International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

IT SECURITY IN NATIONAL IDENTIFICATION NUMBER, RISK EVALUATION AT UNIVERSITY

Takeshi Niiyama, Doshisha University Graduate School of Policy and Management, Kyoto, Japan;
Toshiro Kita, Graduate School of Business Doshisha University, Kyoto, Japan

Abstract

National Identification Number called "My Number (MN)" will be effective from Jan 2016 and delivered all resident including foreign people in Japan. It is big challenge for Japan and Japanese to protect this personal information leakage problem. There is a big difference between "MN" and Ex-MN called Resident Registration Code (RRC) "Juki-Net" in Japan. "Juki-Net" is limited availability for only public use. However, "MN" is used for not only public use but also commercial use. It is easily predicable that information leakage incidents would be happened more than the case of "Juki-Net"

In this paper, research at University was focused because many information leakage incidents in USA and Japan were reported and analyzed. It is predicable when "MN" is used at University instead of Student ID, information leakage incidents happened would be increased. Many patterns of attack were clarified. Based on the analysis, risk evaluation for "MN" use case at University was done using risk analysis method. As results, many hints to prevent the incidents were shown and these would be helpful and useful for related people who work at University.

Introduction

"MN" passed by the House of Councilors on May 24th 2013. 12 digit numbers is provided for each citizen. Same number will be used for health insurance, welfare, care insurance, and pension. It will also be used for commercial use after public service release. The one of the most advantage of that it is efficient use for public service using only one managed card. On the other hands, one of the big issues is information leakage of MN. Mainly Ministry of Internal Affairs and Communications (MIC) efforts to execute "MN" service with secure in Japan that "Special Code" is used the interface between each systems instead of "MN". Normally, based on a security policy, system related to "MN" would be constructed with secure to prevent information leakage.

In case "Juki-Net", there was no information leakage on that system since on Nov 2004. It showed that system was very secure [1]. However, security risk was reported even if "Special Code" would be used. [2]

Safe use of "MN" has been discussion in Japan. A recommend necessary solution or countermeasure against information leakage related to "MN" is required.

Related Work

Analysis of information leakage incidents related to Social Security Number (SSN) in the United States, Resident Registration Number (RRN) in Korea, and "Juki-Net" in Japan was done [3]. The report clarified that it was predicable that when "MN" is used for commercial use, information leakage incidents happened would be increased at various places. Simulation model of future commercial use of "MN" was made and it was appeared that three facilities could be security vulnerability. Three facilities were user devices including PC or Smartphone, equipment of commercial company, and equipment of government including server. The risk evaluation was conducted for three parts of facilities using typical risk evaluation method and analysis results of information leakage at other countries outside Japan. Risk management was come up with based on the risk evaluation. Finally recommend necessary solution or countermeasure against information leakage was proposed for government for their public policy. However, more detail simulation and risk evaluation was required.

In this paper, risk evaluation of "MN" at Campus of University should be reported.

Information Leakage incidents at Campus related to SSN in the United States

In 1936 SSN was begun to issue. In my research, information leakage incident has been happened in 2002. At University, 7 incidents (44%) happened. At Company, 8 incidents (50%) happened including 1 incident happened related to FaceBook (SNS) .

University is most dangerous place to give out SSN [4] that is why this paper focuses on University. According to this report, 1st ranking is University, 2nd is Bank, 3rd is hospital, and following Government, Medical Service.

There are a lot of reasons why so many security incidents happened at Campus of University. There is a lot of personal information, however, stakeholder like student or faculty doesn't have enough security knowledge and various services like streaming Video or Music are used by them. [5] Leakage incidents related to SSN at Campus of the University are shown in Table 1.

ISSN:2319-7900

Table 1. SSN leakage incidents at Campus in US

No	Date	Explanation	Name	Type	*
1	2011/11/1	7093 SSN of students who belonged to math course from 2000 to 2005 could be accessed by someone doing Illegal access	Perdue	Lack of preparation	L
2	2011/8/1	75,000 SSN of students could be accessed by hacking using malware	Wisconsin	Hacking	H
3	2011/8/1	43,000 SSN of involved parties could be accessed by Google search for 10 months (Directory traversal)	Yale	Lack of preparation	L
4	2005/2/1	Theft of 30,000 SSN of students and faculties was done by hacking	George Mason	Hacking	M
5	2004/10/1	Theft of 1,400,000 SSN of state people was done by Hacking.	UC Berkeley	Hacking	H
6	2004/6/1	Theft of 145,000 SSN of blood donor in notebook was done at locked car.	UCLA	Theft	L
7	2004/3/1	Theft of about 100,000 SSN of alumni, master course students, and applicants in notebook was done.	UC Berkeley	Theft	L

*** Technical Difficulty * H: High, M: Middle, L: Low**

As Threat Type, it was outstanding that 3 incidents (43%) happened by Hacking, 2 incidents (29%) happened cause of lack of preparation 2 incidents (29%) happened cause of theft of PC etc. Technical difficulty aspect, 3 incidents (43%) happened by using high or middle technology. In information leakage incidents happened by Hacking using high technology. It is indicate that latest counter measure is necessary for latest attack method.

Recent Information Leakage incidents at Campus of University in Japan

In Japan, many security incidents are reported [6] which is shown in Appendix.

In task, there were 12 incidents (40%) in instruction task, 8 incidents (27%) research, 3 incidents (10%) in employment, 2 incidents (7%) in medical care, 2 incidents (7%) in scholarship, 2 incidents (7%) in entrance exam, and 1incidents (3%) in External affairs. 17 incidents (57%) were caused by University staff, 12 incidents (40%) were caused by faculty, and only 1 incident (3%) was caused by student.

It was very differ from prediction before analysis. Prediction was that student caused many security incidents because there are many students in University more than staff and faculty, students have security knowledge less than staff and faculty, students use many various tools like video streaming or music which have sometimes security vulnerability used by malicious people.

Analysis of Rate of Threat Type and Technical Difficulty of the information leakage incident at Campus of University in Japan is shown in Table 2.

Table 2. Rate of Threat Type and Technical Difficulty of the information leakage incident at Campus of University in Japan

	Threat Type					Technical Difficulty		
	Hacking	Theft or Lost	ID Theft	Lack of preparation	Inside malicious person	H	M	L
%	10	40	0	50	0	10	0	90
Frequency	M	H	L	L	L			

In view of threat type, 3 incidents (10%) were caused by Hacking. Based on the analysis of the case of the United States. The ratio of attack caused by Hacking will be increased in the near future. It is indicate that latest counter measure is necessary for latest attack method. On the other hands, 27 incidents (90%) were happened using low technology including Wrong transmission of e-mail, PC Theft, and lack of preparation for leakage. It shows that counter measure to prevent security incident by University is not enough. In security counter measure related "MN", education for related people or simple security implementation or setting is required.

Risk Evaluation for "MN" use at Campus of University in Japan

In this research, evaluation method of ISMS (Information Security Management System, (ISO/IEC 27001)) was used.

In ISMS, risk is represented using multiplication. Risk equals assets multiply threats multiply vulnerability.

Risk = Assets * threat * Vulnerability

Just example of risk evaluation score table is shown below.

Based on analysis of information leakage incidents at campus of University in Japan (Appendix), Score depended on the level of technical difficulty is shown in Table 3. For in-

stance, Hacking is caused by high level technique, therefore, it is difficulty for malicious people to do that and score is 1.

Table 3. Level of Technical Difficulty

Level	Explanation	Score
H	- Hacking, - APT (Advanced Persistent Threat)	1
M	- ID Theft. However, it is caused by inside malicious person or criminal organization	2
L	- ID Theft, Voice imitation, easily access using web, and Various memory device like PC, Hard Desk, and USB, - lack of preparation for leakage	3

Based on analysis of information leakage incidents at campus of University in Japan (Appendix), Score depended on the level of frequency is shown in Table 4. For instance, theft and lost were happened very frequently, therefore, score is 3.

Table 4. Level of Technical Difficulty

Frequency	Explanation	Score
H	- Theft / Lost - Lack of preparation	3
M	- Hacking	2
L	- ID Theft - Inside malicious people	1

System in University is created for each task. For example, Systems for each task of Doshisha University in Kyoto are listed in Table 5.

Table 5. Systems for each task of Doshisha University

Category	Task	Explanation
Student	Entrance exam	Admission decision, acceptance letter, statistic analysis document
	Academic fee	Demand, Payment management
	Instruction	Student and Subject Registration management, Class management, GPA management, Course support
	Medical Care	Data management of medical check, Making statistic data of medical check
	Certificate issuing	Instruction and Medical care
	Employment	Management of Company information and Student information. Making statistic data of employment
	Scholarship	Selection of scholarship, Management of Scholarships return
	Course / Research	Course	Syllabus including CD-ROM, Bulletin board of class information (Lecture cancellation)
		Research	Attending conference, Submit research paper
		Researcher	Researcher information
		Intellectual property	Management of intellectual property
	Management Information	External affairs	Work with another organization (Government, Commercial company or other universities, Document publication
		Finance	Budget management (daily and monthly), Bank account management, Order shipment Management, Accounting
		Research funding	Acceptance of research fund, Execution management, Report
		Human resource, Payroll	Service management, Approval human resource assignment (including albeit), Payroll (including tax calculation), welfare, Statistic data of Human resource
	Academic information	Library search, Academic information search, Portal site Management, Circulation, computerized book and document, Bulletin production

Based on analysis of information leakage incidents at campus of University in Japan (Appendix), most security incidents were happened in instruction or research as task.

According to the risk evaluation method, risk evaluation instruction and research as task related to student, staff, and faculty was done in this paper and the results are shown in Table 6.

Table 6. Risk Evaluation of the task related to instruction or research

Threat	Score	Vulnerability	Score	Risk Evaluation
"MN" can be known by staff and faculty when the number is printed on the card.	1	It is easy for malicious people look at the card	3	3
If "MN" is leakage, malicious people can access to other services.	1	"MN" is managed with no security. Ex) "MN is put the desk with stick note.	2	2
Wrong transmission of e-mail including "MN" is happened by staff	3	- No solution is implemented against wrong transmission of e-mail- No education for staff how to use e-mail or	3	9

ISSN:2319-7900

		security awareness		
In task related to scholarship, after malicious people know the "MN" and password, they can log in to the bank account and steal the money.	2	If staff of the University is malicious people, "MN" can be know easily.	1	2
Print out some document including "MN" and the document is left on the printer or somewhere at campus.	1	Lack of security awareness of staff and faculty	2	2
USB Memory, PC, and HDD including "MN" are theft or lost	3	Lack of security awareness of staff and faculty Malicious people can steal USB Memory, PC, and HDD easily	3	9
Setting of Access control of NAS was wrong and MN can be opened to the Internet	2	Lack of security awareness of staff and faculty	3	6

Score of "Wrong transmission of e-mail including "MN" is 9. E-mail is one of frequency tool among student, staff and faculty.

Based on analysis of information leakage incidents at campus of University in Japan (Appendix), ratio of information leakage related to e-mail transaction is 16% (5 incidents) as high. Wrong transmission of e-mail was happened because of human error. Therefore, there is no technical difficulty. It is very important for University people to implement service to stop wrong transmission of e-mail and have security education.

Score of "USB Memory, PC, and HDD including "My number" are theft or lost" is 9 as same as above. Based on analysis of information leakage incidents at campus of University in Japan (Appendix), many incidents were happened at conference oversea. More awareness is needed over sea than in Japan. University should have security policy that USB Memory, PC, and HDD with no including "My number" Strict rule is needed for them to keep rule.

Score of "Setting of Access control of NAS was wrong and MN can be opened to the Internet" is 6. University should have security policy that such a kind of equipment can't be connected to the internal network of University or if University permits to connect, a strict security policy should be established.

Conclusion and Future work

In this paper, risk evaluation of "MN" use at campus of University was done using actual task related to instruction and research by staff, and faculty in Doshisha University.

Based on analysis of information leakage incidents at campus of University in Japan (Appendix), there were at least 30 number of incidents happened from Sep 2013 to Jan 2015.

Only 3% (1 incident) of all incidents was caused by student. However, 57% (17incidents) of all incidents was caused by staff and 40% (12incidents) was caused by faculty

In view point of task, 40% (12incidents) of all incidents was caused in task of instruction and 27% (8incidents) of all incidents was caused in task of research.

Score of "Wrong transmission of e-mail including "MN" or "USB Memory, PC, and HDD including "My number" is same 9. Both are the biggest security holes. Countermeasure against two big security holes should be prepared. This paper is the first trial to evaluate the risk of "MN" use at campus of University. It will be helpful and useful for future research for security issue related to "MN" use.

In near future, other security evaluation related to another task should be done. In addition, same risk evaluation method would be adopted for other industries. Finally, based on the results, public policy will be proposed for government.

Acknowledgments

The authors are thankful to IJACT Journal for the support to develop this document.

The author would like to acknowledge the support by the Grants-in-Aid for Scientific Research (C) by Japan Society of the Promotion of Science and the Japan Securities Scholarship Foundation.

References

[1] Toshiro Kita, "Electronic government in Japan, Towards harmony between technology solutions and administrative systems" in Recovering from success innovation and technology management in Japan edited by D. Hugh Whittaker, Robert E. Cole, pp.286-297 Oxford University Press, 2006

[2] Hiromitsu Takagi, "Toward the better design of a national identification number and its utilization system" Information Processing Society of Japan Technical Report, pp. 1–8, Vol.2013-CSEC-61, No.29, 2013

[3] Takeshi Niiyama, "Information Security in National Identification Number - Called My Number in Japan" International Conference on Business Innovation and Technology Management, pp. 290–326, Oct 2014

[4] McAfee report 2010 Top Ten Most Dangerous Places to Leave Your Social Security Number http://robertsiciliano.com/blog/2010/10/18/mcafee-reveals-the-top-ten-most-dangerous-places-to-leave-your-social-security-number/
[5] Alicia Anderson, "Effective Management of Information Security and Privacy", EDUCAUSE, pp. 15–20, Jan 2006
[6] Information leakage incidents in Japan http://www.security-next.com/053330
[7] ISMS http://www.isms.jipdec.or.jp/english/index.html

Appendix

No	Date	Explanation	University Name	Type	*	Task	Person
1	2015/1	USB Memory including 39 student personal information was lost in Malaysia for business trip	Osaka City	Lost (oversea)	L	Research	Faculty
2	2015/1	Roentgen files of 9336 students was lost after medical check in 2013	Keio	Lost	L	Medical	Staff
3	2014/12	ID/PWs were taken	Doshisha	Phishing mail.	H	Instruction	Student
4	2014/12	USB Memory including 17 personal information related to hiring for faculty was lost	Miyazaki	Lost (oversea)	L	Employment	Staff
5	2014/12	Administrative document including personal information was made mistake to publish	Niigata College of Nursing	Lack of Preparation	L	External affairs	Staff
6	2014/11	Network Attached Storage (NAS) with no password was opened to the Internet	Akita	Lack of Preparation	L	Instruction	Faculty
7	2014/10	Wrong transmission of e-mail including 2634 students personal information for 105 albite	Ryukoku	Lack of Preparation	L	Instruction	Staff
8	2014/10	HDD including 277 students personal information was theft in Spain.	Osaka City	Theft (oversea)	L	Instruction	Faculty
9	2014/9	PC including personal information of whom faculty's students	Sophia	Theft (oversea)	L	Instruction	Faculty
10	2014/9	PC including personal information of students, almni, and researcher in Sweden	Kyushu	Theft (oversea)	L	Instruction	Faculty
11	2014/6	Wrong transmission of e-mail including 172 students personal information for 181 of applicant of scholarship	Yokohama City	Lack of Preparation	L	Scholarship	Staff

ISSN:2319-7900

12	2014/5	USB Memory including 58 personal information visiting to medical room was lost	Hiroshima	Lost (oversea)	L	Medical	Staff
13	2014/4	HDD including 47,000 personal information was opened to the Internet because of poor security setting.	Chiba	Lack of Preparation	L	Instruction	Faculty
14	2014/3	Wrong transmission of e-mail including 20 students personal information for 1824 of applicant of scholarship	Meiji Pharmaceutical	Lack of Preparation	L	Instruction	Staff
15	2014/3	A Server including 356 personal information was opened to the Internet because of poor security setting.	Nagoya graduated school	Lack of Preparation	L	Instruction	Faculty
16	2014/3	USB Memory including 40 personal information room was lost	Osaka Women's Junior College	Lost	L	Instruction	Faculty
17	2014/2	NAS including 450 personal information was opened to the Internet because of poor setting access control	Tsukuba	Lack of Preparation	L	Instruction	Staff
18	2014/1	Wrong transmission of e-mail including 77 students personal information for 277	Fukuoka	Lack of Preparation	L	Instruction	Staff
19	2014/1	PC including 2264 personal information by car break in	Hyogo Health Sciences	Theft	L	Instruction	Faculty
20	2013/12	A server including personal information was illegal access	Shinshu	Hacking	H	Employment	Staff
21	2013/12	Application form for University including personal information was lost	Hiroshima	Lost	L	Entrance exam	Staff
22	2013/11	USB Memory including 273 personal information room was lost	Shitennoji	Lost	L	Instruction	Faculty
23	2013/11	13 lists of scholarship application was put on a public place in campus	Tokyo	Lack of Preparation	L	Scholarship	Staff
24	2013/11	Two digital combined machine including 115 personal information were opened to the Internet	Tokyo	Lack of Preparation	L	Instruction	Staff
25	2013/10	USB Memory including 200 personal information room was lost	Taisho	Lost	L	Instruction	Faculty
26	2013/10	A server including personal information was illegal access	Seiwa	Hacking	H	Employment	Staff
27	2013/10	Presentation material 12 including personal information was taken public at academic conference	Tokyo Medical and Dental	Lack of Preparation	L	Research	Faculty
28	2013/10	Wrong transmission of e-mail including 339 personal information	Tokyo graduated	Lack of Preparation	L	Instruction	Staff
29	2013/10	Answer sheet of employment exam was lost	Aeronautical Safety College	Lack of Preparation	L	Entrance exam	Staff
30	2013/9	Wrong transmission of e-mail including 141 personal information	Nagoya	Lack of Preparation	L	Instruction	Staff

*** Technical Difficulty H: High, M: Middle, L: Low**

ISSN:2319-7900

Biographies

TAKESHI NIIYAMA received the B.S. degree in Faculty of Engineering, Department of Molecular Science and Technology Organic Chemistry from the Doshisha University, Kyoto, Japan, in 1997, the M.S. degree in Faculty of Engineering, Department of Molecular Science and Technology Organic Chemistry from the Doshisha University, Kyoto, Japan, in 1999, the M.S. degree in Master of Science information Technology Information Security (MS-IT IS) from the Carnegie Mellon University Graduated School, Pittsburgh, United States

TOSHIRO KITA received the B.S. degree in Electronic-Mechanical Engineering from the Nagoya University, Nagoya, Japan, in 1974, the M.S. degree in Electronic-Mechanical Engineering from the Nagoya University, Nagoya, Japan, in 1976, the Ph.D. degree in Electronic-Mechanical Engineering from Nagoya University, Nagoya, Japan