Risk Assessment Quantification of Social-media Utilization in Enterprise

Shigeaki Tanimoto, Motoi Iwashita
Faculty of Social Systems Science
Chiba Institute of Technology
Chiba, Japan
shigeaki.tanimoto@it-chiba.ac.jp

Yoshiaki Seki
Faculty of Informatics
Tokyo City University
Kanagawa, Japan
seki@tcu.ac.jp

Hiroyuki Sato
Information Technology Center
The University of Tokyo
Tokyo, Japan
schuko@satolab.itc.u-tokyo.ac.jp

Atsushi Kanai
Faculty of Science and Engineering
Hosei University
Tokyo, Japan
yoikana@hosei.ac.jp

***Abstract*—The purpose of this study is to make social media utilization by enterprises safer, more secure, and more convenient. Enterprises use social media for marketing, but this presents a lot of risks. These risks were comprehensively extracted in our previous study, but it was only a qualitative study, so a quantitative evaluation is needed to make the risks' countermeasures more practical. Thus, in this paper, the risk factors identified in the previous study are analyzed and quantitatively evaluated. Specifically, the values of the risk factors were approximately calculated by using a risk formula used in the field of information security management systems (ISMS). In this way, it was found that the countermeasures in the previous study could reduce their corresponding risk factors by about 60%. The results herein can contribute to helping enterprises to utilize social media more safely, securely, and conveniently in the future.**

Keywords- Social-media Utilization; SNS; Risk Assessment; Risk Breakdown Structure; Risk Matrix; Quantification

I. INTRODUCTION

In recent years, social media (this is so-called Social Networking Service, and after this, abbreviates to SNS), such as Twitter [1] and Facebook [2], are progressing with the popularization of the Internet. Moreover, not only an individual but use of an enterprise is increasing as a user. In investigation of IDC Japan, the SNS capacity factor in the enterprise in the 2012 fiscal year is 36.9%, and the rise of ten points is seen as compared with the 2011 fiscal year [3]. And it is "advertisement" that was the highest about the utilization purpose and the use of SNS in an enterprise, and rates are 63.2% of 400 companies which are utilizing SNS [4]. The trend which is going to strengthen and complement with SNS from this "advertisement" which was being made by the mass media, such as a newspaper and television, until now is seen. On the other hand, the mid- and long-term use purposes, such as a "brand" and "an increase in a potential customer", are increasing as the degree of SNS utilization of an enterprise increases [4]. It is thought that there is expectation for the information diffusion between the users who are the features of SNS as a background of such use. In the conventional marketing, it was that the mass media, such as television and radio, offer "one way information dissemination" to consumers.

On the other hand, in marketing using SNS, it is possible it not only to disseminate information only to those who are interested in its own brand, but to disseminate information to its own brand to those who are not interested. Furthermore, SNS is very effective at the point that construction is possible to those who are not interested through the new point of contact of "friendship" [5].

In this way, SNS is being increasingly utilized by enterprises as ICT-ization progresses. This is because enterprises can easily use SNS to advertise and describe their products and services. However, SNS presents many risks. For example, a photograph of a salesclerk in a convenience store stepping into a freezer for food was uploaded to Twitter in Japan [6]. As the result, the convenience store was obliged to apologize and a franchise contract was canceled. In this way, a photo on a SNS led to reputational damaged and financial loss for an enterprise. However, enterprises have not implemented sufficient countermeasures against SNS risks.

In this paper, we describe a quantitative evaluation of the risk factors of SNS utilization for an enterprise obtained in our previous study and their proposed countermeasures. Specifically, a risk value is approximately calculated on the basis of a formula for each risk factor used in the field of information security management systems (ISMS) [7]-[9]. Then, on the basis of this value, the effect of the countermeasures on the risks can be quantitatively evaluated. It is shown that the countermeasures in the previous study can reduce their corresponding risk factors by about 60%. The results herein can contribute to helping enterprises to utilize social media more safely, securely, and conveniently in the future.

978-1-5090-0806-3/16/$31.00 copyright 2016 IEEE

Section 2 summarizes features of SNS and related research. Section 3 reviews our previous study and its remaining problems. Section 4 describes the quantitative evaluation of risk assessment for SNS utilization by an enterprise. Section 5 is a conclusion and describes future work.

II. SUMMARY OF SNS AND RELATED WORK

A. Feature of SNS

SNS is often used by the mass media, such as TV news and a newspaper, in recent years. The definition of SNS is shown in the following. SNS is one of the information media expanded on the Internet. In SNS, they are the media containing social elements, such as information distribution using the information dissemination by an individual, communication between individuals, and connection of people and a person [10].

In order to disseminate information using equipment etc., a large amount of funds are required for the conventional mass media, and information has been disseminated only in one way. However, since SNS appeared, the fund for the equipment which disseminates information has not necessarily been required. And information can also disseminate information to both directions instead of one way. In this way, the feature of SNS is as follows. The sources of information which the visitor itself needs can be chosen from various dissemination subjects. Circulation of information is controlled using human relations, such as a friend and a coworker. Next, service of typical SNS is mentioned [11].

B. Related Work

Many papers about SNS security have been published [12]-[19]. Some researchers [12]-[17] have researched it from a technical viewpoint on the basis of various security incidents regarding privacy protection. Moreover, other works have investigated SNS utilization and its risks for enterprises [18]-[19].

However, these are qualitative studies, while quantitative studies have been insufficient. A quantitive viewpoint is important in order to investigate from a more practical viewpoint, for example, cost effectiveness. In this paper, the risks of the SNS utilization for an enterprise are quantified on the basis of our previous research [19].

III. PREVIOUS STUDY: RISK ASSESSMENT OF SNS UTILIZATION IN AN ENTERPRISE

A. Extraction of Risk Factor

The RBS (Risk Breakdown Structure) method which is the typical method of risk management is used for extraction of a risk factor [20]. A result is shown in Table I. As shown in the table, the risk factor in SNS utilization of an enterprise was analyzed hierarchical from a comprehensive viewpoint, and 19 items of risk factor was extracted on the whole [19].

TABLE I. RISK FACTOR LIST BASED ON RBS TO SNS UTILIZATION OF ENTERPRISE

High Level	Middle Level	Minimum Level: Risk Factors	Detail Contents of Risk Factor
1. Dissemination Method	**1.1 Information Leakage**	1.1.1 Intentional information leakage by employee	An employee does information leakage of the confidential information of an enterprise intentionally, and there is fear of brand loss of an enterprise.
		1.1.2 Unprepared Leak of Information by Employee	Information leakage of the confidential information of an enterprise is carelessly carried out from an employee's individual account.
	1.2 Blog Flaming	1.2.1 "Faking": employee's etc. remark is thought to be "Faking."	The observation from enterprise staffs to a consumer is thought to be "faking", and has a bad influence on the impression of an enterprise.
		1.2.2 Spoofing	The information which made the mistake in faking account or employee of an enterprise is passed.
2. Contents of Dissemination	**2.1 Information Leakage**	2.1.1 Information leakage using SNS by part-time job salesclerk	A part-time job salesclerk needs to post a practical joke easily, and carry out blog flaming.
		2.1.2 Information leakage using SNS by visitor	To an enterprise, consumers contribute a practical joke and do blog flaming.
	2.2 Blog Flaming	2.2.1 Net slander to customer and others by employee	A trouble occurs and carries out blog flaming from the slander and slander to the customer by an employee.
		2.2.2 Expansion of the criticism based on the unsuitable correspondence for criticism	To the criticism from claimer on SNS, etc., it cannot be coped with appropriately, but criticism is expanded, and blog flaming is carried out.
		2.2.3 Infringe on copyright when posting.	An employee's etc. post infringes on copyright and affects the brand of an enterprise.
		2.2.4 Post about dealings enterprise etc. and trouble occurs.	For a dealings enterprise, an employee makes a disadvantageous remark and affects dealings.
		2.2.5 The scandal of an enterprise, etc. spread to SNS and become a trouble.	The scandal of an enterprise in a public field should be reproduced by SNS, and should carry out blog flaming to it.
3. Dissemination Cost	**3.1 Shortage of Information Dissemination**	3.1.1 The information which sends is insufficient.	The shortage of communication with the consumer by the shortage of information dissemination
		3.1.2 The number of followers does not increase.	There are few the followers and fans of SNS whom an enterprise uses.
		3.1.3 A user's engagement (reaction) is not obtained.	Neither the number of retweet of a twitter nor the number of "Like" of Facebook increases.
	3.2 Lack of Understanding of System	3.2.1 Shortage of employment know-how of SNS	The know-how over the marketing utilization method by SNS is insufficient.
		3.2.2 Shortage of person in charge and budget	An enterprise cannot increase the number of a SNS section.
		3.2.3 Measurement of effect is difficult.	Measurement of the effect by SNS is difficult.
		3.2.4 Management's lack of understanding	An understanding of SNS is insufficient of executive officers.
		3.2.5 Cooperation between departments is difficult.	It is hard to take cooperation with the SNS administration and its other position.

B. *Risk Analysis in SNS Utilization*

Next, we devised potential countermeasures against the identified risks; these are shown in Table I. The risk matrix method was used to deduce these countermeasures [21]. As shown in Fig. 1, this method classifies risks into four kinds, *i.e., Risk Transference*, *Risk Mitigation*, *Risk Acceptance*, and *Risk Avoidance*, in accordance with their generation frequency and degree of incidence. Furthermore, it gives guidelines to draw up countermeasures. Table II lists the classification of the risk matrix methods in correspondence with its proposed countermeasures.

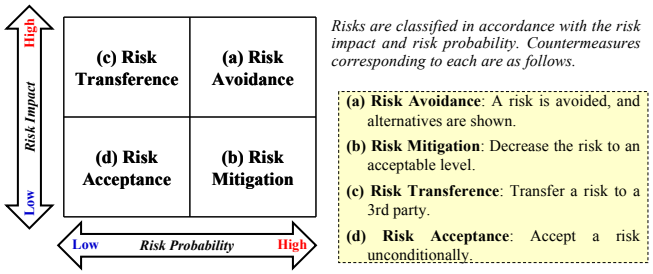

Figure 1. Risk Matrix Method

TABLE II. RISK FACTORS EXTRACTED BY RBS AND PROPOSED COUNTERMEASURES

Risk Factors	Risk Probability	Risk Impact	Classification of Risk Matrix	Proposed Countermeasures of SNS Utilization in Enterprise	Classification of Countermeasure
1.1.1 Intentional information leakage by employee	Low	High	Risk Transference	The organization which creates the guideline on SNS and it educates to an employee is established.	Employee Education
1.1.2 Unprepared Leak of Information by Employee	Low	High	Risk Transference	The organization which creates the guideline on SNS and it educates to an employee is established.	Employee Education
1.2.1 "Faking": employee's etc. remark is thought to be "Faking."	Low	High	Risk Transference	Selection of language and the method of information dissemination which do not become unpleasant for consumers are devised.	Systems Configuration
1.2.2 Spoofing	Low	High	Risk Transference	Giving a server certificate etc. strengthens the authentication system of an enterprise.	Systems Configuration
2.1.1 Information leakage using SNS by part-time job salesclerk	High	High	Risk Avoidance	The organization which I have observed on a par with an employee by contract terms, such as work rules, also to a part-time job salesclerk is established.	Employee Education
2.1.2 Information leakage using SNS by visitor	High	High	Risk Avoidance	The report of the net slander to an enterprise is supervised.	Systems Configuration
2.2.1 Net slander to customer and others by employee	Low	High	Risk Transference	The organization which creates the guideline on SNS and it educates to an employee is established.	Employee Education
2.2.2 Expansion of the criticism based on the unsuitable correspondence for criticism	Low	High	Risk Transference	The solution for claimer on SNS, etc. is created, and it devises so that the contents of the copyright which establishes the organization to educate may be made to permeate all employees.	Employee Education
2.2.3 Infringe on copyright when posting.	High	High	Risk Avoidance	For example, at the field of the employee training to SNS, copyright is also educated collectively.	Employee Education
2.2.4 Post about dealings enterprise etc. and trouble occurs.	Low	High	Risk Transference	The organization which creates the guideline on SNS and it educates to an employee is established.	Employee Education
2.2.5 The scandal of an enterprise, etc. spread to SNS and become a trouble.	Low	High	Risk Avoidance	When it makes efforts not to generate a scandal and generates, an enterprise performs apology correspondence and it keeps it from spoiling an enterprise brand.	Employee Education
3.1.1 The information which sends is insufficient.	High	Low	Risk Mitigation	The information which can be offered to consumers is extracted and consumers are always provided with information.	Systems Configuration
3.1.2 The number of followers does not increase.	Low	Low	Risk Acceptance	The information of an enterprise enables it to match appropriately to consumers' needs.	Systems Configuration
3.1.3 A user's engagement (reaction) is not obtained.	Low	Low	Risk Acceptance	The information of an enterprise enables it to match appropriately to consumers' needs.	Systems Configuration
3.2.1 Shortage of employment know-how of SNS	High	Low	Risk Mitigation	The budget of SNS utilization is obtained.	Systems Configuration
3.2.2 Shortage of person in charge and budget	High	Low	Risk Mitigation	Cost effectiveness of SNS is clarified and an understanding of the executives is obtained.	Visualization of Cost Effectiveness
3.2.3 Measurement of effect is difficult.	High	Low	Risk Mitigation	In order to clarify cost effectiveness of SNS, KGI (important goal achievement index) and KPI (important key performance indicator) are used, for example [22].	Visualization of Cost Effectiveness
3.2.4 Management's lack of understanding	High	Low	Risk Mitigation	In order to clarify cost effectiveness of SNS, KGI (important goal achievement index) and KPI (important key performance indicator) are used, for example.	Visualization of Cost Effectiveness
3.2.5 Cooperation between departments is difficult.	Low	Low	Risk Acceptance	Strengthening of the cooperation between departments based on top management	Visualization of Cost Effectiveness

C. *Tendancy of Countermeasure*

Here, the tendency for every measure over each phenomenon is analyzed based on Table II.

(1) *Risk Transference*: seven risk measures were set to Risk Transference. The main countermeasures were creating the guideline on SNS to an employee and establishing the organization to educate. This is clarifying the posture as an enterprise and clarifying locus of responsibility.

(2) *Risk Mitigation*: The number of the risk measures of Risk Mitigation was five. It is clarifying cost effectiveness by SNS utilization as proposed measures, and strengthening an understanding of executive officers.

(3) *Risk Avoidance*: The number of risks of measures having been set to Risk Avoidance was four. As proposed measures, it is establishing the organization which can always be supervised for SNS.
(4) *Risk Acceptance*: The number of risks of having been set to Risk Acceptance was three. As proposed measures, marketing which understood the characteristic of SNS is important.

IV. Quantitative Evaluation: Risks of SNS Utilization for an Enterprise

Here, the validity of a countermeasure is evaluated through a quantification of the risk factors shown in Table II. First, a risk formula used in the field of information security management systems (ISMS) is shown [7]-[9]. Next, an approximation is described for calculating a risk value on the basis of our previous qualitative results [19]. Finally, a risk value for SNS utilization in an enterprise is deduced by using the formula and approximation.

A. Risk formula

Each risk value is quantified by using (1), which is used in the field of ISMS [7]-[9].

$$\textit{Risk value} = \textit{value of asset} * \textit{value of threat} * \textit{value of vulnerability} \quad (1)$$

Generally, all elements of the right-hand side of (1) are very difficult to calculate. In this paper, the following approximation is used to simplify these elements [23].

1) Approximation of the Asset Value

Here, the asset value of (1) is approximated in terms of the risk impact in the risk matrix, as shown in Figure 2. This approximation is based on the following reasons. The amount of damage to assets was considered. As the further approximation, the amount of damage was considered to be the risk impact. Additionally, other works [7]-[9] define the risk impact from 1 (low) to 5 (high). As a further approximation, these values are mapped in risk impact to a risk matrix [23]. As shown in Figure 2 he risk impact of the risk matrix is divided in two. For simplicity, the higher division approximates the maximum risk impact (risk value ≒ 5). Similarly, the lower division approximates the minimum risk impact (risk value ≒ 1).

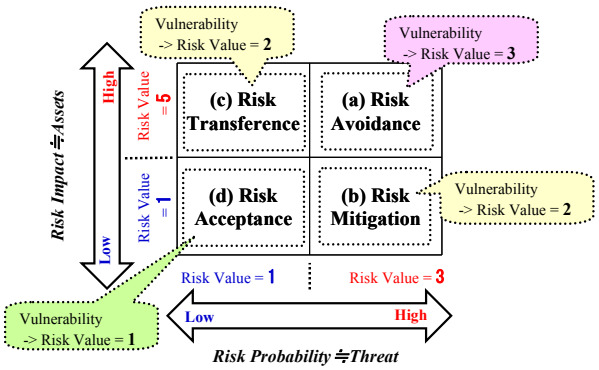

Figure 2. Risk Value Approximation of Risk Matrix [15]

2) Approximation of the Threat Value

The threat value of (1) is approximated in terms of the risk probability in the risk matrix, as shown in Figure 2. This approximation is based on the following reasons. Threat was thought to strongly depend on risk probability. In other works [7]-[9], the risk probability is defined as ranging from 1 (low) to 3 (high). These values are mapped to the generation frequencies of the risk matrix in Figure 2, as well as the above-mentioned risk impact approximation. That is, the higher division approximates the maximum risk probability (risk value ≒ 3), and the lower division approximates the minimum risk probability (risk value ≒ 1).

3) Approximation of the Value of Vulnerability

The vulnerability evaluation is defined in other works [7]-[9] as well. It is defined on a three-level scale: 3 (High), 2 (Medium), and 1 (Low). These levels were approximated in accordance with the classification of the risk matrix in Figure 2. Below, the four domains in the figure are classified into three categories in accordance with the risk probability and risk impact.

- *Risk Avoidance*: both the risk probability and risk impact are high. It approximately corresponds to the highest risk classification.
- *Risk Transference and Risk Mitigation*: either the risk probability or the risk impact is high. They approximately correspond to the second highest risk classification.
- *Risk Acceptance*: both the risk probability and risk impact are low. It approximately corresponds to the lowest risk classification.

In the above-mentioned classification, *Risk Avoidance* cases are approximated to 3 (High), *Risk Transference* and *Risk Mitigation* cases to 2 (Medium), and *Risk Acceptance* cases to 1 (Low). As mentioned above, (1) is approximated as (2). In addition, the approximate value of each parameter of (2) becomes as shown in Tables III and IV.

$$\textit{Risk value} \fallingdotseq \textit{value of risk impact} * \textit{value of risk probability} * \textit{value of vulnerability} \quad (2)$$

TABLE III. Approximate Value of Risk Impact and Risk Probability of (2)

	Asset ≒ Risk Impact	Threat ≒ Risk Probability
High	**5**	**3**
Low	**1**	**1**

TABLE IV. Approximate Value of Vulnerability of (2)

	Vulnerability
Risk Avoidance	**3**
Risk Transference and Risk Mitigation	**2**
Risk Acceptance	**1**

TABLE V. RISK VALUE BEFORE AND AFTER COUNTERMEASURES

Risk Factors	Proposed Countermeasure (Classification of Countermeasure)	Threat≒ Risk Probability	Asset ≒ Risk Impact	Vulnerability ≒ Classification of Risk Matrix		Value of Risk	
				Before Counter-measure	After Counter-measure	Before Counter-measure	After Counter-measure
1.1.1 Intentional information leakage by employee	Employee Education	1	5	2	1	10	5
1.1.2 Unintentional Leak of Information by Employee	Employee Education	1	5	2	1	10	5
1.2.1 "Faking": employee's remark is thought to be "Faking."	Systems Configuration	1	5	2	1	10	5
1.2.2 Spoofing	Systems Configuration	1	5	2	1	10	5
2.1.1 Information leakage on SNS by part-time job salesclerk	Employee Education	3	5	3	1	45	15
2.1.2 Information leakage on SNS by customer	Systems Configuration	3	5	3	1	45	15
2.2.1 Online slander of customers and others by employee	Employee Education	1	5	2	1	10	5
2.2.2 Expansion of the criticism based on an unsuitable response to criticism	Employee Education	1	5	2	1	10	5
2.2.3 Infringement on copyright when posting.	Employee Education	3	5	3	1	45	15
2.2.4 Post about dealings of enterprise that causes trouble.	Employee Education	1	5	2	1	10	5
2.2.5 The scandal of an enterprise spreads to SNS and causes trouble.	Employee Education	1	5	3	1	15	5
3.1.1 The information uploaded is insufficient.	Systems Configuration	3	1	2	1	6	3
3.1.2 The number of followers does not increase.	Systems Configuration	1	1	1	1	1	1
3.1.3 No user engagement (reaction) is obtained.	Systems Configuration	1	1	1	1	1	1
3.2.1 Shortage of employment know-how of SNS	Systems Configuration	3	1	2	1	6	3
3.2.2 Shortage of people involved and budget	Visualization of Cost Effectiveness	3	1	2	1	6	3
3.2.3 Measurement of effect is difficult.	Visualization of Cost Effectiveness	3	1	2	1	6	3
3.2.4 Management's lack of understanding	Visualization of Cost Effectiveness	3	1	2	1	6	3
3.2.5 Cooperation between departments is difficult.	Visualization of Cost Effectiveness	1	1	1	1	1	1
Total						**253**	**103**

B. Calculation Result of Risk Value

The risk values before applying countermeasures against risks were calculated using (2) (see Table V (Before Countermeasure)).

Next, the risk values after applying countermeasures as shown in Table II were calculated. Table V (After Countermeasure) shows the resulting risk values when performing the countermeasures.

Here, supposing an ideal case, vulnerability was assumed to be 0 as a result of using the proposed countermeasure. Moreover, supposing an actual case, this countermeasure is not always perfect. Thus, the vulnerability of an actual case is approximated to 1 (the minimum level).

Table VI summarizes the results shown in Table V. This table shows that the risk can be reduced by about 60%.

TABLE VI. EVALUATION RESULTS (SUMMARIZATION OF RISK VALUE BEFORE AND AFTER COUNTERMEASURES)

	Before countermeasure against risk factors (①)	After countermeasure against risk factors (②)
Total risk value	**253**	**103**
Risk reduction rate = (①－②) / ①	**-**	**0.60**

C. Discussion

As shown in Table VI, it turned out that the risk reduction rate when the countermeasures were taken is about 60 percent. Here, as Section IV.B showed, it is assumed that the vulnerable value after the countermeasure against a risk is 1 (low). Originally, from the viewpoint of an ideal result,

the vulnerable value after a countermeasure should be 0. Therefore, this evaluation is similar as a real-world situation.

Next, the individual effect of proposed measures is shown in Table VII. "Employee education" can apparently reduce risk by about 63 percent.

TABLE VII. EVALUATION RESULTS (SUMMARIZATION OF RISK VALUE BEFORE AND AFTER COUNTERMEASURES)

Proposed Countermeasure (Classification of Countermeasure)	Reduction Number of Risk Value by Countermeasure Implementation	Reduction Rate of Risk Value
Employee Education	95	0.63
Systems Configuration	46	0.31
Visualization of Cost Effectiveness	9	0.06
Total	150	-

These results also show that a detailed numerical expression can treat a risk more specifically by quantifying it and its prospective countermeasure.

V. CONCLUSION AND FUTURE WORK

In this paper, risks in SNS utilization for an enterprise were quantifiably assessed. In our previous study, although countermeasures were developed from a qualitative risk assessment, their effectiveness could not be quantified. Hence, in this study, we performed a quantitative evaluation that used a risk value. It was shown that countermeasures in the previous study could reduce their corresponding risk factors by about 60%. These results mean that the effect of countermeasures developed in our previous qualitative evaluation can be more specifically evaluated by introducing a risk value.

In the future, we will further improve countermeasures and verify their cost effectiveness.

ACKNOWLEDGMENTS

This work was supported by the Japan Society for the Promotion of Science (JSPS, KAKENHI Grant Number 15H02783).

REFERENCES

[1] H. Kwak, et al., What is Twitter, a Social Network or a News Media?, WWW 2010, April 26–30, 2010, Raleigh, North Carolina, USA

[2] C. Dwyer, et al., Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace, Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09–12 2007

[3] IDC Japan investigation : ITmedia news, (in Japanese) http://www.itmedia.co.jp/news/articles/1210/23/news100.html

[4] Tribal Media House,Inc.& Cross marketing Inc., "Social-media white paper 2012", (in Japanese)

[5] Progressing social media and social marketing, (in Japanese), http://www.yhmf.jp/pdf/activity/adstudies/vol_34_01_01.pdf

[6] The newest current-events term 2015 editions, Seibido Shuppan, 2013, (in Japanes)

[7] M. S. Toosarvandani, N. Modiri, and M. Afzali, "The Risk Assessment and Treatment Approach in order to Provide LAN Security based on ISMS Standard," International Journal in Foundations of Computer Science & Technology (IJFCST), pp. 15–36, Vol. 2, No. 6, Nov., 2012

[8] H. Sato, T.Kasamatsu, T. Tamura, and Y. Kobayashi, "Information Security Infrastructure," Kyoritsu Shuppan Co., Ltd., 2010, (in Japanese)

[9] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4

[10] IT term dictionary , e-Words, (in Japanese) http://e-words.jp/w/E382BDE383BCE382B7E383A3E383ABE383A1E38387E382A3E382A2.html

[11] DIAMOND,Inc., Social network revolution, (in Japanese) http://www.diamond.co.jp/book/9784478015766.html

[12] Chi Zhang et al., Privacy and security for online social networks: challenges and opportunities, IEEE Network, Vol. 24, Issue 4, pp.13–18, 2010

[13] Ralph Gross, et al., Information revelation and privacy in online social networks, WPES '05 Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71–80, 2005

[14] Aaron Beach, et al., Solutions to Security and Privacy Issues in Mobile Social Networking, Computational Science and Engineering, CSE '09. International Conference on Vol. 4, pp.1036–1042, 2009

[15] Leucio Antonio Cutillo, et al., Privacy preserving social networking through decentralization, Wireless On-Demand Network Systems and Services, WONS 2009. Sixth International Conference on, pp.145–152, 2009

[16] George Danezis, Inferring privacy policies for social networking services, AISec '09 Proceedings of the 2nd ACM workshop on Security and artificial intelligence, pp. 5–10, 2009

[17] Hongyu Gao, et al., Security Issues in Online Social Networks, IEEE Internet Computing, Vol. 15, Issue 4, pp. 56–63

[18] Japan Computer System Seller Association, The countermeasure against the risk of the SNS utilization in an enterprise, pp. 45–84, 2015, (in Japanese) , http://www.jcssa.or.jp/img/jcssa-pdf150109.pdf

[19] S. Tanimoto, et al., Risk Assessment of Social-media Utilization in an Enterprise, SNPD 2015, 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, pp. 577–580, 2015

[20] Risk Breakdown Structure, http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html

[21] Cox's risk matrix theorem and its implications for project risk management, http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/

[22] activecore Inc. , KPI of social media, (in Japanese) http://www.activecore.jp/column/sns_6

[23] S. Tanimoto, et al., Risk Assessment Quantification in Hybrid Cloud Configuration, SECURWARE 2015 : The Ninth International Conference on Emerging Security Information, Systems and Technologies, pp. 1–6