IPSJ Journal Vol. 52 No. 7 2087–2096 (July 2011)

Regular Paper

Analysis of Awareness Gap between Security Managers and Workers in an Organization with Regard to the Effectiveness of the Information Security Measures

Toshihiko Takemura,[†1] Hideyuki Tanaka[†2] and Kanta Matsuura[†2]

In this paper, we investigate the awareness gaps between information security managers and workers with regard to the effectiveness of organizational information security measures in Japanese organizations by analyzing micro data from two Web-based surveys of information security managers and workers. As a result, we find that there are no awareness gaps between information security managers and workers with regard to the effects of the organizational information security in large companies. However, we find that awareness gaps between them tend to exist in small or medium-sized companies. Next, we argue how to bridge the gaps. We propose that information security managers could implement the two-sided organizational measures by communicating with workers in their organizations.

1. Introduction

Generally, in many organizations there are some persons with a high level of skills and knowledge of ICT and information security, and other persons without a sufficient level of knowledge and skills. Installing security technology in the organization would protect users uniformly from the threats even if persons have a different level of skill and knowledge. This is a product of accumulating researches on security technologies such as cryptographic technology and self-defense networking, and is one of the effective measures against the threats. However, as newspapers sometimes report, information security accidents occur. This implies that the technological measures cannot cover these issues alone [1),2)]. These issues arise due to human error rather than adopting the inadequacy in the security technologies. Therefore, it requires an approach from social science to challenge to solve these issues within the organization and the errors made by human beings. In the past decade, studies on information security in social science have been actively conducted [⋆1].

In addition, the other reason that approaches from social science are adopted is that information security accidents and troubles are becoming impactful issues in society. There are several empirical studies on the impact of economic loss caused by security incidents and system troubles [5)–8)]. For example, it is reported that the average amount of loss per one illegal access was $85,621 and the average amount of loss per one virus damage was $69,125, respectively [5)]. Additionally, it is estimated that the total amount of Japanese GDP loss caused by spam mails was around $46,400 billion per year in 2004 [8)]. These studies imply that huge losses occur unless enough measures are implemented. Therefore, these studies give incentives for implementing organizational information security measures by inspiring a feeling of fear.

On the other hand, there are some empirical studies that show how implementing information security measures contributes to business performance [9),10)]. Implementing some information security measures contributes to the improvement of the market value and the assessment of the organization. Therefore, results from these researches give an incentive for implementing the measure to organizations proactively. But, unfortunately the results cannot explain why information security accidents occur even if the measures are implemented in an organization.

Recently, as approaches from social psychology and behavioral economics, it garners attention to investigate effective information security measures from the perspectives on awareness and behaviors [11)–19)]. These approaches are novel and offer interesting results. Some empirical studies investigate their views on and experience of information security practices in organizations and tell that effects of the measures may be not worked enough if there are any differences on assessment between information security managers and workers with regard to the organizational information security measures [11)–13)]. In other words, employing

†1 Kansai University
†2 The University of Tokyo

⋆1 Empirical study on information security has just started in around 2000 and the studies from various perspectives have been promoted in a decade. For details, refer to the comprehensive survey articles reviewing and summarizing these studies [3),4)].

workers who do not understand the importance of the organizational measures may deteriorate effects on the measures even if organizations equip with excellent security technology. In addition, these studies argue that the basis arises from low level of worker's awareness or lack of knowledge with regard to information security and then propose the necessity of education and training for enhancing information security awareness [15),18)].

This paper aims to investigate awareness gaps between information security managers and workers in Japanese organizations with regard to the effectiveness of organizational information security measures by exploring their views and experience of information security practices. Here, awareness gap means difference between information security managers and workers with regard to accepting the effectiveness of organizational information security measures. In the previous studies, it is considered that the gaps arise from because there are some workers who prioritize completing day to day works over complying with the information security measures [11),17)]. This purpose is approached by analyzing micro data from two Web-based surveys of information security managers and workers, which we conducted, quantitatively [⋆1]. There, we investigate whether or not there are awareness gaps in Japanese organizations. This result of analysis would offer significant knowledge on the organizational information security measures to information security managers.

The paper consists of the following sections. In Section 2, we explain the design of surveys used in this paper, and then summarize data sources from these surveys. In addition, we show our hypotheses and briefly explain the statistical method. Results and discussion are interwoven in Section 3. Finally, concluding remarks and future works are shown in Section 4.

2. Surveys and Analysis

2.1 The Background of Study

Comparing with the usual surveys, it is extremely difficult to conduct surveys on organizational information security measure. The reason is simple. Information security is one of the most sensitive themes and there is a desire not to share information about information security performance with outsiders [20)]. Therefore, it is not expected that collection rate in mail survey is high. Consequently, messages and implications of quantitative analysis based on data from the survey become sometimes restrictive [⋆2]. Similarly, messages and implications of qualitative analysis based on information from interview survey would be restrictive. For example, the sample size (the number of respondents) of mail survey for information security managers in several Norwegian organizations and mail survey for users working in a Norwegian public agency that Albrechtsen and Hovden conducted are 87 and 151, respectively [12)]. Previously, Kotulic and Clark experienced the same response rate problem in a US study of information security management effectiveness, as they received only 67 completed questionnaires out of a total of 1,474 possible respondents [20)]. However, many of these studies have fruitful implications.

The difficulty of collecting micro data from the survey is barrier against empirical studies. To break this barrier, we employ a Web-based survey as survey method. A Web-based survey is well-used in the field of marketing. On the other hand, it is known that this survey has the Internet bias. That is, the representativeness of general (intended) population may not be guaranteed because the survey is not necessarily based on a random sampling. This problem has not been solved yet [21),22)]. If subjects are interpreted as individuals who register with a Japanese Internet survey company, we could see no problem and analyze it [⋆3].

2.2 Outline of Two Surveys

In this paper, we use data from two independent surveys: a survey of Japanese information security managers and a survey of Japanese workers.

2.2.1 Survey of Information Security Managers

The survey of information security managers (manager survey) was conducted by a Web-based survey method in November, 2008. The purpose of this survey is

⋆1 Technological issues are dealt with only in a brief manner. Focusing on non-technological issues of information security makes comparisons easier as well as richer, as it is likely that many users have no specific insight into the technological aspects of information security.

⋆2 Because micro data used in previous studies are restrictive, these studies naturally contain certain weakness of the analytical approach.

⋆3 We presume that these data sets are useful for reasonable analysis. We have no intention of ignoring problem of the Internet bias. Currently, studies on representativeness of data from the Web-based survey are promoted. In the near future, we anticipate development of it and will develop this study.

Table 1 Demographic data for the organizations of the manager survey and the worker survey.

		Manager survey (%)	Worker survey (%)
Listed option	Listed company	17.80	52.87
	Unlisted company	82.20	47.13
Degree of public nature of business	Very low	28.40	27.60
	Low	36.80	33.40
	High	21.80	28.47
	Very high	13.00	10.53
Annual sales (yen)	<50 million	14.20	10.07
	50–100 million	8.00	6.73
	100–500 million	19.60	13.53
	0.5–3 billion	18.00	13.07
	>3 billion	40.20	56.6
Number of employees	1–49	32.20	19.53
	50–299	27.20	21.13
	300–999	15.00	13.80
	>1,000	25.60	45.54

to grasp the current picture of information security measures implemented within Japanese organizations. Respondents to this survey are information security managers or information system managers who have at least two years of work experience with information security, especially network security, in the same organization [⋆1]. Collection rate in manager survey is 100% and sample size is 500.

The number of survey items is more than 50. For example, there are questions on whether the organizational measures were implemented or not, and questions regarding perceived information security performance of the organization, and so on. In addition, we have attributes such as gender, age, and characteristics of organization which the respondent belongs to.

Table 1 shows demographic data for the organizations which the managers belong to.

In the manager survey there are some questions with regard to the problems on the organizational information security that the managers experience. According to the result of manager survey, many respondents point out that usual workers' information awareness is at low level and that the criterion of cost-benefit performance with regard to investing in information security measures is incomprehensible.

2.2.2 Survey of Workers

The survey of workers (worker survey) was conducted by a Web-based survey method in March, 2009. The purpose of worker survey is to investigate usual workers' information security awareness and behaviors within Japanese organizations. Respondents to this survey are workers who have at least two years working experience in the same organization. Collection rate in worker survey is 100% and sample size is 1,500.

The number of survey items is more than 50 including individual attributions and organizational attributes. For instance, there are questions with regard to the organizational measures implemented, and questions with regard to their information security awareness.

Table 1 shows demographic data for the organizations which the workers belong to.

In addition, the worker survey shows that many respondents understand the importance of implementing the information security measures, but that some respondents do not comply with the measures rightly in their day to day work. This survey reveals that some workers are unsatisfied with the organizational measures. This is consistent with the view of previous studies [11),12),18)].

2.2.3 Overviews of Two Surveys

The data sets of two surveys were collected for purposes that differed slightly from the objective of this paper [⋆2]. In this respect, the present approach is a secondary analysis of available data. In other words, these surveys are not originally designed for the current study. However, the two surveys were designed in a way that made the present comparative study possible since the two surveys included a set of questions relevant to the present comparative study.

Since it can be assumed that the respondents are competent and interested in information security, we can also assume that they assess correctly the effectiveness of the information security measures. Hence, the quality and reliability of

⋆1 A condition on the manager who works at least two years at the same organization is imposed because of comparing with situation two years ago.

⋆2 If you want to see slips of these surveys, please contact the corresponding author.

Table 2 Ratio of implementating organizational information security measures (%).

	Manager survey	Worker survey
Establishment of information security policy	59.20	55.07
Information security education and training	58.00	62.80
Installation of firewall or firewall applications	84.60	75.93
Establishment of information security department	49.40	48.60

the study also improves though it might not have been the case for a broader sample of respondents regarding knowledge and experience.

In the same way as on the previous studies, the current study inescapably contains certain weakness of the analytical approach. Though, we believe to provide a breakthrough of the studies in the future.

2.3 The Data Source and Statistical Analysis

Our paper does not aim at presenting a representative picture of organizational information security measures, but rather aims at exploring awareness gap between information security managers and workers with regard to the effectiveness of the measures.

As mentioned above, two surveys have the some common questions and we used the question with regard to the comprehensive assessment on the effectiveness of the information security measures that are implemented in respondents' organizations for the purpose of analysis. In this paper, the organizational information security measures are introducing information security technologies, such as firewall system and anti-virus software, and adopting information security management, such as establishment of information security policy.

If the information security measures implemented are different in the organizations, the assessment of the effectiveness would be different. Thus, **Table 2** shows ratio of the organizational measures implemented from each survey. In both surveys, the most used item is "installation of firewall or firewall applications." Compared with two surveys, it is similar to the ratio of organizational information security measures implemented.

We adopt nine expected effects shown in **Table 3**, which are introduced in the survey which a Japanese research company conducted [23].

In each survey, we ask questions with regard to which you assess on each effect from your experience or report in your organization or workplace. By the managers and workers, these effects are assessed on a four-point scale from 1 = no effect to 4 = very good effect. Wording in these surveys follows to the survey mentioned above.

Table 3 Effectives of the measures.

Item	Contents
E1	Reviewing of information asset
E2	Reviewing and modifying of business process
E3	Improving of users' information security awareness
E4	Advancement of understanding importance of risk management
E5	Promoting of information sharing in organization
E6	Improving of evaluation from business partners and/or customers
E7	Strengthening of competing power
E8	Promoting of CSR
E9	Improving of quality of service and/or goods provided

These are intermediate effects that contribute to improve market value, and are divided into the effect within the organization and the effect in the market [10]. In addition, E1-E5 are regarded as the former effect and E6-E9 are regarded as the latter one [⋆1]. These effects are able to be accepted and assessed by not only the information security managers but also workers.

In recent years, researchers actively analyze micro data from various surveys in economics or behavioral economics. Many of surveys have some questions which are subjectively assessed by respondents. The treatment on subjective questionnaires is widely discussed and employed in many studies [24].

Table 4 represents the statistics of the respondents' assessment on the effects in two surveys and **Fig. 1** shows the distribution of their assessment on the effects. Compared with the mean of data from two surveys, the mean of the worker survey is slightly higher than one of the manager survey. On the other hand, data from the manager survey varies widely because the standard deviation of the latter is smaller than the former.

The effects assessed by many of the managers and workers is E4 (advancement of understanding importance of risk management).

In this paper, we explore awareness gap between information security managers and workers with regard to the effectiveness of the measures. This exploring

⋆1 Note that we do not focus on the difference between the effects shown in Table 3.

Table 4 The descriptive statistics of the respondents' assessment on the effects.

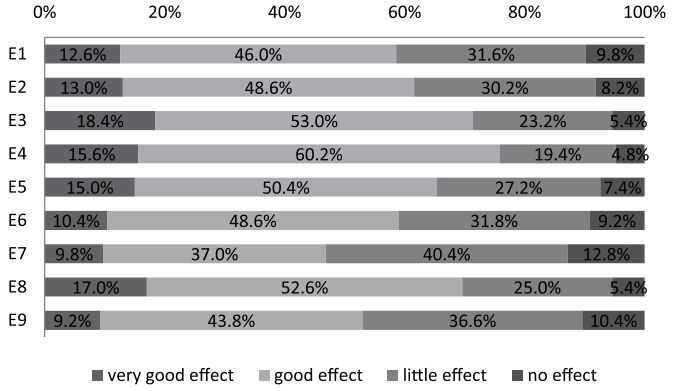
Effect	Manager survey		Worker survey	
	Mean	Std. Dev.	Mean	Std. Dev.
E1	2.614	0.8284786	2.867	0.6577903
E2	2.664	0.8052334	2.851	0.6624632
E3	2.844	0.7803088	3.030	0.6324819
E4	2.866	0.7246338	3.047	0.6164519
E5	2.73	0.8039856	2.897	0.6640403
E6	2.602	0.7955261	2.800	0.6774752
E7	2.438	0.8363941	2.701	0.6998510
E8	2.812	0.7757962	2.993	0.6482559
E9	2.518	0.8018491	2.761	0.7031234

becomes first step for discussing the effectiveness of organizational information security measure. As mentioned in the previous studies, it is expected that the effects of the measures (Table 3) are worked if there are not differences between information security managers and workers with regard to assessment of the organizational information security measures [12]. Thus, we expect that there are no differences between the managers and the workers with regard to the effects accepted from implementing the measures. Given that there are differences, we have to argue how to bridge the gap as the next step.

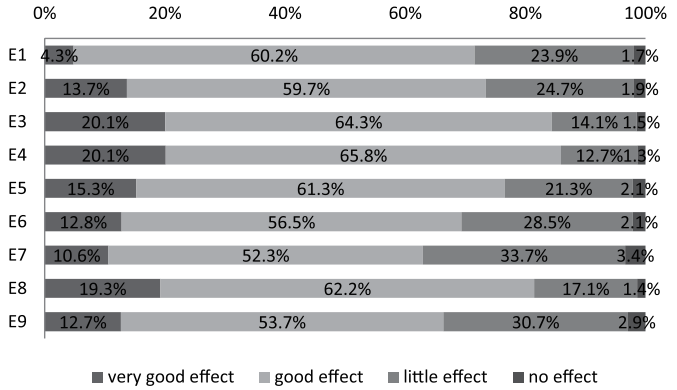
As showed in Table 1, two surveys have the respondents who belong to the organizations with various organizational attributes such as company size. Thus, we test whether or not there are significant difference between the managers and the workers with regard to assessment of the organizational measures by controlling the organizational attributes in Table 1.

Categories 1–6 in **Table 5** are made based on demographic data in Table 1. Categories 3 and 4 represent degree of public nature of business in the organization which the respondents belong to. If the respondents select 1: very low or 2: low, their organization would be included in Category 3. Otherwise, their organization would be included in Category 4. In addition, if the respondents answer that the number of employees in their organization is under 1,000 persons, they would be included in Category 5. Otherwise, they would be included in Category 6. The number of employees is regarded as company size.

Because the effects are assessed on a four-point scale, we have to employ nonparametric method with multiple comparisons. As famous nonparametric



(a) Manager survey



(b) Worker survey

Fig. 1 Distribution of the respondents' assessment on the effects.

method, there are Mann-Whitney rank-sum test with Bonferroni correction procedure or multiple comparison such as Steel-Dwass test and Shirley-Williams test [25]. In this paper, we employ Mann-Whitney rank-sum test with Bonferroni correction.

For the convenience of readers, we briefly explain the procedure. The Mann-Whitney rank-sum test examines whether two independent samples are from populations with the same distribution by using the Mann-Whitney (two-sample)

statistics. For Mann-Whitney rank-sum test, there are two independent groups, X_1 and X_2, and we have a sample of size n_1 from X_1 and another of size n_2 from X_2.

The data are ranked with regard to the sample which they belong to. If the data are tied, average ranks are used. Mann-Whitney's U statistic is the number of pairs (X_{1i}, X_{2j}) such as $X_{1i} > X_{2j}$. The statistics is calculated by

$$U = T_1 - \frac{n_1(n_1+1)}{2}$$

where T_1 is Wilcoxon's test statistic is the sum of the ranks for data in X_1 ⋆1.

Average and variance of T_1 are calculated by using Fisher's principle of randomization and we obtain z statistics using a normal approximation.

Next, we have to perform multiple sample contrasts because the Type I error rate tends to become inflated. Therefore, the initial (original) level of risk, or p, must be adjusted. The procedure is the Bonferroni correction procedure, shown in the following formula, to adjust p.

$$A = \frac{p}{k}$$

where A is the adjusted level of risk and k is the number of comparisons. When we set $p = 5\%$ and k is 28, A is 0.1786%. Then, by using this z statistics, at this adjusted level of risk, we test the null hypothesis that managers and workers are from populations with the same distribution.

Table 5 Categories.

Contents		# of managers	# of workers
Category 1	Listed company	89	793
Category 2	Unlisted company	411	707
Category 3	Degree of the public nature is not high	326	915
Category 4	Degree of the public nature is high	174	585
Category 5	# of employees is under 1,000	372	817
Category 6	# of employees is over 1,000	128	683

⋆1 Here, it is assumed that the sum of the ranks for data in X_1 is larger than the sum of the ranks for data in X_2. Note that the number of X is assigned smaller (larger) than the number of Y if $X > Y$ (resp. $Y > X$). That is, a rank is given in ascending order.

3. Results and Discussion

3.1 Results

Table 6 shows the results of the Mann-Whitney test with Bonferroni correction procedure ⋆2. This table includes the Mann-Whitney's U statistics, z-value and p-value.

Table 6 The effects of information security measures I.

	U	z	Prob $>\|z\|$	U	z	Prob $>\|z\|$
	Category 1			Category 2		
E1	33936.0	−0.683	0.4944	125066.0	−4.282	0.0000*
E2	33322.0	0.993	0.3207	130934.5	−3.053	0.0023
E3	34877.5	0.211	0.8332	133254.0	−2.642	0.0083
E4	34793.5	−0.256	0.7979	133276.0	−2.718	0.0066
E5	32389.5	1.462	0.1436	130330.0	−3.213	0.0013*
E6	35111.0	−0.088	0.9302	129226.5	−3.402	0.0007*
E7	33769.0	0.738	0.4605	117653.5	−5.761	0.0000*
E8	34907.0	−0.195	0.8452	133961.0	−2.443	0.0146*
E9	34593.0	0.339	0.7344	122096.5	−4.860	0.0000*
	Category 3			Category 4		
E1	125850.0	−4.656	0.0000*	42248.0	−3.886	0.0001*
E2	126441.5	−4.572	0.0000*	47857.5	−1.350	0.1770
E3	132197.0	−3.492	0.0005*	44643.0	−2.866	0.0042
E4	128594.5	−4.329	0.0000*	46538.0	−2.040	0.0413
E5	133326.0	−3.219	0.0013*	46078.5	−2.142	0.0322
E6	133677.5	−3.111	0.0019	42897.5	−3.470	0.0005*
E7	119361.0	−5.873	0.0000*	43958.5	−2.962	0.0031
E8	127727.0	−4.341	0.0000*	47614.5	−1.503	0.1328
E9	124366.0	−4.890	0.0000*	43639.0	−3.147	0.0017
	Category 5			Category 6		
E1	123975.0	−5.626	0.0000*	43531.5	0.086	0.9315
E2	127990.5	−4.857	0.0000*	40332.0	1.589	0.1119
E3	135237.0	−3.476	0.0005*	42929.0	−0.378	0.7053
E4	134246.5	−3.779	0.0002*	43418.5	−0.144	0.8857
E5	130682.5	−4.365	0.0000*	40988.0	1.274	0.2026
E6	128679.0	−4.684	0.0000*	41713.5	0.926	0.3542
E7	116023.0	−7.126	0.0000*	42031.0	0.761	0.4466
E8	131564.5	−4.195	0.0000*	40766.0	1.409	0.1589
E9	119437.5	−6.480	0.0000*	41567.0	0.976	0.3290

* indicates significance level

⋆2 We use Stata SE/11.1 as software for statistics and data analysis.

Table 7 Cronback's alpha.

	Sign	item-test correlation	item-rest correlation	average interitem covariance	α
E1	+	0.8234	0.7698	0.2993514	0.9248
E2	+	0.8403	0.7917	0.2979020	0.9234
E3	+	0.7825	0.7222	0.3080108	0.9276
E4	+	0.7988	0.7451	0.3086791	0.9264
E5	+	0.7784	0.7142	0.3059091	0.9281
E6	+	0.8085	0.7509	0.3011853	0.9259
E7	+	0.8084	0.7478	0.2982140	0.9262
E8	+	0.8124	0.7583	0.3033449	0.9255
E9	+	0.8229	0.7670	0.2970711	0.9250
Test scale				0.3021853	0.9336

Table 8 Descriptive statistics of the compound scale.

	Mean	Std. Dev.
Whole	25.483	5.120432
Manager survey	24.088	5.587369
Worker survey	25.948	4.868925

First of all, all results in Categories 1 and 6 indicate that the medians are not statistically different at 0.1786% significance level. These fail to reject the null hypothesis at (original) 5% significance level. Additionally, many results in Category 4 (p-value is more than 0.001786) fail to reject the null hypothesis. That is, these results show that there are not differences between information security managers and workers with regard to assessment of the organizational information security measures. On the other hand, all results in Category 5 and many results in Category 2 and 3 reject the null hypothesis at (original) 5% significance level. These results show that there are some differences between the managers and the workers with regard to the effectiveness of the measures. These results imply awareness gaps between them.

Next, we make a compound scale on the effects of the organizational information security measures by simple addition of each item in Table 4 and employ Mann-Whitney rank-sum test with Bonferroni correction for this data.

It is recommended to check Cronback's α which assesses the internal consistency (reliability) of items. **Table 7** shows the result. Because Cronback's α is 0.9336 and is enough high, we can make a compound scale. **Table 8** and **Fig. 2** show the descriptive statistics of the compound scale on the effects and distribution of the respondents' the compound scale.

Fig. 2 Distribution of the respondents' the compound scale on the effects.

Table 9 The effects of information security measures II.

	U	z	Prob $> \|z\|$
Category 1	34649.0	0.285	0.7754
Category 2	121064.5	−4.689	0.0000*
Category 3	119832.5	−5.331	0.0000*
Category 4	41759.5	−3.640	0.0003*
Category 5	116572.5	−6.506	0.0000*
Category 6	41337.0	0.990	0.3221

Table 8 shows that the effectiveness of the organizational measures that workers assess would be higher than one of the managers[⋆1]. We can interpret this result as meaning that that the workers tend to accept the effectiveness of the measures rather than managers because of staying job site or that the managers properly tend to assess the effectiveness of the measures because their expected effectiveness is not achieved.

Table 9 shows the results of the Mann-Whitney test. Results in Categories 1 and 6 indicate that the medians are not statistically different at 0.1786% signifi-

⋆1 Note that the standard deviation of the manager survey is larger than the worker survey.

cance level. These fail to reject the null hypothesis at 5% significance level. On the other hand, results in Category 2, 3, 4 and 5 reject the null hypothesis at 5% significance level. These results are consistent with results in Table 5.

3.2 Discussion

Some results of the Mann-Whitney test with Bonferroni correction reveal that with regard to the effectiveness of the organizational information security measures there are no awareness gaps between information security managers and workers, who belong to the listed company or the company with over 1,000 employees. About the organizations with high degree of public nature of business, results show that there are no awareness gaps between them.

From these findings, in large companies there are no awareness gaps between information security managers and workers with regard to the effectiveness of the organizational information security measures. On the contrary, other results show that there are awareness gaps between them with regard to the effectiveness of the measures, who belong to the company with low degree of public nature of business or under 1,000 employees. Thus, in this kind of the organization such as small or medium-sized companies, awareness gaps between information security managers and workers tend to exist [⋆1].

Here, we argue how to bridge the gaps. As mentioned in the previous studies, one-sided information security measure is not sustainable and makes gaps between the managers and the workers. If they bridge the gaps by installing many security technologies or implementing various management measures, the gaps might be enlarged adversely because some workers are unsatisfied with the organizational measures.

If organization is small or medium-sized, we propose that information security managers could implement the two-sided organizational measures by communicating with workers in their organizations. Then, the gaps between them may be bridged with relative ease.

⋆1 An anonymous referee pointed out the issue on the balance of the data when some categories in Table 5 are combined. However, in this paper, we do not have to consider this issue since we do not derive any conclusion from combining categories in Table 5. Of course, when we run a multiple comparison, we should be careful about the indication by the referee.

4. Concluding Remarks and Future Works

In this paper, we investigated awareness gaps between information security managers and workers with regard to the effectiveness of organizational information security measures in Japanese organizations by analyzing micro data from two Web-based surveys of information security managers and workers which we conducted. We adopted nine effects in the survey which a Japanese research company conducted (Table 3). We approached our hypothesis by employing the Mann-Whitney rank-sum test with Bonferroni correction procedure.

As a result, we found that there were no awareness gaps between information security managers and workers with regard to the effects of the organizational information security measures in large companies. Subsequently, we found that awareness gaps between them tended to exist in small or medium-sized companies. Next, we argued how to bridge the gaps. We proposed that information security managers could implement the two-sided organizational measures by communicating with workers in their organizations.

Finally, let us briefly explain future works. Through analysis and discussion, we came to know the necessity of analyzing the organizational information security measures from the perspectives of both workers' awareness and behaviors. Even if workers understand the importance of implementing the information security measures, some workers might not comply with the measures rightly in their day to day work. Thus, we will analyze relations between awareness and behavior in the near future. This analysis will be approached at the next level by employing the latest studies in social psychology and behavioral economics.

Acknowledgments This work was supported by research grant from the Murata Science Foundation, and subsidy from JSPS: Grant-in-Aid for Young Scientists (B) (22730241).

We are thankful to anonymous referees and some participants at IFIPTM 2010 for helpful comments.

References

1) Thomson, M.E. and Solms, R.: Information Security Awareness: Educating Your Users Effectively, *Information Management & Computer Security*, Vol.6, No.4,

pp.167–173 (1998).
2) Schultz, E.: The Human Factor in Security, *Computers & Security*, Vol.24, pp.425–426 (2005).
3) Anderson, R. and Moore, T.: Information Security: Where Computer Science, Economics and Psychology Meet, *Philosophical Transactions of the Royal Society A*, Vol.367, pp.2717–2727 (2009).
4) Camp, L.J.: The State of Economics of Information Security, *A Journal of Law & Policy in the Information Society*, Vol.2, No.2, pp.189–205 (2006).
5) Cavusoglu, H., Mishra, B. and Raghunathan, S.: The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce*, Vol.9, No.1, pp.69–104 (2004).
6) Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R.: *2005 CSI/FBI Computer Crime & Security Survey*, Computer Security Institute (2005).
7) Farahmand, F., Navathe, S.B., Sharp, G.P. and Enslow, P.H.: Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach (online), available from ⟨http://infosecon.net/workshop/pdf/39.pdf⟩ (accessed 2010-04-11).
8) Takemura, T. and Ebara, H.: Spam Mail Reduces Economic Effects, *Proc. 2nd Intl. Conf. of Digital Society*, pp.20–24 (2008).
9) Liu, W., Tanaka, H. and Matsuura, K.: Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, *IPSJ Journal*, Vol.48, No.9, pp.3204–3218 (2007).
10) Takemura, T. and Minetaki, K: An Empirical Analysis on Information Security Management and the Effects, *Journal of Economic Policy Studies*, Vol.7, No.2, pp.46–49 (2010).
11) Albrechtsen, E.: A Qualitative Study of Users' Views on Information Security, *Computer & Security*, Vol.26, pp.276–289 (2007).
12) Albrechtsen, E. and Hovden, J.: The Information Security Digital Divide between Information Security Managers and Users, *Computer & Security*, Vol.28, pp.476–490 (2009).
13) Hagen, J.M., Albrechtsen, E. and Hovden, J.: Implementation and Effectiveness of Organizational Information Security Measures, *Information Management & Computer Security*, Vol.16, No.4, pp.377–397 (2008).
14) Hamaya, T.: Information Security, Organizational Emotion and Enterprise 2.0, *FRI Research Report*, No.345 (2009).
15) Mcilwraith, A.: *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness*, Gower Pub Co. (2006).
16) Stantona, J.M., Stama, K.R., Mastrangelob, P. and Jolton, J.: Analysis of End User Security Behaviors, *Computers & Security*, Vol.24, pp.124–133 (2005).
17) Takemura, T.: A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey, *American Journal of Economics & Business Administration*, Vol.2, No.1, pp.20–26 (2010).
18) Takemura, T.: Statistical Analysis on Relations between Information Security Education and Behaviors Using Micro Data from Web-based Survey, *The Review of Information & Communication Policy*, Vol.1, No.3, pp.1–16 (2010).
19) Werlinger, R., Hawkey, K. and Beznosov, K.: An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management, *Information Management & Computer Security*, Vol.17, No.1, pp.4–19 (2009).
20) Kotulic, A.G. and Clark, J.G.: Why There Aren't More Information Security Research Studies, *Information & Management*, Vol.41, pp.597–607 (2004).
21) Couper, M.P.: Web Surveys: A Review of Issues and Approaches, *Piblic Opinion Quarterly*, No.64, pp.464–494 (2000).
22) Hoshino, T.: *Statistical Science of Observed Data in the Survey: Causal Inference, Selection Bias and Data Fusion*, Iwanami Shoten (2009).
23) NRI Secure technologies: Surveillance Report of Actual Conditions on Information Security in Companies: 2006, *Information Security Report*, Vol.2, No.2 (2006).
24) Tomioka, J.: Utilization of Subjective Data in Labour Economics, *The Japanese Journal of Labour Studies*, No.551, pp.17–31 (2006).
25) Corder, G.W. and Foreman, D.I.: *Nonparametric Statistics for Non-Statisticians: a Step-by-step Approach*, Wiley, Publishing, Inc. (2009).

(Received October 18, 2010)
(Accepted April 8, 2011)
(Original version of this article can be found in the Journal of Information Processing Vol.19, pp.253–262.)

Toshihiko Takemura was born in 1975. He received his Bachelor (in 1998) in informatics from Kansai University, his Master Degree (in 2002) in economics, and his Ph.D. (in 2006) in applied economics, from Osaka University. He is currently an Assistant Professor at the Research Institute for Socionetwork Strategies, Kansai University. His research interests include information and communication technology policy, economics of information security, medical safety culture, behavioral economics and game theory. He is a member of the JEA, JSPUE, JSMI, JEPA and JSHA.

Hideyuki Tanaka is a Professor of the Graduate School of Interdisciplinary Information Studies at the University of Tokyo. His reseaarch interests include information and communication technology policy, economics of information society and organizational changes in digital economies. He is a member of the board of directors of the Japan Association for Social and Economic Systems Studies and a member of the American Economic Association. He recieved his Bachelor Degree in Economics from the University of Tokyo and his Master Degree in international relations from the Fletcher School of Law and Diplomacy, Tufts University. He completed a 15-year career as an administrative officer in the Ministry of International Trade and Industry of the Japanese government.

Kanta Matsuura was born in Osaka, Japan, in 1969. He received his Bachelor of Engineering degree in electrical engineering from the University of Tokyo in 1992. He then received his Master of Engineering degree in electronics (in 1994) and his Ph.D. (in 1997) from the University of Tokyo. He is currently an Associate Professor at the Institute of Industrial Science, the University of Tokyo. His information-security laboratory studies information-security only, but almost everything in information security: cryptology, network security, computer security, and security management. He is a member of IPSJ and IACR. He is a senior member of IEEE, ACM, and IEICE. He is a member of the board-of-directors of JSSM (Japan Society of Security Management).