International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:2, No:10, 2008

Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers

Toshihiko Takemura, Makoto Osajima, and Masatoshi Kawano

Abstract**—**This paper includes a positive analysis to quantitatively grasp the relationship among vulnerability, information security incidents, and the countermeasures by using data based on a 2007 questionnaire survey for Japanese ISPs (Internet Service Providers). To grasp the relationships, logistic regression analysis is used. The results clarify that there are relationships between information security incidents and the countermeasures. Concretely, there is a positive relationship between information security incidents and the number of information security systems introduced as well as a negative relationship between information security incidents and information security education. It is also pointed out that (especially, local) ISPs do not execute efficient information security countermeasures/investment concerned with systems, and it is suggested that they should positively execute information security education. In addition, to further heighten the information security level of Japanese telecommunication infrastructure, the necessity and importance of the government to implement policy to support the countermeasures of ISPs is insisted.

Keywords**—**Information security countermeasures, information security incidents, internet service providers, positive analysis

I. Introduction

INFORMATION and Communication Technology (Abbreviation, ICT) including the Internet, improves the productivity of firms, and creates new businesses. ICT provides a positive impact to society and the economy [1], [2]. On the other hand, according to an "information security white paper 2008" [3], serious problems have also occurred at the same time. These problems are caused by Internet threats such as illegal access, malware, Spam mails, and system troubles. Many accidents caused by these incidents are reported all over the world. These threats evolve hour by hour every day and increase rapidly. Moreover, vulnerability (chiefly, in Web application) has increased every year. Therefore, firms and individuals are exposed to those threats. Although secured networks, or NGNs (Next Generation Networks or New Generation Networks) have appeared recently, information security countermeasures against these threats must be executed because the Internet has no security of its own.

As academic research in the field of natural science, much research on information security as technology (cryptographic technology and secured networking) exists. This accumulated information achieves a constant result. However, Internet threats evolve minute by minute every day. Management tries to support workers against these threats, but more researches are needed. Unfortunately, research in the social sciences about how management can avoid these threats is still limited, and still exploratory. The majority of research is theoretical and uses the framework of game theory, and empirical research is limited. It is believed that many scholars are not interested in empirical research because of scant data on information security countermeasures/investment[1].

In this paper, the authors focus on telecommunication infrastructure, especially in Japanese Internet Service Providers (Abbreviation, ISPs) that provide an Internet environment for users. Considering the ISPs influence on society and the economy, the level of information security countermeasures is not necessarily uniform. In other words, the authors believe that the level of information security countermeasures in critical infrastructures should be set higher than in general firms [4], [5][2]. It is quantitatively explained the relation among information security incidents, vulnerability, and the information security countermeasures of ISPs, and effective countermeasures are suggested. To achieve this purpose, the authors used the results (micro data) of the questionnaire survey Takemura conducted in 2007, and logistic regression analysis as the statistical method.

Recently, many countries, including Japan, have begun to gather data and analyze them on information security incidents because they recognize that this kind of research is important. In Japan, the Information Security Countermesures Promotion Office was established in the Cabinet Secretariat in 2001, and the office has worked on security policy. This policy was promoted further by the reestablishment of the NISC (National Information Security Center) in 2005. Every year, the

This work is supported in part by the Telecommunications Advancement Foundation in Japan and the Ministry of Education, Culture, Sports, Science and Technology, Japan: Grant-in-Aid for Young Scientists (B) (20730196).

Toshihiko Takemura is with the Research Institute for Socionetwork Strategies, Kansai University, Osaka, 564-8680 Japan (corresponding author to provide phone: +81-66368-1111 (ext.4533); fax: +81-66330-3304; e-mail: takemura@rcss.kansai-u.ac.jp).

Makoto Osajima is with the Global Information and Telecommunication Studies, Waseda University, Tokyo, 169-0051 Japan (e-mail: osajima@aoni.waseda.jp).

Masatoshi Kawano is with the Ministry of Internal Affairs and Communications, Tokyo, 100-8926 Japan (e-mail: m-kawano@soumu.go.jp).

[1]It seems that the majority of firms might not disclose the information security countermeasure and the investment even if the data exists.

[2]Some research exists on the layer of the infrastructure and its interdependent relationship [6], [7]. In particular, the telecommunication infrastructure discussed in this paper is a critical infrastructure following the electric power infrastructure. Critical infrastructure includes the following fields; telecommunications, finance, airlines, railways, electric power, gas, government and administrative service (including the local public entity), medical treatment, water service, and distribution.

NISC implements a new national information security policy package called “Secure Japan”. In [8], “accident assumption society” are keywords, which stand for accidents that happen in the Internet society, and what information security policy the government should implement is discussed.

In addition, since 2007, there is a project of the Cyber Clean Center (Abbreviation, CCC), which MIC (the Ministry of Internal Affairs and Communications) and METI (the Ministry of Economy, Trade and Industry) in Japan has been set up to coordinate countermeasures against bot threats. The project gathers information on bots, and suggests countermeasures. Nippon Information Communications Association gathers the information on Spam mails, and suggests the countermeasures as correspondence to Spam mails. These organizations have achieved constant effects. The Information-technology Promotion Agency Japan (Abbreviation, IPA) also provides various information analyses and enlightening activities on security as well as Telecom-ISAC Japan (Telecom Information Sharing and Analysis Center Japan), National Institute of Information and Communications Technology (Abbreviation, NICT), JVN (the Japan Vulnerability Notes), JNSA (the Japan Network Security Association), and JPCERT/CC (the Japan Computer Emergency Response Team Coordination Center). Thus, in Japan, academic investigation is still rare although the accumulation of surveillance study data has advanced.

This paper consists of the following sections. Section II introduces related work. In Section III Japanese ISPs are summarized. Section IV explains logistic regression analysis and the data sets used in this paper. In Section V, the estimation results are shown. Finally, a summary and future work is presented in Section VI.

II. Related Work

In this section, the authors briefly introduce related works on information security in the fields of social science. The authors classify three types of the related works and discuss Tanaka and Matsuura’s work [9].

The first type of related work models the relations among information security incidents, information security countermeasures/investment from the viewpoint of economics and management science. Theoretical representative research includes models of Gordon and Loeb, and Varian [10], [11]. In the former, the economic effect of information security investment is theoretically analyzed, and the latter discusses the free rider problem by analyzing the information security system as public goods[3]. Under these frameworks, there are some positive analyses [14], [15].

The second type of related work models the relations between the value of the firm (market value) and information security investment/countermeasures from the viewpoint of economics and management science. The representative model is the market value model of Brynjolfsson, Hitt and Yang [1] applied to information security investment instead of ICT investment. For example, Tanaka, and Takemura carry out positive analysis using their framework [16], [17], and Nagaoka and Takemura [18] discuss a new type of model from the viewpoint of BCP (Business Continuity Plan). Moreover, in recent years many firms have paid pay attention to the information security report based on this model.

The third type of related work calculates the amount of damage and influence to economy using the frameworks of economics, business administration, and law. For instance, JNSA calculates the amount of compensation when information leakage was caused [19]. References [20]-[24] calculate the amount of GDP loss caused by Spam mails in Japan. Reference[25] gives summary on necessity of firms’ Spam mail countermeasure.

III. Summary on Japanese ISPs

In this section, the authors present a short summary on Japanese ISPs by referring to [4], [26] for investigation and research on Japanese ISPs.

The commercial use of the Internet in Japan started in around 1992, and the ISP was born. ISPs are key movers that provide the Internet environment to individuals and firms so that Japan achieves the status of an advanced ICT society. In other words, ISPs have played an important role in developing the Internet to a business platform with a social infrastructure (critical infrastructure) in only decades.

Originally, in Japan, ISPs were defined as businesses (companies) providing only a connectivity service to users. With time, the definition has changed to businesses providing various services such as applications, operations, and support services. The characteristics of Japanese ISPs differ from overseas’ ISPs. According to [4], Japanese ISPs divide the classification of ISPs into local ISPs and nationwide ISPs[4]. The former are businesses that provide service for users in a limited area or local community, and the latter provides service for users in multiple areas or a nationwide area. According to [26], a polarization in management efficiency exists between the these types of ISPs. These authors show that there are differences of financial health in the level of efficiency scores between local ISPs and nationwide ISPs. The reasons for this difference may be found in the differences in the number of potential Internet users they can cover in a service area, and the scale of capital. Concretely, the Internet Provider Association illustrates how there are only a few (nationwide) ISPs with 1% or more share of the market [27]. In addition to these providers, through a low-priced broadband strategy of Yahoo! BB in Japan, which diversified in 2000, Internet users in Japan have come to expect high quality service and low price. On the other hand, from the viewpoint of ISPs, this fact implies that the providers are taken off the market unless they provide high quality service and low price. Therefore, the financial health of many (local) ISPs has been deteriorating. Under such financial health situations, Internet threats such as Spam mails, illegal access, malware and DoS attacks have become increasing serious as social and economical problems. In addition, against the background of increasing cyber crimes, governments, firms, and individuals now demand various countermeasures such

[3]References [12] and [13] enhance the model in Gordon and Loeb [10].

[4]Reference [4] classify ISPs by viewpoints such as the management organization, too.

as the Provider Responsibility Limited Act and information security countermeasures to ISPs.

Under such a situation in Japan, Takemura conducted a questionnaire survey on the situation of information security countermeasures against Japanese ISPs in February 2007 [5]. In recent years ISPs have improved their attitudes to information security within an improvement of social consciousness. Although ISPs still have a problem of capital and a human resource shortage, they recognize social corporate responsibility (CSR) and act under this recognition. Nevertheless, some problems such as users' convenience and legal interpretations for role of ISPs in society still exist. For example, some ISPs are confused with guidelines concerned with information security, and these ISPs cannot execute information security countermeasures for the users' convenience.

Though many ISPs execute various information security countermeasures, information security accidents still occur (some ISPs encounter information security incidents). the reasons for some of these incidents in the following sections are discussed. In the next section, based on the results of the questionnaire survey in [5], the authors statistically analyze the relationships in risk factors that ISPs encounter with information security incidents.

IV. Framework

A. Model

The purpose of this paper is to clarify quantitatively the relationships among information security incidents, information security countermeasures, and vulnerability. By clarifying the relationships, the authors can discuss which factors reduce the risk that ISP s will encounter information security incidents. In other words, the authors provide suggestions about what efficient countermeasures are available.

For a long time, logistic regression (or multiple logistic regression) has been widely used as a statistical method for grasping the relationships among explanatory variables and explained variables in various fields such as psychology, sociology, economics, and business administration. In logistic regression, an explained variable is a probability that a certain event happens p, and explanatory variables are co-variables that influence p. Note that p follows logit distribution, $\text{logit}(p) = \log(p/1-p)$.

In this paper, a logistic regression is used and the authors build their model. The authors build the model showing which factors such as vulnerabilities and information security countermeasures influence the risk that ISPs encounter in information security incidents. The relationship is described by using (1).

$$\log(p_j/1-p_j) = a + b_V X_V + b_C X_C + cZ_C, \qquad (1)$$

where p_j represents the probability that ISPs encounter information security incident j, and X_V, X_C and Z_C represent vulnerability, information security countermeasure, and characteristics of ISPs, respectively.

The explained variable on the left side of (1) represents a logarithm odds ratio. This can be interpreted as one of the risk indices[5]. Also, the coefficient parameter of each explanatory variable on the right side represents a logarithm odds ratio when the explanatory variable increases one unit. For example, this increase implies that the risk that ISPs encounter information security incident j becomes $\exp[b_V]$ times when X_V increases one unit.

By using this model, the authors can discuss which countermeasures ISPs can use to reduce the risks that they encounter from an information security incident. At the same time, the risk that each ISP faces are able to be evaluated.

Combining vulnerability with various threats such as artificial mistakes creates the risk that a user may encounter as an information security incident. Vulnerability is one of the factors that raise risk. This implies that the coefficient parameter of X_V in (1) is positive; $b_V > 0$.

Generally, information security countermeasures are executed to reduce the risk that a user encounters an information security incident. Therefore, the coefficient parameter of X_C in (1) is negative; $b_C < 0$. It is assumed that information security countermeasures are roughly divided into technical information security countermeasures and non-technical information security countermeasures. The former introduces and operates various information security systems, and the latter manages countermeasures such as information security education and reminder of information security incident to users. In this paper, the authors focus on two kinds of information security countermeasures, and they see the effects of both. It is particularly interested in countermeasures concerned with management.

The authors use the difference of areas providing service as characteristics of ISPs. The reason for different areas is the differences in the financial health between local ISPs and nationwide ISPs, as discussed in Section II. It is assumed that the possibility of differences causes the difference of the risks encountered by information security incidents[6].

Finally, the authors introduce methods and processes to estimate coefficient parameters in (1), and to evaluate the fitness of their model.

To estimate each coefficient parameter in (1), the general maximum likelihood estimation method based on a binominal distribution are used. Because calculating the estimation is too complex, SPSS are used as a statistical computer software in this paper[7]. SPSS has a) a method by compulsion inserting explanatory variables, b) a variable increase (decrease) method by likelihood ratio, c) a variable increase (decrease) method by Wald, and d) a conditional variable increase (decrease) method as a method of variable selection. From these methods, the authors apply the variable increase (decrease) method by likelihood ratio as a method of variable selection in this paper. This method is often used as one of the most preferable indices.

Next, the Hosmer-Lemeshow test to evaluate the fitness of

[5] An odds ratio is a statistical measurement showing the odds of an event occurring in one group to the odds of it occurring in another group.

[6] Reference [17] points out that because the financial health of local ISPs have deteriorated, they might not execute enough information security countermeasures.

[7] SPSS version 16.0J for Windows, SPSS, Inc. is used.

the model is run. Note that the null hypothesis of this test H_0 is that the model is well suited[8]. In addition, the authors evaluate the validity of the model by using a positive distinction rate, which forecasts this model correctly[9].

B. Dataset

Takemura conducted the mailing questionnaire survey for ISPs in Japan from February to March 2007[10]. As a result, they received answers from 63 ISPs (the recovery percentage was about 10.3%). The purpose of this questionnaire was to clarify the realities regarding information security countermeasures of Japanese ISPs. Overall, the contents included the general business conditions of ISPs, the situation of the information security countermeasure, the situation of the information security incidents, and opinions toward government. The authors use a part of the results and analyze them below[11].

1) Information Security Incidents: As information security incidents, the authors used the following: illegal access, computer viruses and worms, and system trouble. Although the authors set four outcomes on information security incidents in the questionnaire survey, the authors replaced them with binary outcomes (whether or not ISPs encounter information security incidents) as follows[12]:

For $j = IA, CV$, and ST,

$$p_j = \begin{cases} 1 & \text{if ISP encounters information security incident } j, \\ 0 & \text{Otherwise,} \end{cases}$$

where IA, CV, and ST are illegal access, computer viruses and worms, and system trouble, respectively.

In Fig. 1, conditions on each information security incident are shown.

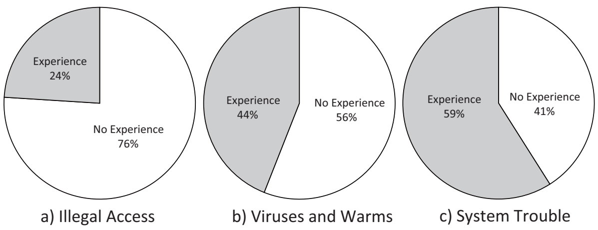

Fig. 1. Conditions on Information Security Incidents

From Fig. 1, it is found that the rate of ISPs that encounter system trouble is about 59%, and at least one or more system troubles occurred in more than half of the ISPs. According to [5], the rate of crashes in all ISPs systems was about 6%.

For reference, the authors calculate the odds ratio between risks (probability) that ISPs encounter at each information security incident. The results are shown in Table I. It is found that the risk is not mutually independent. From these results, it is clear that discussing efficient countermeasures against information security incidents is needed.

TABLE I
ODDS RATIO BETWEEN INFORMATION SECURITY INCIDENTS

	Illegal Access	Computer Virus and Warms	System Trouble
Illegal Access	—	9	19
Computer Virus and Warms	1/9	—	3
System Trouble	1/19	1/3	—

2) Vulnerability: In this paper, the authors use the following two vulnerability indices; one is the number of users as a proxy variable of the vulnerability caused by the users, and the other is the number of servers as a proxy variable of the vulnerability caused by vulnerabilities of Web application and/or computer software and programs[13].

The number of users and servers vary greatly in scale among ISPs; that is, these distributions are too large. Therefore, the authors control the model by taking their logarithm[14]. Therefore, vulnerability $X_{V,m}$ is the following:

For $m = U$ and S,

$$X_{V,m} = \log(m)$$

where U and S represent the number of users and the number of servers, respectively.

Table II shows a descriptive statistics on the number of users and servers.

TABLE II
DESCRIPTIVE STATISTICS ON THE NUMBER OF USERS AND SERVERS

	Mean	Standard Deviation	Skewness	Kurtosis
$X_{V,U}$	8.121	1.917	-1.019	2.134
$X_{V,S}$	2.814	1.314	0.056	-0.435

3) Information Security Countermeasures: The number of introduced information security systems as a technical information security countermeasure index are used. The kinds of systems are six: 1) a firewall (FW), 2) an Intrusion Detection System (IDS), 3) an Intrusion Prevention System (IPS), 4) a virus check on the Web, 5) setting a DMZ segment, and 6) the others. On the other hand, the following four indices are used as a non-technical information security countermeasure index: 1) information security education, 2) reminder of information security incident to users, 3) a penetration test, and 4), a system audit. The non-technical information security countermeasure indices are given by binary choices (whether or not the ISP executes the information security countermeasure) as follows:

[8] Refer to [28] about details of this test.

[9] The higher the positive distinction rate, the more correctly the model is forecasted. Therefore, this model is said to be preferable.

[10] Strictly speaking, Takemura conducted this questionnaire survey to ISPs in the Internet Service Provider Association, Japan.

[11] This questionnaire survey has other data including the data used in this paper. Refer to [5] about these results in the questionnaire survey.

[12] The four outcomes are the following; 1) nothing, 2) there is a network fault, but servers are not downed, 3) some servers are downed, and 4) the entire system crashes.

[13] There are data on the number of individuals and firms, separately. First, the authors tried to estimate coefficient parameters in (1). Unfortunately, they could not find a significant result. Therefore, in this paper the authors use data on the sum of the number of individual users and firm users. The number of users can be considered as not only a proxy variable of the vulnerability, but also the scale of the ISP.

[14] Reference [15] use mail accounts as a proxy variable of the vulnerability.

International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:2, No:10, 2008

For $k = EDU, RU, PT$, and SA,

$$X_{C,k} = \begin{cases} 1 & \text{if ISP executes the countermeasures } k, \\ 0 & \text{otherwise,} \end{cases}$$

where EDU, RU, PT, and SA represent information security education, reminder of information security incident to users, the penetration test, and the system audit, respectively.

Table III shows descriptive statistics on the number of introduced security systems, and Fig. 2 shows conditions on each information security countermeasure.

TABLE III
DESCRIPTIVE STATISTICS ON THE NUMBER OF INTRODUCED SECURITY SYSTEMS

	Mean	Standard Deviation	Skewness	Kurtosis
$X_{C,NS}$	2.480	1.424	-0.072	-0.811

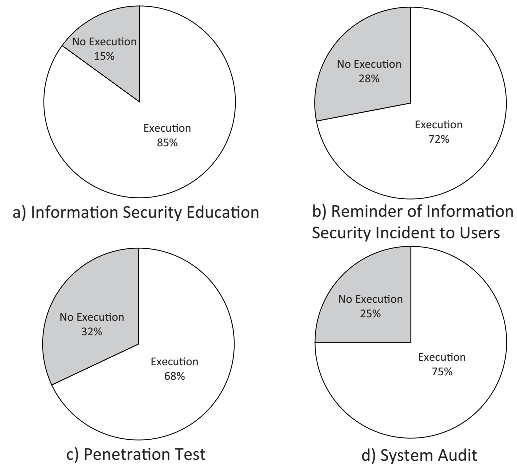

Fig. 2. Conditions on Information Security Countermeasures

4) Characteristics of ISPs: The authors use the differences of the areas providing service as characteristics of the ISPs. In other words, this index shows whether the ISP is local or nationwide. Concretely,

$$Z_C = \begin{cases} 1 & \text{if ISP is nationwide,} \\ 0 & \text{if ISP is local.} \end{cases}$$

Fig. 3 shows the rates of local ISPs and nationwide ISPs.

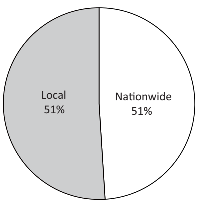

Fig. 3. Local ISPs and Nationwide ISPs

V. ESTIMATION RESULTS

Before logistic regression, the authors examine (rank) the correlations among explanatory variable correlations. Unless the variables are mutually independent, the authors cannot run logistic regression. Table IV shows the rank correlation coefficient of explanatory variables because many explanatory variables are discrete.

TABLE IV
CORRELATION COEFFICIENT OF EXPLANATORY VARIABLES

	$X_{V,U}$	$X_{V,S}$	$X_{C,NS}$	$X_{C,EDU}$	$X_{C,RU}$	$X_{C,SA}$	$X_{C,PT}$	Z_C
$X_{V,U}$	—	0.216	-0.076	0.211	0.177	-0.035	0.168	-0.092
$X_{V,S}$	0.216	—	0.223	0.123	0.268	0.189	0.173	0.281
$X_{C,NS}$	-0.076	0.223	—	0.313	0.333	0.323	0.139	-0.042
$X_{C,EDU}$	0.211	0.123	0.313	—	0.338	0.093	0.209	0.080
$X_{C,RU}$	0.177	0.268	0.333	0.338	—	0.196	0.090	0.090
$X_{C,SA}$	-0.035	0.189	0.323	0.093	0.196	—	0.365	0.093
$X_{C,PT}$	0.168	0.173	0.139	0.209	0.090	0.365	—	0.145
Z_C	-0.092	0.281	-0.042	0.080	0.090	0.093	0.145	—

It is easily found that each rank correlation coefficient is far less than 1. Therefore, the authors can use these data for their analysis as explanatory variables.

Next, the authors divide estimation results in some cases and estimate the coefficient parameters in (1). Hereafter, the results are sequentially shown. Unfortunately, the authors cannot attain significant results using the risks that ISPs encounter with virus and worm accidents as an explained variable. Therefore, the authors omit these cases in this paper.

A. Illegal Access

In Tables V-VII, the authors show the explained variables, which are the estimation results using the risk that ISPs encounter with illegal access accidents. Note that in Table V both the numbers of users and servers are used as the vulnerability index. In Table VI, the authors use only the logarithm of the number of users as the vulnerability index

TABLE V
ESTIMATION RESULT I

	Estimated Coefficient Parameter (B)	Standard Error	Wald	Significance probability	exp[B]
$b_{C,NS}$	1.755	0.789	4.956	0.026	5.686
$b_{C,EDU}$	-4.515	1.966	5.272	0.022	0.011
Constant term	-2.108	1.436	2.155	0.142	0.121
	7 Steps Chi-square(5)=2.556 [0.768] Positive distinction rate: 80.6%				

TABLE VI
ESTIMATION RESULT II

	Estimated Coefficient Parameter (B)	Standard Error	Wald	Significance probability	exp[B]
$b_{C,NS}$	1.373	0.533	6.641	0.010	3.947
$b_{C,EDU}$	-3.659	1.555	5.539	0.019	0.026
Constant term	-1.971	1.148	2.947	0.086	0.139
	6 Steps Chi-square (5)=2.059 [0.841] Positive distinction rate: 76.3%				

TABLE VII
ESTIMATION RESULT III

	Estimated Coefficient Parameter (B)	Standard Error	Wald	Significance probability	exp[B]
$b_{V,S}$	0.732	0.423	2.996	0.083	2.079
$b_{C,NS}$	0.893	0.459	3.791	0.052	2.443
$b_{C,EDU}$	-2.833	1.254	5.101	0.024	0.059
Constant term	-3.428	1.609	4.538	0.033	0.032
	5 Steps Chi-square (8)=2.990 [0.935] Positive distinction rate:82.9%				

and they use only the logarithm of the number of servers as the index in Table VII. Chi-square in each Table is used to run the Hosmer-Lemeshow test.

In Tables V-VII, it is found that it is common to the results that the estimated coefficient parameter of the number of countermeasures, $b_{C,NS}$, is positive, and the estimated coefficient parameter of the information security education, $b_{C,EDU}$, is negative. Both parameters are statistically significant. Oppositely, variables such as the logarithm of the number of users, reminder of information security incident to users, the system audit, the penetration test, and the area providing service were not selected as inappropriate variables during the process of the logistic regression. In addition, the coefficient parameter of the logarithm of the number of users, $b_{V,S}$, in Table VII becomes positive at a 10% significance level.

From the results of the Hosmer-Lemeshow test, the authors can evaluate how these models are fit to some degree because each model has a 5% or more significance level. In addition , because the positive distinction rate is at a level between 76.3 and 82.9%, it is insisted that the models are valid.

B. System Trouble

In Tables VIII and IX, the estimation results using the risk that ISPs encounter system trouble as explained variables are shown. Note that in Table VIII the authors use both the numbers of users and servers as the vulnerability index and they use only the logarithm of the number of users as the vulnerability index in Table IX. In the case using the logarithm of the number of servers as the vulnerability index, the authors cannot gain significant results. Thus, the results are omited.

TABLE VIII
ESTIMATION RESULT IV

	Estimated Coefficient Parameter (B)	Standard Error	Wald	Significance probability	exp[B]
$b_{V,U}$	0.534	0.290	3.397	0.065	1.706
$b_{C,NS}$	1.085	0.587	3.420	0.064	2.959
$b_{C,EDU}$	-3.562	1.719	4.295	0.038	0.028
$b_{C,PT}$	-1.915	1.201	2.543	0.111	0.147
c	2.886	1.303	4.906	0.027	17.918
Constant term	-5.110	3.091	2.733	0.098	0.006
	3 Steps Chi-square (7)=3.730 [0.881] Positive distinction rate: 80.6%				

TABLE IX
ESTIMATION RESULT V

	Estimated Coefficient Parameter (B)	Standard Error	Wald	Significance probability	exp[B]
$b_{C,NS}$	0.522	0.292	3.192	0.074	1.685
$b_{C,EDU}$	-1.968	1.220	2.604	0.100	0.140
Constant term	0.877	1.169	0.563	0.453	2.403
	6 Steps Chi-square (5)=7.659 [0.176] Positive distinction rate:73.7%				

In Tables VIII and IX,it is found that it is common to the results that the estimated coefficient parameter of the number of countermeasures, $b_{C,NS}$, is positive, and the estimated coefficient parameter of the information security education, $b_{C,EDU}$, is negative. Both parameters are statistically significant. Oppositely, variables such as the logarithm of the number of servers, reminder of information security incident to users, and the system audit were not selected as inappropriate variables during the process of the logistic regression. In addition, the coefficient parameters of the logarithm of the number of users, $b_{V,S}$, the penetration test, $b_{C,PT}$, and the area providing service, c, in Table VIII become positive (at a 10% significance level) and negative (but statistically significant), respectively.

From the results of Hosmer-Lemeshow test, the authors can evaluate how these models are fit to some degree because each model has a 5% or more significance level. In addition to these results, because the positive distinction rate is at a level between 73.7 and 80.6%, the authors can insist that their models are valid.

C. Personal Opinions of Estimated Results

The estimated results in the previous subsection are interesting. First, the number of introduced information security systems and information security education show that the estimated coefficient parameters are statistically significant and the same sign through all models. The former is positive and the latter is negative. The former means that the more ISPs introduce information security systems, the higher the risk will be that they will encounter information security incidents[15]. On the other hand, the latter means that the more positively ISPs execute information security education, the lower the risk will be. If the education is executed more positively, the risk can be reduced.

Generally, many people think that the risk would be reduced if ISPs introduce various information security systems. Of course, when network security (countermeasures) against Internet threats is discussed, systems such as FW and IDS play an important role and they are needed. However, the former result throws doubt on this thinking. This result is interpreted as follows. First, ISPs may tend to hesitate on investment on information security countermeasures and use old information security systems because the amount of investment is vast. This fact is pointed out in [17]. Therefore, there is a possibility that the old systems will not be able to correspond to present threats. Next, even if ISPs introduce the recent systems, the various systems may be not efficiently operated because ISPs have few employees of a high technical level, such as system administrators[16]. Third, including ISPs that had encountered an information security incident, the causal relation might be reversed. In other words, the higher the risk becomes that ISPs encounter information security incidents, the more ISPs introduce information security systems. If these possibilities exist, coefficient parameters of the number of introduction systems can be considered intentionally positive.

Moreover, it seems that the result that executing information security education reduces the risk has the great meaning. Though costs are necessary to execute information security education, the cost-benefit is higher than introducing information security systems in the long term. The reason is that executing information security education is effective (reduces the risk that ISPs encounter information security incidents), and is covered by management only to some degree.

Reference [5] reported that in information security education, etiquette on the Internet, knowledge about not only viruses and worms, but also the knowledge about security laws, and correspondence in emergencies were discussed[17]. The information security education is executed with not only prior countermeasures, but also posterior countermeasures in mind. Moreover, according to [5], the ratio of ISPs planning to execute information security education in the future is over 95%. In other words, many ISPs intend to execute information security education. It expected that the risk of ISPs encountering information security incidents will be reduced in the future.

As part of the results, the estimated coefficient parameters of the logarithm of the number of servers and users are positive. These results imply that these vulnerabilities heighten the risk that ISPs encounter information security incidents, and these results are consistent with the theoretical consideration in Section IV-A[18]. In addition, the authors confirm that some countermeasures are not effective now because their coefficient parameters are not statistically significant. In Table VIII, the estimated coefficient parameter of the area providing service is positive. That is, nationwide ISPs have a higher risk than local ISPs that they will encounter system trouble. The reason may be that the systems and networks they handle are too complex and widespread. At first it is assumed that local ISPs have a higher risk rather than nationwide ISPs. However, the results overrule the auhors' initial intuition.

VI. Concluding Remarks and Future Work

Purpose of this paper has been to quantitatively clarify the relation among information security incidents, information security measures, and vulnerability. The authors have used positive analysis to do this by using data on a 2007 questionnaire survey for Japanese ISPs and logistic regression analysis as their statistical method. As a result, it is found that there are statistically significant relations between information security incidents and some information security countermeasures. Concretely, the relation between information security incidents and the number of introduced information security systems (resp. information security education) is positive (resp. negative). The results mean that the risk would rise if the number of introduced information security systems increases, and the risk would decrease if information security education were executed. The results are valid and provide important information when considering the financial health of ISPs. That is, the timing of countermeasures and investments that correspond to their financial health is key, and information security education that is a non-technological countermeasure is also efficient. Therefore, the authors believe that information security education should be enhanced to maintain a higher security level. This higher information security level cannot be achieved by the IPSs alone, because these ISPs need to cooperate with the government. Particularly efficient policy recommendations discussed at the seminar on information security showed that IPA, JNSA, and/or JPCERT/CC should cooperate with governmental offices such as the METI as well as the MIC in Japan. In addition, the government should put out united guidelines on information security, instead of many different kinds of the guidelines from different ministries. Moreover, seminars concerning policy recommendations should be held regularly. This idea of holding seminars on security countermeasures also applies to general firms, of course. In the future, it is expected that NISC will play an important role in coordinating information security policies among ministries, and should implement such policies with unions [29].

To discuss deeply the effect of a number of information security systems introduced in this paper, the authors need to check the causal relation with information security incidents. This will be one of the authors' future endeavors. In addition, the authors will continue to research the social and

[15] This result might represent an opposite causal relation. That is, the higher the risk, the more ISPs will introduce information security systems. The authors want to discuss this relation further in the future.

[16] The authors believe that enough effects cannot be demonstrated unless the system is introduced to employees such as the SE (System Engineer) who has enough knowledge.

[17] Reference [5] asks the question about two types who receive the information security education; 1) all employers and employees, and 2) only engineers.

[18] The estimated coefficient parameter of penetration test, $b_{C,PT}$, in Table VIII is negative, but the parameter is not statistically significant at a10% level.

economic effects of information security countermeasures and investment, and help to accumulate research on the economics of information security.

ACKNOWLEDGMENT

The authors are grateful to Toru Muneoka (Professor, Kansai University, Japan), Hiroyuki Ebara (Associate Professor, Kansai University, Japan), Shota Moriwaki (Associate Professor, Takushoku University, Japan), Muneki Yokomi (Lecturer, Osaka University of Commerce, Japan), and Taiyo Maeda (Post Doctral Fellow, Kansai University, Japan). The authors also express their gratitude to the ISPs who cooperated with their survey. The remaining errors are the authors.

REFERENCES

[1] E. Brynjolfsson, L. Hitt and S. Yang, "Intangible assets: how the interaction of computers and organizational structure affects stock market valuations," *Brookings Papers on Economic Activity: Macroeconomics*, vol.1, pp.137-199, 2002

[2] T. Takemura, *Economic analysis on information and communication technology*. Tokyo: Taga-shuppan, 2008.

[3] Information-technology Promotion Agency, *Information security white paper 2008*. Tokyo: Jikkyo Shuppan, 2008.

[4] H. Ebara, A. Nakaniwa, T. Takemura and M. Yokomi, *Empirical analysis for internet service providers*. Tokyo: Taga-shuppan, 2006.

[5] T. Takemura, "The 2nd investigation of actual conditions report on information security countermeasures for internet service providers," Kansai University, 2007.

[6] Information-technology Promotion Agency (2000, January). Investigation report: case study of information security countermeasures in critical infrastructure. [Online]. Available: http://www.ipa.go.jp/security/fy11/report/contents/intrusion/infrasec_pts/infrasec_pj.pdf

[7] S. Yamaguchi (2007, February). Expectation for academic society. *JSSM Security forum distributed material*. [Online]. Available: http://www.jssm.net/

[8] National Information Security Center (2008, June). Secure Japan 2008: concentrated approach for strengthening information security base. [Online]. Available: http://www.nisc.go.jp/active/kihon/pdf/sj_2008_draft.pdf

[9] H. Tanaka and K. Matsuura, "Empirical analysis at firm level on economical incentive of information security investment," *Research investigation reports (The Telecommunications Advancement Foundation)*, vol.21, pp.9-16, 2006.

[10] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," in *ACM Transactions on Information and System Security*, vol.5, pp.438-457, 2002.

[11] H. R. Varian, "System Reliability and Free Riding," in *ACM Transactions on Information and System Security*, vol.5, pp.355-366, 2002.

[12] L. A. Gordon, M. P. Loeb and W. Lycyshyn, "Sharing information on computer systems security: an economic analysis," *Journal of Accounting and Public Policy*, vol.22 (6), pp.461-485, 2003.

[13] L. A. Gordon and M. P. Loeb, "Expenditures on competitor analysis and information security: a managerial accounting perspective," in *Management Accounting in the Digital Economy*, A. Bhimni Ed., Oxford: Oxford Univ Press, 2003, pp.95-111.

[14] H. Tanaka, K. Matsuura and O. Sudoh, "Vulnerability and information security investment: an empirical analysis of e-local government in Japan," *Journal of Accounting and Public Policy*, vol.24 (1), pp.37-59, 2005.

[15] W. Liu, H. Tanaka and K. Matsuura, Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms, *Information Processing Society of Japan Digital Courier*, vol.3, pp.585-599, 2007.

[16] H. Tanaka, "Information security as intangible assets: a firm level empirical analysis on information security investment, *Journal of information studies (The University of Tokyo)*, vol.69, pp.123-136, 2005.

[17] T. Takemura, "Proposal of information security policy in telecommunication infrastructure," in *What is socionetwork strategies*, T. Murata and S. Watanabe Eds. Tokyo: Taga-shuppan, 2007, pp.103-127.

[18] H. Nagaoka and T. Takemura, "A business continuity plan to heighten enterprise value," in *the Proceedings of 55th National Conference (Japan Society for Management Information)*, Nagoya, Japan, 2007, pp.149-152.

[19] Japan Network Security Association (2008, July). Fiscal 2006 information security incident survey report (information leakage: projected damages and observations). [Online]. Available: http://www.jnsa.org/en/reports/incident.html

[20] Y. Ukai and T. Takemura (2007, March). Spam mails impede economic growth. *The Review of Socionetwork Strategies*, vol.1 (1), pp.14-22. [Online]. Available: http://www.springerlink.com/

[21] T. Takemura and H. Ebara, "Spam mail reduces economic effects," in *the Proceedings of the 2nd International Conference on the Digital Society*, Martinique, 2008, pp.20-24.

[22] T. Takemura and H. Ebara, "Economic loss caused by spam mail in each Japanese industry," presented at the 1st International Conference on Social Science, Izmir, Turkey, 2008.

[23] T. Takemura and H. Ebara, "Estimating economic losses caused by spam mails through production function approach," *Journal of International Development*, to be published.

[24] Nippon Information Communications Association (2008, March). Inspection slip of Influence That Spam Mail Exerts on Japanese Economy. [Online]. Available: http://www.dekyo.or.jp/

[25] T. Takemura, M. Osajima and T. Maeda, "The impact of mail security countermeasure in firms," in *the Proceedings of 57th National Conference (Japan Society for Management Information)*, Miyazaki, Japan, 2007, to be published.

[26] M. Yokomi, H. Ebara, A. Nakaniwa and T. Takemura, "Evaluation of technical efficiency for internet providers in Japan: problems for regional providers," *Journal of Public Utility Economics*, vol.56(3), pp.85-94, 2004.

[27] Internet Provider Association, *Actual conditions on investigation of nationwide internet services 2003*. Tokyo: Internet Provider Association, 2003.

[28] D. W. Hosmer and S. Lemeshow, *Applied Logistic Regression* (2nd ed.). New York: Wiley-Interscience publication, 2000.

[29] T. Takemura and M. Osajima, "About some topics on countermeasures and policies for information security incidents in Japan," *GITI Research Bulletin 2007-2008*, to be published.

Toshihiko Takemura Toshihiko Takemura was born in Osaka, Japan. He is received his Bachelor Degree (1998) in Informatics from Kansai University, and his Master Degree (2002) in Economics and Ph.D. (2006) in Applied Economics, from Osaka University. He is an assistant professor of the Research Institute for Socionetwork Strategies, Kansai University. His research interests include economics of information security, ICT economics, and microeconometrics. He is a member of the Japanese Economic Association, Japan Society of Public Utility Economics, Japan Society for Management Information, and Japan Economic Policy Association.

Makoto Osajima Makoto Osajima is received his Bachelor Degree (1992) in Politics from Waseda University. He is visiting associate professor of Graduate School of International Telecommunications Studies, Waseda University and former visiting scholar of Asia Pacific Research Center, Stanford University. He is also a staff of Ministry of Internal affairs and Communications of Japan and has been working for ICT policy planning and regulations from 1992. He is a member of Japan Society for Management Information.

Masatoshi Kawano Masatoshi Kawano was born in Kyoto, Japan. He received his Bachelor Degree (1993) and Master Degree (1995) in Electronics from Kyoto University, and Master Degree (1998) in Engineering Economics Systems and Operations Research from Stanford University. He had been working for NISC (National Information Security Center) for around two years and been engaged in policy planning and coordination in Information Security in the Goverment of Japan.