Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2012-08-10 (ITC-2418)
Certification No.	C0421
Sponsor	Hitachi, Ltd.
TOE Name	Hitachi Unified Storage 110 Microprogram
TOE Version	0917/A
PP Conformance	None
Assurance Package	EAL2
Developer	Hitachi, Ltd.
Evaluation Facility	ECSEC Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2013-12-12

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

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme."

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

Evaluation Result: Pass

"Hitachi Unified Storage 110 Microprogram" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Hitachi Unified Storage 110 Microprogram 0917/A" (hereinafter referred to as "this TOE") developed by Hitachi, Ltd., and the evaluation of the TOE was finished on 2013-10 by ECSEC Laboratory Inc. Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Hitachi, Ltd., and provide security information to consumers and procurement personnel who are interested in the TOE.

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

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

1.1 Product Overview

An overview of the functions and operational conditions of this TOE is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

The assurance Package of this TOE is EAL2.

1.1.2 TOE and Security Functionality

This TOE is a control program (software) running in a disk array subsystem "Hitachi Unified Storage 110" which is a storage product of Hitachi, Ltd.

This TOE implements the control when a host computer connected to the disk array subsystem is trying to access to the storage area assigned on the disk array.

There is no assumed threat in this TOE, and the TOE provides security functions to fulfill the assumed organizational security policies. As for the security functions, the following functions are included;

- A function to control access to the storage area in response to the host computer's request;
- A function to allow management operations on disk array subsystem only for the administrators being identified and authenticated; and
- Audit log function that records events for management operation.

For these security functionalities, the evaluation for the validity of the design policy and the correctness of the implementation is conducted in the scope of the assurance package. The next section describes the assumptions that this TOE is assumed.

1.1.2.1 Threats and Security Objectives

Since there is no assumed threat for this TOE, security objectives to counter threats do not exist.

1.1.2.2 Configuration and Assumptions

This TOE is assumed to be operated under the following configuration and assumptions.

- TOE Administrators do not perform malicious operations that may compromise the security of the TOE.

- TOE Administrators are requested to faithfully follow the usage as shown in the guidance documents when they use the TOE. In addition, any undescribed action in the guidance documents for the TOE is strictly prohibited including incorrect operations.

  * Unexpected actions which are not described in the guidance documents include, for example, connecting a PC to the TOE maintenance port and/or installing software unrelated to the TOE to the management console except for the dedicated utility program and browser.

- In this TOE, disk array subsystem including the TOE, host computers, dedicated network to connect host computers with the disk array subsystem, management console, and LAN to connect the management console with the disk array subsystem - all of these are to be mounted under the secure environment where only TOE administrators and maintenance personnel are allowed to enter/leave, and where each network is set inaccessible from the external network by firewall, etc.

- In this TOE, if the setting of audit log transfer to the Syslog server will be enabled, the transferred audit logs are requested to be managed under secure environment where only Audit Log Administrators are allowed to access in all circumstances including at the timing of transfer and/or after transferring. The audit logs obtained from the TOE are also to be securely managed by the Audit Log Administrators.

- As for TOE security functions, such as audit function, administrator identification and authentication function, and access control function of host computers, each function is set up to be enabled by an administrator of each role when the product is mounted, and it is not allowed to make it disabled after the operation starts.

- As for the operation of the management function of the TOE security functions, it is prohibited to operate using other than the dedicated utility program "Hitachi Storage Navigator Modular 2 (21.70 version)" which is attached to the TOE.

- Regarding the management console that operates the management function of the TOE security functions, all the WEB access is prohibited except for the web operation to the TOE, such as maintenance operation (within the assurance) and the WEB screen operation by the dedicated utility program.

- All the files obtained from the TOE (except for audit logs) are appropriately managed so as to limit the access only to the administrators who obtained by themselves and maintenance personnel. Additionally, the obtained files are not allowed to open and view except for the maintenance personnel (including the administrators themselves).

  * Although administrators do not know about the existence of these files since it is not described in the guidance documents for administrators, there is a certain case like when

any failure occurs, administrators may implement the maintenance operation (within the assurance), which is unnecessary for identification and authentication from the management console, in accordance with maintenance personnel's instruction, and obtain the trace information indicating the usage status like memory information of the disk array subsystem from the TOE. In such a case, decoding the files is not allowed except for the maintenance personnel since there is a possibility that the files may contain any information related to security.

◆ TOE administrators are prohibited to access all the files in the directory, in which the dedicated utility program of the management console is installed.

1.1.3 Disclaimers

1) This TOE was evaluated under the condition of up to two host computers connected to the disk array subsystem. Therefore, if three or more host computers are connected to use, the case is exempt from the assurance of this evaluation.

2) This TOE will be exempt from the assurance of this evaluation when the status changes from the regular mode to the maintenance mode by PC direct connection to the maintenance port of the disk array subsystem or by physical switch-on on the disk array subsystem, because the resulting environment is not the configuration covered by this evaluation.

   The main maintenance operations (exempt from the assurance) are shown as below.

   - Setting of the removed hard disk detecting function on start-up
     It is the setting of the function to detect the removed hard disk when restarting and to prevent its start-up, in case there is any removed hard disk from the disk array subsystem during power-off.

   - Implementation of initialization
     It is the function to put the disk array subsystem, including the TOE, back to before shipment status.

   - Full dump extracting function
     It is the function utilized by maintenance personnel to perform more detailed failure analysis when an intricate failure occurs, which is unable to analyze with the trace information obtained by maintenance operations (within the assurance).

3) This TOE is not evaluated with the optional software, except for the three paid-for options "LUN Manager," "Account Authentication," and "Audit Logging" as security functionality; therefore, if any optional software except for the above three types is installed and operated, it will be exempt from the assurance.

4) There are two types in this TOE depending on the shipment destinations; for Japan and for overseas. The destinations are not limited as for the products for Japan, whereas overseas destinations are limited only to the following three companies in Hitachi group; "Hitachi Data Systems Corporation," "Hitachi Computer Products (America), Inc.," and "Hitachi Computer Products (Europe) S.A.S." Further shipments from these three companies are exempt from the assurance.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2013-10, based on functional requirements and assurance requirements of this TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility and the related evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

This TOE is identified as follows:

TOE Name:	Hitachi Unified Storage 110 Microprogram
TOE Version:	0917/A
Developer:	Hitachi, Ltd.

It is possible for procurement personnel and consumers to confirm that the product is this TOE which is evaluated and certified by the following methods.

There are two delivery styles of this TOE; one is for Japan and another is for overseas. In case of the products for Japan, the TOE is installed into the disk array subsystem and delivered. As for the products for overseas, the software image is transformed into ZIP file and delivered.

The method of confirmation is common between products for Japan and overseas. After confirming the identification of each guidance name and version with the ST, three kinds of information will be displayed on the WEB screen of the maintenance PC connected to the maintenance port of the disk array subsystem or on the screen of the dedicated utility program on the management console connected to the disk array subsystem via LAN. The combined information of the above is collated with the guidance, which makes it possible to recognize the identification information of the TOE.

With these, it is possible for procurement personnel and consumers to confirm the mounted product is this TOE which is evaluated and certified.

3. Security Policy

This chapter describes security function policies and organizational security policies adopted in this TOE.

This TOE accesses to the storage area on the disk array in response to access requests from the host computers connected to the disk array subsystem.

When this TOE accepts an access request from a host computer, the TOE checks if the host computer is allowed to access to the requested storage area, based on the identification information of the host computer which is included in the request script. Only if it is allowed, it enables the access to the requested storage area. With this function, it prevents the access to the unauthorized storage area.

This TOE provides functions to manage these security functions and makes them available only to the reliable and authorized administrators.

The administrator roles of this TOE are divided into three management functions, such as "Account Management," "Disk Array Management," and "Audit Log Management." As for the "Audit Log Management," it is further divided into two; "Administrator (view and modify)" having a permission to set up the Syslog server transferring and "Administrator (view only)" having only a permission to read audit logs. Thus, there are four administrator roles in total. (Refer to Table 3-1.)

Table 3-1 TOE Administrator Role

Account Administrator	Setting of accounts for all the administrators; Forced logout procedure of login administrator; and Setting of session timeout value
Storage Administrator	Management concerning the assignment of host computers' storage area
Audit Log Administrator (view and modify)	Audit log readout; Setting of enabling/disabling audit log transfer to the Syslog server
Audit Log Administrator (view only)	Audit log readout

When the security-related operations are performed, this TOE generates audit logs only if the operation results turn out to be auditable events. For the generated audit logs, only Audit Log Administrators (view and modify) and Audit Log Administrators (view only) are allowed to refer to.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1 and to fulfill the organizational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

There is no assumed threat for this TOE.

3.1.1.2 Security Function Policies against Threats

Since there is no assumed threat for this TOE, there is no security function policy to counter.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

This TOE assumes to provide the organizational security policies, limiting to the organization requesting the organizational security policies shown in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.Exclusive_assign	A logical storage area for each host computer must be assigned exclusively to each host computer. In other words, the access from other host computers to the logical storage area used by a host computer must be prohibited.
P.Audit	The TOE must record the following operational events by administrators as audit logs. – Successful and/or failure events on identification and authentication of administrators – Successful events on the setting of enabling/disabling audit log data transfer to the Syslog server – Successful events for the modified operation against session timeout values – Successful and/or failure events on performing the forced logout procedure of login administrators – Successful and/or failure events on the operation of either change_default, modification, or deletion of information associating host computers with logical storage areas When the audit log storage area becomes full, the oldest data must be overwritten by the newest data in turn.
P.User_role	The TOE must distinguish the following roles of users. – Account Administrator (view and modify)* – Account Administrator (view only)* (General functions are provided.)

Identifier	Organizational Security Policy
	– Storage Administrator (view and modify)* – Storage Administrator (view only)* (General functions are provided.) – Audit Log Administrator (view and modify) – Audit Log Administrator (view only) In addition, the following TOE operations are allowed only for the users who have their permissions. – Account Administrator (view and modify)*: Setting of accounts for all the administrators, the forced logout procedure for login users – Account Administrator (view and modify)*: Setting of the session timeout value – Storage Administrator (view and modify)*: Setting of the access control for disk drive storage media – Audit Log Administrator (view and modify): Readout of the audit trail, Setting of enabling/disabling audit log data transfer to the Syslog server – Audit Log Administrator (view only): Readout of the audit trails *) As for the terms, Account Administrator (view and modify), Account Administrator (view only), Storage Administrator (view and modify), and Storage Administrator (view only), are the terms used in the ST and not defined in this report. The meaning of these terms are: – Account Administrator (view and modify): Synonym with the Account Administrator in this report. – Account Administrator (view only): Administrator allowed to refer to the management information of administrators. – Storage Administrator (view and modify): Synonym with the Storage Administrator in this report. – Storage Administrator (view only): Administrator allowed to refer to the management information of Storage Administrators. These organizational security policies are determined by the Evaluation Facility that readers can sufficiently understand. However, it is judged by the Certification Body that it is hard for readers to understand the detailed requirements of user roles specific to the product specification as the organizational security policies, so the Certification Body added the following contents for better

Identifier	Organizational Security Policy
	understanding of what the above security policies intend. As for the information related to security, the administrators allowed to operate must be restricted per operations shown as below: 1) Setting of the disk array storage area 2) Setting of audit logs 3) Readout of audit logs 4) Setting of administrators
P.Session_timeout	The TOE must forcibly terminate the session of an administrator if the specified session timeout value is exceeded during the operation of the TOE by the administrator.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to fulfill the organizational security policies shown in the Table.

(1) Measures to the organizational security policy "P.Exclusive_assign"

When a host computer requests to access, this TOE checks based on the identification information granted to a host computer, and allows to access only for the storage area assigned to the host computer in advance.

As a result, P.Exclusive_assign is fulfilled.

(2) Measures to the organizational security policy "P.Audit"

This TOE generates audit logs when the events shown in P.Audit occur, and if the audit log storage area becomes full, the oldest data will be overwritten with the newest data in turn so that the loss of new audit logs will be prevented.

As a result, P.Audit is fulfilled.

(3) Measures to the organizational security policy "P.User_role"

This TOE restricts the operations shown in P.User_role to the following administrators.

1) As for the setting of the disk array storage area, it is limited only to the Storage Administrator.

2) As for the setting of audit logs, it is limited only to the Audit Log Administrator (view and modify).

3) As for the readout of audit logs, it is limited only to the Audit Log Administrator (view and modify) and Audit Log Administrator (view only).

4) As for the setting of administrators, it is limited only to Account Administrator.

As a result, P.User_role is fulfilled.

(4) Measures to the organizational security policy "P.Session_timeout"

This TOE provides the forced termination of the administrator's session when the session timeout value of the administrator exceeds the specified limit that was set by the administrator in advance. In addition, the management function to set the session timeout value is limited only to the Account Administrator.

As a result, P.Session_timeout is fulfilled.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate this TOE as useful information for the assumed readers to determine the use of this TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate this TOE. The effective performances of the TOE security functions are not assured unless these assumptions are fulfilled.

Table 4-1 Assumptions

Identifier	Assumptions
A.Environment	In this TOE, disk array subsystem including TOE, host computers, dedicated network to connect host computers with disk array subsystem, management console, and LAN to connect management console with disk array subsystem - all of these are to be mounted under the secure environment where only administrators and maintenance personnel are allowed to enter/leave, and where each network is set inaccessible from the external network by firewall, etc. If the setting of audit log transfer to the Syslog server is enabled, the transferred audit logs are to be securely managed by Audit Log Administrators in all circumstances including at the timing of transfer and/or after transferring.
A.Administrator	TOE administrators are requested to faithfully follow the usage as shown in the guidance documents when they use the TOE. In addition, actions which are not described in the guidance documents for the TOE are strictly prohibited including incorrect operations. * Unexpected actions which are not described in the guidance documents include, for example, connecting a PC to the TOE maintenance port and/or installing software unrelated to the TOE to the management console except for the dedicated utility program and browser.
A.Configuration	As for TOE security functions, such as audit function, administrator identification and authentication function, access control function of host computers, each function is set up to be enabled by an administrator of each role when the product is mounted, and it is not allowed to make it disabled after the

Identifier	Assumptions
	operation starts.

4.2 Environmental Assumptions

This TOE, disk array subsystem including the TOE, host computers, dedicated network to connect host computers with disk array subsystem, management console, and LAN to connect management console with disk array subsystem - all of these are mounted under the secure environment where only TOE administrators and maintenance personnel are allowed to enter/leave, and where each network is set inaccessible from the external network by firewall, etc.

If the operation to transfer audit logs to the Syslog server will be implemented, the Syslog server and the network to connect the Syslog server with the disk array subsystem are also necessary to be mounted in a secure environment. The assumed operational environment of this TOE is shown as Figure 4-1.

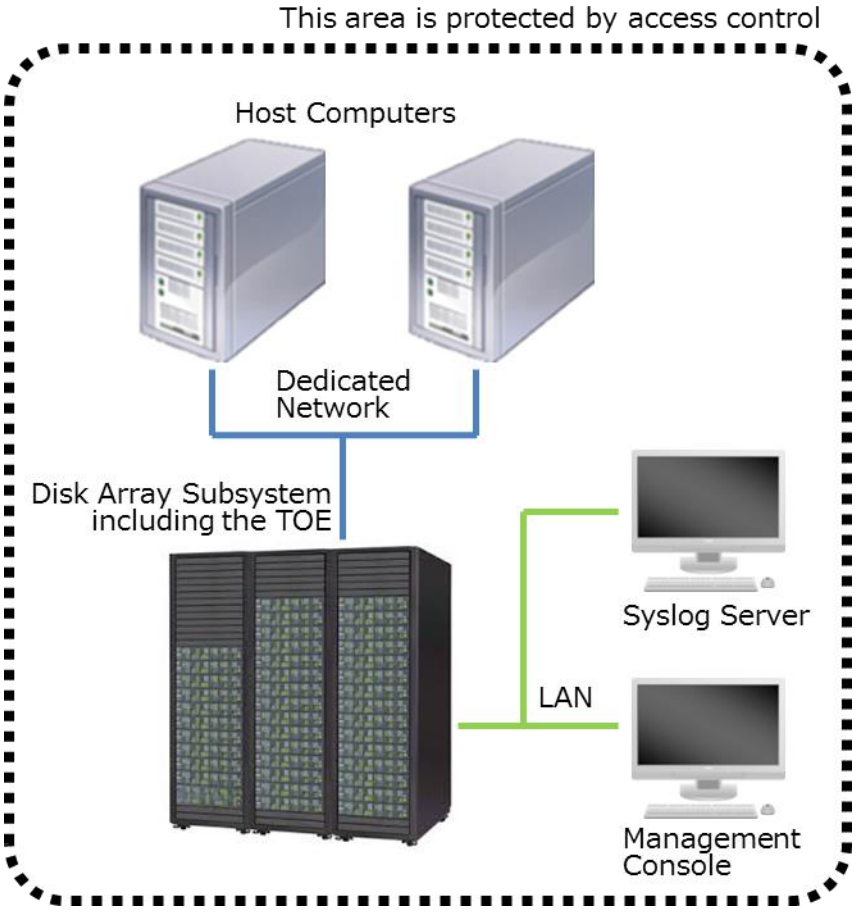

Figure 4-1 Example of Operational Environment of the TOE

The disk array subsystem including the TOE is interconnected to the host computers (up to two computers) via the dedicated network and provides mass storage service having RAID configuration. There are two types of the dedicated networks available; FC-SAN (Fibre Channel Storage Area Network) and IP-SAN (IP Storage Area Network). As for the host

computers connected, it is not limited to the specific models or types, and the operational environment also corresponds to the various OS, such as Windows, HP-UX, and Solaris.

The PC is utilized as the management console of the TOE. The OS of this PC is Windows XP SP3, and this PC is a general-purpose product, on which WEB browser (IE ver.8.0) operates, and the dedicated utility program "Hitachi Storage Navigator Modular 2 (21.70 version) is installed to operate the TOE. This utility program is essential software to use management function of the TOE security functions, and is provided attached to the TOE.

Although it is not shown in the Figure 4-1, there is a possibility that disk array subsystem may be connected to the maintenance PC for the maintenance personnel. The connection method is to connect via LAN, as is the case with the management console.

Note that the reliability of hardware and relevant software shown in this configuration is not covered in this evaluation. (It is assumed to be trustworthy.)

4.3 Clarification of Scope

This TOE decreases the opportunity for administrators to incorrectly input against the received script from the management console by checking the input contents prior to TOE's receiving with the dedicated utility program "Hitachi Storage Navigator Modular 2 (21.70 version)" on the management console. Thus, it is inevitably required to use the dedicated utility program for the management operations of the TOE from the management console, because the prohibition of incorrect operations by administrators, which is required by the assumptions, must be within the realistic scope.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. The TOE is a part of the control software inside the disk array subsystem. The TOE operates on the control hardware. The TOE and control hardware manage a group of disk drives, and it allows the host computers to utilize the assigned storage areas' resources.

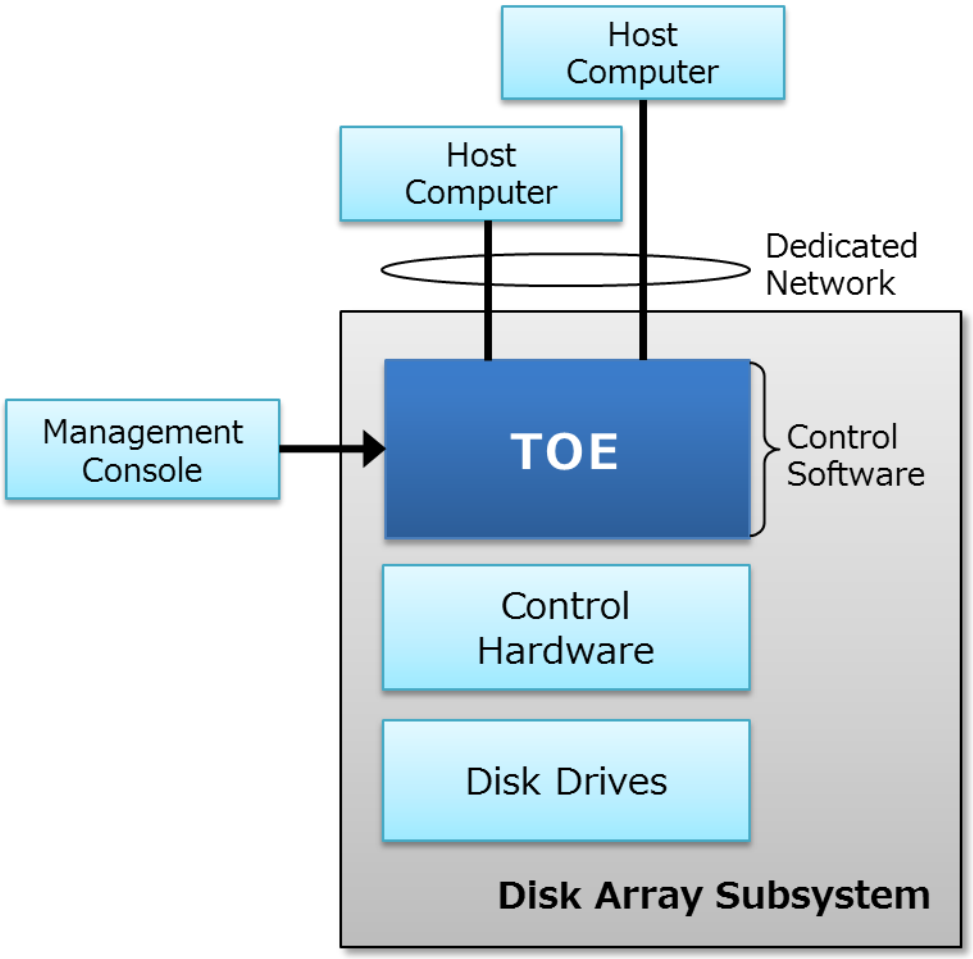

Figure 5-1 TOE Boundary

As the main subsystem of constituting the TOE, the dedicated control of the storage area, identification and authentication of administrators, and audit are explained as follows:

- Dedicated Control of the Storage Area

  It is a subsystem to provide access control of host computers. When a host computer requests operations, based on the identification information (WWN or iSCSI name) of the host computer which is included in the request script as well as on the identification information in the requested storage area, it checks the registered information inside the TOE. Only when the access is allowed (when the host computer and the storage area are

being mapped), it allows access to the requested storage area.

- Identification and Authentication of Administrators

  It is the subsystem to control the administrators' login and administrators' access to each function. When the management console requests to log in, based on the identification information and password of administrators which are included in the request script, it checks the registered information inside the TOE. Only when they are registered as administrators, it allows login. If it is allowed, it issues session ID and stores identification and authentication information, such as administrators' identification information at the timing of login, password, and administrator roles, inside the TOE. Then, the status at the timing of login will be enabled by the time of logout. When the management console requests operations of the management functions after the successful login, based on the session ID and operational command which are included in the request script, it allows the operation of the management functions only if the session ID registered inside the TOE is checked and turns out to be valid, and if the operational command is the allowed operation by the administrator role at the time of login.

- Audit

  It is a subsystem to generate audit logs against the operations of auditable events. When the management console requests operations, the operations are allowed by the account authentication control subsystem, and the operation will either succeed or fail. If the operation result is considered as an auditable event, the audit log control subsystem is called, and it generates audit logs of the operation result.

5.2 IT Environment

This TOE operates on the hardware shown as below, which is in the disk array subsystem.

Control Hardware	HT-4017-XSS/XSL/XSSA/XSLA (DF850XS)
Disk Drive Unit	HT-F4017-DBS/L (24 units for 2.5 type Drive / 12 units for 3.5 type Drive / 3.5 type 48 Drive Chassis)

From a host computer, the request script is sent to the disk array subsystem via the dedicated network, and the input format of the request script is checked by the protocol chip equipped on the disk array subsystem. If the input contents are appropriate, the request script is sent to the TOE, and the request script is processed by the received TOE.

From the management console, the input contents are checked by the dedicated utility program. If the input contents are appropriate, it is transformed by the dedicated utility program into the dedicated protocol of Hitachi, Ltd. Then, it is sent to the TOE via LAN, and the request script is processed by the received TOE.

6. Documentation

The identification of documents attached to this TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to fulfill the assumptions.

In case of this TOE, guidance documents of 1 to 11 in Figure 6-1 are attached to the products for Japan, whereas all the guidance documents in Figure 6-1 are attached to the products for overseas.

Figure 6-1 List of Guidance Documents

Type		Japanese version English version
Program ProductUser's guide	1	Account Authentication ユーザーズガイド（HUS 100シリーズ）第6版
		Hitachi Unified Storage 100 Account Authentication User's Guide 5th
	2	Audit Logging ユーザーズガイド（HUS 100シリーズ）第5版
		Hitachi Unified Storage 100 Audit Logging User's Guide 5th
	3	LUN Manager ユーザーズガイド（HUS 100シリーズ）第4版
		Hitachi Unified Storage 100 LUN Manager User's Guide 4th
Disk array User's guide (with maintenance)	4	HUS 100シリーズ ディスクアレイ ユーザーズガイド 第6版
		Hitachi Unified Storage 100 Series Disk Array System User's Guide 6th
	5	HUS 100シリーズ ディスクアレイ サービスガイド 第6版
		Hitachi Unified Storage 100 Series Disk Array System Service Guide 6th
Disk array User's guide (without maintenance)	6	Hitachi Unified Storage 110 ディスクアレイ ユーザーズ ガイド 第6版
		Hitachi Unified Storage 110 Disk Array System User's Guide 6th
Hitachi Storage Navigator Modular 2 User's Guide	7	Hitachi Storage Navigator Modular 2(for GUI) ユーザーズガイド 第54版
		Hitachi Storage Navigator Modular 2(for GUI) User's Guide 54th
	8	Hitachi Storage Navigator Modular 2(for CLI) ユーザーズガイド 第58版
		Hitachi Storage Navigator Modular 2(for CLI) User's Guide 58th
Host Installation Guide	9	Hitachi Unified Storage 100シリーズ Fibre Channel接続用 ホストインストールガイド 第3版
		Hitachi Unified Storage 100 Series Host Installation Guide for Fibre Channel Connection 3rd
	10	Hitachi Unified Storage 100シリーズ iSCSI接続用 ホストインストールガイド 第2版
		Hitachi Unified Storage 100 Series Host Installation Guide for iSCSI Connection 2nd
Hitachi Unified Storage 100	11	Hitachi Unified Storage 100 ISO/IEC15408 認証取得機能取扱説明書(管理者/利用者編) 第2版

Type	Japanese version English version	
ISO/IEC15408 Certified Functions Guide		Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Administrators/Users) 2nd
	12	Hitachi Unified Storage 100 ISO/IEC15408 認証取得機能取扱説明書(保守員編) 初版
		Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Maintenance) 1st

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of this TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.2 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2012-08 and concluded upon completion of the Evaluation Technical Report dated 2013-10. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2012-09, and examined the procedural status conducted in relation to each work unit for configuration management and delivery by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2012-09 and 2013-07.

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

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and the verification results of the testing performed by the developer, the evaluator performed the reproducibility testing and additional testing that were determined as necessary. Then, it was determined that the penetration testing based on vulnerability assessments was not necessary.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

(1) Developer Testing Environment

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

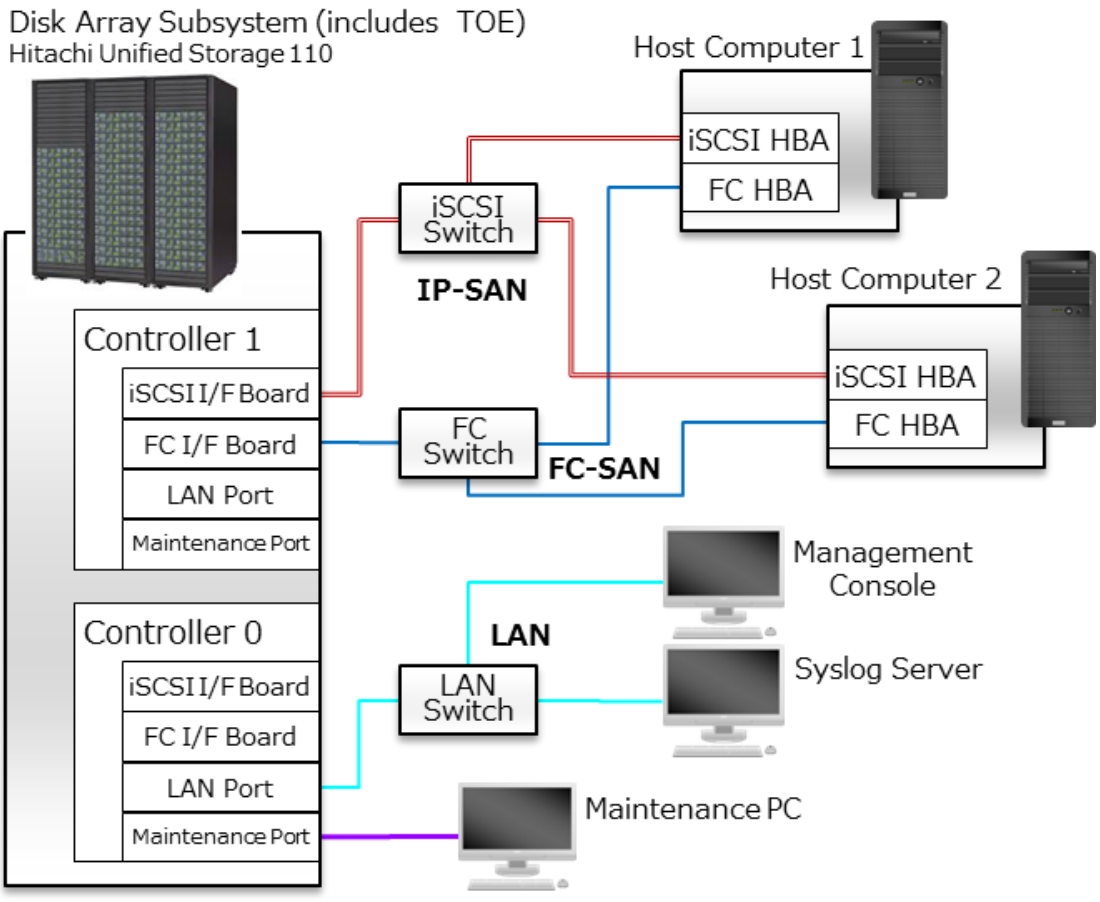

Figure 7-1 Configuration of the Developer Testing

The target TOE for the developer testing is “Hitachi Unified Storage 110 Microprogram 0917/A.”

The components of the developer testing except the TOE are shown in Table 7-1.

Table 7-1 Testing Components except the TOE

#	Name	Overview/Utilization Purpose
1	Disk array subsystem	It is the disk array subsystem "Hitachi Unified Storage 110," on which the TOE is installed.
2	Host Computer 1	The general-purpose PC connected to disk array subsystem via the dedicated network. It is equipped with Host Bus Adapter for iSCSI (iSCSI HBA) and Host Bus Adapter for Fibre Channel (FC HBA). OS: Windows Server 2003 (R2)
3	Host Computer 2	Same as Host Computer 1.
4	Dedicated Network	SAN Network connecting host computers with disk array subsystem. There are two types; FC-SAN and IP-SAN.
5	FC Switch	Equipment Type Name: Brocade 300 It is a relaying device between host computer and disk array subsystem connected by FC-SAN.
6	iSCSI Switch	Equipment Type Name: Brocade 8000 It is a relaying device between a host computer and disk array subsystem connected by IP-SAN.
7	LAN Switch	Equipment Type Name: PCi FXG-05MK It is a switching HUB relaying LAN.
8	LAN	It is a network connecting the management console, maintenance PC, and Syslog server, with disk array subsystem.
9	Management Console	It is a general-purpose PC for management. The dedicated utility program "Hitachi Storage Navigator Modular 2 (21.70 version)" and Java Run time "Java 6 Update 10 (JRE 1.6.0_10)" are to be installed. It is connected to LAN. OS: Windows XP SP3 Browser: Internet Explorer 8.0
10	Maintenance PC	It is a general-purpose PC for maintenance. It is directly connected to the maintenance port of the disk array subsystem, or connected to LAN. The configuration connecting to the maintenance port is used for the start-up test when the product is mounted. In case of the testing for maintenance operation (within the assurance), it is connected to LAN.

#	Name	Overview/Utilization Purpose
		OS: Windows XP SP3 Browser: Internet Explorer 8.0
11	Syslog Server	It is a general-purpose PC for transferring audit logs of the TOE. It is connected to LAN. OS: Windows XP SP3
12	Software for Syslog Server	Software Name: Kiwi Syslog Daemon 8.3.48 It is software to receive audit logs running on the Syslog server, which is a transferring destination, at the testing for the audit log transfer. It is installed to the Syslog server.
13	SCSI Command Issuing Tool	Tool Name: Testtool.exe V1.3 It is a tool to issue the SCSI command (Read/Write) which designates up to the logical address for the storage area inside the disk array subsystem from a host computer. It is saved on the host computer and executed.
14	Batch file for the Testing	File name: Configuration generation script.bat for confirmation of overwriting audit logs It is a script to continuously implement auditable events in order to generate a large number of audit logs of the TOE. It is executed from the dedicated utility program of the management console.

The developer testing is implemented under the TOE testing environment which is the same as the TOE configuration identified in this ST.

(2) Summary of the Developer Testing

(a) Developer Testing Overview

An overview of the developer testing is as follows.

<Developer Testing Approach and Contents>

As for the access to the storage area of a host computer, an operation request was sent to the TOE from the host computer. Then, its behaviour was confirmed, and the expected value and the result were verified.

In addition, regarding a part of the host computer testing, it is impossible to access to certain areas that specified the logical address of the storage area with the regular operations. Therefore, by implementing the testing tool from the host computer generating and sending the request command which is able to access to certain area that designates the logical address of storage area, its behaviour was confirmed, and the expected value and the result were verified.

As for the login to the TOE as well as the management function and audit function of the TOE, login and operations to each function are implemented from the dedicated utility program of the management console, and its behaviour was confirmed, and the expected value and the result were verified.

Furthermore, as for the overwrite function when the audit log area of the TOE reaches the upper limit, the testing batch file which continuously sends the operation request of the auditable events from the management console is implemented. Then, its behaviour was confirmed, and the expected value and the result were verified.

As for the maintenance operations (within the assurance), unlike the configuration in Figure 7-1, the TOE operation is implemented by connecting the maintenance PC with LAN. Then, its behaviour was confirmed, and the expected value and the result were verified.

<Developer Testing Tools>

The testing tools utilized at the developer testing are listed in 12 to 14 of Figure 7-1. The evaluator performed the operation confirmation of these tools at the timing of the evaluator testing and confirmed the appropriateness as testing tools.

(b) Scope of the Performed Developer Testing

The developer testing was performed on 106 items. By the coverage analysis, it was verified that all the security functions and interfaces described in the functional specification had been tested. As a result, the functions to which insufficient tests were provided were supplemented by performing the independent testing.

(c) Result

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

7.3.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the implementation of the security functions of the product by the test items extracted from the developer testing. The evaluator also performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions of the product are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained below.

(1) Independent Testing Environment

The configuration of the independent testing performed by the evaluator was the same as the configuration of the developer testing as shown in Figure 7-1 and Table 7-1. Although it is not shown in Figure 7-1, a testing PC (general-purpose PC) is connected to the mirror port in the mirroring HUB replaced from LAN switch, as necessary in the independent testing.

Furthermore, as for the used testing tools, in addition to the ones used for the developer testing, additional tools prepared by the evaluator are utilized. The specification confirmation, operation test, and calibration for these tools are provided by the evaluator.

(2) Summary of Independent Testing

A summary of the independent testing performed by the evaluator is described as follows.

(a) Independent Testing Viewpoints

The viewpoints for the independent testing that the evaluator designed from the developer testing and the provided evaluation evidential materials are shown below.

<Independent Testing Viewpoints>

1) In the sampling test, tests will be implemented for the test items selected by the following reasons among all the developer testing.
   - The interfaces with more security functions implemented are to be intensively selected and tested.
   - As for the similar tests that differ only in parameters, only one pattern is to be selected and tested.

2) All the interfaces are to be covered by at least one test; either sampling test or independent testing.

3) To cover all the security functions, a testing subset is to be extracted so that it can be tested in the developer testing or independent testing. As a result, some missing behaviors of security functions from the developer testing are found, so the functions which are not covered by the developer testing are to be tested in the independent testing.

4) In the developer testing, the variations of parameters and confirmation methods are insufficient. Therefore, the tests with changed parameters and/or confirmation methods are to be added in the independent testing.

5) A test of updating data for a login administrator, which was not performed in the developer testing, is to be implemented. An additional test having a possibility of affecting the information of the login administrator is implemented by another administrator to confirm if it is appropriately processed as per specification.

(b) Independent Testing Overview

An overview of the independent testing performed by the evaluator is as follows.

<Independent Testing Approach>

It was implemented with the same approach as the developer testing. However, as necessary, the observation and storing communications from the testing PC connected to LAN to the testing tool are performed in addition to the developer testing methodology.

<Independent Testing Tools>

The testing tools used in the independent testing are listed in 12 to 13 of Table7-1. An additional tool used other than the above is shown in Table 7-2. The additional tool is used after installing it to the testing PC. The evaluator performed the operation confirmation of the tool and confirmed the appropriateness as a testing tool.

Table 7-2 Independent Testing Tool

Tool Name	Overview/Utilization Purpose
Wireshark Ver.1.10.0	With this tool, LAN communications are captured, and real-time observation was performed during the testing. The stored communication contents are used as evidence of the testing results.

<Contents of Independent Testing Performed>

The tests were performed, including 34 sampling test and the independent testing with additional 78 test items by the evaluator. The viewpoints of the independent testing and the corresponding test contents are described in Table 7-3.

Table 7-3 Independent Testing Performed

Viewpoints	Overview of the Independent Testing
1) and 2)	Among 106 test items implemented by the developer, 34 test items are extracted based on the viewpoints of the independent testing, and tests are implemented to confirm if the same result will be obtained as the developer testing.
2) and 3)	As for TOE installation, a normal TOE installation is implemented since it was not done in the developer testing, to confirm if the TOE is installed correctly.
	As a supplement of the developer testing, regarding audit log generation, it is to be confirmed if the audit log generation at the time of the startup/shutdown of the TOE is correctly performed.
	As a supplement of the developer testing, regarding the secure initialization of the TOE, a corrupted TOE installation is implemented to confirm that an incomplete TOE will not be installed as a result of the installation failure caused by the completeness checking function against the TOE's self program.
	As a supplement of the developer testing, regarding a host computer accessing to the storage area, a test to change the assigned information of the storage area registered in the TOE is implemented to confirm if the host computer is rejected to access right after the change.
2) and 4)	As for the test of the functions in which the variations of parameters are insufficient, such as letter type of password, threshold, and un-input, parameters are to be changed and tested.
	In order to maintain the consistency of data, as for the function to make the simultaneous login impossible for the administrators who have the same role, tests for only one role were confirmed in the

Viewpoints	Overview of the Independent Testing
	developer testing for making the simultaneous login both possible and impossible. Therefore, in order to confirm all the roles, tests for making it both possible and impossible are to be implemented by changing the roles. The role resulting in making the simultaneous login impossible is only if the role is possible for setting operations.
	As for the access control of administrators, whether all the roles in each function are allowed or rejected is not confirmed in the developer testing, so all the roles in any function are tested to confirm whether it is allowed or rejected at least once. In addition, since it is possible to set up multiple roles for one person, the tests are implemented to confirm the configurable combination of all the roles.
	As a supplement of the developer testing, input is implemented with mixing in the control code, such as delimiter character or file termination character, for the audit log output items. Then, it is to be confirmed if the audit log output is correct after processing appropriately as the specification shows that those control codes are replaced empty or eliminated.
2) and 5)	As a supplement of the developer testing, for the login administrator A and administrator B who have separate roles, administrator C changed the role of administrator A to the same role as administrator B. Then, a test is implemented to confirm that the changed role of administrator A is not reflected by the time of logout, which ensures the impossibility of simultaneous login for the administrators who have the same role, so it prevents the inconsistent data generation.
	As a supplement of the developer testing, regarding a login administrator, if another administrator deletes the login administrator's account. Then, the deleted administrators' sessions are disabled immediately after deletion. Thus, it is to be confirmed if the operation from the deleted administrator is prevented.

(c) Result

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

7.3.3 Evaluator Penetration Testing

The evaluator provided the analysis for the necessity of the evaluator penetration testing

(hereinafter it is called “penetration testing”) on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level, from the evidence shown in the process of the evaluation. As a result, there is no concerned vulnerability under the following assumptions, thus the evaluator determined that there is no need for the penetration testing.

- In this TOE, the operational environment of the TOE is set by the assumptions as secure environment where only administrators and maintenance personnel can enter/leave, and where there is no access from the external network.
- In this TOE, there are no malicious administrators by the assumptions.
- In this TOE, no usage of the TOE other than being described in the guidance is adopted by the assumptions. No incorrect operation occurs.

Therefore, the evaluator confirmed that there is no possibility to occur the concerned vulnerability by the assumptions, and made a judgmental decision that the penetration testing is unnecessary is appropriate.

7.4 Evaluated Configuration

In this evaluation, the configurations shown in “7.3.2 Evaluator Independent Testing” and Figure 7-1 were evaluated.

This TOE does not assume the case of operating different configuration from the above evaluation configuration, such as connecting more than 3 host computers with the disk array subsystem.

Therefore, the evaluator determined the evaluation configuration of the above is appropriate.

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 extended

- Security assurance requirements: Common Criteria Part 3 conformant

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

- All assurance components of EAL2 package

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

7.6 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to the procurement personnel.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. The submitted evidential materials were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

4. Rational of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Report, and related evaluation deliverables, the Certification Body determined that this TOE satisfies all assurance requirements for EAL2 in the CC Part 3.

8.2 Recommendations

In this TOE, if the actions in "1.1.3 Disclaimers" are made, the subsequent impact to the security functions will be exempt from the assurance of this TOE. Therefore, it is advised to make a judgment at the administrator's responsibility about the acceptance of "1.1.3 Disclaimers."

This TOE assumes many assumptions and/or organizational security policies, depending on the product specification. The scope of assurance is also very limited. It is necessary for readers to thoroughly review and consider if those requirements and the scope of the assurance is adaptable for their own operational environments before being installed.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of this TOE is provided as a separate document along with this Certification Report.

Hitachi Unified Storage 110 Microprogram Security Target, Version 1.2, September 25, 2013, Hitachi, Ltd.

11. Glossary

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

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

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

Account Administrator	The administrator allowed to manage TOE administrators, who configures the setting for administrators.
Administrator	A generic name for the administrators allowed to operate the disk array management, account management, and audit log management, which are the management functions of the TOE security functions.
Audit Log Administrator (view and modify)	The administrator allowed to read the audit logs of the TOE and to configure the setting whether the audit log transfer to the Syslog server is implemented or not.
Audit Log Administrator (view only)	The administrator allowed to read the audit logs of the TOE.
Dedicated Utility Program	It is the dedicated utility program “Hitachi Storage Navigator Modular 2 (21.70 version)” which is installed to the management console. It is attached to the TOE. In case of operating the management function of the TOE security functions, it is prohibited to operate using other than this program. Java Runtime “Java 6 Update 10 (JRE 1.6.0_10)” is necessary to operate. There are command line or WEB, and two types of user interfaces.
Disk array subsystem	It is the disk array “Hitachi Unified Storage 110” that the TOE is installed.
Maintenance Mode	It is the maintenance status that enables to switch by connecting the maintenance PC to maintenance port or by entering the physical switch on the disk array subsystem. This

	switching operation is only allowed for the maintenance personnel. Following these procedures, it will be exempt from the assurance once it is switched to another mode.
Maintenance PC	The PC which is used by the maintenance personnel to provide the maintenance work (within the assurance) as well as the maintenance work (exempt from the assurance).
Maintenance Personnel	The personnel who provide the maintenance operations of the disk array subsystem.
Maintenance Port	The port directly connecting the maintenance PC which is mounted on the disk array subsystem.
Maintenance Work (exempt from the assurance)	It is the maintenance work that is exempt from the assurance, which is performed by displaying the maintenance screen via WEB from the maintenance PC connected to the maintenance port or LAN after it is switched to the maintenance mode. There is no need for identification and authentication to operate this maintenance screen. This operation is only allowed for the maintenance personnel.
Maintenance Work (within the assurance)	It is the maintenance work to display the maintenance screen via WEB from the PC connected to the disk array subsystem with LAN in the regular mode. There is no need for identification and authentication to display the maintenance screen. It is possible to obtain the trace information indicating the usage status of memory information in the disk array subsystem and the configuration information (types, quantity, status, etc., of the configured parts). This operation is only allowed for the maintenance personnel and administrators. It will not be exempt from the assurance when this maintenance operation is implemented.
Management Console	The PC utilized by administrators to operate the management functions of the TOE security functions. Depending on the cases, it is used for the maintenance operations (within the assurance) by administrators. OS: Windows XP SP3 Browser: General-purpose products running IE 8.0
Optional Software	The software as paid-for optional function of the disk array subsystem. It is installed in the disk array subsystem in advance as a part of the TOE, but it is inactive and will be activated when the license key of each option is entered.

	The security functions of the TOE, such as audit function, identification and authentication function of administrators, access control function of host computers, will be enabled when the optional software “Audit Logging,” “Account Authentication,” and “LUN Manager” will be activated when the product is mounted. It should be noted that activating software other than those three optional software is prohibited by the guidance.
Regular Mode	The regular operation status which is not switched to the maintenance mode.
Storage Administrator	The administrator allowed for disk array management of the TOE, who configures the setting for assigning storage area on the disk array of a host computer.

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

Disk Array	By logically unifying multiple disk drives (hard disks, in general), it is handled as one disk drive. The disk array subsystem including this TOE is a type in which a unified disk drive is logically divided, and each drive is assigned to the separate host computers and used.
FC-SAN	FC-SAN (Fibre Channel Storage Area Network) is a network that the optical fibre is served as a medium.
Host Computer	It is the PC connecting to use the storage service provided by the disk array subsystem including this TOE. The interfaces provided by this disk array subsystem are independent from the specific file system, and it is possible to use various OS, such as Windows, HP-UX, and Solaris.
IP-SAN	IP-SAN (IP Storage Area Network) is a network using SCSI protocol on the IP network such as Ethernet.
iSCSI Name	iSCSI Name is, in case of a host computer connected via IP-SAN, cognitive information given as specific information to the iSCSI HBA (Host Bus Adaptor) mounted on the host computer.
WWN	WWN (World Wide Name) is, in case of a host computer connected via FC-SAN, an identification information given as a unique number to the Fibre Channel HBA (Host Bus Adaptor) mounted on the host computer.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2013, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

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

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

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

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

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

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

[12] Hitachi Unified Storage 110 Microprogram Security Target, Version 1.2, September 25, 2013, Hitachi, Ltd.

[13] Hitachi Unified Storage 110 Microprogram 0917/A Evaluation Technical Report, Version 2.3, October 8, 2013, ECSEC Laboratory Inc. Evaluation Center