DOC version	V2.8

WEBS-RAY V2.5

Security Target

Web Application Firewall Solution

ST

2008-10-22

TrinitySoft

Revision History

Revision	Date	Prepared By	Details of Changes
1.0	2006-06-14	Lee, Ju Young	Following the last consultation – integrated organization of the contents and unification of the version
1.1	2006-08-11	Lee, Ju Young	Correct the DB as environmental aspect
1.2	2006-11-09	Lee, Ju Young	ST 1st OR correction
2.0	2007-01-31	Kim, Young Ju	Overall correction/supplementation of ST in accordance with functional changes
2.1	2007-02-08	Kim, Young Ju	Correction due to changes in the subject web server and OS version
2.2	2007-09-17	Kim, Young Ju	Correction due to changes in the added gateway method
2.3	2007-10-15	Lee, Dong Un	Correction due to changes in the subject OS version
2.4	2008-09-16	Kim, Jin Kwan	Correction due to changes in the subject hardware specification
2.5	2008-09-30	Kim, Jin Kwan	Title of TOE changed : V2.5
2.6	2008-10-09	Kim, Jin Kwan	The number fo Device NIC and exclusive OS version
2.7	2008-10-15	Kim, Jin Kwan	Correction due to changes according to result of test (08-10-14/08-10-16)
2.8	2008-10-22	Kim, Jin Kwan	Correction due to changes according to result of test (08-10-21)

Table of Contents

1 Introduction to Security Target

This document is security target of WEBS_RAY V2.5, which is web application firewall, that defines the security function and security means that web application firewall must be equipped with, and describes general issues such as security requirements, realization methods and technological information used as the basis for evaluation.

This security target has been prepared by Trinity Soft Co., Ltd. and defines product type, scope of TOE, threats of TOE and presumptions, and describes security goals and requirement as well as explains security functions on the requirements supplied by TOE.

1.1 Identification of Security Target

Provides information necessary in identifying and controlling ST and TOE.

- Title: WEBS-RAY V2.5 Security Target V2.8
- Product: WEBS-RAY V2.5
- Identification of TOE: WEBS-RAY V2.5(Agent V2.5, Master Server V2.5, Admin Console V2.5)
- Target Web server: Apache 2.2.8
- Prepared by: Kim, Young Ju, Director of Research Institute, a subsidiary organization of Trinity Soft Co., Ltd.
- Evaluation standard
    1. Common criteria for information security system (Ministry of Public Administration and Security])
    2. CC Version: V2.3
- Evaluation assurance level: EAL4
- Security target version: V2.8
- Prepared on: October 25, 2008

1.2 Overview of Security Target

TOE is software-based web application firewall with functions that detects and intercepts, in advance, intrusions that uses HTTP(S) protocol by using vulnerability of web server and web application.

TOE must be front of the web server, it is protecting the web server. Furthermore, it performs the functions of detecting and intercepting intrusion and attack by analyzing the HTTP(S) Data of external or internal users on real-time.

This Security Target is document for CC certification on EAL4 of WEBS-RAY V2.5, and introduces Security Target, explains TOE as well as describes issues on TOE security environment, security goals, requirement definition, TOE summary specification and theoretical basis.

1.3 Composition of Security Target

- Chapter 1 deals with introduction to Security Target.
- Chapter 2 deals with brief explanation on TOE.
- Chapter 3 deals with presumptions, threatening elements and security policies on TOE.
- Chapter 4 deals with security goals.
- Chapter 5 organizes security function requirement and assurance requirements.
- Chapter 6 summarizes TOE functions.
- Chapter 7 presents theoretical basis for correspondence of security requirements with the security functions of TOE.
- Chapter 8 defines reference material.

1.4 Appropriateness of Common criteria

This Security Target complies with the following common criteria.

- Common Criteria for Information Security System (Public Announcement No. 2005-25 by the Ministry of Information and Communication)
- Compliance with Security Function Requirements of Part 2 of Common Criteria (CC) for Information Security System, Version 2.3
- Compliance with Assurance Requirement of Part 3 of Common Criteria (CC) for Information Security System, Version 2.3
- Strength of function targeted by this TOE is strength of function-medium.
- This TOE complies with EAL4.
- This ST does not accommodate security profile.

1.5 Definition of Terminologies

Among the terminologies used in this Security Target, those that are same as the terminologies used in the Common Criteria for Information Security System shall comply primarily with the corresponding basis.

a. HTTP Request

It is request made to web server on the client of the user, and the web server enables monitoring of data by conveying to TOE prior to processing of the corresponding request.

b. HTTP Response

It refers to responding of the result of processing by web server to the client of user, and the web server enables monitoring of data by conveying to TOE prior to responding.

c. Agent

performs the role of detecting and intercepting attacks approaching the web server, and coping with attacks.

d. Master Server

Plays central role such as intrusion attempt log management, policy management and real-time information integrated conveyance function by forming interface mainly with Agent and Admin Console.

e. Admin Console

It is security management program installed on administrator's PC, and performs the role of applying necessary policy issues, or verifying or searching audit record information by accessing the Master Server.

f. OWASP

It is abbreviation of Open Web Application Security Project and is an open project accomplished through voluntary participation of companies and individuals with vision on web application security. It is an organization that researches web application security with authority that provides diverse range of information and tools. This TOE has the Top 10 vulnerabilities announced by this organization in 2004 as its basis.

g. NTP

It is an abbreviation of Network Time Protocol and is the protocol that provides time stamp. Currently, time on Agent and Master Server are synchronized through same address of NTP by delivering NTP address to Agent when the Master Server sets address of NTP on TOE.

h. SSL

It is an abbreviation of Secure Socket Layer and uses SSL in order to protect TSF data transmitted between TOE that are segregated by layer of program category for coding of inputting and outputting of data of network socket. RSA (1024 bit) is used for generation of key while 3DES (168 bits) is used for coding. SHA-1 (128 bits) is used to support flawlessness.

i. White URL

Registration of page that is normally operated and serviced on web server is estabilished to as White URL collection with the collected files estabilished to as White URL.

j .Trust IP

It is referred to as trusted IP and indicates IP that does not undergo security audit for having been deemed to be normal user at the time of requesting specific service with web server.

k. Access denial IP

It is IP that is being limited to access even for normal web service. It refers to the IP for which access (manual) is denied automatically or by administrator when the number of access denial has reached the critical number.

l. Authorized administrator

Authorized administrator is administrator who can access TOE through identification and certification, and there exist installer, super administrator, administrator and monitor account.

m. Web application firewall

Security products which monitors HTTP and HTTPS DATA and controls its flow in order to detect and intercept attacks using the vulnerability of web server or web application are referred to as web application firewall.

N, Operation mode

TOE is operation as 3 kind of mode as following, disable mode, detect mode and protect mode

a). In case of disable mode, It's equal with state that TOE is not installed. When you upload a policy or you don't receive log file normally, you can set this mode. therefore It does not become defence and detection about attacks

b). In case of detect mode, Before protect mode is operated, detect violation and achieve inspection recording because information flowing control is forced when apply test and rule, but this mode does not become connection interception.

c). In case of protect mode, which device provides security control management service normally, session and connection are intercepted as information flow control is forced at invasion reading.

1.6 Rules of Preparation

This Security Target uses English mixedly for some abbreviations and in order to convey precise meaning, and Common Criteria allows selection, allocation, elaboration and repeated operation that can be executed in the security function requirements. Each operation is used in this Security Target.

Repetition

It is used when same component is repeated in diverse range of operations. The outcome of the repetition operation is indicated as repetition number in parenthesis that comes after the identification code of the component, that is, (repetition number).

Selection

It is used in selecting more than one selections provided in the Common Criteria for Information Security System at the time of describing the requirements. Outcome of selection operation is indicated in <u>*underlined Italic font*</u>.

Elaboration

It is used in further limiting the requirements by adding detailed items in the requirements. Outcome of the elaboration operation is indicated in **bold font**.

Allocation

It is used in allocating the specific value of medium variable that is not specified (e.g. length of password).

The outcome of allocation operation is indicated by the large bracket, that is, [allocation value].

2 Explanation of TOE

This chapter briefly describes composition and environment of TOE, and explains the fundamental issues on TOE. TOE satisfies the EAL4 level of requirements for Common Criteria for Information Security System.

WEBS-RAY V2.5 is a web application firewall product that provides functions that can strongly detect the attacks that can be generated in web by collecting White URL collection and key contents information in order to detect and intercept attack on web server services. It is a software-based security product that offers centrally concentrated management and expandability through 3-Tier Architecture.

2.1 Composition of TOE

2.1.1 Compositon of gateway method(Single)

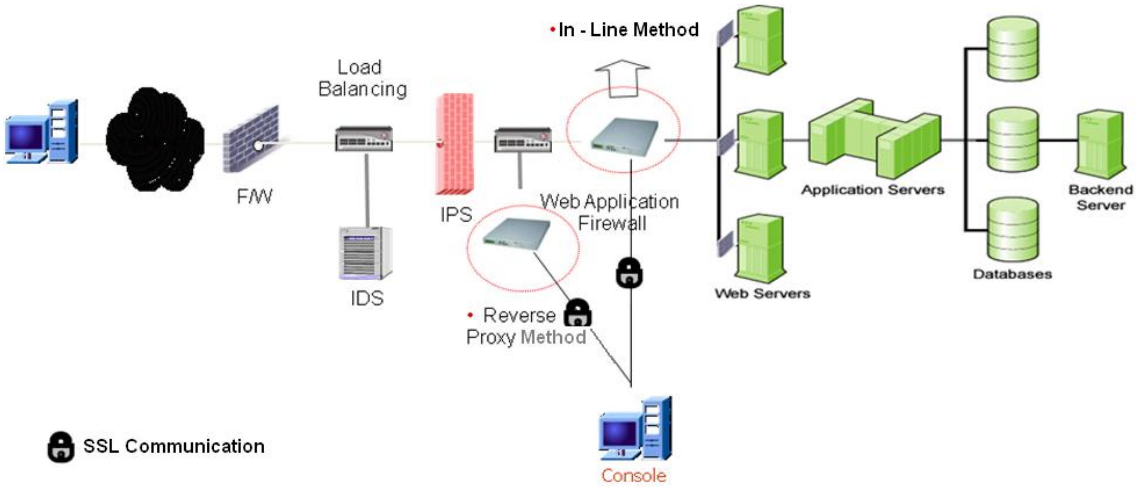


Diagram 2. 1 Composition of TOE

TOE, as shown above, is composed of Agent, Master Server and Admin Console(install administrator PC). Here, TOE, since it is a product that audits HTTP(S) Data only and cannot defend attack on the network, it is recommendable to maximize the efficiently by installing firewall, IDS and IPS that detects and intercepts network attack in front of the TOE for safe composition

The Admin Console has secured channel and route through which TSF data can be transmitted safely by using SSL protocol between Agent and Master Server, and between

Admin Console and Master Server in order to protect the TSF data being transmitted between the segregated TOEs.

2.1.2 Compositon of gateway method(Multiple)

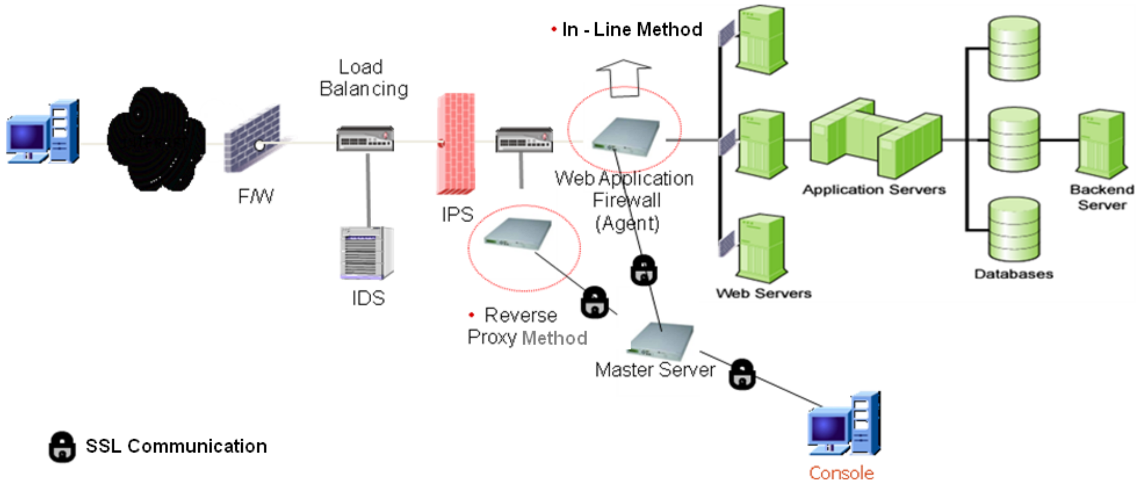


Diagram 2. 2 Composition of TOE

TOE, as shown above, is composed of Agent and Master Server install to special administration system and Admin Console(install admistrator PC). Here, TOE, since it is a product that audits HTTP(S) Data only and cannot defend attack on the network, it is recommendable to maximize the efficiently by installing firewall, IDS and IPS that detects and intercepts network attack in front of the TOE for safe composition

2.2 TOE Environment

2.2.1 IT Environment

WEBS-RAY V2.5 secures temporal validity of audit record generated on real-time through temporal synchronization between segregated TOEs using NTP server. Here, it communicates with NTP server by using Network Time protocol realized by using RFC 130. It uses SSL protocol for safe communication, and communicates between Agent and Master Server, and between Admin Console and Master Server on the OpenSSL v0.9.8b basis. It stores audit record information by using MySQL 4.1 in order to store all audit record data generated in TOE.

2.2.1 Operating Environment

System operating environment of WEBS-RAY V2.0 is illustrated in the following Table 2.1. WEBS-RAY V2.0 is a software format, and its hardware and operation system is excluded from being subjected to evaluation.

Table 2.1 System Operating Environment

- Composition of gateway method(single)

Table 2.1 Composition of gateway(single) method Operating Environment

Model	Composition Elements	Items	Minumum Specification
GW-1000 	Common	CPU	Intel DuoCore 2.0GHz * 1 EA
		OS	Exclusive use OS (2.5)
		NIC	10/100M/1G bps (UTP*6)
		Momery	2GB
		Disc	160GB
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
GW-2500 	Common	CPU	Intel QuadCore 2.0GHz * 1EA
		OS	Exclusive use OS (2.5)
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		Momery	4GB
		Disc	250GB
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
GW-3000 	Common	CPU	Intel QuadCore 2.5GHz * 2EA
		OS	Exclusive use OS (2.5)
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		Momery	8GB
		Disc	250GB
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
Common	Admin Console (S/W)	CPU	Pentium IV 1GHz 이상
		OS	Windows XP SP2
		NIC	10/100/1G bps
		Momery	More than 256M
		Disc	More than 40G

- Composition of gateway method(multiple)

Table 2.2 Composition of gateway(multiple) method Operating Environment

Model	Composition Elements	Items	Minumum Specification
GW-1000 	Agent	CPU	Intel DuoCore 2.0GHz * 1 EA
		OS	Exclusive use OS (2.5)
		Proxy Server	Apache 2.2.8
		NIC	10/100M/1G bps (UTP*6)
		Momery	2GB
		Disc	160GB
		Disc	160GB
GW-2500 	Agent	CPU	Intel QuadCore 2.0GHz * 1EA
		OS	Exclusive use OS (2.5)
		Proxy Server	Apache 2.2.8
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		Momery	4GB
		Disc	250GB
GW-3000 	Agent	CPU	Intel QuadCore 2.5GHz * 2EA
		OS	Exclusive use OS (2.5)
		Proxy Server	Apache 2.2.8
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		Momery	8GB
		Disc	250GB
Common	Master Server (S/W)	CPU	More than Intel DuoCore 2.0GHz * 1 EA
		OS	Fedora Core 6 + Linux Kernel 2.6.20
		DB	MySQL 4.1
		NIC	10/100/1G bps
		Momery	More than 2Giga
		Disc	More than 160Giga
	Admin Console (S/W)	CPU	More than Pentium IV 1GHz
		OS	Windows XP SP2
		NIC	10/100/1G bps

		Momery	More than 256M
		Disc	More than 40G

2.3 Scope and Boundary of TOE

The scope and boundary of TOE illustrates the physical and logical boundary that composes TOE, and this boundary is illustrated in the following diagram

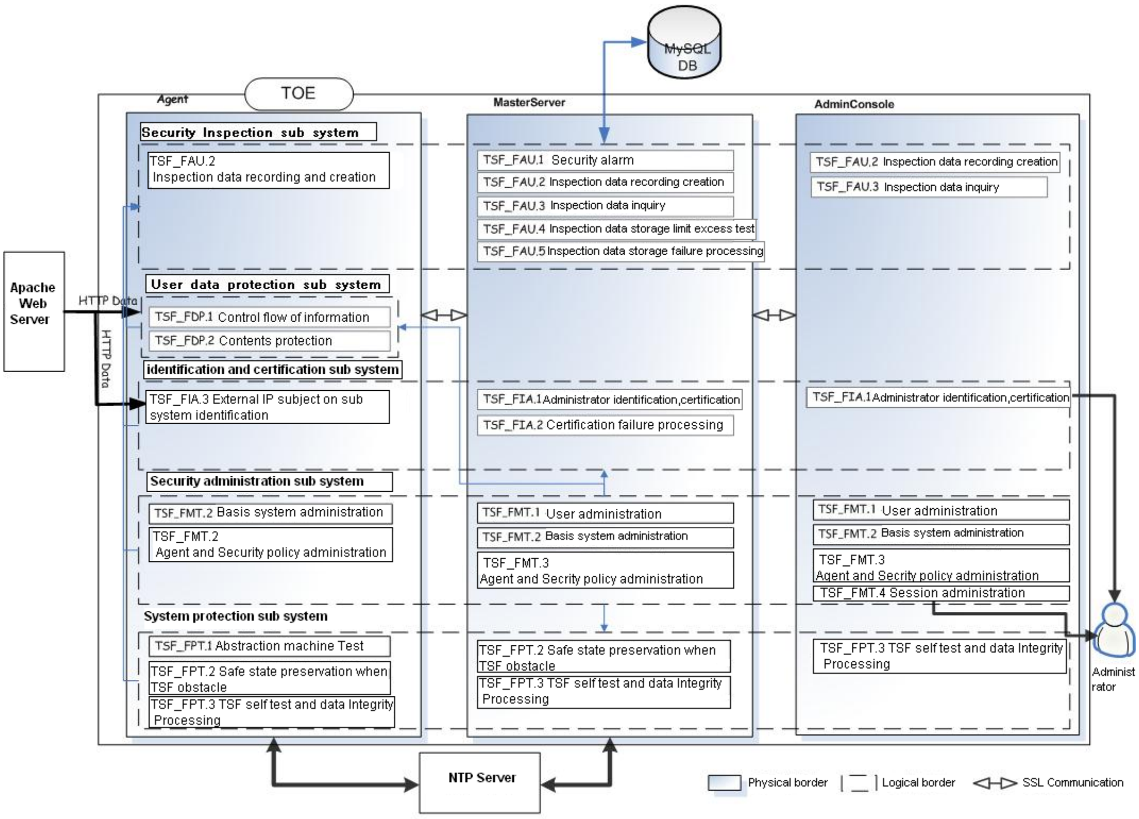

MySQL DB
TOE
Agent
MasterServer
AdminConsole
Security Inspection sub system
TSF_FAU.2 Inspection data recording and creation
User data protection sub system
TSF_FDP.1 Control flow of information
TSF_FDP.2 Contents protection
identification and certification sub system
TSF_FIA.3 External IP subject on sub system identification
Security administration sub system
TSF_FMT.2 Basis system administration
TSF_FMT.2 Agent and Security policy administration
System protection sub system
TSF_FPT.1 Abstraction machine Test
TSF_FPT.2 Safe state preservation when TSF obstacle
TSF_FPT.3 TSF self test and data Integrity Processing
TSF_FAU.1 Security alarm
TSF_FAU.2 Inspection data recording creation
TSF_FAU.3 Inspection data inquiry
TSF_FAU.4 Inspection data storage limit excess test
TSF_FAU.5 Inspection data storage failure processing
TSF_FIA.1Administrator identification,certification
TSF_FIA.2 Certification failure processing
TSF_FMT.1 User administration
TSF_FMT.2 Basis system administration
TSF_FMT.3 Agent and Secrity policy administration
TSF_FPT.2 Safe state preservation when TSF obstacle
TSF_FPT.3 TSF self test and data Integrity Processing
TSF_FAU.2 Inspection data recording creation
TSF_FAU.3 Inspection data inquiry
TSF_FIA.1Administrator identification,certification
TSF_FMT.1 User administration
TSF_FMT.2 Basis system administration
TSF_FMT.3 Agent and Secrity policy administration
TSF_FMT.4 Session administration
TSF_FPT.3 TSF self test and data Integrity Processing
Apache Web Server
HTTP Data
HTTP Data
Administ rator
NTP Server
Physical border
Logical border
SSL Communication

Diagram 2. 3 Physical/Logical Scope and Boundary of TOE

2.3.1 Physical Boundary

Physical scope and boundary of TOE corresponds to the Agent, Master Server and Admin Console that composes the segregated TOE, and NTP server, that are connected to interface of TOE are IT environment. Actual connection composition elements of TOE that belongs to the physical scope and boundary of TOE are as follows.

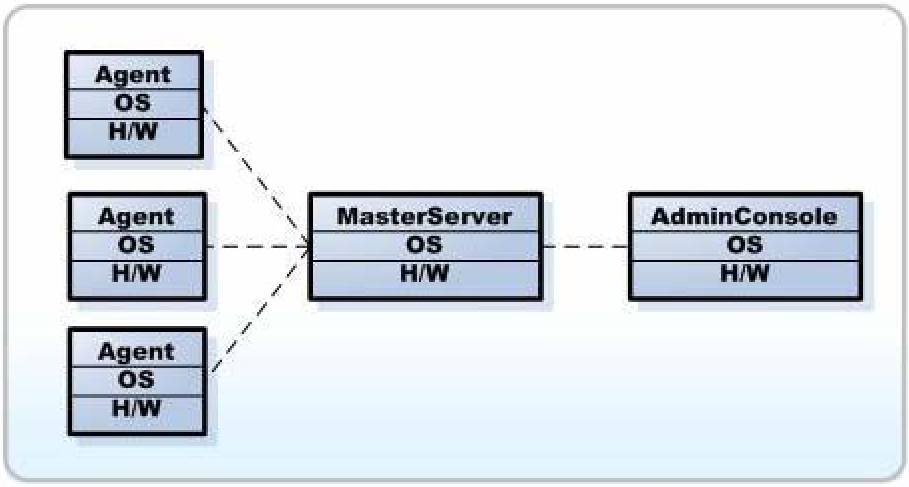


Diagram 2.4 Physical range of TOE

Agent

Agent is installed on independent system just as module of proxy server. It detects and intercepts web attacks that use vulnerability of web server or web application.

Agent can be installed with Master Server on same machine or on other machine.

Agent Demon creats in the ratio of 1:1 with web server to be protected.

Each Agent generates audit record on all data on to which attack on web server occurs, and such audit record information is conveyed to the Master Server and deleted immediately upon their generation. If the audit record is not conveyed to the Master Server due to abnormality in the status of the network, then the audit record information is stored in Agent temporarily. Once the network operates normally, the audit record data which was not transmitted is conveyed to the Master Server.

Master Server

Master Server is a software program that is installed on independent system. It receives and stores all audit record data generated at the Agent, Master Server and Admin Console, and supports real-time viewing of the audit record as well as inquiry and search on audit record through Admin Console for each purpose being requested by the administrator. Furthermore, it supports alarm service function, thereby receiving all warnings generated in the TOE and notifies to the administrator.

NTP can be set on the Master Server for temporal synchronization on audit records, and IP information of NTP is conveyed to Agent and temporal synchronization achieved between 2 segregated TOEs. Therefore, with regards to the audit record information generated at Agent and Master Server, audit record information is generated at same time value conveyed from single NTP server.

Admin Console

Admin Console is a security management program that is operated by being installed on PC of each administrator.Admin Console is categorized into websray, super administrator, and monitor account

In the case of websray account, it is an account that can generate super administrator account. Once the super administrator account is generated and logged in, the websray account is automatically deleted.

Practically, account necessary in managing the audit data and security policy through Admin Console includes super administrator, administrator and monitor account. In the case of super administrator, it, as an account that manage the TOE integratingly, can generate administrator and monitor account. The administrator has the control management authority only on the Agent system designated to be managed at the time of granting of account by the super administrator. Although the monitor account also has the authority to access the Agent system designated for monitoring at the time of granting of the account by the super administrator, similar to the administrator account, it does not have control authority and can only view set information.

2.3.2 Logical Boundary

The logical boundary of TOE, as illustrated in the Diagram 2-3, can be categorized into boundaries for security management, security audit, system protection, identification and certification and user data protection.

a. Security Management

Security Management enables administrator, authorized for the purpose of securely operating the TOE, to manage the setting information and security policy necessary for operation of TOE. Such security management can be divided largely into system management and security policy management. System management can be performed only by the administrator with super administrator account. Security policy management can be performed by administrator with super administrator account and administrator account. In the case of monitor account, addition, correction and deletion among the security policy management activities are not possible, with only inquiries of the security policies allowed.

b. System Protection

System protection provides 3 functions including assurance of maintenance of secured status on disability of service daemon operating in the TOE, provision of flawlessness on contents and property value of various security policies and TSF execution code, and TSF data protecting from exposure and modification on transmission data at the time of TSF data between the segregated TOEs. For this purpose, TSF service daemon and flawlessness examination is performed at designated period. Furthermore, it provides SSL communication channel between Agent and Master Server and between Admin Console and Master Server installed on the authorized administrator’s PC for secured communication. It uses Key Exchange Algorithm (RSA-1024bit), Confidentiality Algorithm (3DES-168bit), and Flawlessness Algorithm (SHA-1-128bit) at the time of SSL communication.

c. Identification and Certification

Identification and certification on the authorized administrator (installer, super administrator, administrator, and monitor account) is executed through ID and password in order to prevent illegal acquisition of authority by unauthorized user. Furthermore, Client IP is used for identification on user requesting service through web server.

d. Security Audit

Security audit generates security related audit data information generated in the TOE for the purpose of verifying the outcome for confirmation and ex post facto tracing of all information of TOE in operation. Audit data includes normal access to web server, countermeasure against abnormal access, setting information of administrator, identification and certification information on user, and daemon operation information. Such audit data are reviewed through inquiries, real-time viewing and searching, and is utilized in analysis of potential infringement.

f. User Data Protection

User data protection is main function of information flow control, Information flow control is the function that securely protects key information and resources that are registered in the web server by detecting and intercepting harmful traffic in advance by receiving and analyzing the HTTP(S) Data accessing the web server. Harmful traffic includes intrusion attack on 10 vulnerabilities defined in the OWASP, including unauthorized access to HTTP(S) service, cross site scripting, SQL Injection, and web service rejection attack.

3 TOE Security Environment

TOE security environment is composed of presumptions describing the security on TOE environment, threat that can be imparted onto the OTE asset or environment by the threatening source, and security policies of the organization which are the regulations, procedures, customary practices, and guidelines that TOE must comply with for security.

Presumptions

It is presumed that the following conditions exist in the operating environment of TOE.

Table 3.1 Presumptions

Name	Explanation
A. Physical security	TOE is located in physically secured environment to which only the authorized personnel can be accessed.
A. Security maintenance	In the event of changes in the security environment due to changes in the composition of network, composition of host, composition of web server and composition of web application, changed environment and security policies are reflected onto the TOE operation policy immediately in order to maintain security at the level same as before.
A. Trusted administrator	Authorized administrator of TOE has no ill-intentions, has received appropriate training on the TOE administrations functions and executes its duties accurately in accordance with administrator's guidelines.
A. Fortification of operating system	Assure reliability and security on the operating system by removing the vulnerability of operating system in advance through elimination of services (service port) and means on the operating system that are not necessary for TOE.
A. Fortification of web server	Assure reliability and security on the operating system by removing the vulnerability of operating system in advance through elimination of unnecessary program existing on the web server for TOE and patch with the latest version.
A. Secured external server	The latest time is downloaded from the NTP server in order to maintain reliable time of TOE, which assures reliability and security of the server.
A. Secured SSL	SSL used between TOEs are securely operated and confidentiality

	of data conveyed between the TOEs is assured.
A. Secured DB	Securely stores audit data generated in TOE and assures the security of DB used in searching and arraying of audit data.

Threats

This Security Target categorizes and defines the security threats that the external source of threat can used on protection asset of TOE into threat on TOE and threat on TOE operating environment.

Key assets that TOE is protecting are the web server and web application resources and data provided through the web application. External source of threat either prevents normal usage by attacking vulnerabilities of web server and web application or uses key information it has abstracted maliciously.

The source of threat has low level specialization knowledge, resources and motivation, and it is presumed that the possibility of the source of threat discovering the vulnerability that can be used maliciously is low. The source of threat that generates such threat is either user who is not authorized for the right to use TOE or external IT entity.

Threats on TOE

Table 3.2 Threat

Name	Explanations
T. Disguise	Source of threat may access TOE by disguising as authorized administrator.
T. Defect	If TOE is being used or defectiveness occurs due to external attack, then it may not provided normal services to user...
T. Record failure	Security related cases of TOE may not be recorded due to exhaustion of storage capacity
T. Abnormal transfer of information	The source of threat may induce erroneous operation of web server by transmitting web service requested information with abnormal structure, or by transmitting web service request information that includes unauthorized information.
T. Attack on new vulnerability	The source of threat may attack by maliciously using the new vulnerability of computer system of the internal network in the TOE or TOE operating environment.

T. Service rejection attack	The source of threat may hinder usage of normal users by making abnormal web service request to cause abnormal and excessive usage of the resources of web server in TOE operating environment.
T. Continuous certification attempts	The source of threat may access TOE by disguising as authorized administrator by continuous attempt at certification on TOE.
T. Unauthorized changes of TSF data	SF data may be changed without authorization due to buffer overflow attack of the source on TOE.

Threats on TOE Operating Environment

Table 3.3 Threats on operating environment

Name	Explanation
TE. Incompetence in management	TOE may be composed, managed and used in unsecured format by the authorized administrator에.
TE. Distribution installation	The security of TOE may be damaged in the process of distribution and installation

Policy

Table 3.4 Policy

Name	Explanation
P. Security audit	Security-related cases must be recorded and maintained and the recorded data reviewed in order to trace responsibilities on related behaviors.
P. Secured administrations	Authorized administrator shall manage TOE with secured method.

4 Security Target

This Security Target describes the security target to be accomplished by TOE or environment in order to cope with security environment. Security target is categorized and defined as TOE security target and security target on environment. TOE security target is the security target that needs to be handled by TOE directly and security target on environment is the security target handled by IT domain or non-technical/procedural means.

Security Target of TOE

Following are the security targets that are handled directly by TOE.

Table 4.1 Security Target by TOE

Name	Explanation
O. Security audit	TOE must record and maintain security related cases in order to enable tracing of responsibilities for security related actions, and provide means of reviewing recorded data
O. Security management	TOE shall provide management method of efficiently managing TOE by authorized administrator of TOE in secured method.
O. Abnormal interception of web service	TOE must intercept HTTP(S) Data that has abnormal structure and information among the HTTP(S) Data that passes TOE.
O. Interception of service refusal attack	TOE, in the event of usage of service resources of the web server by attackers by abnormally requesting web service, must be able to intercept such in order to enable web service of the web server being protected to allow normal users to use the web service.
O. Identification and certification	TOE must certify the identity of administrator prior to allowing access to TOE following identification of administrator. Furthermore, it must certify the identity of Agent after having identified Agent.
O. TSF data protection	TOE must protect TSF data stored in TOE from exposure, changes and deletion that are not authorized.
O. Self function protection	During operation of TOE, it must protect itself from changes of and non-activation of TOE security functions.

Security Target on Environment

The following are security targets to be accomplished by IT domain or non-technical/procedural means.

Table 4.2 Security Target on Environment

Name	Explanation
OE. Physical security	TOE must be located in physically secured environment to which only the authorized administrator can access.
OE. Maintenance of security	In the event of changes in the security environment due to changes in the composition of network, host, web server and web application, it must reflect the changed environment and security policies onto TOE operating policies immediately in order to maintain level of security that is same as before.
OE. Trusted administrator	Authorized administrator of TOE has no ill-intentions, has received appropriate training on the TOE administrations functions and executes its duties accurately in accordance with administrator's action guidelines and procedures.
OE. Secured management	TOE is distributed and installed with secured method, and must be composed, managed and used in secured method by authorized administrator.
OE. Fortification of operating system	Assure reliability and security on the operating system by removing the vulnerability of operating system through elimination of services or means on the operating system that are not necessary for TOE and by performing fortification on vulnerability of operating system.
OE. Fortification of Web server	Assure reliability and security on the web server by fortifying the vulnerability of operating system by TOE.
OE. Renewal of vulnerability list	The administrator must renew and manage the data base on the vulnerability that the TOE is managing in order to protect from the external attack using new vulnerability of web server.
OE. Secured external server	NTP server located externally must be secured in order to maintain reliable time of TOE.
OE. Secured SSL	Assure the security of SSL used in communication between segregated TOEs and confidentiality of data conveyed between the TOEs.
OE. Secured DB	Securely stores audit data generated in TOE and assures the security of management and operation of DB used in searching and arraying of audit data.

5 Definition of Requirements

IT security requirements describe security functions and assurance requirements, which is describe in this Security Target that TOE satisfies.

TOE security function requirements

IT security requirements of this security target are composed of functional components of Part 2 of Common Criteria (CC v2.3).

FIA_UAU.2 with probability and arraying mechanism has mid-level strength of function

TOE security function requirement components used in this security target are as per the Table 5.1 below.

Table 5.1 Security function requirements

Security function class	Security function components	
Security audit	FAU_ARP.1	Security alarm
	FAU_GEN.1	Generation of audit data
	FAU_GEN.2	Association of user identity
	FAU_SAA.1	Analysis of potential infringement
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Audit evidence protection
	FAU_STG.3	Countermeasure actions in the event of anticipated loss of audit data
	FAU_STG.4	Prevention of loss of audit data
User data protection	FDP_IFC.1(1)	Control of partial information flow (1)
	FDP_IFC.1(2)	Control of partial information flow (2)
	FDP_IFF.1(1)	Property of unitary class security (1)
	FDP_IFF.1(2)	Property of unitary class security (2)
Identification and certification	FIA_AFL.1	Processing of certification failure
	FIA_ATD.1(1)	Definition of user property (1)
	FIA_ATD.1(2)	Definition of user property (2)
	FIA_UAU.2	Certification of user prior to all actions
	FIA_UAU.7	Certification feed-back protection
	FIA_UID.2(1)	Identification of user prior to all actions (1)
	FIA_UID.2(2)	Identification of user prior to all actions (2)
Security management	FMT_MOF.1(1)	Security function management (1)
	FMT_MOF.1(2)	Security function management (2)
	FMT_MOF.1(3)	Security function management (3)
	FMT_MOF.1(4)	Security function management (4)
	FMT_MSA.1	Security property management
	FMT_MSA.3	Static property initialization

	FMT_MTD.1(1)	TSF data management (1)
	FMT_MTD.1(2)	TSF data management (2)
	FMT_MTD.1(3)	TSF data management (3)
	FMT_MTD.1(4)	TSF data management (4)
	FMT_MTD.2(1)	Management of limit of TSF data (1)
	FMT_MTD.2(2)	Management of limit of TSF data (2)
	FMT_SMF.1	Management function specification
	FMT_SMR.1	Security role
TSF protection	FPT_AMT.1	Testing of abstract machine
	FPT_FLS.1	Maintenance of secured status at the time of disability
	FPT_TST.1	TSF self testing
Accessing TOE	FTA_SSL.1	Closure of session by TSF

Security Audit

FAU_ARP.1 Security Alarm

Class relationship: None

Subordinate relationship: FAU_SAA.1 Analysis of potential infringement

FAU_ARP.1.1 TSF, in the event of detecting potential security infringement, must take [the following countermeasure actions].

[

- Notify the authorized administrator through the alarm window of administrator’s screen
- Transmission of alarm mail to authorized administrator

]

FAU_GEN.1 Generation of audit data

Class relationship: None

Subordinate relationship: FPT_STM.1 Trustable time stamp

FAU_GEN.1.1 TSF must be able to generate audit record on the following cases to be subjected to audit.

a) Start-up and shut-down of audit function
b) ***Not designated*** All cases to be subjected to audit in accordance with the level of audit
c) [[Table 5.2] Cases to be subjected to audit]

Table 5.2 Cases to be subjected to audit

Function component	Cases to be subjected to audit	Additional audit record contents
FAU_ARP.1	Countermeasure actions taken due to urgent security infringement	Means of countermeasures
FAU_SAA.1	Automatic measures taken through Start-up and shut-down of analysis mechanism and tools.	Identification of authorized administrator that conducts the action
FAU_STG.3	Countermeasure actions in the event of exceeding the critical value	-
FAU_STG.4	Countermeasure action in the event of failure in audit storage	-
FDP_IFF.1	Decision on interception, allowance and detection of requested information flow	Identification information of object, number of intrusion attempts, URL route, countermeasure method
		-
FIA_AFL.1	Reaching the limit of failed certification attempts and countermeasure actions taken, if appropriate, recovery to normal status to follow.	Identification of illegal user and authorized administrator
FIA_UAU.2	Failure in usage of certification mechanism	User identity provided to TOE
FIA_UID.2	Failure in usage of user identification mechanism including user identification provided	User identity provided to TOE
FMT_MSA.1	All changes on security property value	Value of security property
FMT_MTD.1	All changes on TSF data value	Value of changed TSF data
FMT_MTD.2	All changes on limit of TSF data	Limit of changed TSF data
FPT_AMT.1	Execution and result of test on lower portion abstract machine	-
FPT_FLS.1	Occurrence of TSF disability	-
FPT_TST.1	Execution and test result of TSF self test	-
FTA_SSL.1	Closing of mutually reacting session due to session closure mechanism	-
FMT_SMF.1	Usage of administrative function	Identity of authorized administrator performing the operation

FAU_GEN.1.2 TSF must record the following information in each audit record as the very minimum.

a) Date of case, type of case, identity of the subject, outcome of the case (success or failure)

b) For each type of audit case, [[Table 5.2] Information related to cases to be subjected to audit] based on the definition of cases to be subjected to audit of function components including in the **Security Target**

FAU_GEN.2 Association of user identity

Class relationship: None

Subordinate relationship: FAU_GEN.1 Generation of audit data
FIA_UID.1 identification

FAU_GEN.2.1 TSF must be able to associate the identity of the user that caused the case with the case to be subjected to audit.

Caution at the time of application: User refers to the authorized administrator and identified person (administrator ID or client IP address) on audit record activities on web service request.

FAU_SAA.1 Analysis of potential infringement

Class relationship: None

Subordinate relationship: FAU_GEN.1 Generation of audit data

FAU_SAA.1.1 TSF must be able to apply rule set in the event of examining audited case, and must be able to indicated potential infringement on TSP on the basis of this rule.

FAU_SAA.1.2 TSF, in the event of examining audited case, must apply the following regulations.

a) Known accumulation or combination of [partial set of cases to be subjected to audit as follows] that indicates potential security infringement

[

- Fail to identify and certify administrator 3 times(1 minute)
- Abnormal status of proxy server
- Abnormal status of process
- Registration of access interception IP according to accumulation of intrusion attempt

- Occurrence of DOS case
- Occurrence of DDOS case

]

b) [None]

FAU_SAR.1 Review of audit

Class relationship: None

Subordinate relationship: FAU_GEN.1 Generation of audit data

FAU_SAR.1.1 TSF must provide to the [authorized administrator (super administrator, administrator, monitor account)] the function that can read [audit data as follows] from the audit record.

[

- Intrusion attempt log
- Work log
- Notification message

]

FAU_SAR.1.2 TSF must provide audit record to enable the user to appropriately interpret information.

FAU_SAR.3 Selectable audit review

Class relationship: None

Subordinate relationship: FAU_SAR.1 Audit review

FAU_SAR.3.1 TSF shall provide ability *to sequentialize* audit data on the basis of [the following standard].

[

- Identity of subject
- Identity of object
- Date of case
- Type of case
- Countermeasure action of the case
- Outcome of case (success or failure)

]

FAU_STG.1 Audit evidence protection

Class relationship: None

Subordinate relationship: FAU_GEN.1 Generation of audit data

FAU_STG.1.1 TSF shall protect the stored audit record from unauthorized deletion.

FAU_STG.1.2 TSF must *prevent* unauthorized changes on audit record.

FAU_STG.3 Countermeasure actions in the event of anticipated loss of audit data

Class relationship: None

Subordinate relationship: FAU_STG.1 Audit evidence protection

FAU_STG.3.1 TSF, in the event of the audit evidence exceeding [80~89%(standard value of 80%) of the usage capacity], must take [the following countermeasure actions].

[

- Notify authorized administrator (alarm window (standard value), alarm mail)
- Generation of audit record

]

FAU_STG.4 Prevention of loss of audit data

Class relationship: FAU_STG.3

Subordinate relationship: FAU_STG.1 Audit evidence protection

FAU_STG.4.1 TSF, in the event of saturation of audit storage space, must perform *prevention of cases to be subjected to audit with the exception of actions taken by the authorized user with special authority* and [countermeasure actions as follows].

[

- Notification to authorized administrator (alarm window (standard value), alarm mail)
- Generation of audit record
- Stoppage of all TSF service with the exception of access and back-up by authorized administrator(super administrator account)

]

User data protection

FDP_IFC.1 (1) Control of partial information flow (1)

Class relationship: None

Subordinate relationship: FDP_IFF.1 Property of unified class security

FDP_IFC.1.1 TSF, for the [following subject list, information list and operation list], must enforce [policy of allowing information flow].

[

- Subject list: client that requests web service to the web server
- Information list: HTTP(S) Data
- Operation list: Allow HTTP(S) Data

]

FDP_IFC.1 (2) Control of partial information flow (2)

Class relationship: None

Subordinate relationship: FDP_IFF.1 Property of unified class security

FDP_IFC.1.1 TSF, for the [following subject list, information list and operation list], must enforce [policy of intercepting information flow].

[

- Subject list: client that requests web service to the web server
- Information list: HTTP(S) Data
- Operation list: Intercept HTTP(S) Data

]

FDP_IFF.1(1) Property of unified class security (1)

Class relationship: None

Subordinate relationship: FMT_MSA.3 Initialization of static property
FDP_IFC.1 Control of partial information flow

FDP_IFF.1.1 TSF shall at the least enforce [policy of allowing information flow] on the basis of subject security property and information security property types such as [the following subject security property and information security property.

[

- Subject security property: Client IP address that requests web service to web server

- Information security property
  - Trust IP: Client IP that is to be trusted at all times
  - Unfiltered file: File information of trusted URL that needs not be audited
  - Up-load allowed file: Information of file expander that allows uploading onto web server using notice board, etc.
  - Service domain: Domain information that requests normal service that is to be protected
  - White URL: Web page URL that requests normal service that is to be protected
  - Parameter allowance rule: Rule on allowing input value of parameter
  - Rule: Signature that detects know attack pattern
  - Name and value of cookie/hidden field: value of cookie and hidden field that will audit presence of alteration
  - User defined Rule : Signature of detecting the pattern defined as attack by the user

]

FDP_IFF.1.2 TSF, if the following rules are maintained, shall **allow** information flow between the controlled subject and controlled information through controlled operation.

[

- IP of the subject is IP that is registered in the Trust IP.
- Registration in unfiltered file
- Registration in upload allowed file
- Domain of HTTP(S) Data exist in service domain, URL exist in White URL, input value of parameter satisfies allowance rule, there are not Rule and user defined Rule and there are no alterations in cookie/hidden field.

]

FDP_IFF.1.3 TSF shall enforce [None].

FDP_IFF.1.4 TSF shall provide [None].

FDP_IFF.1.5 TSF shall explicitly authorize information flow on the basis of [None].

FDP_IFF.1.6 TSF shall explicitly deny information flow on the basis of [None].

FDP_IFF.1(2) Property of unified class security (2)

Class relationship: None

Subordinate relationship: FMT_MSA.3 Initialization of static property
FDP_IFC.1 Control of partial information flow

FDP_IFF.1.1 TSF shall at the least enforce [policy of intercepting information flow] on the basis of subject security property and information security property types such as [the following subject security property and information security property.

[

- Subject security property: Client IP address that requests web service to web server
- Information security property
  - Access intercepted IP: Client IP that is being intercepted for having been deemed to be ill intended attacker
  - DOS IP: Client IP defined as DOS
  - DDOS: Temporarily deny all services to come through for having been defined as DDOS.
  - Up-load intercepted file: Information of file expander that intercepts uploading onto web server using notice board, etc.
  - Service domain: Domain information that requests normal service that is to be protected
  - White URL: Web page URL that requests normal service that is to be protected
  - Parameter allowance rule: Rule on allowing input value of parameter
  - Rule: Signature that detects know attack pattern
  - Name and value of cookie/hidden field: value of cookie and hidden field that will audit presence of alteration
  - User defined Rule : Signature of detecting the pattern defined as attack by the user

]

FDP_IFF.1.2 TSF, if the following rules are maintained, shall **intercept** information flow between the controlled subject and controlled information through controlled operation.

[

- IP of the subject is IP that is registered in the access prevented IP.
- IP of the subject is IP that is registered in the DOS IP.
- DDOS case is registered
- Registration in upload prevented file
- Domain of HTTP(S) Data does not exist in service domain
- URL of HTTP(S) Data does not exist in White URL
- Input value of parameter of HTTP(S) Data violates allowance rule
- HTTP(S) Data has been detected by Rule and user defined Rule
- Alteration has been detected in the examination of value of cookie/hidden field of HTTP(S) Data.

]

FDP_IFF.1.3 TSF shall enforce [None].

FDP_IFF.1.4 TSF shall provide [None].

FDP_IFF.1.5 TSF shall explicitly authorize information flow on the basis of [None].

FDP_IFF.1.6 TSF shall explicitly deny information flow on the basis of [None].

Identification and Certification

FIA_AFL.1 Processing of certification failure

Class relationship: None

Subordinate relationship: FIA_UAU.1 Certification

FIA_AFL.1.1 TSF shall, in the event of occurrence of certification attempts that have failed *3 times (within 1 minute)* in relations to [certification attempt of administrator], detect such.

FIA_AFL.1.2 If the failed certification attempt reaches or exceeds the defined number, then TSF shall perform the [following countermeasure action list].

[

- Notify (alarm window (standard value), alarm mail) to the authorized administrator (super administrator account))
- Closure of account

]

FIA_ATD.1(1) Define user property (1)

Class relationship: None

Subordinate relationship: None

FIA_ATD.1.1 TSF shall maintain the following security property list that belongs to each **authorized administrator**:

[

- List of security property: administrator ID, password

]

Precautions at the time of application: Authorized administrator includes installer,

super administrator, administrator, and monitor account.

FIA_ATD.1(2) Define user property (2)

Class relationship: None

Subordinate relationship: None

FIA_ATD.1.1 TSF shall maintain the following list of security properties that belongs to each **external IT entity**:

[

- List of security properties: Client IP

]

FIA_UAU.2 User certification prior to all actions

Class relationship: FIA_UAU.1

Subordinate relationship: FIA_UID.1 Identification

FIA_UAU.2.1 TSF, on behalf of the **authorized administrator,** must successfully certify the **authorized administrator** prior to allowing all actions that TSF mediates.

FIA_UAU.7 Certification feedback protection

Class relationship: None

Subordinate relationship: FIA_UAU.1 Certification

FIA_UAU.7.1 TSF, during processing of certification, shall only provide [‘*’ at the time of password input] to the **authorized administrator**.

FIA_UID.2(1) Identification of user prior to all actions (1)

Class relationship: FIA_UID.1 Identification

Subordinate relationship: None

FIA_UID.2.1 TSF, on behalf of the user, shall successfully identify each **authorized administrator** prior to allowing all actions mediated by TSF.

Precautions at the time of application: User of TOE is categorized into administrator and external IT entity, and this component requires identification of administrator.

FIA_UID.2(2) Identification of user prior to all actions (2)

Class relationship: FIA_UID.1 Identification
Subordinate relationship: None

FIA_UID.2.1 TSF, on behalf of the user, shall successfully identify each **external IT entity** prior to allowing all actions mediated by TSF.

Precautions at the time of application: User of TOE is categorized into administrator and external IT entity, and this component requires identification of external IT entity.

Security Management

FMT_MOF.1(1) Management of security function (1)

Class relationship: None
Subordinate relationship: FMT_SMF.1 Specification of management function
FMT_SMR.1 Security role

- FMT_MOF.1.1 TSF, for the function of [addition of super administrator account], shall limit the ability to *decide action* by the [authorized administrator (installer account)].

FMT_MOF.1(2) Management of security function (2)

Class relationship: None
Subordinate relationship: FMT_SMF.1 Specification of management function
FMT_SMR.1 Security role

- FMT_MOF.1.1 TSF shall, for the functions of the [following functions], limit the ability to *decide, stop, commence and change actions* by the [authorized administrator (super administrator account)].
  [
  - User management
  - Change code

- Agent management
- Management of basic setting
- Management of flawlessness
- Management of audit storage space
- Log back-up
- Management of key contents
- Management of access interception IP
- Management of setting of White URL
- Management of cookie hidden field
- Management of service domain
- Management of basic information
- Management of Trust IP
- Management of upload file
- Management of unfiltered file
- Real-time log view
- Log search
- Log statistics
- Setting of screen lock-up

]

FMT_MOF.1(3) Management of security function (3)

Class relationship: None

Subordinate relationship: FMT_SMF.1 Specification of management function
FMT_SMR.1 Security role

- FMT_MOF.1.1 TSF shall, for the functions of the [following functions], limit the ability to *decide, stop, commence and change actions* by the [authorized administrator (administrator account)].

  [

  - Change code
  - Management of key contents
  - Management of access interception IP
  - Management of setting of White URL
  - Management of cookie hidden field
  - Management of service domain
  - Management of basic information

- Management of Trust IP
- Management of upload file
- Management of unfiltered file
- Real-time log view
- Log search
- Log statistics
- Setting of screen lock-up

]

FMT_MOF.1(4) Management of security function (4)

Class relationship: None

Subordinate relationship: FMT_SMF.1 Specification of management function

FMT_SMR.1 Security role

- FMT_MOF.1.1 TSF shall, for the functions of the [following functions], limit the ability to *decide, stop and commence actions* by the [authorized administrator (monitor account)].

[

- Change of code
- Real-time log view
- Log search
- Log statistics
- Setting of screen lock-up

]

FMT_MSA.1 Management of security properties

Class relationship: None

Subordinate relationship: FDP_IFC.1 Controal of partial information flow

FMT_SMF.1 Specification of management function

FMT_SMR.1 Security role

FMT_MSA.1.1 TSF shall enforce the [information flow allowance and interception policy] in order to limit the ability to *change fundamental value, change, question, delete and [generate]* the properties of security illustrated in the [following Table 5.3] by the [authorized administrator(super administrator, administrator account)].

Table 5.3 Properties of security

Security properties	Computation	Authorized administrator
Access denial IP	Access denial IP address (registration, deletion)	Super administrator, administrator
White URL	White URL condition (generation, deletion)	Super administrator, administrator
Trust IP	Trust IP (generation, deletion)	Super administrator, administrator
Service domain	Additional domain (addition, deletion)	Super administrator, administrator
Parameter allowance rule	Parameter information (generation, change, deletion)	Super administrator, administrator
Name and value of cookie/hidden field	Name of cookie/hidden field (generation, deletion)	Super administrator, administrator
Upload allowance /interception file	Name of expander allowed or denied for uploading (generation, deletion)	Super administrator, administrator
Rule	Rule for each type of attack (to be examined, not to be examined)	Super administrator, administrator
DOS	Setting of critical value of DOS (change the value of fundamental value)	Super administrator, administrator
DDOS	Setting of critical value of DDOS (change the value of fundamental value)	Super administrator, administrator
User defined Rule	User defined Rule (addition, change, deletion)	Super administrator, administrator
Unfiltered file	Expander of file that is designated as trusted URL at all times (addition, deletion)	Super administrator, administrator

FMT_MSA.3 Initialization of static property

Class relationship: None
Subordinate relationship: FMT_MSA.1 Management of security property
FMT_SMR.1 Security role

FMT_MSA.3.1 TSF shall enforce the [information flow allowance and interception policy] in order to provide *limited* default value of the security property used in enforcing SFP.

FMT_MSA.3.2 TSF shall enable [authorized administrator (super administrator, administrator account)] to specify selectable initialization value in order to replace fundamental value at the time of generation of object or information.

FMT_MTD.1(1) Management of TSF data (1)

Class relationship: None
Subordinate relationship: FMT_SMR.1 Security role
FMT_SMF.1 Specification of management function

FMT_MTD.1.1 TSF shall limit the ability to [back-up] [audit data] to [authorized administrator (super administrator account)].

FMT_MTD.1(2) Management of TSF data (2)

Class relationship: None
Subordinate relationship: FMT_SMR.1 Security role
FMT_SMF.1 Specification of management function

FMT_MTD.1.1 TSF shall limit the ability to *change value of default, question, change, delete and [generate]* [basic setting information, Agent registration information, user information, flawlessness examination setting information, audit storage space management information, and NTP setting information] to [authorized administrator (super administrator account)].

FMT_MTD.1(3) Management of TSF data (3)

Class relationship: None

Subordinate relationship: FMT_SMR.1 Security role

FMT_SMF.1 Specification of management function

FMT_MTD.1.1 TSF shall limit the ability to *change value of default, question, change, delete and [generate]* [basic Agent information, White URL information, contents information, service domain information, Trust IP information, access denied IP information, cookie/hidden field information, upload file information, unfiltered file information] to [authorized administrator (super administrator, administrator account)].

FMT_MTD.1(4) Management of TSF data (4)

Class relationship: None

Subordinate relationship: FMT_SMR.1 Security role

FMT_SMF.1 Specification of management function

FMT_MTD.1.1 TSF shall limit the ability to *change* [user code which is the data for identification and certification, session closure time-out time] to [authorized administrator(super administrator, administrator, and monitor account)].

FMT_ MTD.2(1) Management of limit of TSF data (1)

Class relationship: None

Subordinate relationship: FMT_MTD.1 TSF Data management,

FMT_SMR.1 Security role

FMT_MTD.2.1 TSF shall limit the specification of limit on [session closure time-out time] to [authorized administrator (super administrator, administrator, and monitor account)].

FMT_MTD.2.2 TSF shall execute [storage of audit record and session closure] when the TSF data reaches or exceeds the designated limit.

FMT_ MTD.2(2) Management of limit of TSF data (2)

Class relationship: None

Subordinate relationship: FMT_MTD.1 TSF Data management,

FMT_SMR.1 Security role

FMT_MTD.2.1 TSF shall limit the specification of limit on [capacity of audit storage space] to [authorized administrator (super administrator account)].

FMT_MTD.2.2 TSF shall execute [countermeasure actions specified in FAU_STG.3.1, FAU_STG.4.1] when the TSF data reaches or exceeds the designated limit.

FMT_SMF.1 Specification of management function

Class relationship: None

Subordinate relationship: None

FMT_SMF.1.1 TSF must be able to execute the following security management functions:

[

- Management of security properties (list specified in FMT_MSA.1)
- Management of TSF data (list specified in FMT_MTD.1)
- Management of security function (list specified in FMT_MOF.1)

]

FMT_SMR.1 Security role

Class relationship: None

Subordinate relationship: FIA_UID.1 Identification

FMT_SMR.1.1 TSF must maintain the role of [following authorized administrator].

[

- Installer account
- Super administrator account
- Administrator account
- Monitor account

]

FMT_SMR.1.2 TSF must be able to associate the role with **authorized administrator**.

Precautions at the time of application: Authorized administrators to be maintained is categorized into installer, super administrator, administrator, and monitor account in accordance with the authority given.

- Installer account: It is an account that is automatically generated at the time of installation of Master Server. It can generate super administrator account and is automatically deleted once the super administrator account is generated and logged in.

- Super administrator account: Has the highest authority and is able to set all security policies of agents registered in the Master Server.
- Administrator account: It is an administrator added by the super administrator account, and can control the agents designated by the super administrator account.
- Monitor account: It is an administrator added by the super administrator account, which cannot set security policies. It is an administrator only with authority to read.

TSF protection

FPT_AMT.1 Abstract machine test

Class relationship: None

Subordinate relationship: None

FPT_ATM.1.1 TSF, in order to illustrate that the security presumptions related to TSF lower portion abstract machine is accurately operating, shall execute a series of testing at the time of *initial start-up*.

FPT_FLS.1　Maintenance of secured status at the time of disability

Class relationship: None

Subordinate relationship: ADV_SPM.1 Non-standardized TOE security policy model

FPT_FLS.1.1 TSF, in the event of occurrence of the following types of disability, shall maintain secured status:

[

- Disability of TSF service daemon
- Communication disability between physically segregated TOEs
- Flawlessness error of TSF data

]

FPT_TST.1　TSF Self test

Class relationship: None

Subordinate relationship: FPT_AMT.1　Abstract machine test

FPT_TST.1.1 TSF, in order to verify accurate operation of *TSF*, shall conduct self testing at the time of *start-up and during regular operation, periodically*.

FPT_TST.1.2 TSF shall provide function that verifies the flawlessness of *[security policy file, system operation setting file, security policy TABLE file]*는 among the stored *[TSF data]* to the authorized user.

FPT_TST.1.3 TSF shall provide function that verifies the flawlessness of stored TSF execution code to the authorized user.

Accessing TOE

FTA_SSL.1 Session closure by TSF

Class relationship: None
Subordinate relationship: FIA_UAU.1 Certification

FTA_SSL.1.1 TSF shall close the mutually acting session after [non-active period of authorized administrator: 60~99999 seconds (basic value 600 seconds)] in accordance with the following method.

a) Erase or overwriting the screen indication apparatus to disallow other from viewing the current content.

b) Incapacitation of all actions of accessing the data/screen indication apparatus of the **authorized administrator** rather than cancelling closure of session.

FTA_SSL.1.2 TSF shall request [recertification of administrator] prior to cancelling closure of session.

SOF Declaration

Strength of function required by this Security Target is medium level, and the security function requirement FIA_UAU.2 satisfies the security strength of function SOF-medium required by the Common Criteria for Information Security, v2.3.

TOE Assurance Requirement

Assurance requirements of this Security Target are composed of assurance components of the Part 3 of Common Criteria, with assurance level of EAL4. The following table illustrates the summary of the assurance components.

Table 5.4 TOE Assurance Requirements

Assurance Class	Assurance Components	
Configuration management	ACM_AUT.1	Partial automation of configuration management
	ACM_CAP.4	Generation support and accommodation procedure
	ACM_SCP.2	Scope of problem tracing configuration management
Distribution and operation	ADO_DEL.2	Detection of changes
	ADO_IGS.1	Installation, generation, start-up procedure
Development	ADV_FSP.2	Completely defined external interface
	ADV_HLD.2	Fundamental design that segregated security function and non-security function
	ADV_IMP.1	Expression of realization of portion of TSF
	ADV_LLD.1	Descriptive detailed design
	ADV_RCR.1	Verification of non-standardized alignment
	ADV_SPM.1	Non-standardized TOE security policy model
Manual	AGD_ADM.1	Administrator manual
	AGD_USR.1	User manual
Support for life cycle	ALC_DVS.1	Identification of security countermeasure
	ALC_LCD.1	Life cycle model defined by the developer
	ALC_TAT.1	Well-defined development tool
Testing	ATE_COV.2	Analysis of scope of test
	ATE_DPT.1	Fundamental design test
	ATE_FUN.1	Functional test
	ATE_IND.2	Independent test: specimen test
Evaluation of vulnerability	AVA_MSU.2	Verification of analysis of manual
	AVA_SOF.1	Evaluation on the strength of function of TOE security
	AVA_VLA.2	Analysis of independent vulnerability

Configuration Management

ACM_AUT.1 Partial automation of configuration management

Subordinate relationship:

ACM_CAP.3 Certification control

Requirements of Developer

ACM_AUT.1.1D Developer must use configuration management system.

ACM_AUT.1.2D Developer shall provide configuration management plan.

Evidence Requirements

ACM_AUT.1.1C Configuration management system shall provide means of automation that enables only the authorized changes to be generated in the expression of realization of TOE.

ACM_AUT.1.2C Configuration management system shall provided automated means of supporting TOE generation.

ACM_AUT.1.3C Configuration management plan shall describe method of using automated tools in the configuration management system.

ACM_AUT.1.4C Configuration management plan shall describe the method of using automated tools in the configuration management system.

Requirements of Evaluator

ACM_AUT.1.1E Evaluator shall confirm that the information provided satisfies all the Evidence Requirements.

ACM_CAP.4 Generation support and accommodation procedure

Subordinate relationship:

ALC_DVS.1 Identification of security measures

Developer Requirements

ACM_CAP.4.1D Developer shall provide references on TOE.

ACM_CAP.4.2D Developer shall use configuration management system.

ACM_CAP.4.3D Developer shall provide configuration management documents.

Evidence Requirements

ACM_CAP.4.1C References on TOE must be unique for each version of TOE.

ACM_CAP.4.2C Label for references on TOE must be attached.

ACM_CAP.4.3C Configuration list must uniquely identify all configuration items that composes TOE.

ACM_CAP.4.4C Configuration management documents shall include configuration list, configuration management plan, and accommodation plans.

ACM_CAP.4.5C Configuration management list shall describe the configuration items that compose the TOE.

ACM_CAP.4.6C Configuration management document shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.7C Configuration management system shall identify all configurations uniquely.

ACM_CAP.4.8C Configuration management plan shall describe the method of using configuration management system.

ACM_CAP.4.9C Evidence must prove that configuration management system is being operated in accordance with configuration management plan.

ACM_CAP.4.10C Configuration management document shall provide evidence that all configuration items are effectively managed and is being managed in the configuration management system.

ACM_CAP.4.11C Configuration management system must provide means of allowing only the changes that are authorized for the configuration list.

ACM_CAP.4.12C Configuration management system shall support generation of TOE.

ACM_CAP.4.13C Accommodation plan must describe the procedures used in accommodating changed or newly generated configuration items as a portion of TOE.

Requirements of Evaluator

ACM_CAP.4.1E Evaluator shall confirm that information provided satisfy all the Evidence Requirements.

ACM_SCP.2 Scope of problem tracing configuration management

Subordinate relationship:

ACM_CAP.3 Control of certification

Requirements of Developer

ACM_SCP.2.1D Developer shall provide configuration item list on TOE.

Evidence Requirements

ACM_SCP.2.1C Configuration item list shall include expression of realization, defectiveness in security and evaluation evidences required by the assurance component of Security Target.

Requirements of Evaluator

ACM_SCP.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

Distribution and operation

ADO_DEL.2 Detection of changes

Subordinate relationship:

ACM_CAP.3 Control of certification

Requirements of Developer

ADO_DEL.2.1D Developer shall document the procedure of distributing TOE or portion of TOE to user.

ADO_DEL.2.2D Developer shall use distribution procedure.

Evidence Requirements

ADO_DEL.2.1C Distributed document must describe all procedures necessary in maintenance of security at the time of distribution of TOE to user.

ADO_DEL.2.2C Distributed document must describe diverse range of procedures and technical methods for detecting changes and non-alignment between the original cope of the developer and version executed by the user.

ADO_DEL.2.3C Distributed document must describe diverse range of procedures for detection of distribution attempt under the disguise as developer even if the developer has not sent anything to the user.

Requirements of Evaluator

ADO_DEL.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADO_IGS.1 Installation, generation, start-up procedure

Subordinate relationship:

AGD_ADM.1 Administrator manual

Requirements of Developer

ADO_IGS.1.1D Developer shall document the procedures necessa4ry in secured installation, generation and start-up of TOE.

Evidence Requirements

ADO_IGS.1.1C Document must describe phases necessary in secured installation, generation and start-up of TOE.

Requirements of Evaluator

ADO_IGS.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADO_IGS.1.2E Evaluator must determine whether the TOE is securely composed in accordance with installation, generation and start-up procedure.

Development

ADV_FSP.2 Completely defined external interface

Subordinate relationship:

ADV_RCR.1 Verification of non-standardized accordance

Requirements of Developer

ADV_FSP.2.1D Developer shall provide functional specifications.

Evidence Requirements

ADV_FSP.2.1C Functional specification shall describe the TSF and TSF external interface in non-standardized format.

ADV_FSP.2.2C Functional specification must have internal accordance.

ADV_FSP.2.3C Functional specification must describe purpose and method of usage of all TSF external interface, and appropriate provide detailed items on all effects, exceptions, and error messages.

ADV_FSP.2.4C Functional specification shall completely express TSF.

ADV_FSP.2.5C Functional specification manual shall include theoretical basis for complete expression of TSF.

Requirements of Evaluator

ADV_FSP.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADV_FSP.2.2E Evaluator shall determine whether the functional specification has accurately and completely realized the TOE security functional requirements.

ADV_HLD.2 Fundamental design that segregated security function and non-security function

Subordinate relationship:

ADV_FSP.1 Non-standardized functional specification

ADV_RCR.1 Verification of non-standardized accordance

Requirements of Developer

ADV_HLD.2.1D Developer shall provide basic design of TSF.

Evidence Requirements

ADV_HLD.2.1C Basic design must be expressed in non-standardized format.

ADV_HLD.2.2C Basic design must have internal accordance.

ADV_HLD.2.3C Basic design shall describe the structure of TSF as sub-systems.

ADV_HLD.2.4C Basic design shall describe security functionality provided by each sub-system of TSF.

ADV_HLD.2.5C Basic design shall identify lower portion hardware, firmware and software required by the TSF by expressing the functions provided by the supplementary protection mechanism realized in lower portion hardware, firmware and software.

ADV_HLD.2.6C Basic design shall identify all interfaces of TSF sub-system.

ADV_HLD.2.7C Basic design shall identify external interface of TSF sub-system.

ADV_HLD.2.8C Basic design shall describe the purpose and method of usage of all interfaces of sub-system of TSF by providing, appropriately, detailed items on effect, exceptions and error messages.

ADV_HLD.2.9C Basic design shall describe TOE by distinguishing it as TSP-execution sub-system and other sub-systems.

Requirements of Evaluator

ADV_HLD.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADV_HLD.1.2E Evaluator shall determine whether the basic design accurately and securely realizes the TOE security function requirements.

ADV_IMP.1 Expression of realization of portion of TSF

Subordinate relationship:

ADV_LLD.1 Descriptive detailed design

ADV_RCR.1 Verification of non-standardized accordance

ADV_TAT.1 Well-defined development tool

Requirements of Developer

ADV_IMP.1.1D Developer shall provide expression of realization on selected TSF.

Evidence Requirements

ADV_IMP.2.1C Expression of realization shall define the TSF, without being vague, in detail that enables generation of TSF without further design procedure.

ADV_IMP.2.2C Specification of non-standardized function must have internal accordance.

Requirements of Evaluator

ADV_IMP.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADV_IMP.2.2E Evaluator shall determine whether the expression of realization accurately and securely realizes the TOE security function requirements.

ADV_LLD.1 Descriptive detailed design

Subordinate relationship:

ADV_HLD.2 Basic design that segregates security function and non-security function

ADV_RCR.1 Verification of non-standardized accordance

Requirements of Developer

ADV_LLD.1.1D Developer shall provide detailed design of TSF.

Evidence Requirements

ADV_LLD.1.1C Detailed design shall be expressed in non-standardized format.

ADV_LLD.1.2C Detailed design shall have internal accordance.

ADV_LLD.1.3C Detailed design shall describe TSF as module.

ADV_LLD.1.4C Detailed design shall describe purpose of each module.

ADV_LLD.1.5C Detailed design shall define the mutual relationship between the modules as security functionalities provided and subordinate relationship between other modules.

ADV_LLD.1.6C Detailed design shall describe method of provision of each TSP-execution function

ADV_LLD.1.7C Detailed design shall identify all interfaces of TSF module.

ADV_LLD.1.8C Detailed design shall identify external interface of TSF module.

ADV_LLD.1.9C Detailed design shall describe purpose and method of usage of all interfaces on the TSF module by appropriately providing details on effect, exception and error messages.

ADV_LLD.1.10C Detailed design shall describe TOE by categorizing it into TSP-execution module and other modules.

Requirements of Evaluator

ADV_LLD.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADV_LLD.1.2E Evaluator shall determine whether the detailed design accurately and securely realizes the TOE security function requirements.

ADV_RCR.1 Verification of non-standardized alignment

Subordinate relationship: None

Requirements of Developer

ADV_RCR.1.1D Developer shall provide analysis of accordance between expressions all neighboring TSF provided.

Evidence Requirements

ADV_RCR.1.1C With regards to the analysis of expressions each neighboring TSF provided, it must be verifies that the all relevant security functionality of more abstract TSF expression is more accurately and completely detailed in more specific TSF expression.

Requirements of Evaluator

ADV_RCR.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ADV_SPM.1 Non-standardized TOE security policy model

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

Requirements of Developer

ADV_SPM.1.1D Developer shall provide TSP model.

ADV_SPM.1.2D Developer shall verify the accordance between functional specification and TSP model.

Evidence Requirements

ADV_SPM.1.1C TSP model must be non-standardized.

ADV_SPM.1.2C TSP model shall describe rules and characteristics of all policies of TSP that can be modeled.

ADV_SPM.1.3C TSP model shall include theoretical basis that illustrates accordance and completeness of all policies of TSP that can be modeled.

ADV_SPM.1.4C In the event of illustration of accordance between TSP model and functional specification, it must be verified that the all security functions specified in the functional specification is in accordance with and complete for the TSP model.

Requirements of Evaluator

ADV_SPM.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

Manual

AGD_ADM.1 Administrator manual

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

Requirements of Developer

AGD_ADM.1.1D Developer shall provide Administrator manual for the personnel who manage the system.

Evidence Requirements

AGD_ADM.1.1C Administrator manual shall describe management function and interface that can be used by TOE administrator.

AGD_ADM.1.2C Administrator manual shall describe method of managing TOE in secured method.

AGD_ADM.1.3C Administrator manual shall include caution on the functions and special authority that need to be controlled in secured processing environment.

AGD_ADM.1.4C Administrator manual shall describe all presumptions on user actions related to secured operation of TOE.

AGD_ADM.1.5C Administrator manual shall describe all security medium variables under the control of administrator by indicating secured value appropriately.

AGD_ADM.1.6C Administrator manual shall describe each type of security related cases on management functions that must be carried out including changes in the actual security properties under the control of TSF.

AGD_ADM.1.7C Administrator manual shall have accordance with all other documents submitted for evaluation.

AGD_ADM.1.8C Administrator manual shall describe all security requirements of IT environment regarding administrator.

Requirements of Evaluator

AGD_ADM.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

AGD_USR.1 User manual

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

Requirements of Developer

AGD_USR.1.1D Developer shall provide User manual

Evidence Requirements

AGD_USR.1.1C User manual shall describe functions and interface that can be used by TOE users other than administrator.

AGD_USR.1.2C User manual shall describe usage of TOE security functions that can used by user.

AGD_USR.1.3C User manual shall include caution on function and special authority that can be used by user to be controlled in secured processing environment.

AGD_USR.1.4C User manual shall clearly indicate all responsibilities of user necessary in secured operation of TOE including responsibilities related to presumptions on actions of user under the TOE security environment.

AGD_USR.1.5C User manual shall have accordance with all other documents submitted for evaluation.

AGD_USR.1.6C User manual shall describe all security requirements under IT environment on user.

Requirements of Evaluator

AGD_USR.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

Support for life cycle

ALC_DVS.1 Identification of security countermeasure

Subordinate relationship: None

Requirements of Developer

ALC_DVS.1.1D Developer shall prepare development security document.

Evidence Requirements

ALC_DVS.1.1C Development security document shall describe all physical, procedural, personnel and other security measures necessary in protecting confidentiality and flawlessness of process of TOE design and realization within development environment.

ALC_DVS.1.2C Development security document shall provide evidence that such security measures are complied with during development and maintenance of TOE.

Requirements of Evaluator

ALC_DVS.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ALC_DVS.1.2E Evaluator shall confirm whether security measures are being applied.

ALC_LCD.1 Life cycle model defined by the developer

Subordinate relationship: None

Requirements of Developer

ALC_LCD.1.1D Developer shall establish life cycle model used in development and maintenance of TOE.

ALC_LCD.1.2D Developer shall provide document on definition of life cycle.

Evidence Requirements

ALC_LCD.1.1C Document on definition of life cycle shall describe model used in development and maintenance of TOE.

ALC_LCD.1.2C Life cycle model shall provide control necessary in development and maintenance of TOE.

Requirements of Evaluator

ALC_LCD.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ALC_TAT.1 Well-defined development tool

Subordinate relationship:

ADV_IMP.1 Expression of realization on portion of TSF

Requirements of Developer

ALC_TAT.1.1D Developer shall identify development tools used in TOE.

ALC_TAT.1.2D Developer shall document details of selections made in realization of development tool-subordinate selections.

Evidence Requirements

ALC_TAT.1.1C All development tools used in realization must have been well-defined.

ALC_TAT.1.2C Development tool documents must define the significance of all commands used in realization without being vague.

ALC_TAT.1.3C Development tool documents must define the significance of all realization-subordinate selection without being vague.

Requirements of Evaluator

ALC_TAT.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

Testing

ATE_COV.2 Analysis of scope of test

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

ATA_FUN.1 Functional test

Requirements of Developer

ATE_COV.2.1D Developer shall provide analysis of scope of test.

Evidence Requirements

ATE_COV.2.1C Analysis of scope of test shall verify the accordance between the test items identified in the test document and TSF describe in the functional specification.

ATE_COV.2.2C Analysis of scope of test shall verify that the TSF described in the functional specification and test items identified in the test document are in complete accordance.

Requirements of Evaluator

ATE_COV.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ATE_DPT.1 Fundamental design test

Subordinate relationship :

ADV_HLD.2 Basic design that segregates security function and non-security function

ADV_LLD.1 Descriptive detailed design

ATE_FUN.1 Functional test

Requirements of Developer

ATE_DPT.1.1D Developer shall provide analysis of detailed level of test.

Evidence Requirements

ATE_DPT.1.1C Analysis of detailed level of test shall verify that identified test items on the test document are sufficient to verify that TSF operates in accordance with the basic design.

Requirements of Evaluator

ATE_DPT.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ATE_FUN.1 Functional test

Subordinate relationship: None

Requirements of Developer

ATE_FUN.1.1D Developer shall document the outcome of test on TSF.

ATE_FUN.1.2D Developer shall provide test document.

Evidence Requirements

ATE_FUN.1.1C Test document shall be composed of test plan, explanation on test procedures, anticipated outcome and actual outcome of test.

ATE_FUN.1.2C Test plan shall identify the security function to be tested and describe the purpose of test to be executed.

ATE_FUN.1.3C Explanation on test procedures shall identify the test items to be executed and describe scenario for testing of each security function. Such scenario shall include sequential subordinate relationship on results of other test.

ATE_FUN.1.4C Anticipated outcome of test shall verity the result anticipated from the successful execution of the test.

ATE_FUN.1.5C Outcome of test executed by the developer shall verify that each security function being tested operates as per specification.

Requirements of Evaluator

ATE_FUN.1.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ATE_IND.2 Independent test: specimen test

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

AGD_ADM.1 Administrator manual

AGD_USR.1 User manual

ATE_FUN.1 Functional test

Requirements of Developer

ATE_IND.2.1D Developer shall provide TOE to be tested.

Evidence Requirements

ATE_IND.2.1C TOE must be appropriate for testing.

ATE_IND.2.2C Developer shall provide resources equivalent to the resources used in the TSF functional test of the developer.

Requirements of Evaluator

ATE_IND.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

ATE_IND.2.2E Evaluator shall appropriately test portion of TSF in order to verify that TOE operates in accordance with the specification.

ATE_IND.2.3E Evaluator shall execute specimen testing on the test items within the test documents in order to verify the outcome of test conducted by the developer.

Evaluation of Vulnerability

AVA_MSU.2 Verification of analysis of manual

Subordinate relationship:

ADO_IGS.1 Installation, generation and start-up procedure

ADV_FSP.1 Specification of non-standardized function

AGD_ADM.1 Administrator manual

AGD_USR.1 User manual

Requirements of Developer

AVA_MSU.2.1D Developer shall provide manual.

AVA_MSU.2.2D Developer shall document analysis of manual.

Evidence Requirements

AVA_MSU.2.1C Manual shall identify relevant issues for all possible operational mode of TOE, its effect and maintenance of secured operation (including operation following disability or operation following error in operation).

AVA_MSU.2.2C Manual must complete, clearly defined, coherent and appropriate.

AVA_MSU.2.3C Manual shall list all presumptions on intended environment.

AVA_MSU.2.4C Manual shall list all requirements on external security measures (including procedural, physical and personnel control of external aspect).

AVA_MSU.2.5C Document on analysis of manual shall verify that the manual is complete.

Requirements of Evaluator

AVA_MSU.2.1E Evaluator must confirm that information provided satisfy all the Evidence Requirements.

AVA_MSU.2.2E Evaluator shall, in order to confirm that the TOE is securely composed and used by using only the manual provided, shall repeat all composition and installation procedures, and selectively repeat other procedures.

AVA_MSU.2.3E Evaluator shall determine whether it is possible to detect all unsecured status by using manual.

AVA_MSU.2.4E Evaluator shall confirm whether the manual provides secured operation on all operational modes of TOE in the analysis document.

AVA_SOF.1 Evaluation on the strength of function of TOE security

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

ADV_HLD1 Descriptive detailed design

Requirements of Developer

AVA_SOF.1.1D Developer shall perform TOE security functional strength analysis for the each identified mechanism in the Security Target for which TOE security functional strength has been declared.

Evidence Requirements

AVA_SOF.1.1C TOE security functional strength analysis for each mechanism for which TOE security functional strength has been declared shall verify that the TOE security functional strength satisfy or exceeds the minimum functional strength level defined in the protection profile/Security Target.

AVA_SOF.1.2C TOE security functional strength analysis for each mechanism for which specific TOE security functional strength has been declared shall verify that the TOE security functional strength satisfy or exceeds the specific functional strength level defined in the protection profile/Security Target.

Requirements of Evaluator

AVA_SOF.1.1E Evaluator shall verify that information provided satisfies all Evidence Requirements.

AVA_SOF.1.2E Evaluator shall verify whether the functional strength declaration is accurate.

AVA_VLA.2 Analysis of independent vulnerability

Subordinate relationship:

ADV_FSP.1 Specification of non-standardized function

ADV_HLD.2 Fundamental design that segregated security function and non-security function

ADV_IMP.1 Expression of realization on portion of TSF

ADV_LLD.1 Descriptive detailed design

AGD_ADM.1 Administrator manual

AGD_USR.1 User manual

Requirements of Developer

AVA_VLA.2.1D Developer shall analyze and document TOE submission material in order to find the method of infringement of TSP by user.

AVA_VLA.2.2D Developer shall document the characteristics of identified vulnerability.

Evidence Requirements

AVA_VLA.2.1C Describe the analysis of TOE submission material executed in order to find the method of infringement of TSP by user of vulnerability analysis.

AVA_VLA.2.2C Vulnerability analysis document must list the identified vulnerabilities.

AVA_VLA.2.3C Vulnerability analysis document, for all identified vulnerabilities, must verify that the vulnerability cannot be abused in the intended environment of TOE.

AVA_VLA.2.4C Vulnerability analysis document must justify that TOE with the identified vulnerability has resistance against clearly defined intrusion attack.

Requirements of Evaluator

AVA_VLA.2.1E Evaluator shall verify that the information provided satisfy all the Evidence Requirements.

AVA_VLA.2.2E Evaluator shall perform intrusion testing based on vulnerability analysis of the developer in order to assure that identified vulnerability has been handled.

AVA_VLA.2.3E Evaluator shall perform independent vulnerability analysis.

AVA_VLA.2.4E Evaluator, in order to determine the possibility of abuse of additionally identified vulnerability in intended environment, shall perform independent intrusion test base on the independent vulnerability analysis.

AVA_VLA.2.5E Evaluator shall determine whether TOE has resistance against attack of attacker with low level of possibility of succeeding in attack.

Security Function Requirements on IT Environment

Table 5.5 Security Function Requirements on IT Environment

Security Function Class	Security Function Components	
Security audit	FAU_SAR.3	Selectable audit review
TSF protection	FPT_STM.1	Trusted time stamp
	FPT_ITT.1	Fundamental protection of internally transmitted TSF Data

Security Audit

FAU_SAR.3 Selectable audit review

Class relationship: None

Subordinate relationship: FAU_SAR.1 Audit review

FAU_SAR.3.1 **IT Environment**, on the basis of the [following standards], provides ability to *search and array* audit data.

[

- Identity of subject
- Identity of object
- Date of case
- Type of case
- Countermeasure action of case
- Outcome of case (success or failure)

]

TSF Protection

FPT_STM.1 Trusted time stamp

Class relationship: None

Subordinate relationship: None

FPT_STM.1.1 **IT Environment** must be able to provide trusted time stamp for usage by TSF.

FPT_ITT.1 Fundamental protection of internally transmitted TSF data

Class relationship: None

Subordinate relationship: None

FPT_ITT.1.1 **IT Environment** must protect the TSF data from exposure and changes at the time of transmission of TSF data between the segregated portion of TOE.

6 Specification of Summary of TOE

This chapter briefly and clearly describes how the security functions of TOE are realized. In addition, it explains how the supplementary requirements are satisfied.

TOE Security Function

Explanation on the TOE security function is composed of the methods through which the issues are satisfied in coping with each associated functional requirement. The security functional strength is required at the time of certification of administrator with the functional strength at medium and defined in TSF_FIA.1. Specification of summary of security function of TOE is as per the following table.

Security function of TOE is composed as follows.

- **Security audit**
  - TSF_FAU.1 Security alarm
  - TSF_FAU.2 Audit data record generation
  - TSF_FAU.3 Audit data inquiry
  - TSF_FAU.4 Examination of exceeding of the audit data storage limit
  - TSF_FAU.5 Processing at the time of saturation of audit data storage space

- **Protection of user data**
  - TSF_FDP.1 Control of information flow

- **Identification and Certification**
  - TSF_FIA.1 Identification and certification of administrator
  - TSF_FIA.2 Processing of certification failure
  - TSF_FIA.3 Identification of external IT entity

- **Security management**
  - TSF_FMT.1 User management
  - TSF_FMT.2 Basic system management
  - TSF_FMT.3 Management of Agent and security policy
  - TSF_FMT.4 Session management

- **TSF protection**
  - TSF_FPT.1 Abstract machine test
  - TSF_FPT.2 TSF Maintenance of secured status at the time of disability
  - TSF_FPT.3 TSF Self test and data flawlessness processing

- **TOE Access**
  - TSF_SSL.1 Session closure and cancellation

Table 6.1 Specification of summary of security function

Function	Identity No.	Contents
Security audit (TSF_FAU)	TSF_FAU.1	Security alarm
	TSF_FAU.2	Audit data record generation
	TSF_FAU.3	Audit data inquiry
	TSF_FAU.4	Examination of exceeding of the audit data storage limit
	TSF_FAU.5	Processing at the time of saturation of audit data storage space
Protection of user data (TSF_FDP)	TSF_FDP.1	Control of information flow
Identification and certification (TSF_FIA)	TSF_FIA.1	Identification and certification of administrator
	TSF_FIA.2	Processing of certification failure
	TSF_FIA.3	Processing of certification failure
Security management (TSF_FMT)	TSF_FMT.1	User management
	TSF_FMT.2	Basic system management
	TSF_FMT.3	Management of Agent and security policy
	TSF_FMT.4	Session management
TSF protection (TSF_FPT)	TSF_FPT.1	Abstract machine test
	TSF_FPT.2	TSF Maintenance of secured status at the time of disability
	TSF_FPT.3	TSF Self test and data flawlessness processing
TOE Access	TSF_SSL.1	Session closure and cancellation

Explanation of Summary of TOE Security Function

Security audit (TSF_FAU)

TSF_FAU.1 Security alarm

TSF, with regards to the authorized administrator account, shall generate security audit record log at the time of infringement of identification and certification policy more than the number defined, analyze such as security violation and as the countermeasure actions notify the alarm contents through alarm window (fundamental value), alarm mail such that the administrator can confirm the corresponding violation.

Abnormal status of web server, abnormal status of process, registration of access denial IP according to the accumulation of intrusion attempts, occurrence of DOS case, occurrence of DDOS case among the generated audit record log shall be analyzed and as countermeasure action against such happening, notify the alarm contents through alarm window (fundamental value), alarm mail such that the administrator can confirm the corresponding violation

Relevant SFR: **FAU_ARP. 1 Security alarm**
FAU_SAA.1 Analysis of potential violation

TSF_FAU.2 Audit data record generation

All audit record information generated in TOE are categorized into administrator access log, administrator work log, intrusion interception log, security function execution log, and exceeding of audit storage space log. Generate audit record by associating the associated user identity and case to be subjected to audit on all cases generated in TOE.
Audit record shall be generated in association with the authorized administrator.
Audit record information generated in TOE generates audit record on audit cases described in [Table 5-2] Cases to be subjected to audit on start-up and end of audit function and security target on security related functions.

Audit data record is generated for each module inside the segregated TOE. This information is conveyed to the Master Server on real-time through analysis procedure, and is stored in MySQL DB.

In order to synchronize the audit record information generated on the data conveyed on real-time, set IP of trusted NTP server in Master Server. IP information is conveyed to Agent and brings same time of NTP server at the time of installation for each system. Furthermore, it brings time of NTP server stored at 4 AM everyday during operation, to synchronize the time of all audit data record generated between segregated TOE.

Audit records generated in TOE are categorized into the following audit record types and the purposes that corresponds are as follows.

Table 6.2 Audit record for each type

Types of audit record	Purpose
Intrusion attempt log	Manages record on contents of execution of intrusion interception at the web service generated in the host to be subjected to management, analyses the web service intrusion actions generated in the corresponding host through log search for each security class, and used for the purpose of utilizing as the base material for setting of security policy
Work log	Manages record of accessing to Master Server through Admin Console by administrator, and record and security function execution log on details of security management activities performed by the administrator. It can be utilized as basic material for setting of administrator identification/certification policy or as evidence material for non-authorized attack on administrator's identification/certification, or as base material for setting of security policy by utilizing it in log search and search for each condition
Alarm message	Manages ending of process and error in flawlessness examination, record of DOS/DDOS/access interception IP/closure of account/contents alteration, and record on contents that exceeded at the time of examination of key audit storage space

Relevant SFR: **FAU_GEN.1 Generation of audit data**
FAU_GEN.2 Association with user identity

TSF_FAU.3 Audit data inquiry

Authorized administrator (super administrator, administrator, and monitor) of TOE searches and displays the audit data that is stored in the MySQL DB provided in the IT environment on the screen in accordance with the information format of audit record conditions for each type below. Searched data prevents the changes by the non-authorized account.

- Identity of subject
- Identity of object
- Date of case
- Type of case
- Countermeasure action of case

- Outcome of case (success or failure)

In particular, for the alarms generated in the property of administrator access log, intrusion interception log, and security function execution log, the authorized administrator can confirm the corresponding information on real-time through real-time log view.

Table 6.3 Information of condition of audit record for each type

Type of audit record	Contents of outcome of audit record
Intrusion interception log	Log identifier, Agent ID, Date of intrusion attempt, Domain, Intrusion attempt IP , URL, Intrusion type, No. of intrusion attempt, Countermeasure method, Detected item, Cookie
Work log	Log identifier, administrator identifier, date of work, contents of work, outcome, details of outcome
Alarm message	Log identifier, Date of audit, Outcome of audit

Relevant SFR: **FAU_SAR.1 Audit review**
FAU_SAR.3 Selectable audit review
FAU_STG.1 Audit evidence protection

TSF_FAU.4 Examination of exceeding of the audit data storage limit

TSF executes examination of the capacity of usage of corresponding file system at each designated time period (standard value of 5 minutes) during ordinary operation. TSF, in the event of the accumulated audit data evidence exceeding the storage limit (80~89%(standard value of 80%)), generates audit record and notifies the authorized administrator (alarm window (standard value), alarm main).

Relevant SFR: **FAU_STG.3 Countermeasure action in the event of anticipated loss of audit data**

TSF_FAU.5 Processing at the time of saturation of audit data storage space

In the event of saturation of audit data storage space (90~95%(standard value 90%)), notification is sent to the authorized administrator (alarm window(standard value), alarm mail) and the authorized administrator(super administrator) ceases all TSF Services with the exception of access, back-up and deletion.

Relevant SFR: **FAU_STG.4 Prevention of loss of audit data**

Protection of user data (TSF_FDP)

TSF_FDP.1 Control of information flow

TOE, in order to allow only the normal HTTP request, collects page information from the web server and domain, as well as route of domain (White URL collection), at the time of system installation. Once White URL is collected, security policy properties with allowance and interception tool are mapped for each corresponding page, thereby allowing normal access request but intercepting attack and request by that which is not registered in White URL.

TOE, on the basis of the While URL information so collected, provides the following functions for controlling of the information flow (allowance and interception policy).

No.	Function	Category
1	Set the quantity of information that can be accommodated for control of information flow by critical value for access (setting of number of processing per user per second (DOS), setting of number of processing per several user per second (DDOS), critical value (alarm, interception of session, interception of access)).	Access control by critical value for access
2	Prepare standard formal equation and field name on allowable name and value in order control information flow by validity of information or to verify validity	Access control by information validity
3	Reflect already defined rules on the OWASP vulnerability in order to control the information flow by Rule	Access control by Rule
4	Reflect rules for control of information flow by expander	Access control in accordance with expander
5	Reflect rule for control of information flow by control on access IP	Access control by control on access IP
6	Prepare detection pattern in order to control the information flow by user defined Rule	Access control by user defined rule

Countermeasure method for control of information flow by critical value for access is as follows.

- TSF sets the level of access (1 user access or number of processing of several user) for service denial attack (DOS) and dispersed service denial attack (DDOS), and intercepts access in the event of occurrence of access in excess of the inputted processing number, thereby not allowing acceptance of corresponding packet information. That is, if the number of service of subject IP reaches the DOS critical value, it is registered as corresponding DOS IP, and if the overall service number reaches the DDOS critical value, then it executes registration of occurrence of DDOS case. Furthermore, generation of audit record data and alarm message occurs and conveyed to the administrator. Registered DOS and DDOS are automatically cancelled after 10 minutes.
- TSF sets attack critical value (alarm, interception of session, interception of access) for general attack. If attack on alarm critical value occurs, alarm message is displayed through web page. If attack on session interception critical value occurs, it intercepts session of web page. If attack on access interception critical value occurs, it makes it impossible to receive services for normal assess to web page.

Countermeasure method for control of information flow by validity of information is as follows.

- TSF, in the event where the length of parameters of URL, among the URL of HTTP information requested by the subject, is smaller than the designated minimum length or longer than the designated maximum length, intercepts the information flow.
- TSF, in the event where the value of parameters of URL, among the URL of HTTP information requested by the subject, is contains text other than those included in the designated allowance rule, intercepts the information flow.
- TSF, in the event where the request method of designated URL, among the of HTTP information requested by the subject, is not the Method (GET, POST, HEAD, OPTIONS) that is not included in the designated Method, intercepts the information flow.
- TSF, in the event where the HTTP Version of HTTP information requested by the subject is not normal version (HTTP 0.9, HTTP 1.0, HTTP 1.1), intercepts the information flow.
- TSF, in the event where the Cookie of HTTP information being requested by the subject is Cookie generated by TOE, examines the corresponding Cookie and if alteration of Cookie value or Hidden value has occurred, intercepts the information flow.
- TSF changes the Server, x=powered-by among the Header information of Response Data of HTTP information requested by the subject into specific value.

- TSF intercepts information flow if the Status Code among the Header information of Response Data of HTTP information requested by the subject is erroneous (4XX, 5XX).

Countermeasure method of control of information flow by Rule is as follows.

- It can manage interception rule (policy focused on interception with policy of operating in accordance with operational mode [Detect/Protect]), detection record rule (policy of leaving only record following detection regardless of the operational mode [Detect/Protect]), alternation rule (policy related to data protection in the format of changing or coding portion in order to protect the user data which is key data [resident registration number, card number] that are sent out regardless of the operational mode [Detect/Protect]) in accordance with the properties of attack in order to control information flow of HTTP(S) Data on the basis of Rule, and can add “user rule” onto the rule to which user wishes to add.
- In order to control information flow of HTTP(S) Data, attacks on 10 vulnerabilities of OWASP are categorized as follows for countermeasures against such attack. Number of attack patterns currently held is 320.
  - HTTP(S) Request Data Examination Rule
    - Certification detour (interception)
    - Authorization detour (interception)
    - Session fixation (interception)
    - Cross site scripting (interception)
    - Insertion of command (interception)
    - Insertion of OS command (interception)
    - Insertion of SQL (interception)
    - Insertion of SSI (interception)
    - Buffer overflow (text) (interception)
    - Forced access into directory (interception)
    - Anticipated search of directory (interception)
    - Worm attack (interception)
    - Acquisition of Response Header Information (interception)
    - MassSQL Insertion(Interception)
    -
  - HTTP(S) Response Data Examination Rule
    - Inducement of functional error (interception)
    - Viewing directory information (interception)

- Random substitution (interception)
- Extraction of key information (change)

Countermeasure method of control of information flow by expander is as follows.

- Upload file: Enables uploading (allow or intercept) of file only for the registered expander by applying rules on expander of file that attempts to allow or intercept uploading.
- Unfiltered file: Enable allowing of file access only for the registered expander by applying rules on expander of file that will not be examined by White URL.

Countermeasure method of control of information flow by control on access IP is as follows.

- Allow access of IP registered as Trust IP.
- Intercept the access of IP registered as access denied IP.
- Disable access event for the normal service in the event of occurrence of attack on corresponding number in accordance with the set status in the critical value (access interception) by automatically registering in access denied IP.

Countermeasure method of control of information flow on specific value such as Overflow is as follows. In order to prevent the danger of generating overflow, in advance, for the arbitrarily large value by code that accepts input value of user that accesses web server, enable limitation on length value by registering the following items in the Rule.

- Request URL Length: Maximum length of URL that allows request (less than the maximum length value: allow, greater than the maximum length value: intercept) (standard value: 9kbytes)
- Request Query String Length: Maximum length of allowable Query (less than the maximum length value: allow, greater than the maximum length value: intercept) (standard value: 8kbytes)
- Request Query Argument name Length: Maximum length of allowable name of Query (less than the maximum length value: allow, greater than the maximum length value: intercept) (standard value: 1024bytes)
- Request Query Argument value length: Maximum length of allowable Query value (less than the maximum length value: allow, greater than the maximum length value: intercept)   (standard value: 8kbytes)
- Request Method: Method information of HTTP version used (designated method information: allow, non-designated method: intercept) (standard value: select all)
- Allowable HTTP Version: HTTP version information that can be used (Designated HTTP version information; allow, non-designated HTTP version information:

intercept)

Relevant SFR: **FDP_IFC.1(1) Control of partial information flow (1)**
FDP_IFC.1(2) Control of partial information flow (2)
FDP_IFF.1(1) Property of unified class security (1)
FDP_IFF.1(2) Property of unified class security (2)

Identification and Certification (TSF_FIA)

With regard to Identification and certification provided in TOE, action of user is performed prior to accessing of the security management interface by authorized administrator through Admin Console. Policy on identification and certification function of user must satisfy the functional strength requirement (functional strength – medium) targeted by TOE.

TSF_FIA.1 Identification and certification of administrator

TOE, in the event of accessing of Admin Console by authorized administrator (installer, super administrator, administrator, and monitor account) for the purpose of security management of TOE, allows access by administrator who is registered in the user management information.

In the case of administrator and monitor account, access to TOE is possible by identify the information on IP, ID, and Password. In the case of installer and super administrator account, access to TOE is possible by identifying information only on ID and Password. Here, the Password shall be coded by using SEED (128 Bit) block coding technique.

In the event of attempting access to TOE, ID and Password of user is verified for normal information. If the corresponding user input normal information, it is compared for accordance with the IP address into which the information on starting point IP address is stored. Even if normal ID and Password are entered, if the starting point IP address does not match with the previously registered IP address, log in attempt will be denied.

At the time of installation of Master Server, installer account referred to as ‘websray’ is generated as the initial account information, first access into Admin Console is made with this account. Since the installer account has only the authority to register the super administrator account, once the administrator with super administrator account is logged in, the installer account is automatically terminated. There are super administrator, administrator and monitor account that can operate security management by accessing TOE, and the categorization these administrators are as follows.

Table 6.4 Authority of authorized administrator

Categories	Explanation
Super administrator account	Administrator with authority to use all security function setting that TOE provides. Corresponding account is generated by the installer account.
Administrator account	Has authority to manage designated Agent and log view. Corresponding account is generated by the super administrator account.
Monitor account	Has authority to only view policy information and log information. Corresponding account is generated by the super administrator account.

TOE identifies, on behalf of the administrator, ID entered by authorized administrator (super administrator, administrator, monitor account) prior to execution of all actions mediated by TSF on the basis of administrator identity among the list of security properties of administrator table.
Furthermore, general password format is used as a means of certifying all administrators. This certification of administrator is made on the basis of the certification information among the security property list of authorized administrator. Disclosure of password is prevented by only providing the character "*" rather than ordinary text to the administrator during the process of certification.

General password certification mechanism executes certification with the following code combination rules.

- Password must be more than 6 characters and less than 15 characters.
- Text that can be used include "a-z(26), A-Z(26), 0-9(10), as well as specialized text ((! @ # $ % ^ & * ( ) _ + | ` - = \ { } : " < > ? [ ] ; ' , . / ").
- Combination rule must mixedly use alphabet and number or specialized text (alphabet+number or alphabet+specialized text).
- Repetition of text is allowed unto 3 characters.

Administrator password of administrator and monitor account, with the exception of installer and super administrator account, is automatically closed on the maturation date (1 month (standard value)) designated in advance by the administrator of super administrator account. Status information of 'Access Denied' will be displayed on the user management window of administrator of super administrator account and is audit recorded. In order for the corresponding administrator to normally log-in, administrator with super administrator account must cancel the maturation date for the code.

Relevant SFR: **FIA_ATD.1(1) Definition of user property (1)**
FIA_UAU.2 Certification of user prior to all actions

FIA_UAU.7 Protection of certification feed-back

FIA_UID.2(1) Identification of user prior to all actions (1)

TSF_FIA.2 Processing of certification failure

TOE detects occurrence of more than 3 continuous failures in 1 minute in certification on single user account in a specific terminal unit. In the event of having detected certification failure in excess of the critical value, it terminates administrator console and performs account closure and report (alarm window(standard value), alarm mail), which are designated countermeasure actions.

Relevant SFR: **FIA_AFL.1 Processing of failure in certification**

TSF_FIA.3 Identification of external IT entity

TOE identifies external IT entity by using client IP among the information of HTTP(S) Data that is conveyed at the time of requesting from the external IT entity (client) to web server, and determines the level of countermeasure action including denial/alarm/interception of session/access interception by comparing the accumulated number of intrusion attempt of the corresponding IP with the critical value..

Relevant SFR: **FIA_ATD.1(2) Definition of user property (2)**

FIA_UID.2(2) Identification of user prior to all actions (2)

Security management (TSF_FMT)

Security management for TOE is accomplished through security management program referred to as Admin Console. Authorized administrator (super administrator, administrator, and monitor) manages the security function after having logged in the server through normal access, and manages TSF data. Functions being managed are as follows.

TSF_FMT.1 User management

User management performs addition, correction and deletion on the following functions.

Menu	Contents	Authorized administrator

User management	Account management	Management of super administrator, administrator, and monitor account . Setting of certification on all account . Countermeasure actions on setting of account maturity	Installer, super administrator
	Change of password	Change password of logged in administrator	Super administrator, administrator. monitor

In order to access the TOE, it is possible to access with authority of administrator of installer, super administrator, administrator, and monitor account. Access can be made through Window security management program referred to as Admin Console.

Installer account among the authorized administrators generates the super administrator and is deleted when super administrator account is logged in.

Super administrator account among the authorized administrators can add, correct and delete administrator and monitor account. At the time of adding user account, password that has been randomly generated is transmitted to the mail address of the corresponding administrator. Administrator and monitor account can access the security management program by using the randomly conveyed password, and can change the random or currently used password.

In the event of certification attempt number reaching or exceeding the designated limit value, account closure is executed through notification (alarm window (standard value), alarm mail) to authorized administrator (super administrator) or designated countermeasure actions.

Relevant SFR: **FMT_SMF.1 Specification of management function**
FMT_MOF.1(1) Management of security function (1)
FMT_MOF.1(2) Management of security function (2)
FMT_MOF.1(3) Management of security function (3)
FMT_MOF.1(4) Management of security function (4)
FMT_SMR.1 Security role
FMT_MTD.1(2) Management of TSF data (2)
FMT_MTD.1(4) Management of TSF data (4)

TSF_FMT.2 Basic system management

Basic system management can add, correct and delete the following functions.

Menu		Contents	Authorized administrator
Basic System Management	Setting of NTP	Setting of NTP IP address for temporal synchronization between segregated TOEs	Super administrator
	Log back-up and deletion	Administrator directly performs back-up and deletion rather than automatic back-up in order to efficiently manage the audit storage space.	Super administrator
	Agent management	Registration and deletion of information of Agents connected to Master Server	Super administrator
	Management of basic setting	. Verify the status information on current Master Server . Manage presence of usage of SMTP . Management of critical value	Super administrator
	Management of flawlessness	Management of execution code of Master Server, Agent, and Admin Console, corresponding contents on various security policies, and setting of period of flawlessness' examination of property information	Super administrator
	Management of audit storage space	Setting of period of examination of audit storage space of Master Server and setting of countermeasure actions on anticipated loss of audit data	Super administrator

Basic system management supports function of registering and deleting setting information for management of Master Server (NTP setting, back-up and deletion of log, management of basic setting, management of flawlessness, management of audit storage space) and Agent. Fundamentally, only the authorized administrator with super administrator account can manage the information on basis system management.

(Setting of NTP) TOE provides function that sets time of TOE. Fundamentally, TOE brings time from trusted NTP server and synchronizes time among the segregated TOEs. Time is designated by bringing time from NTP server at the time of installation of each system, and synchronization is achieved by brining time from NTP server at 4AM everyday.

(Back-up and deletion of Log) TOE provides function that enables back-up and deletion of log in the storage space of TOE. Fundamentally, TOE re-operates the system after having secured audit storage space by suing this function when the audit storage space is saturated. It can execute back-up and deletion by selecting the target of log back-up and log is backed-up into designated location.

(Management of Agent) Authorized administrator granted with authority to manage Agent can manage security policy by registering the corresponding Agent. During operation of security management program, agent can be registered immediately by transmitting agent registration message. Furthermore, agent can be deleted after having terminated the Agent.

(Management of Basic Setting) TOE can confirm information on system, license and allowed number of Agents of the Master Server, and enable registration of presence of usage of SMTP of alarm mail used in TOE and information on critical value number (alarm/session interception/access interception).

(Management of Flawlessness) TOE provides flawlessness function to Master Server by monitoring falsification/alteration of file by unauthorized user of Master Server. Flawlessness examination maintains SHA-256 hash value on corresponding contents and property information for execution code of TSF and various security policies, and executes flawlessness' examination at every designated period during ordinary operation. Flawlessness can be set for each period (in the unit of month, week, day), and in the event of occurrence of flawlessness error, enables conveyance of corresponding event to administrator through alarm window and alarm mail by setting the countermeasure action. Administrator, upon execution of verification of flawlessness error of TSF data, can restore to previous data or reset the hash value on the corresponding data through Admin Console.

(Management of audit storage space) TOE protects the stored audit record by preventing unauthorized deletion and changes on the Master Server. For this purpose, examination of quantity of usage of corresponding file system is executed for every designated period during ordinary operation. TSF, in the event of audit evidence exceeding the designated limit (standard value 80%), enables the corresponding event to be conveyed to the administrator through alarm window, alarm mail as designated report, and such designated report is performed in the event of saturation of the audit storage space (more than 90%). Here, TSF, in the event of saturation of audit storage space, prevents security audit record and stops execution of all functions of TSF with the exception of back-up/deletion executed by super administrator.

Relevant SFR: **FMT_SMF.1 Specification of management function**
FMT_MOF.1 (2) Management of security function (2)
FMT_MTD.1 (1) Management of TSF data (1)
FMT_MTD.1 (2) Management of TSF data (2)
FMT_MTD.2 (2) Management of limit value of TSF data (2)

TSF_FMT.3 Management of Agent and security policy

Agent and security policy management performs addition, correction and deletion on the following function.

Menu			Contents	Authorized administrator
Management of Agent and security policy	Setting of operation mode		Change status of operational mode of TOE (Protect, Detect, Disable)	Super administrator, administrator
	Basic information management		Change fundamental information of Agent	Super administrator, administrator
	Setting of policies	Management of access interception IP	Management of IP for which access to web service in which security policies are being operated is intercepted	Super administrator, administrator
		Setting of White URL	Collection of key pages of web server to be protected and reflect policy rule on the corresponding page	Super administrator, administrator

		Management of Cookie and hidden field	Registration of cookie/hidden list that can be used in White URL	Super administrator, administrator
		Management of upload file	Setting of access control policy on upload allowed file and upload intercepted file	Super administrator, administrator
		Management of service domain	Setting of policy on access control on additionally used domain	Super administrator, administrator
		Management of Trust IP	Setting of access control policy through registration and deletion of Trust IP	Super administrator, administrator
		Rule Setting	Setting whether or not attack type rule's application for OWASP access control item	Super administrator, administrator
		User defined rule	Registering rule that user for OWASP access control item defines access control policy	Super administrator, administrator
		Managemenent of unfilitered file	Even if do not inspection, access control policy sets for file that do not filtering to define to confidence URL	Super administrator, administrator
		Setting of critical value for access	Access control policy setting through input critical value of D/DOS	Super administrator, administrator

Several web servers can be operated on a system in which a single Agent is installed operated. Therefore, it is possible to control security policy on corresponding web service by registering one Agent and registering several web service on the Agent. Corresponding access control policy enables only the authorized administrator with super administrator or administrator account to control access.

(Setting of operational mode) Operation on TOE is accomplished by 3 types of mode. There are disable mode, detect mode and protect mode. The disable mode is the mode being operated when log cannot be received normally or when uploading policy, and is the same as the status in which TOE is not installed. Detect mode is the mode used when applying test and rule prior to operation in protect mode. It is a mode which detects infringement and executes audit record by enforcing control on information flow, it cannot intercept access. In protect mode, equipment normally provides security management function service, and intercepts session and access in the event of intrusion attempt with the control on information flow enforced.

(Basic information management) It can inquire fundamental information on each Agent, and can correct name of host, host IP, type and version of OS, type and version of web server.

(Setting of policy)

Setting of SFP on security property where web service is accomplished. Limited standard value is provided in order to enforce corresponding SFP and the following menu is provided in order to apply information flow allowance and interception policy.

- **Management of access interception IP:** It is possible to inquire and delete information of IP which has been intercepted due to exceeding of critical number (time of occurrence of interception, time of termination of interception), and the administrator can directly register/delete the IP to be intercepted.
- **Setting of White URL:** TOE, for security policy of each Agent, provides security management function that registers the URL information of web server that protects TOE to White URL. TOE can collect White URL for each service which is provided for each web server, and can register URL information to be protected by registering White URL by designating directory to be collected in order to apply rules for each White URL. It also provides function of registering security policy issues to be reflected for each page of collected White URL.
- **Management of Cookie/Hidden Field:** By enabling usage of value of key cookie/hidden field that are transferred through web site in White URL by registering them, enable audit to be performed on the value of cookie/hidden field that is falsified or altered.
- **Management of upload file:** TOE, for the security policies on each Agent, enables selective allowance of files registered by user accessing the web server. For such purpose, it enables selective loading of upload file that are registered in specific notice board, and provides functions on allowed file in order to reduce the load of TOE or those that are independent of the specific environment among the files registered in the web server. It provides function of registering expander who can change the rule on White

URL collected in the case of file to which access interception rule is applied.

- **Management of service domain:** TOE, for the security policies on each Agent, enables selective allowance of domain accessing by users who accesses web server. For this purpose, function of adding/deleting additional domain is provided.
- **Management of Trust IP:** TOE, for the security policies on each Agent, registers trust IP. In the case of Trust IP, by allowing access on IP registered to reduce the inconvenience of developers or administrator in their usage, enable them to be free of control by rule that has been registered earlier.
- **Rule setting:** TOE, for the security policies on each Agent, supports function that can set whether to apply the Rule in accordance with the attack type for each White URL.
- **User defined Rule:** TOE, for the security policies on each Agent, supports function that can register/correct/delete user defined Rule**.**
- **Management of unfiltered file:** TOE, for the security policies on each Agent, enables user accessing web server to selectively allow accessing files. It provides functions on allowed file in order to reduce the load of TOE or those that are independent of the specific environment among the files registered in the web server.
- **Setting of critical value for access:** TOE, for the security policies on each Agent, sets critical value for specific attacks that accesses TOE and if it reaches the corresponding critical value, displays outcome value in accordance with the conditions. It can set critical value on DOS/DDOS. This, with regards to the critical value for DOS/DDOS, provides function of setting critical value on the interval of second.

Relevant SFR: **FMT_SMF.1 Specification of management function**
FMT_MOF.1 (2) Management of security function (2)
FMT_MOF.1 (3) Management of security function (3)
FMT_MSA.1 Management of security property
FMT_MSA.3 Initialization of static property
FMT_MTD.1(3) Management of TSF data (3)

TSF_FMT.4 Session management

Session management adds, corrects and deletes the following functions.

Menu		Contents	Authorized administrator
Session management	Setting of screen closure	Security closure on non-usage of screen of Admin Console	Super administrator, administrator,

			monitor

Relevant SFR: **FMT_SMF.1 Specification of management function**
FMT_MOF.1(2) Management of security function (2)
FMT_MOF.1(3) Management of security function (3)
FMT_MOF.1(4) Management of security function (4)
FMT_MTD.1(4) Management of TSF data (4)
FMT_ MTD.2(1) Management of limit value for TSF data (1)

TSF protection (TSF_FPT)

TSF_FPT.1 Abstract machine test

Agent, at the initial start-up, tests whether the web server is operating normally in order to prove that web service is operated normally. Furthermore, at the time of initial start-up of the Agent, it confirms license and license key is coded by suing SEED(128 Bit) block coding technique.

If disability occurs in web server, it is reported to authorized administrator through alarm window(standard value) and alarm mail, and enables status of web server to be reported.

Relevant SFR: **FPT_AMT.1 Testing of abstract machine**

TSF_FPT.2 TSF Maintenance of secured status at the time of disability

TOE, in the event of disability of TSF service daemon, communication disability, and flawlessness error in TSF data, in order to maintain secured status, verifies the status of normal service of TOE at every 30 second interval. In the event of occurrence of error and disability of TSF, it detects such as performs designated report. Furthermore, in the event of occurrence of disability of TSF service daemon (Dispatcher, Emanager, LogManager, etc), it enables maintenance of secured status by restarting the corresponding daemon.

Relevant SFR: **FPT_FLS.1 Maintenance of secured status during disability**

TSF_FPT.3 TSF Self-test and data flawlessness processing

TOE, in order to verify that TSF is operating normally, performs self-testing of TSF at the time of start-up and at regular interval during regular operation.

It performs flawlessness examination at every designated period (standard value of 5 minutes) during ordinary operation by maintaining SHA-256 hash value on security policy TABLE file, TSF execution code and security policy file of TOE and system activation file. In the event of occurrence of flawlessness error, it notifies alarm contents to enable administrator to verify the corresponding infringement if the administrator has designated alarm window<standard value>, and alarm mail as countermeasure action.

In the event of occurrence of error on flawlessness, security alarm content is conveyed to the authorized administrator in accordance with set countermeasure action information, and the administrator, after having performed confirmation of flawlessness error through outcome view, can reset the hash value on the corresponding data by suing hash value reapplication button.

Relevant SFR: **FPT_TST.1 TSF Self-test**

TOE Access (TSF_SSL)

TSF_SSL.1 Session closure and cancellation

TOE provides security management interface that can set the session through setting of screen closure time. Screen closure time outputs session closure display if there are no actions for designated time period (standard value of 10 minutes). It intercepts all access on TOE which outputs session closure display. Re-certification of authorized administrator is necessary to cancel session closure.

Relevant SFR: **FTA_SSL .1 Session closure by TSF**

Assurance Methods

This clause describes the assurance methods of TOE. Assurance methods are the methods utilized to satisfy the assurance requirements and are illustrate in the following table 6.5

Table 6. 5 Assurance method

Assurance Class	Assurance Component	Assurance Method
Configuration Management	ACM_AUT.1 Automation of partial configuration management	WEBS-RAY V2.5 Configuration Management Document
	ACM_CAP.4 Generation support and accommodation procedure	
	ACM_SCP.2 Scope of problem tracing and configuration management	
Distribution and Operation	ADO_DEL.2 Detection of changes	WEBS-RAY V2.5 Distribution Document
	ADO_IGS.1 Procedures of installation, generation and start-up	WEBS-RAY V2.5 Installation Guideline
Development	ADV_FSP.2 Completely defined external interface	WEBS-RAY V2.5 Functional Specification
	ADV_HLD.2 Basic design that segregated security function and non-security function	WEBS-RAY V2.5 Basic Design
	ADV_IMP.1 Expression of realization on TSF	WEBS-RAY V2.5 Realization Verification Specification
	ADV_LLD.1 Descriptive detailed design	WEBS-RAY V2.5 Detailed Design
	ADV_RCR.1 Verification of non-standardized accordance	WEBS-RAY V2.5 Functional Specification WEBS-RAY V2.5 Basic Design WEBS-RAY V2.5 Detailed Design WEBS-RAY V2.5 Realization Verification Specification
	ADV_SPM .1 Non-standardized TOE security policy model	WEBS-RAY V2.5 security Policy Model
Manual	AGD_ADM.1 Administrator manual	WEBS-RAY V2.5 Administrator manual
	AGD_USR.1 User manual	N/A
Support Life Cycle	ALC_DVS.1 Identification of security countermeasure	WEBS-RAY V2.5 Life Cycle Support
	ALC_LCD.1 Developer defined life cycle model	
	ALC_TAT.1 Well-defined development tool	
Testing	ATE_COV.2 Analysis of scope of testing	WEBS-RAY V2.5 Testing Manual
	ATE_DPT.1 Testing of basic design	
	ATE_FUN.1 Functional test	
	ATE_IND.2 Independent test: specimen test	
Evaluation of Vulnerability	AVA_MSU.2 Verification of analysis of manual	WEBS-RAY V2.5 Abuse Analysis
	AVA_SOF.1 Evaluation of functional strength of TOE security	WEBS-RAY V2.5 Vulnerability Analysis
	AVA_VLA.2 Analysis of independent vulnerability	

Assurance component on configuration management ACM_AUT.1 automation of partial configuration management ACM_CAP.4 support for generation and accommodation procedures, ACM_SCP.2 and scope of problem tracing and configuration management is assured by the WEBS-RAY V2.5 configuration management document.

Detection of change of ADO_DEL.2 of distribution and operation class is assured by the WEBS-RAY V2.5 distribution document, and procedures of installation, generation and start-up of ADO_IGS.1 is assured by WEBS-RAY V2.5 Installation guideline

Under the development class, ADV_FSP.2 Completely defined external interface is assured by WEBS-RAY V2.5 Functional specification, ADV_HLD.2 basic design that segregated security function and non-security function is assured by WEBS-RAY V2.5 basic design manual, ADV_IMP.1 expression on realization of TSF is assured by WEBS-RAY V2.5 specification of realization verification, ADV_LLD.1 descriptive detailed design is assured by WEBS-RAY V2.5 detailed design manual, ADV_RCR.1 verification of non-standardized accordance is assured by WEBS-RAY V2.5 Basic design manual, WEBS-RAY V2.5 Detailed design manual, WEBS-RAY V2.5 Functional specification and WEBS-RAY V2.5 specification of realization verification. Furthermore, ADV_SPM.1 Non-standardized policy model for TOE security is assured by the WEBS-RAY V2.5 Security policy model manual.

Under the manual class, AGD_ADM.1 Administrator manual is assured through WEBS-RAY V2.5 Administrator manual and AGD_USR.1 User manual is not applied since user other than the administrator has not be distinguished.

Under the life cycle class, ALC_DVS.1 Identification of security countermeasure, ALC_LCD.1 Developer defined life cycle model and ALC_TAT.1 well-defined development tools are assured through WEBS-RAY V2.5 Life cycle support manual.

Under the test class, ATE_COV.2 analysis of scope of test, ATE_DPT.1 testing of basic design, ATE_FUN.1 functional test, ATE_IND.2 independent testing: specimen test are assured through WEBS-RAY V2.5 test manual.

Under the vulnerability analysis class, AVA_MSU.2 Verification of analysis of manual is assured through WEBS-RAY V2.5 abuse analysis manual while the other aspects, namely, AVA_SOF.1 TOE Evaluation on functional strength of security and AVA_VLA.2 analysis of independent vulnerability are assured through WEBS-RAY V2.5 Vulnerability analysis manual.

7 Theoretical Basis

This Chapter describes theoretical basis of security requirements that satisfies defined security target and security target on the basis of security environment (threat, presumptions, security policy of organization). Theoretical basis proves that TOE provides efficient IT security countermeasure within TOE security environment.

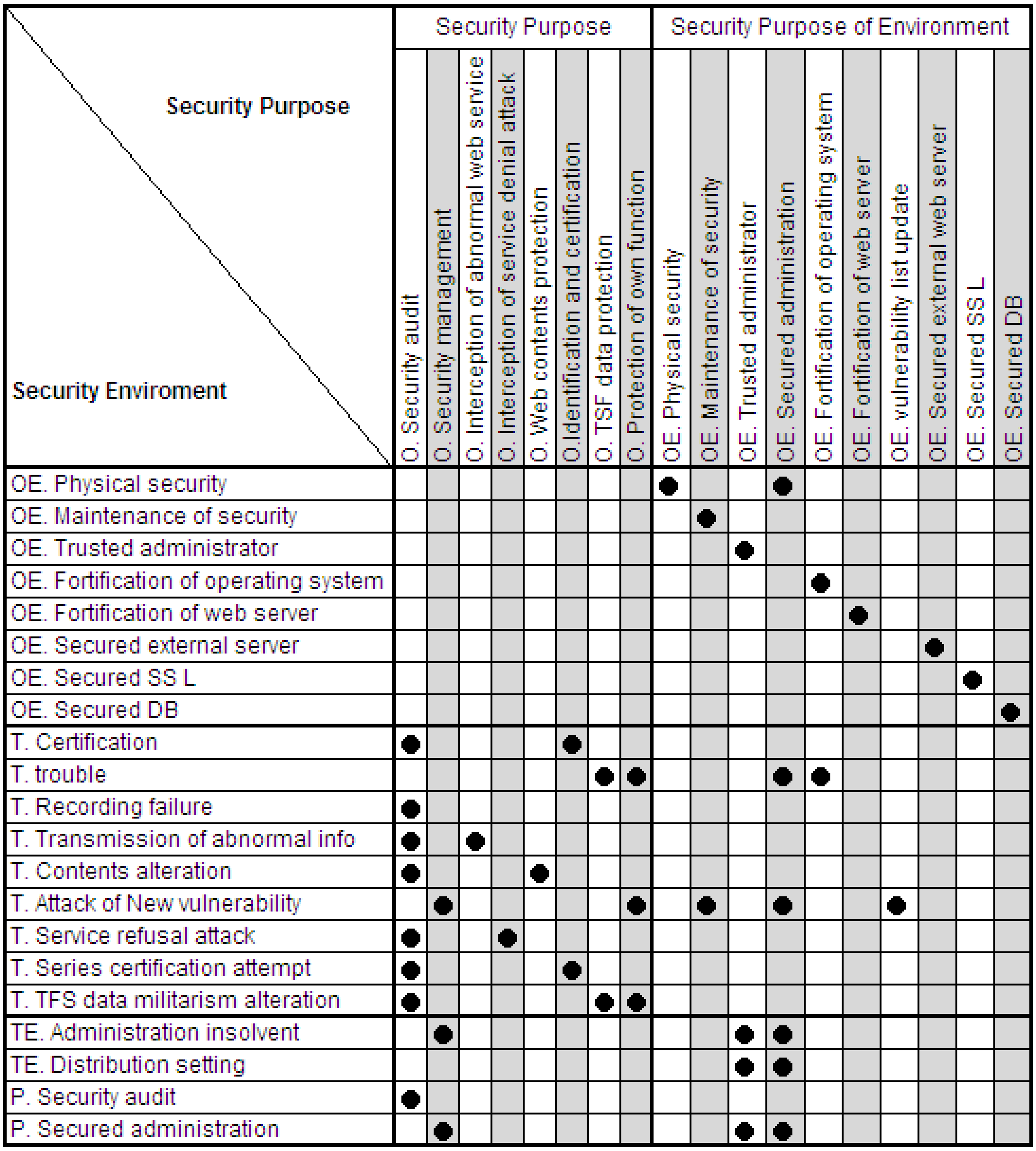
Theoretical Basis for the Security Target

Theoretical basis of security target proves that it is appropriate for the specified security target, sufficient to handle security issues, is not excessive and is essential.

Theoretical basis of the security target proves the following.

- Each presumption, threat and security policy of organization are handled by at least by single security target.
- Each security target handles at least one presumption, threat and security policy of organization. The following table explains the correspondence relationship between security environment and security target.

Table 7.1 Correspondence between security environment and security target



Security Purpose / Security Enviroment	Security Purpose								Security Purpose of Environment									
	O. Security audit	O. Security management	O. Interception of abnormal web service	O. Interception of service denial attack	O. Web contents protection	O.Identification and certification	O. TSF data protection	O. Protection of own function	OE. Physical security	OE. Maintenance of security	OE. Trusted administrator	OE. Secured administration	OE. Fortification of operating system	OE. Fortification of web server	OE. vulnerability list update	OE. Secured external web server	OE. Secured SS L	OE. Secured DB
OE. Physical security									●			●						
OE. Maintenance of security										●								
OE. Trusted administrator											●							
OE. Fortification of operating system													●					
OE. Fortification of web server														●				
OE. Secured external server																●		
OE. Secured SS L																	●	
OE. Secured DB																		●
T. Certification	●					●												
T. trouble							●	●				●	●					
T. Recording failure	●																	
T. Transmission of abnormal info	●		●															
T. Contents alteration	●				●													
T. Attack of New vulnerability		●						●		●		●			●			
T. Service refusal attack	●			●														
T. Series certification attempt	●					●												
T. TFS data militarism alteration	●						●	●										
TE. Administration insolvent		●									●	●						
TE. Distribution setting											●	●						
P. Security audit	●																	
P. Secured administration		●									●	●						

Theoretical basis for TOE security target

O. Security audit

This TOE security target assures that TOE provides means of recording, maintaining, and reviewing security related cases in detail and accurately. That is, TOE, when the audit record storage space is saturated, provides stoppage of TSF service and countermeasure methods, and enables tracking of the attacks that hinders normal service of web server by using audit record.

Therefore, this security target is necessary in coping with threat T.presumption, T.record failure, T.abnormal information transmission, T.service denial attack, T.continuous certification attempt, T.TSF change of data without authorization and to support the security policy of organization P. security audit.

O. Security management

TOE controls illegal access to internal network by setting rules on control of information flow in order to execute security policy. For this purpose, TOE must provides means of securely managing TSF data and TOE including generation and management of TOE composition data, management of latest vulnerability signature.

Therefore, since this security target provides means of safely managing the TOE by the authorized administrator, it is necessary in coping with threat on operating environment T. attack on new vulnerability, TE. Unreliable management, and to support security policy of organization P. secured management.

O. TSF data protection

TSF data may be altered in situation where administrator is not aware of due to unexpected attack from outside or due to occurrence of defectiveness in TOE thereby disabling the security policy to be executed properly. As such, by examining intentional and unintentional changes of TSF data by Toe in order to assure that TSF functions normally by assuring flawlessness of TSF data.

Therefore this security target is necessary in coping with threats T.DEFECTIVENESS, and T.CHANGE OF TSF DATA WITHOUT AUTHORITY.

O. Interception of abnormal web service

Intercepts the situation where abnormal HTTP(S) Data is generated and serviced due to packet not appropriate or packet with abnormal information for the HTTP protocol among the HTTP(S) Data entering from outside into TOE.

Therefore this security target copes with threat T.ABNORMAL INFORMATION TRANSMISSION.

O. Interception of service denial attack

Attacker may perform service denial attack with the internal web server as the target by passing the TOE. Representative web service denial attack is to consume system resources by making abnormally large amount of service requests to the internal web server by the remote user. Here, the internal computer allocates large amount of resources to the attacker, preventing the normal user from receiving web service. In coping with such situation, TOE intercepts exclusive usage of the specified computer resources by specific user in order to assure that normal user can use the web service normally.

Therefore, this security target of TOE copes with T.SERVICE DENIAL ATTACK.

O. Identification and certification

TOE security target assures that TOE identifies and certifies authorized administrator and external IT entity registered in TOE. Authorized administrator grants responsibility on all functions that the administrator activates. As such identification function is essential. It is an essential function since the external IT entity (web server) is registered in TOE and is able to generate audit record and categorize service requests that come through this. Certification is a requirement for authorized administrator, and it is necessary for secured management of TOE by identifying the user accessing with authorized account.

Therefore, this security target copes with Threat T.Disguise and T.Continuous certification attempt attack.

O. Protection of own function

TOE provides self protection function in order to protect TOE itself on the changes that are generated at initial start-up and during operation as well as for the vulnerability that are newly discovered.

Therefore, this security target copes with Threats T.DEFECTIVENESS, T. Attack on new vulnerability, and T.Change of TSF data without authority.

Theoretical basis of security target on environment

OE. Physical security

This security target on environment assures that only the administrator authorized by TOE can access and is located in physically secured environment.

Therefore, this security target on environment copes with Presumptions A.physical security.

OE. Maintenance of security

This security target on environment assures that it maintains security at level same as before by immediately reflecting the changed environment and security policy onto TOE operating policy in the event of changes in internal network environment due to changes in internal network composition, increase in host, increase in service.

Therefore, this security target on environment supports Presumptions A.Maintenance of security and copes with Threat T.Attack on new vulnerability.

OE. Trusted administrator

This security target on environment assures that administrator authorized by TOE can be trusted and is able to securely manage TOE.

Therefore, this security target on environment supports Presumption A.Trusted administrator and copes with Threats TE. Unreliable management and TE.Distribution installation, as well as supports security policy of organization P.Secured management.

OE. Secured management

This security target on environment assures that TOE is distributed and installed in secured methods, and is composed, managed and used in secured method by authorized administrator.

Therefore, this security target on environment supports Presumption A.physical security, copes with Threats T.DEFECTIVENESS, T.Attack on new vulnerability, TE.Unreliable management, and TE.Distribution installation, and supports Security policy P.Secured management.

OE. Fortification of operating system

This security target on environment assures that the operating system is secured and trusted by performing removal of services and means not necessary for operating system and fortifying vulnerabilities in operating system by TOE.

Therefore, this security target on environment supports Presumptions A.Fortification of operating system and copes with Threat T.DEFECTIVENESS.

OE. Fortification of web server

This security target on environment assures that web server is secured and trustable by performing fortification on vulnerability by removing unnecessary program or module and installing version with bug removed on the web server.

Therefore, this security target on environment supports Presumptions A.Fortification of web server.

OE. Renewal of list of vulnerability

This security target on environment assures that TOE renews and manages rule on vulnerability that TOE is managing in order to protect the new vulnerability of TOE and web server that TOE is protecting from the external attack using such new vulnerability.

Therefore,. Security target for this environment is copes with threat T. threat of new vulnerability.

OE. Secured external server

This security target on environment assures that the NTP server located in external aspect is secured in order to maintain trusted time of TOE.

Therefore, Security target for this environment is copes with presumption A. secured external server.

OE. Secured SSL

This security target on environment assures the SSL function in order to protect the TSF data mutually transmitted between the segregated TOEs by forming secured communication channel between segregated TOEs within TOE.

Therefore, Security target for this environment is copes with presumption A. secured SSLB.

OE. Secured DB

This security target on environment assures secured storage of audit data generated by TOE.

Therefore, Security target for this environment is copes with presumption A. secured DB.

Theoretical Basis of Security Requirements

Theoretical basis of security requirements must prove that the IT security requirements described are appropriate to satisfy the security target and is appropriate in handling the security issues as the result.

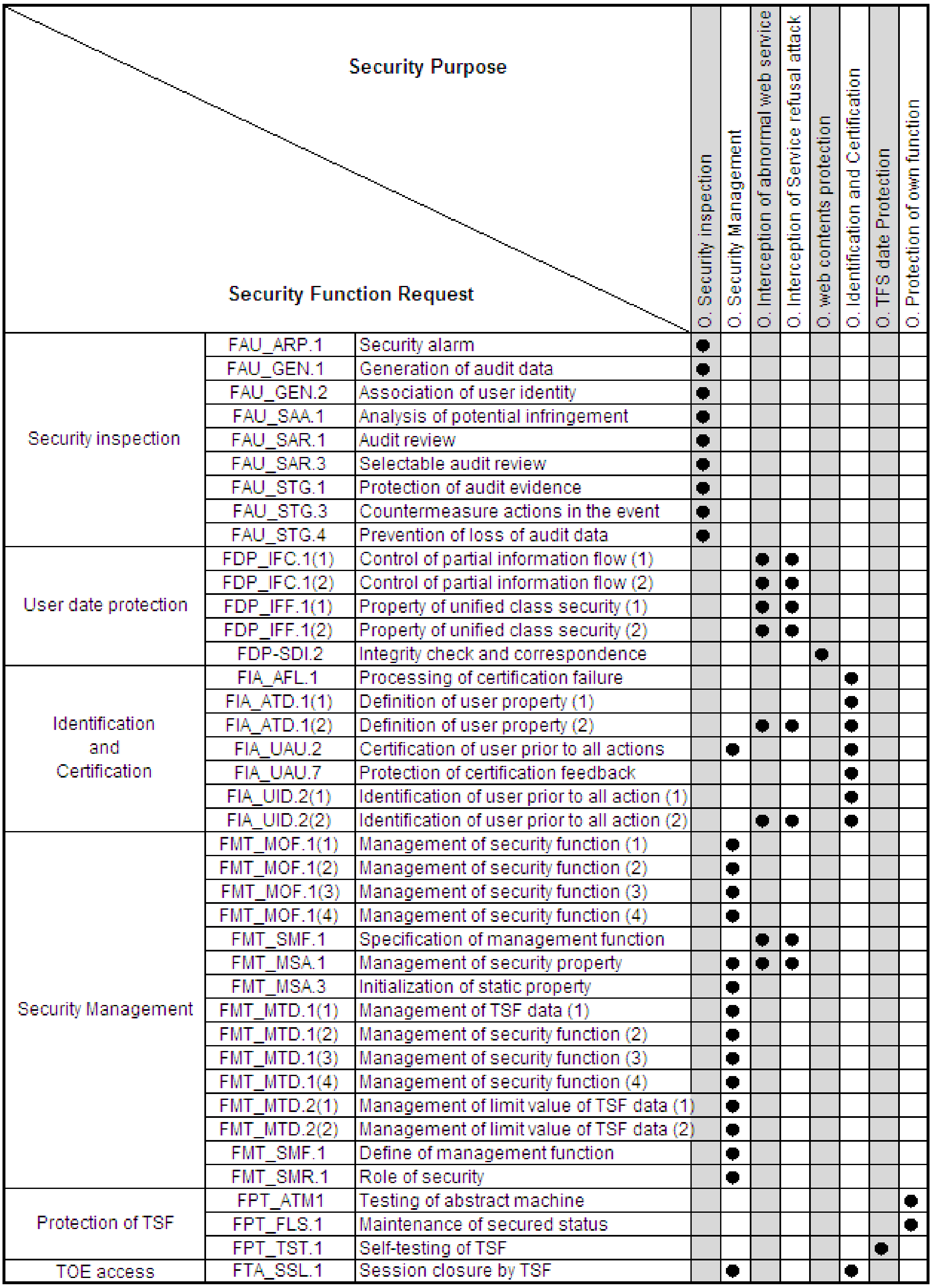
Theoretical Basis for TOE Security Function Requirements

Theoretical basis for TOE security function requirements prove the following.

- Each TOE security target is being handled by at least one TOE security function requirement.
- Each TOE security function requirement handles at least one TOE security target.

- Integratingly prepared on the security requirements in accordance with IT environment.

Table 7.2 Correspondence between security target and security function requirement



Security Purpose Security Function Request			O. Security inspection	O. Security Management	O. Interception of abnormal web service	O. Interception of Service refusal attack	O. web contents protection	O. Identification and Certification	O. TFS date Protection	O. Protection of own function
Security inspection	FAU_ARP.1	Security alarm	●							
	FAU_GEN.1	Generation of audit data	●							
	FAU_GEN.2	Association of user identity	●							
	FAU_SAA.1	Analysis of potential infringement	●							
	FAU_SAR.1	Audit review	●							
	FAU_SAR.3	Selectable audit review	●							
	FAU_STG.1	Protection of audit evidence	●							
	FAU_STG.3	Countermeasure actions in the event	●							
	FAU_STG.4	Prevention of loss of audit data	●							
User date protection	FDP_IFC.1(1)	Control of partial information flow (1)			●	●				
	FDP_IFC.1(2)	Control of partial information flow (2)			●	●				
	FDP_IFF.1(1)	Property of unified class security (1)			●	●				
	FDP_IFF.1(2)	Property of unified class security (2)			●	●				
	FDP-SDI.2	Integrity check and correspondence					●			
Identification and Certification	FIA_AFL.1	Processing of certification failure						●		
	FIA_ATD.1(1)	Definition of user property (1)						●		
	FIA_ATD.1(2)	Definition of user property (2)			●	●		●		
	FIA_UAU.2	Certification of user prior to all actions		●				●		
	FIA_UAU.7	Protection of certification feedback						●		
	FIA_UID.2(1)	Identification of user prior to all action (1)						●		
	FIA_UID.2(2)	Identification of user prior to all action (2)			●	●		●		
Security Management	FMT_MOF.1(1)	Management of security function (1)		●						
	FMT_MOF.1(2)	Management of security function (2)		●						
	FMT_MOF.1(3)	Management of security function (3)		●						
	FMT_MOF.1(4)	Management of security function (4)		●						
	FMT_SMF.1	Specification of management function			●	●				
	FMT_MSA.1	Management of security property		●	●	●				
	FMT_MSA.3	Initialization of static property		●						
	FMT_MTD.1(1)	Management of TSF data (1)		●						
	FMT_MTD.1(2)	Management of security function (2)		●						
	FMT_MTD.1(3)	Management of security function (3)		●						
	FMT_MTD.1(4)	Management of security function (4)		●						
	FMT_MTD.2(1)	Management of limit value of TSF data (1)		●						
	FMT_MTD.2(2)	Management of limit value of TSF data (2)		●						
	FMT_SMF.1	Define of management function		●						
	FMT_SMR.1	Role of security		●						
Protection of TSF	FPT_ATM1	Testing of abstract machine								●
	FPT_FLS.1	Maintenance of secured status								●
	FPT_TST.1	Self-testing of TSF							●	
TOE access	FTA_SSL.1	Session closure by TSF		●				●		

FAU_ARP.1 Security alarm

This component assures ability to take countermeasure actions in the event of detecting security infringement. As such, it satisfies the TOE Security Target O.Security audit.

FAU_GEN.1 Generation of audit data

This component assures ability to define case to be subjected to audit and generation of audit record. As such, it satisfies the TOE Security Target O.Security audit.

FAU_GEN.2 Association of user identity

This component assures ability to associate the user who generated the case and subject of audit. As such, it satisfies the TOE Security Target O.Security audit.

FAU_SAA.1 Analysis of potential infringement

This component assures ability to point out security infringement by examining audited case. As such, it satisfies the TOE Security Target O.Security audit.

FAU_SAR.1 Audit review

This component assures ability of the authorized administrator to review audit record. As such, it satisfies the TOE Security Target O.Security audit.

FAU_SAR.3 Selectable audit review

This component assures ability to search and array audit data in accordance with standard with logic relationship. As such, it satisfies the TOE Security Target O.Security audit.

FAU_STG.1 Protection of audit evidence

This component assures ability to protect the audit record from changes and deletion that are not authorized. As such, it satisfies the TOE Security Target O.Security audit.

FAU_STG.3 Countermeasure actions in the event of anticipated loss of audit data

This component assures ability to take countermeasure actions in the event the audit evidence exceeds the predetermined limit. As such, it satisfies the TOE Security Target O.Security audit.

FAU_STG.4 Prevention of loss of audit data

This component assures ability to take countermeasure actions in the event the audit storage space is saturated. As such, it satisfies the TOE Security Target O.Security audit.

FDP_IFC.1(1) Control of partial information flow (1)

This component assures that security policy by control (allowance) of information flow of TOE is defined and that scope of security policy is defined. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack.

FDP_IFC.1(2) Control of partial information flow (2)

This component assures that security policy by control (allowance) of information flow of TOE is defined and that scope of security policy is defined. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack.

FDP_IFF.1(1) Property of unified class security (1)

This component describes countermeasure (allowance) function on explicit attack. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack.

FDP_IFF.1(2) Property of unified class security (2)

This component describes countermeasure (denial) function on explicit attack. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack.

FIA_AFL.1 Processing of certification failure

Since this component defines the number of failure in certification attempt of authorized administrator and assures that the ability to take countermeasure actions if the number reaches or exceeds the defined number, it satisfies the TOE Security Target O.Identification and certification.

FIA_ATD.1(1) Definition of user property (1)

This component is an item that requests identification on administrator. As such, it satisfies the TOE Security Target O.Identification and certification.

FIA_ATD.1(2) Definition of user property (2)

This component is an item that requests identification on external IT entity. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack, O.Identification and certification.

FIA_UAU.2 Certification of user prior to all actions

This component assures ability to successfully certify the user. As such, it satisfies the TOE Security Target O.Security management, O.Identification and certification.

FIA_UAU.7 Protection of certification feedback

This component assures that only the designated certification feedback is provided to the user during progress of certification. As such, it satisfies the TOE Security Target O.Identification and certification.

FIA_UID.2(1) Identification of user prior to all action (1)

This component is an item that requests identification on administrator. As such, it satisfies the TOE Security Target O.Identification and certification.

FIA_UID.2(2) Identification of user prior to all action (2)

This component is an item that requests identification on external IT entity and requests identification of client IP address. Client IP address generates audit record by identifying external IT entity, and forms the basis for control of service denial attack and information flow. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Interception of service denial attack, O.Identification and certification.

FMT_MOF.1(1) Management of security function (1)

This component assures ability of the authorized administrator (installer) to manage security function and assure usability during defectiveness in TOE. As such, it satisfies the TOE Security Target O.Security management.

FMT_MOF.1(2) Management of security function (2)

This component assures ability of the authorized administrator(super administrator) to manage security function and assure usability during defectiveness in TOE. As such, it satisfies the TOE Security Target O.Security management.

FMT_MOF.1(3) Management of security function (3)

This component assures ability of the authorized administrator (administrator) to manage security function and assure usability during defectiveness in TOE. As such, it satisfies the TOE Security Target O.Security management.

FMT_MOF.1(4) Management of security function (4)

This component assures ability of the authorized administrator (monitor) to manage security function and assure usability during defectiveness in TOE. As such, it satisfies the TOE Security Target O.Security management.

FMT_SMF.1 Specification of management function

This component specifies the security function that authorized administrator can manage. As such, it satisfies the TOE Security Target O.Security management.

FMT_MSA.1 Management of security property

This component assures that security property data, which is TSF data necessary in performing the TOE security function, can be accessed only by authorized administrator. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Security management, O.Interception of service denial attack.

FMT_MSA.3 Initialization of static property

This component provides the initial value of security property used in policy of control for arbitrary access. As such, it satisfies the TOE Security Target O.Interception of abnormal web service, O.Security management, O.Interception of service denial attack.

FMT_MTD.1(1) Management of TSF data (1)

This component provides function (back-up) with which the authorized administrator can manage TSF data. As such, it satisfies the TOE Security Target O.Security audit, O.Security management.

FMT_MTD.1(2) Management of security function (2)

This component provides function (basic setting information, Agent registration information, user information, flawlessness examination setting information, audit storage space setting information, NTP setting information) with which the authorized administrator can manage TSF data. As such, it satisfies the TOE Security Target O.Security audit, O.Security management.

FMT_MTD.1(3) Management of security function (3)

This component provides function (Agent basic information, White URL information, contents information, service domain information, Trust IP information, access intercepted IP information, cookie/hidden field information, unload file information, unfiltered file information) with which the authorized administrator can manage TSF data. As such, it satisfies the TOE Security Target O.Security audit, O.Security management.

FMT_MTD.1(4) Management of security function (4)

This component provides function (identification and certification data, setting of time-out time) with which the authorized administrator can manage TSF data. As such, it satisfies the TOE Security Target O.Security audit, O.Security management.

FMT_MTD.2(1) Management of limit value of TSF data (1)

This component assures that authorized administrator manages limit value of TSF data (time-out for session closure) and countermeasure action will be taken in the event of reaching or exceeding the designated limit value. As such, it satisfies the TOE Security Target O.Security management.

FMT_MTD.2(2) Management of limit value of TSF data (2)

This component assures that authorized administrator manages limit value of TSF data (audit record storage space) and countermeasure action will be taken in the event of reaching or exceeding the designated limit value. As such, it satisfies the TOE Security Target O.Security management.

FMT_SMR.1. Role of security

This component assures that the user is associated with the role of authorized administrator. As such, it satisfies the TOE Security Target O.Security management.

FPT_ATM1. Testing of abstract machine

This component assures execution of series of tests for illustration of accurate operation of TSF lower portion abstract machine. As such, it satisfies the TOE Security Target O.Protection of own function.

FPT_FLS.1 Maintenance of secured status at the time of disability

This component assures that the secured status is maintained in the event of occurrence of disability. As such, it satisfies the TOE Security Target O. Protection of own function.

FPT_TST.1 Self-testing of TSF

This component assures self-testing for accurate operation of TSF, and function of verification of flawlessness of TSF data and TSF execution code by the authorized administrator. As such, it satisfies the TOE Security Target O.Protection of TSF data.

FTA_SSL.1 Session closure by TSF

This component closes session that mutually acts after non-active period of user, and requests case to be generated prior to cancelling the closure. As such, it satisfies the TOE Security Target O.Security management, O.Identification and certification.

Theoretical Basis on TOE Assurance Requirements

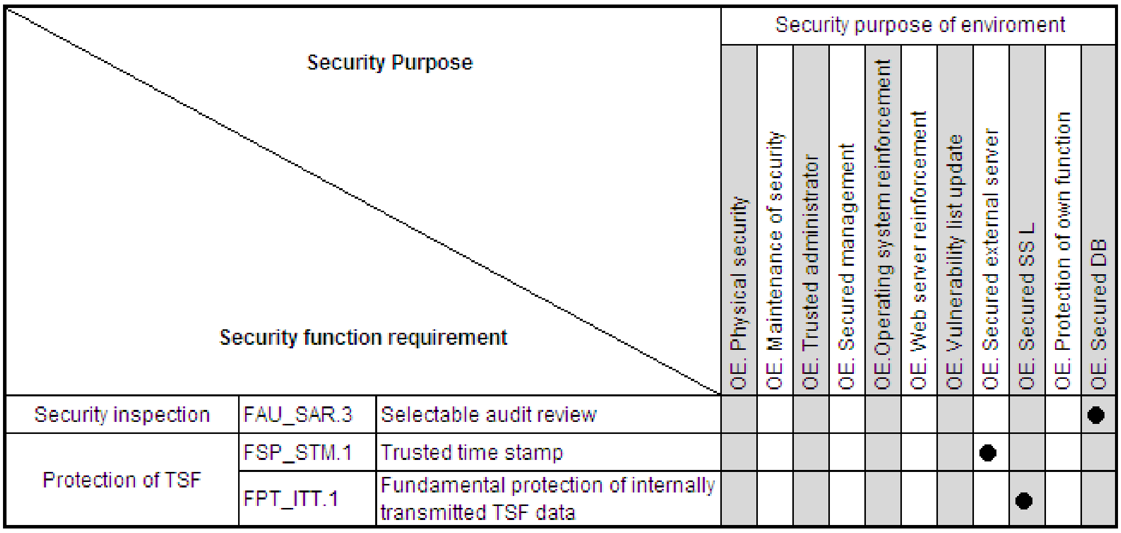
In this Security Target it is presumed that the level possibility of the external attack to discover the vulnerability on the asset to be low, and the attacker has low level knowledge on the computer and network. Countermeasure against such attacker with low level possibility and knowledge was decided at classification of EAL4, which requires fortification of development document and analysis of vulnerability, assurance on automated configuration management of development process.

EAL4 classification is a evaluation assurance classification that can counter the low level of attack in overall with fortified analysis of vulnerability including analysis of independent vulnerability of evaluator and verification of abuse analysis, as well as fortification of development procedures such as life cycle model of developer, definition and detailed design of all external interfaces of TOE, and provision of non-standardized TOE security policy model.

Theoretical basis of security requirements on IT environment

Theoretical basis of security requirements on IT environment is as per the table below.

Table 7.3 Theoretical basis of security requirements on IT environment



Security Purpose / Security function requirement			Security purpose of enviroment										
			OE. Physical security	OE. Maintenance of security	OE. Trusted administrator	OE. Secured management	OE.Operating system reinforcement	OE. Web server reinforcement	OE. Vulnerability list update	OE. Secured external server	OE. Secured SS L	OE. Protection of own function	OE. Secured DB
Security inspection	FAU_SAR.3	Selectable audit review											●
Protection of TSF	FSP_STM.1	Trusted time stamp								●			
	FPT_ITT.1	Fundamental protection of internally transmitted TSF data									●		

FAU_SAR.3 Selectable audit review

This component assures ability to sequentialize the audit data in accordance with standard with logical relationship As such, it satisfies TOE security target OE. Secured DB.

FSP_STM.1 Trusted time stamp

This component provides trusted time stamp that is being used by TSF, and the component FAU_GEN requests accurate date. As such, it satisfies TOE security target OE. Secured external server.

FPT_ITT.1 Fundamental protection of internally transmitted TSF data

This component prevents exposure or alteration of TSF data by suing SSL in order to protect data transferred between the segregated TOEs. As such, it satisfies Security target on environment OE. Secured SSL.

Theoretical Basis of Specification of Summary of TOE

Theoretical basis of TOE security functions

Theoretical basis of specification of summary of TOE is as per the following table.

Table 7.4 Theoretical basis of TOE security functions

Security function Security requirement		TSF-FAU1 Security alarm	TSF-FAU2 Generation of audit data	TSF-FAU3 Inquiry of audit data	TSF-FAU4 Excess inspection storage limit of audit data	TSF-FAU5 Process as full storage of audit data	TSF-FDP1 Flow Control of information	TSF-FDP2 Contents protection	TSF-FIA1 Administrator discernment and certification	TSF-FIA2 Certification failure processing	TSF-FIA3 Externer IP discernment processing	TSF-FMT1 User administration	TSF-FMT2 Basis system administration	TSF-FMT3 Agent and Security policy administration	TSF-FMT4 Session administration	TSF-FPT1 Abstraction identification	TSF-FPT2 Maintenance of secured status on TSF obstacle	TSF-FPT3 TSF test by itself and process of date integrity	TSF-SSL1 Session fastening cancellation
FIA_UAU.2	Security alarm	●																	
FAU_GEN.1	Generation of audit data		●																
FAU_GEN.1	Association of user identity		●																
FAU_SAA.1	Analysis of potential infringement	●																	
FAU_SAR.1	Audit review			●															
FAU_SAR.3	Selectable audit review			●															
FAU_STG.1	Protection of audit evidence			●															
FAU_STG.3	Countermeasure actions in the event				●														
FAU_STG.4	Prevention of loss of audit data					●													
FDP_IFC.1(1)	Control of partial information flow (1)						●												
FDP_IFC.1(2)	Control of partial information flow (2)						●												
FDP_IFF.1(1)	Properties of unified class security (1)						●												
FDP_IFF.1(2)	Properties of unified class security (2)						●												
FDP_SDI.2	Recorded data integrity							●											
FIA_AFL.1	Processing of failure in certification									●									
FIA_ATD.1(1)	Definition of user properties (1)								●										
FIA_ATD.1(2)	Definition of user properties (2)										●								
FIA_UAU.2	User certification prior to all actions								●										
FIA_UAU.7	Protection of certification feedback								●										
FIA_UID.2(1)	User identification prior to all actions (1)								●										
FIA_UID.2(2)	User identification prior to all actions (2)										●								
FMT_MOF.1(1)	Management of security function (1)											●							
FMT_MOF.1(2)	Management of security function (2)											●	●	●	●				
FMT_MOF.1(3)	Management of security function (3)											●		●	●				
FMT_MOF.1(4)	Management of security function (4)											●			●				
FMT_MSA.1	Management of security properties													●					
FMT_MSA.3	Initialization of static properties													●					
FMT_MTD.1(1)	Management of TSF data (1)												●						
FMT_MTD.1(2)	Management of TSF data (2)											●	●						
FMT_MTD.1	Management of TSF data (3)													●					
FMT_MTD.1	Management of TSF data (4)											●			●				
FMT_ MTD.2(1)	Management of limit value of TSF data (1)														●				
FMT_ MTD.2(2)	Management of limit value of TSF data (2)												●						
FMT_ SMF.1	Administration function specification											●	●	●	●				
FMT_SMR.1	Role of security											●							
FPT__ATM.1	Testing abstract machine															●			
FPT_FLS.1	Maintenance of secured status																●		
FPT_TST.1	Self-testing of TSF																	●	
FTA_SSL.1	Session closure by TSF																		●

FAU_ARP.1 Security alarm

TOE satisfies TSF_FAU.1 Security alarm by performing transmission of security alarm to the authorized administrator on the infringement actions by using alarm window, notice window and alarm mail.

FAU_GEN.1 Generation of audit data

TOE satisfies TSF_FAU.2 Generation of audit data record by generating audit data on all audit cases generated in TOE.

FAU_GEN.1 Association of user identity

TOE satisfies TSF_FAU.2 Generation of audit data record by associating identity of related user with case to be subjected to audit on all cases generated in TOE.

FAU_SAA.1 Analysis of potential infringement

TOE satisfies TSF_FAU.1 Security alarm by examining audited cases on cases that infringes web application security policy and by executing transmission of security warning to the administrator for the corresponding case by using alarm window and alarm mail.

FAU_SAR.1 Audit review

TOE satisfies TSF_FAU.3 Inquiry on audit data by reviewing the audit record by the authorized administrator.

FAU_SAR.3 Selectable audit review

TOE satisfies TSF_FAU.3 Inquiry on audit data by reviewing audit record with logical relationship.

FAU_STG.1 Protection of audit evidence

TOE satisfies TSF_FAU.3 Inquiry on audit data by protecting the audit record from unauthorized deletion by providing function that prevents loss of audit data and by preventing unauthorized changes to the audit record within the audit record.

FAU_STG.3 Countermeasure actions in the event of anticipated loss of audit data

TOE satisfies TSF_FAU.4 Examination of exceeding the limit of audit data storage by taking countermeasure actions in the event of exceeding the predetermined limit for audit evidence storage..

FAU_STG.4 Prevention of loss of audit data

TOE satisfies TSF_FAU.5 Processing at the time of saturation of audit data storage space by taking countermeasure actions in the case of saturation of audit evidence.

FDP_IFC.1(1) Control of partial information flow (1)

TOE satisfies TSF_FDP.1 Control on information flow by defining the web application security policy (allowance) for Control on information flow.

FDP_IFC.1(2) Control of partial information flow (2)

TOE satisfies TSF_FDP.1 Control on information flow by defining the web application security policy (denial) for Control on information flow.

FDP_IFF.1(1) Properties of unified class security (1)

TOE satisfies TSF_FDP.1 Control on information flow by controlling the properties of http requests through web application security policy (allowance) for Control on information flow.

FDP_IFF.1(2) Properties of unified class security (2)

TOE satisfies TSF_FDP.1 Control on information flow by controlling the properties of http requests through web application security policy (denial) for Control on information flow.

FIA_AFL.1 Processing of failure in certification

TOE satisfies TSF_FIA.2 processing of failure in certification by assuring ability to take countermeasure actions when the number of failure in certification attempt defined for user reaches the corresponding number.

FIA_ATD.1(1) Definition of user properties (1)

TOE satisfies TSF_FIA.1 administrator identification and certification by defining the security properties of authorized administrator at the time of executing security policy on the basis of management

FIA_ATD.1(2) Definition of user properties (2)

TOE satisfies TSF_FIA.3 Identification of external IT entity by defining the security properties of external IT entity at the time of executing security policy on the basis of management.

FIA_UAU.2 User certification prior to all actions

TOE satisfies TSF_FIA.1 administrator identification and certification by executing certification on administrator that requires administrator certification.

FIA_UAU.7 Protection of certification feedback

TOE satisfies TSF_FIA.1 administrator identification and certification by assuring that only the designated certification feedback is provided to the administrator during process of certification.

FIA_UID.2(1) User identification prior to all actions (1)

TOE satisfies TSF_FIA.1 administrator identification and certification by successfully identifying the identity of authorized administrator.

FIA_UID.2(2) User identification prior to all actions (2)

TOE satisfies TSF_FIA.3 Identification of external IT entity by successfully identifying the identity of external IT entity.

FMT_MOF.1(1) Management of security function (1)

TOE satisfies TSF_FMT.1 User management by assuring the ability of the authorized administrator (by assuring the ability of the authorized administrator (super administrator) in accordance with corresponding management authority) in accordance with corresponding management authority.

FMT_MOF.1(2) Management of security function (2)

TOE satisfies TSF_FMT.1 User management, TSF_FMT.2 Management of basic system, TSF_FMT.3 Management of Agent and Security Policy, TSF_FMT.4 Session management by assuring the ability of the authorized administrator (super administrator) in accordance with corresponding management authority.

FMT_MOF.1(3) Management of security function (3)

TOE satisfies TSF_FMT.1 User management, TSF_FMT.3 Management of Agent and Security Policy, TSF_FMT.4 Session management by assuring the ability of the authorized administrator (administrator) in accordance with corresponding management authority.

FMT_MOF.1(4) Management of security function (4)

TOE satisfies TSF_FMT.1 User management, TSF_FMT.4 Session management by assuring the ability of the authorized administrator (Monitor) in accordance with corresponding management authority.

FMT_SMF.1 Specification of management function

TOE satisfies TSF_FMT.1 User management, TSF_FMT.2 Management of basic system, TSF_FMT.3 Management of Agent and Security Policy, TSF_FMT.4 Session management by performing the security functions of security property management (FMT_MSA.1), TSF data management (FMT_MTD.1), and security function management (FMT_MOF.1).

FMT_MSA.1 Management of security properties

TOE satisfies TSF_FMT.3 Management of Agent and Security Policy providing management of security properties of web application security policy for control of information flow.

FMT_MSA.3 Initialization of static properties

TOE satisfies TSF_FMT.3 Management of Agent and Security Policy by assuring administrator security policy to enable only the authorized administrator at the time of initialization of security properties of TSF data necessary in executing security functions.

FMT_MTD.1(1) Management of TSF data (1)

TOE satisfies TSF_FMT.2 Management of basic system by enabling the authorized administrator to back-up and restore the key file that composes TOE into semi-permanent memory apparatus.

FMT_MTD.1(2) Management of TSF data (2)

TOE satisfies TSF_FMT.1 User management, TSF_FMT.3 Management of basic system by granting ability to add, change and delete key data by the authorized administrator.

FMT_MTD.1 Management of TSF data (3)

TOE satisfies TSF_FMT.3 Management of Agent and Security Policy by granting ability to add, change and delete key data and security policy information of Agent by the authorized administrator.

FMT_MTD.1 Management of TSF data (4)

TOE satisfies TSF_FMT.1 User management, TSF_FMT.4 Session management by granting ability to change the time (identification and certification data, time-out period for session closure) by the authorized administrator.

FMT_ MTD.2(1) Management of limit value of TSF data (1)

TOE satisfies TSF_FMT.4 Session management by managing the limit value (time-out period for session closure) of data and by assuring ability of the authorized administrator to take countermeasure actions in the event of reaching or exceeding the designated limit value..

FMT_ MTD.2(2) Management of limit value of TSF data (2)

TOE satisfies TSF_FMT.2 Management of basic system by managing the limit value (capacity of audit record) of data and by assuring ability of the authorized administrator to take countermeasure actions in the event of reaching or exceeding the designated limit value.

FMT_SMR.1 Role of security

TOE satisfies TSF_FMT.1 User management by limiting the role of supplementary administrator of TOE to authorized administrator.

FPT__ATM.1 Testing abstract machine

TOE satisfies TSF_FPT.1 Testing of abstract machine by verifying whether the web server can continuously perform service by detecting error on web server and interface.

FPT_FLS.1 Maintenance of secured status at the time of disability

TOE satisfies TSF_FPT.2 TSF maintenance of secured status at the time of disability in order to assure that the key security functions operate during system disability and disability in communication connection between systems.

FPT_TST.1 Self-testing of TSF

TOE satisfies TSF_FPT.3 Self-testing of TSF and processing of flawlessness of data by examining the flawlessness on the TSF data and execution binary files and by illustrating the outcome to authorized administrator.

FTA_SSL.1 Session closure by TSF

TOE satisfies TSF_SSL.1 Closure and cancellation of session by closing the session and limiting the unauthorized security management activities during non-active period of the authorized administrator.

Theoretical basis for TOE assurance method

Table 7. 5 Theoretical basis for assurance method

Assurance Class	Assurance Component	Assurance Method

Configuration Management	ACM_AUT.1 Automation of partial configuration management	WEBS-RAY V2.5 Configuration management document
	ACM_CAP.4 Support for generation and accommodation procedure	
	ACM_SCP.2 Scope of problem tracing and configuration management	
Distribution and Operation	ADO_DEL.2 Detection of changes	WEBS-RAY V2.5 Distribution document
	ADO_IGS.1 Procedures for installation, generation and start-up	WEBS-RAY V2.5 Installation guideline
Development	ADV_FSP.2 Completely defined external interface	WEBS-RAY V2.5 Function specification
	ADV_HLD.2 Basic design that segregated security function and non-security function	WEBS-RAY V2.5 Basic design manual
	ADV_IMP.1 Expression of realization on TSF	WEBS-RAY V2.5 Specification on verification of realization
	ADV_LLD.1 Descriptive detailed design	WEBS-RAY V2.5 Detailed design manual
	ADV_RCR.1 Verification of non-standardized accordance	WEBS-RAY V2.5 Function specification WEBS-RAY V2.5 Basic design manual WEBS-RAY V2.5 Detailed design manual WEBS-RAY V2.5 Specification on verification of realization
	ADV_SPM .1 Non-standardized TOE security policy model	WEBS-RAY V2.5 Security policy model manual
Manual	AGD_ADM.1 Administrator manual	WEBS-RAY V2.5 Administrator manual
	AGD_USR.1 User manual	N/A
Support for Life Cycle	ALC_DVS.1 Identification of security countermeasures	WEBS-RAY V2.5 Life cycle support manual
	ALC_LCD.1 Developer defined life cycle model	
	ALC_TAT.1 Well-defined development tool	
Testing	ATE_COV.2 Analysis of scope of testing	WEBS-RAY V2.5 Test manual
	ATE_DPT.1 Testing of basic design	
	ATE_FUN.1 Functional test	
	ATE_IND.2 Independent test: specimen test	
Evaluation of Vulnerability	AVA_MSU.2 Verification of analysis of manual	WEBS-RAY V2.5 Abuse analysis manual
	AVA_SOF.1 Evaluation of strength of function of TOE security	WEBS-RAY V2.5 Vulnerability analysis manual
	AVA_VLA.2 Analysis of independent vulnerability	

ACM_AUT.1 Automation of partial configuration management

TOE provides automated means of generating authorized changes in the expression of realization of TOE in the configuration management system and further provides WEBS-RAY V2.5 Configuration management document in order to assure that automated means that support generation of TOE is used.

ACM_CAP.4 Support for generation and accommodation procedure

TOE provides control to assure that unauthorized changes do not occur and further provides WEBS-RAY V2.5 Configuration management document in order to assure appropriate functionality and usage of configuration management system.

ACM_SCP.2 Scope of problem tracing and configuration management

TOE provides WEBS-RAY V2.5 Configuration management document to assure that the configuration items under the configuration management are changing in controlled method in accordance with appropriate authorization.

ADO_DEL.2 Detection of changes

TOE provides WEBS-RAY V2.5 Distribution document to assure system control and distribution facility and procedures that assure TOE sent by the sender is received by receiver without changes.

ADO_IGS.1 Procedures for installation, generation and start-up

TOE provides WEBS-RAY V2.5 Installation guidelines in order to assure that installation, generation and start-up is being executed in the secured manner intended by the developer.

ADV_FSP.2 Completely defined external interface

TOE provides WEBS-RAY V2.5 Specification of function in order to examine and define all external interfaces and to realize fundamental explanations on interface and actions, and TOE security function requirements that the users of TSF can see.

TOE provides WEBS-RAY V2.5 Basic design manual in order to describe TSF in terms of key composition units, explain the composition units as well as functions and relations provided by such, and to assure that, because of this, TOE provides structure that is appropriate in realizing the TOE security function requirements

ADV_IMP.1 Expression of realization on TSF

TOE provides WEBS-RAY V2.5 Specification on verification of realization in order to assure analysis by enabling assessment of detailed internal actions of TSF.

ADV_LLD.1 Descriptive detailed design

TOE provides WEBS-RAY V2.5 Detailed design manual in order to describe the internal actions of TSF as mutual and subordinate relationship between modules, and to assure that sub-systems of TSF are being detailed accurately and effectively.

ADV_RCR.1 Verification of non-standardized accordance

TOE provides WEBS-RAY V2.5 Specification of function, WEBS-RAY V2.5 Basic design manual, WEBS-RAY V2.5 Detailed design manual, WEBS-RAY V2.5 Specification on verification of realization in order to assure the coherence and diversity in expression of TSF (specification of summary of TOE, specification of function, basic design, detailed design, and expression of realization).

ADV_SPM .1 Non-standardized TOE security policy model

TOE provides WEBS-RAY V2.5 Security policy model analysis manual in order to describe rules and characteristics of all policies of TSF and to assure coherence and completeness of all policies as well as to satisfy Subordinate relationship of FPT_FLS.1.

AGD_ADM.1 Administrator manual

TOE provides WEBS-RAY V2.5 Administrator manual on the documented material to be used by those with responsibility to maintain composition and manage TOE in accurate manner in order to maximize the security.

AGD_USR.1 User manual

In the case of user manual of TOE, such has not been prepared since the FMT of TOE does not mention anything on User management.

ALC_DVS.1 User manual

TOE provides WEBS-RAY V2.5 Life cycle support manual in order to protect TOE by suing physical, procedural, personnel and other security measures that can be used in the development environment.

ALC_LCD.1 Developer defined life cycle model

TOE provides WEBS-RAY V2.5 Life cycle support manual in order to assure that life cycle model used in development and maintenance of TOE is being supported well.

ALC_TAT.1 Well-defined development tool

TOE provides WEBS-RAY V2.5 Life cycle support manual in order to assure that development tools that are wrongly defined, lacks in coherence or inaccurate have not be used in developing TOE.

ATE_COV.2 Analysis of scope of testing

TOE provides WEBS-RAY V2.5 Test manual to prove that TSF has been systematically testing in accordance with the functional specification.

ATE_DPT.1 Testing of basic design

TOE provides WEBS-RAY V2.5 Test manual to assure that stages of TSF sub-systems are properly realized.

ATE_FUN.1 Functional test

TOE provides WEBS-RAY V2.5 Test manual in order to assure that all security functions are being executed as specified.

ATE_IND.2 Independent test: specimen test

TOE provides WEBS-RAY V2.5 Test manual in order to assure that security functions are being executed as specified.

AVA_MSU.2 Verification of analysis of manual

TOE provides WEBS-RAY V2.5 Abuse analysis manual to assure that there are no guidelines within the manual that is misleading, irrational or contract, and that deals with secured procedures for all operational mode.

AVA_SOF.1 Evaluation of strength of function of TOE security

TOE provides WEBS-RAY V2.5 Vulnerability analysis manual in order to determine the statistical or quantitative analysis results on the security activities of lower security mechanism and strength of the security actions by the efforts needed to overcome such.

AVA_VLA.2 Analysis of independent vulnerability

TOE provides WEBS-RAY V2.5 Vulnerability analysis manual in order to confirm that securityvulnerability exist, and to assure that vulnerability cannot be abused under the intended environment of TOE.

7.4 Theoretical Basis on Subordinate Relationship

7.4.1 Subordinate relationship of TOE security function requirements

Table 7. 6 Subordinate relationship of functional components

No.	Function Component	Subordinate relationship	Reference No.
1	FAU_ARP.1	FAU_SAA1	4
2	FAU_GEN.1	FPT_STM.1	38
3	FAU_GEN.2	FAU_GEN.1	2
		FIA_UID.1	20, 21 (Select upper level subordinate relationship FIA_UID.2)
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_STG.1	FAU_GEN.1	2
8	FAU_STG.3	FAU_STG.1	7
9	FAU_STG.4	FAU_STG.1	7
10	FDP_IFC.1(1)	FDP_IFF.1	12,13
11	FDP_IFC.1(2)	FDP_IFF.1	12,13
12	FDP_IFF.1(1)	FDP_IFC.1	10,11
		FMT_MSA.3	27
13	FDP_IFF.1(2)	FDP_IFC.1	10,11
		FMT_MSA.3	27
14	FIA_AFL.1	FIA_UAU.1	18 (Select upper level subordinate relationship FIA_UAU.2)
15	FIA_ATD.1(1)	–	–
16	FIA_ATD.1(2)		–
17	FIA_UAU.2	FIA_UID.1	20, 21 (Select upper level subordinate relationship FIA_UID.2)
18	FIA_UAU.7	FIA_UAU.1	18 (Select upper level subordinate relationship FIA_UAU.2)
19	FIA_UID.2(1)	–	–
20	FIA_UID.2(2)	–	–
21	FMT_MOF.1(1)	FMT_SMF.1	34
		FMT_SMR.1	35
22	FMT_MOF.1(2)	FMT_SMF.1	34
		FMT_SMR.1	35
23	FMT_MOF.1(3)	FMT_SMF.1	34
		FMT_SMR.1	35

24	FMT_MOF.1(4)	FMT_SMF.1	34
		FMT_SMR.1	35
25	FMT_MSA.1	FDP_IFC.1	10,11
		FMT_SMF.1	34
		FMT_SMR.1	35
26	FMT_MSA.3	FMT_MSA.1	26
		FMT_SMR.1	35
27	FMT_MTD.1(1)	FMT_SMF.1	34
		FMT_SMR.1	35
28	FMT_MTD.1(2)	FMT_SMF.1	34
		FMT_SMR.1	35
29	FMT_MTD.1(3)	FMT_SMF.1	34
		FMT_SMR.1	35
30	FMT_MTD.1(4)	FMT_SMF.1	34
		FMT_SMR.1	35
31	FMT_MTD.2(1)	FMT_MTD.1	28,29,30,31
		FMT_SMR.1	35
32	FMT_MTD.2(2)	FMT_MTD.1	28,29,30,31
		FMT_SMR.1	35
33	FMT_SMF.1	-	-
34	FMT_SMR.1	FIA_UID.1	20, 21 (Select upper level subordinate relationship FIA_UID.2)
35	FPT_AMT.1	-	-
36	FPT_FLS.1	ADV_SPM.1	Assurance requirement
37	FPT_STM.1	-	Provide as security function requirements on IT environment
38	FPT_ITT.1	-	Provide as security function requirements on IT environment
39	FPT_TST.1	FMT_AMT.1	36
40	FTA_SSL.1	FIA_UAU.1	18 (Select upper level subordinate relationship FIA_UAU.2)

Although FAU_GEN.2, FIA_UAU.1, and FMT_SMR.1 have subordinate relationship to FIA_UID.1, this is satisfied by FIA_UID.2 which has class relationship with FIA_UID.1.

Although FIA_AFL.1, FIA_UAU.7, and FTA_SSL.1 have subordinate relationship to FIA_UAU.1, this is satisfied by FIA_UAU.2, which has class relationship with FIA_UAU.1.

7.4.2 Subordinate relationship of TOE assurance requirements

Subordinate relationship of each assurance package provided by Common Criteria for Information Security System has already been satisfied. As such theoretical basis on this is omitted.

7.5 Theoretical Basis on Strength of Function

Strength of function is applied to "FIA_UAU.2", which is security requirement with probability and permutation mechanism, and "TSF_FIA.1 administrator identification and certification" function which realized above into function. "FIA_UAU.2" has medium strength of function, with password certification mechanism-based "TSF_FIA.1 administrator identification and certification" function also having medium strength of function. Therefore, the "TSF_FIA.1 administrator identification and certification" function with medium strength of function that realized "FIA_UAU.2" security requirements with medium strength of function is sufficient to counter low level source of threat.

8 Reference Material

- [1] Common Criteria for Evaluation of IT Security, V2.3, 2005.8
  – Korea Information Security Agency
- [2] Common Methodology for Evaluation of IT Security, V2.3, 2005.8
  - Korea Information Security Agency
- [3] Preparatory Course for Evaluation of CC Foundation, 2004.4
  - Korea Information Security Agency
- [4] Collection of Presentation on Protection Profile of Information Security System, 2004.4
  - Korea Information Security Agency
- [5] Preparatory Education on Evaluation of CC Foundation, 2005.6
  - Korea Information Security Agency