Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviors in Japan

Toshihiko Takemura
Kansai University

This paper discusses the relationship between information security awareness and behavior by analyzing data collected from a Web-based survey on information security measures in Japan. First, it is found that individuals would not have problematic behavior from the viewpoint of information security measures if the individual's awareness is higher. Next, it is found that the awareness of individuals who have problematic behavior despite being totally prohibited in the enterprise is different from individuals who do not have problematic behavior, and the awareness of individuals in the latter group is larger than the awareness of individuals in the former group, with a slightly higher probability.

INTRODUCTION

Many enterprises face business issues regarding information security. For example, there are inadequate levels of information security in organizations, risks of encountering Internet threats, and labor loss caused by spam mails. In many of the recent issues on information security, management solutions have been applied rather than with technical solutions (Thomson, 1998; Schultz, 2005). We cannot solve the problem of information security by only depending on the technology. Even if the technology is excellent, human-beings who use the technology would sometimes make errors because they are not perfect. Decreasing this human error contributes to solving the problems of information security. Therefore, along with an approach from natural science such as the development of cryptographic technology, approachs from social science such as economics, psychology and management science have started. Camp (2006) and Anderson and Moore (2009) closely review the literature on the economics of information security.

In the latter approach, many theoretical models of information security measures/investment have been conducted, or best practices based on business experience have been studied (Gordon and Loeb, 2002; Varian, 2002; Gordon and Loeb, 2006; Gordon, Loeb, Lycyshyn, 2003). They show that what presidents and managers should do as a norm and best practice of information security measures, but indeed do not tell whether or not the measures work well. Therefore, we need empirical studies for checking which measures work well. However, the number of empirical studies are few because many researchers are immediately confronted with the problem of data collection and the accumulation of micro data. Kotulic and Clark (2004) pinpoint the difficulty of conducting social surveys on information security in enterprises. The empirical studies included focus on enterprises and the studies included are for individuals. For instance, in Japan, Liu, Tanaka and Matsuura (2007) conduct analysis on an incentive to invest in organizational information security measures in Japanese enterprises. They point out that it is more important and effective to invest in intangible assets such as information security education/training

or information security management rather than building the information security system. Furthermore, Takemura and Minetaki (2010) analyze statistically the relationship between organizational information security measures and the positive business effects in Japanese enterprises. They confirm positive a relationship between them and that the effects that managers have as being different by each information security manager. Both studies suggest that enriching information security education/training is the an effective measure. This kind of study supplies beneficial information to information security programs or system managers and possesses social significance. However, aspects on behaviors and/or awareness of workers are not necessarily considered in this kind of study. So, we know the incentive to implement for organizational information security measures, but we do not know whether or not the organizational measures may give motivation for individuals who are members of organization.

On the other hand, in recent years, some studies approaching from the individual's information security awareness have appeared. Generally, these kind of studies analyze the individual's awareness and attitude to act upon information security measures based on behavioral economics and social psychology. Their challenge is novel. The current study is included into this stream. In the remaining part of this section, we briefly introduce some previous studies and position this study.

Albrechtsen (2007) conducts interview survey for some IT companies and banks in Norway and confirms that many of the workers are not especially aware of the organizational information security measures and tend to prioritize productivity of work. In addition, Albrechtsen and Hovden (2009) conduct interview surveys for information security managers and employees in some Norwegian enterprises and confirm that there is an information security digital divide between information security managers and employees in many organizations. In their discussion, they claim many of issues on information security would be caused by a lack of employee 's knowledge or awareness rather than inadequate technologies.

As with similar studies in Japan, we have Takemura (2010), and Takemura, Tanaka and Matsuura (2010). Takemura (2010) conducts a Web-based survey for employee ranks in Japanese enterprises and clarifies that information security awareness is different by organizational attributes and individual attributes through statistical analyses. Besides, Takemura, Tanaka and Matsuura (2010) conduct another Web-based survey for information security managers and employee ranks in Japanese enterprises and clarifies that there are awareness gaps on effects of some information security measures between the managers and the employee ranks. Then, they indicate that employee ranks need to improve their information security awareness in order to upgrade the level of organizational information security measure, and they propose to provide information security education and training.

Many previous studies claim that it is important to make employee ranks improve their information security awareness through information security education and training. As the next step, we need to study the relationship between the awareness and behavior. The reason is simple. Even if employee ranks can improve their information security awareness, it is meaningless unless the improvement reflects on their behaviors. That is, we need to investigate how they behave correctly from the viewpoint of information security measure in addition to improving their awareness. Therefore, this paper aims to discuss the relationship between information security awareness and behavior. This purpose is approached by statistically analyzing data collected from Web-based survey on information security measure in Japan. This paper is to contribute to the knowledge about not only the organizational perspective, but also the user's perspective on information security. This study also provides basic information on whether or not information security awareness leads to correct behavior from the viewpoint of information security measures when we can alter the workers' awareness. Furthermore, we supply material for discussing effective information security measures.

FRAMEWORK

Web-based Survey

A Web-based survey well-used in the field of marketing is employed as the survey method. However, a Web-based survey has statistical problems called Internet bias because respondents of Web-based surveys are not selected by random sampling (Cooper, 2000). So, it is natural that we carefully need

to discuss employing a Web-based survey. The Japan Institute for Labour Policy and Training (2005) suggests that it is not necessarily undesirable to use a Web-based survey if the aim of the survey is to offer judgmental materials that are useful for individual and organizational decision making. Of course, we must discuss the accuracy of the survey, but unfortunately we cannot make comparison as there are no similar surveys other than the Web-based surveys. So, we presume that data sets are useful for reasonable analysis but the sample has limited potential for generalizing. In other words, respondents are limited to being individuals registered with the Internet survey company and are somewhat interested in information security measures, but not general individuals.

Survey Design and Survey Overview

The author conducted a Web-based survey entitled "Survey on Japanese workers' awareness and behavior to information security measures" in March 2010. This study does not aim at presenting a representative picture of organizational information security measures, but rather aims at exploring workers' awareness and behaviors toward information security measures. Since it can be assumed that the respondents are competent and interested in information security, we can also assume that they give a reliable and correct assessment. Hence, the quality and reliability of the study also improves, which might not have been the case for a broader sample of respondents with regard to knowledge and experience.

Subjects of this survey are Japanese people who have been working for more than two years in the same enterprise. This survey asks more than 50 questions, items such as attitude toward risks, individual attributes such as gender and annual income, information security awareness and organizational attributes they belong to. The respondents are pre-arranged by gender, age group and living area in Japan. To arrange three dimensions, we use the data on the size of the population by age group and prefecture divisions in "the number of population and household movements based on basic resident registration on the 31st March 2008" (URL: http://www.stat.go.jp/data/roudou/index.htm).

Generally, a Web-based survey can achieve high collection rates. This survey includes 1,299 respondents (collection rate is around 84.2%).

Table 1 shows the distribution of type and size for the respondents' organizations. The respondents in this survey are well distributed among these variables.

Information Security Awareness and Behavior

First of all, in this study to measure information security awareness, we use six questionnaires shown in Table 2. These questionnaires are used in Japanese some studies (Takemura, 2010; Takemura, Tanaka and Matsuura, 2010). Each item in Table 2 is assessed on a seven-point scale from 1 = strictly disagree to 7 = strictly agree. Therefore, in this study it is assumed that information security awareness is high if the score of item is high. In addition, we use the score (numerical number) assigned on measuring information security awareness as micro data in the following analysis. Table 2 shows frequency distribution and row ratio of each item that respondents subjectively assessed in the survey.

TABLE 1
DEMOGRAPHIC DATA FOR THE RESPONDENTS OF THE SURVEY

Attribute	Contents					
Organizational attribute	Degree of publicness			Listed/non-listed option		
	very few	333	25.64%	Listed enterprise	591	
	low	483	37.18%	Non-listed enterprise	45.50%	
	high	338	26.02%		708	
	very high	145	11.16%		54.50%	
	Number of employees (Persons)			Annual sales (Yen)		
	< 50	292	22.48%	< 50 million	73	5.62%
	50-99	75	5.77%	50-100 million	38	2.93%
	100-999	334	25.71%	100-500 million	108	
	1000-4999	171	13.16%	0.5-3 billion	8.31%	
	>5000	399	30.72%	> 3 billion	106	
	unclear	28	2.16%	unclear	8.16%	
					946	
					72.83%	
					28	2.16%
Individual attribute	Gender			Working pattern		
	Male	712	54.81%	Regular	801	
	Female	587	45.19%	Non-regular	61.66%	
					498	
					38.34%	
	Age group			Number of career change		
	15-20's	240	18.48%	Nothing	478	
	30's	320	24.63%	1 or 2 times	36.80%	
	40's	289	22.25%	3-5 times	408	
	50's	270	20.79%	Over 5 times	31.41%	
	Over 60's	180	13.86%		243	
					18.71%	
					170	
					13.09%	
	Education					
	Elementary/Junior high school	341	26.50%	University	569	
				Graduate school	44.21%	
	High school	35	2.72%	Other	59	4.58%
	Junior college	147	11.42%		136	
					10.57%	

The items in A1)-A4) measure awareness to problematic behavior from the viewpoint of information security measures. From these items, we can investigate whether or not individuals correctly understand that these are the problematic behaviors. On the contrary, the items in A5)-A6) measure awareness to collecting information on information security actively. From these items, we can investigate whether or not individuals understand the necessity of collecting information on information security for the purpose of catching up the latest trend of the security and/or avoiding the various threats.

TABLE 2
SIGNIFICANT VARIABLES FROM THE REGRESSION ANALYSIS

	Strictly Low <- Awareness -> Strictly High						
	1	2	3	4	5	6	7
A1)	26	34	37	172	190	347	493
	2.00	2.62	2.85	13.24	14.63	26.71	37.95
A2)	17	53	66	371	272	313	207
	1.31	4.08	5.08	28.56	20.94	24.10	15.94
A3)	22	54	136	689	236	120	42
	1.69	4.16	10.47	53.04	18.17	9.24	3.23
A4)	33	50	78	218	217	361	342
	2.54	3.85	6.00	16.78	16.71	27.79	26.33
A5)	15	29	65	461	471	187	71
	1.15	2.23	5.00	35.49	36.26	14.40	5.47
A6)	15	24	55	306	525	290	84
	1.15	1.85	4.23	23.56	40.42	22.32	6.47

A1) It is problematic behavior that business person forwards the mails to his friends when he receive chain mails.
A2) It is problematic behavior that business person connects the Internet by using others' wireless networks not encrypted.
A3) It is problematic behavior that business person would give priority to productivity of work rather than hewing to information security measure.
A4) It is problematic behavior that business person uses a computer without anti-virus software.
A5) Business person should learn information security himself with willingness
A6) Business person should receive education for information security

Next, in this study, we use items with regard to respondents' behaviors or experiences which correspond to seven questionnaires shown in Table 2. Experiences with regard to items in A1)-A3) are evaluated on a four-point scale (1=Never experience, 2=sometimes experience, 3=experience once in a while and 4= frequently experience). In addition, experiences with regard to items in A4)-A6) are evaluated on a binary scale (1=Yes and 2=No). Therefore, in this study it is assumed that individual fairly behaves from the viewpoint of information security measure is high if score of item is low. Tables 3 and 4 show frequency distribution and row ratio of each item.

TABLE 3
EXPERIMENCE WITH REGARD TO INFORMATION SECURITY (1)

	Never <- Experience -> Frequently			
	1	2	3	4
B1) I forwards the mails to my friends when I receive chain mails.	1,136	124	38	1
	87.45	9.55	2.93	0.08
B2) I connect the Internet by using others' wireless networks not encrypted.	1,106	122	59	12
	85.14	9.39	4.54	0.92
B3) I prioritize productivity of work rather over hewing to information security measure.	771	348	155	25
	59.35	26.79	11.93	1.92

TABLE 4
EXPERIMENCE WITH REGARD TO INFORMATION SECURITY (2)

	1. Yes	2. No
B4) I install anti-virus software in my computer	1,111	188
	85.53	14.47
B5) I learn information security himself with willingness	279	1,020
	21.48	78.52
B6) I receive education for information security	325	974
	25.02	74.98

From Table 3, with regard to problematic behavior in B1) and B2), it is found that about 86% of respondents do not take the problematic behavior from the viewpoint of information security measure. On the other hand, from Table 4, it is found that almost respondents have no qualification with regard to information security and that around 75% of the respondents do not necessarily collect information on the latest trend of information security.

Third, as an example, we go over four items with regard to some organizational measures that prevent information the leaks in Table 5. In recent years, many Japanese enterprises have implemented some organizational measure to prevent information leaks. Many of the measures are extreme and totally prohibit employees from use of customer information data in external organizations and/or access to Websites such as 2 Channel. The measures are principally implemented by information security managers or information system managers. They can forcibly have control over employees by implementing these measures. Table 5 shows frequency distribution. The column of Table 5 represents the degree of prohibition in enterprises; totally prohibited or not prohibited, and the row represents existence or nonexistence of respondent's experience.

Here, we are interested in respondents who take the behavior leading to information leak despite totally prohibited in enterprise. Whatever the reason is, the respondents come to break rules.

TABLE 5
SIGNIFICANT VARIABLES FROM THE REGRESSION ANALYSIS

Item \ Experience		Experience	No experience
C1) External taking out of customer information data by portable devices such as USBs	Totally prohibited	77	433
	Not prohibited	96	139
C2) Accessing to Website such as 2 Channel	Totally prohibited	49	545
	Not prohibited	150	187
C3) External taking out of customer information data by printed paper	Totally prohibited	53	447
	Not prohibited	81	150
C4) taking out mobile computer enterprise-owned	Totally prohibited	44	375
	Not prohibited	89	153

In fact, from Table 5, we find that in organizations, around 65% of respondents belong to these items are totally prohibited. Note that respondents who provided unclear answers are excluded from Table 5. From Table 5, it is found that about 8.2-15.1% of respondents who have behavior which may lead to information leaks despite being in a totally prohibited enterprise. In section 3.2, we will conduct an analysis of respondents who have problematic behavior despite being in a totally prohibited enterprise.

Hypotheses and Method

First, I investigated the relationship between information security awareness and behavior by correlation analysis. Since information security awareness and behaviors are measured by ordinal scales, I employed an analysis of Spearman's rank correlation coefficient in this study. Analysis of Spearman's

rank correlation coefficient offers an advantage of assuming neither regularity nor the homoscedasticity of data. In this analysis, the correlation coefficients between two variables are computed and the coefficients are tested statistically. The analysis tests whether or not Spearman's rank correlation coefficient (Spearman's rho) is zero. Then, null hypothesis is that the population correlation coefficient is zero. Therefore, if the null hypothesis is rejected, we would find that there is positive or negative relation between two variables.

In this study, I make the following hypotheses:

H-1) Individuals who correctly understand the problematic behaviors do not take such problematic behaviors.

H-2) Individuals who understand the necessity of collecting information on information security take such behaviors.

Strictly speaking, a correlation analysis clarifies a relationship between two variables, but does not clarify a causal correlation. Therefore, even if there is a positive relationship between awareness and behavior, we cannot judge awareness change behavior. In this study, it is assumes awareness change behaviors. In the near future, I will check for a causal correlation between awareness and behavior from the viewpoint of social psychology. For instance, if she correctly understands that forwarding the mails to her friends is problematic behavior, she would not forward the mails to her friends. Similarly, if she understands the necessity of receiving education for information security, she would receive information security education. That is, in these examples, Spearman's rank correlation coefficient (Spearman's rho) between A1) (resp. A6)) and B1) (resp. B6)) is expected to be negative (sign). In the other cases, the coefficients are expected to be negative.

Next, an examination of whether or not information security awareness of respondents differs according to respondents' behavior to the concrete measure that enterprises implement using the Mann-Whitney rank sum test. The Mann-Whitney rank-sum test examines whether that two independent samples are from populations with the same distribution by using the Mann-Whitney (two-sample) statistic. This test is a nonparametric method and has features where data do not have to follow to normal distributions. In this analysis, the data are ranked without regard to the sample to which they belong to, Mann-Whitney's U statistic is calculated and the statistics calculated are tested statistically. Here, it tests the null hypothesis that two independent samples are from populations with the same distribution. Concretely, in this study, two independent groups are one group of respondents who take problematic behavior despite totally prohibited in enterprise and the other group of respondents who do not take problematic behavior. I examine whether or not information security awareness of members in both groups differ. If a relationship between information security awareness and behaviors is accepted, then we expect that information security awareness of member in both groups differs.

RESULTS

Results of Analysis of Spearman's Rank Correlation Coefficient

Table 6 shows results of analysis of Spearman's rank correlation coefficient with regard to relations between information security awareness and behaviors.

TABLE 6
SPEARMAN RANK CORRELATION COEFFICIENT RESULTS

Case		Spearman's rho	Pr>|t|
1	A1) vs B1)	-0.3214	0.0000
2	A2) vs B2)	-0.2164	0.0000
3	A3) vs B3)	-0.0223	0.4229
4	A4) vs B4)	-0.2916	0.0000
5	A5) vs B5)	-0.2578	0.0000
6	A6) vs B6)	-0.2321	0.0000

From Table 6, we confirm that the relationship between information security awareness and behavior has a negative relationship in all cases excluding Case 3. In addition, with Spearman's rho, these cases are statistically significant at the 1% level. These results support two hypotheses, H-1) and H-2). In other words, it is found that individual would not take problematic behavior from the viewpoint of information security measure if individual's information security awareness is higher. Therefore, we can imagine that improving an individual's information security awareness leads to correct behaviors from the viewpoint of information security measure.

On the other hand, with regard to Case 3, this asserting is not valid because Spearman's rho of this case is not statistically significant. That is, relation between information security awareness and behavior on prioritizing productivity of work rather over hewing to information security measure is independent. Thus, even if individual considers that prioritizing productivity of work rather over hewing to information security measure is problematic behavior, his awareness would not affect his behavior. With regard to relation between productivity of work and information security measure, the other factors may influence to behavior, not the information security awareness. Albrechtsen (2007) points out that it is important to clarify relation between productivity of work and information security measure from the viewpoint of implementing the effective information security measure in organization. Therefore, additional analysis would be desired.

Results of the Mann-Whitney Rank-Sum Test

Table 7 shows the results of the Mann-Whitney rank-sum test with regard to the information security awareness of respondents who belong to enterprises that implement the organizational measures to prevent information leak. Note that in Table 7 U is Mann-Whitney's U statistic and "p" is probability that the variable for experience group is larger than the variable for no experience group. The probability is computed by $p=U/(n_e n_n)$, where n_e and n_n represent the size of two groups, respectively.

TABLE 7
MANN-WHITNEY RANK SUM RESULTS

	C1				C2			
	U	z	Pr>|z|	p	U	z	Pr>|z|	p
A1)	13335	-2.936	0.0033	0.400	7960.5	-4.903	0.0000	0.298
A2)	12932.5	-3.219	0.0013	0.388	9057	-3.824	0.0001	0.339
A3)	14519	-1.924	0.0543	0.435	10534.5	-2.618	0.0089	0.394
A4)	14361.5	-1.993	0.0462	0.431	8745.5	-4.116	0.0000	0.327
A5)	14941	-1.520	0.1285	0.448	9727	-3.301	0.0010	0.364
A6)	14591	-1.821	0.0687	0.438	7798.5	-5.062	0.0000	0.292
	C3				C4			
	U	z	Pr>|z|	p	U	z	Pr>|z|	p
A1)	8985	-3.021	0.0025	0.379	5390.5	-3.921	0.0001	0.327
A2)	8174	-3.779	0.0002	0.345	5147.5	-4.179	0.0000	0.312
A3)	11121.5	-0.783	0.4337	0.469	6903	-1.922	0.0546	0.418
A4)	9152	-2.780	0.0054	0.386	5528.5	-3.672	0.0002	0.335
A5)	10095	-1.844	0.0652	0.426	6409.5	-2.533	0.0113	0.388
A6)	9901.5	-2.043	0.0411	0.418	5341	-3.996	0.0001	0.324

It is found that the respondents' information security awareness is different in many items. With regard to A3), in almost all cases (median of) information security awareness of member in two groups is not different at least at a 5% significant level. After all, with regard to productivity of work, other factors may influence the behavior, not the information security awareness. In addition, with regard to A5) in C1 and C3, (median of) information security awareness of member in two groups is not different at least 5% significant level, too. Furthermore, the probability that the awareness of members in the experience group is larger than the awareness of members in the non-experience group at less than about 0.5 in all cases. That is, (median of) information security awareness of member in group who take problematic behavior

despite totally prohibited in the enterprise is different from one of the other groups who do not have problematic behavior, and the information security awareness of members in the latter group is larger than the awareness of members in the former group with slightly high probability.

SUMMARY AND FUTURE WORK

This paper discusses the relationship between information security awareness and behavior. This purpose is approached by statistically analyzing data collected from a Web-based survey on information security measures in Japan. First of all, from the results of the analysis of Spearman's rank correlation coefficient, it is found that individuals would not have problematic behavior from the viewpoint of information security measure if individual's information security awareness is higher. Next, from the results of the Mann-Whitney rank-sum test, it is found that information security awareness of individuals who have problematic behavior despite being in a totally prohibited enterprise is different from one of individuals who do not have problematic behavior, and the information security awareness of individuals in the latter group is larger than the awareness of individuals in the former group with a slightly higher probability. However, with regard to the item that prioritizes productivity of work rather than information security measures, we can confirm neither relationship with behavior nor difference of information security awareness of member in two groups exists.

From the results of analyses, some employee ranks break rules even if enterprises implement some organizational measures to prevent information leaks. If anything, their information security awareness tends to be low. We should look to improve their awareness through information security education and training, as one method noted.

Finally, let us briefly explain future works. As mentioned in section 1, studies on the "economics of information security" are not only meaningful in the social sciences, but also essential in business practices. Researchers have an order of mission that continues to deeply analyze information security measures by approaching them from the social sciences. Therefore, from the other aspects, we will supply more empirical studies by using some statistical methods and micro data collected from the survey in the near future.

REFERENCES

Albrechtsen, E. (2007). A Qualitative Study of Users' Views on Information Security. *Computer and Security*, 26, 276-289.

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

Anderson, R., & Moore, T. (2009). Information Security: Where Computer Science, Economics and Psychology Meet. *Philosophical Transactions of the Royal Society*, 367, 2717-2727.

Camp, L.J. (2006). The State of Economics of Information Security. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.6038&rep=rep1&type=pdf, 2006

Couper, M.P. (2000). Web Surveys: A Review of Issues and Approaches. *Public Opinion Quarterly*, 64, 464-494.

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

Gordon, L.A., Loeb, M.P., & Lycyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, 22, (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: Oxford University Press.

Kotulic, A.G., & Clark, J.G. (2004). Why There Aren't More Information Security Research Studies. *Information and Management*, 41, 597-607.

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 Japan Digital Courier*, 3, 585-599.

Schultz, E. (2005). The Human Factor in Security. *Computers and Security*, 24, 425-426.

Takemura, T. (2010). A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey. *American Journal of Economics and Business Administration*, 2, (1), 20-26.

Takemura, T., & Minetaki, K. (2010). An Empirical Analysis on Information Security Management and the Effects. *Journal of Economic Policy Studies*, 7, (2), 46-49 (in Japanese).

Takemura, T., Tanaka, H., & Matsuura, K. (2010). Awareness Gaps on Effects of Information Security Measure between Managers and Employees: An Empirical Study Using Micro Data Collected from Web-based Survey. *Short Paper Proceedings of the Fourth IFIP WG 11.11 International Conference on Trust management*, 25-32.

Thomson, M.E., & Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively. *Information Management and Computer Security*, 6, (4), 167-173.

The Japan Institute for Labour Policy and Training (2005). Can the Internet Survey Be Used for the Social Survey?: A result by Experiment. *Reports on Labour Policy* 17 (in Japanese).

Varian, H. R. (2002). System Reliability and Free Riding. *ACM Transactions on Information and System Security*, 5, 355-366.