪Method of Adding the Hitachi Adaptable Modular Storage~~2300~~ Version
ADO_DEL.1	Distribution procedure	▪Hitachi Adaptable Modular Storage~~2300~~ Distribution Method
ADO_IGS.1	Installation, creation and startup procedure	▪Hitachi Adaptable Modular Storage~~2300~~ ISO/IEC15408 Certification Instruction; Instruction Manual (Maintenance staff)
ADV_FSP.1	Informal function specification	▪Hitachi Adaptable Modular Storage2100 Function Specification ▪Hitachi Adaptable Modular Storage2300 Function Specification ▪Hitachi Adaptable Modular Storage2500 Function Specification
ADV_HLD.1	Descriptive design of the upper level	▪Hitachi Adaptable Modular Storage2100 Higher Level specification ▪Hitachi Adaptable Modular Storage2300 Higher Level specification ▪Hitachi Adaptable Modular Storage2500 Higher Level specification
ADV_RCR.1	Demonstration of the informal response	▪Hitachi Adaptable Modular Storage2100 Representation Correspondence Analysis ▪Hitachi Adaptable Modular Storage2300 Representation Correspondence Analysis ▪Hitachi Adaptable Modular Storage2500 Representation Correspondence Analysis
AGD_ADM.1	Administrator guidance	▪Hitachi Adaptable Modular Storage~~2300~~ ISO/IEC15408 Certification Instruction; Instruction Manual (Administrator)
AGD_USR.1	User guidance	▪Hitachi Adaptable Modular Storage~~2300~~ ISO/IEC15408 Certification Instruction; Instruction Manual (User)
ATE_COV.1	Proof of the coverage	▪Hitachi Adaptable Modular Storage2100 Test Analysis ▪Hitachi Adaptable Modular Storage2300 Test Analysis ▪Hitachi Adaptable Modular Storage2500 Test Analysis
ATE_FUN.1	Function test	▪Hitachi Adaptable Modular Storage2100 Test Specification ▪Hitachi Adaptable Modular Storage2300 Test Specification ▪Hitachi Adaptable Modular Storage2500 Test Specification
ATE_IND.2	Independency test - sample	▪Hitachi Adaptable Modular Storage2100 Test Specification ▪Hitachi Adaptable Modular Storage2300 Test Specification ▪Hitachi Adaptable Modular Storage2500 Test Specification ▪TOE
AVA_SOF.1	Evaluation of the TOE security function strength	▪Hitachi Adaptable Modular Storage 2100 function Specification Analysis ▪Hitachi Adaptable Modular Storage 2300 function Specification Analysis ▪Hitachi Adaptable Modular Storage 2500 function Specification Analysis
AVA_VLA.1	Developer's analysis of	▪Hitachi Adaptable Modular Storage 2100 Analysis of

vulnerability	Vulnerability ▪Hitachi Adaptable Modular Storage 2300 Analysis of Vulnerability ▪Hitachi Adaptable Modular Storage 2500 Analysis of Vulnerability

7. PP Claims

This ST does not claim for any PP.

8. Rationale

This chapter shows the rationales for the security objectives, the security requirements, and TOE summary specifications.

8.1. Security Objectives Rationale

This section shows the rationale for the security objectives.

The security objectives are to realize the assumption and the organizational security policies opposing the threats specified in the TOE security environment. Table 16 shows the corresponding relations among the threats opposing the security objectives, assumptions to be realized, and the organizational security policies.
The table shown below clarifies that each security objective corresponds with one or more assumptions, threats, or organizational security policies.

Table 16 Correspondence of the TOE Security Objectives and the Security Objectives

Security Objectives / Security Environments	TOE			IT environment	Non- IT environment		
	O.I&A	O.Log	O.Role	OE.SSL	OE.Administrator	OE.CustomerEngineer	OE.Environment
A.Administrator					X		
A.CustomerEngineer						X	
A.Environment							X
A.SSL				X			
T.MaliciousClient	X	X					
T.MaliciousApplication	X	X					
P.Role		X	X				

Next, it is shown that each threat can oppose with the security objective or the security policy of the prerequisite/organization can be realized by the security objective.

(1) Prerequisite

A.Administrator

This prerequisite, as shown in OE.Administrator, can be realized by assigning a reliable person to the disk array administrator, account administrator, and audit log administrator. Furthermore, by educating the person, a possibility of performing a setting or operation which interferes the security can be eliminated.

A.CustomerEngineer

This prerequisite, as shown in OE.CustomerEngineer, can be realized by assigning a reliable person who has enough capability but not commit a fraud to the maintenance staff.

A.Environment

This prerequisite, as shown in OE.Environment, can be realized by the following conditions:

- FC-SAN connecting the disk array subsystem, host, or both must be protected physically,
- FC-SAN must be dedicated to the connection between the disk array subsystem and host,
- The Host must be managed so that only the host user can use the host,
- The communication must be controlled by installing the firewall or others between the management LAN and the external network,
- The management PC and the maintenance staff PC must be managed so that any unauthorized programs are not installed,
- RAID Manager must not use the disk array subsystem,
- Only the packet created by Hitachi Storage Navigator Modular 2 can access,
- In the maintenance work, the procedure for setting the operation in the Web maintenance window must be released to the maintenance staff only (including the physical operation of the disk array subsystem known by only the maintenance staff in the procedure for setting the operation so that any administrators other than the maintenance staff cannot set the operation in case they accidentally access the Web maintenance window by the management LAN),
- The maintenance staff PC must be managed to connect it to the management LAN only when the maintenance work is performed and to prohibit the maintenance staff from the unauthorized physical access to this PC.

The acquisition of the identity authentication and the audit log is not required because the operation in the Web maintenance window is the secured maintenance work performed by the maintenance staff.

A.SSL

This prerequisite, as shown in OE.SSL, is realized by utilizing the SSL function provided by the IT environment.

(2) Threats

T.MaliciousClient

This threat is eliminated by O.I&A and O.Log.

O.I&A, even if the connection requests are from HSNM2 prepared in the operation environment, identifies/authenticates the operators before permitting the operation, and denies the login by a third person who is not given the operation authority other than the administrator registered in advance. Therefore, unauthorized operations can be prevented.

O.Log, when an operation event occurs, definitely records the information of the operator and the information of the event as the audit log. If a lot of accesses, such as a brute force attack, occur under this threat, a lot of identified/authenticated audit logs are recorded. Therefore, the trouble is detected and the attack can be prevented by the appropriate response. The number of audit logs that can be stored inside the disk array subsystem is 2,048, and this is enough to detect the attack. Furthermore, only the audit log administrator can erase the audit log, and this administrator is much reliable than the assumptions.

T.MaliciousApplication

This threat is eliminated by O.I&A and O.Log.

O.I&A identifies/authenticates the operator before permitting the operation, and denies the login by a third person who is not given the operation authority other than the administrator registered in advance. Therefore, unauthorized operations can be prevented.

O.Log, when an operation event occurs, definitely records the information of the operator and the information of the event as the audit log. If a lot of accesses, such as a brute force attack, occur under this threat, a lot of identified/authenticated audit logs are recorded. Therefore, the trouble is detected and the attack can be prevented by the appropriate response. The number of audit logs that can be stored inside the disk array subsystem is 2,048, and this is enough to detect the attack. Furthermore, only the audit log administrator can erase the audit log, and this administrator is much reliable than the assumptions.

(3) Organizational security policies

P.Role

The security policies of this organization are realized, as shown in O.Role, by restricting the management operation that the operator can perform based on the role set for the account of the operator when performing the setting operation of the disk array subsystem. Furthermore, O.Log realizes those by recording the event of the management operation (general function setting parameter change or disk array subsystem status change).

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 17 shows the correspondence relation between the TOE security function requirements and the TOE security objectives, and the correspondence relation between the security function requirements for the IT environment and the security objectives for the IT environment. As shown in the table below, it clarifies that each security function requirement of TOE corresponds to one or more TOE security objectives, and each security function requirement for the IT environment corresponds to one or more security objectives for the IT environment.

Table 17 Correspondence of the Security Function Requirements to the Security Objectives

Security Objectives / Security Function Requirements		TOE			IT environment
		O.I&A	O.Log	O.Role	OE.SSL
TOE	FAU_GEN.1		X		
	FAU_GEN.2		X		
	FAU_STG.1		X		
	FAU_STG.4		X		
	FDP_ACC.1			X	
	FDP_ACF.1			X	
	FIA_ATD.1			X	
	FIA_SOS.1	X			
	FIA_UAU.2	X			
	FIA_UID.2	X			
	FIA_USB.1	X			
	FMT_MOF.1			X	
	FMT_MSA.1			X	
	FMT_MTD.1			X	
	FMT_SMF.1			X	
	FMT_SMR.1			X	
	FPT_RVM.1	X	X	X	
	FPT_SEP.1	X	X	X	
	FPT_STM.1		X		
	FTA_SSL.3	X			
	FTA_TSE.1	X			
Environment	FTP_ITC.1				X

Next, it shows that each security objective can be realized by the security function requirement.

O.I&A

The security objectives of this TOE are realized by FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FPT_RVM.1, FPT_SEP.1, FTA_SSL.3, and FTA_TSE.1.

By FIA_UAU.2 and FIA_UID.2, TOE definitely identifies/authenticates the operator before performing the management setting of the disk array subsystem by Hitachi Storage Navigator Modular 2, and does not permit any management/setting operations for the disk array subsystem unless otherwise it is successful.

By FIA_USB.1, if the above-mentioned identity/authentication is successful, it corresponds the operator (process on behalf of) to the user ID, session ID, and role.

By FIA_SOS.1, TOE maintains the quality measure of the secret (password) used for the authentication.

By FTA_TSE.1, TOE permits the session establishment only for the operator whose account is not disabled, and prevents the login to the disabled account.

By FPT_RVM.1, TOE assures that, when performing the management setting operation, the identity/authentication function including the confirmation of the account disabled, and the session time-out function are definitely invoked and successful.

By FPT_SEP.1, TOE, for executing TSF, maintains the security domain to protect TSF from the interference and falsification by the unreliable subjects, and performs the separation between the security domains of the subjects.

By FTA_SSL.3, TOE terminates the session of the operator after the time interval in which the operator is inactive (time specified by Account Administrator (View and Modify), any of 20, 25, 30, 35, 40, 45, 50, 55, 60, 70, 80, 90, 100, 110 and 120 minutes and 24 hours).

O.Log

The security objectives of this TOE are realized by FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FPT_RVM.1, FPT_SEP.1 and FPT_STM.1.

By FAU_GEN.1, TOE creates an audit log of the determined event (event of identity authentication of an operator, event related to the general function setting parameter change or disk array subsystem status change occurred by the operation management). In that case, TOE acquires the time information by FPT_STM.1, and gives the audit log the user ID of the operator who occurred the event. This enables to specify the auditable event, the occurrence date, and the user ID of the operator.

By FAU_STG.1, TOE prevents the unauthorized modification of the audit log.

By FAU_STG.4, TOE, when the number of audit logs exceeds the specified maximum number, overwrites the oldest audit log and prevents the case not recording the most recent auditable event.

By FPT_RVM.1, TOE assures that the functions related to the creation/protection of the audit log are invoked and successful.

By FPT_SEP.1, TOE, for executing TSF, maintains the security domain to protect TSF from the interference and falsification by the unreliable subjects, and performs the separation between the security domains of the subjects.

O.Role

The security objectives of this TOE are realized by FAU_STG.1, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1 and FPT_SEP.1.

By FMT_MOF.1, TOE restricts the operator who can manage the security function behavior to the specified administrator.

By FMT_MSA.1, TOE restricts the operator who can manage the security attribute to the specified administrator.

By FMT_MTD.1, TOE restricts the operator who can manage the TSF data which affects the security function behavior to the specified administrator.

By FMT_SMF.1, TOE provides the function to manage the settings which affect the security functions such as the account management and time information management when operating the disk array subsystem. By FMT_SMR.1, TOE also maintains the roles of Account Administrator (View and Modify), Account Administrator (View Only), Audit Log Administrator (View and Modify), Audit Log Administrator (View Only), Storage Administrator (View and Modify) and Storage Administrator (View Only), and relates to the administrator. Furthermore, by FDP_ACC.1 and FDP_ACF.1, it restricts the general function setting parameter of the microprogram that can be operated based on the role of the operator. Furthermore, by FIA_ATD.1, TOE maintains the security attribute of the operator.

By FPT_RVM.1, TOE assures that the functions to restrict the operator who can perform the management setting of the security function and general function are invoked and successful.

By FPT_SEP.1, TOE, for executing TSF, maintains the security domain to protect TSF from the interference and falsification by the unreliable subjects, and performs the separation between the security domains of the subjects.

OE.SSL

The security objectives for this IT environment are realized by FTP_ITC.1.

By FTP_ITC.1, the IT environment protects the communication path between Hitachi Storage Navigator Modular 2 and the disk array subsystem from the disclosure and modification.

8.2.2. Dependency of the security function requirements

Table 18 shows the dependency of the security function requirements and the sufficiency. As shown in the table below, the dependency of all the security function requirements used in this ST is satisfied.

Table 18 Dependency of Security Function Requirements

#	TOE/ IT environment	Security function requirements	Dependency defined in CC part2	Security function requirements corresponded by this ST
1	TOE	FAU_GEN.1	FPT_STM.1	#20
2	TOE	FAU_GEN.2	FAU_GEN.1	#1
			FIA_UID.1	#11(*1)
3	TOE	FAU_STG.1	FAU_GEN.1	#1
4	TOE	FAU_STG.4	FAU_STG.1	#3
5	TOE	FDP_ACC.1	FDP_ACF.1	#6
6	TOE	FDP_ACF.1	FDP_ACC.1	#5
			FMT_MSA.3	None(*2)
7	TOE	FIA_ATD.1	None	N/A
8	TOE	FIA_SOS.1	None	N/A
9	TOE	FIA_UAU.2	FIA_UID.1	#11(*1)
10	TOE	FIA_UID.2	None	N/A
11	TOE	FIA_USB.1	FIA_ATD.1	#7
12	TOE	FMT_MOF.1	FMT_SMF.1	#16
			FMT_SMR.1	#17
13	TOE	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	#5
			FMT_SMF.1	#16
			FMT_SMR.1	#17
14	TOE	FMT_MTD.1	FMT_SMF.1	#16
			FMT_SMR.1	#17
15	TOE	FMT_SMF.1	None	N/A
16	TOE	FMT_SMR.1	FIA_UID.1	#11(*1)
17	TOE	FPT_RVM.1	None	N/A
18	TOE	FPT_SEP.1	None	N/A
19	TOE	FPT_STM.1	None	N/A
20	TOE	FTA_SSL.3	None	N/A
21	TOE	FTA_TSE.1	None	N/A
22	IT environment	FTP_ITC.1	None	N/A

*1 : Although it essentially depends on FIA_UID.1, the dependency is satisfied by the upper hierarchy FIA_UID.2.

*2 : Because the objects treated by this TOE are no longer created newly, the dependency on FMT_MSA.3 can be eliminated.

8.2.3. Mutual complementarity of the security function requirements

Other than the dependency in the previous section, the mutual complement is made by the security function requirements without the dependency as described below.

Circumvention:

By FPT_RVM.1, it is assured that all TOE security function requirements are definitely executed and not circumvented.

Interference:

By FPT_SEP.1, all TOE security function requirements are protected from the interference and falsification by the unreliable subjects.

Deactivation:

By FMT_MOF.1, it enables to restrict the run and stop of FAU_GEN.1 to the audit log administrator and the run and stop of FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 to the account administrator, and the run and stop of each can be commanded by operating Hitachi Storage Navigator Modular 2.
Other measures cannot stop running the security function requirements and prevent the deactivation. Since the function stop and behavior change cannot be performed by the operation about other security function requirements, it is not necessary to consider of preventing the deactivation.

8.2.4. Rationale for the internal consistency of the security requirements

It is shown below that each security function requirement is internally consistent, and there is no inconsistency.

(1) Audit

The four security function requirements, FAU_GEN.1, FAU_GEN.2, FAU_STG.1 and FAU_STG.4, relate to the audit. These security function requirements define the audit log, there is no competition or inconsistency, and the contents are consistent.
FIA_UID.2 having the dependency relation with these requirements supports FAU_GEN.2, and FPT_STM.1 supports FAU_GEN.1. FMT_MTD.1 also defines the audit log management and supports FAU_STG.1. FPT_RVM.1 is the requirement for preventing bypass and FPT_SEP.1 is the one for separating the security domain. No competition or inconsistency occurs.

(2) Access control

The two security function requirements, FDP_ACC.1 and FDP_ACF.1, relate to the access control. These security function requirements define the access control. They request the same SFP application for the same subject and object, there is no competition or inconsistency, and the contents are consistent.
FPT_RVM.1 is the requirement for preventing bypass and FPT_SEP.1 is the one for separating the security domain. No competition or inconsistency occurs.

(3) Identity/authentication

The five security function requirements, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2 and FIA_USB.1, relate to the identity/authentication. These security function requirements respectively define the identity/authentication by the user ID and password for the access from Hitachi Storage Navigator Modular 2 and the identification by the session ID afterwards, correspondence of the process (microprogram control operation) on behalf of the operator and the operator, and maintenance of the security attribute. There is no competition or inconsistency among these and the contents are consistent.

Furthermore, FPT_RVM.1 is the requirement for preventing bypass and FPT_SEP.1 is the one for separating the security domain. No competition or inconsistency occurs.

(4) Security management

The four security function requirements, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1, relate to the security management. These security function requirements define the security management. There is no competition or inconsistency of the target security attribute and action to be the target, and the contents are consistent.

FIA_UID.2 having the dependency relation with these requirements supports FMT_SMR.1.

FDP_ACC.1 supports FMT_MSA.1, but there is no competition or inconsistency as they refer to the same SFP. FPT_RVM.1 is the requirement for preventing bypass and FPT_SEP.1 is the one for separating the security domain. No competition or inconsistency occurs.

(5) TSF protection

The three security function requirements, FPT_RVM.1, FPT_SEP.1 and FPT_STM.1, relate to the TSF protection. FPT_STM.1 is the requirement for the time stamp, 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 no competition or inconsistency occurs between the security function requirements and between other security function requirements.

(6) TOE access

The two security function requirements, FTA_SSL.3 and FTA_TSE.1, relate to the TOE access. These security function requirements set a limit for the TOE session establishment, but there is no competition or inconsistency between them and between other security function requirements, and the contents are consistent.

FPT_RVM.1 is the requirement for preventing bypass and FPT_SEP.1 is the one for separating the security domain. No competition or inconsistency occurs.

8.2.5. 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 the section “5.1.2”, “SOF-basic” is insisted as the minimum level of function strength, and the attack capability of the threat agent and the minimum level of function strength are consistent.

8.2.6. Rationale for the Evaluation Assurance Level

The disk array subsystem including this TOE is set in the secured area where entering/leaving is managed, and the attack route is limited to via Interface of the management LAN.
Therefore, it is sufficient if the evaluation for the explicit vulnerability is performed.
Furthermore, since TOE is software and does not include the information to be kept secret such as encryption key, the protection by the development security is not required.
Therefore, EAL2 is appropriate as the evaluation assurance level.

8.3. TOE Summary Specification Rationale

8.3.1. Rationale for the TOE Security Functions

As shown in “Table 14” of “6.1TOE Security Functions”, each TOE security function corresponds to one or more TOE security function requirements. The rationale that each TOE security function requirement can be realized by the TOE security function is shown below.

FAU_GEN.1: Audit data generation

SF.Audit_Logging creates the audit log when the auditable events related to the security function in TOE occur. The auditable events to be the record target are shown in “Table 7 Auditable Events”.
SF.Audit_Logging creates the audit log based on the time managed by the OS of the disk array subsystem for the date and time used at creating the audit log.
Therefore, FAU_GEN.1 is realized by SF.Audit_Logging.

FAU_GEN.2: Relating to the operator identification information

SF.Audit_Logging gives the user ID of the account which has caused each auditable event to the audit log to be created.
Therefore, FAU_GEN.2 is realized by SF.Audit_Logging.

FAU_STG.1: Protected audit trial storage

SF.Account_Authentication permits erasing the audit log (batch deletion of all audit logs) only to the operator who has the role of Audit Log Administrator (View and Modify).
Therefore, FAU_STG.1 is realized by SF.Account_Authentication.

FAU_STG.4: Preventing audit data loss

SF.Audit_Logging stores up to 2,048 audit logs inside the disk array subsystem. If the number of audit logs exceeds 2,048, it erases the oldest audit log and overwritten by the newly occurred audit log.
Therefore, FAU_STG.4 is realized by SF.Audit_Logging.

FDP_ACC.1: Subset access control

SF.Account_Authentication, when the operator changes/refers to the values in the RAID group/LU information table, LU assignment information table, configuration information table, and priced option information table (except for the Audit Logging function and Account Authentication function), checks the role set to the account of the operator, and performs the access control to permit the operation within the authorized range.
Therefore, FDP_ACC.1 is realized by SF.Account_Authentication.

FDP_ACF.1: Security attribute based access control

SF.Account_Authentication, when the operator changes/refers to the values in the RAID group/LU information table, LU assignment information table, configuration information table, and priced option information table (except for the Audit Logging function and Account Authentication function), checks the role set to the account of the operator, and performs the access control to permit the operation within the authorized range.
Therefore, FDP_ACF.1 is realized by SF.Account_Authentication.

FIA_ATD.1: User attribute definition

SF.Account_Authentication maintains each attribute of the user ID which is the security attribute, session ID, role, and account disabled.
Therefore, FIA_ATD.1 is realized by SF.Account_Authentication.

FIA_SOS.1: Verification of secrets

SF.Account_Authentication checks whether the number of letters satisfies the quality measure which should be six letters or more, and does not authorize the password not satisfying the quality measure.
Therefore, FIA_SOS.1 is realized by SF.Account_Authentication.

FIA_UAU.2: User authentication before any action (Authentication by password)

SF.Account_Authentication does not authorize any management/setting operations for the disk array subsystem unless the identity/authentication by password is successful.
Therefore, FIA_UAU.2 is realized by SF.Account_Authentication.

FIA_UID.2: User identification before any action (Identity by user)

SF.Account_Authentication does not authorize any management/setting operations for the disk array subsystem unless the identity/authentication by the user ID is successful.
Therefore, FIA_UID.2 is realized by SF.Account_Authentication.

FIA_USB.1: User-subject binding

SF.Account_Authentication, if the identity/authentication is successful, relates the process (microprogram control operation) on behalf of the operator to the provided session ID, user ID, and role.
Therefore, FMT_USB.1 is realized by SF.Account_Authentication and SF.Configuration.

FMT_MOF.1: Management of security functions behavior

For SF.Configuration, the enabled/disabled setting of the Account Authentication function is only allowed to the operator who is given Account Administrator (View and Modify), and the enabled/disabled setting of the Audit Logging function is only allowed to the operator who is given Audit Log Administrator (View and Modify).
Therefore, FMT_MOF.1 is realized by SF.Account_Authentication and SF.Configuration.

FMT_MSA.1: Management of security attributes

SF.Account_Authentication provides the measures of operating the query of the role and modification. It permits all the above-mentioned operations for the operator who has the role of Account Administrator (View and Modify), and only permits the query of the above-mentioned attributes for the operator who has the role of Account Administrator (View Only).
Therefore, FMT_MSA.1 is realized by SF.Account_Authentication.

FMT_MTD.1: Management of TSF data

SF.Account_Authentication provides the measures of operating the query, creation, and deletion of the user ID, creation, modification, and deletion (as entire account) of the password, query and modification of the account disabled attribute, and deletion (forced logout) of the session ID. It permits all the above-mentioned operations for the operator who has the role of Account Administrator (View and Modify). For other operators, it permits only the operation of the modification of own password.

SF.Audit_Logging permits erasing the audit log (batch deletion of all audit logs) only to the operator who has the role of Audit Log Administrator (View and Modify).
Therefore, FMT_MTD.1 is realized by SF.Account_Authentication and SF.Audit_Logging.

FMT_SMF.1: Specification of Management Functions

SF.Account_Authentication, according to the request by the operator, provides the measures of operating the query, creation, and deletion of the user ID, creation, modification, and deletion (as entire account) of the password, query and modification of the account disabled attribute, and deletion (forced logout) of the session ID. It permits all the above-mentioned operations for the operator who has the role of Account Administrator (View and Modify). For other operators, it permits only the operation of the modification of own password.
SF.Audit_Logging permits erasing the audit log (batch deletion of all audit logs) only to the operator who has the role of SF.Audit_Logging.
SF.Configuration provides the enabled/disabled setting function of the Account Authentication function only to Account Administrator (View and Modify) and the enabled/disabled setting function of Audit Logging function only to Audit Log Administrator (View and Modify).
Therefore, FMT_SMF.1 is realized by SF.Account_Authentication and SF.Audit_Logging.

FMT_SMR.1: Security roles

SF.Account_Authentication, after the identity/authentication was successful, relates the role to the account concerned and maintains it.
Therefore, FMT_SMR.1 is realized by SF.Account_Authentication.

FMT_RVM.1: Non-bypassability of the TSP

SF.Account_Authentication, when the administrator accesses the management function, assures that SF.Account_Authentication is definitely performed when accepting the identity/authentication requirements of the operator by the user ID/password or session ID from Hitachi Storage Navigator Modular 2.
SF.Audit_Logging assures that SF.Audit_Logging is definitely performed when the auditable event occurs.
SF.Configuration assures that SF.Configuration is definitely performed when accepting the enabled/disabled setting of the Account Authentication function and the request related to enabled/disabled of the Audit Logging function.
Therefore, FMT_RVM.1 is realized by definitely invoking SF.Account_Authentication, SF.Audit_Logging and SF.Configuration, performing the identity authentication, access control, log creation, etc., and not bypassing these functions.

FMT_SEP.1: TSF domain separation

SF.Account_Authentication, SF.Audit_Logging and SF.Configuration protect TSF itself used for respective function and protect from the interference/falsification by the unreliable subjects.

Therefore, FMT_SEP.1 is realized by SF.Account_Authentication, SF.Audit_Logging and SF.Configuration.

FMT_STM.1: Highly-reliable time stamp

SF.Audit_Logging creates the audit log based on the time managed by the OS of the disk array subsystem for the date and time used at creating the audit log.

Therefore FMT_STM.1 is realized by SF.Audit_Logging.

FTA_SSL.3: Termination by TSF start-up

SF.Account_Authentication times out the session when there is no operation for a certain period of time and requests the identity/authentication again.

Therefore, FTA_SSL.3 is realized by SF.Account_Authentication.

FTA_TSE.1: TOE session establishment

SF.Account_Authentication determines the identity/authentication successful only if "Account disabled" attribute is not set for the account concerned.

Therefore, FTA_TSE.1 is realized by SF.Account_Authentication.

8.3.2. Rationale for the level of TOE Function Strength

In this TOE, the security function based on the stochastic or permutable mechanism is SF.Account_Authentication. The security function strength of these security functions is determined as "SOF-basic" in "6.2". On the other hand, the minimum level of function strength of TOE is determined as "SOF-basic" in "5.1.2". Therefore, they are both consistent.

8.3.3. Rationale for Assurance Measures

This section describes that the security assurance measures are required and sufficient for the security assurance requirements specified in the evaluation assurance level EAL2.

The correspondence relation between the security assurance requirements and security assurance measures is shown in "Table 15". Table 15 shows that all the security assurance measures are necessary for some security assurance requirements. Furthermore, the contents described in the assurance measures cover the evidences requested by the security assurance requirements specified by this ST.

As mentioned above, each assurance measure described in this ST indicates that it is able to trace the TOE security assurance requirements and also indicates that all the TOE security assurance requirements are satisfied by installing the described assurance measures.

8.4. PP Claims Rationale

This ST does not claim for any PP.