Who Sometimes Violates the Rule of the Organizations?: Empirical Study on Information Security Behaviors and Awareness

Toshihiko Takemura
The Research Institute for Socionetwork Strategies, Kansai University
3-3-35, Yamate-cho, Suita, Osaka, Japan
Security Economics laboratory, IT Security Center
Information-Technology Promotion Agency
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan
Email: a084034@kansai-u.ac.jp

Ayako Komatsu
Security Economics laboratory, IT Security Center
Information-Technology Promotion Agency
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan
Email: a-koma@ipa.go.jp

June 1, 2012

Abstract

In this article, we investigate to determine some key factors which have effects on employees' behaviors of violating the rule which is related to the information leak given a condition that the behaviors are prohibited totally by the organizational measures. By using the collected data from a survey that we conducted in March 2011 and employing a stepwise logit model as a statistical tool, we analyze the relationships above. As a result, we found out the some features on the respondent's behavior of violating the organizational rule. The primary results are followings. First of all, myopic cognition and hypermetro cognition measured by CFC scale have effects on the behaviors of violating the organizational rules in almost cases. Next, in many cases individual whose information security awareness is higher tends not to violate the rule. Third, the behavior of violating the rule is independent of the degree of the measure satisfaction and the scale of the organization, but is not related to the degree of the workplace satisfaction and the evaluation toward the managers in some cases. Fourth, in the organization which the permanent employment is introduced, the individual tends to violate the rule. It is not easy to control psychological factors such as the individual's attitude toward risk. Conversely, the factors regard to the organizational attributes such as the degree of

workplace satisfaction or the employment system may be controlled by designing the appropriate organizational environment. Consequently, we consider that it may be effective to improve the information security awareness by information security education and training.

keywords: information security behavior; information security awareness; risk attitude; violation of organizational rule

1 Introduction

Primary interests of empirical studies on information security are clarifying appropriate level of information security investment, effective technical and management measures. These accumulations of studies are useful for the manager who introduce and implement the information security measures as the organization. So, the targets in these researches are organizations in which the managers introduce and implement the measures. However, many of these ones had missed the important point. They discussed and analyzed only one-side measures of managers' standpoints excluding consideration of the employees (users) who confirm to the measures. This one-side measure may not sometimes work well unless the users understand meaning of the measures. The reason is that the some users have grievance against the managers and the measures. For instance, as mentioned in the previous literatures [1], [2], [3], the users might not sometimes comply with the measures or may tend to put dairy-task ahead the measures even if the policy is established in the organization.

In response to the issues, in late years, some empirical studies on information security approaching from the users' standpoints appear. In this kind of researches, one discusses the ability that managers in the organization implement more effective measures by analyzing the users' information security awareness, the other discusses the measure to prevent the undesirable behaviors by analyzing computer abuse problem and insider security contravention. This article belongs to the latter researches. Therefore, here we briefly introduce some related literatures and then show the signification of this article. Many of these literatures are approached from the behavioral science. For example, there are theory of planned behavior (TPB) and general deterrence theory (GDT)[1]. TBP is one of the most widely successful and applied frameworks to explain human behavior and was suggested by Ajzen [6]. TPB shows that the best way to predict an individual's behavior is by examining how that individual intentions to behave. In TPB, behavioral intentions influence a certain actual behavior, and the behavioral intentions (how much effort one is willing to exert to perform a given action) are formed from three determinants, attitude toward the behavior, subjective

[1]These studies provide good reviews about these theories regarding with the information security [4], [5].

norms and perceived behavioral control. The attitude toward the behavior is the degree to which the person has a favorable or unfavorable evaluation of the behavior in question, subjective norm is the influence of social pressure that is perceived by the individual to perform or not perform a certain behavior, and perceived behavioral control is the perceived ease or difficulty of performing the behavior, respectively. TPB has been explicitly applied to software piracy problem [7], [8], non-work-related computing [9], the Internet abuse [10], [11], security policy compliance [12], [13], [14] and insider security contravention [15]. On the other hand, GDT has been widely used in the study of criminal and antisocial behavior and is a well-established theory within the criminology field. GDT explains how security measures implemented by organizations rely primarily on technology without considering other factors, such as people and processes. Previous computer abuse studies or misuse problems have been mainly based on GDT [16], [17], [18]. In addition, TBP and GDT generally employ structural equation modeling (SEM) or partial least square (PLS) method. On the other hand, we need to note that in the studies based on TPB or GDT, a few researchers only clarify relation between behavioral intentions and actual behaviors. Based on original TPB or GDT, researchers implicitly discuss under assumption that individual exactly behaves if he intends to behave. However, Komatsu et al point out that the behavioral intention does not necessarily lead to the actual behavior from analysis of behavior regarding with bot measures [19].

Besides, a few studies are approached from behavioral economics. In approaches from TPB and GDT human behavior is assumed to be rational, but is not rational necessary in behavioral economics. We will discuss whether or not the human behavior, a certain kind of fraud, is rational or irrational in the following section. Takemura models employees' problematic behaviors (violation of the organizational rule) relating the information leak in the organization employing logit regression equation [3]. This model provides straightforward results and possesses strong power to predict.

It is needless to say that in many cases users' behaviors mentioned above are inconsistent with the decision of their organizations. If an individual commits a fraud, he might achieve some sort of his purpose, but his behavior would be disadvantageous for his organization. Therefore, managers in the organization must pay attention to such individuals. In each study, it is found that the psychological factors such as attitude toward the risk and the working environment influence their intention and/or behaviors directly or indirectly. The organization would admit of changing the working environment, but would have an issue that it is difficult to control the individual's psychological factors.

This article includes new breed of behavioral modeling based on Takemura's model [3] incorporating into some factors in TPB and the other new factors. The purpose of this article is to determine key factors which have effects on employees' behaviors (rule violation) relating the information leak

given a condition that the behaviors are prohibited totally by the organizational measures. This condition enables to discuss the effectiveness of organizational measures.

This article consists of the following sections. In the next section, we explain our behavioral modeling and the survey data. Section 3 shows the results of analysis and the implications. Finally, in section 4 we summarize our analysis and show the future work.

2 Framework

2.1 Behavioral modeling

Even if the information security policy and organizational rule is established, almost all employees would comply with the rule, but some employees would violate the rule unfortunately. In addition, it is pointed out that even if the rules have compelling force, an individual might not occasionally regard violation of the rule as serious problems to complete dairy-tasks [3]. This misjudgment becomes sometimes a trigger of a major information security accident such as information leak. Of course, to some degree, we can prevent to encounter the information security accidents by establishing the policy and the information security education/training [20]. For exerting the effects of them more, we grasp the factors effecting violation of the rule by the employees including managers and need to implement the measure to reduce violation of the rule. Therefore, this article focuses on the employee's behavior of violating the organizational rules or not.

The primary research question of this article is what determinants of employee's violating the organizational rules are. As mentioned in Section 1, TPB suggests that the behavioral intentions, which influence a certain actual behavior, are formed from three factors, labeled attitude toward the behavior, subjective norms and perceived behavioral control. In addition to TPB, there is theory of fraud triangle suggested by Cressey [21] as one famous theory relating to such violation of the rules or fraud in the criminal psychology [22]. The fraud of triangle consists of three conditions generally present when fraud occurs: incentive/pressure, (perceived) opportunity, and attitude/rationalizations. This implies that anyone may commit a fraud if the three conditions are satisfied at the same time. Each theory has something in common such as attitude toward the behavior, assessment from persons involved, and individual circumambient environment. Furthermore, human behavior is assumed to be rational in both theories.

We support effect of almost psychological factors above, but query an assumption that the human behavior of violating the organizational rule is rational. For example, suppose that employee would be fired if he violates the organizational rule. Then, would he violate the rule for the purpose of completing his dairy-task? If he is rational, he would not violate the rule

because he hates to be fired. In this case, his behavior may be rational in the short term but not in the long term. That is, it seems that the behavior of violating the organizational rule is rational in the short term but not in the long term. From the viewpoint of implementing the information security measures, it seems to be important to make assumption that human behavior is rational or not. So, we check whether or not the behavior results from myopic and hypermetropic cognition in this article.

Based on the factors used in these theories, we incorporate key factors (attitude, motivation toward the behavior and workplace environment) in our behavioral model.

Attitude Attitude represents the degree to which the individual has a favorable or unfavorable evaluation of the behavior, e.g., risk attitudes [23], [24], or consideration of future consequences (CFC) [25].

Motivation toward the behavior Motivation toward the behavior is the driving force by which individual achieves his/her goal. As general motivational strategies or specific motivational appeals, there are five factors; monetary rewards, assessment from peers, self-realization, morality, and pleasantness [26].

Information security awareness Information security awareness represents the degree to measure individual's evaluation and/or knowledge of the information security. The concept of awareness is one important of factors and enables to be exogenously controlled by educating or training members in the organization effectively [27], [28].

Workplace environment Workplace environment consists of two elements in the organization to which the individual belongs. One is subjective element, e.g., the degree of workplace satisfaction, or the degree to which the individual has evaluations of the information security manager and the organizational measures. On the other hand, the other is objective element, e.g., working pattern, the scale of organization, or incentive system for members' working which is introduced in the organization.

To answer this research question, we employ the following logit regression equation[2].

$$\ln \frac{p_j}{1-p_j} = a + X_b b + X_c c + X_d d + X_e e \tag{1}$$

where p_j represents the probability that individual violates the rule j. In addition, X_b, X_c, X_d, and X_e, , and X_f represent vectors of attitude, mo-

[2]Generally, behavioral model using a logit regression equation is devoted to explaining and predicting human behavior and has been used in the various fields for a long time.

tivation toward the behavior, awareness, workplace environment, and the other individual attributes, respectively.

The log of the odds ratio in equation (1) is simply equal to the coefficient of X and this is a measure of the effect of X.

Here, we briefly explain the process to estimate the coefficients in equation (1) [29]. We employ a stepwise procedure for deletion of variables from the model (backward selection procedure). This procedure is based on a statistical algorithm that checks for the importance of the variables and excludes them on the basis of a fixed decision rule. In other words, employing this stepwise selection procedure can provide a fast and effective means to screen a large number of variables and to fit a number of logit regression equations simultaneously. This selection to fit the full model on all explanatory variables at first step and remove the least-significant term and re-estimate while it is insignificant. In other words, the variables deleted in the selection process are not significant and not affecting factors to the explained variable.

2.2 Methodology

To test the relationships implied by the model in equation (1) and the research question, we conducted a Web-based survey for data collection. This survey method inescapably contains certain weakness of the data collection. A Web-based survey is well-used in the field of marketing, but has the Internet bias. In other words, the data may not guarantee representativeness of intended population because the survey is not necessarily based on a random sampling. Unfortunately, this problem has not been solved yet [30]. Wherein, we interpret and analyze data from population of Japanese registered with the Internet survey company. In addition, we presume that these collected data are useful for reasonable analysis[3].

We conducted Web-based survey entitled "Survey on Japanese workers' awareness and behavior to information security measures" in March 2011. This survey aims at exploring workers' awareness and behaviors to information security measures.

Subjects of this survey are Japanese people who have been working for more than two years in the same companies. The number of survey items is more than 60 including individual attributions such as gender and annual income. For instance, the items contain questions on whether or not the organizational measures are implemented, and questions regarding their information security awareness and behavior. This survey includes 1,800 respondents.

[3]Of course, we do not intend to ignore this statistical problem. We expect the future studies on representativeness of data from the Web-based survey are promoted.

2.2.1 The behavior of violating the organizational rules

We have various organizational measures to prevent information leak. We pick up a part of the measures (1: Prohibition against bringing out the secret customer data by using portable devices, 2: Prohibition against attaching the secret customer data to e-mail, 3: Prohibition against accessing the non-work related website such as 2 Channel at the office, 4: Prohibition against forwarding the office's e-mail address to the private address, 5: prohibition against installing the software used at home on office's computer, and 6: prohibition against bring out the company's note PC to the outside of company) [3], [31]. According to information security white paper in Japan [32], many of companies answer that the route of virus infection is portable devices such as USB memory. Additionally, installing the software used at home on office's computer is relevant to software piracy [7], [8]. Wrong sending e-mail or accessing the non-work-related Website is also a trigger of information security accident [9], [10], [11], [33]. Because these measures enable to prevent encountering the information security accidents such as information leaks, many of Japanese companies recently establish and implement some the measures above. It is thought that the information security or system managers can forcibly have control over employees by implementing these measures. Really, would the employees comply with the measures?

Table 1 shows cross tabulation between implementation status and individual experiences[4]. If the behavior is totally prohibited within the organization by Measure, the implementation status is "Totally prohibited." If there are no rule in the organization, the status is "Unprohibited." Besides, individual experience is whether or not to experience the behavior shown in Measures. If the measures are implemented, the option "I have experience (resp. I have no experience)" means "I have experience to violate the rule (resp. I comply with the rule always)."

Irrespective of implementing the organizational measures, more than half of respondents have no experience or they comply with the rule always except forwarding the office's e-mail address to the private address within the organization which implementation status is unprohibited. On the other hand, about 6-13% of respondents had experience to violate the rule even if the behaviors are prohibited totally by the organizational measures.

In this article, especially we focus on their behaviors given a condition that the behaviors are prohibited totally by the organizational measures. Thus, descriptive statistics is calculated by the subsample of the survey (the sample size is 1,564), not full sample.

[4]Because some respondents select "I do not know whether or not the measures are prohibited within the organization" or "the measures are prohibited with some conditions within the organization" in the survey, these respondents are excluded.

Table 1: Cross tabulation between implementation status and individual experiences

Measures	Status	Individual experiences	
		I have experience (I have experience to violate the rule)	I have no experience (I comply with the rule always)
Measure 1	Totally prohibited	102	685
	Unprohibited	103	160
Measure 2	Totally prohibited	55	662
	Unprohibited	93	202
Measure 3	Totally prohibited	56	918
	Unprohibited	165	181
Measure 4	Totally prohibited	80	578
	Unprohibited	278	237
Measure 5	Totally prohibited	54	854
	Unprohibited	120	180
Measure 6	Totally prohibited	38	501
	Unprohibited	126	162

2.2.2 Attitude

Attitude relates mainly to the degree to which the individual has a favorable or unfavorable evaluation of the behavior. A positive attitude toward the behavior of violating the rule increases to perform those behaviors. Among various concepts of attitudes, the concept of risk has been successfully used in theories of decision making in economics, financial engineering, and the other sciences. So, we introduce the degree of risk aversion and risk tolerance as risk attitude.

The survey has some questions asking amount of certainty equivalent that brings in uncertain profit such as pricing lotteries and/or desired insurances for the damages from the robbery. From the amount of the certainty equivalent that respondents reveal, we can calculate their degree of risk aversion (on lottery and insurance) based on BMD method. In this article, we assume situations that there is a lottery with a 1% chance of winning 100 thousand JY and a 99% chance of winning nothing, and that there is a 1% chance of being robbed of 100 thousand JY. Figure 1 shows the distribution for the degree of risk aversion.

The distributions of Figure 1 show that many of the respondents are risk-averse on the lottery because the degree of risk aversion is positive and that they are adversely risk-loving on the insurance. This implies that their attitudes toward the risk vary by conditions such as the probability and the situation. In some ways, this result is consistent with the asserting of Prospect Theory suggested by Kahneman and Tversky [34].

In addition, the survey has one question asking the degree of risk tolerance. The risk tolerance shows the level of risk that individual can perceive, or the degree of loss that they can receive. Concretely, we ask the following hypothetical question: Now let's assume that your computer at home would be at high risk of becoming infected with computer virus unless you

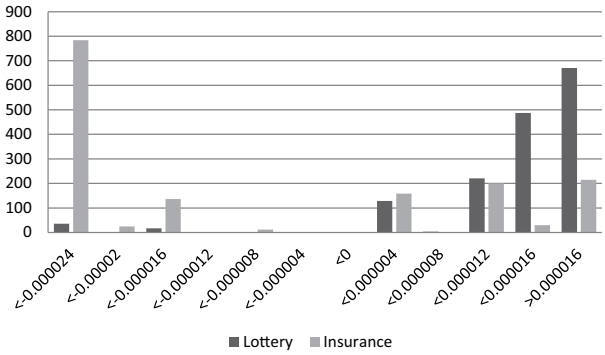

Figure 1: The degree of risk aversion

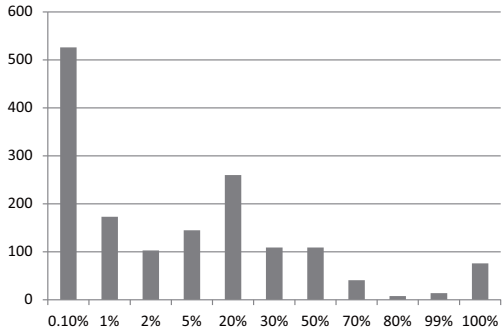

Figure 2: The degree of risk tolerance

install the latest anti-virus software on the computer. You have the option to purchase and install the latest anti-virus software on your computer or do nothing. Compare the timing (probability of virus infection) in option "A" (implementing the measure) with option "B" (do nothing) and indicate which timing you would prefer to implement the measure for all 10 choices (0.1%, 1%, 2%, 5%, 20%, 30%, 50%, 70%, 80% and 99%)[5]. Figure 2 shows the distribution for the degree of risk tolerance.

If the probability of infecting virus is lower than 1%, about 44.7% of respondents answer to implement the measure. On the contrary, about 4.86% of respondents answer to not implement the measure even if the probability is 99%. Figure 2 shows that most respondents cannot tolerate the risk of virus infection.

As the other concept of attitude, we introduce the CFC scale used in the field of psychology. The CFC scale is scored so that higher score indicates a greater consideration of future consequences. To create the CFC scale,

[5]If the respondent selects option "B" when the probability is 99%, we assume that he tolerate the all risks.

Table 2: The descriptive statistics of two factors of CFC scale

	Average	Median	Min	Max
Myopic cognition	4.476 E-09	-0.169	-3.890	3.736
Hypermetropic cognition	1.471 E-09	0.147	-3.579	4.846

we set 12 statements (for example, "I consider how things might be in the future, and try to influence those things with my day to day behavior") based on the previous study [25], which are measured on a five-point Likert scale, in the survey. Then, by using factor analysis with promax rotation to the questions, two factors are assumed; myopic and hypermetropic cognition[6]. Table 2 shows descriptive statistics of these factors.

2.2.3 Motivation toward the behavior

It is generally agreed that individual performance depends on motivation in addition to ability and working conditions. In order to measure the motivation, we introduce the importance indicator of five factors (monetary rewards, assessment from peers, self-realization, morality, and pleasantness) with regard to doing something used in the previous study [26]. Each factor is closely related to the conditions in theory of fraud triangle.

In the survey, we directly ask the following question: Now let's assume that you do something. How much importance of the following items (1: To gain a money or reward, 2: To be assessed from peers or neighbors, 3: To achieve self-realization, 4. To do right moralistically, and 5: To be pleasure) do you regard as motivation behind the behavior? Which way of thinking is close to yours? On a scale of 1-5 with "1" being important not at all, and "5" being very important, please rate your consideration. Figure 3 shows the distribution for the importance indicator of five factors.

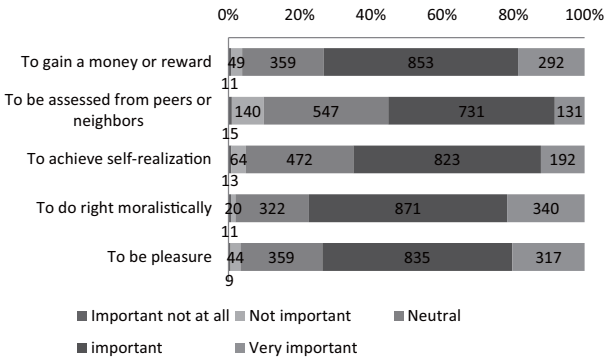

Figure 3: The importance indicator of five factors

[6]Cronbach's alpha of the scale was 0.691, which showed adequate internal consistency of the scale.

Table 3: The descriptive statistics of information security awareness

Average	Median	Min	Max
-1.905 E-08	0.116	-3.260	2.050

Over half of respondents answer that either items are important on motivation behind the behaviors.

2.2.4 Information security awareness

Many previous studies make appeal that it is important to improve the information security awareness and knowledge. This survey incorporates 11 questions regarding the information security awareness and the understanding of the measures used in the previous study [35]. These questions are measured on a five-point Likert scale. By using factor analysis to the questions, one factor is assumed. Cronbach's alpha of the scale was 0.734. The factor is scored so that higher score indicates a higher information security awareness. Table 3 shows descriptive statistics of information security awareness.

2.2.5 Workplace environment

Factors shown above have roots in the individual characteristics. On the other hand, workplace environment represents his or her environment surrounding. As mentioned above, workplace environment is divided by subjective evaluation regarding the workplace and objective indicator such as the organizational attribute.

The survey has some question asking the degree of his or her workplace satisfaction and the organizational information security measure satisfaction. Each question is scored in the range between 0 and 10 points. Figure 4 shows the distributions for the degrees of workplace satisfaction and the measure satisfaction.

The average degree of the workplace satisfaction is about 6.378 points and the average degree of the organizational information security measure satisfaction is about 6.664 points.

According to Albrechtsen and Hovden [2], the organization has the digital divides between employees and information security managers and the gap arises from employee's unsatisfaction or criticism toward the managers and the measures. In this survey, we directly ask a question regarding the evaluation toward the managers in addition to the evaluation of the measures. Concretely, on a seven-point Likert scale we ask to select the appropriate response to the statement that the information security manager implements the measure with understanding the job site and the other statement that the information security manager implements the unforgiving measure. The factors are scored so that higher numbers indicate a higher

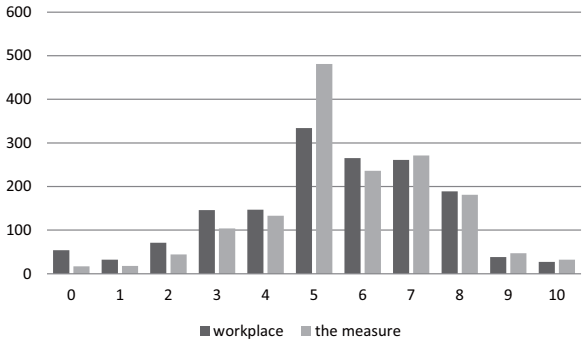

Figure 4: The distributions for the degrees of workplace satisfaction and the measure satisfaction

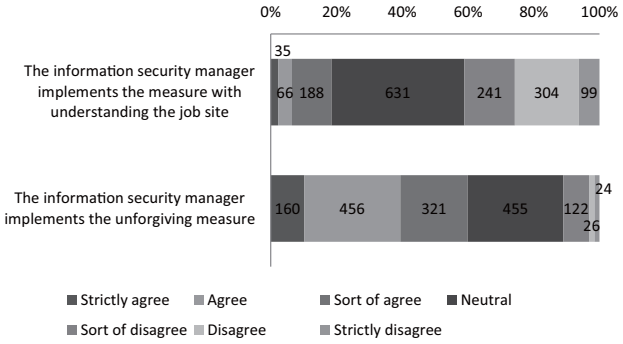

Figure 5: The evaluations toward the managers

the evaluation toward the managers. Figure 5 shows the evaluations toward the managers.

On the other hand, as objective indicators, we use the organizational attributes as follows; listed/non-listed option, the number of employees, and incentive systems for members' working and the employment system which introduced in the organization. We pick up the same five incentive systems used in the previous study [3]. Besides, we use working pattern as the other objective indicator. Table 4 shows these demographic data regarding with the organizational attributes for the respondents of the survey.

2.2.6 The other individual attributes

We have gender, age, education and annual income as popular individual attributes. In addition, in this survey, we ask questions on the experience of encountering the some sort of information security accidents. For example, with regard to a question "have you experienced virus infection in the past two years?" According to the result of this survey, about 10.7% of

Table 4: Demographic data regarding with the organizational attributes

Item		#
Listed/non-listed	Listed company	768
option	Non-listed company	796
# of employees	$<$ 100 (persons)	403
	100-999	439
	1000-4999	295
	5000-9999	125
	$\geq$ 10000	302
Incentive system	Delegating the power from ruling body to lower organization	Yes: 290 No: 1,274
	Introducing the stock option system	Yes: 159 No: 1,405
	Introducing the employee's stock ownership	Yes: 582 No: 982
	Introducing the flexible schedule	Yes: 434 No: 1,130
	Introducing the reassign for the purpose of training	Yes: 203 No: 1,361
Employment system	Introducing permanent employment	Yes: 765 No: 799
Working pattern	Regular	978
	Non-regular	586

Table 5: Demographic data regarding with the individual attributes

Item		#
Gender	Male	1,033
	Female	531
Age	Under 30's	549
	40's	654
	50's	306
	Over 60's	55
Education	University degree or more	968
	The other	596
Annual income	$<$ 2 (million yen)	293
	2-6	708
	6-10	400
	$\geq$ 10	163
Experience of encountering the accidents	Experienced	526
	Not experienced	1,038

respondents experienced some sort of information security accidents. These demographic data regarding with the individual attributes for the respondents of the survey are shown in Table 5.

3 Results of Analysis

We need to set criteria (p-value) of removing insignificant variables in stepwise logit model [29]. In this study, we set $p = 0.15$ as criteria. We enter 28 explanatory variables, and eventually 8 variables such as "Education" and "Age" are removed in the selection process of either cases. In this article, Stata/MP 12.0 is used as statistical analysis software. Table 6 shows the estimated results.

Table 6: Estimated Results

		Coef.	S.E.	z	Remark
1)	Myopic	-0.188	0.110	-1.71	# of obs = 787
	Hypermetro	-0.258	0.113	-2.29	chi2(10) =103.77
	Awareness	-0.320	0.119	-2.69	LL =-251.612
	Satisfaction-WP	-0.079	0.053	-1.50	Pseudo R2 = 0.171
	Manager-2	-0.253	0.085	-2.97	
	Incentive-3	-0.461	0.253	-1.82	
	Employment Sys.	0.573	0.274	2.09	
	Working Pattern	0.948	0.340	2.79	
	Gender	0.523	0.331	1.58	
	Exp. of Accidents	1.119	0.238	4.71	
2)	Myopic	-0.345	0.154	-2.25	# of obs =717
	Hypermetro	-0.307	0.145	-2.11	chi2(10) = 72.31
	Awareness	-0.580	0.149	-3.88	LL = -157.904
	Manager-2	-0.235	0.120	-1.95	Pseudo R2 = 0.186
	Listed	0.501	0.343	1.46	
	Incentive-3	-0.695	0.362	-1.92	
	Employment Sys.	-0.552	0.353	-1.57	
	Working Pattern	0.938	0.425	2.21	
	Income	0.349	0.204	1.71	
	Exp. of Accidents	0.915	0.307	2.98	
3)	Myopic	-0.267	0.141	-1.89	# of obs = 974
	Hypermetro	-0.459	0.142	-3.24	LR chi2(7) = 65.83
	Awareness	-0.490	0.145	-3.37	LL = -181.381
	Manager-1	-0.167	0.106	-1.58	Pseudo R2 =0.154
	Incentive-4	-0.572	0.348	-1.64	
	Working Pattern	0.688	0.343	2.01	
	Exp. of Accidents	0.751	0.295	2.54	
4)	Risk Tolerance	0.065	0.044	1.46	# of obs = 658
	Myopic	-0.319	0.119	-2.67	LR chi2(10) = 69.40
	Hypermetro	-0.219	0.126	-1.74	LL = -208.803
	Motivation-5	0.264	0.171	1.54	Pseudo R2 = 0.143
	Manager-1	-0.296	0.092	-3.22	
	Incentive-2	-0.867	0.469	-1.85	
	Employment Sys.	0.430	0.297	1.45	
	Working Pattern	0.705	0.363	1.94	
	Income	0.274	0.172	1.59	
	Exp. of Accidents	0.863	0.261	3.31	
5)	Myopic	-0.516	0.145	-3.55	# of obs = 908
	Hypermetro	-0.415	0.147	-2.82	LR chi2(8) = 72.74
	Motivation-2	-0.360	0.189	-1.90	LL = -168.392
	Awareness	-0.285	0.144	-1.98	Pseudo R2 = 0.178
	Manager-2	-0.251	0.112	-2.23	
	Incentive-3	-0.635	0.319	-1.99	
	Gender	1.143	0.408	2.80	
	Exp. of Accidents	0.805	0.307	2.62	
6)	Hypermetro	-0.592	0.163	-3.64	# of obs =539
	Motivation-2	-0.623	0.289	-2.16	LR chi2(9) = 61.07
	Motivation-3	0.730	0.312	2.34	LL = -106.874
	Awareness	-0.511	0.166	-3.09	Pseudo R2 = 0.222
	Incentive-1	0.709	0.437	1.62	
	Incentive-2	0.807	0.482	1.68	
	Working Pattern	1.393	0.481	2.90	
	Income	-0.476	0.276	-1.72	
	Exp. of Accidents	0.680	0.381	1.78	

First of all, the estimated coefficients of the hypermetro cognition (Hypermetro) and the experience of information security accidents (Exp. of Accidents) are statistically significant in all cases. The former sign is negative and the latter one is positive in all cases. That is, these factors commonly influence taking problematic behaviors. Next, in almost case, the estimated coefficients of the myopic cognition (Myopic), the information security awareness (Awareness) and working pattern (Working Pattern) are statistically significant, and the sign of the first two coefficients are negative and the sign of the rest is positive. In some cases, the estimated coefficients of either the incentive system (Incentive-1 to Incentive-4) are statistically significant. The sign of the coefficients of Incentive-1 and Incentive-2 in Case 6) are positive and the one of others is negative. In this analysis, the estimated coefficients of the some motivations toward the behavior (Motivation-2, Motivation-3 and Motivation-5) are statistically significant, and the sign of the first one coefficient is negative and the sign of the rest are positive. In addition, with regard to some organizational or individual attributes some of the factors such as evaluation toward the manager (Manager-1 or Manager-2), employment system (Employment Sys.) and annual income (Income). Finally, with regard to the risk attitude, the estimated coefficient of the risk tolerance (Risk Tolerance) is statistically significant and the sign is positive only in the Case 4).

From these estimated results, we can find out the some features on the respondent's behavior of violating the organizational rule, and compare with the previous study [3].

According to Takemura [3], the degrees of both risk aversion and risk tolerance have an effect on the behavior of violating the organizational rule. However, in this analysis the degree of risk tolerance has an effect on only the behavior of forwarding the office's e-mail address to the private address, the risk attitudes do not on have an effect on the other behaviors. With regard to the behavior of forwarding the e-mail, the more individual can tolerate the risk, the more he tends to violate the rule. This is consistent with the asserting of the previous study.

With regard to CFC scale, both myopic cognition and hypermetro cognition have an effect on the behaviors of violating the organizational rules in almost cases. The higher either cognitions of individual is, the less the tendency to violate the rule is. This means that the behavior of violating the rule is related to not only the short-term cognition, but also the long-term cognition. In addition, these cognitions have the same effect to the behavior and are important factors toward the behaviors.

The behaviors of violating the rule are related to the motivations on assessment from peers, self-realization and pleasure, not the motivations on the money and morals. Intriguingly, the greater value on the assessment from peers individual places, the less the tendency to violate the rule is. On the contrary, the individual who places greater value on the self-realization

(or pleasure) tends not to comply with the rule.

With regard to the information security awareness, in many cases it is found that the higher the awareness is, the less the tendency to violate the rule is.

The behavior of violating the rule is independent of the degree of the measure satisfaction, but is not related to the degree of the workplace satisfaction and the evaluation toward the managers in some cases.. In addition, the higher the evaluation toward the managers is, the less the tendency to violate the rule is.

The number of employees which represents the one scale of the organization is not related to the behavior of violating the rule. Additionally, some incentive systems shown in Table 4 are related to the behavior in some cases. And, the individual tend to violate the rule if incentive system of delegating the power from ruling body to lower organization (Incentive-1) is introduced. On the other hand, by introducing the other incentive systems (Incenive-2, Incentive-3 and Incentive-4), the individual tends not to violate the rule. This result is consistent with the result of the previous study.

Intriguingly, in the organization which the permanent employment is introduced, the individual tends to violate the rule. The individual whose working pattern is regular also tends to violate the rule. The fact that individual whose working pattern is regular also tends to violate the rule is consistent with the result of the previous study. Message from this result might be that the individual might violate the organizational rule for the purpose of completing the dairy-task because he confirms not to get fired from his job by the employment system.

With regard to the other individual attributes, encountering the information security accidents is related to the behavior similar to the previous study, but the education is not related to the behavior.

4 Summary and Future Work

In this article, we investigate to determine some key factors which have effects on employees' behaviors of violating the rule which is related to the information leak given a condition that the behaviors are prohibited totally by the organizational measures. As a result, we found out the some features on the respondent's behavior of violating the organizational rule.

First of all, the individual's attitude toward the risk or the cognition of risk (the psychological factors such as risk aversion and risk tolerance) are not related to the behavior of violating the organizational rule in many cases. On the other hand, both myopic cognition and hypermetro cognition measured by CFC scale have effects on the behaviors of violating the organizational rules in almost cases.

Next, the behaviors of violating the rule are related to the motivations

on assessment from peers, self-realization and pleasure, not the motivations on the money and morals.

Third, in many cases individual whose information security awareness is higher tends not to violate the rule.

Fourth, the behavior of violating the rule is independent of the degree of the measure satisfaction and the number of employees which represents the one scale of the organization, but is not related to the degree of the workplace satisfaction and the evaluation toward the managers in some cases. Additionally, some incentive systems shown in Table 4, are related to the behavior in some cases. Intriguingly, in the organization which the permanent employment is introduced, the individual tends to violate the rule. The individual whose working pattern is regular also tends to violate the rule.

With regard to the other individual attributes, encountering the information security accidents is related to the behavior of violating the rule, but the education is not related to the behavior.

It is not easy to control psychological factors such as the individual's attitude toward risk, motivations toward the behaviors or consideration of future consequences. Conversely, the factors regard to the organizational attributes such as the degree of workplace satisfaction or the employment system may be controlled by designing the appropriate organizational environment. Consequently, we consider that it may be effective to improve the information security awareness by information security education and training which is suggested in the some previous literature [28], [36]. Actually, as mentioned above, individual whose information security awareness is higher tends not to violate the rule.

Finally, let us briefly explain future work. Although the empirical studies on the information security measures have meaningful messages in social science and are essential in business practices, the number of the empirical studies are a few yet. So, there are many of yet-to-be-defined information security behaviors and the mechanism. Therefore, the individuals ' information security behaviors should be deeply analyzed from the perspectives of economics and the behavioral science. We will tackle the issues. Though in this article we build a behavioral model by using the logit model, we will build the models based on TPB, GDT or theory of fraud triangle by using statistical tool such as SEM or PLS.

Furthermore, we expect for this article to become an academic contribution to this field, and to become a help to give the incentive for companies to invest in and implement information security measures.

Acknowledgment

This work is supported in part by a Grant-in-Aid from the Zengin Foundation for Studies on Economics and Finance and by Japan Society for the

Promotion of Science: Grantin-Aid for Young Scientists (B) (22730241).

References

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

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

[3] Takemura, T., Empirical Analysis of Behavior on Information Security. *The Proceeding of 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, 358-363, 2011.

[4] Lee, J. and Lee, Y., A Holistic Model of Computer Abuse within Organizations. *Information Management and Computer Security*, Vol.10, No.2, 57-63, 2002.

[5] Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E., The Insider Threat to Information Systems and the Effectiveness of ISO17799. *Computer and Security*, Vol.24, 472-484, 2005.

[6] Ajzen, I., The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, Vol.50, 179-211, 1991.

[7] Chang, K.M., Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior. *Journal of Business Ethics*, Vol.17, No.16, 1825-1834, 1998.

[8] Peace, A.G., Galletta, D.F. and Thong, J.Y.L., Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, Vol.20, No.1, 153-177, 2003.

[9] Pee, L.G., Woon, I.M.Y. and Kankanhalli, A., Explaining Non-work-related Computing in the Workplace: A Comparison of Alternative Models. *Information and Management*, Vol.45, 120-130, 2008.

[10] Galletta, D.F. and Polak, P., An Empirical Investigation of Antecedents of Internet Abuse in the Workplace. *Proceedings of the Second Annual Workshop on HCI Research in MIS*, 47-51, 2003.

[11] Woon, I.M.Y. and Pee, L.G., Behavioral Factors Affecting Internet Abuse in the Workplace: An Empirical Investigation. *Proceedings of the Third Annual Workshop on HCI Research in MIS*, 80-84, 2004.

[12] Foltz, C.B., Schwager, P.H. and Anderson J.E., Why Users (Fail to) Read Computer Usage Policies. *Industrial Management and Data Systems*, Vol.108, No.6, 701-712, 2008.

[13] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., Roles of Information Security Awareness and Percieved Fairness in Information Security Policy Compliance. *Proceedings of the Fifteenth Americas Conference on Information Systems*, Paper 419, 1-9, 2009

[14] Zhang, J., Reithel, B.J., Li, H., Impact of Perceived Technical Protection on Security Behaviors. *Information Management and Computer Security*, Vol.17, No.4, 330-340, 2009.

[15] Workman, M. and Gathegi, J., Punishment and Ethics Deterrents: A Study of Insider Security Contravention. *Journal of the American Society for Information Science and Technology*, Vol.58, N0.2, 212-222, 2007.

[16] Straub, D., Effective IS Security: an Empirical Study. *Information Systems Research*, Vol.1, No.3, 255-276, 1990.

[17] Lee, S.M., Lee, S.G., Yoo, S., An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories. *Information and Management*, Vol.40, 707-718, 2004.

[18] D'Arcy, J., Hovav, A. and Galletta, D., User Awareness of Security Countermeasures and Its Impact on Information System Misuse: A Deterrence Approach. *Information Systems Research*, 1-20, 2008.

[19] Komatsu, A., Akai, K., Ueda, M. and Matsumoto, T., Is the Security Measurement Situation a Social Dilemma? Applying Bot Measurement Operation. *IPSK SIG Technical Report*, Vol.2009-CSEC-46, No.40, 1-8, 2009.

[20] Reason, J., Parker, D. and Lawton R., Organizational Controls and Safety: The Varieties of Rule-Related Behaviour. *Journal of Occupational and Organizational Psychology*, Vol.71, 289-304, 1998.

[21] Cressey, D.R., *Other People's Money: A Study in the Social Psychology of Embezzlement*, New Jersey: Patterson-Smith, 1973.

[22] Wells, J.T., *Principles of Fraud Examination*, 3rd ed, New Jersey: John Wiley and Sons, 2010.

[23] Cramer, J.S. Hatog, J. Jonker, N. and Van Praag, C.M., Low Risk Aversion Encourages the Choice for Entrepreneurship: an Empirical Test of A Truism. *Journal of Economic Behavior and Organization*, Vol.48, 29-36, 2002.

[24] Becker, G.M. Degroot, M.H. and Marschak, J., Measuring Utility by a Single Response Sequential Method. *Behavioral Science*, Vol.9, 226-32, 1964.

[25] Strathman, A., Gleicher, F., Boninger, D.S., and Edwards, C.S., The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior. *Journal of Personality and Social Psychology*, Vol.66, No.4, 742-752, 1994.

[26] Tsukahara, Y., Human Motivating Behavior and Employee's Behavior. Chida, R., Tsukahara, Y. and Yamamoto, M. (eds), *Behavioral Economics: Theory and Practice*, Tokyo: Keiso-shobo, 50-71, 2010.

[27] Thomson, M.E. and Solms R., Information Security Awreness: Educating Your Users Effectively. *Information Management and Computer Security*, Vol.6, No.4, 167-173, 1998.

[28] Albrechtsen, E. and Hovden, J., Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computer and Security*, Vol.29, 432-445, 2010.

[29] Hosmer, D.W. and Lemeshow, S., *Applied Logistic Regression*, 2nd ed., New York: Wiley-Interscience Publication, 2000.

[30] Couper, M.P., Web Surveys: A Review of Issues and Approaches. *Piblic Opinion Quarterly*, No.64, 464-494, 2000.

[31] Lim, V.K.G., The IT Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice. *Journal of Organizational Behavior*, Vol.23, 675-694, 2002.

[32] Information-Technology Promotion Agency, *Information Security White Paper*. Information-Technology Promotion Agency, Japan, 2011.

[33] Chen, J.V., Chen, C.C. and Yang, H.H., An Empirical Evaluation of Key Factors Contributing to Internet Abuse in the Workplace. *Industrial Management and Data Systems*, Vol.108, No.1, 87-106, 2008.

[34] Kahneman, D. and Tversky, A., Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, Vol.47, No.2, 263-292, 1979.

[35] Takemura, T., 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*, Vo.2, No.1, 20-26, 2010.

[36] Mcilwraith, A., *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness.* Hampshire: Gower Pub Co., 2006.