



# Certification Report

Koji Nishigaki, Chairman  
Information-technology Promotion Agency, Japan

## Target of Evaluation

Application date/ID	2008-03-25 (ITC-8210)
Certification No.	C0220
Sponsor	Hitachi, Ltd.
Name of TOE	Hitachi Adaptable Modular Storage 2300 Microprogram
Version of TOE	0862/A-M
PP Conformance	None
Conformed Claim	EAL2
Developer	Hitachi, Ltd.
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

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

2009-06-29

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

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

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

## Evaluation Result: Pass

"Hitachi Adaptable Modular Storage 2300 Microprogram" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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 .....	1
1.1 Introduction .....	1
1.2 Evaluated Product .....	1
1.2.1 Name of Product .....	1
1.2.2 Product Overview .....	1
1.2.3 Scope of TOE and Overview of Operation.....	1
1.2.4 Participants of TOE.....	5
1.2.5 TOE Functionality.....	6
1.3 Conduct of Evaluation.....	7
1.4 Certification .....	7
1.5 Overview of Report .....	8
1.5.1 PP Conformance.....	8
1.5.2 EAL .....	8
1.5.3 SOF .....	8
1.5.4 Security Functions.....	8
1.5.5 Threat.....	8
1.5.6 Organisational Security Policy .....	8
1.5.7 Configuration Requirements .....	9
1.5.8 Assumptions for Operational Environment .....	9
1.5.9 Documents Attached to Product .....	10
2. Conduct and Results of Evaluation by Evaluation Facility.....	12
2.1 Evaluation Methods .....	12
2.2 Overview of Evaluation Conducted .....	12
2.3 Product Testing .....	12
2.3.1 Developer Testing.....	12
2.3.2 Evaluator Testing.....	14
2.4 Evaluation Result .....	15
3. Conduct of Certification .....	16
4. Conclusion.....	17
4.1 Certification Result.....	17
4.2 Recommendations.....	17
5. Glossary .....	18
6. Bibliography .....	19

## 1. Executive Summary

### 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Hitachi Adaptable Modular Storage 2300 Microprogram" (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Hitachi, Ltd.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

### 1.2 Evaluated Product

#### 1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product: Hitachi Adaptable Modular Storage 2300 Microprogram  
Version: 0862/A-M  
Developer: Hitachi, Ltd.

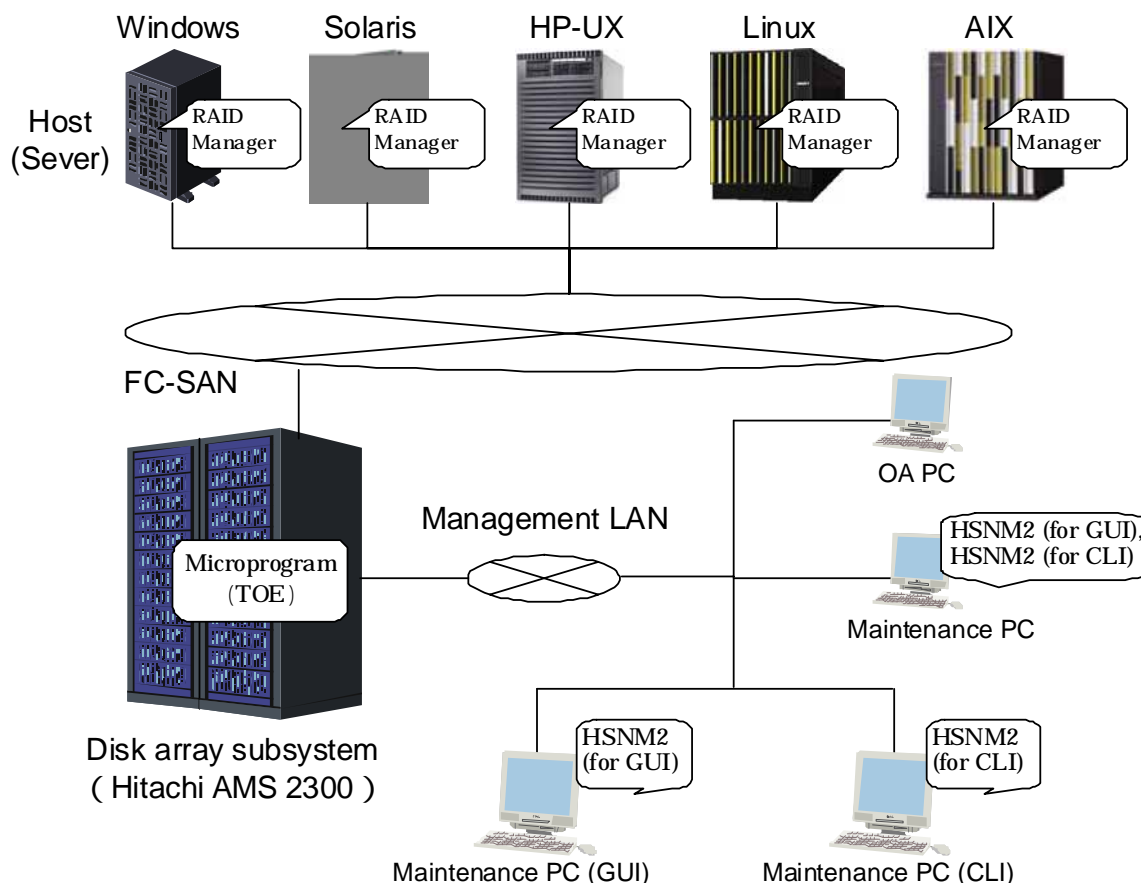
#### 1.2.2 Product Overview

TOE is a control program (software) operated in Hitachi disk array subsystem "Hitachi Adaptable Modular Storage 2300" (hereinafter referred to as Hitachi AMS2300) and controls the operation of the disk array subsystem such as data transfer between the disk array subsystem and the host connected to the disk array subsystem.

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 a security function.

#### 1.2.3 Scope of TOE and Overview of Operation

The disk array subsystem including TOE is generally used in the configuration shown in Figure 1-1.



**Figure 1-1 System Configuration including Disk Array Subsystem**

The system configuration is described below.

(1) Host

Hosts are various open-system servers such as Windows, Solaris and HP-UX connecting with and using the disk array subsystem. The host enables to install RAID Manager which is software for managing the subsystem control information of the disk array subsystem. However, this evaluation targets the subsystem configuration not using RAID Manager.

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

FC-SAN is a dedicated network for the storage system connecting the host and the 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.

(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.

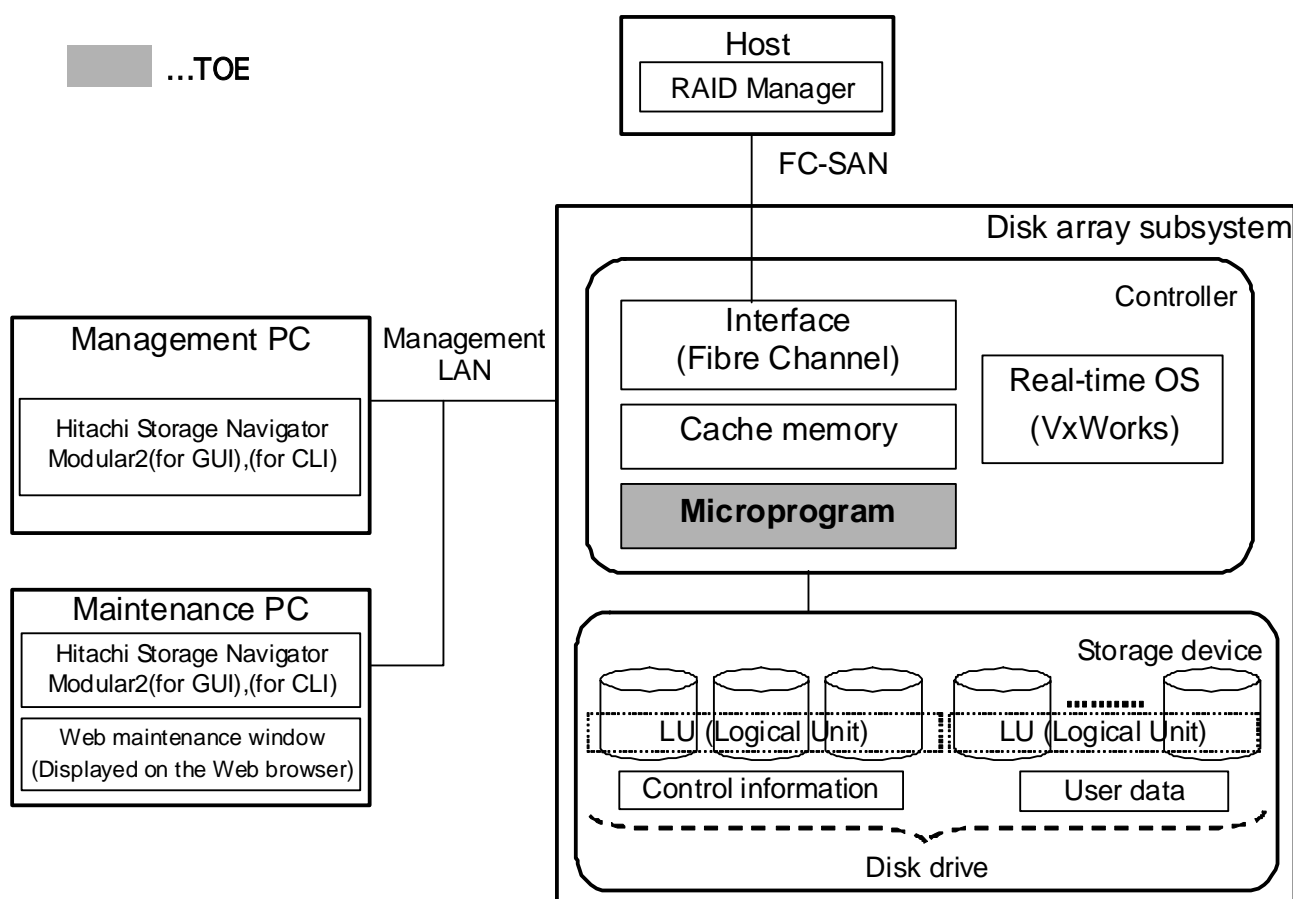
(5) Management PC (GUI)

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) (hereinafter, Hitachi Storage Navigator Modular 2 is referred to as HSNM2), which is a disk array subsystem setting program, is installed. The administrators (disk array administrators, account administrators, and audit log administrators) to be described later or maintenance staff operates this subsystem. This computer and the disk array subsystem are connected via the management LAN. It uses the Web browser, starts HSNM2 (for GUI), and accesses TOE of the disk array subsystem.

- (6) Management PC (CLI)  
The management PC (CLI), as well as the management PC (GUI), is a computer used for setting, operating, and managing the disk array subsystem, and HSNM2 (for CLI) is installed.
- (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. HSNM2 (for GUI) or (for CLI) necessary for performing the maintenance work is installed. Furthermore, it may access TOE of the disk array subsystem using the Web maintenance window from the Web browser for the maintenance work. This subsystem and the disk array subsystem are 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 used for setting and displaying the disk array subsystem configuration, displaying 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 can co-exist HSNM2 (for GUI) and (for CLI) in each computer if the conditions of the hardware configuration factors are satisfied.

The relation between the configuration of the disk array subsystem and TOE is shown in Figure 1-2, and TOE is "Microprogram".



**Figure 1-2 Configuration of Storage Subsystem and TOE**

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. The description of each component is shown below. Note that the devices to be embedded in the disk array subsystem and software are factory-installed.

The configuration of the disk array subsystem is described below.

(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 and, 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 (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.

(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 of this evaluation. This program controls the operation of the disk array subsystem.
- (5) **Storage device**  
The storage device comprises two or more disk drives and stores user data and control information which is 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.

#### 1.2.4 Participants of TOE

The people shown below relate to this TOE.

- (1) **Disk array administrator**  
The disk array administrator is a person who operates HSNM2 in the management PC and manages the disk array subsystem. The role of Storage Administrator (View and Modify) is assigned to this person.
- (2) **Account administrator**  
The account administrator is a person who operates HSNM2 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. The role of Account Administrator (View and Modify) is assigned to this person.
- (3) **Audit log administrator**  
The audit log administrator is a person who operates HSNM2 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 setting for erasing by using the Audit Logging function which is the TOE function. The role of Audit Log Administrator (View and Modify) is assigned to this person.
- (4) **Maintenance staff**  
The maintenance staff is a person belonging to the organization exclusive 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. HSNM2 and the Web maintenance window (a window displayed by entering an IP address of the disk array subsystem in the Web browser) are used when performing the maintenance work. When using HSNM2, the maintenance staff is assigned some administrator roles given by the account administrator of the customer and performs the management operation within the authorized range. In this report, the above-mentioned people from (1) to (4) may be collectively 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/to the host for the storage area of the disk array

subsystem. This person does not manage the disk array subsystem.

### 1.2.5 TOE Functionality

#### 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.

#### 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 HSNM2.

This 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 security functions.

#### (1) Account Authentication function

This function comprises the following functions.

##### [Identity/Authentication]

TOE 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 are matched and "Account Disabled" attribute is not set for the account concerned, the identity/authentication is successful.

Furthermore, when the identity/authentication is successful, it issues a session ID corresponding to the account concerned and distributes it to HSNM2. When managing the disk array subsystem, HSNM2 combines the operation command and session ID and transmits it to the disk array subsystem. When the session ID matches with the one issued, TOE 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]

This manages the user ID, password, account disabled attribute, and role response per account as account information. Furthermore, it provides the measures of managing the account information settings.

#### (2) Audit Logging function

This function comprises the following functions.

[Audit log acquisition]

This 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, it provides the measures of Enabled/Disabled settings of the audit log acquisition.

[Audit log erasing]

This provides the measures of erasing the audit log (batch erasing of all audit logs).

(3) Setting function

This provides the measures of enabling or disabling the Account Authentication function and the Audit Logging function.

### 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Hitachi Adaptable Modular Storage 2300 Microprogram Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "Evaluation Technical Report(BSE-ETR-0001-02)" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

### 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2009-06 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body

prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

## 1.5 Overview of Report

### 1.5.1 PP Conformance

There is no PP to be conformed.

### 1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL2 conformance.

### 1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.

This TOE assumes the attack capability of the threatening agent to be "low", so that "SOF-basic" is sufficient for the minimum level of function strength.

### 1.5.4 Security Functions

Refer to "1.2.5 TOE Functionality" for the security functions of this TOE.

### 1.5.5 Threat

This TOE assumes threats shown in Table 1-1 and provides the functions to counter them.

The third person 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.

**Table 1-1 Assumed Threats**

Identifier	Threat
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.

### 1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

**Table 1-2 Organisational Security Policy**

Identifier	Organisational Security Policy
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.

### 1.5.7 Configuration Requirements

TOE is included in Hitachi disk array subsystem "Hitachi Adaptable Modular Storage 2300".

### 1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE present in the Table 1-3. The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

**Table 1-3 Assumptions in Use of the TOE**

Identifier	Assumptions
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 staff is assumed to be the reliable person who has 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. <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- The account management of the host must be</li> </ul>

	<p>performed appropriately, and the third person other than the host user must not use the host illegally.</p> <ul style="list-style-type: none"> <li>- The management LAN must have the configuration not accessed directly from external networks such as Internet by the firewall, etc.</li> <li>- The management PC and the maintenance staff PC must be managed appropriately so that unauthorized programs (malware such as keylogger) are not installed or they are not infected by computer viruses.</li> <li>- RAID Manager must not be used in the disk array subsystem where TOE operates.</li> <li>- The password of the account of the Account Authentication function must be the character string combining a number, the alphabet, and a sign (any of ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt;=&gt; ? @ [¥] ^ _ ` {   } ~) among the half-width characters.</li> <li>- When accessing the disk array subsystem via the management LAN, the administrator must use Hitachi Storage Navigator Modular 2 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) (Note: Do not access with the tool other than Hitachi Storage Navigator Modular 2.)</li> <li>- 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 than the maintenance staff must not perform the setting operation in the Web maintenance window. (Note: The provision of the use method and operation procedure of the Web maintenance window necessary for the maintenance work must be limited to the maintenance staff.)</li> <li>- 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.</li> </ul>
--	---

#### 1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Hitachi Adaptable Modular Storage 2300 ISO/IEC 15408 Certification Acquisition

- **Function; Instruction Manual (Administrator Volume)**
- **Hitachi Adaptable Modular Storage 2300 ISO/IEC 15408 Certification Acquisition Function; Instruction Manual (User Volume)**
- **Hitachi Adaptable Modular Storage 2300 ISO/IEC 15408 Certification Acquisition Function; Instruction Manual (Maintenance Staff Volume)**
- **Hitachi Adaptable Modular Storage 2100/2300 Series Disk Array User's Guide**

## 2. Conduct and Results of Evaluation by Evaluation Facility

### 2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

### 2.2 Overview of Evaluation Conducted

The history of evaluation conducted was presented in the Evaluation Technical Report as follows.

Evaluation has started on 2008-05 and concluded by completion the Evaluation Technical Report dated 2009-06. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2008-09, 2009-02, 2009-03 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-02, 2009-03.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

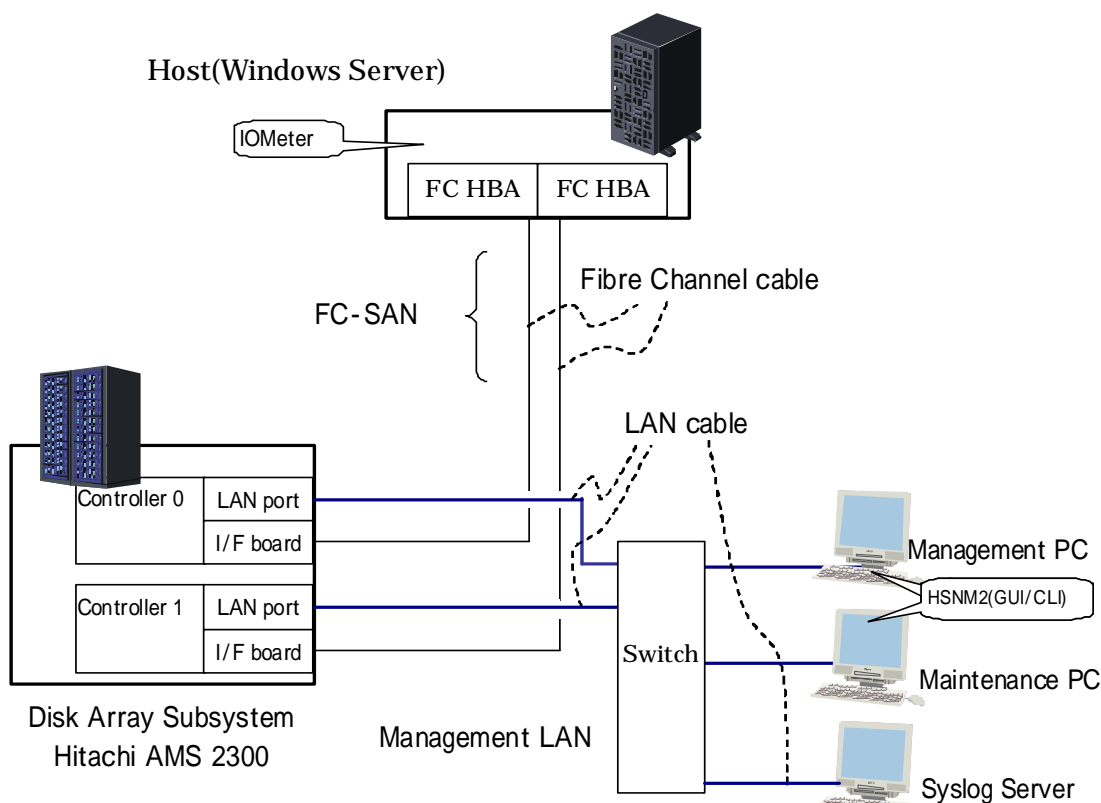
### 2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

#### 2.3.1 Developer Testing

##### 1) Developer Test Environment

Test configuration performed by the developer is shown in the Figure 2-1.



**Figure 2-1 Configuration of Developer Testing**

## 2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

### a. Test configuration

Test configuration performed by the developer is shown in the Figure 2-1. Developer testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

### b. Testing Approach

For the testing, following approach was used.

1. Window display on HSNM2 which is a test tool
2. Result record by audit log function
3. Communication detail log recorded by HSNM2 which is a test tool

### c. Scope of Testing Performed

Testing is performed about 17 items by the developer.

The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

### d. Result

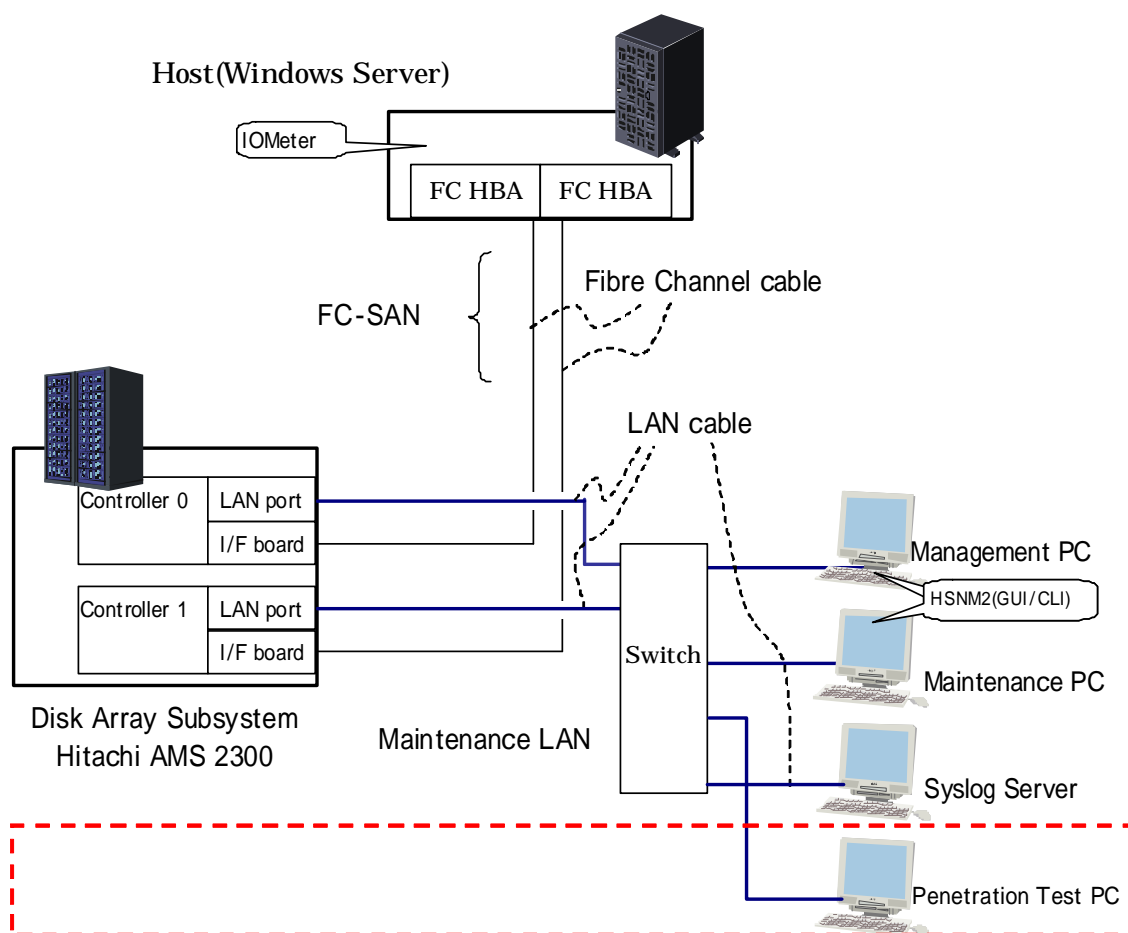
The evaluator confirmed consistencies between the expected test results and the

actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

### 2.3.2 Evaluator Testing

#### 1) Evaluator Test Environment

The configuration of the test performed by the evaluator is the same as the configuration of the developer test, and the PC for the penetration test (to confirm the packet which flows on the network) is added in the penetration test. The configuration is shown below.



**Figure 2-2 Configuration of Evaluator Test**

#### 2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

##### a. Test configuration

Test configuration performed by the evaluator is shown in the Figure 2-2. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

#### b. Testing Approach

For the testing, following approach was used.

1. The test was performed in the same method as the developer test.
2. The network communication packet was captured and the communication contents were observed.

#### c. Scope of Testing Performed

The test of 28 items consisting of 9 independent tests created uniquely by the evaluator, 6 penetration tests, and 13 sampling tests of the developer test was performed.

The followings are considered as the selection criteria of the test items.

1. In the developer test, the sampling test is performed considering completeness/importance of the security functions.
2. In the independent test, the completeness-related test including completeness of combinations and limit values is performed in the TSFI parameter.
3. In the invasion test, based on the vulnerability analysis of the developer, the test related to the behavior due to communication errors, setting information confirmation, etc., and illegal use by similar product information is performed.

#### d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

### 2.4 Evaluation Result

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

### 3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of 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 certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

## 4. Conclusion

### 4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL2 assurance requirements prescribed in CC Part 3.

### 4.2 Recommendations

The threatening agent of this TOE assumes only the attack capability using Hitachi Storage Navigator Modular 2 which is a program for setting the disk array subsystem.

## 5. Glossary

The abbreviations 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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

TOE-specific abbreviations used in this report are shown below.

HSNM2	Hitachi Storage Navigator Modular 2
-------	-------------------------------------

The glossaries used in this report are listed below.

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.
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:	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.
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.

## 6. Bibliography

- [1] Hitachi Adaptable Modular Storage 2300 Microprogram Security Target Revision.11 (April 13, 2009) Hitachi, Ltd.
- [2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01
- [3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02
- [4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03
- [5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001
- [6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002
- [7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003
- [8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)
- [9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)
- [10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)
- [11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- [12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004
- [15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)
- [16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation
- [17] Evaluation Technical Report (BES-ETR-0001-02) Version 1.02, June 18, 2009,

Electronic Commerce Security Technology Laboratory Inc. Evaluation Center