SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 User Data Protection Function Security Target

Version 3.7

June 14, 2007

Hitachi, Ltd.

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

External Trademarks

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

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

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

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

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

AIX is a trademark or registered trademark of IBM Corporation.

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

-Table of Contents -

1. ST Introduction

This section describes the identification information of ST and TOE, the outline of ST, the compatibility with CC, and the glossary.

1.1. ST Identification

The identification information of ST and TOE targeted by ST is described below:

ST: SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 User Data Protection Function Security Target, Version 3.7, June 14, 2007, Hitachi Ltd.

TOE: SANRISE Universal Storage Platform CHA/DKA Program

Version 50-04-34-00/00 (for Japan)

TagmaStore Universal Storage Platform CHA/DKA Program

Version 50-04-34-00/00 (International)

SANRISE Network Storage Controller CHA/DKA Program

Version 50-04-34-00/00 (for Japan)

TagmaStore Network Storage Controller CHA/DKA Program

Version 50-04-34-00/00 (International)

SANRISE H12000 CHA/DKA Program Version 50-04-34-00/00 (for Japan)

SANRISE H10000 CHA/DKA Program Version 50-04-34-00/00 (for Japan)

For the development of this ST, we used the following criteria.

- Common Criteria for Information Technology Security Evaluation Version 2.1(Reference [1][2][3])
- Common Criteria for Information Technology Security Evaluation Version 2.1, Translation Version 1.2, January, 2001 (Reference [4][5][6])
- CCIMB Interpretations-0407 (Reference [7])
- Annex-0210 Version 2 (Reference [8])
- Annex-0407 (Reference [9])

1.2. ST Overview

SANRISE Universal Storage Platform (∗1) and SANRISE H12000, both of which are the storage devices produced by Hitachi Ltd., which realized large capacity, high-speed processing and high reliability. Furthermore, SANRISE SANRISE Network Storage Controller (∗1) and SANRISE H10000 are the storage devices for the mid-range class that maintains the large capacity, the high-speed processing and the high reliability of SANRISE Universal Storage Platform (hereafter referred to as “storage devices”). To a storage device, many hosts of various platforms are connected, via the SAN environment and the IP network environment. Therefore, access control is required for preventing unintended access to user data in the storage device (i.e. changes due to illegal access or erroneous operations to user data which must not be changed).

This ST describes the security functions to protect the integrity of user data in SANRISE Universal Storage Platform, SANRISE H12000, SANRISE Network Storage Controller and SANRISE H10000.

(∗1) Their international names are “TagmaStore Universal Storage Platform” and “TagmaStore Network Storage Controller.”

1.3. CC Conformance

This ST conforms to the following CC specifications:

- The TOE conforms to the CC Part 2.
- The TOE conforms to the CC Part 3, in EAL 2.
- There are no PPs to which this ST conforms.

1.4. Glossary

- LDEV

Short for Logical Device. A unit of volumes created in the user area in the storage. Also called Logical Volume.

- RAID (Redundant Arrays of Inexpensive Disks)

The technology for realizing the disk system that is high-speed, large-capacity and highly reliable, by distributing access across multiple memory devices such as hard disks. RAID is defined varying from RAID0 to RAID6 according to each function.

- SAN

Short for Storage Area Network. The network for the storage only, connecting the storage device to the host computer via Fibre Channel. Fibre Channel enables high-speed and highly reliable data communication.

- Access Attribute

The attribute that shows whether an LDEV is rewritable or read-only. The access attributes is either “write allowed” or “write denied.” To change the access attribute, Data Retention Utility is used.

- S-VOL

The target volume to be used in the copying function of the storage device.

- Remote Copy

The function of copying user data among storage devices for the purposes of user data backup and disaster recovery. Storage devices are connected to one another via Fibre Channel interface. This ST uses the remote copy function when copying user data from another storage device to TOE.

2. TOE Description

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

2.1. TOE Classification

TOE, i.e. “SANRISE Universal Storage Platform CHA/DKA Program Version 50-04-34-00/00,” “SANRISE Network Storage Controller CHA/DKA Program Version 50-04-34-00/00,” “TagmaStore Universal Storage Platform CHA/DKA Program Version 50-04-34-00/00,” “TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00,” “SANRISE H12000 CHA/DKA Program Version 50-04-34-00/00,” and “SANRISE H10000 CHA/DKA Program Version 50-04-34-00/00” (hereafter referred to as CHA/DKA Program”) are the programs (software) operating on the storage devices produced by Hitachi Ltd., “SANRISE Universal Storage Platform,” “SANRISE Network Storage Controller,” “TagmaStore Universal Storage Platform,” “TagmaStore Network Storage Controller,” “SANRISE H12000,” and “SANRISE H10000.”

The above-described storage devices are, though they are different in scale as hardware, all controlled by “CHA/DKA program.” The “CHA/DKA program” used by those storage devices is completely the same one. TOE is loaded on multiple boards in the storage device, and has the role of controlling data transmission between the host connected to the storage device and the storage device.

This TOE provides the function of protecting the user data which must not be changed from any changes due to the users’ erroneous operations or illegal access.

2.2. General Configuration of the System Including the Storage Device

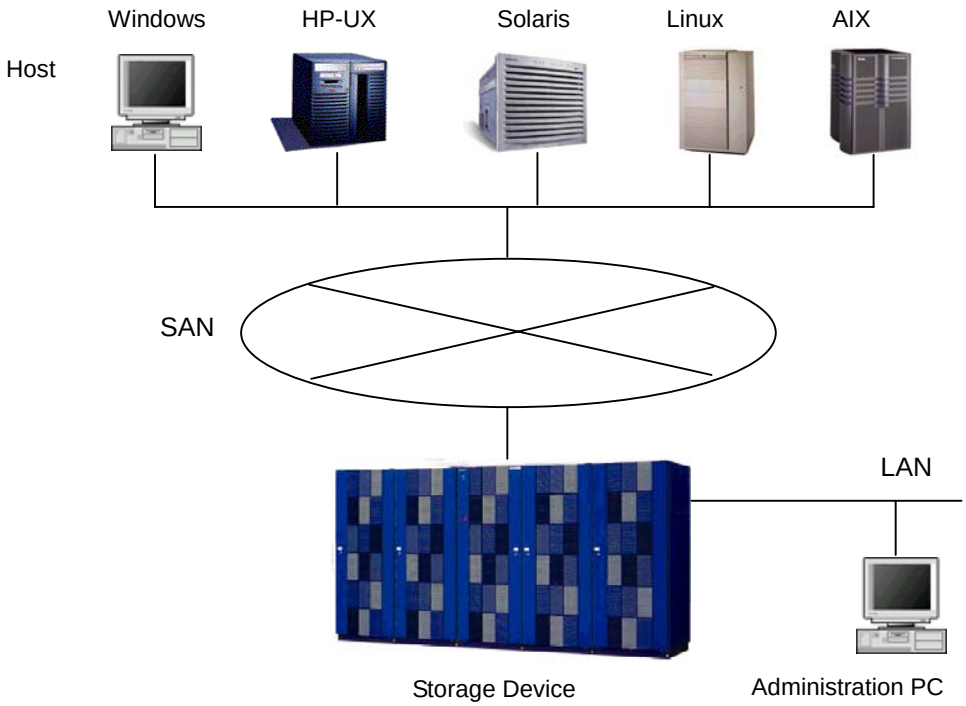

Figure 2.1 General Configuration of the System Including the Storage Device

Figure 2.1 illustrates the general configuration of the system including the storage device. The following is the description of Figure 2.1.

(1) Installation Site of the Storage Device

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

(2) SAN and Hosts

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

(3) Administration PC

The administration PC is the PC for setting up device control information of the storage device from remote sites. Operates the program for the storage device administrator to set up the device control information on the administration PC. The administration PC and the storage device are connected via LAN (Local Area Network).

The administration PC and other PCs are duly connected to LAN by the organization, assuming the environment where only proper people can operate it e.g. those authenticated by the function of the OS.

(4) Storage Device Including TOE

The storage device including TOE is connected to the storage device for remote copy via the Fibre Channel interface. For the storage device for remote copy, the environment is assumed where the storage device is connected as allowed based on the guidance.

2.3. TOE and Storage Device

Figure 2.2 illustrates the general configuration of a storage device.

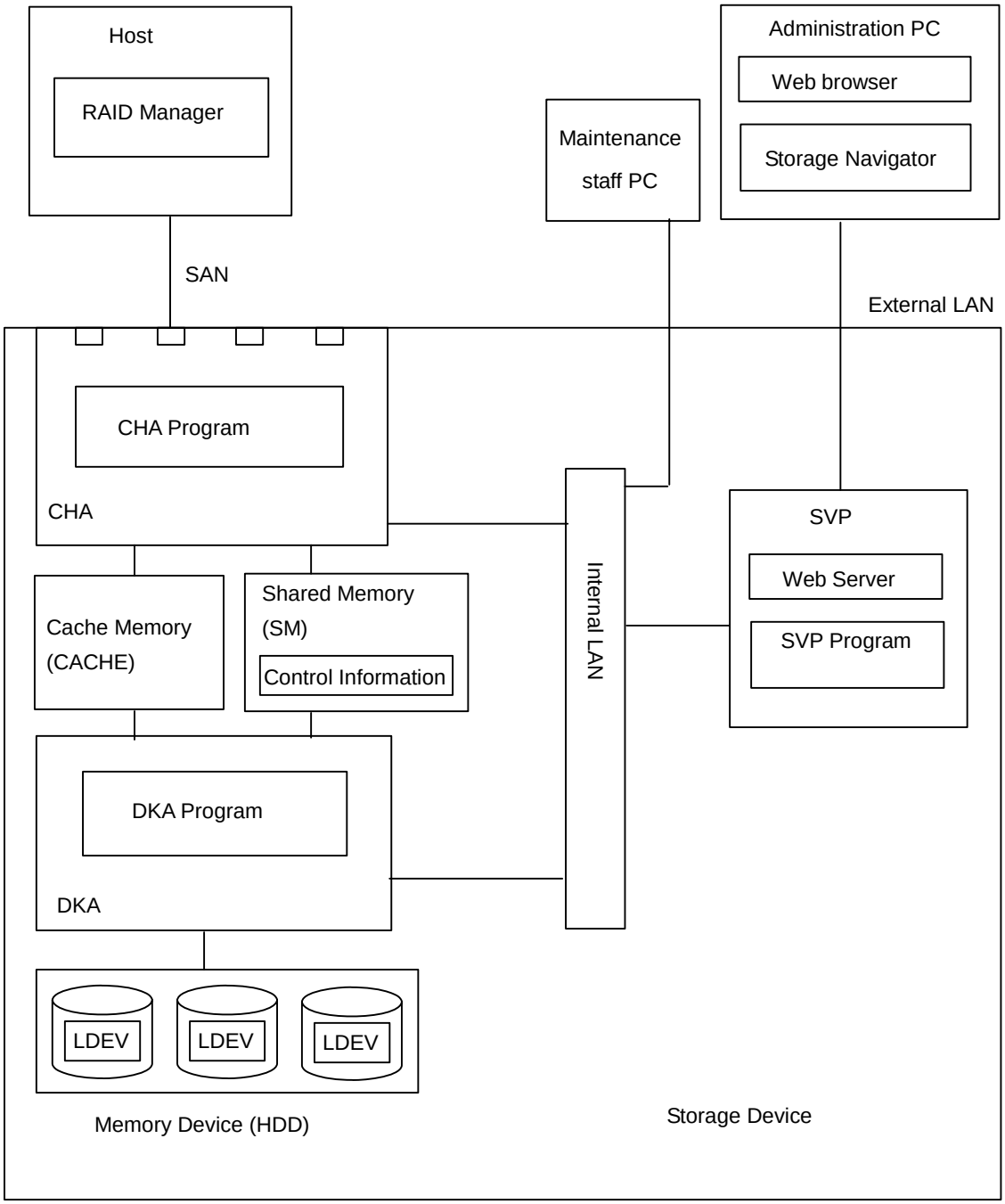

Figure 2.2 Storage Device Configuration

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

2.3.1. Control System

(1) Channel Adapter

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

(2) Disk Adapter

Disk Adapter (DKA) controls data transmission between CACHE and HDD. On DKA, the DKA program which is part of TOE operates. The CHA program and the DKA program work together to realize the “CHA/DKA program” function.

(3) Cache Memory

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

(4) Shared Memory

Shared Memory (SM) is the memory that is accessible both from the CHA program and from the DKA program. Control information for accessing data from CHA and DKA is stored in it. This control information includes the setting information required for the security function to operate is included. Control information on Shared Memory is updated by TOE, according to the commands from SVP or Storage Navigator (see 2.3.2).

(5) Memory Device

Memory Device (HDD) consists of multiple hard disks, in which user data is recorded.

In HDD, an LDEV which is the volume to store user data is created. Access to user data is controlled by the LDEV. HDD improves its reliability by the RAID configuration.

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

2.3.2. Management System

(1) SVP

SVP is a service processor embedded in the storage device for managing the whole storage device. An SVP program operating on the SVP is the software for managing the maintenance function of the storage device (addition, reduction or replacement of components, and program updates) and the device control information, and it has the function of transmitting a command received from Storage Navigator to TOE, to set the device control information. The SVP program has the function to set the operations of the Security function in the storage device. (i.e. Data Retention Utility. See section 2.6.2 for more details.) The SVP program is not included in the TOE.

(2) Maintenance Staff PC

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

(3) Storage Navigator

Storage Navigator is the software used by the storage administrator of the customer (see section 2.4) for administrating the device control information of the storage device. Storage Navigator is an Applet program, which is downloaded from the SVP to the customer PC (administration PC) to be used. To prevent illegal use of Storage Navigator by any malicious third person (see section 3.2), Storage Navigator has the function of identifying and authenticating the user.

Storage Navigator has the function to set the operations of the security function in the storage device (i.e. Data Retention Utility. See section 2.6.2 for more details). The setting command from Storage Navigator to the CHA/DKA program which is TOE is made via SVP. The administrator PC and SVP are connected to each other via external LAN.

Storage Navigator is not included in the TOE.

(4) RAID Manager

RAID Manager is the software used for administrating the device control information of the storage device. A customer who is storage administrator (see section2.4) operates RAID Manager on their host. RAID Manager is not included in TOE. Note that this ST targets device configurations that do not use RAID Manager. (For using RAID Manager, a command device (an LDEV for receiving a command from RAID Manager) needs to be produced, although this ST assumes the environment where a command device is not produced.)

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

Note that the equipments embedded in the storage device are factory-installed, and the user will not prepare or change any of them by themselves.

2.3.3. TOE Range

Figure 2.3 illustrates the range of TOE.

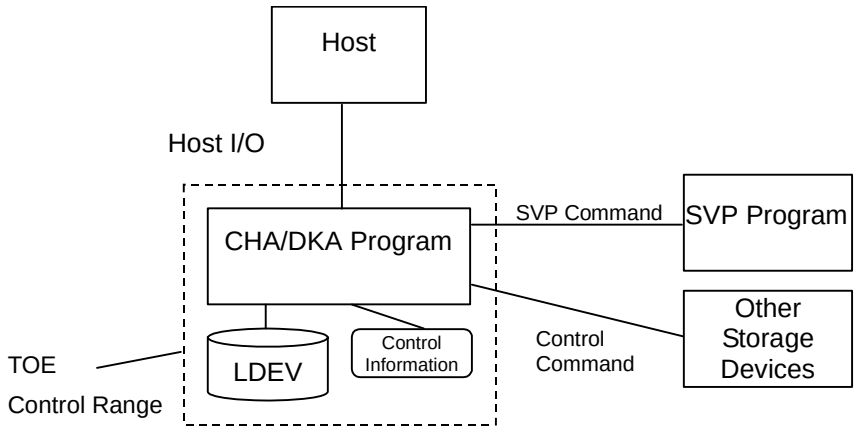

Figure 2.3 TOE Control Range

The CHA/DKA program in Figure 2.3 is TOE, and the area outlined with a dotted line is under the control of TOE. TOE controls the access to the LDEV created in the memory device (HDD) based on the control information stored in Shared Memory.

2.4. Storage Device User

This ST assumes the following users as those concerned with the storage device.

- Storage Administrator

  Administrates the storage device using Storage Navigator on the administration PC. Allowed to operate the setting of Data Retention Utility which is a TOE function (see 2.6.2 for more details).

- Maintenance Staff

  Staff of the special organization for maintenance, with whom the customer who uses the storage device has signed a contract concerning maintenance. Manages the initial startup process in installing the storage device, changing the settings required in maintenance operations such as replacement or addition of parts or disaster recovery. Maintenance staff access SVP from the maintenance staff PC, and executes maintenance operations. Only maintenance staff can directly contact the equipments inside the storage device and manipulate the equipments connected to internal LAN.

- Storage Users

  Storage device users who use the data saved in the storage device through the host connected to the storage device.

2.5. Property To Be Protected

The most important property for a storage device is user data of storage users that is stored in disk drives, and its integrity must be maintained. This ST specifies the user data whose alteration is prohibited according to the command of the storage administrator (or maintenance staff) as the property to be protected. TOE provides the security function of executing access control over the LDEV where user data is stored which must not be changed, and of completely protecting the user data integrity from any changes due to the users' erroneous operations or illegal access. Note that this ST does not discuss the matter of availability of illegally changing the LDEV from access-allowed to access-denied.

2.6. TOE Functions

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

2.6.1 General IT Functions Provided by TOE

The CHA/DKA program which is TOE is the software that controls the operation of the storage device. The CHA program controls the data transmission between the host and the storage device, and the DKA program controls the data transmission between the cache and the disk drive.

For the host to access an LDEV, the port on CHA connected to the host and the LDEV must be associated. The setting of this association is executed on Storage Navigator/SVP. More concretely, a host group (one or more host grouped whose platform(s) is/are equal) is created, and then an LU path is created between the host group and the LDEV whose access is allowed. Data read and write is only possible from the host that belongs to the host group to which the LU path has been set, and no data read or write is allowed from any host that belongs to a host group to which an LU path has been set.

Note that the CHA/DKA program includes the security function described in section 2.6.2 below.

2.6.2 Security Functions Provided by TOE

(1) Data Retention Utility Function

The Data Retention Utility function controls the access from the host to the LDEV based on the access attribute “write allowed” or “write denied,” set to the LDEV in the storage device, and prevents the LDEV with its attributes set to “write denied” from being altered due to the storage user’s erroneous operation or unauthorized access.

As for Data Retention Utility, if the attribute of “write denied” is set to the LDEV, the validity period of that attribute is to be set at the same time. TOE prohibits changing the attribute from “write denied” to “write allowed” during the validity period, no matter what request is made by anything that is not TOE. Changing the access attribute to “write allowed” is accepted when the validity period of the access attribute has expired. In addition, for changing the validity period that has already been set, the period can be extended but cannot be shortened. This is out of consideration for the significance of the user data which is treated by the storage device.

Setting the access attribute and the validity period can be executed on Storage Navigator/SVP. The function of Identifying and authenticating of the storage administrator, and of operating the setting is out of TOE's range, but the process is executed on TOE, of reflecting the setting information received from Storage Navigator/SVP on the control information of the storage device.

The storage device has the function of copying user data for the purpose of user data backup etc. As for the copying function, the copying operation to the LDEV whose access attribute is "write denied" is inhibited. (The use of the copying function from Storage Navigator/SVP to the LDEV whose access attribute is "write allowed" is executed according to the plan of the storage administration operation.)

Also, as for the remote copy function, on a write command from another storage device to an S-VOL in TOE, TOE executes write regardless of access attribute. However, another storage device determines whether to transmit the write command to an S-VOL in TOE, and the whole storage system inhibits any write to the S-VOL that is "write denied."

In addition, as for LDEV creation and updating (i.e. deleting, formatting and shredding), TOE executes any of those operations on command regardless of access attribute. However, it is Storage Navigator/SVP that determines whether to execute update operations, and the whole storage system inhibits any update operations to the S-VOL that is "write denied." Note that updating an LDEV is an extremely important operation which directly affects user data, and it is executed according to the plan of the storage administration operation. Therefore, no update to an LDEV is executed during that operation, from Storage Navigator/SVP to any LDEV that is "write denied."

While the storage user is executing data write or read to or from an LDEV, the whole operation does not allow the storage administrator change the access attribute of the LDEV and the validity period. Related to this inhibition of setting changes, it is Storage Navigator/SVP that determines whether to transmit a command to change the settings to TOE.

Even if the association of the host group and the LDEV, which is a general function of TOE, is erroneously set, or if the host and the port on CHA are erroneously connected, user data in the LDEV stays protected as long as the attribute is set to "write denied" in the LDEV.

The reasons why this function is required are described below.

For limiting access to an LDEV to Read Only by the host OS's function, it might be possible to mount the LDEV Read Only. However, the OS of some hosts does not have the function to mount the LDEV Read Only. In such cases, the storage device will have to set the access

attribute of the LDEV to “write denied.” Even in other cases where the host can mount Read Only, if there are multiple hosts that access the LDEV, the storage device must set the LDEV to “write denied” so as to prevent any wrong manipulation.

Also, if the LDEV is not mounted on the host and the application on the host will access the LDEV by blocks (such as data base), the storage device must set the LDEV to “write denied” since the OS file system cannot set access control.

3. TOE Security Environment

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

3.1. Assumptions

A.PhysicalProtection-Storage

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

A.Protection-Network

It is assumed that, in the customer's network environment including the storage device (external LAN), the storage device cannot be connected from any other product than the administration PC that is used by the storage administrator for administration and operation of the storage device.

A.Protection-PC

The administration PC is assumed to be managed so that the PC can only be used by the storage administrator can use it.

A.Responsibility-Admin

The storage administrator is assumed to be trusted as the person who has the sufficient ability to administrate and operate the storage device, executes the operations exactly as specified by the manual, and never commits any inappropriate behavior.

A.Responsibility-Maintenance

Maintenance staff are assumed to be trusted as the person who has the sufficient skills to

safely execute the general maintenance operations of the storage device, including the connecting operations between the host and the port on CHA, executes the proper operations as specified by the manual, and never commits any inappropriate behavior.

A.Connect-Storage

It is assumed that, if another storage device is connected to TOE for the purpose of remote copy of user data, the storage device that is connected should be the one where the copy operation is executed according to the access attribute of the LDEV in TOE.

3.2. Threats

The property to be protected by this TOE is, out of the user data stored in the storage device, the user data that is defined not to be changed by the storage administrator (or by maintenance staff). The threats that could arise against such user data are described below. Note that “a third person” in the following description indicates the person that is not a storage administrator, a storage user or a maintenance staff, and is not authorized to use the storage device.
In addition, the attack capability of the attacker is assumed to be “low.”

T. Delete/Change_User_Data

A storage user or a third person might make a request for write from the host or the device connected to the SAN to the LDEV where the user data is stored which is prohibited to be changed, and the user data might be changed or deleted.

3.3. Organizational Security Policies

The security policy of the organizations asks Data Retention Utility for the following functions. The requirements described below are the conditions which Data Retention Utility is asked to implement, and they are not prepared for any attacks of the property to be protected.

P.Protect_DRU

TOE must prohibit the change of the attribute from “write denied” to “write allowed,” during the validity period which is set to the LDEV where the user data that must not be changed is stored.

P.Retention_Period

TOE must prohibit the validity period which is set to the access attribute “write denied.” from being shortened.

4. Security Objectives

This section defines the security objectives related to TOE and its environment.

4.1. Security Objectives for the TOE

The security objectives for the TOE is described below.

O.Protect_LDEV

TOE has to be able to control whether to allow any write from the host to the LDEV, based on the access attribute set to the LDEV.

More concretely, TOE has to control whether to allow any write from the host to the LDEV, based on the attribute “write allowed” or “write denied.”

O.Protect_DRU

TOE has to inhibit the change of the attribute from “write denied” to “write allowed” during the validity period which is set to the access attribute.

O.Retention_Period

TOE has to inhibit the validity period set to the attribute “write denied” from being shortened.

4.2. Security Objectives for the Environment

The security objectives for the environment is described below.

OE.PhysicalProtection-Storage

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

OE.Protection-Network

In the customer's network environment including the storage device (external LAN), the storage device must be administrated so that it cannot be connected from any other product than the administration PC that is used by the storage administrator for administration and operation of the storage device.

OE.Protection-PC

The administration PC is must be managed so that the PC can only be used by the storage administrator.

OE.Responsibility-Admin

The storage administrator must be the person who is trusted to have the sufficient ability to administrate and operate the storage device, to execute the operations exactly as specified by the manual, and never to commit any inappropriate behavior.

OE.Responsibility-Maintenance

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

OE.Connect-Storage

The storage devices connected to TOE must be those for Enterprise produced by Hitachi Ltd.

The models that can be connected will be listed in the guidance.

5. IT Security Requirements

This section defines the IT security requirements which TOE or its environment must satisfy.
Note that the parts that has been allocated, chosen or detailed are bracketed with [ ].

5.1. TOE Security Requirements.

5.1.1. TOE Security Functional Requirements

All the following components are included in CC Part 2.

FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [assignment: DRU access control SFP] on [assignment:

- Subject; the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device's requirement
- Object; LDEV

Operation; write to the LDEV from the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device's requirement].

Dependency: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: DRU access control SFP] to objects based on the following: [assignment:

- Subject; the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device's requirement

- Object; LDEV
- Security attribute; Access attribute

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

Based on the access attribute defined in the control information on SM, access to the LDEV from the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device's requirement is controlled. More concretely, the rules are listed as below.

Process of carrying out the host requirement:

Access attribute	Rules on the operation for the object
Write allowed	Write I/O from the host is allowed.
Write denied	Write I/O from the host is denied

Process of carrying out the SVP requirement:

The following operations of creating and updating an LDEV from SVP are allowed regardless of access attribute.

- Creating an LDEV (Creating an object itself.)
- Deleting the LDEV (Deleting an object itself.)
- Formatting the LDEV (Writing format data to the LDEV. The object itself is not deleted.)
- Shredding the LDEV (Writing dummy data to the LDEV several times, and completely deleting the data. The object itself is not deleted.)

In addition, on the command from the SVP to execute the copy function, the following rules are executed by the access attribute of the LDEV.

Access attribute	Rules on the operation for the object
Write denied	Write from the copy operation is denied.

Process of carrying out another storage device's requirement:

Executes write from another storage device to the LDEV regardless of access attribute of the LDEV.

].

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

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

Dependency: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.2 The TSF shall allow the [assignment: none] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: host, Storage Navigator/SVP and other storage devices].

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

Dependency: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Lower Hierarchy: FIA_UID.1

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

Dependency: None

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: DRU access control SFP] to restrict the ability to [selection: modify] the security attributes [assignment: access attribute] to [assignment: Storage Navigator/SVP].

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

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values [refinement:

- Changing the access attribute from “write denied” to “write allowed” is only accepted when the validity period of the access attribute has expired.
- Changing the access attribute from “write allowed” to “write denied” is accepted regardless of the validity period.
- For changing the validity period of the access attribute, only the period longer than the current one is accepted.

the values that satisfy the rules above] are accepted for security attributes.

Dependency: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

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

Dependency: None

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: access attribute administration function and validity period administration function].

Dependency: None

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

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

Dependency: None

FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: access attribute] to [assignment: Storage Navigator/SVP].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: change to the status where it can change the access attribute “write denied” to “write allowed”] after the expiration time for the indicated security attribute has passed.

Dependency: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependency: None

5.1.2. Minimum Level of Function Strength

The minimum level of function strength of this TOE is SOF-based. Note that there are no functional requirements in this TOE to use the probabilistic or permutational mechanism.

5.1.3. TOE Security Assurance Requirements

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

Table 5.1 TOE Security Assurance Requirements

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

5.2. Security Requirements for the IT Environment

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

6. TOE Summary Specification

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

6.1. TOE Security Functions

6.1.1 SF.DRU

[Satisfied requirements] FDP_ACC.1, FDP_ACF.1, FMT_MSA.3 , FMT_SMR.1 , FIA_UID.2 , FMT_MSA.1, FMT_MSA.2, FPT_RVM.1, FMT_SMF.1, FPT_STM.1, FMT_SAE.1, FPT_SEP.1

Based on the access attribute of the LDEV, TOE executes “DRU access control SFP” to the access to the LDEV from the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device’s requirement.

A validity period is specified to the access attribute “write denied.” The access attribute and the validity period are managed and stored as a part of the control information on SM.

[DRU Access Control SFP] consists of the following rules:

- When the host makes access to an LDEV, TOE checks the access attribute of the LDEV, and controls the access so that only the allowed access (write allowed and write denied) may be executed.
- If the access attribute of the S-VOL is “write denied” to SVP’s command to execute the copy function, write to the target LDEV is denied.
- Creating and updating an LDEV (i.e. deleting, formatting and shredding) is allowed regardless of access attribute of the LDEV. (Except when the access attribute is write denied based on the function of Storage Navigator / SVP which is outside the range of TOE, in which case such updating is not executed.)
- Any write to the LDEV from another storage device in executing the copy function is allowed regardless of the access attribute of the S-VOL. (Except when the access attribute is write denied based on the function of another storage device which is outside the range of TOE, in which case such write process is not executed.)

- When an LDEV is created, “DRU Access Control SFP” gives a permissive default value as an access attribute. This means that, since the attribute “write allowed” has been given as the default value of the access attribute when an LDEV is created, access from the host to the LDEV is not limited. Note that there is no function to change the initial value that could be an alternative to that default value.
- Within the validity period that is set by the attribute “write denied,” changing such attribute to “write allowed” is inhibited.
- Updating the access attribute is only possible from Storage Navigator/SVP.

Availability of changing the access attribute is listed below.

Table 6.1 Availability of Changing the Access Attribute

After the change / Before the change	Within the validity period		Past the validity period	
	Write allowed	Write denied	Write allowed	Write denied
Write allowed	-(∗1)	-(∗1)	-	Yes
Write denied	No	-	Yes	-

(∗1) The attribute “write allowed” has not validity period set. No: Unchangeable; Yes: Changeable.

TOE maintains the roles of the host, Storage Navigator/SVP and other storage devices, and executes the identification of them before executing the other security functions.

TOE must assure that, when a TOE function is executed, “DRU Access Control SFP” is applied. Also, SF.DRU-related TSF must assure that it protects itself, and that no interference or alteration by an untrusted subject will happen.

In addition, TOE has the following functions related to the validity period.

- After the validity period has expired, it becomes possible to change the attribute from “write denied” to “write allowed.” Note that the access attribute is not automatically changed even after the validity period has expired. To change the attribute to “write allowed,” the operation is executed by the storage administrator (or by maintenance staff).
- For changing the validity period that has already been set, the period can be extended but cannot be shortened.

Note that, as for the validity period that is administrated and stored on the control information on SM, TOE calculates the elapsed time based on the counter value administrated in the hardware on CHA/DKA, and updates information on the validity period.

6.2. Level of Security Function Strength

No level of security function strength is claimed here as this TOE has no IT security function realized by any permutational or probabilistic mechanism.

6.3. Assurance Measures

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

Table 6.2 Security Assurance and Assurance Measures

Security Assurance Requirements		Assurance Measures
ACM_CAP.2	Components	• SANRISE USP Microprogram Configuration Administration List • Method of Adding the DKCMAIN/SVP Version
ADO_DEL.1	Distribution procedure	• SANRISE USP Distribution Method
ADO_IGS.1	Installation, creation and startup procedure	[SANRISE Universal Storage Platform / SANRISE H12000] • A/H-65A3, A/H-65A7, A-65B3, A-65B7, HT-40B3, HT-40B7 Disk Subsystem Maintenance Manual [SANRISE Network Storage Controller / SANRISE H10000] • A/H-65A4, A-65B4, HT-40B4 Disk Subsystem Maintenance Manual [TagmaStore Universal Storage Platform] • DKC510I, DKU505I Maintenance Manual [TagmaStore Network Storage Controller] • DKC515I Maintenance Manual

Security Assurance Requirements		Assurance Measures
ADV_FSP.1	Informal function specification	• SANRISE USP Data Retention Utility Function Specification
ADV_HLD.1	Descriptive design of the upper level	• SANRISE USP Data Retention Utility Function Specification
ADV_RCR.1	Demonstration of the informal response	• SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 User Data Protection Function Representation Correspondence Analysis
AGD_ADM.1	Administrator guidance	• SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 ISO15408 Function of Acquiring Authentication; Instruction Manual • TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller ISO15408 Certification Instructions Manual
AGD_USR.1	User guidance	None
ATE_COV.1	Proof of the coverage	• SANRISE USP Test Analysis
ATE_FUN.1	Function test	• SANRISE USP Test Analysis
ATE_IND.2	Independency test - sample	• SANRISE USP Test Analysis • TOE
AVA_SOF.1	Evaluation of the TOE security function strength	• SANRISE USP Function Strength Analysis
AVA_VLA.1	Developers' analysis of vulnerability	• SANRISE USP Analysis of Vulnerability

7. PP Claims

This ST does not claim for any PP.

8. Rationale

This section provides the rationale used for mainly evaluating ST.

8.1. Security Objectives Rationale

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

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

Table 8.1 Correspondence of TOE Security Environment to the Security Policy

		Security Policy								
		O.Protect_LDEV	O.Protect_DRU	O.Retention_Period	OE.PhysicalProtection-Storage	OE.Protection-Network	OE.Protection-PC	OE.Responsibility-Admin	OE.Responsibility-Maintenance	OE.Connect-Storage
TOE security environment	A.PhysicalProtection-Storage				X					
	A.Protection-Network					X				
	A.Protection-PC						X			
	A.Responsibility-Admin							X		
	A.Responsibility-Maintenance								X	
	A.Connect-Storage									X
	T.Delete/Change_User_Data	X								
	P.Protect_DRU		X							
	P.Retention_Period			X						

Table 8.2 shows that the security policy helps cope with the threats.

Table 8.2 Validity of the Security Policy to Cope with Threats

Threats	Rationale That Threats Are Being Coped with
T.Delete/Change_User_Data	T.Delete/Change_User_Data is removed by O.Protect_LDEV as follows: ・ To an LDEV, the storage administrator (or a maintenance staff) sets the attribute either “write allowed” or “write denied,” and by TOE controlling access based on that setting, inappropriate write to any data in the LDEV can be inhibited. To the user data which must not be changed, for example, setting the LDEV where that user data exists to “write denied” makes write to the LDEV prohibited, and keeps the user data protected.

Table 8.3 shows that the Assumptions are satisfied by the security policy.

Table 8.3 Validity of the Security Policy for the Assumptions

Assumptions	Rationale That the Assumptions Are Satisfied
A.PhysicalProtection-Storage	A. PhysicalProtection-Storage is realized by physically protecting the storage device, as described in OE.PhysicalProtection-Storage
A.Protection-Network	A. Protection-Network is realized by preventing any illegal PC, host or other equipments from being connected to the network which includes the storage device, as described in OE.Protection-Network.
A.Protection-PC	A. Protection-PC is realized by preventing any person other than the storage administrator from operating the administration PC, as described in OE.Protection-PC.
A.Responsibility-Admin	A. Responsibility-Admin is realized by assigning a reliable person to be the storage administrator, as described in OE.Responsibility-Admin.
A.Responsibility-Maintenance	A. Responsibility- Maintenance is realized by assigning a reliable person to be a maintenance staff, as described in OE.Responsibility- Maintenance.
A.Connect-Storage	A. Connect-Storage is realized by connecting the storage device produced by Hitachi Ltd., that executes the copy operation based on the access attribute of the LDEV in TOE, and as described in OE.Connect-Storage.

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

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

Security Policy of the Organization	Rationale that the security policy of the organization is satisfied
P.Protect_DRU	P.Protect_DRU is realized by, as long as TOE is within the validity period set by the access attribute, providing the function of inhibiting the change of the attribute from “write denied” to “write allowed,” as described in O.Protect_DRU.
P.Retention_Period	P.Retention_Period is realized by providing the function of inhibiting the shortening of the validity period which is set by the access attribute, as described in O.Retention_Period.

8.2. Security Requirements Rationale

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

8.2.1. Rationale for the Security Function Requirements

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

Table 8.5 Correspondence of TOE Security Policy to the Security Function Requirements

		TOE Security Function Requirements											
		FDP_ACC.1	FDP_ACF.1	FMT_MSA.3	FMT_SMR.1	FIA_UID.2	FMT_MSA.1	FMT_MSA.2	FPT_RVM.1	FMT_SMF.1	FPT_STM.1	FMT_SAE.1	FPT_SEP.1
SecurityPolicy	O.Protect_LDEV	X	X	X		X			X				X
	O.Protect_DRU				X	X	X	X		X	X	X	
	O.Retention_Period				X	X		X		X	X	X	

Table 8.6 shows that TOE security policy is realized by TOE security function requirements.

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

TOE Security Policy	Rationale for the Realization of TOE Security Policy
O.Protect_LDEV	O.Protect_LDEV requires that, for protecting the LDEV that this TOE considers the property to be protected, TOE have the control over whether to write to the LDEV, based on the access attribute set to the LDEV. The details of the procedures and the functions required for this requirement are as follows: a. Identify the user before using TOE. Before TOE is used, TOE must identify whether it is the requirement from the host, from the SVP or from another storage device. Therefore, it is necessary to identify the user before operating other security functions, and the security function requirement that corresponds to this requirement is FIA_UID.2. b. Specify and execute access control. For each user, TOE, based on the access attribute of the LDEV, must decide whether to allow the write to the LDEV according to the rules defined as “DRU access control SFP,” and execute the access control accordingly. Thus it can control whether to allow write from the host or from another storage to the LDEV. The security function requirement that corresponds to this requirement is FDP_ACC.1 and FDP_ACF.1. c. Specify the initial value of the access attribute so that the intended access control will be executed. For the access attribute which is the security attribute used in access control, write from the host or from another storage to the LDEV is allowed by default. It is specified by “DRU access control SFP” that there be no function to change the initial value that could be an alternative to that default value, which has to be realized. The security function requirement that corresponds to this requirement is FMT_MSA.3.

TOE Security Policy	Rationale for the Realization of TOE Security Policy
	d. Be sure to execute access control. To ensure the execution of access control, TSF related to access control has to be called before the subject operates an object. The process has to be protected from any interference or alteration, and TSF has to protect itself from being interfered or altered by any untrusted subject. The security function requirements that correspond to this requirement are FPT_RVM.1 and FPT_SEP.1. O.Protect_LDEV can be satisfied by achieving all of the a, b, c, and d procedures above. Therefore, O.Protect_LDEV can be satisfied by achieving FIA_UID.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FPT_RVM.1, and FPT_SEP.1 that correspond to those procedures.
O.Protect_DRU	O.Protect_DRU requires that, for preventing the access attribute being illegally changed and the user data from being altered, TOE set the validity period of the access attribute “write denied,” and that, within the validity period, changing the attribute from “write denied” to “write allowed” be inhibited. The details of the procedures and the functions required for this requirement are as follows: a. Identify the user before using TOE. Before TOE is used, TOE must identify whether it is the requirement from the host, from the SVP or from another storage device. Therefore, it is necessary to identify the user before operating other security functions, and the security function requirement that corresponds to this requirement is FIA_UID.2. b. Within the validity period, inhibit changing the attribute from “write denied” to “write allowed.” For each user, TOE, within the validity period that has been set by the attribute “write denied,” has to inhibit changing the attribute from “write denied” to “write allowed.” Therefore, TOE has to control whether to change the access attribute according to the rules defined as “DRU access control SFP.” The security function requirements that correspond to this requirement are FMT_SMF.1, FMT_MSA.1 and FMT_MSA.2.

TOE Security Policy	Rationale for the Realization of TOE Security Policy
	In addition, if the validity period has expired, TOE has to allow the access attribute to be changed from “write denied” to “write allowed.” The security function requirement that corresponds to this requirement is FMT_SAE.1. In addition, so as to identify the role of managing the access attribute, TOE has to maintain the roles of the host, Storage Navigator /SVP and another device, and get them associated with the user, and the security function requirement that corresponds to this requirement is FMT_SMR.1. In addition, for TOE to control the validity period, the time stamp has to be provided. The security function requirement that corresponds to this requirement is FPT_STM.1. O.Protect_DRU can be satisfied by achieving both of the a and b procedures above. Therefore, O.Protect_DRU can be satisfied by achieving FIA_UID.2, FMT_SMF.1, FMT_MSA.1, FMT_MSA.2, FMT_SAE.1, FMT_SMR.1, FPT_STM.1 that correspond to those procedures.

TOE Security Policy	Rationale for the Realization of TOE Security Policy
O.Retention_Period	O.Retention_Period requires, for preventing the access attribute within the validity period from being illegally changed, that TOE inhibit the shortening of the validity period which is set to the access attribute “write denied.” The details of the procedures and the functions required for this requirement are as follows: a. Identify the user before using TOE. Before TOE is used, TOE must identify whether it is the requirement from the host, from the SVP or from another storage device. Therefore, it is necessary to identify the user before operating other security functions, and the security function requirement that corresponds to this requirement is FIA_UID.2. b. Manage the validity period. TOE has to have the function of managing the validity period (i.e. the function of reflecting the validity period of the access attribute set by Storage Navigator/SVP on control information on SM). The security function requirement that corresponds to this requirement is FMT_SMF.1. In addition, so as to identify the role of managing the validity period, TOE has to maintain the roles of the host, Storage Navigator /SVP and another device, and get them associated with the user, and the security function requirement that corresponds to this requirement is FMT_SMR.1.
	c. In managing the validity period, inhibit the shortening of the validity period. TOE, in managing the validity period, has to inhibit the shortening of the validity period which is set to the access attribute “write denied,” and only allow the extension of the period. The security function requirements that correspond to this requirement are FMT_SAE.1 and FMT_MSA.2. In addition, for TOE to control the validity period, the time stamp has to be provided. The security function requirement that corresponds to this requirement is FPT_STM.1. O.Retention_Period can be satisfied by achieving all of the a, b, and c

TOE Security Policy	Rationale for the Realization of TOE Security Policy
	procedures above. Therefore, O.Retention_Period can be satisfied by achieving FMT_SMF.1, FMT_SMR.1, FMT_SAE.1, FMT_MSA.2 and FPT_STM.1 that correspond to those procedures.

8.2.2. Rationale for the Internal Consistency of the Security Requirements

The table below describes the dependency of the security function requirements.

Table 8.7 Dependency of Security Function Requirements

Item number	TOE/IT Environment	Security Function Requirements	Dependency Defined by CC part 2	Item Number of the Equivalent Function Requirement(s) in this ST
1	TOE	FDP_ACC.1	FDP_ACF.1	2
2	TOE	FDP_ACF.1	FDP_ACC.1	1
			FMT_MSA.3	3
3	TOE	FMT_MSA.3	FMT_MSA.1	6
			FMT_SMR.1	4
4	TOE	FMT_SMR.1	FIA_UID.1	5 *1
5	TOE	FIA_UID.2	None	-
6	TOE	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	1
			FMT_SMF.1	9
			FMT_SMR.1	4
7	TOE	FMT_MSA.2	ADV_SPM.1	Dependency not satisfied
			FDP_ACC.1 or FDP_IFC.1	1
			FMT_MSA.1	6
			FMT_SMR.1	4
8	TOE	FPT_RVM.1	None	-
9	TOE	FMT_SMF.1	None	-
10	TOE	FPT_STM.1	None	-
11	TOE	FMT_SAE.1	FMT_SMR.1	4
			FPT_STM.1	10
12	TOE	FPT_SEP.1	None	-

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

In this ST, the dependency between IT security function requirements and assurance requirements are achieved except for ADV_SPM.1 on which FMT_MSA.2 depends. However, as refinement has been made to FMT_MSA.2, and the rules to follow are explicitly described, its dependency on ADV_SPM.1 can be removed.

There are no competitions between IT security requirements, either. For each security function requirement, rationale is shown in Table 8.8 for consistency which the definition has through the function requirement of the same category.

Table 8.8 Consistency among Security Function Requirements

Item number	Category	Security Function Requirement	Rationale for Consistency
1	Access control	FDP_ACC.1 FDP_ACF.1	Definitions related to access control are made based on these function requirements. It is required that the same SFP be applied to the same subject or object and there are no competitions or inconsistency. The whole contents are consistent.
2	Administration	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SAE.1 FMT_SMF.1 FMT_SMR.1	Definitions related to security management are made based on these function requirements. There are no competitions or inconsistency in any targeted security attributes or actions. The whole contents are consistent.
3	Identification and authentication	FIA_UID.2	This function requirement realizes the identification, and as there is only one function requirement in this category, it is obvious that the contents are consistent.
4	Complementation	FPT_RVM.1 FPT_SEP.1 FPT_STM.1	These function requirements are for complementing the other function requirements. Since FPT_RVM.1 is the one for preventing bypass and FPT_SEP.1 is the one for separating the security domain, it is obvious that there is no competition or inconsistency among the function requirements in this category, and that the whole contents are consistent.

Item number	Category	Security Function Requirement	Rationale for Consistency
5	Among categories	#1-#2	The requirements concerning access control define the control over the LDEV that is the property to be protected, and the requirements concerning management define TSF data management. Therefore, there is no competition or inconsistency with each other.
		#1-#3 #2-#3	The requirement concerning identification and the one concerning access control or management have no competition or inconsistency with each other.
		#1-#4 #2-#4 #3-#4	As described above, it is obvious that FPT_RVM.1 and FPT_SEP.1 cause no competition or inconsistency with the other requirements. In addition, FPT_STM.1 is for providing time information for SMT_SAE.1, where there is no competition or inconsistency with the other requirements.

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

- FPT_RVM.1 assures that another security function is called and succeed, which prevents bypass.
- In this TOE, the security function is always on, and the security function cannot be stopped independently while TOE is operating. Therefore, it is not necessary to consider the prevention of deactivation.
- FPT_SEP.1 prevents any interference or alteration to the security domain.
- As this TOE does not include any security function that is realized by the probabilistic or permutational mechanism, nullification attacks do not have to be considered. Therefore, no

function requirements of the FAU class are required.

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

8.2.3. Rationale for the Minimum Level of Function Strength

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

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

8.2.4. Rationale for the Evaluation Assurance Level

The storage device including this TOE is installed in a secure area where entrance and exit is controlled, and the attack route can be limited to the one via the host. Which means the evaluation of obvious vulnerability is all that is needed.
Furthermore, as TOE is software, and at the same time, it does not include any confidential information such as a cryptography key, it does not have to be protected by the security at the time of development.
Therefore, the evaluation assurance level 2 should be valid.

8.3. TOE Summary Specification Rationale

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

8.3.1. Rationale for TOE Security Functions

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

Table 8.9 Correspondence of TOE Security Function Requirements to TOE IT Security Functions

		IT Security Functions of TOE
		SF.DRU
TOE Security Function Requirements	FDP_ACC.1	No
	FDP_ACF.1	No
	FMT_MSA.3	No
	FMT_SMR.1	No
	FIA_UID.2	No
	FMT_MSA.1	No
	FMT_MSA.2	No
	FPT_RVM.1	No
	FMT_SMF.1	No
	FPT_STM.1	No
	FMT_SAE.1	No
	FPT_SEP.1	No

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

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

TOE Security Function Requirements	IT Security Functions
FDP_ACC.1	FDP_ACC.1 describes SF.DRU as follows, which has been realized accordingly. "Based on the access attribute of the LDEV, TOE executes "DRU access control SFP" to the access to the LDEV from the process of carrying out the host requirement, the process of carrying out the SVP requirement, and the process of carrying out another storage device's requirement."
FDP_ACF.1	FDP_ACF.1 describes SF.DRU as follows, which has been realized accordingly. • When the host makes access to an LDEV, TOE checks the access attribute of the LDEV, and controls the access so that only the allowed access (write allowed and write denied) may be executed. • If the access attribute of the S-VOL is "write denied" to SVP's command to execute the copy function, write to the target LDEV is denied. • Creating and updating an LDEV (i.e. deleting, formatting and shredding) is allowed regardless of access attribute of the LDEV. (Except when the access attribute is write denied based on the function of Storage Navigator / SVP which is outside the range of TOE, in which case such updating is not executed.) • Any write to the LDEV from another storage device in executing the copy function is allowed regardless of the access attribute of the S-VOL. (Except when the access attribute is write denied based on the function of another storage device which is outside the range of TOE, in which case such write process is not executed.)

TOE Security Function Requirements	IT Security Functions
FMT_MSA.3	FMT_MSA.3 describes SF.DRU as follows, which has been realized accordingly. "When an LDEV is created, "DRU Access Control SFP" gives a permissive default value as an access attribute.... Note that there is no function to change the initial value that could be an alternative to that default value."
FMT_SMR.1	FMT_SMR.1 describes SF.DRU as follows, which has been realized accordingly. "TOE maintains the roles of the host, Storage Navigator/SVP and other storage devices, and executes the identification of them before executing the other security functions"
FIA_UID.2	FIA_UID.2 describes SF.DRU as follows, which has been realized accordingly. "TOE maintains the roles of the host, Storage Navigator/SVP and other storage devices, and executes the identification of them before executing the other security functions."
FMT_MSA.1	FMT_MSA.1 describes SF.DRU as follows, which has been realized accordingly. "[DRU Access Control SFP] consists of the following rules: • Updating the access attribute is only possible from Storage Navigator/SVP."
FMT_MSA.2	FMT_MSA.2 describes SF.DRU as follows, which has been realized accordingly. "[DRU Access Control SFP] consists of the following rules: • Within the validity period that is set by the attribute "write denied," changing such attribute to "write allowed" is inhibited." "In addition, TOE has the following functions related to the validity period. • After the validity period has expired, it becomes possible to change the attribute from "write denied" to "write allowed." Note that the access attribute is not automatically changed even after

TOE Security Function Requirements	IT Security Functions
	the validity period has expired. • For changing the validity period that has already been set, the period can be extended but cannot be shortened.
FPT_RVM.1	FPT_RVM.1 describes SF.DRU as follows: "TOE maintains the roles of the host, Storage Navigator/SVP and other storage devices, and executes the identification of them before executing the other security functions," which assures that the identification function is called before each function is allowed, and assures that it will succeed. Furthermore, it says: "TOE must assure that, when a TOE function is executed, "DRU Access Control SFP" is applied," which assures that the TSP execution function is called and succeed. By these contents, FPT_RVM.1 has been realized.
FMT_SMF.1	FMT_SMF.1 describes SF.DRU as follows, which has been realized accordingly. "A validity period is specified to the access attribute "write denied." The access attribute and the validity period are managed and stored as a port of the control information on SM."
FPT_STM.1	FPT_STM.1 describes SF.DRU as follows, which has been realized accordingly. "Note that, as for the validity period that is administrated and stored on the control information on SM, TOE calculates the elapsed time based on the counter value administrated in the hardware on CHA/DKA, and updates information on the validity period."
FMT_SAE.1	FMT_SAE.1 describes SF.DRU as follows, which has been realized accordingly. "In addition, TOE has the following functions related to the validity period. • After the validity period has expired, it becomes possible to change the attribute from "write denied" to "write allowed." Note that the access attribute is not automatically changed even after

TOE Security Function Requirements	IT Security Functions
	the validity period has expired. • For changing the validity period that has already been set, the period can be extended but cannot be shortened.
FPT_SEP.1	FPT_SEP.1 describes SF.DRU as follows. "Also, SF.DRU-related TSF must assure that it protects itself, and that no interference or alteration by an untrusted subject will not happen." These contents, in SF.DRU, protect TSF used for the function and its information from being interfered or altered, and by maintaining them, protect them from being interfered or altered by any other subjects. In addition, SF.DRU stores the subject it needs in the security domain, separating it from the other subjects. Therefore, FPT_SEP.1 has been realized by installing SF.DRU.

8.3.2. Rationale for the Level of TOE Function Strength

Since this ST does not include any IT security functions based on the probabilistic or permutational mechanism, this kind of rationale is not discussed here.

8.3.3. Rationale for Assurance Measures

The assurance measures described in Table 6.2 are the names of the documents that imply they satisfy the equivalent security assurance requirements, and the security assurance requirements and the assurance measures correspond to each other. The additional remarks are described below, regarding the assurance measures.

- ADO_IGS.1 describes four manuals, each of which corresponds to a different kind of equipment.
- ADV_HLD.1 describes the contents of the upper level design in “SANRISE USP Data Retention Utility Function Specification”
- AGD_ADM.1 describes two manuals, whose only difference is that one is in Japanese and the other in English, and their contents are the same.
- AGD_USR.1 does not have any corresponding assurance measures that corresponds to it. This is because, as the storage device user uses the user volume in the storage device from the host, based on the environment built by the storage device administrator, they can use user volumes if only they have common knowledge on the host, and they do not need any special knowledge on the storage device.

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

8.4. PP Claims Rationale

This ST does not claim for any PP.

9. Reference

[1] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model
Version 2.1, August 1999, CCIMB-99-031

[2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements
Version 2.1, August 1999, CCIMB-99-032

[3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements
Version 2.1, August 1999, CCIMB-99-033