Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-12-27 (ITC-0331)
Certification No.	C0305
Sponsor	Hewlett-Packard Company
Name of TOE	HP StorageWorks P9000 Command View Advanced Edition Software Common Component
Version of TOE	7.0.1-00
PP Conformance	None
Assurance Package	EAL2 Augmented with ALC_FLR.1
Developer	Hewlett-Packard Company
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2011-8-15

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

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

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

Evaluation Result: Pass

"HP StorageWorks P9000 Command View Advanced Edition Software Common Component" 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

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "HP StorageWorks P9000 Command View Advanced Edition Software Common Component, Version 7.0.1-00" (hereinafter referred to as "the TOE") developed by Hewlett-Packard Company, and evaluation of the TOE was finished on 2011-7-25 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Hewlett-Packard Company and provides information to the users and system operators who are interested in this TOE.

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

This certification report assumes "TOE users (Storage administrators, Account administrators and System integrators)" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions is as follows. Refer to Chapter 2 or subsequent ones for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL2 augmented with ALC_FLR.1.

1.1.2 TOE and Security Functionality

The target of evaluation, HP StorageWorks P9000 Command View Advanced Edition Software Common Component (abbreviated hereafter to *CVAECC*), runs as the base module that provides the common functions for storage management software (in HP StorageWorks P9000 Command View Advanced Edition Software Series) that centrally manages multiple storage devices connected in a SAN environment. The storage management software includes HP StorageWorks P9000 Device Manager Software (abbreviated hereafter to *DevMgr*), HP StorageWorks P9000 Replication Manager Software (abbreviated hereafter to *RepMgr*), and HP StorageWorks P9000 Tiered Storage Manager Software (abbreviated hereafter to *TSMgr*), HP StorageWorks P9000 Tuning Manager Software (abbreviated hereafter to *TunMgr*), etc. These products and CVAECC are generically referred to as HP StorageWorks P9000 Command View Advanced Edition Software.

CVAECC is bundled with each product package as the base module of HP StorageWorks P9000 Command View Advanced Edition Software.

The TOE provides common security functions for the storage management software, such as authentication, the display of permissions information, and a graphical user interface for displaying information on the client terminal when the storage administrator requests a required operation, such as copying, by accessing the necessary storage management software from a client terminal.

Regarding such security functionality, the validity of the design policy and the accuracy of implementation have been evaluated in the range of the assurance package. The threat and the assumption that this TOE assumes is as follows;

1.1.2.1 Threats and Security Objectives

This TOE assumes the following threats, and offers the security functions to oppose them.

The threats assumed are that if an illegal user or authenticated storage administrator or account administrator performs the originally unauthorized operation from the client terminal, the permissions information of account as assets might be deleted, modified, or revealed, or the text information used by the warning banner function might be deleted or modified.

In order to counter the threat, when the user accesses the storage management software from the client terminal, the TOE identifies and authenticates the users, manages session of user who has logged in by request from the storage management software, and confirms that the identification and authentication of user are maintained (Identification and authentication function). Moreover, the TOE manages each user's authentication method, account information, an ACL table, banner information, a security parameter, etc. (Security information management function) and replies an advisory warning message (Set-up banner information) regarding illegal use of the storage management software. (Warning banner function)

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

The place where the TOE is installed shall be a locked business server area/computer center, and the entry to and exit from the area is restricted. Those who are permitted to enter the area are only the trusted administrators of hardware and software who will not perform malicious acts. The TOE is assumed to be set up at business server area/center protected from an external network by the firewall as a management network, with the management server, storage, and peripherals, etc.

When the external authentication server and external authorization server are substituted for the TOE identification and authentication function, they are installed in the same business server area as the storage management software server. When the both servers are installed in a different business server area from that of the storage management server, confidentiality and integrity of the channel between those servers shall be guaranteed.

The TOE is the module which is bundled with the storage management software and

to be used in combination with any of the following products:

DevMgr v5.6.0 or later
TSMgr v5.5.0 or later
RepMgr v5.6.0 or later
TunMgr v7.0.0 or later

1.1.3 Disclaimers

- This TOE assumes the operational environment that the client terminal accesses via the interface of Web. The attacker whom this TOE assumes does not have advanced expertise. Furthermore, the attack is restricted only to the attackers who use the interface of Web from the client terminal which an administrator can operate.

- When the external authentication function or the linkage functionality for external authentication groups is used, the identification and the authentication function of the external authentication server and the external authorization server are not included in the TOE. Moreover, the impersonation of the external authentication server and external authorization server is assumed to be prevented by the operational environment.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-07 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of TOE	HP StorageWorks P9000 Command View Advanced Edition Software Common Component
Version of TOE	7.0.1-00
Developer	Hewlett-Packard Company

The user can verify that a product is the TOE, which is evaluated and certified, by the following means.

The version can be confirmed by the operation according to the version confirmation procedure described in guidance. Furthermore, it can also be confirmed from the security guidance at the time of purchase.

3. Security Policy

This chapter describes security function policies and organisational security policies.

This TOE offers the following common security functions to the storage management software group. The purpose is that the identified and authenticated appropriate storage administrator obtains the management environment based on the storage management authority by acquiring the appropriate permissions information according to the authentication.

(1) Identification and Authentication function

The identification and authentication function uses IDs and corresponding passwords to authenticate users when the user logs on to the storage management software, and generates and maintains sessions based on the result. Moreover, based on the authentication result, it also passes permissions information to the requesting user (Storage Management Software).

If successive authentication attempts by the user fail for a predefined number of times, the user's account for the TOE is locked.

Instead of the TOE's internal authentication function, the TOE can use the external authentication functionality of an external authentication server or an external authentication group linkage function. However, the TOE does not contain identification and authentication functionality provided by external authentication servers or external authorization server.

(2) Security Information Management function

A function to manage the TOE user's account information (user ID, password, and lock status) and to set security parameter ("Account self locking" and "Password complexity check"). When the TOE user, who is registered, identified and authenticated at the TOE, performs originally unauthorized operation from the client terminal, this function prevents the permissions information managed by the TOE from being deleted, modified and revealed, and it also prevents the banner information from being deleted and modified.

(3) Warning Banner function

A function to display the banner information for warning on a login screen regardless of the permissions and role of the TOE user at login to the storage management software. Banner information is entered by the system integrator or account administrator.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1 and to meet the organisational security policy shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions for countermeasure against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_ACCESS (illegal connection)	From a management client, an illegal user might delete, modify, or reveal the permissions information managed by the TOE for the storage management software functions, or might delete or modify the banner information.
T.UNAUTHORISED_ACCESS (unauthorized access)	From a management client, an authenticated storage administrator or account administrator might delete, modify, or reveal the permissions information managed by the TOE, or delete or modify banner information by performing an unauthorized operation.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1) Countermeasure against threat "T.ILLEGAL_ACCESS"

If the user of storage management client terminal is specified to use the internal authentication, the TOE identifies and authenticates the user and confirms whether the user is permitted to access the TOE and storage management software. If the user is specified to use the external authentication, the external authentication server identifies and authenticates the user.

The TOE and the external authentication server limit the registration patterns of passwords so that difficult-to-guess passwords are set. Moreover, the users set passwords that are difficult to guess on the basis of password length and character types used and change them at an appropriate interval, so that passwords are not revealed; thus, a safe password management can be realized. In addition, the TOE automatically locks the account of a user for which authentication fails more than the defined number of times, to defend against brute-force password attacks.

(2) Countermeasure against threat "T.UNAUTHORISED_ACCESS"

The TOE controls the access to permissions information and banner information by storage management client terminal users in accordance with the permissions information provided for the storage management software and the TOE users.

3.1.2 Organisational Security Policy and Security Function Policy

3.1.2.1 Organisational Security Policy

Organisational Security Policy required in use of the TOE is shown in Table 3-2.

Table 3-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.BANNER (warning banner)	Storage management software must have functions that display advisory warning messages related to its illegal use of the software.

3.1.2.2 Security Function Policy to Organisational Security Policy

The TOE provides the security function to fill the Organisational Security Policy shown in Table 3-2.

(1) Countermeasure against Organizational Security Policy **"P.BANNER"**

The TOE provides the storage management software with advisory warning messages regarding illegal use of the storage management software. The storage management software has functionality for displaying advisory messages (provided by the TOE) about the illegal use of the storage management software.

4. Assumptions and Clarification of Scope

In this chapter, it describes the assumptions and the operational environment to operate the TOE as useful information for the judgment before the assumed reader uses the TOE.

4.1 Usage Assumptions

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

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.PHYSICAL (management of hardware)	The management server on which the TOE and storage management software run, peripheral devices, the external authentication server and external authorization server that the TOE uses, storage devices, the internal network, and the firewall at the boundary of the internal network must be installed in a physically isolated business server area. Only the administrators of the hardware and software installed in that area are permitted to enter this area. The administrators must be trusted persons who will not perform malicious acts in the area.
A.ADMINISTRATORS (Administrators)	The system integrators must be trusted persons. Account administrators, storage administrators, and administrators of other servers, including application servers, do not perform malicious acts with regard to one another's work; it includes the management of accounts and permissions information of storage management software users, the management of storages, and the management of other servers.
A.PASSWORD (complex passwords)	Any passwords that are set must be difficult to guess on the basis of password length and character types used in order to prevent unauthorized users from logging in to the system through guesswork. In addition, a function that limits the number of repeated authentication attempts must be used to prevent unlimited authentication attempts.
A.SECURE_CHANNEL (communication security)	The network between the management server and management clients, on which the TOE and storage management software run, or between the TOE and the external authentication server and the external authorization server that the TOE uses is secure with regard to confidentiality and integrity of communication.
A.NETWORKS (networks)	The internal network in the business server area housing the management network connected to the management server must be restricted to communication from storage management client

	terminals by means of a firewall.
A.SRV_MGMT (server management)	The settings of services that run on the server, server settings, and accounts registered on the server must be managed to prevent management clients from directly accessing the internal network without using the TOE. **(Supplementation)** Since the remote access by SSH and telnet is considered as an access to internal network, it is assumed to be prohibited.
A.CLIENTS (management of storage management clients)	Harmful software does not exist in the storage management client.
A.VERSION (product versions that can be used with the TOE)	The TOE is to be used in combination with any of the following products: DevMgr version 5.6.0 or later TSMgr version 5.5.0 or later RepMgr version 5.6.0 or later TunMgr version 7.0.0 or later

4.2 Environment Assumptions

The TOE (CVAECC) is the basic module that executes the common functionality for the storage management software in the HP StorageWorks P9000 Command View Advanced Edition Software series and is installed in a management server along with storage management software.

The management server shall be installed in a locked (in a physically isolated) business server area/computer center along with application servers, storage servers and peripheral devices and is protected from an outside network by the firewall.

The storage administrator and the account administrator as users access the storage management software in the business server area from the storage management client terminal outside the business server area via the firewall to perform a required operation such as copying for the storage management business.

A storage system is connected to an application server that runs business applications and maintains information necessary for the business application execution in the volume. Therefore it belongs to both the management (an internal) network and business (an external) network; however, an independent network card is installed for each network connection, so that two management networks are separated, and not interfered with mutually.

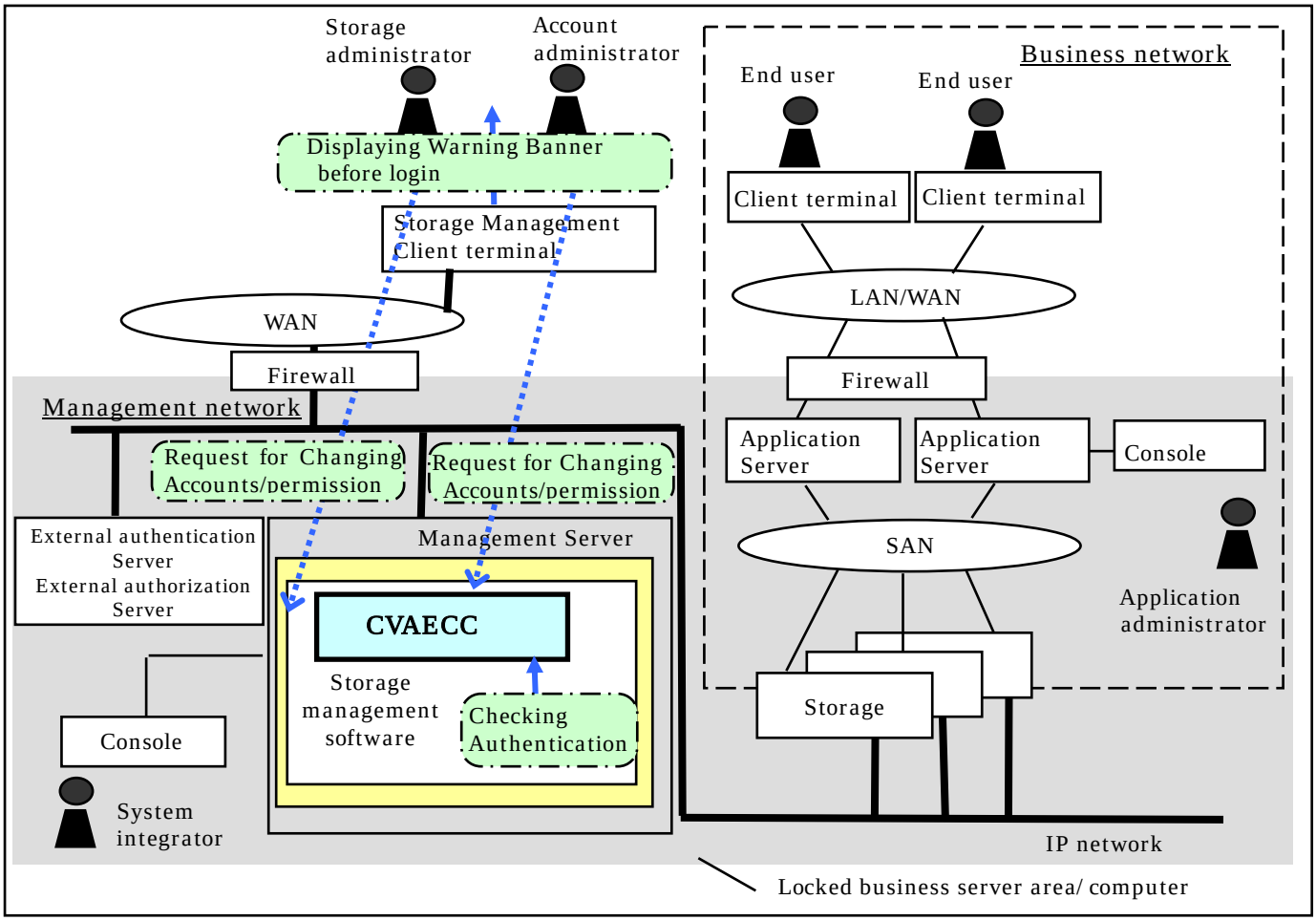

Figure 4-1 Operational Environment and Configuration

TOE Configuration

Storage Management Software (Product version that can be used by combining with TOE.)

- HP StorageWorks P9000 Device Manager Software (*DevMgr* version 5.6.0 or later)
- HP StorageWorks P9000 Replication Manager Software (*RepMgr* version v5.6.0 or later)
- HP StorageWorks P9000 Tiered Storage Manager Software (*TSMgr* version 5.5.0 or later)
- HP StorageWorks P9000 Tuning Manager Software (*TunMgr* version 7.0.0 or later)

The TOE operates on the platform which fills either of followings.

(1) Management server

- Platform running Java™ VM (Version 1.5.0_11 or later) that has been installed by HP StorageWorks P9000 Command View Advanced Edition Software Common Component for Windows
- Platform running Java™ VM (Version 1.5.0_05 or later) that has been installed by HP StorageWorks P9000 Command View Advanced Edition Software Common

Component for Linux

(2) Storage management client terminal
[When the client OS is Windows]
- Microsoft Internet Explorer 6.0, 7.0, or 8.0

[When the client OS is Linux]
- Firefox 3.6.0 or later

(3) External authentication server / external authorization server
Microsoft Active Directory (supplied with the Windows Server 2003 series or Windows Server 2008 series of operating systems)

4.3 Clarification of scope

The external authentication server and the external authorization server can be set up in the business server area, and "External authentication function" and "External authentication group linkage function" in place of the TOE identification and the authentication function can be used. However, the identification and the authentication function of the external authentication server and the external authorization server are not within the range of the TOE. Applying a system securely according to security objectives becomes an operator's responsibility.

The TOE is the server program that runs on the popular OS (depends on the OS functions (process management/process separation)). From the assumption, the access to TOE is limited to the access by the management client terminal. Moreover, malicious software to the management client terminal doesn't exist, and OS commands will not be abused.

5. Architectural Information

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

5.1 TOE boundary and component

Figure 5-1 shows the composition of the TOE. The TOE is a range composed of the library and the program enclosed in the dotted line. The operating system (applicable platform) is not included in the TOE.

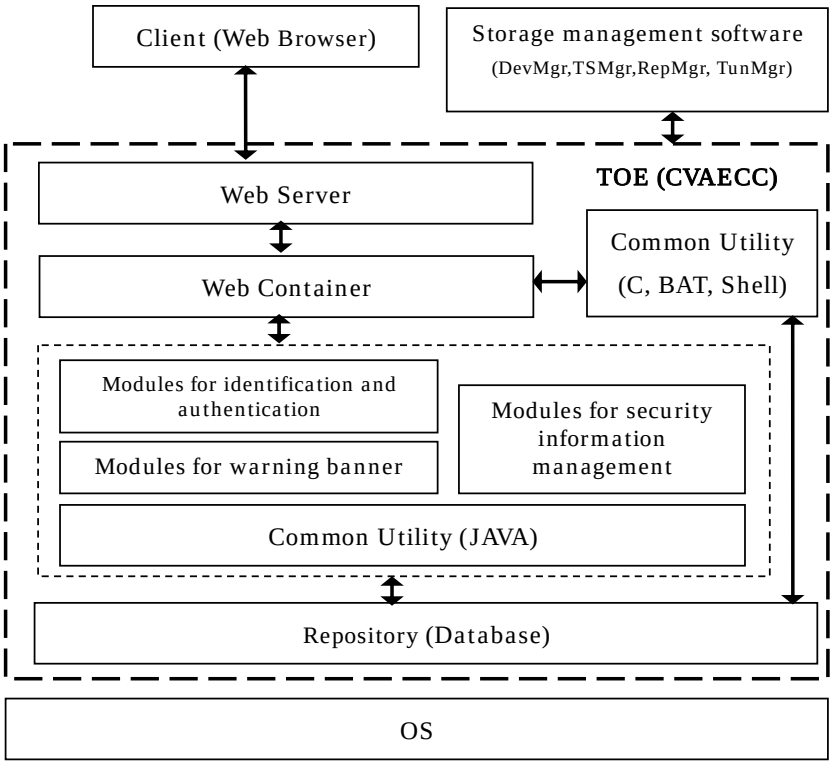

Figure 5.1 TOE boundary

- Identification and Authentication Module is a module that implements the identification and authentication function of the TOE.
- Security Information Management Module is a module that implements the security information management function of the TOE.
- Warning Banner Module is a module that implements the warning banner functionality of the TOE.
- Common Utility is a module that implements the common functions of the TOE.
- Web Service Module is a module that implements the TOE Web service.
- GUI Framework is a module that implements the TOE graphical user interface.
- Repository is the database that stores data for the TOE.

5.2 IT Environment

The TOE is the basic module that implements common functions for the storage management software to manage multiple storage devices connected in a SAN environment centrally. It is installed on the management server in which either Windows (Platform running Jav™ VM (Version 1.5.0_11 or later)) or Linux (Platform running Java™ VM (Version 1.5.0_05 or later)) is the OS as an operation platform, together with the storage management software.

The TOE user operates it from the client terminal as a browser by Microsoft Internet Explorer 6.0, 7.0, 8.0 (When Client OS is Windows) or Firefox 3.6.0 or later (When client OS is Linux).

In the authentication server, Microsoft Active Directory (supplied with the Windows Server 2003 series or Windows Server 2008 series of operating systems) is used.

In the external authentication, the authentication function of the LDAP directory server, the RADIUS server, or the Kerberos server is used.

6. Documentation

The identification of documents attached to the TOE is listed below.

TOE users are required fully understanding and complying with the following documents in order to satisfy the assumptions.

HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Guide	TB581-96059

And the following guidance which is a component of the above-mentioned security guide.

- HP StorageWorks P9000 Command View Advanced Edition Suite Software Administrator Guide	TB581-96037
- HP StorageWorks P9000 Command View Advanced Edition Suite Software User Guide	TB581-96041
- HP StorageWorks P9000 Command View Advanced Edition Suite Software Installation and Configuration Guide	TB581-96036
- HP StorageWorks P9000 Replication Manager Software Configuration Guide	TB584-96016
- HP StorageWorks P9000 Replication Manager Software User Guide	TB584-96017
- HP StorageWorks P9000 Tuning Manager Software Server Administration Guide	TB588-96020
- HP StorageWorks P9000 Tuning Manager Software User Guide	TB588-96022
- HP StorageWorks P9000 Tuning Manager Software Installation Guide	TB588-96019

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2011-01 and concluded by completion of the Evaluation Technical Report dated 2011-07. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-02 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview. Further, the evaluator executed the sampling check of the developer test and the evaluator test by using developer test environment at developer site on 2011-02.

7.3 IT Product Test

The evaluator confirmed the validity of the test that the developer had executed. Based on the evidence shown by the process of the evaluation and those confirmed validity, the evaluator executed the reappearance test, additional test and penetration test based on vulnerability assessments judged to be necessary.

7.3.1 Developer Test

The evaluator evaluated the integrity of the developer test that the developer executed and the test documentation of actual test results. It explains the content of the developer test evaluated by the evaluator as follows.

1) Developer Test Environment

Figure 7-1 shows the test configuration executed by the developer.

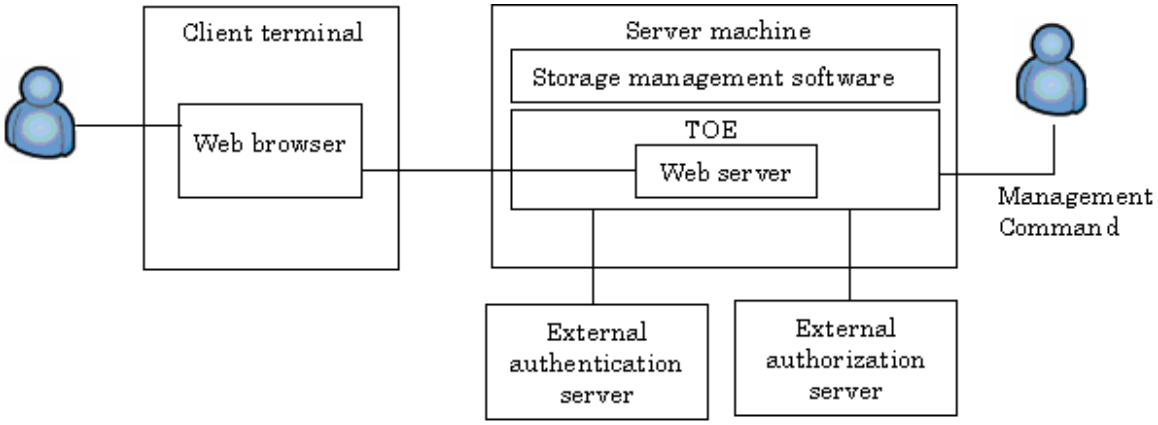

Figure 7-1 Configuration of the Developer Test

The developer test is executed in the same TOE test environment as the TOE configuration identified in this ST. The test using all the storage management products described in the ST as a version of the product that contains the TOE is executed.

2) Summary of Developer Test

Summary of the developer test is as follows.

a) Developer Test Outline
Outline of the developer test is as follows.

<Developer Test Approach>

Web interface, the Java interface, and the command interface are tested by accessing through a browser and each console and observing them. Regarding a part of Java interface, the storage management product that fills assumption of

the ST doesn't use those interfaces. Therefore, it executed by observing the operation by activating the method by the test module.

<Tools for the Developer Test>

Table 7-1 shows the tools used in the developer test.

Table 7-1 Tools for the Developer Test

	No	Name of Hardware and Software	Details
Configuration	1	PC server (Client terminal, Server Machine, External authentication Server)	- Model: dc7900SF/CT - CPU: Core2Quad - Memory: 4GB - HDD capacity: 1000GB
Software	1	TOE	- Version : 7.0.1-00
	2	Windows (OS of PC server)	- Windows : Windows 2008 R2 Server Enterprise Edition
	3	Linux (OS of PC server)	- RedHat Enterprise Linux Advanced Edition 5 update 4 - SuSE Linux Enterprise Server 11
	4	Active Directory	- Program of Windows Server 2008
	5	Internet Explorer	- Version : 7
	6	Firefox	- Version : 3.6.9
	7	HP StorageWorks P9000 Device Manager Software 7.0.1-00	- Version : 7.0.1-00
	8	HP StorageWorks P9000 Replication Manager Software 7.0.1-00	- Version : 7.0.1-00
	9	HP StorageWorks P9000 Tiered Storage Manager Software 7.0.1-00	- Version : 7.0.1-00
	10	HP StorageWorks P9000 Tuning Manager Software 7.0.0-01	- Version : 7.0.0-01
	11	Eclipse	- Version : 3.1.1

Eclipse is not included in the configuration described in the ST.
It is judged that it never influences other parts of the TOE because it accesses only the interface to be tested though it is software for the development used to test a specific Java interface of the TOE.

b) Scope of Execution of the Developer Test

422 tests of storage management products, OS, and each browser described in Table 7-1 were executed. The executed test targets all TSFI.

By the coverage analysis, it was confirmed that "the relation between the test item and the security function" provided by the developer matches the correspondence of security function and test ID.

It was verified that the correspondence of the test in the test evidence material and TSFI in the functional specification is accurate and there is no point that becomes a problem for the security function.

c) Result

The evaluator confirmed an approach of the executing developer test and legitimacy of tested items, and confirmed consistencies between test approach described in the test plan and actual test approach.

In the test result, the difference arising from storage management products was not found. The storage management product is used to call the interface of the TOE, and the evidence that storage management products affect the behavior of a security function was not found in the development documentation.

7.3.2 Evaluator Independent Test

The evaluator executed the sample test to reconfirm the execution of the security function by the test items extracted from the developer test. And the evaluator executed the evaluator independent test (hereinafter referred to as "The Independent Test") to reconfirm that security functions are certainly implemented from the evidence shown by the process of the evaluation. It explains the independent test executed by the evaluator as follows.

1) Independent Test Environment

Table 7-2 shows the independent testing configuration executed by the evaluator. The configuration of the independent test that the evaluator executed is the same configuration as a developer test.

Table 7-2 Tools for the Evaluator Test

Use	Hardware	Software
Server machine	Model Name: HP Compaq dc7900SF/CT CPU: Intel Core2 Quad Memory: 4GB HDD: 1000GB (Common for Windows/Linux)	- Windows Server 2008 R2 Enterprise Edition - HP StorageWorks P9000 Device Manager 7.0.1-00 - HP StorageWorks P9000 Replication Manager 7.0.1-00 (JavaVM Version 1.5.0_11 that has been installed by HP StorageWorks P9000 Command View Advanced Edition Software Common Component for Windows.)

		- RedHat Enterprise Linux Advanced Edition5 update4 - HP StorageWorks P9000 Device Manager 7.0.1-00 - HP StorageWorks P9000 Replication Manager 7.0.1-00 (JavaVM Version 1.5.0_05 that has been installed by HP StorageWorks P9000 Command View Advanced Edition Software Common Component for Linux.) - Firefox 3.6.9
		- SuSE Linux Enterprise Server 11 - HP StorageWorks P9000 Device Manager 7.0.1-00 - HP StorageWorks P9000 Replication Manager 7.0.1-00 (JavaVM Version 1.5.0_05 that has been installed by HP StorageWorks P9000 Command View Advanced Edition Software Common Component for Linux.) - Firefox 3.6.9
External authentication server, External authorization serer	Model Name: HP Compaq dc7900SF/CT CPU: Intel Core2 Quad Memory: 4GB HDD: 1000GB	- Windows Server 2008 Enterprise Edition - Active Directory (supplied with the above-mentioned OS)
Client terminal	Model Name: HP Compaq dc7900SF/CT CPU: Intel Core2 Quad Memory: 4GB HDD: 1000GB (Common for Windows/Linux)	- Windows Server 2008 Enterprise Edition - Internet Explorer 7
		- RedHat Enterprise Linux Advanced Edition5 update4 - Firefox 3.6.9
		- SuSE Linux Enterprise Server 11 - Firefox 3.6.9

The independent test is executed in the same environment as the TOE configuration identified in the ST.

2) Summary of Independent Test

Summary of the Independent test is as follows.

a) Viewpoint of Independent Test

The viewpoint of the independent test that the evaluator designed from the developer test and the provided evaluation evidence material is shown below.

From the following viewpoints the evaluator extracted testing items from the testing specifications by the developer.

1. Viewpoint of security function
   Performing a sampling test from each security function (SF.I&A, SF.MGMT, SF.BANNER) in order to test security functions uniformly.

2. Viewpoint of interface
   Confirming behavior in the Web interface, the Java interface, and the command interface, take a sampling from each interface type and cover all SFRs. It takes into consideration that the Java interface is called from a Web interface.

The subset of the test was designed from the following viewpoints.

i) Variation of developer test
   Supplementing the cases of operation which are not carried out by a developer test and the case where the variation of the parameter is limited although it carries out by the developer test.

i i) Viewpoint of interface
   Testing all TSFIs in order to confirm the behavior of Web interfaces, Java interfaces and command interfaces. Moreover, it takes into consideration that a Java interface is called from a Web interface.

b) Independent Test Outline

54 tests were executed as a sampling test of the developer test at each combination of OS and a browser. As sampling, security functions and interfaces are considered as shown in 1 and 2 of "a) Viewpoint of Independent Test".

12 tests were executed as an evaluator test. In designing the independent test, supplementing with the developer test by considering the parameter and the role that are not considered by the developer test (as shown in above-mentioned i) and ii) of "a) Viewpoint of Independent Test").

Excluding the interface not related to SFR and the interface of the logout, all the interfaces were covered. It was judged that the interface not covered in the evaluator test does not have to be tested because the behavior can be confirmed enough by the test technique that the developer executed.

Outline of the independent test that the evaluator executed is as follows.

<Content of Execution of the Independent Test >

Table 7-3 shows the points of view for the independent test and the content of the test corresponding to them.

Table 7-3 Viewpoints for the Independent Test

Viewpoints for the independent test	Outline of the independent test
1. Function test of User addition	Confirming the behavior of user's registration by an account administrator. The developer tested the user registration by the system integrator, but other administrators' cases were not confirmed. Confirming the behavior by the administrator of the different role.
2. Function test of Password change	Confirming the behavior of password change by an account administrator. The developer tested own password change by the system integrator, but other administrators' cases were not confirmed. Confirming the behavior by the administrator of the different role.
3. Function test of password complexity setting change	Confirming the behavior of password complexity setting. The developer did not confirm the case where "0" and a negative number were contained as a password complexity setting. Confirming the behavior concerning the rule including "0" and a negative number.
4. Change function test of warning banner in Web interface	Confirming the behavior of a warning banner at the time of a setup. The developer tested a single HTML tag. However, the case where the character and the attribute were contained to compose tag was not confirmed.
5. Change function test of warning banner in command interface	Confirming the behavior of a warning banner setup with a command interface. The developer tested the new setting of the banner. However, once it was set in the Web interface, the change was not confirmed. Confirming the behavior at the time of executing the command, after setting up with a Web interface.
6.Function test of Lock status of hcmdslink command	Confirming the behavior of hcmdslink command. The developer tested the relation of the frequency of continuous authentication failure influences on the interface that causes the event. However, the developer did not confirm the relation of failure frequency in other interfaces. Confirming the relation of frequency of continuous authentication failure of other interfaces.
7. Function test of Lock status of hcmdsrep command	Confirming the behavior of hcmdsrep command. The developer tested the relation of frequency of continuous authentication failure was influenced on the interface that causes the event. However, the developer did not confirm the relation of failure frequency in other interfaces. Confirming the relation of frequency of continuous authentication failure of other interfaces.

8. Function test of Lock status of hcmdsxrep command	Confirming the behavior of hcmdsxrep command. The developer tested the influence of the frequency of continuous authentication failure was influenced on the interface that causes the event. However, the developer did not confirm the relation of failure frequency in other interface. Confirming the relation of failure frequency in other interfaces.
9. Function test of Lock release function test of hcmdsunlockaccount command	Confirming the behavior of (hcmdsunlockaccount) command. The developer did not confirm the behavior when the password more than prescribed password length was input. Confirming the behavior at the time of inputting the password length of the more than set up.
10.Authentication function test of external authentication (LDAP)	Confirming the behavior of the external authentication function when LDAP is specified for an external authentication. The developer tested the external authentication function by the storage administrator, and other administrator's cases were not confirmed. Confirming the behavior by the administrator of the different role.
11. Authentication function test of external authentication (RADIUS)	Confirming the behavior of the external authentication function when RADIUS is specified for an external authentication. The developer tested the external authentication function by the storage administrator, and other administrator's cases were not confirmed. Confirming the behavior by the administrator of the different role.
12. Authentication function test of external authentication (Kerberos)	Confirming the behavior of the external authentication function when Kerberos is specified for an external authentication. The developer tested the external authentication function by the storage administrator, and other administrator's cases were not confirmed. Confirming the behavior by the administrator of the different role.

c) Result

All the executed independent test was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the test results.

7.3.3 Evaluator Penetration Test

The evaluator devised the necessary evaluator penetration test (hereinafter referred to as "the penetration test") from the evaluation deliverables provided in process of evaluation, and executed the test about the exploitable vulnerability of

concern in the operational environment and the attack level which is assumed.

It explains the penetration test executed by the evaluator as follows.

1) Summary of the Penetration Test

Summary of the penetration test executed by the evaluator is as follows.

a) Vulnerability of concern

The evaluator searched for the potential vulnerabilities from the provided evaluation deliverables (security architecture specifications, a structural design document, a functional specification document) and from the public domain information, which identified the following vulnerabilities that require the penetration test.

1. Since the TOE uses the database, the possibility of causing SQL injection can be conceivable.
2. Since the TOE is a software that works on OS, the possibility of causing OS command injection can be conceivable.
3. As the problem generally concerned on a Web site application, the possibility of causing "unchecked path name parameter" or "directory traversal" is considered.
4. From the view point of a direct attack, the possibility of being attacked by the token with insufficient random nature or the illegal token can be considered.
5. As the problem generally concerned on a Web site application, the possibility of causing the cross site scripting is considered.
6. The TOE receives the password entered on the login screen that an upper class product offers, and the TOE itself is not offering the login screen. Therefore, SFR of the authentication feedback has not been selected. However, when the password is entered at login, there is a risk that the password displayed on the screen is peeped.
7. The TOE has the function which has restriction in the number of characters of a warning message or the maximum number. Therefore, unexpected operation may be carried out by inputting the data of the size exceeding the restriction. Moreover, when sanitization etc., are performed on the client, unexpected operation may be carried out by inputting the characters that need to sanitize directly for the TOE.
8. Other well-known vulnerabilities

b) Penetration Test Outline

The evaluators executed the following penetration test to identify possibly exploitable vulnerabilities.

< Penetration Test Environment>

The penetration test was executed in the environment that added inspection PC to the environment that executed an independent test.

Table 7-4 shows details of components of the penetration test configuration and tools used by the penetration test. As for the parts other than inspection PC, it is the same as the environment that executes an independent test. The penetration test was executed for all servers set up in the environment that executed an independent test.

Table 7-4 Components and Tools used for the penetration test

Components	Purpose of use
OS	WindowsXP SP3
Web browser	Microsoft Internet Explorer Version 6.0
	Microsoft Internet Explorer Version 8.0
Scan Tool	Nessus 4.4.0 -Security Scanner -The vulnerability database of the latest one as of February 9, 2011 is used.
Web server scan	Nikto 2.1.3 -Free ware -Security scanner intended for Web server -The vulnerability database of the latest one as of February 9, 2011 is used.
Tamper IE	TamperIE 1.2 -Free ware -The capture of the transmission data from IE and falsification to arbitrary data are available.

< Penetration Test Approach >

The test was executed for all servers set up in the environment that executed an independent test by stimulating the interface of the TOE using upper class products.

- Giving the stimulation from TSFI and confirming the behavior.
- Capturing the packet transmitted from the management client to the TOE and confirming the content.
- Falsifying the captured contents and transmitting them to the TOE.
- Executing the scan with the vulnerability inspection tool.

In the binary inspection, the binary file was opened with binary editor (Stirling), and part that can be recognized as character string was confirmed in the viewpoint "whether a secret parameter exists in a binary file in the form which can be extracted."

<Execution item of penetration test>

The penetration test was executed from the viewpoint of the problem about which we are generally concerned in the bypass, the direct attack, surveillance, and a Web site application. These tests were concretely classified into the following eight kinds of tests.

Table 7-5 shows vulnerabilities concerned and the content of related penetration test.

Table 7-5 List of Executed Penetration Test

Vulnerability	Outline of the penetration test
1. Test of SQL injection	The parameter which may cause SQL injection is set as a POST parameter, inputs it into the TOE, and checks operation.
2. Test of OS command injection	The parameter which may lead to OS command injection is set as a POST parameter, inputs it into the TOE, and checks operation.
3. Test of directory traversal	Confirm the operation specifying the directory directly.
4. Confirmation of random nature of token and confirmation of execution by illegal token	Acquire the token and confirm that there is no rule. Input an illegal token to the parameter, and confirm the operation of the TOE.
5. Test of Cross Site Scripting	The parameter which may lead to Cross Site Scripting is set as a POST parameter, inputs it into the TOE, and checks operation.
6. Test of input value protection at inputting password	When the password is input, confirm whether there is a risk that the password displayed on the screen is peeped or not.
7. Test of buffer overflow	Regarding the parameter that has a restriction in the size, set the value that exceeds the restriction and confirm the operation.
8. Inspection with tools	To inspect other well-known vulnerabilities, inspect it with the tools.

c) Result

In the penetration test conducted by evaluator, the evaluator could not find the existence of the exploitable vulnerability that attackers with the attack capability assumed could exploit.

7.4 Evaluated Configuration

The penetration test was executed in the environment that added inspection PC to the environment that executed an independent test. It is the same as the environment that executes an independent test excluding inspection PC. The penetration test was executed for all servers set up in the environment that executed an independent test.

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 Conformant

- Security assurance requirements: Common Criteria Part 3 Conformant

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

- All assurance components of EAL2 package

- Additional assurance component ALC_FLR.1

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

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

1. Evaluation deliverables submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL2 and components ALC_FLR.2 in the CC part 3.

8.2 Recommendations

Note the following points as the part is explained by 1.1.3.

- This TOE assumes the operational environment that the client terminal accesses via the interface of Web. A remote access by SSH or the telnet is supposed to be prohibited so that an internal network is never directly accessed from the management client without using the TOE. The environment that the attacker accesses locally is not included in the target.
- Since the TOE doesn't offer the execution environment of the application, DoS attack is not considered as the target of evaluation.
- When the external authentication function or the linkage functionality for external authentication groups is used, identification and authentication function of the external authentication server and the external authorization server are not included in the TOE. Security objectives in that case shall be covered with the security objectives for the IT environment, and the security objectives achieved during operations.
- The impersonation of the external authentication server or the authorization server is assumed to be prevented by the operational environment.
- The TOE and data exist as a file that OS manages. It is necessary to install the TOE by the manager authority of OS. After the installation, the manager authority of OS is necessary for change/deletion of the file of the module etc. that compose the TOE. Moreover, the manager authority of OS is required to change or to delete the data.

- The online help of the product is not included in the guidance for the guarantee. As for the guidance for the guarantee, refer to "6. Documentation".

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided within a separate document of this certification report.

HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target Version 1.03 (April 8, 2011) Hewlett-Packard Company

11. Glossary

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

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

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

ACL	Access Control List
CVAECC	HP StorageWorks P9000 Command View Advanced Edition Software
DevMgr	HP StorageWorks P9000 Device Manager Software
RepMgr	HP StorageWorks P9000 Replication Manager Software
SAN	Storage Area Network
TSMgr	HP StorageWorks P9000 Tiered Storage Manager Software
TunMgr	HP StorageWorks P9000 Tuning Manager Software

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

ACL table	Table used for managing permissions information for account and storage management.
CVAECC	HP StorageWorks P9000 Command View Advanced Edition Software Common Component. CVAECC is a part of HP StorageWorks P9000 Command View Advanced Edition Software, and is the base module that provides common functions for the storage management software available in HP StorageWorks P9000 Command View Advanced Edition Software.
DevMgr	HP StorageWorks P9000 Device Manager Software. DevMgr is storage management software. It is part of HP StorageWorks P9000 Command View Advanced Edition Software, and provides volume management

	functionality for storage.
External authentication	Authentication method that uses an external authentication server (LDAP directory server, RADIUS server, or Kerberos server) external to the TOE from inside the TOE.
External authentication group linkage	A function of the TOE that acquires information about a group registered on an external authorization server and the accounts in the group, and then passes permissions information to the TOE. Because this function requires authentication functionality external to the TOE and the accounts belong to a group, this function is called *external authentication group linkage*.
Internal authentication	An authentication method that uses only the TOE internal authentication function. This is the same authentication method that is used in CVAECC 6.0.0-01.
Permissions (permissions information)	Indicates the type of operation that the TOE allows storage management software to perform. Permissions include User Management permissions for managing user information, View permissions for viewing storage, Modify permissions for modifying storage, and Execute permissions for executing tasks. Each user is assigned a permission or a combination of permissions as permissions information.
RepMgr	HP StorageWorks P9000 Replication Manager Software. RepMgr is storage management software. It is part of HP StorageWorks P9000 Command View Advanced Edition Software, and provides functionality for managing the copying between volumes in storage.
Security parameter	Parameter information related to CVAECC security functions. Parameter information includes such information as number and type of characters permitted in passwords; number of consecutive login failures and the corresponding threshold; and whether the threshold has been exceeded, in which case the account is locked.
TSMgr	HP StorageWorks P9000 Tiered Storage Manager Software. TSMgr is storage management software. It is part of HP StorageWorks P9000 Command View Advanced Edition Software, and controls the movement of data between volumes in storage.
TunMgr	HP StorageWorks P9000 Tuning Manager Software. TunMgr is storage management software. It is part of HP StorageWorks P9000 Command View Advanced Edition Software, and provides functionality for managing the efficiency with which the resources in storage are used.
Warning banner	Warning text displayed before users use storage management software. A warning banner is mainly used to call attention to the possibility of illegal use.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, February 2011, Information-technology Promotion Agency, Japan, CCS-01

[2] IT Security Certification Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-02

[3] Evaluation Facility Approval Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

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

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

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

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

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

[12] HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target, Version 1.03, (April 8, 2011), Hewlett-Packard Company

[13] HP StorageWorks P9000 Command View Advanced Edition Software Common Component Evaluation Technical Report, Version 2, July 25, 2011, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

[14] HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Guide, TB581-96059, Hewlett-Packard Company