RCSS ディスカッションペーパーシリーズ ISSN-1347-636X
第 86 号　2009 年 7 月
Discussion Paper Series
No.86　July, 2009

An Economic Approach to Issues on the Information Security

Toshihiko Takemura

文部科学大臣認定　共同利用・共同研究拠点
関西大学ソシオネットワーク戦略研究機構
関西大学ソシオネットワーク戦略研究センター
（文部科学省私立大学学術フロンティア推進拠点）

Research Center of Socionetwork Strategies,
“Academic Frontier” Project for Private Universities, 2003-2009
Supported by Ministry of Education, Culture, Sports, Science and Technology
The Research Institute for Socionetwork Strategies,
Joint Usage / Research Center, MEXT, Japan
Kansai University
Suita, Osaka, 564-8680 Japan
URL: http://www.rcss.kansai-u.ac.jp
http://www.kansai-u.ac.jp/riss/index.html
e-mail: rcss@ml.kandai.jp
tel: 06-6368-1228
fax. 06-6330-3304

An Economic Approach to Issues on the Information Security

Toshihiko Takemura, Assistant Professor,
The Institute for Socionetwork Strategies, Kansai University,
Research Fellow, the Research Center of Socionetwork Strategies, Kansai University
3-3-35, Yamate-cho, Suita, Osaka, Japan, 564-8680
E-mail: takemura@rcss.kansai-u.ac.jp

Abstract

In this paper from the viewpoint of economics, the author analyzes the interrelationship between information security countermeasures and economic activities by statistical methods such as covariance structure analysis and logistic regression analysis. The sophisticated micro data set in this work, which includes countermeasures, (psychological) awareness on information security and various other attributes, is collected through a "Web-based survey", a remarkable survey in Japan that uses sophisticated social investigation methods. First, we find that there are positive relationships between the expected effects and some management countermeasures on information security. Second, the result shows that we need to build an information security system. Third, we can see that workers' awareness of information security is different in its attributes such as organizational attributes and the education about information security countermeasures.

Keywords: Information Security, Education, Awareness, Quantitative Analysis
JEL Classification: D78, C12, C35

1. Introduction

The Internet has become a critical infrastructure. The Internet has greatly revolutionized not only individuals' life styles, but also business styles and business environments. This fact is indisputable. In other words, there is no doubt that the Internet plays a great role in an individual's life and in forms of business in our advanced information society.

To keep up with this quickly changing infrastructure, many firms have advanced the digitalization of various pieces of information used by firms. As a result, information and communication technology (ICT) such as the Internet continues to improve productivity and efficiency in many firms. From the viewpoint of productivity and the efficiency, introducing ICT is welcome in the business process because it creates positive economic effects.[1] On the other hand, some problems occur at the same time. One problem centers around the existence of information security incidents such as malware,

[1] Brynjolfsson (2004) insists that there are organizations in which ICT investment contributes to productivity. He calls such an organization a digital organization.

illegal access and system troubles.[2] The number of threats keeps increasing rapidly because criminals can find information that the firms possess, for example, R&D data and customer data is valuable. That is, information is exposed to various threats and risks in the digitalized world via the Internet. In addition, under the progress of informationization, digitalization and the advent of a ubiquitous society, many individuals are confronted with serious problems, too.

Of course, many firms execute information security countermeasures to protect their information assets from these threats and risks. However, some business executives have said that there are no effects of information security countermeasures in their firm and that they have few incentives to invest in the countermeasures because the costs of information security countermeasures are prohibitive.[3] Some research investigations report similar cases. These reports imply that firms require not only a protection of their assets including information, but also a protection of the effect of the countermeasures. Obviously, the countermeasures might not be executed if the effects of the countermeasures are not clear. A significant question arises: namely, do countermeasures alone bring positive effects such as an increase of market value or efficient improvement of business processes? Unequivocally, the answer is yes. In this paper, we emphasize that strategic information security countermeasures play the most important role in a firm from the results of this paper. To verify our position, we examine several hypotheses on the relationships between expected effects and information security countermeasures. In other words, we are interested in clarifying which countermeasure executions have a positive effect. Next, we investigate the relationships between workers' awareness of information security and various attributes such as working patterns, organizational attributes, and individual attributes. We discuss the effective countermeasures through the results of the analysis. This result possesses not only academic significance, but also business and political significance.

The paper consists of the following sections. Section 2 mainly introduces related works on the economics of information security. Section 3 explains an economic model of firms and the data set. In addition, section 4 investigates the workers' awareness of information security from the Web-based survey. Section 5 discusses effective countermeasures and information security policy in Japan. Section 6 presents concluding remarks and future research.

2. Literature Review

Although information security technology such as cryptographic technology is advancing every day, an unrelenting succession of damages and cyber crimes caused by information security incidents are occurring all over the world. This situation implies that even with highly advanced new technologies, incidents of damage are still widespread. Cook and Keromytis (2006) discuss security technologies such as cryptographic technology in detail.

Besides cryptographic technology to reduce damages, what other types of countermeasures will be necessary? In this paper, aspects of management and policy as countermeasures for information security will be explored fully from an economic point of view. Approaches to management and policy on information security in the social sciences first began in 2000, and have continued to blossom.

In recent years, in the field of management science, qualitative research on various kinds of management systems such as ISMS (information security management system), ISO27000 (International Organization for Standardization 27000) and BCMS (business continuity management

[2] For example, according to Information-technology Promotion Agency (2008), the accidents caused by these incidents are reported in Japan.

[3] Few firms know concretely which information security countermeasures they should execute. As a result, they often over-invest in the countermeasures and/or do not execute enough countermeasures.

system) have quickly accumulated. Nonetheless, this research is insufficient in giving incentives to individuals and/or firms to execute information security countermeasures.

In this paper, we discuss the necessity of information security countermeasures, the importance of BIA (business impact analysis), the style of management systems, and research on how to use these factors to improve market value. For instance, Nagaoka and Takemura (2007) discuss the importance of strategic information security countermeasures and investment from the viewpoint of BCP (business continuity plan).

In the field of economics, economic analyses on information security have not been researched as well as the analysis of ICT on economics. We can easily imagine the reasons as follows: Many scholars are interested in only the positive effects of ICT investment, but are incurious as to its negative effects. It is not easy to measure the return on information security investment. The definition of information security investment/countermeasures is vague. Data on information security investment/countermeasures have not accumulated because disclosed data does not exist. In addition, research on information security investment/countermeasures has not attracted great attention recently. However, since the negative effects caused by incident damages are too serious to avoid altogether, some research on the economics of information security have begun worldwide.

Pioneering theoretical research on the economics of information security are Varian (2002) and Gordon and Loeb (2002). The former looks on an information system as a form of public goods and discusses the 'free-rider problem' on information security countermeasures. The latter builds an economic model on vulnerability and the level of information security and discusses information security investment from the view of economics. Gordon et al. (2003) and Gordon and Loeb (2006) research the interdependency of information security countermeasures and information sharing.

Within theoretical research, empirical research is also carried out. In much empirical research, the amount of damages caused by certain incidents is calculated. For example, in Japan, this sort of investigation is carried out by the Japan Network Security Association (2008), Takemura and Ebara (2008), and the Japan Data Communications Association (2008). The Japan Network Security Association has been calculating the amount of expected damage caused by leaks of information since 2002; the amount of this damage in 2008 totaled about 200 million yen (2 million dollars). Takemura and Ebara (2008) and the Japan Data Communications Association (2008) have calculated the amount of economic losses caused by spam mail. As a result, both studies show that the amount of GDP loss is about 730billion yen, and labor loss time was about 200 million hours in fiscal year 2006. The amount of these damages provides a case for the need of investment, countermeasures, and policy. On the other hand, it is not possible for such research to clarify the scale of investment concretely.

By calculating the amount of damage, cost benefit analyses on information security have begun recently. For example, see Tanaka et al. (2005), Lie et al. (2007), Takemura (2007), Takemura et al. (2009), and Takemura and Minetaki (2009a, 2009b, 2009c) in Japan. Tanaka et al. use data of an information processing investigation of actual conditions in Japan and analyze the economic effect of information security investment. Takemura et al. use data from mailings and a Web-based survey they conducted as well as research on economic analysis on information security countermeasures. In each research investigation, Takemura et al. mention the necessity for the enhancement and effectiveness of management and personnel training on information security countermeasures while also suggesting that it is important to introduce and operate an information security system. Subjects of these surveys are Japanese firms. Then again, it has been pointed out that such research has its limits because it is difficult to grasp each worker's awareness of information security, which is an important factor. Recently, analyses from the viewpoint of the worker's awareness to information security have appeared, for example, Albrechtsen (2007), Albrechtsen and Hovden (2009), and Takemura (2009b).

Albrechtsen (2007), and Albrechtsen and Hovden (2009) analyze the effectiveness of information security countermeasures qualitatively by using data from their interview studies. On the other hand, Takemura (2009b) analyzes countermeasures by using data collected through Web-based surveys that they conducted. This research points out that it is meaningless for a firm to just execute formal countermeasures systematically if the level of awareness of these countermeasures and their effectiveness is low.

3. Empirical Analysis I (Firm)

3.1 Model I

According to the Ministry of Internal Affairs and Communications (2006), the Internet adoption rate of a firm was about 99.1% at the end of fiscal year 2005. The Internet is an essential business platform for firms. Firms have rapidly strengthened and continue to strengthen their dependency on ICT, and this situation is only expected to increase in the future. Therefore, ``do not stop using the information system'' has become almost equivalent to ``do not stop business'' for many firms.

Up until now, many parts of information security countermeasures were just reactive because they simply served conservative motivations such as compliance and/or contracts with the client. Reactive countermeasures do not necessarily accomplish social responsibility. In this paper, we insist on the necessity of strategic information security countermeasures and investment, not reactive countermeasures. Strategic information security countermeasures and investment are proactive actions for the purpose of not only protecting information assets and other assets, and avoiding risks, but also for flexible business processes that protect the stockholder and cultivate a culture of security by adjusting risk. Certain risk assessments from society and markets improve the firm's overall market value. This concept is based on the idea of intangible assets in Brynjolfsson et al. (2002). Therefore, it is important that firms not only execute information security countermeasures inside their internal organization, but that they also disclose the contents and assessment on information security countermeasures toward society and markets through IR (Investor Relations) information or information security reports. Figure 1 shows a process through which strategic information security countermeasures improve market value

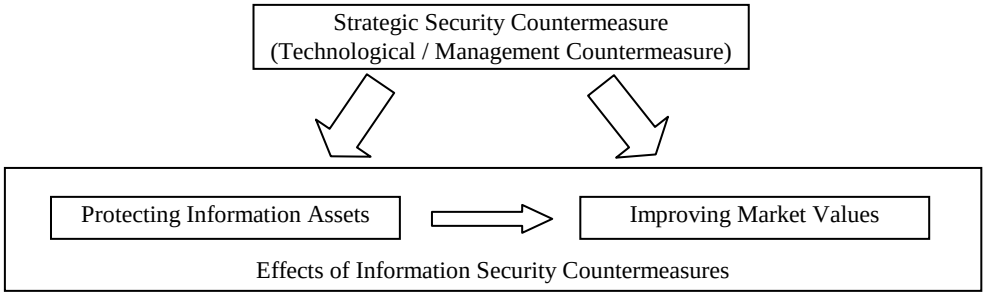


Figure 1: A Process through which Strategic Information Security Countermeasures Improve Market Value

Besides the effect of protecting information assets, the expected effects of information security countermeasures will provide an efficient improvement of the business process, a strengthening of competitiveness, improvement of assessment from clients and better organizational ability. Each effect contributes to improve the firm's market value. However, information security countermeasures do not improve the firm's market value by executing the countermeasures haphazardly.

Next, we verify which information security countermeasures contribute to improving the market value or not. In this paper, we clarify the relations in Figure 1 through quantitative analysis.

We use logistic regression analysis as one of our statistical methods. Logistic regression analysis is widely applied in various fields such as sociology, economics, psychology and medical science. The merits of this method are as follows: 1) we do not need strict assumptions on distribution of explanatory variables, 2) because we can obtain the odds ratio as a coefficient, the interpretation is easy, and 3) we can obtain the probability that a certain event happens for each object.

In logistic regression analysis, 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).

In this paper, we quantitatively grasp relations between expected effect and the information security countermeasures using the following equation:

$$\log \frac{p_j}{1-p_j} = a + b_T X_T + b_M X_M + b_F X_F \qquad (1)$$

where p_j is the probability that a firm feels the effect j, and X_T, X_M, and X_F represent the number of information security technologies introduced in firm, management characteristics, and attributes of the firm, respectively.

Each coefficient parameter b_k (for k=T, M, and F) represents the odds ratio in equation (1). If the odds ratio is positive and X_k increases (resp. decreases) one unit, the probability that the firm feels the effect j similarly increases (resp. decreases).

If information security countermeasures/investment improve the firm's market value, the coefficient parameter $b_{k'}$ (for k'=T and M) will be positive in equation (1).[4]

The coefficient parameter of the attributes of firm b_F is expected to be zero; b_F =0. This implies that we have no relations between the expected effects of information security and the scale of the firm. The reason that X_F is incorporated in equation (1) is to confirm whether or not the difference of effects is caused by the scale of firm.

We introduce methods and processes to estimate coefficient parameters in equation (1), and to evaluate the fitness of their 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 the statistical computer software in this paper. (SPSS version 17.0J for Windows, SPSS, Inc. is used.) SPSS has (a) a method by compulsion for 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 paper. This method is often used as one of the most preferable indices. Next, the Hosmer-Lemeshow test to evaluate the fitness of the model is run. Note that the null hypothesis of this test H_0 is that the model is well suited. Refer to Hosmer and Lemeshow (2000) for the details of this test. In addition, the authors evaluate the validity of the model by using a positive distinction rate, which forecasts this model correctly.[5]

[4] In this paper, we do not necessarily suggest that various kinds of information security systems and management should be introduced in the firm if these coefficient parameters are positive. Importantly, we give weight to grasping which countermeasures can actually feel the effects in a firm.

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

3.2 Model II

As mentioned in section 3.1, various threats such as malware, phishing, DoS (Denial of Service) attacks, zero-day attacks and botnets exist on the Internet. According to the IPA, the number of inquiries on these information incidents has increased in Japan. Therefore, information security countermeasures to protect information assets and other assets from these threats are needed.

In this subsection, we accept the analysis of covariance structure as a statistical method for examining the interrelationships between different kinds of security countermeasures and their effects. We use this method because 1) we want to grasp the casual interrelationship between some kinds of information security countermeasures and their effects, and 2) we need to treat both countermeasures and their effects as (unobservable) latent variables. Basically, we formularize the casual interrelationship between the latent variable of information security countermeasures and the latent variable of effects by countermeasures. We assess the model by using five representative indexes such as goodness fit, the chi-square test, GFI (goodness of fit index), AGFI (adjusted goodness of fit index), CFI (comparative fit index) and RMSEA (root mean square error of approximation). The chi-square test verifies the null hypothesis that the structured model is right. However, the chi-square test does not work effectively when the sample size is large. The GFI is the measure of the relative amount of variance. The AGFI is adjusted by the number of degrees of freedom to the GFI. We consider the model appropriate, when the GFI and the AGFI are higher than 0.90. The CFI is derived from the comparison of a hypothesized model with the independent model. The requirement level is above 0.90 of the CFI. The RMSEA shows the discrepancy between the model's distribution and the true distribution. Values of RMSEA less than 0.05 indicate a good fit while values higher than 0.10 indicate a poor fit.

3.3 Web-based Survey I

In this paper, we use the data of the Web-based survey we conducted in November, 2008.[6]

The Web-based survey has some social survey problems, but contains parts that will help to create a new style of social surveys in the academic fields.[7] By comparing the other mailing survey with similar content, we carefully consider the problems of the Web-based survey when we analyze the data.

The object of this survey was to gather responses from well-informed people such as people in charge of information security, especially, network security in firms, who have or have had an official position and have been involved in this sort of work for at least a year. The aim of this survey is to understand the current situation of information security countermeasures in Japanese firm. This survey has more than 50 question items and 500 respondents. Here, we briefly explain the data used in our analysis.

As explained variables in equation (1), we use p_j to represent the probability of whether or not a firm feels the effects in Table 1 as follows:

For j =1, 2, …, 9,

[6] This survey is supported by the Okawa Foundation: in 2007-2008. The data we have collected can be used all over the world for research purposes by applying to the Research Institute for Socionetwork Strategies (RISS), Kansai University. Our data can be accessed through the Website (http://www.kansai-u.ac.jp/riss/en/shareduse/database.html), or by direct contact.

[7] Trade-offs exists between the response percentage and the bias of the population in Web-based surveys and other social surveys. For example, the recovery response percentage of the mailing survey has decreased every year. In this paper, the Web-based survey is adopted to secure the highest number of respondents.

$$p_j = \begin{cases} 1 & \text{if firm feels expected effect } j \\ 0 & \text{otherwise} \end{cases}$$

The items in Table 1 can be divided roughly into two. The Contents of Nos.1-5 in Table 1 can be considered the expected effect that the firm feels in its internal organization. On the other hand, the contents of Nos.6-9 in Table 1 can be considered the expected effect that the firm feels in external organizations or markets.

Table 1: Notation of Explained Variables

No	Content	(%)[a)]
1	Review of information assets	58.6
2	Review and change of internal business processes	61.6
3	Improvement of business efficiency	54.6
4	Acquisition of commitment on information security from managers	65.4
5	Improvement of information security management abilities in organization	66.4
6	Evaluation from business partners and/or customers	59.0
7	Strengthening of competitiveness	46.8
8	Improvement of quality of product and service	53.0
9	Consciousness of corporate social responsibility (CSR)	69.6

a) Ratio of firms which feel the effect

As Explanatory variables in equation (1), we use technological and management countermeasures on information security, and the attributes of firms. Those contents are as shown in Table 2.

Table 2: Notation of Exploratory Variables

Variable	Content	
Technological countermeasures on information security		Ave.
X_T	The number of introduced technical countermeasures on information security	8.557
Management countermeasures on information security		(%)[a)]
X_{M1}	Execution of total information security management	67.2
X_{M2}	Execution of information security management in each section	61.4
X_{M3}	Acquisition of public certification concerning information security	40.4
X_{M4}	Countermeasures based on ROI (return on investment)	40.4
X_{M5}	Execution of concrete countermeasures based on BCP	47.2
X_{M6}	Physical information security countermeasures	59.4
X_{M7}	Publication of information security report or description to CSR report	45
X_{M8}	Making of information security policy	59.2
X_{M9}	Establishment of information security department and clarification of responsibility	49.4
X_{M10}	Personnel training of technical staff on information security	47.6
X_{M11}	Information sharing and accumulation on knowledge of information security in firm	52
X_{M12}	Maintenance of procedures on incident response and/or possession of the incident response team	43.6
X_{M13}	Employee's information security education and training	58
X_{M14}	Performance assessment of employees information security knowledge	44
Attributes of firms		(%)
X_{FE}	Number of employees	74.4[b)]
X_{FR}	Annual sales	59.8[c)]
X_{FL}	listed or non-listed firm	17.8[d)]
X_{FS}	Dependency on information system	60.6 [e)]
X_{FI}	Dependency on the Internet	71.6[e)]

a) Ratio of firms which execute management countermeasures
b) Ratio of firms possessing less than 1000 employees
c) Ratio of firms whose annual sales are less than 3 billion yen
d) Ratio of listed firms
e) Ratio of firms whose dependency is less than 50%

As technological countermeasures on information security, we use the number of introduced technical countermeasures. In the survey, we show 25 kinds of technologies and systems; firewall, IDS, IPS, quarantine network system, thin client, encryption of data, PKI, biometrics system, one-time password, and anti-virus software, for example.

This survey found that 70% of firms had 6-10 kinds of technologies and systems.[8]

As management countermeasures on information security, we use 14 kinds of management such as information security education, CSR, BCP, organizational. The variable is assigned as follows:

For m = 1, 2, …, 14,

$$X_{Mm} = \begin{cases} 1 & \text{if firm executes countermeasure } m \\ 0 & \text{otherwise} \end{cases}$$

As attributes of firms, we use number of employees, annual sales, listed or non-listed firm, and dependency on information systems and the Internet.

3.4 Results

3.4.1 Firm I

By applying the variable decrease method to the likelihood ratio, we gain the estimated results in Tables 3 and 4.[9] Chi-square values in each table are used when we run the Hosmer-Lemeshow test. To evaluate the validity of the model, positive distinction rates are shown. In addition, Log Likelihood, Cox-Snell R^2 and Nagelkerke R^2 are shown. Note that value in [ ] is p-value.

First, the explanatory variables such as the number of employees and annual revenue used as attributes of firms are deleted in the process of logistic regression analysis.Therefore, we cannot confirm that these variables are statistically significant.

Next, the coefficient parameter of the number of introduced technical countermeasures on information security, b_T, is statistically significant and positive only if consciousness of CSR (No.9) is used as an explained variable (see Table 4).

Third, in Tables 3 and 4, many coefficient parameters of management countermeasures on information security are statistically significant and positive. The coefficient parameter of the establishment of the information security department and clarification of responsibility, b_{M9}, is statistically significant and negative only if improvement of business efficiency (No.3) is used as an explained variable (see Table 3).

Fourth, the coefficient parameter of listed or non-listed firm, X_{FL}, is statistically significant and negative only if a review of information assets (No.1) is used as an explained variable (see Table 3), but it is not statistically significant in the other cases. In some cases, the coefficient parameter of dependency to the Internet, X_{FI}, is statistically significant and positive (see Tables 3 and 4). In addition, coefficient parameter of dependency to information system, X_{FS}, is statistically significant and positive or negative by case (see Table 3).

[8] In Liu et al (2007), the number of information security countermeasures is used as a proxy variable. We adopt a similar idea for technological countermeasures.

[9] At the same time we apply the variable increase method to the likelihood ratio. Because the results are almost the same, we give only the results by applying the variable decrease method to the likelihood ratio in this paper.

Table3: Estimated Results I

		Coefficient parameter (B)	Standard error	exp[B]	Remarks
No.1	b_{M1}	1.069	0.254	2.912	-2 Log Likelihood: 494.519 Cox-Snell R^2: 0.308 Nagelkerke R^2: .0.414 Chi-Square (7)= 8.399 [0.299] Positive distinction rate: 75.8%
	b_{M4}	0.582	0.304	1.789	
	b_{M5}	0.859	0.297	2.361	
	b_{M7}	0.615	0.322	1.849	
	b_{M8}	0.615	0.275	1.851	
	b_{FL}	-0.671	0.327	0.511	
	b_{FI}	0.238	0.117	1.268	
	Constant	-1.839	0.282	0.159	
No.2	b_{M1}	1.015	0.247	2.758	-2 Log Likelihood: 493.569 Cox-Snell R^2: 0.292 Nagelkerke R^2: 0.396 Chi-Square (8)= 9.092 [0.335] Positive distinction rate: 78.6%
	b_{M5}	0.726	0.289	2.067	
	b_{M7}	0.757	0.315	2.132	
	b_{M14}	0.923	0.283	2.518	
	b_{FS}	0.227	0.104	1.255	
	Constant	-1.581	0.268	0.206	
No.3	b_{M1}	0.792	0.247	2.208	-2 Log Likelihood: 583.527 Cox-Snell R^2: 0.190 Nagelkerke R^2: .0.254 Chi-Square (8)=4.755 [0.783] Positive distinction rate: 71.2%
	b_{M4}	1.081	0.261	2.948	
	b_{M9}	-0.610	0.263	0.543	
	b_{M14}	1.052	0.255	2.862	
	b_{FS}	-0.244	0.117	0.784	
	b_{FI}	0.239	0.126	1.270	
	Constant	-0.822	0.255	0.439	
No.4	b_{M1}	0.530	0.302	1.700	-2 Log Likelihood: 462.493 Cox-Snell R^2: 0.306 Nagelkerke R^2: 0.422 Chi-Square (5)=4.433 [0.489] Positive distinction rate: 79.4%
	b_{M2}	0.920	0.300	2.510	
	b_{M7}	0.881	0.295	2.413	
	b_{M11}	0.810	0.271	2.247	
	b_{M13}	0.678	0.284	1.971	
	Constant	-1.201	0.190	0.301	
No.5	b_{M1}	0.925	0.312	2.521	-2 Log Likelihood: 397.804 Cox-Snell R^2: 0.382 Nagelkerke R^2: 0.530 Chi-Square (8)=1.321 [0.995] Positive distinction rate: 83.0%
	b_{M2}	0.889	0.317	2.433	
	b_{M5}	0.886	0.352	2.426	
	b_{M6}	0.551	0.289	1.735	
	b_{M7}	0.701	0.373	2.016	
	b_{M12}	0.642	0.353	1.900	
	b_{FS}	0.291	0.119	1.337	
	Constant	-1.993	0.307	0.136	

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, because the positive distinction rate is at a level between 71.0 and 83.0%, we can insist that our models are valid.

From the estimated results, we discuss the effective countermeasures needed to create expected effects and investigate whether or not the firm can feel the differences in expected effects from the attributes of the firms.

For the expected effect that the firm feels in its internal organization, from Table 3, we see “execution of total information security management” is effective in all cases. Subsequently, there are “publication of information security reports or description to CSR report” and “execution of concrete countermeasures based on BCP” are effective in many cases, too.

For the expected effect that the firm feels in external organizations or markets from Table 4, we see “execution of information security management in each section” is effective in all cases. Subsequently, there are “introduction of approach on employee’s information security into performance assessment,” “personnel training of technical staff on information security,” “information sharing and

accumulation on knowledge of information security in firm," "countermeasures based on ROI (return on investment)" and "execution of concrete countermeasures based on BCP" are effective in many cases, too.

Table 4: Estimated Results II

		Coefficient parameter (B)	Standard error	exp[B]	Remarks
No.6	b_{M2}	0.712	0.238	2.038	-2 Log Likelihood: 552.200
	b_{M5}	0.607	0.264	1.835	Cox-Snell R^2: 0.221
	b_{M10}	0.895	0.264	2.448	Nagelkerke R^2: 0.298
	b_{M14}	0.622	0.266	1.863	Chi-Square (3)=.064 [0.996]
	Constant	-0.946	0.166	0.388	Positive distinction rate: 71.0%
No.7	b_{M2}	0.534	0.276	1.706	-2 Log Likelihood: 493.503
	b_{M3}	0.534	0.295	1.707	Cox-Snell R^2: 0.326
	b_{M4}	0.760	0.276	2.137	Nagelkerke R^2: 0.436
	b_{M7}	0.582	0.305	1.789	Chi-Square (7)=2.544 [0.924]
	b_{M11}	0.485	0.266	1.624	Positive distinction rate: 77.6%
	b_{M14}	0.654	0.279	1.924	
	b_{FI}	0.315	0.115	1.370	
	Constant	-2.440	0.293	0.087	
No.8	b_{M2}	0.768	0.243	2.156	-2 Log Likelihood: 532.854
	b_{M4}	1.211	0.266	3.357	Cox-Snell R^2: 0.272
	b_{M11}	0.644	0.252	1.904	Nagelkerke R^2: 0.363
	b_{M14}	0.638	0.260	1.893	Chi-Square (5)=6.208 [0.286]
	Constant	-1.387	0.183	0.250	Positive distinction rate: 73.4%
No.9	b_T	0.066	0.030	1.069	-2 Log Likelihood: 450.381
	b_{M1}	0.909	0.303	2.483	Cox-Snell R^2: 0.279
	b_{M2}	0.795	0.314	2.215	Nagelkerke R^2: 0.395
	b_{M5}	0.812	0.316	2.252	Chi-Square (8)=5.597 [0.692] Positive
	b_{M10}	0.677	0.300	1.968	distinction rate: 80.4%
	Constant	-1.182	0.239	0.307	

Management countermeasures necessary to actually feel the effect in internal and external organization are somewhat different, but there are some common features.

We can expect that using existing information systems and/or conducting existing education schemes will achieve further economic effects. For example, information sharing and accumulation of knowledge plays an important role in the general business environment.[10] By incorporating the element of information security into existing information systems and education schemes, firms do not need to invest in information security countermeasures.

We investigate whether or not firms feel a difference in expected effects from the attributes of the firms. We found no difference in expected effects from the number of employees or from the annual revenue. On the other hand, firms feel a difference in expected effects by a dependency on information systems and the Internet.

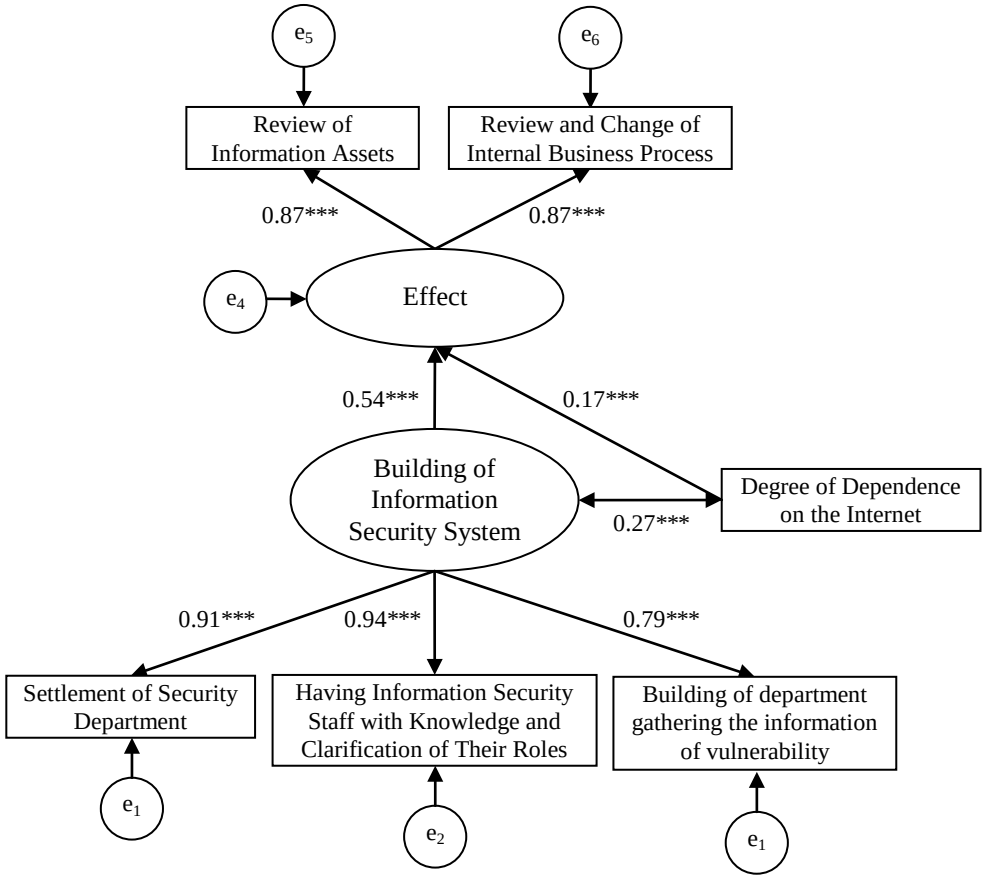
3.4.2 Firm II

We conduct various models by the analysis of covariance structures. We show two models here. Figure 2 and Table 5 show a path diagram and the result of the goodness of fit indexes. This model shows the probability that the null hypothesis by the chi-square test is not rejected, and is 0.011. Also, this model indicates quite a good fit because GFI, AGFI, and CFI are 0.984, 0.951, and 0.991, respectively. RMSEA is 0.066 so it cannot be good fit, but it is an allowable level.

[10] Minetaki and Takemura (2009) insist on the importance of general information sharing and an educational scheme.

The latent variable “building of an information security system” consists of three variables, namely, C-1’) Settlement of security department, C-2’) Having information security staff and clarification of their roles, C-3’) Building of a department gathering the information of vulnerability, and C-4’) Knowledge sharing within the firm and its utilization. Also, the latent variable of effects consists of two variables, namely, E-1) Review of information assets, and E-2) Review and change of internal business processes in Table 5.

Therefore, the latent variable of “building of information security system” influences the latent variable of “effects”, and at the same time, the degree of dependence on the Internet influences the latent variable of the effects. Table1 shows that every normalized coefficient is statistically significant at 0.01% level.



Ellipses cells represent the latent variables; square cells represent the (observed) variables; circles represent the errors

Figure 2: Path Diagram 1

Table 5: Goodness of Fit Indexes 1

Index	Value
Chi-square(probability)	18.183 (0.011)
GFI	0.984
AGFI	0.951
CFI	0.991
RMSEA	0.066

Next, we show an alternative path diagram that adopts variables of C-4) education of security staff, and C-5) knowledge sharing within the firm and its utilization for the components of the latent variable, building of security system. Figure 3 and Table 2 show the alternative path diagram and the result of goodness of fit indexes. This model indicates quite a good fit because GFI, AGFI, and CFI are 0.990, 0.977, and 1.00, respectively. RMSEA is 0.008 and it is a better fit. From the above discussion, we think that our structured model is good fit generally. The goodness of fit index in Table 6 has a higher performance than the path diagram shown in Figure 3. Also, every normalized coefficient is statistically significant at 0.01% level.

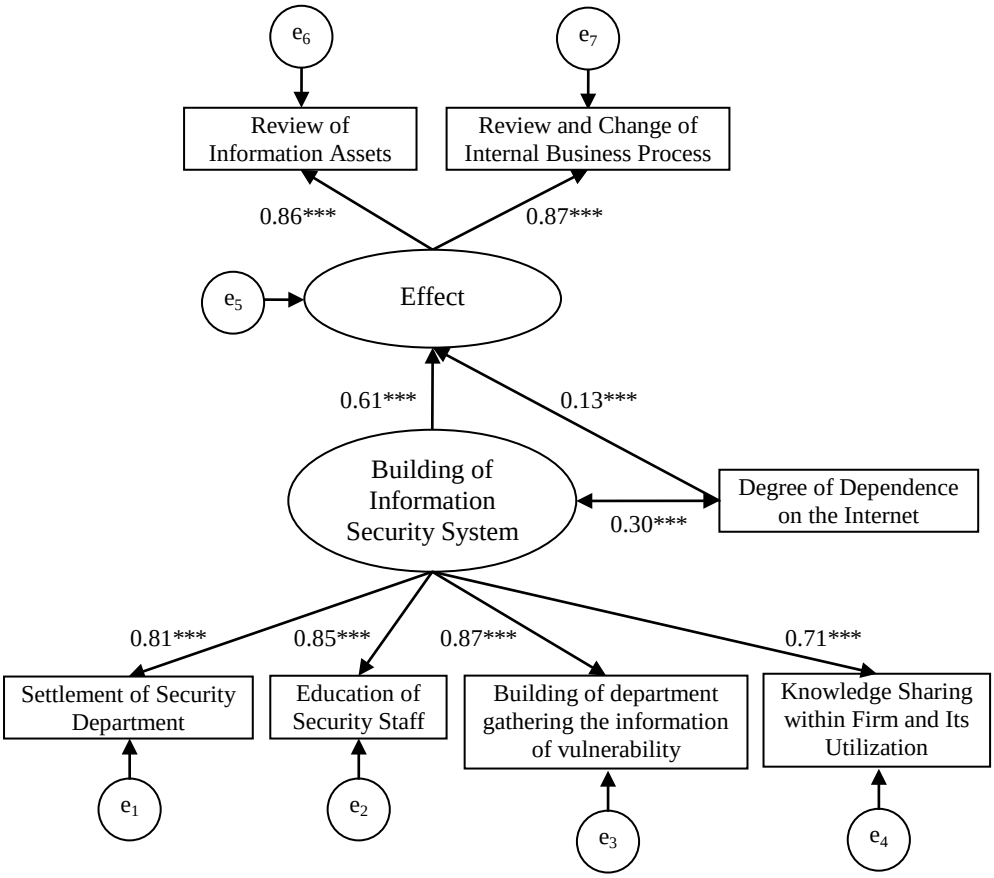


Figure 3: Path Diagram 2

Table 6: Goodness of Fit Indexes 2

Index	Value
Chi-square (probability)	12.267 (0.424)
GFI	0.990
AGFI	0.977
CFI	1.00
RMSEA	0.008

Finally, from the results, we find that possessing human capital with special and advanced knowledge, and building information systems within firms is necessary. This fact is consistent with many of the works on the economics of information security in Japan; for example, Lie, et al. (2007), Tanaka, et al. (2005), Takemura and Minetaki (2009), and Takemura, et al. (2009).

Furthermore, we find that the above-mentioned countermeasures are needed as ex-ante countermeasures from the result of the degree of dependence on the Internet. That is, firms need countermeasures for preventing the troubles such as a system trouble if the firm is highly dependent on the Internet.

4. Empirical Analysis II (Worker)

4.1 Hypotheses

From general damage caused by information security incidents, it is clear that the workers' awareness to information security differs according to attributes such as working pattern and organization attributes. Up until now, in many surveys, merits of IT usage have been analyzed. However, these merits and awareness to information security have not been quantitatively verified. Therefore, in this paper, we examine whether or not the awareness to information security is different by attributes based on the categories in Table 3. We set up the following hypotheses: H1) there is no difference in awareness on the information security by working pattern; hypothesis H2) there is no difference in awareness on the information security by organization attributes, and hypothesis H3) there is no difference in awareness on information security by individual attributes.

First, we examine whether hypotheses H1, H2, and H3 are uniform.[11] It is important for all workers in society to keep the awareness to information security at high level. Even if many users with a rich awareness of the information security exist, the level of information security in society in general becomes low if even a few users with poor awareness exist. If these hypotheses are verified according to human social factors in addition to quantitative verification, we should be able to reach an understanding of a true security level. We expect that there will be no difference in awareness of the information security by attributes in the subcategories in Table 3 excluding degree of infrastructure. As Takemura et al. (2009) has explained forms with a high degree of infrastructure will require higher security levels than in firms with a lower level of infrastructure. Therefore, we expect that there will be a difference in awareness of information security by the degree of infrastructure.[12]

In order to verify this hypothesis, we run an analysis of variance (AOV).

4.2 Web-based Survey II

Takemura analyzes the workers' awareness to information security using the data collected from the Web-based survey "investigation on workers' Internet usage and awareness to information security," conducted in March 2009. Subjects of this survey are Japanese people who have been working for more than two years in firms. The number of the sample is 600. The sample in this survey is arranged by working pattern and listed/non-listed firms, as in Table 7.

Table 7: Arrangement of Sample

Working pattern	Listed firm	Non-listed firm
Regular	200	200
Non-regular	100	100

Table 8 shows elementary statistics on indices of workers' awareness to information security. We investigate awareness to information security by dividing the four kinds of indices roughly as: 1) recognition concerning individual information, 2) recognition concerning countermeasures, and 3)

[11] A possibility arises such that information security may be kept at a low level even if the awareness of the information security is uniform. We can examine the level of information security in each group by using the average value and the median of the groups.

[12] We can check the level of information security in each group by using the average value and the median of the groups.

moral awareness of information use. Each index is qualitative / ordinal scale data and the values are assigned between 1 and 5. The index assigns a small value if the recognition is poor. Inversely, the index assigns a large value if the recognition is rich.

Table 9 shows information on some attributes used as categories. The contents are divided roughly into three kinds of categories: 1) working patterns, 2) organizational attributes, and 3) individual attributes. Furthermore, each category has some subcategories.

Table 8: The Information on Indices of Workers' Awareness of Information Security

	Variable	Content of questionnaire	Ave.	Standard deviation
Recognition concerning individual information	X1	If you can freely see others' individual data such as address, name, age and e-mail address, do you use them?	3.72	0.986
Recognition concerning countermeasures	X21	Do you think that there is a problem using a computer without anti-virus software?	4.12	0.960
	X22	When you receive chain mail, do you think that there might be a problem forwarding the mail to your friends and acquaintances?	4.31	0.911
	X23	Do you think that information security education is not needed if security software has been introduced?	3.70	0.899
	X24	Do you think that information security education is not necessary?	3.91	0.830
	X25	Compared with one year ago, have you changed your attitude to information security, for example, in terms of information management?	3.64	0.632
Moral awareness of information use	X31	Do you think that it is ok to send private mails during work?	3.35	0.941
	X32	Do you think that it is ok to violate any rules if a problem does not occur?	3.78	1.019

Table 9: The Information on Attributes (Categories)

Category	Subcategory	Explanation
Working pattern	Working pattern	1: Regular 2: Non-regular
Organizational attribute	Number of employees	1: Less than 9 persons 2: 10-49 persons 3: 50-99 persons 4: 100-299 persons 5: 300-999 persons 6: 1000-2999 persons 7: 3000-4999 persons 8: 5000-9999 persons 9: 10000-99999 persons 10: 100000-149999 persons 11: More than 150,000 persons
	Degree of infrastructure	1: Lowest 2: Low 3: High 4: Highest
	Prohibited matter as information security countermeasures	Taking customer information data outside of the firm by portable devices such as USBs / Attachment of customer information data to e-mail / Taking customer information data outside of the firm by paper / Taking a firm notebook computer outside the firm / Connecting LAN with private personal computer (1: Overall prohibition 2: Conditional and possible 3: No prohibition)
	Motivational system	Authority handover / Stock option / Employee stock ownership program / Spin-out (1: Introduced 2: Not introduced)
	Listed/non-listed	1 Listed firm 2 Non-listed firm
Individual attributes	Age	1: One's twenties 2: One's thirties 3: One's forties 4: One's fifties 5: One's sixties
	The Internet terms of use	1: Less than one year 2: 1-2 years 3: 2-3 years 4: 4-5 years 5: 6-7 years 6: 8-9 years 7: More than 10 years
	Education about information security	1: Not educated 2: Some formal training and/or the university.

4.3 Results

Before running AOV, we need to check whether or not data follows a normal distribution. We have various kinds of tests of normality. Generally, the Kolmogorov-Smirnov test and the Shapiro-Wilk test are accepted as more reliable among various tests. In these tests, the null hypothesis represents data that does not follow a normal distribution. Therefore, if the significance probability is less than 5%, the null hypothesis cannot be rejected and we can conclude that the data do not follow a normal distribution. Oppositely, if the data follows a normal distribution, we can reject the null hypothesis.

Table 10 shows the result of the Kolmogorov-Smirnov test and the Spapiro-Wilk test. From Table 10, we can see that data we use in this paper does not follow a normal distribution because we cannot reject the null hypothesis. Unfortunately, we cannot run AOV by a parametric method such as the t test and/or Tukey test. Therefore, we should run AOV based on a non-parametric method. Concretely, we examine whether or not we have a difference in the median, not in the average, in each category. As a feature of the non-parametric method, data is assumed not to follow the normal distribution and we can use (questionnaire) data with an ordinal scale.

Hereafter, we run four kinds of test (AOV) according to the categories in Table 9: the Mann-Whitney test, the Wilcoxon test and the Kruskal-Wallis test. Next, we explain the procedure of each test.[13]

First, the Mann-Whitney test (Mann-Whiteney's U test) and the Wilcoxon test are rank sum tests that examine the difference of the median between two groups. In these tests, we use the rank sum of data arranged in ascending order, not the observed data. The test statistics are U and W statistics. Note that we calculate the statistics by using the average rank if there is the same order in data. From these statistics, we calculate the Z-value by using standard deviation and average value. Because the distributions of U and W approximately follow the normal distribution, we can obtain asymptotic significant probabilities from the standard normal distribution table. Incidentally, the null hypothesis in either test is that there is no difference in the median of two groups.

Next, the Kruskal-Wallis test is a rank sum test that examines the difference of the median between more than three groups. Test statistics in this test are calculated by using data arranged in ascending order as well as the Wilcoxon test. We can calculate H statistics and then obtain the asymptotic significant probabilities because the distribution of H statistics approximately follows the chi-square distribution of degree of freedom K-1. Then, we can obtain the asymptotic significant probabilities from the standard normal distribution table because the distributions of these statistics approximately follow the normal distribution. Incidentally, the null hypothesis in either test is that there is no difference in the median of each group (more than three groups).

Table 10: Test of Normality

	Kolmogorov-Smirnov test (Search)*		Shapiro-Wilk test	
	Statistics	Significance probability	Statistics	Significance probability
X1	0.204	0.000	0.883	0.000
X21	0.248	0.000	0.807	0.000
X22	0.315	0.000	0.741	0.000
X23	0.285	0.000	0.861	0.000
X24	0.261	0.000	0.851	0.000
X25	0.280	0.000	0.771	0.000
X31	0.212	0.000	0.898	0.000
X32	0.245	0.000	0.866	0.000

*: Modified Lilliefors significance probability

[13] Refer to Wasserman (2007) for details of AOV based on a non-parametric method.

Tables 11-26 are the results of the analysis. From results of analysis, we found that the workers' awareness to information security is different by many attributes. In each table, *, ** and *** represent that p<10%, p<5%, and p<1%, respectively.

Table 11: Regular/Non-regular

	U	W	Z	Prob.
X1	35464.000	115664.000	-2.369	.018**
X21	38085.500	58185.500	-1.022	0.307
X22	37618.000	117818.000	-1.318	0.188
X23	39164.500	59264.500	-0.450	0.653
X24	38112.000	58212.000	-1.014	0.310
X25	35665.500	55765.500	-2.412	0.016**
X31	34539.000	114739.000	-2.878	0.004***
X32	37560.000	57660.000	-1.282	0.200

Table 12: Number of Employees

	H statistics	DF	Prob.	Size
X1	10.171	10	0.426	600
X21	19.353	10	0.036**	600
X22	7.461	10	0.681	600
X23	28.206	10	0.002***	600
X24	24.436	10	0.007***	600
X25	27.260	10	0.002***	600
X31	11.166	10	0.345	600
X32	12.557	10	0.250	600

Table 13: Degree of Infrastructure

	H statistics	DF	Prob.	Size
X1	0.882	3	0.830	600
X21	7.033	3	0.071*	600
X22	3.890	3	0.274	600
X23	10.099	3	0.018**	600
X24	13.588	3	0.004***	600
X25	21.354	3	0.000***	600
X31	8.283	3	0.041**	600
X32	12.740	3	0.005***	600

Table14: Customer Information Data Taken Outside the Firm I

	H statistics	DF	Prob.	Size
X1	5.218	2	0.074*	526
X21	8.620	2	0.013***	526
X22	11.431	2	0.003***	526
X23	13.686	2	0.001***	526
X24	14.055	2	0.001***	526
X25	13.337	2	0.001***	526
X31	19.504	2	0.000***	526
X32	9.475	2	0.009***	526

Table 15: Attachment of Customer Information Data to e-mail

	H statistics	DF	Prob.	Size
X1	9.265	2	0.010***	480
X21	3.051	2	0.217	480
X22	7.207	2	0.027**	480
X23	9.443	2	0.009***	480
X24	10.785	2	0.005***	480
X25	18.109	2	0.000***	480
X31	25.132	2	0.000***	480
X32	8.802	2	0.012***	480

Table 16: Customer Information Data Taken Outside the Firm II

	H statistics	DF	Prob.	Size
X1	2.980	2	0.225	505
X21	3.829	2	0.147	505
X22	4.990	2	0.083*	505
X23	11.820	2	0.003***	505
X24	12.518	2	0.002***	505
X25	16.769	2	0.000***	505
X31	16.578	2	0.000***	505
X32	6.838	2	0.033**	505

Table 17: Taking a Notebook Computer Outside the Firm

	H statistics	DF	Prob.	Size
X1	1.797	2	0.407	536
X21	1.933	2	0.380	536
X22	9.818	2	0.007***	536
X23	20.386	2	0.000***	536
X24	16.544	2	0.000***	536
X25	12.361	2	0.002***	536
X31	21.524	2	0.000***	536
X32	3.437	2	0.179	536

Table 18: Connecting LAN with Private Personal Computer

	H statistics	DF	Prob.	Size
X1	3.964	2	0.138	501
X21	18.866	2	0.000***	501
X22	16.762	2	0.000***	501
X23	26.487	2	0.000***	501
X24	25.681	2	0.000***	501
X25	19.483	2	0.000***	501
X31	11.742	2	0.003***	501
X32	8.362	2	0.015**	501

Table 19: Authority Handover

	U	W	Z	Prob.
X1	23243.000	147494.000	-1.412	0.158
X21	22525.000	146776.000	-1.925	0.054**
X22	21261.500	145512.500	-2.872	0.004***
X23	22454.500	146705.500	-1.989	0.047**
X24	22577.500	146828.500	-1.902	0.057*
X25	19224.000	143475.000	-4.312	0.000***
X31	25233.500	30486.500	-0.109	0.913
X32	21978.000	146229.000	-2.254	0.024**

Table 20: Stock Option

	U	W	Z	Prob.
X1	17242.500	156370.500	-1.501	0.133
X21	14992.000	154120.000	-3.267	0.001***
X22	17099.500	156227.500	-1.704	0.088*
X23	17594.000	156722.000	-1.275	0.202
X24	16477.500	155605.500	-2.137	0.033**
X25	13925.000	153053.000	-4.262	0.000***
X31	16859.000	155987.000	-1.806	0.071*
X32	16128.000	155256.000	-2.354	0.019**

Table 21: Employee Stock Ownership Program

	U	W	Z	Prob.
X1	41087.000	116165.000	-0.066	0.947
X21	37306.000	112384.000	-2.056	0.040**
X22	37548.500	112626.500	-1.999	0.046**
X23	33701.000	108779.000	-3.986	0.000***
X24	34978.500	110056.500	-3.301	0.001***
X25	33944.500	109022.500	-3.986	0.000***
X31	39394.500	114472.500	-0.945	0.344
X32	35443.000	110521.000	-2.987	0.003***

Table 22: Spin-out

	U	W	Z	Prob.
X1	18594.000	156669.000	-0.814	0.416
X21	16979.500	155054.500	-2.061	0.039**
X22	17399.000	155474.000	-1.805	0.071*
X23	17530.000	155605.000	-1.656	0.098*
X24	17925.000	156000.000	-1.350	0.177
X25	14819.500	152894.500	-3.862	0.000***
X31	16253.500	154328.500	-2.579	0.010***
X32	16591.500	154666.500	-2.318	0.020**

Table 23: Listed/Non-listed Firm

	U	W	Z	Prob.
X1	42968.000	88118.000	-1.001	0.317
X21	41325.500	86475.500	-1.850	0.064*
X22	42662.000	87812.000	-1.220	0.223
X23	40955.500	86105.500	-2.053	0.040**
X24	41180.500	86330.500	-1.935	0.053**
X25	38824.000	83974.000	-3.240	0.001***
X31	40548.000	85698.000	-2.212	0.027**
X32	42635.000	87785.000	-1.171	0.242

Table 24: Age

	H statistics	DF	Prob.	Size
X1	3.279	4	0.512	600
X21	0.537	4	0.970	600
X22	1.643	4	0.801	600
X23	1.609	4	0.807	600
X24	10.541	4	0.032**	600
X25	2.149	4	0.708	600
X31	5.872	4	0.209	600
X32	4.268	4	0.371	600

Table 25: Internet Terms of Use

	H statistics	DF	Prob.	Size
X1	5.023	6	0.541	600
X21	7.293	6	0.295	600
X22	8.829	6	0.183	600
X23	4.523	6	0.606	600
X24	7.522	6	0.275	600
X25	4.974	6	0.547	600
X31	13.168	6	0.040**	600
X32	12.914	6	0.044**	600

Table 26: Education on Information Security

	U	W	Z	Prob.
X1	44725.500	83785.500	-0.027	0.979
X21	39309.000	78369.000	-2.761	0.006***
X22	41111.500	80171.500	-1.918	0.055*
X23	32248.500	71308.500	-6.377	0.000***
X24	33323.500	72383.500	-5.817	0.000***
X25	32583.000	71643.000	-6.415	0.000***
X31	42892.000	81952.000	-0.940	0.347
X32	39031.000	78091.000	-2.853	0.004***

First, as a working pattern, differences in the median of *X1*, *X25* and *X31* in Table 5 are at a 1-5% significance level. From the Mann-Whitney test in Table 11 and the statistics in each subcategory, we cannot strictly claim that there is relationship between awareness to information security and regular and non-regular working patterns because the bigness and smallness of the medium is different in each subcategory.

Next, in organizational attributes (Tables 11-23) we have the differences in the median of many of the subcategories at a 1-10% significance level. Clearly, there are differences in the awareness to information security of workers who belong to organizations that have either some motivational systems or prohibited matter as countermeasures. From the Mann-Whitney test in Tables 19-23 and the statistics in each subcategory, awareness to the information security of workers who belong to organizations with some motivational systems is higher rather than that of workers who belong to organizations without the system. This might imply that the motivational system contributes to improving awareness to information security. In addition, we verify that awareness to the countermeasures of workers in a listed firm is higher than of workers in a non-listed firm. From the Kruskal-Wallis test in Tables 12-18 and the statistics in each subcategory, we can only know that the awareness to the information security of workers is different.

Furthermore, as individual attributes (Tables 24-26), we have a few differences in the median of subcategories excluding information security and in the educational settings. This implies that education about information security changes the workers' awareness of countermeasures. From the Mann-Whitney test in Table 26 and the statistics in each subcategory, workers who received

education on information security have a higher recognition of countermeasures than the other users including self-educated users. Therefore, education in information security is clearly very important.

Finally, we check the three hypotheses in subsection 3.1. As a result of AOV, each hypothesis cannot be affirmed. In order to achieve a higher level of workers' awareness to information security, we need to discuss countermeasures and strategies in the firm and/or in the government in the future.[14]

5. Needed Policy

This section considers the role of the government and ISPs in giving incentives to execute countermeasures and to enhance the awareness to information security on the basis of the analysis results in the previous sections. Here, we suggest what the policy for the countermeasures should be.

Information security policy in Japan has intensified in recent years since the establishment of the National Information Security Center (NISC) in April 2005 and the IT Strategic Headquarters in May 2005, which were set up to provide a fundamental and coordinating role. NISC has annual programs to implement these strategies, which together are called "Secure Japan". These strategies and programs show the grand design of the government's security policy to ensure that both public and private sectors will work together to promote the required countermeasures. In "Secure Japan", the necessity and importance of education is often pointed out. As an example of concrete countermeasures on information security education, "e-net caravan" has been implemented since April 2006 under the cooperation of MIC, the Ministry of Education, Culture, Sports, Science and Technology (MEXT) and relevant public corporations. This is an attempt to carry out lectures for parents and teachers on safe and secure Internet use. Moreover, MIC's website called "Information Security Site for Japanese" has been established since March 2003[15]. This website aims to educate Japanese people with knowledge on information security as well as providing basic information on information security measures in accordance with usage methods. Furthermore, the aforementioned Cyber Clean Center (CCC) has been provided since December 2006 as a counter-bot project through collaboration between the MIC and the Ministry of Economy, Trade and Industry (METI). This center provides information to fight against bots, information which aims at decreasing and eliminating bot-infected computers. Accumulation of these activities are expected to lead to the improved awareness in general public on information security and to help the general public realize a "developed country with matured information security" as a fundamental principle of the Second National Strategy on Information Security. In addition, "Information Security Seminars" that the IPA carries out periodically throughout Japan and other relevant training programs can be a locomotive for enhancing the awareness of information security of Internet users. These measures are meaningful and desirable from the perspective of the analysis result of this paper, i.e., those Internet users who have training on information security tend to possess a higher awareness of information security than those who do not have training.

ISPs also implement various measures on information security education. For example, there are more than 70 ISPs that participate in the operation of CCC to provide counter-bot information. ISPs also engage in enlightenment activities to enhance awareness of information security for Internet users. According to Takemura (2009a), many ISPs provide information on information security such as viruses and vulnerabilities through their own websites and weblogs mainly in order to seek the attention of their customers. In addition, some ISPs attempt to hold seminars and training courses uniquely as an activity to watch the trend of establishing management strategy to survive against fierce competition and corporate social responsibility. These activities, in tandem with government policies, are expected to contribute to enhancing awareness of information security for Internet users.

[14] Takemura and Umino (2009) discuss the role of the government and ISPs for the Internet users in order to enhance their awareness to information security.

[15] URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

Table 27 shows the main actors (organizations) that deal with information security policy and the measures undertaken in Japan.

Table 27: Main Actors Dealing with the Information Security Policy and Countermeasures in Japan

	URL	Main Objective
NISC	http://www.nisc.go.jp/	Information security policy
MIC	http://www.soumu.go.jp/	Information security policy
METI	http://www.meti.go.jp/	Information security policy
CCC	https://www.ccc.go.jp/	Counter-bot countermeasures
JADAC	http://www.dekyo.or.jp/	Countermeasures against unsolicited email
IPA	http://www.ipa.go.jp/	Countermeasures against computer viruses
JVN	http://jvn.jp/	Provision of information on vulnerabilities
JNSA	http://www.jnsa.org/	Countermeasures on network security
NPA	http://www.npa.go.jp/	Countermeasures against cyber-crimes

The government should advance support for business environments so that each firm may execute management countermeasures such as information sharing and the execution of an information security education; for instance, enhancement of public certifications such as ISMS. In addition, the government should show concrete methods and processes regarding the planning and operating of BCP, and the building of a total management system on information security, including personnel training and information sharing. Furthermore the government should continue to hold workshops and/or seminars concerning firms' countermeasures. Of course, it is also necessary to maintain the legal system that manages infringements. Enhancing these policies provide real incentives for firms to execute information security countermeasures. That is, these policies help firms to execute information security countermeasures willingly because executing the countermeasures improves their market value.

If these policies are executed the government can expect not only a growth of GDP (gross domestic product), but also the improvement of the information security level in industry and the country.

6. Concluding Remarks and Future Research

In this paper, from the viewpoint of economics, the author analyzed the interrelations between information security countermeasures and economic activities using statistical methods such as logistic regression analysis, covariance structure analysis, and AOV.

First, as a result of logistic regressions, we find that there are positive relationships between the expected effects and some management countermeasures on information security. Concretely, we find management countermeasures such as information sharing and education on information security necessary to feel a positive social effect. We suggest that by incorporating the element of information security into existing information system by enhancing the educational scheme, firms do not need to invest in information security countermeasures. By incorporating an educational scheme into existing educational scheme on ICT use, further economic effects are achieved. This is confirmed by analysis of covariance structures (Takemura and Minetaki (2009c)). In addition, we have no difference in the effect firms feel by the number of employees or by annual revenue. One the other hand, we have a difference in the effects firms feel in their dependence on information system and the Internet.

Second, the result of the analysis of the covariance structure shows that we need to build an information security system that consists of a security department, which consists of information security staff along with the clarification of their roles, building of organization gathering the information of vulnerability, education of the security staff, and knowledge share within firms. In an organization human resources and information sharing are the important two factors regarding the security system in the firm. The information security system countermeasures and educational

advances discussed in this paper can protect the value of our precious information assets, and reengineering our business processes.

Third, as a result of AOV, we can see that workers' awareness of information security is different in its attributes such as organizational attributes and the education about information security countermeasures. Workers experience a difference in awareness in organizations that offer motivation and prohibit certain countermeasures. This implies that a workers' awareness to information security and the countermeasures are affected by the environment of the organization.

An overall policy is necessary for the firm's information security countermeasures because then, we may suggest to government what advanced support for the business environment is needed so that each firm may execute the management countermeasures. Likewise, the government should show concrete methods and processes about management countermeasures. By doing so, the government can expect not only growth of GDP (gross domestic product), but also the improvement of the information security level in industry and in the country. Furthermore, we suggest that the information security education be enhanced so that the workers may appropriately execute the information security countermeasures. Therefore, such policies as the above-mentioned "e-net caravan" and "Information Security Seminars" will be effective in improving the Internet users' awareness of information security. Researches on the "economics of information security" are not only meaningful in the social sciences, but also essential in real business activities. Therefore, this type of researches needs to accumulate. 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.

Acknowledgements

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

The author is thankful to Kazunori Minetaki, Takuro Imagawa, Makoto Osajima, and Atsushi Umino for helpful comments. Any errors that remain are solely the responsibility of the author.

Reference

[1] Albrechtsen (2007). A Qualitative Study of Users' Views on Information Security. *Computer and Security*, Vol.26, pp.276-289

[2] Albrechtsen, E. & Hovden, J. (2009). The Information Security Digital Divide between Information Security Managers and Users. *Computer and Security*, Vol.28, pp.476-490

[3] Brynjolfsson, E. (2004). *Intangible Assets*. Diamond, Inc.

[4] 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, pp.137-199

[5] Cook, D. & Keromytis, A. (2006). *Cryptographics: Exploiting Graphics Cards for Security*, Springer, New York

[6] Gordon, L.A. and M.P. Loeb (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, Vol.5, pp.438-457

[7] 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.), pp.95-111, Oxford University Press, Oxford

[12] Japan Network Security Association (2008). Fiscal 2007 Information Security Incident Survey Report (Information Leakage: Projected Damages and Observations), Online Available: http://www.jnsa.org/en/reports/incident.html
[13] Liu, 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, pp.585-599
[14] Minetaki, K. & Takemura, T. (2009). An Empirical Analysis on Effects of Internal Information Circulation in Organization by Introducing Information and Communication Technologies, *RCSS Discussion Paper Series (Kansai University)*, No.80, pp.1-17.
[15] 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
[16] Takemura, T. (2007). Proposal of Information Security Policy in Telecommunication Infrastructure, In: *What is Socionetwork Strategies*, Murata, T. & Watanabe, S. (Eds.), pp.103-127, Taga-shuppan, Tokyo
[17] Takemura, T. (2009a). The 3rd Investigation of Actual Conditions Report on Information Security Countermeasures for Internet Service Providers, Kansai University
[18] Takemura, T. (2009b). A Quantitative Study on Workers' Awareness to Information Security Using the Data Collected by Web-based Survey. Mimeo (Kansai University)
[19] Takemura, T. & Ebara, H. (2008). Economic Loss Caused by Spam Mail in Each Japanese Industry, *Selected Proceedings of 1st International Conference of Social Sciences*, Vol.3, pp.29-42
[20] Takemura, T. & Minetaki, K. (2009a). The Policies for Strategic Information Security Countermeasures Improving the Market Value. *The Proceedings of 66th Conference on Japan Economic Policy Association*
[21] Takemura, T. & Minetaki, K. (2009b). An Empirical Analysis on Information Security Countermeasures. The 2nd International Conference on Social Sciences, Turkey (Social Sciences Research Society), September, 2009, forthcoming
[22] Takemura, T. & Minetaki, K. (2009c). An Empirical Study on the Effects of Information Security Countermeasures, Mimeo (Kansai University)
[23] 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)*, pp.163-168
[24] Takemura, T., Osajima, M. & Kawano, M. (2009). Economic Analysis on Information Security Countermeasures: The Case of Japanese Internet Service Providers. In *Advanced Technologies* (A. Lazinica Ed.), intechweb.org, forthcoming
[25] Takemura, T. & Umino, A. (2009). A Research on the Internet Users' Awareness to the Information Security. *Telecom Journal*, August 2009, pp.13-21
[26] 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, pp.37-59
[27] Varian, H. R. (2002). System Reliability and Free Riding. *ACM Transactions on Information and System Security*, Vol.5, pp.355-366
[28] Wasserman, L. (2007). *All of Nonparametric Statistics*, Springer