A Study of Compensation in Personal Identifiable Information Leakage

Tomohisa Ishikawa[1]* and Kouichi Sakurai[2]
[1] N/A, Tokyo, Japan
scientia.admin@gmail.com
[2] Kyushu University, Fukuoka, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract

The organizations and companies that have the leakage of personal identifiable information (sometimes abbreviated as PII) should take a lot of necessary actions such as investigation, public relations, and compensation for customers. Especially, in Japan, mass media tend to broadcast security news and these information leakage incidents as daily news. Therefore, the organizations or companies are also interested in incident prevention and incident handling planning. On the other hand, it is pointed out that there is the difficulty of understanding cost-benefit of security investments. On top of that, the compensation for the victims in personal identifiable information leakage is not prescribed in regulation or guidelines, and there are only few cases of the civil trials for the compensation. Therefore, compensations are determined by past examples. In this paper, firstly, the authors briefly explores the model for security incidents cost-benefit analysis. Secondly, by the evaluation of real examples and JO model, which is a current famous estimation model of compensation for personal identifiable information leakage, the authors show that the actual compensation in Japan, and then the gap between the model and real examples. Finally, the authors points out the considerable points for model in future sophistication.

Keywords: Privacy, Information Leakage, Personal Identifiable Information, Compensation

1 Introduction

As web service advances, registrations of users' personal identifiable information are very popular. By the registration, although both web service providers and users gain the convenience, a number of security incidents related to personal identifiable information leakage contentiously happen. It is because the security level of some web services are not sufficient, and these websites have some weakness. According to the research by Japanese IT Security consulting firm, NRI SecureTechnologies, "Cyber Security Trend - Annual Review 2013"[10], approximately 33% of websites have critical vulnerabilities causing illegal access to sensitive information. Although Japanese companies and organizations have been attacked, the countermeasures and prevention against personal identifiable information leakage have been becoming the one of the management issues after security incidents in a multi-national corporation in 2011. In this paper, firstly, the authors briefly explores the model for security incidents cost-benefit analysis. Secondly, by the evaluation of real examples and JO model, which is a current famous estimation model of compensation for personal identifiable information leakage, the authors show that the actual compensation in Japan, and then the gap between the model and real examples. Finally, the authors points out the considerable points for model in future sophistication.

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 7 (January 15, 2015)
*Corresponding author: Independent(works as IT security consultant in Japan)

2 Related Works

In order to consider the cost of security incidents and personal identifiable information leakage, qualitative model[3] and quantitative models are proposed. This paper briefly explains three quantitative models.

2.1 ROSI Framework

The first quantitative model is ROSI (Return on Security Investment) framework[4]. This model can evaluate the return on investment in security. The purpose of this framework is seeking the cost-effective security, and it is the basis of modern security investment. The basic approach is that the security manager can determine ARE (Annual Loss Expectancy) from estimated SLE (Single Loss Expectancy) and ARO (Annual Rate of Occurrence). By using ARE, security managers can understand the possible loss of the security breach and decide the total amount of security investment. Although ROSI framework is the very popular quantitative approach, and many other researches use this framework concept, the problem is that it is hard to calculate an accurate value of each parameter.

2.2 CyberTab Framework

The second framework is CyberTab[11] made by The Economist Intelligence Unit. This framework leads to calculate the cost of one incident response against a particular threat. By using CyberTab framework, security managers can calculate the cost for one incident, and it is useful for considering ROSI framework. The distinctive feature of this framework is the classification of factors that the security manager should consider. This framework points out that the cost of public relations department and legal department in incident handling and they have significant roles to protect companies. In this perspective, this is very useful to simulate the actual cost of the incident.

2.3 JO Model

The third model is the JO Model (JNSA Damage Operation Model for Individual Information Leak)[1] made by JNSA (Japan Network Security Association), and it focuses on the assumed compensation cost in personal identifiable information leakage. This model evaluates the compensation based on three perspectives; personal information value, social responsibility degree, and post-incident response appraisal. Since JNSA working group designed this model simply, many organizations and companies use this model as the indicator of the possible cost. This paper explains more details of the JO model in order to focus on the consideration of the expected compensation costs of personal identifiable information.

3 How JO Model Works?

According to JO model, the assumed compensation cost should be decided by the multiplication of three factors.

1. Value of Personal Information Leaked
2. Degree of social responsibility of the organization
3. Appraisal of post incident response by the organization

3.1 Value of Personal Information Leaked

The first factor is ”Value of Personal Information Leaked”. In order to handle efficiently, the value should be defined as the multiplication of three parameters.

1. Value of Basic Information
2. Degree of Information Sensitivity
3. Degree of Ease in Identifying the Individual

3.1.1 Value of Basic Information

First parameter is ”value of basic information”, and it is the basis of personal information. In JO model, the default value is 500 yen, and working group referred the case of security incidents in 2003. The famous payment card company, Lawson Card, leaked approximately 560,000 records of personal identifiable information, and compensation is 500 yen[13].

3.1.2 Degree of Information Sensitivity

Second parameter is ”Degree of Information Sensitivity”, and it decides the importance of personal information. The definition is following.

$$IS - Degree = [max(10^{x-1} + 5^{y-1})]$$

X is the maximum of the emotional distress level, and Y is the maximum of the economic distress level. JO Model working group had theoretical analysis, and they classified personal identifiable information into two categories; ”Economic Loss” and ”Emotional Loss”. Then they make an ER Map (Economic Privacy Map). It is a citation from the report[1] made by the working group.

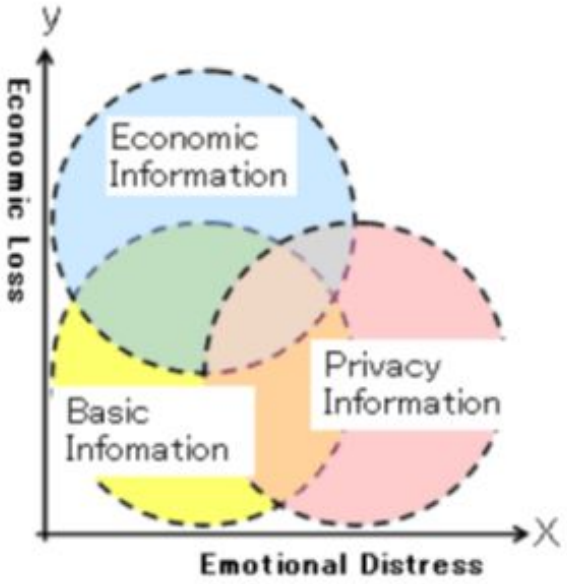

Figure 1: EP Map (Cited from Reference[1])

Then, working group attempted to map each personal identifiable information into ER map, and they simplified the map called Simple EP Map. The authors tried to pick up the famous personal identifiable information from original one. (Please refer [1] if the original one is needed.)

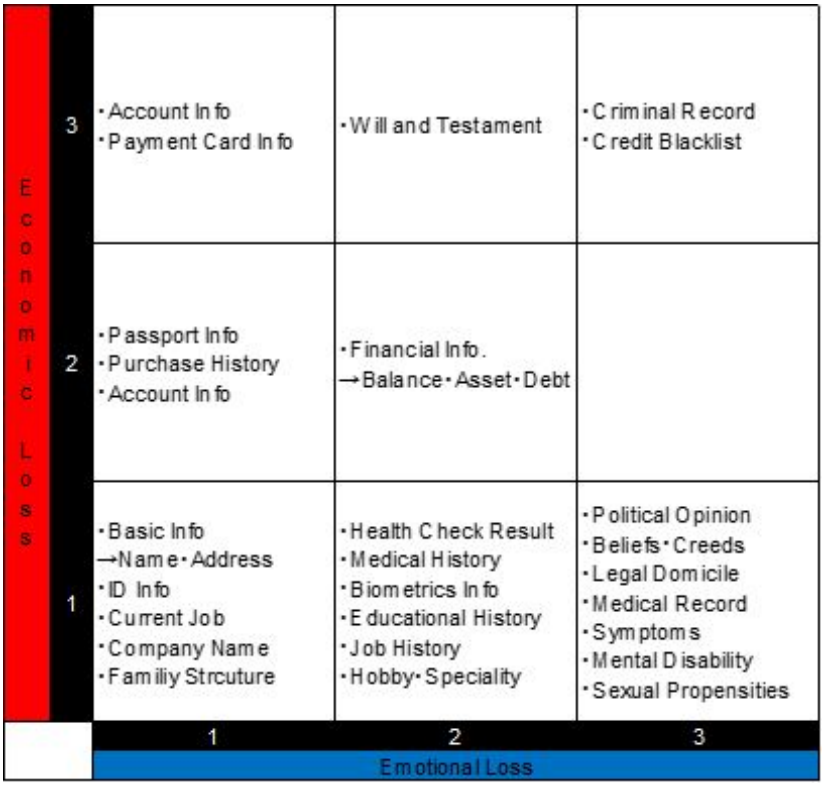

Figure 2: Simple EP Map

In JO model calculation, based on the above classification, the security manager decides the economic distress level and the emotional distress level of leaked information and calculate the value based on the above formula.

3.1.3 Degree of Ease in Identifying the Individual

Third parameter is ”Degree of Ease in Identifying the Individual”. According to the model, if leaked information has name and address, the compensation should be six times because personal identification is easy. Also, if leaked information have address and phone number or only name, the compensation should be triple because personal identification is possible if it takes costs. In another case, compensation fee should not be changed.

3.2 Social Responsibility Degree

The second factor is ”Degree of social responsibility of the organization”. It evaluates the responsibility level of organization, and security manager should choose the level from two; ”Higher than normal” and

”normal”. If organizations are classified into ”Higher than normal”, it is defined that the compensation will be double. Basically, the organizations classified into ”higher than normal” is defined by ”Basic Policies related to the Protection of Personal Information (Cabinet decision April 2, 2004)”, and large companies and public sectors are also included.

3.3 Post Incident Response Appraisal

”Appraisal of post-incident response by the organization” is the final factors in JO model, and it means that the evaluation of attitude after publishing the leakage. If the organization has inadequate responses as incident response, the compensation will be double. In order to simplify the judgment, JO model has qualitative standards of appraisal, such as response speed, the existence of inquiry contact.

3.4 The Application of JO Model

In this paper, the authors have demonstrations of JO models in actual incidents.

3.4.1 Benesse Corporation (Educational Service Provider)

The first case study is the internal fraud in Benesse Corporation, which is a very famous Japanese company as educational service providers. In July 2014, 35.04 million records of personal identifiable information were leaked [2] because a former employee of the outsourcing contractors acquired them without authorization, and he sold this information to mailing list brokers. The leaked information is name, gender, address, birthday, and family structure. Benesse Corporation officially announced that they prepared 20 billion yen as countermeasure budget [21] and sent 500 yen vouchers to all victims. By using JO model, estimated compensation is 24,000 yen for each person, and there is an enormous gap between actual compensation.

Factors	Detailed Parameter	Value	Comments
Leaked Personal Information	Basic information Value	500	-
	Information Sensitivity	2	Based on the definition, X=1 and Y=1
	Personal Identifiability	6	Name + Address are leaked
Social Responsibility Degree	-	2	Large company PrivacyMark are certified by JIPDEC
Post Incident Response Appraisal	-	2	The part of compensation process are criticized

Figure 3: Configured Parameter in Benesse Corporation Incident

3.4.2 JINS Corporation (Eyewear Retails)

Another case study is payment cards leakage in March 2013 by JINS Corporation. JINS Corporation is emerging eyewear retails to sell the product in cheap price. The leaked information included cardholder’s name, PAN (Prime Account Number), expiration date, security code (sometimes called CVV2) [9]. Although 12,036 records were possibly leaked in the first report, final report said that only 2,059 records are leaked[8]. JINS sent the 1,000 yen gift card for 12,036 people as the compensation. Also, JINS defrayed the cost of reissuing payment card. Usually in Japan, reissuing cost was approximately

500 yen. Therefore, the average compensation cost for each person was 1500 yen and total cost of compensation was more than 18 million yen. Also, the cost of transport cost and investigation cost were significant. Especially, in the payment card information leakage, the investigation by a PFI (PCI Forensic Investigator) certified forensic investigator registered by PCI SSC (Payment Card Industry Security Standard Council) is necessary. Therefore, the additional cost was also required. The authors are going to calculate assumed compensation cost by using JO model. The result is 39,000 yen for each person.

Factors	Detailed Parameter	Value	Comments
Leaked Personal Information	Basic information Value	500	-
	Information Sensitivity	26	Based on the definition, X=1 and Y=3
	Personal Identifiability	3	Name is leaked
Social Responsibility Degree	-	1	-
Post Incident Response Appraisal	-	1	-

Figure 4: Configured Parameter in JINS Corporation Incident

This calculated value is useful as a normative example, but there is an enormous gap from actual compensation 1,000 yen and improvement is necessary.

4 Insurance

Recently, the insurance for personal information leakage is available. According to the white paper published by Latham & Watkins [22], insurance is useful as ”last line of defense” against cyber-attacks, and insurance is a workable tool as integrated risk management. Also, Japanese famous insurance companies have started the insurance service for personal identifiable information. As an example, Tokio Marine & Nichido Fire Insurance [12], Sompo Japan Nipponkoa Insurance [6] started this service. Both insurances cover the incident response cost and compensation cost and compensate the part of whole incident costs. Although the insurance only covers particular costs of security incidents and additional analysis. It is effective that each company can make the incident response cost from variable and unpredictable cost to fixed costs.

5 Compensation in Real World

In Japan, there is not clear policy for the response of information leakage when security incidents happened. Also, a personal information protection law protecting personal information does not have actual rules for compensation. Therefore, the compensation should be decided by the court or company’s decision. Sugahara and Harada [20] had a questionnaire research for each company. According to their research, basic personal information such as phone number and purchase history deserve to less than 1000 yen and usually low price.

The authors conducted the study of public information 31 cases from 2002 to 2013, and the authors found that average compensation fee is 3,138 yen. However, the majority are between 500 yen and 1,000 yen (In this graph, more than 10,000 yen are plotted as 10,000 yen). In our research, the only 4 case pays more than 10,000 yen as compensation payment, the compensation is decided in civil court in 2 cases.

TBC (2002)	35,000 yen	[15] (Decided by Court)
JAL Labor Union(2007)	10,000 yen	[5] (Decided by Court)
Mitsubishi UFJ Securities(2009)	10,000 yen	[16]
Alico Japan(2009)	10,000 yen	[17]

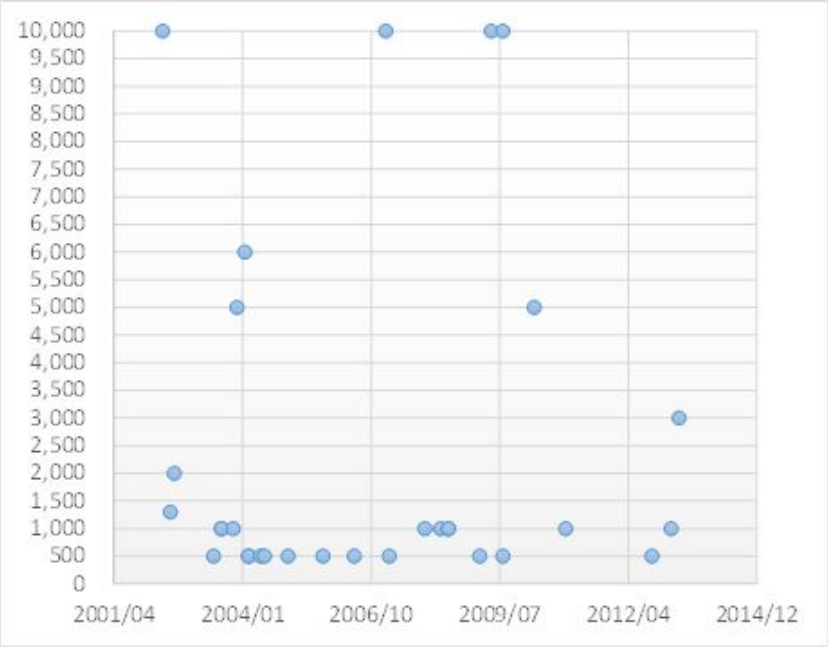

Figure 5: The Map of Compensation Cost

The reason the major compensation is between 500 yen and 1000 yen is that the majority of companies thinks the information leakage of Lawson Cards in 2003 as benchmarks. (The compensation for each person was 500 yen). On the other hands, in the case of civil trial, the compensation fee is higher than usual, such as basic resident register information at Uzi city (1998, 15,000 yen) [15], roster leakage in Waseda university (1998, 5000 yen) [18], data breach in Yahoo!BB (2004, 6000 yen) [15]. In other words, if victims require more than 5,000 yen compensation, sue is necessary.
On top of that, in the above 31 cases, the authors calculate assumed compensation cost from JO model and visualize the gap. (Blue graph is actual compensation cost and orange graph is the calculated model with JO model. In this figure, more than 50,000 yen is plotted as 50,000 yen.)

Above this graph, JO model and actual compensation fee have the huge gap, and in many cases, there are more than double gaps.

6 Considerations

One of the considerations is that the gap between actual compensation and calculated JO model value, even though JO model provides a normative example of compensation. Also, another consideration is the sophistication of the JO model as a normative compensation calculation model. The authors think that the external environment has been changed from 2003 that JO model developed. Especially, in the current case, by using SNS (Social Network Service), personal identifiable information is collectable. By the OSINT (Open Source Intelligence) technique or the diversification of the attack method, the amount

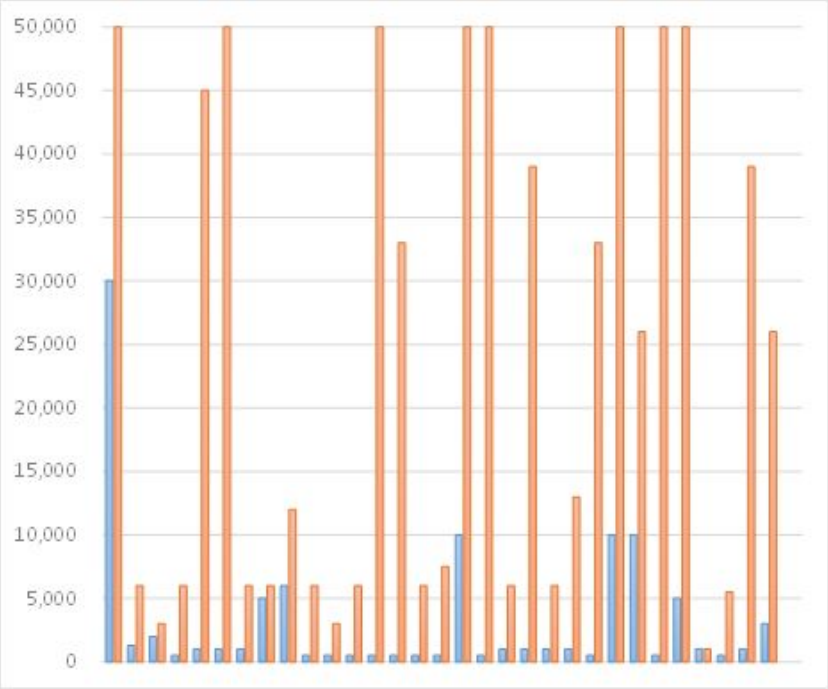

Figure 6: The Gap between actual compensation and JO Model

of personal information in cyberspace and attack technique has been changed. In that perspective, the sophistication is necessary. Especially, the authors point out that following three issues are necessary to improve it.

6.1 Searchability

The first point is ”Searchability”. In the current situation, it is possible to extract personal information from SNS platform. Although the personal information in the SNS is stored based on the free choice of individual, people do not assume that the linkage of stored information in SNS and leaked information. If leaked information have the characteristics of personal identifiable information such as e-mail address, it is easy to link another information. Therefore, by using SNS, there is the possibility that leaked information connected to the photo on SNS.

6.2 Cancelability

The second point is ”cancelability”. For example, although the leakage of password information is very attractive for public, SYK (Something You Know) type authentication [19] information is changeable in the online system. On the contrary, date of birth, address is not changeable even if users would like to change.

6.3 Retrievability

The third issue is ”Retrievability”. In the case that leaked information is posted on PasteBin [14], many people download the data, and it is very hard to retrieve the data. Also, as a lesson from Winny information leakage, it is very hard to retrieve the leaked data in cyberspace [7]. On the contrary, in the case of internal fraud, the majority of motivation is a financial reason, and the leakage is limited such as a

mailing list broker. Since the leaked information is retrieved by public investigation sectors, retrievability is a necessary factor to consider in JO model.

7 Summary

When security information leakage happens, the organizations have to response many perspectives such as public relations, the compensation, and cause investigation. On the contrary, it is very hard to recognize the incident cost and investment costs. Firstly, this paper explains frameworks to plan and simulate the incident response such as ROSI, CyberTab, and JO model. It is a very general idea and provide analytical perspectives. Secondly, this paper analyzes that actual compensation cost is between 500 yen and 1,000 yen. Also, there is at least double group between JO model and actual cost. By this fact, JO model works as a normative indicator for considering compensation, but the example decides actual compensations, especially 2003 Lawson Card incidents (500 yen). Then, the authors point out the improvement points of JO model. Based on the recognition of the change of the external environment from 2003, searchability, cancelability, retrievability should be considered in the future. Moreover, as future work, the authors are going to have the quantitative analysis of the relationship between compensation fee and other factors such as the way of payment, the speed of information disclosure, stock price, and Twitter response. On top of that, the author would like to propose a sophisticated version of JO model.

References

[1] J. J. N. S. Association). 2008 information security incident survey report. http://www.jnsa.org/result/incident/data/2008incident_survey_e_v1.0.pdf, March 2010.

[2] B. Corporation. Report and response regarding leakage of customers' personal information. http://blog.benesse.ne.jp/bh/en/ir_news/m/2014/09/10/uploads/news_20140910_en.pdf, September 2014.

[3] S. Corporation. Assets, threats and vulnerabilities: Discovery and analysis. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Risk_Management.pdf, March 2000.

[4] E. E. U. A. for Network and I. Security). Introduction to return on security investment. http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport, December 2012.

[5] N. Inc. Tokyo district court order the compensation to jal labor union. http://www.nikkei.com/article/DGXNASDG2804F_Y0A021C1CR8000/, October 2010.

[6] S. J. N. I. Inc. Insurance for a business operator handling personal information. http://www.sjnk.co.jp/hinsurance/risk/liability/information/, 2014–2014.

[7] IPA. Faq: File sharing software. http://www.ipa.go.jp/security/anshin/faq/faq-file.html, September 2014.

[8] J. C. Ltd. The final investigation report of illegal access (jins). http://www.jins-jp.com/illegal-access/info.html, May 2013.

[9] J. C. Ltd. The notification of client information leakage by illegal access. http://www.jins-jp.com/illegal-access/info20130315-1600.pdf, March 2013.

[10] N. S. Ltd. Cyber security trend - annual review 2013. http://www.nri-secure.co.jp/news/2013/pdf/cyber_security_trend_report_en.pdf, September 2013.

[11] T. E. I. U. Ltd. Cybertab. https://cybertab.boozallen.com/, April 2014.

[12] T. M. . N. F. I. C. LTD. Private information leakage insurance. http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/, 2006–2014.

[13] N. B. Online. Softbank suffers crushing blow from leakage of customer information. http://business.nikkeibp.co.jp/article/eng/20061213/115608/, March 2004.

[14] PasteBin. Pastebin. http://pastebin.com/, 2002–2014.

[15] I. Pro. The information leakage, with maximum compensation. http://itpro.nikkeibp.co.jp/article/COLUMN/20070215/262166/, February 2007.

[16] I. Pro. Seven billion loss by customer information leakage. http://itpro.nikkeibp.co.jp/article/NEWS/20090909/336929/, September 2009.

[17] I. Pro. "not see" is most dangerous. http://itpro.nikkeibp.co.jp/article/NC/20100702/349899/, July 2010.

[18] I. Pro. The reasoning of compensation in privacy disclosure. http://itpro.nikkeibp.co.jp/article/COLUMN/20110412/359332/, April 2011.

[19] SANS. Ouch! two-factor authentication. http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201211_en.pdf, November 2012.

[20] S. T. and H. Y. A study on the compensation by company/organization when privacy and personal information are compromised - focusing on the money compensation. http://lab.iisec.ac.jp/~harada_lab/lab/2013/20130516.pdf, May 2013.

[21] T. J. Times. Benesse leak suspect held; firm plans compensation. http://www.japantimes.co.jp/news/2014/07/17/national/crime-legal/arrest-warrant-looms-systems-engineer-benesse-data-leak, July 2014.

[22] L. . Watkins. Cyber insurance: A last line of defense when technology fails. http://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage, April 2014.

Author Biography

Tomohisa Ishikawa received the BS in Computer Science from International Christian University in 2009. Then, he is now working at IT security consulting firm as an experienced security consultant. His specializes in penetration testing, incident handling, security training, and global security management. He was an instructor of ASEAN-Japan Security Management Training in 2010, a speaker of SANSFIRE 2011 and 2012. He holds CISSP, CISA, CISM, PCIDSS QSA, Certified Fraud Examiner, GIAC (GPEN, GWAPT, GXPN, GWEB, GSNA, GREM, GCIH). His primary research interests are web application security and incident handling as well as security and privacy problems in Internet.

Kouichi Sakurai is Professor of Department of Computer Science and Communication Engineering, Kyushu University, Japan since 2002. He received B.E., M.E., and D.E. of Mathematics, Applied Mathematics, and Computer Science from Kyushu University in 1982, 1986, and 1993, respectively. He is interested in cryptography and information security.