World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:3, No:12, 2009

A Quantitative Study on Japanese Internet Users' Awareness to Information Security: Necessity and Importance of Education and Policy

Toshihiko Takemura and Atsushi Umino

Abstract—In this paper, the authors examine whether or not there are differences of Japanese Internet users' awareness to information security based on individual attributes by using analysis of variance based on non-parametric method. As a result, generally speaking, it is found that Japanese Internet users' awareness to information security is different by individual attributes. Especially, the authors verify that the users who received the information security education would have rather higher recognition concerning countermeasures than other users including self-educated users. It is suggested that the information security education should be enhanced so that the users may appropriately take the information security countermeasures. In addition, the information security policy such as carrying out "e-net caravan" and "information security seminars" are effective in improving the users' awareness on the information security in Japan.

Keywords—Information security education, variance of analysis, Internet users, information security policy, Web-based survey.

I. Introduction

THE diffusion of the Internet drastically changes not only business style, but also individuals' life style. According to the communication use trend investigation in 2008 that the Ministry of Internal Affairs and Communications (MIC) in Japan conducted, the number of the Internet users in Japan is about 90.91 million people, and the rate of population diffusion achieved around 75.3%[1]. The individuals use the Internet to communicate with others for such purposes as receiving and sending email messages, viewing homepages, and participating in Social Network Services (SNSs). The authors can easily imagine that the Internet is one of the tools to improve the quality of the individuals' life. This is common to all over the world. In such situation, it seems that the Internet promises the brilliant future. Recently, however, it is difficult to mention that the imagination is correct. It is because in the background of the rapid spread of the Internet various serious problems on information security have occurred and the users' worry becomes remarkable. The investigation of MIC points out that the ratio of household that use the Internet with worry reaches about 47.5% in Japan. In addition, a research conducted by the Institute for Information and Communications Policy shows that many non-Internet users enumerate "worry to encounter the troubles" as a primary unused reason [1].

Furthermore, the users always face information security incidents such as malware and illegal access, and appropriate countermeasures are required to be taken against the skillful and complicated method of malfeasants. Concretely, according to the transition of the number of computer viruses submitted to the Information-technology Promotion Agency, Japan (IPA), it is found that it has a peak in 2005 and it is on the decrease after then (see Fig. 1)[2]. However, it is pointed out that the kind of the virus and the number of the users without noticing infection with virus tend to increase. The investigation on domestic bot infected users that Cyber Clean Center (CCC) conducted in June, 2008 reported that the rate of bot virus infection is about 1.0% (the number of broadband users is about 30 million people in Japan). These facts would imply that various security risks have become popular for the Internet users as a negative effect of ICT developments.

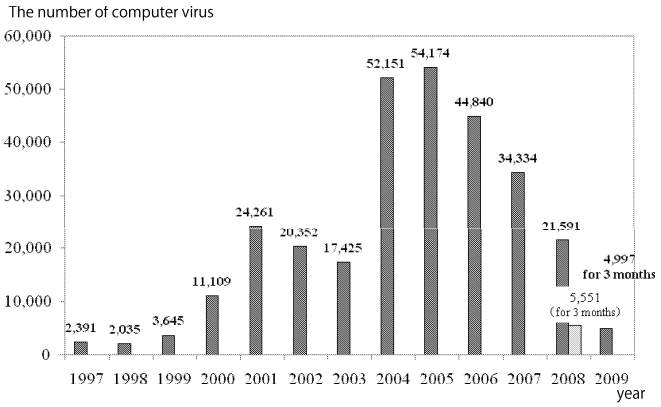

Fig. 1. The transition of the number of computer viruses submitted to IPA

Unless each user takes enough countermeasures to these Internet threats, he would have the possibility of becoming not only a victim but also an assailant oppositely without his intention or recognition. Nowadays, one of the factors to precipitate increases in the number of these possible damages would be the fact that the main purpose of cybercrimes, caused by human immaturity, is to gain money[2]. In the meantime,

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) and the Telecommunications Advancement Foundation in Japan.

Toshihiko Takemura is with the Research Institute for Socionetwork Strategies, Kansai University, 3-3-35, Yamate-cho, Suita, Osaka, Japan, 564-8680 (corresponding author to provide phone: +81-66368-1111 (ext.4533); fax: +81-66330-3304; e-mail: takemura@rcss.kansai-u.ac.jp).

A. Umino is with Faculty of Economics, Nagasaki University, 4-2-1, Katafuchi, Nagasaki, Japan, 850-8506 (e-mail: umino@nagasaki-u.ac.jp).

[1]URL: http://www.soumu.go.jp/main_content/000016027.pdf

[2]The number of computer virus is the one submitted to IPA. Insistently, this number is only in the tip of the iceberg.

the features of these possible damages tend to provoke other pieces of harm such as the second and the third-order damage.

In the field of natural science, a number of academic researches on information security technology such as cryptographic technology and secured networking are accumulated[3]. These accumulated researches achieve a constant result. On the other hand, research in the social sciences is a state of exploratory. Some qualitative researches such as constructing management systems are accumulated in recent years, but quantitative or empirical researches are still limited all over the world. One of the reasons is that many scholars were not interested in empirical research because of scant data on information security countermeasures and investment[4]. Furthermore, in a few empirical researches on the information security, the subjects of analysis are chiefly firms and the Internet users (individuals) are not directly targeted [5]-[11].

In this paper, the authors analyze the Japanese Internet users' awareness to information security based on individual attributes, followed by the discussion on effective countermeasures based on the results of the analysis. They use the data collected of Web-based (Internet) survey "investigation on the Internet use and the awareness of information security" that the Research Center of Socionetwork Strategies (RCSS), Kansai University, Japan conducted in March, 2009[5].

The paper consists of the following sections. Section II explains the summary of the Web-based survey. In section III, the authors show some hypotheses and the statistical methods. In addition, results of analysis are shown. Section IV discusses the role of Government and Internet Service Providers (ISPs) in Japan. Finally, concluding remarks and future works are suggested in section V.

II. Summary of Web-based survey on Internet Use and Awareness of Information Security

As the authors mentioned above, they analyze the difference of Japanese Internet users' awareness on information security by using the data collected by the Web-based survey "investigation on Internet use and the awareness of information security." Subjects of this survey are the Internet users in Japan, and do not include non-Internet users. Sample of this survey are arranged by three axes; age, habitation, and gender[6]. The sample size is 1483.

Table I shows elementary statistics on indices of the Internet users' awareness on information security. In this paper, the authors investigate the awareness to information security by dividing five kinds of indexes roughly; 1) recognition concerning individual information, 2) recognition concerning illegal copy, 3) recognition concerning countermeasures, 4) awareness to moral and 5) recognition concerning the Internet.Each index is the qualitative or ordinal scale data and the values are assigned between 1 and 5. The index assigns the small value if the recognition is poor. Inversely, the one assigns the large value if the recognition is rich. You can refer to [12] in details of data.

TABLE I
Elementary statistics on indexes of the Internet users' awareness to information security

	Variable	Content of questionnaire	Average	Standard deviation
1) recognition concerning individual information	X1	If you can freely see others' individual data such as address, name, age and e-mail address, do you think to see them?	3.68	0.960
2) recognition concerning illegal copy	X21	Do you want to use the copy of the software on the market that the friend made?	3.54	0.874
	X22	Do you think that there is a problem giving the illegal copy to your friends?	3.72	0.893
3) recognition concerning countermeasures	X31	Do you think that there is a problem using computer without anti-virus software?	4.00	0.905
	X32	When you receive the chain mail, do you think that there is a problem sending the mail to your friends and acquaintances?	4.15	0.894
	X33	If you execute information security countermeasure, does your sense of security rise?	2.57	0.754
	X34	Do you think that information security countermeasures are problems of ISPs and no matters that should be individually executed?	3.48	0.832
	X35	Compared with one year ago, have you improved your attitude to information security such as idea of information management?	3.51	0.648
	X36	Do you think that individual security countermeasures are necessary?	4.04	0.828
4) awareness to moral	X4	Do you think that you violate the rule if the problem does not happen?	3.88	1.007
5) recognition concerning the Internet	X51	Do you think that the Internet is safe?	2.32	0.853
	X52	Do not you think that you become an assailant on the Internet?	2.80	0.915
	X53	Do not you think that you become a victim on the internet?	3.44	0.803

Table II shows the information on individual attributes used as categories. The contents are gender, age, job, habitation, attitude toward risk, the Internet use term, the information security educating situation and encountering situation of information security incidents[7].

TABLE II
Elementary statistics on indexes of the Internet users' awareness to information security

Category	Explanation
Gender	1: male 2: female
Age	1: one' s twenties 2: one' s thirties 3: one' s forties 4: one' s fifties 5: one' s sixties 6: more than one' s seventies
Job	1: owner-operator 2: executive 3: family employed person 4: regular member 5: part-time job worker 6: contract worker, contract employee and business contract 7: leave-taking in action 8 neither job nor leave-taking in action 9: full-time housewife 10: student 11: the other
Habitation	1. Tokyo 2. Hokkaido and Tohoku area 3. Kanto area excluding Tokyo 4. Hokuriku and Koshinetsu area 5: Tokai area 6: Kinki area 7: Chugoku area 8: Shikoku area 9: Kyushu and Okinawa area
Attitude toward risk	lottery with the probability of 1/100 and the loss of 100000 yen 1: risk-loving 2: risk-neutral 3: risk-averse
The Internet use term	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
Information security educating situation	1: we were not educated 2: we were educated in some training and/or university
Encountering situation of information security incidents	1: we do not encounter the incidents 2: we have experience of encountering the incidents

[3]For example, you can refer to [3] in details of recent researches on cryptographic technology.

[4]As empirical researches on the information security countermeasures and investment in Japan, there are [4]-[9].

[5]URL: http://www.kansai-u.ac.jp/riss/en/shareduse/database.html

[6]For arranging three axes, we use the data on the number of population by age group and prefecture divisions in "the number of population and household movements based on basic resident register at 31st, March, 2008". URL: http://www.soumu.go.jp/menu_news/s-news/2008/ 080731_6.html.

[7]In this paper, the authors apply the index of absolute risk aversion that is used as attitude toward risk in [13]. They classify the attitude into three kinds; risk loving, risk neutral and risk averse. Note that the absolute risk aversion (RA) is calculated by the following equation:

$$RA = \frac{aZ - p}{1/2[aZ^2 - 2aZ + p^2]}$$

where Z, a and p represent reward of lottery, winning probability, and price of lottery, respectively. RA would be positive (negative) if you are risk aversion (loving), and RA would be zero if you are risk neutral.

III. Analysis

A. Hypotheses and Method of Analysis

Many surveys on awareness to the Internet use chiefly are investigated about the merits of the use and are analyzed still now. One the other hand, scholars discuss and research on whether or not awareness and moral of the Internet use and the awareness on information security follows to the rapid progress of the Internet and information and communication technologies (ICTs) in recent years. In this paper, we examine whether or not the awareness to information security are different by each individual attribute based on categories in Table II. The authors set up the following hypotheses:

1) There is no difference in awareness to the information security by the job.
2) There is no difference in awareness to the information security by the gender.
3) There is no difference in awareness to the information security by the attitude toward risk.
4) There is no difference in awareness to the information security by the age.
5) There is no difference in awareness to the information security by the Internet use term.
6) There is no difference in awareness to the information security by the habitation.
7) There is no difference in awareness to the information security by the information security educating situation.
8) There is no difference in awareness to the information security by the experience of encountering information security incidents.

From the feature of information security, even if many users with rich awareness to the information security exist, the level of information security in the society becomes low if a few users with poor awareness exist[8]. Therefore, it is important for all members in society to keep information security at high level. Then, at first, we examine whether or not they uniform the awareness to information security through the above hypotheses[9]. In order to verify the hypotheses, we run the analysis of variance (ANOVA).

B. Results of Analysis

Before running ANOVA, the authors need to check whether or not data follows to the normal distribution. There are various kinds of test of normality. Generally, it is said that Kolmogorov-Smirnov test and Shapiro-Wilk test are more reliable among them. In this test, null hypothesis is that data does not follow to the normal distribution. Therefore, if the significance probability is less than 5%, the null hypothesis cannot reject and we can conclude that data does not follow to the normal distribution. Oppositely, they judge that data follows to the normal distribution if we can reject the null hypothesis. Table III shows the result of Kolmogorov-Smirnov test and Spapiro-Wilk test.

TABLE III
Test of normality

	Kolmogorov-Smirnov test (Search)*		Shapiro-Wilk test	
	Statistics	Significance probability	Statistics Statistics	Significance probability
X1	0.260	0.000	0.877	0.000
X21	0.217	0.000	0.882	0.000
X22	0.268	0.000	0.867	0.000
X31	0.230	0.000	0.844	0.000
X32	0.244	0.000	0.803	0.000
X33	0.249	0.000	0.846	0.000
X34	0.228	0.000	0.866	0.000
X35	0.322	0.000	0.765	0.000
X36	0.289	0.000	0.809	0.000
X4	0.267	0.000	0.840	0.000
X51	0.230	0.000	0.871	0.000

*: Modified Lilliefors significance probability

From Table III, the authors can judge that data we use in this paper does not follow to the normal distribution because they cannot reject the null hypothesis. Unfortunately, they cannot run ANOVA by parametric method. Therefore, the authors should run ANOVA based on non-parametric method. Concretely, they examine whether or not we have difference of median, not average, in each category. As the feature of non-parametric method, data is assumed not to follow the normal distribution and they can use (questionnaire) data with ordinal scale. Hereafter, they run four kinds of test (ANOVA) according to the categories in Table II; Mann-Whitney test, Wilcoxon test, Kruskal-Wallis test and Jonckheere-Terpstra test. The authors simply explain the procedure of each test[10].

At first, Mann-Whitney test (Mann-Whiteney's U test) and Wilcoxon test are rank sum tests that examined the difference of the median between two groups. In these tests, the authors use the rank sum of data arranged in the ascending order, not the observed data. The test statistics are U and W statistics. Note that the authors calculate the statistics by using the average rank if there is the same order in data. From these statistics, they calculate 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, Kruskal-Wallis test and Jonckheere-Terpstra test are rank sum tests that examined the difference of the median between more than three groups. Test statistics in these tests are calculated by using data arranged in the ascending order as well as Wilcoxon test. In the former, the authors can calculate H statistics and then obtain the asymptotic significant probabilities because the distribution of H statistics approximately follows to the chi-square distribution of degree of freedom $(K-1)$. In the latter, we can calculate J-T statistics and standardized J-T statistics by using standard deviation and

[8] In [14], this situation is called the weakest link.

[9] It is pointed out possibility that information security is kept at low level even if the awareness to information security is uniformed. We can examine the level of information security in each group by using the average value and the median of the group. Actually, we see that the median of groups in almost indices of Table I are around three from results of analysis. Therefore, it is found that the level of information security is the medium degree.

[10] You can refer to [15] in details of ANOVA based on non-parametric method.

average value. Then, they can obtain the asymptotic significant probabilities from the standard normal distribution table because the distributions of these statistics approximately follow to 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). In addition, Jonckheere-Terpstra test has alternative hypothesis that the median of each group rises as the order of group goes up.

Tables IV-XI are results of analysis. Generally speaking, from many results of analysis, it is clear that the Internet users' awareness to information security is different by individual attributes. $a.s.p.$ in each tables represents the asymptotic significant probability.

It is found that there is difference in the many items by the age, the job, the Internet use term and the attitude toward risk (Tables V, VI, VIII and IX). On the other hand, it is found that there are few differences in awareness on the information security by the gender and the habitant (Tables IV and VII). In addition, from Table X, the authors find that by the information security educating situation, there is no difference in awareness to moral and recognition concerning the Internet, but that thre are the difference in a lot of other indexes. Furthermore, it is found that by the experience of encountering information security incidents there is no difference in awareness to moral but that there are the difference in the other items of Table XI.

Especially, from Tables X and XI of Mann-Whitney test and Wilcoxon test and statistics in each item, the authors can obtain the following suggestions. The Internet users (in Japan) who received the information security education would have rather higher recognition concerning countermeasures than the other users including self-educated users. Therefore, they claim that the information security education plays important role. On the other hand, compared with the situations of encountering the information security incidents, indiscriminately the author cannot declare which users' awareness to information security is higher. In addition, from Tables V and IX of Jonckheere-Terpstra test and statistics in each item, the author can claim that the awareness on the information security tends to be heightened as the age and the Internet use term go up.

TABLE IV
GENDER (MANN-WHITNEY TEST AND WILCOXON TEST)

	U statistics	W statistics	Z	$a.s.p.$
X1	237206.5	498209.5	-4.821	0.000^{***}
X21	262694.5	523697.5	-1.549	0.121
X22	252926.5	542867.5	-2.832	0.005^{***}
X31	269065.0	559006.0	-0.727	0.467
X32	271556.5	532559.5	-0.412	0.681
X33	259372.5	520375.5	-2.030	0.042^{**}
X34	257806.5	547747.5	-2.210	0.027^{**}
X35	252905.5	542846.5	-2.975	0.003^{***}
X36	269633.5	559574.5	-0.677	0.499
X4	255092.0	516095.0	-2.527	0.011^{***}
X51	273127.0	563068.0	-0.206	0.837
X52	267199.0	528202.0	-0.975	0.330
X53	266439.5	527442.5	-1.091	0.275

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE V
AGE (JONCKHEERE-TERPSTRA TEST)

	Observed J-T statistics	S.D. of J-T statistics	Standardized J-T statistics	$a.s.p.$
X1	491056.0	8860.636	3.790	0.000^{***}
X21	516096.5	8842.223	6.630	0.000^{***}
X22	473924.5	8763.397	1.877	0.060^{*}
X31	452564.5	8854.507	-0.554	0.579
X32	424521.0	8751.454	-3.765	0.000^{***}
X33	453068.0	8607.355	-0.512	0.609
X34	426447.0	8714.653	-3.560	0.000^{***}
X35	462095.5	8348.201	0.554	0.580
X36	441682.0	8562.301	-1.844	0.065^{*}
X4	490004.5	8843.566	3.679	0.000^{***}
X51	455663.0	8806.574	-0.206	0.837
X52	430782.0	8785.432	-3.038	0.002^{***}
X53	434558.0	8639.966	-2.652	0.008^{***}
The number of level: 6 The average J-T statistics: 457473.0				

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE VI
JOB (KRUSKAL WALLIS TEST)

	H statistics	Degree of freedom	$a.s.p.$
X1	47.156	10	0.000^{***}
X21	38.569	10	0.000^{***}
X22	25.036	10	0.005^{***}
X31	17.175	10	0.071^{*}
X32	11.427	10	0.325
X33	10.081	10	0.433
X34	16.636	10	0.083^{*}
X35	19.159	10	0.038^{**}
X36	16.989	10	0.075^{*}
X4	25.840	10	0.004^{***}
X51	8.107	10	0.618
X52	12.986	10	0.224
X53	12.141	10	0.276

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE VII
HABITATION (KRUSKAL WALLIS TEST)

	H statistics	Degree of freedom	$a.s.p.$
X1	10.901	8	0.207
X21	15.032	8	0.059^{*}
X22	18.081	8	0.021^{**}
X31	15.353	8	0.053^{**}
X32	19.403	8	0.013^{*}
X33	10.280	8	0.246
X34	11.427	8	0.179
X35	6.916	8	0.546
X36	20.224	8	0.010^{***}
X4	12.584	8	0.127
X51	11.609	8	0.170
X52	5.431	8	0.711
X53	2.905	8	0.940

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE VIII
ATTITUDE TOWARD RISK (KRUSKAL WALLIS TEST)

	H statistics	Degree of freedom	$a.s.p.$
X1	6.081	2	0.048**
X21	1.191	2	0.551
X22	10.736	2	0.005***
X31	23.081	2	0.000***
X32	16.829	2	0.000***
X33	15.315	2	0.000***
X34	14.005	2	0.001***
X35	21.705	2	0.000***
X36	26.892	2	0.000***
X4	3.767	2	0.152
X51	2.715	2	0.257
X52	11.413	2	0.003***
X53	4.644	2	0.098*

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE IX
INTERNET USE TERM (JONCKHEERE-TERPSTRA TEST)

	Observed J-T statistics	S.D. of J-T statistics	Standardized J-T statistics	$a.s.p.$
X1	399541.5	8519.404	0.691	0.490
X21	403377.0	8501.709	1.143	0.253
X22	435735.0	8425.919	4.994	0.000***
X31	435992.5	8513.524	4.973	0.000***
X32	455819.0	8414.449	7.388	0.000***
X33	382560.0	8275.909	−1.341	0.180
X34	444931.0	8379.063	6.119	0.000***
X35	419198.5	8026.757	3.182	0.001***
X36	442415.0	8232.584	5.923	0.000***
X4	415322.5	8502.996	2.548	0.011***
X51	417515.5	8467.438	2.818	0.005***
X52	402334.0	8447.100	1.027	0.304
X53	420501.5	8307.257	3.232	0.001***
The number of level: 6 The average J-T statistics: 393656.5				

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE X
THE INFORMATION SECURITY EDUCATING SITUATION (MANN-WHITNEY TEST AND WILCOXON TEST)

	U statistics	W statistics	Z	$a.s.p.$
X1	137942.5	166383.5	−1.787	0.074*
X21	145815.0	174256.0	−0.410	0.682
X22	138257.5	913892.5	−1.751	0.080*
X31	136712.5	912347.5	−2.004	0.045**
X32	135339.0	910974.0	−2.271	0.023**
X33	140069.0	168510.0	−1.457	0.145
X34	127571.0	903206.0	−3.662	0.000***
X35	114585.0	890220.0	−6.235	0.000***
X36	133736.0	909371.0	−2.611	0.009***
X4	146888.0	922523.0	−0.222	0.824
X51	144900.5	920535.5	−0.573	0.567
X52	142642.0	918277.0	−0.973	0.331
X53	140968.0	916603.0	−1.290	0.197

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

TABLE XI
ENCOUNTERING SITUATION OF INFORMATION SECURITY INCIDENTS (MANN-WHITNEY TEST AND WILCOXON TEST)

	U statistics	W statistics	Z	$a.s.p.$
X1	232385.0	363713.0	−2.187	0.029**
X21	229628.5	360956.5	−2.565	0.010***
X22	230998.5	702904.5	−2.401	0.016**
X31	210571.0	682477.0	−5.138	0.000***
X32	231006.5	702912.5	−2.403	0.016**
X33	231829.0	363157.0	−2.329	0.020**
X34	223322.0	695228.0	−3.469	0.001***
X35	219390.0	691296.0	−4.185	0.000***
X36	212685.0	684591.0	−5.017	0.000***
X4	245336.5	376664.5	−0.438	0.661
X51	226512.0	698418.0	−2.999	0.003***
X52	231929.5	703835.5	−2.268	0.023**
X53	215024.5	686930.5	−4.648	0.000***

*: $p < 10\%$ **: $p < 5\%$ ***: $p < 1\%$

IV. ROLE OF GOVERNMENT AND ISPS

This section considers the role of the government and ISPs to enhance the awareness to information security on the basis of the analysis result on the difference of the awareness according to individual attributes described in the previous section. Information security policy in Japan has been intensified in recent years since the establishment of the National Information Security Center in April 2005 and the IT Strategic Headquarters in May 2005 to provide a fundamental and coordinating role. Specifically, Japanese government has drawn up the First National Strategy on Information Security as a middle-term plan between 2006 and 2008 and the Second National Strategy on Information Security as a plan between 2009 and 2011 as well as annual programs to implement these strategies called "Secure Japan". These strategies and programs show the grand design of the security policy to ensure that both public and private sectors will work together to promote required countermeasures.

The Second National Strategy on Information Security has identified four priority areas (governmental organizations and local municipalities, critical infrastructure, enterprises, individuals) to implement information security countermeasures. It also addresses cross-cutting priority policies; promotion of information security technology strategies, promotion of internatiobeen establishednal partnership/cooperation, nurturing and ensuring information security human resources, and crackdown on criminals and protection/redemption of rights/benefits. Among these policies, the most remarkable one from the previous analysis would be the perspective of human resources. Therefore, this section attempts to obtain an overview of some major actions that the Japanese government and many ISPs have taken in recent years from this perspective.

The necessity and importance of education is often pointed out not only in information security policy but also arguments on ICT in general. For example, in Japan "New IT Reform Strategy", established in January 2006 as a general national strategy in the field of ICT, refers to the necessity of revision of information education. In the information security arena, the government is indeed bolstering the security education

to individuals. For instance, the First National Strategy on Information Security set a goal to eliminate individuals feeling anxiety toward ICT utilization, which put emphasis on the action on those who manage information. However, the Second National Strategy on Information Security added referring to the importance of enlightening awareness and actions of those who send information, which promotes information security education (such as information morals) in schools or in regions as well as countermeasures to effectively enhance security levels of general users.

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 corporation. This is an attempt to carry out lectures for safe and secure Internet use to parents and teachers. Moreover, MIC's website called "Information Security Site for Japanese" has been established since March 2003[11]. This website aims at educating Japanese people about knowledge on information security and providing basic information on information security countermeasures in accordance with usage methods. Furthermore, aforementioned CCC has been established since December 2006 as a counter-bot project through collaboration between the MIC and the Ministry of Economy, Trade and Industry (METI). CCC provides information to fight against bot, which aims at decreasing and eliminating the bot-infected computers. It is expected that accumulation of these activities will lead to the improvement of awareness to general public on information security and realize a "developed country with matured information security" that the Second National Strategy on Information Security puts up as a fundamental principles. In addition, "information security seminars" that the IPA carries out periodically throughout Japan and other relevant training programs can be a locomotive to enhance information security awareness of Internet users. These countermeasures are meaningful and desirable from the perspective of the analysis result of this paper (i.e., those Internet users who have trainings on information security tend to possess higher awareness on information security than those who do not have), and thus further replenishment is expected.

Japanese ISPs also implement various countermeasures on information security education. For example, there are more than 70 ISPs that participate in the operation on CCC to provide counter-bot information. ISPs also engage in enlightenment activities to enhance information security awareness of Internet users. According to [16], many ISPs provide information on information security such as viruses and vulnerabilities through their own websites and weblogs mainly in order to seek attention to their own 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 the Internet users' awareness to information security. Table XII shows main actors (organizations) that deal with information security policy and countermeasures in Japan.

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

TABLE XII
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 measures
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

V. Concluding Remarks and Future Works

In this paper, the atuhors have examined whether or not there are differences of Japanese Internet users' awareness to information security based on individual attributes by using ANOVA based on non-parametric method. As a result, generally speaking, it is found that the Internet users' awareness to information security is different by individual attributes. Especially, the atuhors have verified that the Internet users who received the information security education would have rather higher recognition concerning countermeasures than other users including self-educated users. From these findings, it is clear that the information security education is very important and effective. The authors suggest that the information security education be enhanced so that the Internet users may appropriately take the information security countermeasures. Therefore, such policies as the above-mentioned "e-net caravan" and "information security seminars" are effective in improving the Internet users' awareness to the information security. It is expected that these polices will be enhanced in the future.

In this paper, the authors have run ANOVA based on non-parametric method, but the information obtained from the results is still not enough as materials for countermeasure examination. In the near future, we will refine and verify the analyses of this paper by using multiple comparison analysis and/or covariance structure analysis in order to obtain more appropriate information.

Finally, the authors hope that this paper will become an academic contribution to economics and policy science, and will help to give the incentive for individuals to take information security countermeasures.

Acknowledgment

The authors are grateful to Makoto Osajima (Associate Professor, Waseda University, Japan) and Kazunori Minetaki (Senior Researcher for Statistical Analysis, Kansai University, Japan). The possible remaining errors.

REFERENCES

[1] Institute for Information and Communications Policy (2009, March). The investigation on the deciding factors and the current situation of the Internet use. [Online] Available: http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2009/2009-01.pdf (in Japanese)
[2] T. Takemura and M. Osajima, "About some topics on countermeasures and policies for information security incidents in Japan," *GITI Research Bulletin 2007-2008*, pp.163-168, 2008 (in Japanese)
[3] D. Cook, and A. Keromytis. *Cryptographics: exploiting graphics cards for security*. New York: Springer, 2006
[4] H. Tanaka, K. Matsuura and O. Sudoh, "Vulnerability and information security investment: an empirical analysis of e-local government in Japan," *Journal of Accounting and Public Policy*, vol.24 (1), pp.37-59, 2005.
[5] W. Liu, H. Tanaka and K. Matsuura, Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms, *Information Processing Society of Japan Digital Courier*, vol.3, pp.585-599, 2007 (in Japanese)
[6] T. Takemura and A. Umino. "A research on the Internet users' awareness to the information security." *Telecom Journal*, August 2009, pp.13-21, 2009 (in Japanese)
[7] T. Takemura and K. Minetaki. "An empirical analysis on information security countermeasures. *The Selected Proceeding of 2nd International Conference on Social Sciences (Social Sciences Research Society)*, forthcoming (2009)
[8] T. Takemura. "A quantitative study on workers' awareness to information security using the data collected by Web-based survey." *The Proceeding of 2009 Annual Conference of the Applied Business and Entrepreneurship Association International*, forthcoming (2009)
[9] T. Takemura, M. Osajima and M. Kawano. Economic analysis on information security countermeasures: the case of Japanese Internet Service Providers. In *Advanced Technologies* (A. Lazinica Ed.), intechweb.org, forthcoming (2009)
[10] E. Albrechtsen."A qualitative study of users' view on information security." *Computer and Security*, Vol.26, pp.276-289, 2007
[11] E. Albrechtsen and J. Hovden."The information security digital divide between information security managers and users. *Computer and Security*, Vol.28, pp.476-490, 2009
[12] T. Takemura, A. Umino and M. Osajima. "Analysis of variance on the Internet users' awareness to the information security." *GITI Research Bulletin 2008-2009*, pp.193-201, 2009 (in Japanese)
[13] J. S. Cramer,J. Hatog, N. Jonker, and C. M. Van Praag. " Low risk aversion encourages the choice for entrepreneurship: an empirical test of a truism." *Journal of Economic Behavior & Organization*, Vol.48, pp.29-36, 2002
[14] H. R. Varian, "System Reliability and Free Riding," in *ACM Transactions on Information and System Security*, vol.5, pp.355-366, 2002
[15] L. Wasserman. *All of Nonparametric Statistics*. New York: Springer, 2007
[16] T. Takemura. The 3rd investigation of actual conditions report on information security countermeasures for Internet Service Providers. Kansai University, 2009 (in Japanese)

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

Atsushi Umino Atsushi Umino was born in Tokyo, Japan. He received his Bachelor Degree (1994) in Arts and Sciences from University of Tokyo, and his Master Degree (2000) in International Relations from University of Cambridge. He is an associate professor of Faculty of Economics, Nagasaki University. His research interests include ICT policy and law.