Development of Information Security-Focused Incident Prevention Measures for Critical Information Infrastructure in Japan

Hideaki Kobayashi[1], Kenji Watanabe[2], Takahito Watanabe[1], and Yukinobu Nagayasu[1]

[1] Security Engineering Laboratory, IT Security Center,
Information-technology Promotion Agency, Japan (IPA)
2-28-8, Honkomagome, Bunkyo-ku, Tokyo, 113-6591, Japan
{hd-koba, t-watana, y-nagaya}@ipa.go.jp
[2] Nagaoka University of Technology,
1603-1 Kamitomiokamachi, Nagaoka, Niigata, 940-2188, Japan
watanabe@kjs.nagaokaut.ac.jp

Abstract. In recent years, the dilemma of cyber attacks by malicious third parties targeting security vulnerabilities in information and communication systems has emerged, resulting in security incidents. This situation suggests that the establishment of proactive efforts and recurrence prevention measures are becoming imperative, especially in critical infrastructure sectors. This paper provides an analysis of 58 security incident cases, which occurred in critical infrastructures worldwide and were published in media. The purpose of the analysis is to conclude to a valid list of recurrence prevention measures that constitute good practices.

Keywords: Information security, Critical Information Infrastructure security, Security vulnerabilities, Security incidents

1 Introduction

In the present era, Information and Communication Technology (ICT) is becoming an infrastructure that constitutes the "nervous system" of the current economy and society. However, the unauthorized access to the power grid system (United States) and water system (Australia), the prevalence of computer viruses, and the occurrence of accidents/incidents due to the system failures of financial and transportation services portray the exponential increase of the imminent danger and damage that ICT issues may instigate.

The Japanese Government established the National Information Security Center (NISC) to promote information security on April 25, 2005. NISC started "The First National Strategy on Information Security – Toward the creation of a trustworthy society –" from the fiscal year 2006 to 2008. The implementing entities were classified into four areas: a)Central Government/Local Governments, b)Critical

Infrastructures, c)Businesses and d)Individuals [1]. For the Critical Infrastructures, the following 10 sectors are identified: "Telecommunications", "Finance", "Civil aviation", "Railways", "Electricity", "Gas", "Governmental/Administrative services (including local governments)", "Medical services", "Water works" and "Logistics" [2][3]. In the First National strategy, several policies such as information sharing (CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response), analysis of interdependency and cross-sectoral exercises etc. were promoted.

In fiscal year 2009, "The Second National Strategy on Information Security" has started and continues until the fiscal year 2011. The target scope of this Second National Strategy includes preparedness and enhancement of security measures against the incidents [4] [5].

In the midst of the current circumstances and on the premise that information security incidents will occur, it is becoming imperative for the government and private sectors to cooperate in implementing measures for incident prevention, damage control, and rapid recovery in the case security is breached.

Therefore, it is necessary to promote both security and reliability as the two wheels of a chariot to protect critical infrastructures from future ICT incidents. Recognizing information security as a risk to critical infrastructure systems, foreign and domestic incident publications were collected, the causes analyzed, and recurrence prevention measures were identified [6].

2   Analysis of Case Studies on Security Incidents in Critical Infrastructures

2.1   Approach to Incident Information Gathering

To collect information concerning security incidents experienced in critical infrastructures, two methods can be considered. The first is to gather information through publications in the media; the second is to gather information directly from critical infrastructure operators.

As for the latter, it was assumed to be particularly difficult as the details concerning security incidents are considered sensitive information by critical infrastructures. For this reason, gathering of incident information was limited to gleaning information from publications in mass media.

2.2   Subject and Range of Incidents

In gathering incident information, the time frame was limited between the year 2000 and 2008, and incidents were not limited domestically, but included foreign incidents as well. Incidents that occurred overseas were included mainly for the reason that some had great influence in relation to security (by means that were not experienced domestically, caused much greater damage, etc.) and, by gathering and utilizing them

as references, carried great weight from the perspective that they could be positively employed in preventing security incidents before occurring in our own country.

21 different domestic news sites[1] were utilized as sources for domestic incidents and 17 foreign security news sites [2] were utilized to gather foreign incident information. For this analysis, 38 domestic incidents and 20 foreign incidents were selected from a total of 58 security incident cases in critical infrastructures.

2.3   Classification of Incident Information

For the classification of the security incident cases, the items in Table 1 were extracted from the published information.

If there was a need to thoroughly collect information concerning the attacker and the method of attack, they were included in the "Incident Summary" field.

**Table 1.** Incident Information Items

No.	Identification number of the information security incident case.
Incident Case Title	Incident case title including main security causes and the infrastructure operator.
Date of Incident	Occurrence date of the information security incident. In the case that the occurrence date is unknown/unavailable, the date the information security incident was discovered. In the case the discovery date is also unknown/unavailable, the date the information security incident was published
Incident Summary	The summary of the information security incident should be stated. The attacker, victim party, attack method, and damage information should also be extracted and summarized concisely in several lines.
Main Causes	The excerpt of published information word for word from an article should be avoided and the causes are categorized into several types. Refer to section 2.4 for details.
Impact Range	The extent of damage generated by the occurrence of the information security incident. Particularly, numerical recording is encouraged. For example, in case of a data breach, the exact number of cases leaked should be recorded. In case of denial of service incident, the extent (number of services) and period of time services were suspended. In the case of monetary damage, the total sum of loss should be recorded.
Recurrence Prevention Measure	In accordance with the analysis summarized later, a recurrence prevention measure should be proposed, and the recurrence prevention measure ID should be recorded. Refer to section 3 for details.
Remarks	Information worth noting, such as the manner in which the information security incident was discovered and the countermeasure(s) the critical infrastructure operator implemented should be recorded.
Source	The source of the security incident information.

---

[1] e.g., Asahi.com (The Asahi Shimbun Company) http://www.asahi.com/,
   NIKKEI NET (Nikkei Inc. / Nikkei Digital Media, Inc.) http://www.nikkei.co.jp/,
   ITmedia (ITmedia, Inc.) http://www.itmedia.co.jp/
[2] e.g., DHS Daily Open Source Infrastructure Report
   http://www.dhs.gov/files/programs/editorial_0542.shtm,
   Industrial Defender http://www.industrialdefender.com/,
   Cyber Security News http://cicentre.com/news/cyber_security.html

2.4   Analysis of Studied Incidents

In this study, security incidents experienced by existing critical infrastructures were analyzed[3]. The purpose behind gathering and analyzing information security incident cases is to identify causes and recurrence prevention measures. The method employed for analysis was the classification of information through the systematization of incident causes as shown in Fig. 1.
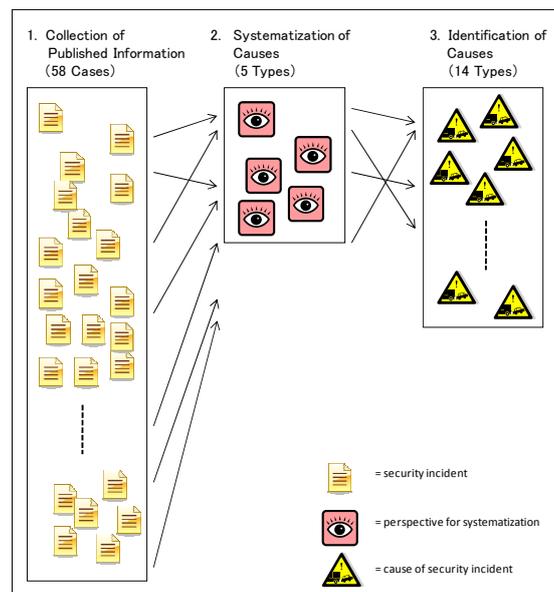
Fig. 1. Classification of Published Information

2.4.1   Cause Systematization

There were many accounts within the published information collected that could be considered as causes of the information security incidents. However, there was no consistency in the manner in which they were recorded, making it difficult to systematize the information from a single perspective. After contemplating possible perspectives from which the information could be systematized, five different perspectives were thought to be feasible. These five perspectives are explained as follows:

---

[3] The same method was employed by Brandstetter et al. as one of their methods. Thomas Brandstetter, Konstantin Knorr, and Ute Rosenbaum: A Structured Security Assessment Methodology for Manufactures of Critical Infrastructure Components: Proceedings of the 24th IFIP TC 11 International Information Security Conference, SEC 2009 Pafos, Cyprus, May 2009, pp248-258, Springer

(1) Unauthorized Access

In many of the published articles, the cause was expressed as "unauthorized access". However, "unauthorized access" in short, allows for the assumption of a vast variety of different circumstances and is exceedingly vague. To overcome the generality of "unauthorized access", this group was supplemented with additional information: the attacking method and the type of perpetrators, such as "SQL Injection" (3 cases), "Denial of Service Attack by External Sources" (6 cases), "Unauthorized Access from External Sources" (10 cases), "Unauthorized Access by Former Personnel" (3 cases), and "Unauthorized Access by Internal Personnel" (2 cases). If no additional information was available, then the cause was just labeled as "Unauthorized Access" (5 cases).

(2) Inappropriate Use of Winny (File sharing software used in Japan)

There were many cases that identified Winny as the source of information leakage (8 cases), and they were systematized under "Inappropriate Use of Winny".

(3) Issues in System Development

"Inadequate Design" (5 cases), "Inappropriate Server Configuration" (2 cases), "Insufficient System Independency" (1 case), and "Network Route Falsification" (1 case) are issues encountered during the course of system development due to the lack of consideration in a certain aspect.

(4) Human Error

Causes that were brought about by error by personnel within an organization consisted of "Error by Internal Personnel" (4 cases) and "Error by Contracted Personnel" (1 case).

(5) Phishing

There were 4 information security incidents due to phishing fraud by web spoofing as a financial institution website. These were categorized under "Phishing".

2.4.2 Causes

After the systematization process using the perspectives explained in the previous section, the causes can be divided into 14 types as shown below:

(1) Unauthorized Access
  a. Denial of Service (DoS) Attack by External Sources (6 cases)
  b. SQL Injection (3 cases)
  c. Unauthorized Access by External Sources (10 cases)
  d. Unauthorized Access by Former Personnel (3 cases)
  e. Unauthorized Access by Internal Personnel (2 cases)
  f. Unauthorized Access (5 cases)
(2) Inappropriate Use of Winny (File sharing software used in Japan)
  a. Inappropriate Use of Winny (8 cases)
(3) Issues in System Development
  a. Inadequate Design (5 cases)
  b. Inappropriate Server Configuration (2 cases)
  c. Insufficient System Independency (1 case)
  d. Network Route Compromise (1 case)

(4) Human Error
    a. Error by Internal Personnel (4 cases)
    b. Error by Contracted Personnel (1 case)
(5) Phishing
    a. Phishing (4 cases)
  There were 4 cases with unknown causes, and 1 case that included 2 causes.

2.4.3 Incident Analysis Table

The results of the analysis conducted in this section concerning the information security incidents above were collated as an incident analysis table. As an example, a case of SQL injection (case#52) is shown in Table 2.

Table 2. Incident Analysis Table Excerpt: Case #52

No.	52
Incident Case Title	Unauthorized Access and Website Falsification of an JOGMEC 's Public Server
Date of Incident	27 Jul 2008
Incident Summary	Japan Oil, Gas and Metals National Corporation (JOGMEC) server was compromised by SQL injection. Viewers may have contracted a virus. The computers that accessed the falsified website were automatically redirected to a server (storage site of malicious programs) set up by the attacker and malicious programs may have been downloaded forcefully.
Main Causes	SQL Injection
Impact Range	JOGMEC as well as viewers/users of the website may have contracted a virus.
Recurrence Prevention Measure	L3-P1, L2-D1, L2-D3, L2-D4, L3-O1, L3-M1
Remarks	Critical Infrastructure Sector: Governmental/Administrative services (including local governments)
Source	http://www.asahi.com/national/update/1020/TKY200810200153.html http://www.jogmec.go.jp/news/release/docs/2008/pressrelease_080918.pdf

3   Recurrence Prevention Measures Derived from Incident Cases

Recurrence prevention measures were identified and classified as seen in Fig. 2. The classification process was conducted through two perspectives – lifecycle and security level. First, recurrence prevention measures for each of 14 analyzed causes were selected (1. Causes). Then each recurrence prevention measure was categorized into one of 4 phases of system lifecycle based on its most effective phase of implementation (2. Lifecycle). Thirdly, a security level was assigned to each measure based on its criticalness (3. Security Level). Lastly, recurrence prevention measures were sorted by security levels and phases of lifecycle they are assigned, and the results from this categorization were tabulated into the recurrence prevention measure table (Appendix A) (4. Recurrence Preventions Measure Table).
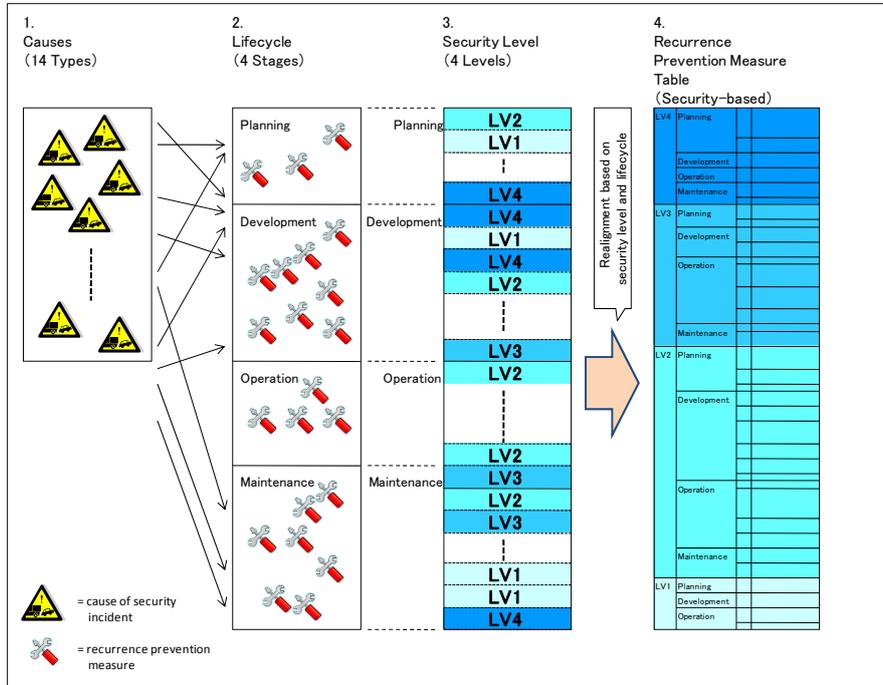
Fig. 2. Classification of Recurrence Prevention Measures

3.1 Identification of Recurrence Prevention Measures

The identification process of recurrence prevention measures was conducted on the 14 different causes utilizing the following 2 methods.

1) IPA had identified the recurrence prevention measures in the light of the reliability of critical infrastructure systems [6]. These measures were assessed for any missing measures from a security viewpoint. If any, they were supplemented.
2) Taking into account the analysis results for the information security incidents in section 2, what could have been done to prevent the incident was evaluated for each incident, adding recurrence prevention measures from an information security perspective.

In this identification process, 23 recurrence prevention measures were identified and are summarized in Appendix A.

3.2 Composition of Recurrence Prevention Measures

In identifying recurrence prevention measures, the following two points were taken into consideration.

3.2.1 The Lifecycle of Information System

Information security measures are necessary at each phase of the information system lifecycle, but the overall cost can be suppressed if the measures are considered in the earliest phase possible.

Also, it is insufficient for information security measures to be conducted just once. The attackers are constantly devising new methods of attack, and new attack methods are conceived each day. For this reason, even if an information system is securely guarded at one point, it will inevitably become unsecure at a later point in time if neglected. This is why during the operation and maintenance phase of the lifecycle, it is necessary to apply recurrence prevention measures in accordance with the PDCA cycle (Plan-Do-Check-Act cycle).

Each recurrence prevention measure was categorized by considering whether the most opportune phase to apply the measure would be the "planning", "development", "operation", or "maintenance" phase.

3.2.2 Security Level

The degree of information security fulfillment in a system can be considered from a condition in which sufficient security measures are in place to a condition in which there are almost no measures applied at all. Furthermore, the necessity of security measures differs depending on the purpose of each system. For example, the implementation of virus protection software for a personal computer is the absolute minimum necessary, while that would be insufficient for backbone systems, which require periodic audits and the establishment and implementation of progressively more sophisticated measures.

After grasping that these can be divided into several stages and debated, in this document the degree of information security fulfillment is labeled as a "security level". There are four degrees of security levels, from level 4 (high level) to level 1 (low level), and each level is defined as shown in Table 3

**Table 3.** Assumed Systems and Their Required Security Levels (based on system criticality)

Assumed System (Category)	Required Security Level
Backbone Information Systems in Critical Infrastructure	LV4
Backbone Information Systems in Business	LV3
Systems with Minimal Social Effect	LV2
Office and Local Systems	LV1

3.2.3 Rule of Bucket

In information security, there is a train of thought domestically called the "Rule of Bucket", which could be equivalent to the Weakest Link Principal in English. This rule implies that as water can only be retained to the lowest point that is made of the boards building up the bucket, and the security of the whole is explained in the same

way. The safety offered by the information security measures is only as good as its weakest point. Consequently, even if information security is substantial in one area, the contribution it provides to the safety of the whole is minimal, implicating the necessity to create the balanced countermeasure levels at each phase of the lifecycle.

In this analysis, each individual recurrence prevention measure was considered and categorized into the four different security levels (refer to section 4.1 for details) between level 4 (high level) and level 1 (low level). If a recurrence prevention measure is said at a certain level, to satisfy that security level, the corresponding recurrence prevention measures under that level must be applied. For example, consider the level 2 recurrence prevention measures. The relevant recurrence prevention measured must be continually fulfilled to satisfy security level 2, 3 and 4.
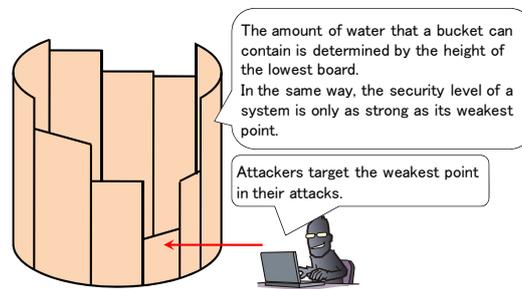
Fig. 3. Security Level Image

The recurrence prevention measure table created based on the information above is shown in the appendix below:

Appendix A – recurrence prevention measure table

3.3   Recurrence Prevention Measure Characteristics

The measures from the recurrence prevention measure table that are characteristic from a security perspective are listed below:

(1) Establishment of Security Policy
    a. A security policy clarifies an organization's policy concerning information security.
    b. In the establishment of a security policy, it is necessary to not only consider the information system itself, but the communication and organization structure of personnel, the measures to take in case of an emergency and an security education plan also must be established in the invocation of a policy.

(2) Designing System Assuming Attack
    a. Attackers with malicious intent exist inside and outside of a system environment.
    b. Equipment failure and operation errors are assumed in the reliability context, but the assumption of attackers with malicious intent are unique to the information security perspective.

(3) Pursuit of Security in Various System Components
    a. To increase the level of security of a system in its entirety, in accordance with the Bucket Rule (the Weakest Link Principal), it is necessary to deliberate the elimination of weak sections in light of the entire system.
    b. As for OS and middleware, for example, acquisition of appropriate support contracts and implementation of appropriate measures to deal effectively with vulnerabilities that are discovered on a daily basis are necessary.

(4) Penetration Testing
    a. To close out the development phase, a security test should be performed.
    b. Apart from the systems test, non-functional testing, assuming attacks with malicious intent, are to be performed.
    c. Periodic penetration tests should be performed on the developed systems.

(5) Periodic Gathering and Check of Vulnerability Information
    a. New vulnerabilities are discovered on a daily basis and security patches are released on a daily basis even after the commencement of system operation.
    b. Planned vulnerability information acquisition and respective action should be executed for OS and middleware.

4 Self Evaluation of Security Level

4.1 Evaluation Method of Security Level

Utilizing the recurrence prevention measure table, a self evaluation can be performed to propose a measure for each security level. To be more specific, it is possible to confirm all the necessary recurrence prevention measures for the targeted security level, and requisitely for the respective security levels below it, are implemented. Every recurrence prevention measure for the security levels below must be employed to achieve the targeted security level.

To conduct a security level self evaluation, the targeted security level must be established. There are 4 different levels as shown in Table 3. Furthermore, there is no need to consider an entire corporate system as a single entity, as it is possible to separate a system into different components and to appoint each part a respective security level.

Next the items concerning the target security level and the security levels below it in the recurrence prevention measure table are utilized for the self evaluation and applied to one of the items in Table 4 to judge the current fulfillment status. For example, if level 3 is targeted, the recurrence prevention measures for level 3, level 2, and level 1 are to be checked.

Table 4. Category of Implementation Condition for Security Measures

C1:	The measure is not implemented, or it is unclear whether it is implemented.
C2:	Some measures are implemented and others are not.
C3:	All of the measures currently necessary are implemented.
C4:	The implemented measures are practically complete now and in the foreseeable future.

In a self evaluation, the recurrence prevention measures evaluated as C3 or C4 are considered to be implemented at a satisfactory level. The security level is judged as accomplished only in the event that all of the necessary recurrence prevention measures are satisfactorily implemented. This can be summarized as illustrated in Table 5

Table 5. System Security Level Achievement Requirements

System Security Level (Category)		Criteria to Achieve Level
LV4:	Backbone Information Systems in Critical Infrastructure	All measures for LV4, LV3, LV2, and LV1 have a C3 or C4 fulfillment status.
LV3:	Backbone Information Systems in Business	All measures for LV3, LV2, and LV1 have a C3 or C4 fulfillment status.
LV2:	System with Minimal Social Effect	All measures for LV2 and LV1 have a C3 or C4 fulfillment status.
LV1:	Office and Local Systems	All measures for LV1 have a C3 or C4 fulfillment status.

5   Conclusion

The deliberation of incident countermeasures was conducted based on the analysis of published information security incidents. The recurrence prevention measures presented are some of many approaches in incident prevention, but they are derived from actual security incidents, and are thought to be sufficiently beneficial for businesses to employ as a reference in real world operation.

"The Second National Strategy on Information Security" includes promoting mitigation plans for seriously influential incidents against civil life and social economic activities in our living world where incidents will happen. Therefore this result from our study may be utilized as guideline toward the recurrence prevention measures for mitigation of IT incidents.

However, with the sophistication of attacking methods and advancement of information technology, it is necessary for countermeasures to constantly evolve as well. So it is necessary to continuously enhance our recurrence prevention measures against new threats.

From this point of view, the ways to share and analyze more detailed security incident information instead of just published reports, and develop up-to-date countermeasures based on those detailed information would be studied and improved in the future.

References

1. NISC: The First National Strategy on Information Security - Toward the creation of a trustworthy society -http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
2. NISC: Action Plan on Information Security Measures for Critical Infrastructures http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

3. Aung, Z., and Watanabe, K., 2009, "Japan's Critical Infrastructure Protection: Risk Components and Modeling Framework" in IFIP WG 11.10 International Federation for Information Processing, Volume xxx, Critical Infrastructure Protection III, (Boston: Springer), Page xxx-xxx. (in printing)
4. NISC Japanese Government's Efforts to Address Information Security Issues (November 2007) http://www.nisc.go.jp/eng/pdf/overview_eng.pdf
5. NISC The Second National Strategy on Information Security (currently Japanese only) http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf
6. IPA: Report of study committee for reliability of critical infrastructure information systems http://sec.ipa.go.jp/reports/20090409.html

Appendix A.

	Phase	Measure ID	Details
LV4	Planning	L4-P1	Infrastructure (network, server, etc.) that can withstand intentional attack from an external source (DDoS: Distributed Denial of Service attacks, etc.) are considered and established.
	Operation	L4-O1	A measure is installed and maintained in which only software approved by authorized personnel can be installed.
		L4-O2	Sufficient security education is applied to personnel and drills have been implemented that are in line with security incident response plans (personnel contact information, media communication, etc.).
LV3	Planning	L3-P1	Security policy is implemented based on the presumption of attack from external sources.
		L3-P2	Risk analysis has been conducted presuming an event in which internal users conduct a malicious act on the system.
		L3-P3	If a section of the system has been intruded, an implemented function is distinguished and allows for the isolation of the problem so that other components are not affected.
		L3-P4	A system to respond to security incidents (CSIRT: Computer Security Incident Response Team) exists.
		L3-P5	Security logs that take forensic use into consideration are considered.
		L3-P6	A system has been established that sufficiently manages the outsources.
		L3-P7	When outsourcing, security requirements are also included in the specifications.
	Development	L3-D1	A mechanism to store security logs is equipped.
	Operation	L3-O1	Real-time monitoring (firewall, IDS: Intrusion Detection System/IPS: Intrusion Prevention System, WAF: Web Application Firewall, security logs, etc.) is conducted for security attacks such as unauthorized access.
		L3-O2	Operators are given only the minimum level of authorization to access necessary information, and a mechanism is implemented that does not allow the access to unnecessary information. Furthermore, the prompt update of authorization is conducted in the event of relocation of operators.
		L3-O3	Penetration tests on servers and web applications are conducted periodically.
	Maintenance	L3-M1	Penetration tests (tests for vulnerability such as cross-site scripting and SQL injection) have been conducted on web applications in maintenance phase.
LV2	Planning	L2-P1	In addition to availability and integrity, risk analysis concerning confidentiality is conducted.
	Development	L2-D1	A well thought out system is structured with security (firewall, IDS: Intrusion Detection System/IPS: Intrusion Prevention System, WAF: Web Application Firewall, etc.) taken into consideration.
		L2-D2	Specification reviews are conducted from a security perspective (unauthorized access, viruses, phishing, etc.).
		L2-D3	Penetration tests are conducted on servers.
		L2-D4	Penetration tests (tests for vulnerabilities such as cross-site scripting and SQL injection) are conducted on web applications in development phase.
	Operation	L2-O1	Security vulnerability related information is gathered and analyzed periodically, and measures have been taken. Security files, such as virus definition files of antivirus software, are updated appropriately.
		L2-O2	Security education, taking phishing into consideration, is conducted for users.
LV1	Development	L1-D1	Security review is conducted for source codes.