# Economic Analysis on Information Security Incidents and the Countermeasures: The Case of Japanese Internet Service Providers

Toshihiko Takemura[1], Makoto Osajima[2] and Masatoshi Kawano[3]
*[1] RISS, Kansai University*
*[2] GITS, Waseda University*
*[3]The Ministry of Internal Affairs and Communications*
*Japan*

## 1. Introduction

Information and Communication Technology (Abbreviation, ICT) including the Internet, improves the productivity of firms, and creates new businesses. Concretely, it is found that ICT provides a positive impact to society and the economy (Brynjolfsson et al., 2002, and Takemura, 2008).

On the other hand, according to an information security white paper 2008 in Japan (Information-technology Promotion Agency, 2008), serious problems have 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 minute by minute every day and the number of them increases rapidly. Moreover, the number of vulnerabilities (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.

We have much academic researches on information security technology in the field of natural science such as cryptographic technology and secured networking[1]. These accumulated researches achieve a constant result. However, Internet threats evolve minute by minute every day. Information security management tries to support workers against these threats. Unfortunately, research in the social sciences about how management can avoid these threats is still limited and exploratory. The majority of researches are theoretical ones, which use the framework of game theory, and ones on management system. On the other hand, empirical researches on information security are limited. We believe that many

[1] For example, refer to Cook and Keromytis (2006) in details of recent researches on cryptographic technology.

scholars were not interested in empirical research still now because of scant data on information security countermeasures and/or investment[2]. Recently, the number of empirical researches tends to increase since the data are accumulated.

In this chapter, we focus on firms in telecommunication infrastructure, especially Japanese Internet Service Providers (Abbreviation, ISPs) that provide Internet environment for users in Japan[3]. From the ISPs' influence on society and economy, they continue to maintain the high level of information security countermeasures. In other words, the level of information security countermeasures in critical infrastructures should be set higher than in general firms (Ebara et al., 2006, and Takemura, 2007a)[4]. In this paper, we investigate the relation among information security incidents, vulnerability, and the information security countermeasures of ISPs, and we show what effective countermeasures are available. To achieve this purpose, we use the micro data on the questionnaire survey we 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 these kinds of researches are important. In Japan, the Information Security Measures Promotion Office was established in the IT strategy headquarters of 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 NISC implements a new national information security policy package called "Secure Japan". In National Information Security Center (2008), "accident assumption society" is one of 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[5]. The project gathers information on bots, and suggests the countermeasures. The information on Spam mails are gathered by Japan Data Communications Association (Abbreviation, JADAC) in Japan, and spam mails countermeasures are discussed. The Information-technology Promotion Agency,

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

[3] Refer to Ebara et al. (2006) and Yokomi et al. (2004) for investigation and research on Japanese ISPs.

[4] Some researches exist on the layer of the infrastructure and its interdependent relationship (Information-technology Promotion Agency, 2000, and Yamaguchi, 2007). In particular, the telecommunication infrastructure is a second important critical infrastructure among all infrastructures. Critical infrastructure in Japan 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.

[5] Bot (virus) is a malicious program with the purpose of fraudulent use of computer. Once computer is infected with bot, the malicious attacker remotely controls your computer from the external. This attack causes serious harm of making public nuisance such as sending numerous number of mails and attacking a particular website, as well as of stealing information stored in your computer, i.e., spying activities.

Japan (Abbreviation, IPA) also provides various information analyses and enlightening activities on security as well as the Japan Vulnerability Notes (Abbreviation, JVN), the Japan Network Security Association (Abbreviation, JNSA), and the Japan Computer Emergency Response Team Coordination Center (Abbreviation, JPCERT/CC). In addition, the National Police Agency (Abbreviation, NPA) in Japan controls the cybercrime. These organizations have achieved constant effects. Thus, in Japan, academic investigation is still rare although the accumulation of surveillance study data has advanced.

Table 1 shows Japanese organizations concerned with information security countermeasures and policies.

| | URL | Remark |
|---|---|---|
| NISC | http://www.nisc.go.jp/ | Security policy |
| MIC | http://www.soumu.go.jp/ | Security policy |
| METI | http://www.meti.go.jp/ | Security policy |
| CCC | https://www.ccc.go.jp/ | Bot |
| JADAC | http://www.dekyo.or.jp/ | Spam mail |
| IPA | http://www.ipa.go.jp/ | Virus and warm |
| JVN | http://jvn.jp/ | Vulnerability |
| JNSA | http://www.jnsa.org/ | Network security |
| JPCERT/CC | http: www.jpcert.or.jp/ | Security incident |
| NPA | http://www.npa.go.jp/ | Cyber crime |

Table 1. Japanese Organizations Concerned with Information Security Countermeasures and Policies

This chapter consists of the following sections. Section 2 introduces some related literatures and shows topics on economics of information security. In Section 3, we summarize ISPs in Japan. Section 4 explains logistic regression analysis and the data used in this chapter. In Section 5, we show the estimation results. Finally, we present a summary and future work in Section 6.

## 2. Related Literatures

In this section, we briefly introduce related works on information security in the fields of social science.

There have been many qualitative researches on information security in the field of management science; concretely, various management systems on information security such as ISMS (information security management system), ISO27000, and BCMS (business continuity management system). However, it seemes that these researches are insufficient to give the incentive for individuals and/or firms to execute information security countermeasures.

On the other hand, in the field of economics, pioneer and representative researches on information security are Gordon and Loeb (2002), and Varian (2002). These include theoretical models of information security countermeasures and investment from the viewpoint of economics and management science. In addition, they discuss the incentive to execute information security countermeasures. In the former, the economic effect of information security investment is analyzed and the latter discusses the free rider problem by analyzing the information security system as public goods[6]. Under these frameworks, some empirical analyses have been accumulated after around 2000.

Mainly, we classify three types of the related works.

1. The first type of related work is modeling relations among information security incidents, information security countermeasures and/or investment. For example, there are a few empirical researches such as Tanaka et al. (2005), Liu et al. (2007), Takemura (2007b) and Takemura et al. (2008) in Japan. Our research in this chapter is included in this type.
2. The second type of related works is modeling relations between the value of the firm (market value) and information security countermeasures and/or investment. The representative model is the market value one of Brynjolfsson et al. (2002) applied to information security investment instead of ICT investment. For example, in Japan, Tanaka (2005), Takemura and Minetaki (2009a, 2009b) and Minetaki, et al. (2009) carry out empirical analysis by using their framework, respectively. In addition, Nagaoka and Takemura (2007) discuss a new type of model from the viewpoint of BCP (business continuity plan)[7]. Moreover, in recent years many firms have paid pay attention to the information security report based on this model.
3. The third type of related works is calculating the amount of damage and influence to economy and society. For instance, JNSA calculates the amount of compensation when information leakage was caused (Japan Network Security Association, 2008). Ukai and Takemura (2007), Takemura and Ebara (2008a, 2008b, 2008c), and Japan Data Communications Association (2008) calculate the amount of GDP loss caused by Spam mails in Japan.

## 3. Summary on Japanese ISPs

In this section, we present a short summary on Japanese ISPs by referring to Ebara et al. (2006) and Yokomi et al. (2004) for investigation and research on Japanese ISPs.

The commercial use of the Internet in Japan started in around 1992, and then Japanese ISPs were born. ISPs are key movers that provide the Internet environment to individuals and firms (users). They help 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 about two decades.

Originally, in Japan, ISPs were defined as businesses (companies) providing only a connectivity service to users. With time, the definition has evolved to businesses providing various services such as applications, operations, and support services. The characteristics of Japanese ISPs differ from overseas' ISPs. According to Ebara et al. (2006), Japanese ISPs divide the classification of ISPs into local ISPs and nationwide ISPs[8]. 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.

[6] Gordon, et al. (2003), and Gordon and Loeb (2006) enhances the model in Gordon and Loeb (2002).

[7] BCP is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

[8] Ebara et al. (2006) classify ISPs by viewpoints such as the management organization, too.

According to Yokomi et al. (2004), a polarization in management efficiency exists between the two classifications. We show that there are differences of financial health in the level of efficiency scores between them. They point out that 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.

The Internet Provider Association illustrates how there are only a few nationwide ISPs with 1% or more share of the market (Internet Provider Association, 2003). 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 situations, Internet threats such as Spam mails, illegal access and malware has become more serious as social and economical problems. In addition, against the background, individuals, firms and governments demand various countermeasures and compliances to ISPs[9].

Under such a situation in Japan, Takemura conducted a questionnaire survey on the situation of information security countermeasures against Japanese ISPs in February 2007 (Takemura, 2007a). He point out that in recent years ISPs have improved their attitudes to information security within an improvement of social consciousness. Although many ISPs still have a problem of capital and a human resource shortage, they recognize social corporate responsibility (Abbreviation, CSR) and act under this recognition[10]. 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). We discuss the reasons for some of these incidents in the following sections. In the next section, based on the micro data of the questionnaire survey in Takemura (2007a), we statistically analyze the relationships in risk factors that ISPs encounter with information security incidents.

## 4. Framework

### 4.1 Model

The purpose of this chapter is to investigate the relationships among information security incidents, information security countermeasures, and vulnerability by using a statistical method. Through the result, we can discuss which factors reduce the risk that ISPs

[9] In Takemura et al. (2009a), ratio of the individuals who consider that only ISPs should take countermeasure is about 8.9% in Japan. They conducted a Web-based survey on the Internet.

[10] CSR is a form of corporate (firm) self-regulation integrated into a business model. Ideally, CSR policy in each firm would function as a built-in, self-regulating mechanism whereby business would monitor and ensure their adherence to law, ethical standards, and international norms.

encounter information security incidents. In other words, we provide suggestions about what efficient countermeasures are available.

We adopt logistic regression analysis as the statistical method. For a long time, logistic regression (or called multiple logistic regression) has been widely used as one of the methods which grasp the relationships among explanatory variables and explained variables in various fields such as psychology, sociology, economics, and business administration. Generally, 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, *logit(p)=log(p/1-p)*.

We 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 equation (1).

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

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 equation (1) represents a logarithm of odds ratio. This can be interpreted as one of the risk indices[11]. 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 in (1), above mentioned, we can discuss which countermeasures ISPs can use to reduce the risks. At the same time, we can evaluate the risk that each ISP faces.

Combining vulnerability with various threats creates the risk that users may encounter as an information security incident. That is, vulnerability is one of the factors raising the probability of risk that they encounter. This implies that the coefficient parameter of $X_V$ in equation (1) is positive; $b_V>0$.

Generally, information security countermeasures are executed to reduce the risk that users encounter an information security incident. Therefore, the coefficient parameter of $X_C$ in equation (1) is negative; $b_C<0$. In this chapter, we roughly divide the information security countermeasures into two kinds of countermeasures; technical information security countermeasures and non-technical information security countermeasures. The former introduces and operates various information security systems and technologies, and the latter manages countermeasures such as information security education and reminder of information security incident to users. We are particularly interested in countermeasures concerned with management.

We use the service area as an attribute of ISPs. The reason is that there are the differences in the financial health between local ISPs and nationwide ISPs, as discussed in Section 3. We set up a hypothesis that the possibility of differences causes the difference of the risks

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

encountered by information security incidents[12].

Finally, here we show the processes to estimate coefficient parameters in equation (1) by using logistic regression, and to evaluate the fitness of our model.

To estimate each coefficient parameter in equation (1), we use the general maximum likelihood estimation method based on a binominal distribution. Because calculating the estimation is too complex, we use SPSS as a statistical computer software in this chapter[13]. 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, we apply the variable increase (decrease) method by likelihood ratio as a method of variable selection in this chapter. This method is often used as one of the most preferable indices.

Next, we run the Hosmer-Lemeshow test to evaluate the fitness of our model. Note that the null hypothesis of this test $H_0$ is that the model is well suited[14]. In addition, we evaluate the validity of the model by using a positive distinction rate, which forecasts this model correctly[15].

### 4.2 Dataset

We conducted the mailing questionnaire survey for ISPs in Japan from February to March 2007[16]. In this questionnaire, we received answers from 63 ISPs (the recovery percentage was about 10.3%).

The purpose of this questionnaire was to investigate the current situation 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. We use a part of the results (micro data) and analyze them below[17].

(a) Information Security Incidents

As information security incidents, we used the following: illegal access, computer viruses and worms, and system trouble. Although we set four outcomes on information security incidents in the questionnaire survey, we replaced them with binary outcomes (whether or not ISPs encounter information security incidents) as follows[18]:

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

[12] Takemura (2007b) points out that ISPs might not execute enough information security countermeasures because the financial health of local ISPs have deteriorated.

[13] We use SPSS version 17.0J for Windows, SPSS, Inc..

[14] Refer to Hosmer and Lemeshow (2000) about details of this test.

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

[16] Strictly speaking, we conducted this questionnaire survey to ISPs in the Internet Service Provider Association, Japan. You can refer to this mailing questionnaire survey by accessing http://www.kansai-u.ac.jp/riss/shareduse/data/07.pdf.

[17] This questionnaire survey has many kinds of information of ISPs. Refer to Takemura (2007a) about these results in the questionnaire survey.

[18] 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.

$$p_j = 1 \text{ if ISP encounters information security incident } j, \quad 0 \text{ otherwise} \qquad (2)$$

where *IA*, *CV*, and *ST* are illegal access, computer viruses and worms, and system trouble, respectively. $p_j$ is indicator function.
In Figure 1, conditions on each information security incident are shown.

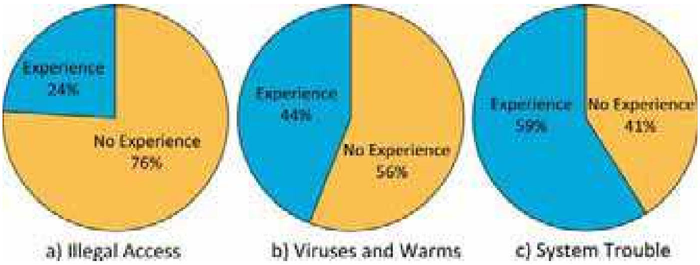

Fig. 1. Conditions on Information Security Incidents

From Figure 1, we see 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 Takemura (2007a), the rate of crashes in all ISPs systems was about 6%.
For reference, we calculate the odds ratio between risks (probability) that ISPs encounter at each information security incident. The results are shown in Table 2. We see that the risk is not mutually independent. From these results, it is clear that we need to discuss efficient countermeasures against information security incidents.

| | Illegal Access | Computer Virus and Warms | System Trouble |
|---|---|---|---|
| Illegal Access | ---------------------- | 9 | 19 |
| Computer Virus and Warms | ---------------------- | ---------------------- | 3 |
| System Trouble | ---------------------- | ---------------------- | ---------------------- |

Table 2. Odds Ratio between Information Security Incidents

(b) Vulnerability
In this chapter, we 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[19].

[19] We have data on the number of individuals and firms, separately. First, we tried to estimate coefficient parameters in equation (1). Unfortunately, we could not find a significant result. Therefore, in this chapter we use data on the total 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.

The number of users and servers vary greatly in scale among ISPs; that is, these distributions are too large. Therefore, we control the model by taking their logarithm[20]. Therefore, vulnerability $X_{V,m}$ is the following:
For $m$=$U$, and $S$,

$$X_{V,m}=log\ (m) \tag{3}$$

where $U$ and $S$ represent the number of users and the number of servers, respectively.
Table 3 shows a 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 |

Table 3. Descriptive Statistics on the Number of Users and Servers

(c) Information Security Countermeasures
We roughly divide the information security countermeasures into two kinds of countermeasures; technical information security countermeasures and non-technical information security countermeasures.
We use the number of introduced information security systems as information security technology index. The kinds of systems we assume 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. Therefore, maximum of $X_{C,NS}$ is 6 and minimum of $X_{C,NS}$ is 0.
Table 4 shows 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 |

Table 4. Descriptive Statistics on the number of Introduced Security Systems

On the other hand, we use the following four indices as a non-technical (management) 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 information security management indices are given by binary choices (whether or not the ISP executes the countermeasure) as follows:
For $k$=$EDU$, $RU$, $PT$, and $SA$,

$$X_{C,k} = \begin{array}{l} 1 \text{ if ISP executes the countermeasure } k, \\ 0 \text{ otherwise} \end{array} \tag{4}$$

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

[20] Liu et al. (2007) uses mail accounts as a proxy variable of the vulnerability.

Figure 2 shows conditions on each information security countermeasure. From Figure 2, it is found that many ISPs (the ratio is over 70%) execute management on information security.

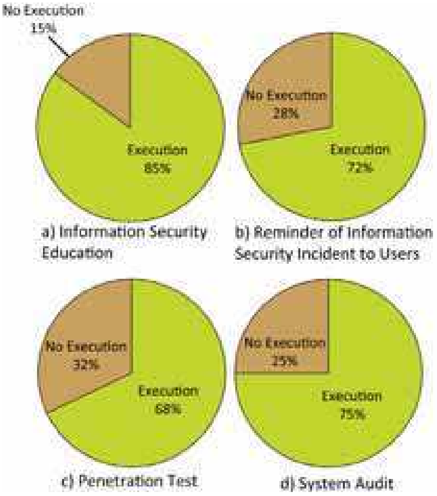

Fig. 2. Conditions on Information Security Countermeasures

(d) Attributes of ISPs

We use the service area as an attribute of ISPs. In other words, this index shows whether the ISP is local or nationwide. Concretely,

$$Z_C = \begin{cases} 1 & \text{if ISP is nationwide,} \\ 0 & \text{if ISP is local.} \end{cases} \qquad (5)$$

where $Z_C$ is an indicator function.

Figure 3 shows the ratios of local ISPs and nationwide ISPs.

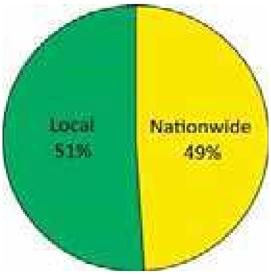

Fig. 3. Local ISPs and Nationwide ISPs

## 5. Estimation Results

Before logistic regression, we examine the rank correlations among explanatory variables. Unless the variables are mutually independent, we cannot run logistic regression. Table 5 shows the rank correlation coefficient of explanatory variables because many explanatory variables are discrete.

We can easily see that each rank correlation coefficient is far less than 1. Therefore, we can use these data for our analysis as 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 | |

Table 5. Correlation Coefficient of Explanatory Variables

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

### 5.1 Illegal Access

In Tables 6-8, we show the explained variables, which are the estimation results using the risk that ISPs encounter with illegal access accidents. Note that in Table 6 both the numbers of users and servers are used as the vulnerability index. In Table 7, we use only the logarithm of the number of users as the vulnerability index and we use only the logarithm of the number of servers as the index in Table 8. Chi-square in each Table is used to run the Hosmer-Lemeshow test.

| | Estimated Coefficient | Standard Error | exp[B] |
|---|---|---|---|
| $b_{C,NS}$ | 1.755 | 0.789 | 5.686 |
| $b_{C,EDU}$ | -4.515 | 1.966 | 0.011 |
| Constant term | -2.108 | 1.436 | 0.121 |
| | Chi-square(5)=2.556 [0.768], 7 Steps<br>Positive distinction rate: 80.6% | | |

Table 6. Estimation Result I

| | Estimated Coefficient | Standard Error | exp[B] |
|---|---|---|---|
| $b_{C,NS}$ | 1.373 | 0.533 | 3.947 |
| $b_{C,EDU}$ | -3.659 | 1.555 | 0.026 |
| Constant term | -1.971 | 1.148 | 0.139 |
| | Chi-square (5)=2.059 [0.841] ,6 Steps<br>Positive distinction rate: 76.3% | | |

Table 7. Estimation Result II

| | Estimated Coefficient | Standard Error | exp[B] |
|---|---|---|---|
| $b_{V,S}$ | 0.732 | 0.423 | 2.079 |
| $b_{C,NS}$ | 0.893 | 0.459 | 2.443 |
| $b_{C,EDU}$ | -2.833 | 1.254 | 0.059 |
| Constant term | -3.428 | 1.609 | 0.032 |
| | Chi-square (8)=2.990 [0.935], 5 Steps<br>Positive distinction rate: 82.9% | | |

Table 8. Estimation Result III

In Tables 6-8, we find 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 8 becomes positive.

From the results of the Hosmer-Lemeshow test, we 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 76.3 and 82.9%, we can insist that our models are valid.

### 5.2 System Trouble

In Tables 9 and 10, the estimation results using the risk that ISPs encounter system trouble as explained variables are shown. Note that in Table 9 we use both the numbers of users and servers as the vulnerability index and we use only the logarithm of the number of users as the vulnerability index in Table 10. In the case using the logarithm of the number of servers as the vulnerability index, we cannot gain significant results. Thus, we omit the results.

In Tables 9 and 10, we find 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

| | Estimated Coefficient | Standard Error | exp[B] |
|---|---|---|---|
| $b_{V,U}$ | 0.534 | 0.290 | 1.706 |
| $b_{C,NS}$ | 1.085 | 0.587 | 2.959 |
| $b_{C,EDU}$ | -3.562 | 1.719 | 0.028 |
| $b_{C,PT}$ | -1.915 | 1.201 | 0.147 |
| $C$ | 2.886 | 1.303 | 17.918 |
| Constant term | -5.110 | 3.091 | 0.006 |
| | Chi-square (7)=3.730 [0.881], 3 Steps<br>Positive distinction rate: 80.6% | | |

Table 9. Estimation Result IV

| | Estimated Coefficient | Standard Error | exp[B] |
|---|---|---|---|
| $b_{C,NS}$ | 0.522 | 0.292 | 1.685 |
| $b_{C,EDU}$ | -1.968 | 1.220 | 0.140 |
| Constant term | 0.877 | 1.169 | 2.403 |
| | Chi-square (5)=7.659 [0.176], 6 Steps<br>Positive distinction rate: 73.7% | | |

Table 10. Estimation Result V

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 9 become positive, respectively.

From the results of Hosmer-Lemeshow test, we 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%, we can insist that our models are valid.

### 5.3 Review of Estimation Results

The estimation results in the previous section are interesting.

First of all, 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 information security systems ISPs introduce, the higher the probability of risk that they encounter information security incident is[21]. On the other hand, the latter means that the more information security education ISPs positively execute, the lower the risk becomes. 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 we discuss network security (countermeasures) against Internet threats, systems such as FW and IDS play an important role and they are needed. However, the former result throws doubt on this thinking. We interpreted this result 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 Takemura (2007b). Therefore, there is a possibility that the old systems will not be able to correspond to present threats. Second, 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[22]. 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

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

[22] We believe that enough effects cannot be demonstrated unless the system is introduced to employees such as the SE (system engineer) who has enough knowledge.

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 it costs to execute information security education, the cost-benefit between information security education and the expected effects is higher than introducing information security systems in the long term. The reason is that executing information security education is effective (reduces the probability of risk that ISPs encounter information security incidents).

Takemura (2007a) reports that information security education includes etiquette on the Internet, knowledge about not only viruses and worms, but also the knowledge about security laws, and correspondence in emergencies. The information security education is executed with not only ex ante countermeasures, but also ex post ones in mind. Moreover, according to Takemura (2007a), 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. We expect that the risk of ISPs encountering information security incidents will be reduced in the future.

Next, 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 4.

Finally, we confirm that some countermeasures are not effective now because their coefficient parameters are not statistically significant. In Table 9, the estimated coefficient parameter of the service area 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. Therefore, our results overrule our initial intuition (hypothesis in section 4) though we assumed that local ISPs have a higher risk rather than nationwide ISPs.

## 6. Concluding Remarks and Future Work

The purpose of this chapter is to investigate the relations among information security incidents, information security countermeasures and vulnerability. We analyze the relations by using data on a 2007 questionnaire survey for Japanese ISPs and logistic regression. As a result, we found that there are statistically significant relationships 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. These results are valid and provide important information when considering the financial health of ISPs. For heightening and maintaining information security level of ISPs, it is efficient to execute information security education as a non-technological countermeasure (management). This higher information security level cannot be achieved by the IPSs alone. We suggest that the government needs to help these ISPs. As one of examples, the government can hold the seminar on information security. Actually, MIC and METI in Japan cooperate with IPA, JNSA, JPCERT/CC and the other organizations, and the seminars have been held several times every year. The challenge seems to be one of efficient policies and we strongly recommend that the seminars should be held regularly.

In addition, we suggest that the government should put out united guidelines on information security. Now, in Japan there are many guidelines on information security. It is necessary to rearrange these guidelines for heightening Japanese information security level. We expect that NISC will play an important role in coordinating policies on information security among ministries (Takemura and Osajima, 2008). This idea of holding seminars on security countermeasures also applies to usual firms.

Of course, it is necessary for NPA to strengthen control in cooperation with the organization of foreign countries, too.

Finally, we discuss the future works. The researches on “economics of information security” are not only meaningful in social sciences, but also help to the real business activities. Therefore, these researches need be accumulated more. We will continue to research the social and economic effects of information security countermeasures and investment quantitatively. This will be one of our future endeavors. Concretely, we will focus on economic behaviors about information security against individuals, who are Internet users, employees, and usual firms (Takemura and Minetaki, 2009a and 2009b, Minetaki, et al., 2009, and Takemura et al., 2009a and 2009b).

## 7. Acknowledgements

This work is supported in part by the Telecommunications Advancement Foundation in Japan, the Ministry of Education, Culture, Sports, Science and Technology, Japan: Grant-in-Aid for Young Scientists (B) (20730196) and Japan Society for the Promotion of Science: Grant-in-Aid for Science Research (B) (21330061).

The authors are grateful to Y. Ukai (Kansai University, Japan), K. Minetaki (Kansai University, Japan), T. Imagawa (The Ministry of Internal Affairs and Communications, Japan), A. Umino (The Ministry of Internal Affairs and Communications, Japan) and T. Maeda (Kansai University, Japan). We also express our gratitude to the ISPs who cooperated with our survey. The remaining errors are the authors.

## 8. References

Brynjolfsson, E.; Hitt, L. & Yang, S (2002). Intangible assets : how the interaction of computers and organizational structure affects stock market valuations. *Brookings Papers on Economic Activity : Macroeconomics*, Vol.1, 137-199

Takemura, T. (2008). *Economic analysis on information and communication technology*, Taga-shuppan, Tokyo

Information-technology Promotion Agency (2008). *Information of security white paper 2008*, Jikkyo Shuppan, Tokyo

Cook, D. & Keromytis, A. (2006). *Cryptographics: exploiting graphics cards for security*, Springer, New York

Ebara, H.; Nakawani, A.; Takemura, T. & Yokomi, M. (2006). Empirical analysis for Internet service providers, Taga-shuppan, Tokyo

Yokomi, M.; Ebara, H.; Nakawani, A. & Takemura, T. (2004). Evaluation of technical efficiency for Internet providers in Japan: problems for regional providers. *Journal of Public Utility Economics*, Vol.56, No.3, 85-94

Takemura, T. (2007a). *The 2nd investigation of actual conditions report on information security countermeasures for Internet service providers, Kansai University*

Information-technology Promotion Agency (2000). 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

Yamaguchi, S. (2007). Expectation for academic society, JSSM Security Forum distributed material, Online Available: http://www.jssm.net/

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

Gordon, L.A. & Loeb, M.P. (2002). The Economics of information security investment. *ACM Transactions on Information and System Security*, Vol.5, 438-457

Varian, H.R. (2002). System reliability and free riding. *ACM Transactions on Information and System Security*, Vol.5, 355-366

Gordon, L.A.; Loeb, M.P. & Lycyshyn, W. (2003). Sharing information on computer systems security: an economic analysis. *Journal of Accounting and Public Policy*, Vol.22, No.6, 461-485

Gordon, L.A. & Loeb, M.P. (2006). Expenditures on competitor analysis and information security: a managerial accounting perspective, In: *Management Accounting in the Digital Economy*, Bhimni, A. (Ed.), 95-111, Oxford University Press, Oxford

Tanaka, H.; Matsuura, K. & Sudoh, O. (2005). Vulnerability and information security investment: an empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, Vol.24, No.1, 37-59

Lie, W.; Tanaka, H. & Matsuura, K. (2007). 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, 585-599

Takemura, T. (2007b). Proposal of information security policy in telecommunication infrastructure, In: *What is Socionetwork Strategies*, Murata, T. & Watanabe, S. (Eds.), 103-127, Taga-shuppan, Tokyo

Takemura, T.; Osajima, M. & Kawano, M. (2008). Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers, *Proceedings of World Academy of Science, Engineering and Technology*, Vol.36, 703-710

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

Takemura, T. & Minetaki, K. (2009a). Strategic information security countermeasure can improve the market value: evidence from analyzing data on Web-based survey, *The Proceedings of 6th International Conference of Socionetwork Strategies*, 243-246

Takemura, T. & Minetaki, K. (2009b). The policies for strategic information security countermeasures improving the market value, *The Proceedings of 66th Conference on Japan Economic Policy Association*

Minetaki, K. ; Takemura, T. & T. Imagawa (2009). An empirical study of the effects of information security countermeasures, *Mimeo*, *Kansai University*

Nagaoka, H. & Takemura, T. (2007) A business continuity plan to heighten enterprise value, *Proceedings of 55th National Conference*, pp.149-152, Aichi-gakuin University, November 2007, Japan Society for Management Information, Nagoya

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

Ukai, Y. & Takemura, T. (2007). Spam mails impede economic growth. *The Review of Socionetwork Strategies*, Vol.1, No.1, 14-22.

Takemura, T. & Ebara, H. (2008a). Spam mail reduces economic effects, *Proceedings of the 2nd International Conference on the Digital Society*, pp.20-24, February 2008, IEEE, Martinique

Takemura, T. & Ebara, H. (2008b). Economic loss caused by spam mail in each Japanese industry, *Selected Proceedings of 1st International Conference of Social Sciences*, Vol.3, 29-42

Takemura, T. & Ebara, H. (2008c). Estimating economic losses caused by spam mails through production function approach. *Journal of International Development*, Vol.8, No.1, 23-33

Japan Data Communications Association (2008). Inspection slip of Influence That Spam Mail Exerts on Japanese Economy, Online Available: http://www.dekyo.or.jp/

Internet Provider Association (2003). *Actual conditions on investigation of nationwide Internet services 2003*, Internet Provider Association, Tokyo

Takemura, T.; Umino, A. & Osajima, M. (2009a). Variance of analysis on information security conscious mind of Internet users. *GITI Research Bulletin 2008-2009 (Waseda University)*, forthcoming

Hosmer, D.W. & Lemeshow, S. (2000). *Applied logistic regression (2nd ed.)*, Wiley-Interscience publication, New York

Takemura, T. & Osajima, M. (2008). About some topics on countermeasures and policies for information security incidents in Japan. *GITI Research Bulletin 2007-2008 (Waseda University)*, 163-168

Takemura, T.; Minetaki, K.; Takemura, T. & Imagawa, T. (2009). Economic analysis on information security conscious mind of workers, *Mimeo*, *Kansai University*

**Advanced Technologies**
Edited by Kankesu Jayanthakumaran

ISBN 978-953-307-009-4
Hard cover, 698 pages
**Publisher** InTech
**Published online** 01, October, 2009
**Published in print edition** October, 2009

This book, edited by the Intech committee, combines several hotly debated topics in science, engineering, medicine, information technology, environment, economics and management, and provides a scholarly contribution to its further development. In view of the topical importance of, and the great emphasis placed by the emerging needs of the changing world, it was decided to have this special book publication comprise thirty six chapters which focus on multi-disciplinary and inter-disciplinary topics. The inter-disciplinary works were limited in their capacity so a more coherent and constructive alternative was needed. Our expectation is that this book will help fill this gap because it has crossed the disciplinary divide to incorporate contributions from scientists and other specialists. The Intech committee hopes that its book chapters, journal articles, and other activities will help increase knowledge across disciplines and around the world. To that end the committee invites readers to contribute ideas on how best this objective could be accomplished.

**How to reference**
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Toshihiko Takemura, Makoto Osajima and Masatoshi Kawano (2009). Economic Analysis on Information Security Incidents and the Countermeasures: The Case of Japanese Internet Service Providers, Advanced Technologies, Kankesu Jayanthakumaran (Ed.), ISBN: 978-953-307-009-4, InTech, Available from: http://www.intechopen.com/books/advanced-technologies/economic-analysis-on-information-security-incidents-and-the-countermeasures-the-case-of-japanese-int

INTECH
open science | open minds

**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821