Installation of Security Policy into Kumamoto University and DNS based Detection of Security Incidents in the Campus Network

Yasuo Musashi[†]

Abstract: In Kumamoto University, we created policies and standards through August 2001 to February 2003, and procedures through March 2003 to March 2004 for the campus information security policy. Afterward, the information security policy was officially installed into the university and it has been taken effect since September 2004. On the other hand, we can be keeping to detect efficiently the security incidents in the campus network system by only watching the domain name resolution traffic since 2004 and can easily take various incident responses. This is because the security policy had been already installed in 2004, we can easily implement the prototype detection system, we can get friendly support from the users of the campus network. We can report how to smoothly install a security policy into a national university corporation and how to use the security policy efficiently to take countermeasures to fix the security incidents in the campus network system.

Keywords: Security Policy, DNS based detection

1. Introduction

It is of considerable importance to pick up a topic that in September, 2005, the National Information Security Center (NICT) indicated the united standards of information security for the governmental organizations (USISGO).[1]

Subsequently, the National Institute of Informatics (NII) and Institute of Electronics, Information and Communication Engineerings (IEICE) worked out a set of sample rules for information security countermeasures in the higher educational organizations (SRISCHEO) with modification of the USISGO or addition of the university requirements.[2]

Recently, on the other hand, several universities are trying to install the information security management systems (ISMS: ISO27001) into their campus information systems.[3]

In Kumamoto University, we have already installed the information security policy into the university campus information systems in September, 2004.[4] Simultaneously, we started to develop and implement the DNS based detection system for the security incidents in the campus network like an internet worm (IW) like W32/Netsky.Q or W32/Mydoom.A mass mailing worm (MMW) infection,[5] or W32/Sasser.D service attack worm (SAW) infection.[6] In this paper, (1) we can introduce how the information security policy into the campus information systems in the Kumamoto University, and (2) the DNS based detection systems in the campus network.

2. Security Policy in University

2.1 Correspondence to United Standards of Information Security for Governmental Organizations

Currently, in Kumamoto University, we have read the USISGO and found it very nice because its structure is very compactly formed and it seems to be almost finished.

In October, 2007, the information security policy working groups of the NII and the IEICE finally published a sample rule book for information security countermeasures in the higher educational organizations (SRISCHEO).

At first, the sample rule book had only 298 pages, however, surprisingly, the book takes 594 pages. This means that we can hardly to read it completely. In Kumamoto University, we are

[†]Center for Multimedia and Information Technologies, Kumamoto University.

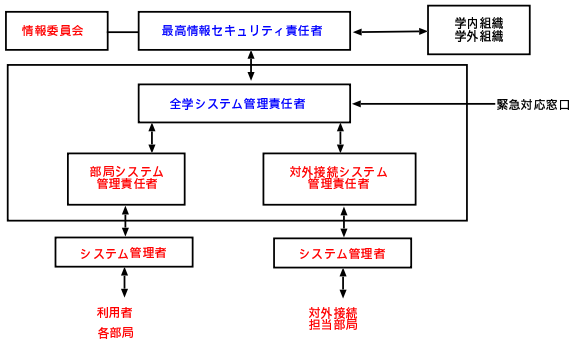

Figure 1. Information security policy and organization.

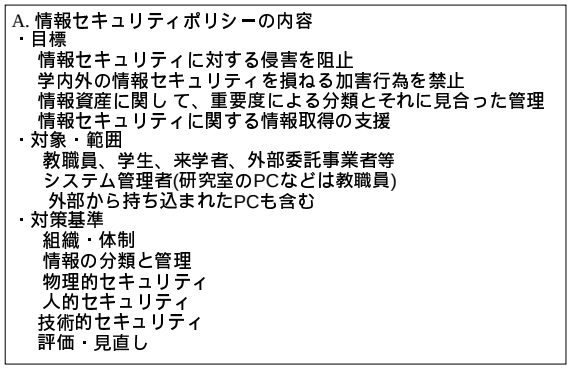

Figure 2. Contents in the information security.

sharing to read and check the book. This is because, currently, we believe that this sample rule book can contribute to develop uncostly or install easily information security policy into the universities.

Recently, Kyoto University has successfully (or not) installed the sample rules book based security policy into the campus information and network systems.[7]

On the other hand, several universities have already partially got an ISO27001 as an ISMS and they are also trying to scale up it *i.e.* they believe that the ISMS should be totally installed to the university.[8]

Especially, Shizuoka University Information Processing Center (SUIPC) has not only got successfully ISO27001 but also has been trying a strategic SaaS to realize a Green IT and to establish or work out a business continuity plan (BCP)/business continuity management (BCM).[3] We should pay much attention to such activity.

2.2 Installation of Security Policy into Kumamoto University

In Kumamoto University, we created a campus information security policy and standards through August, 2001 to February, 2003, and procedures through March, 2003 to March 2004 for the campus information security policy.

When we worked out a proposal for the information security policy and standards, we referred to the document for a way of thinking of the information security policy in the university.[9]

Expectedly, the proposal was unanimously approved by the upper committee and its executive working group for the campus IT promotion activity. The approved policy and standards consist of members and documents shown in Figures 1 and 2, respectively.

Fortunately, we successfully created the security policies and standards for the campus information security policy, however, in the other university, we had got informations that they could be unfortunately unaccepted their proposals like policies, standards, and procedures.

From this situation, we thought that in the next stage, we could not so easily to get a committee's approval to a proposal for procedures. The procedure can be a manual for execution of the policies and the standards is only like a constitution so that the procedures can affect all the members in the university *i.e.* it seems to be harmful at that time. Probably, this situation is unfavorable for us. Especially, if the document is enriched by a lot of pages, it is predicted that the proposal would be difficult to be accepted.

Taking into this kind of information, we dared to challenge to suggest a proposal for procedures ignoring whether or not the proposal document was formed by a lot of pages.

Expectedly, we got a strong opposition, especially, the present author had directly got scornfully a lot of critical and severe comments for the proposal. The proposed document took 57 pages.

Therefore, we started to discuss about on the fixation of the proposed procedures through January

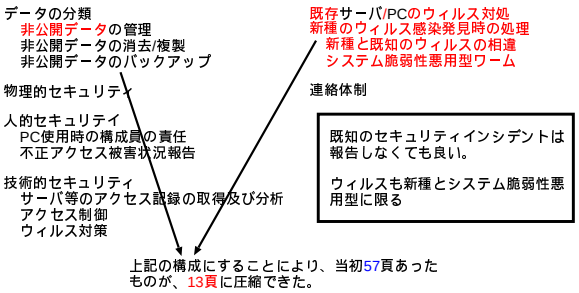

Figure 3. Reduction of pages in the procedures.

to March, 2004 by employing on-line E-mail discussion. This is because we had a strategy for coming out well: (1) The E-mail discussion is slightly verbose but it can give traceability to all the previous informations *i.e.* we can replay all the opinion. (2) We can also easily retrieve very important committees opinions as quickly as possible. And (3) we can quickly response to a important key person who was a tough opponent. Anyway, if we could get approval from the committee members, we could finish working out the campus information security policy.

When watching the 57 paged document of the procedures, the author started to feel to need a security model for contracting or decreasing total pages of the previously proposed procedures. In the document, we found several data asset categorization models to be shrunk. Finally, we reached a simple bipolar model to be public data and secret data. We had an idea that the information data can be mainly divide into two type typical models. And we guess that the simple bipolar models can be easily acceptable for the members of the university. In Japan, we had a lot of information leakages through 2003 to 2004.

After employing this bipolar models, the procedures document was drastically decreased from 57 pages into 13 pages. This bipolar model is shown as follows:

- public data:
  No or lower risk by security incidents like information leakages
- secret data:
  Very important confidential data including personal information.

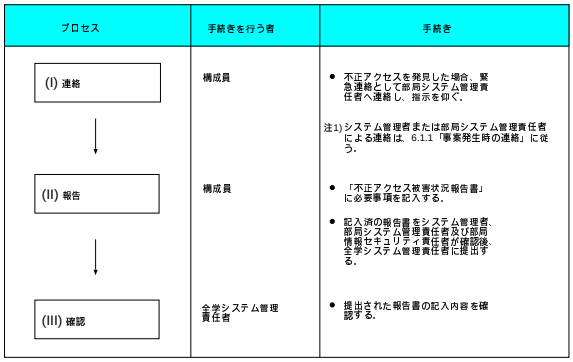

Figure 10. Reporting new security incidents

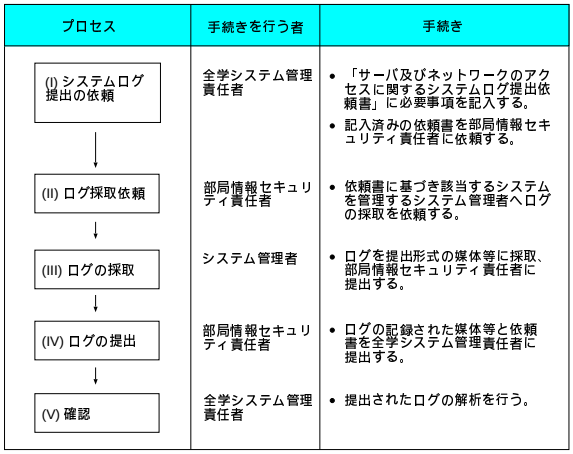

Figure 5. Acquisition system log messages and forensics.

Also, the bipolar model has a merit because we can handle the security policy by only defining the secret data. Afterwards, we created a new proposal and transmitted the new idea to all the committee members.

Expectedly, this idea and proposal was smoothly accepted and the working group is finished.

2.3 Kumamoto University Security Policy and Strategy

We strategically implemented three ideas in the campus security policy procedures: (1) The professors in the Center for Multimedia and Information Technologies (CMIT) can claim the syslog messages of the campus information or network servers relating to the security incidents in the campus information systems and network (Figure 4). (2) The campus members should report when they find new

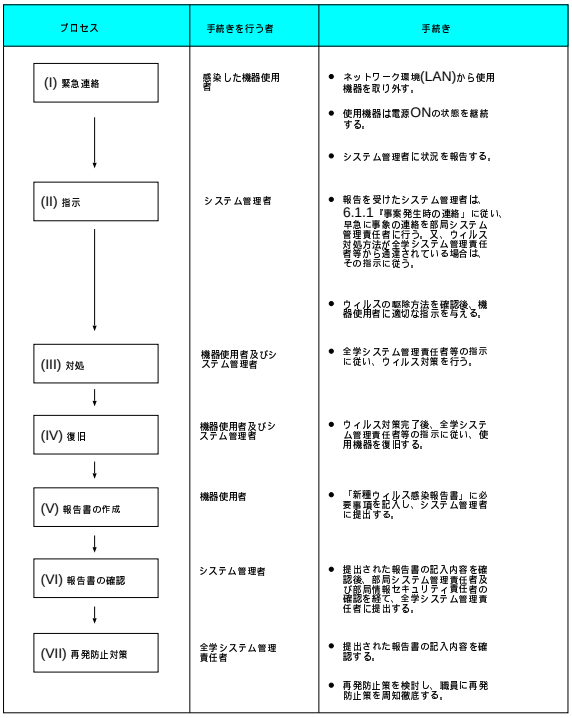

Figure 6. Reporting new virus/worms infections.

security incidents or a large scaled security problems, to professors or staffs in the CMIT (Figure 5). (3) The campus members should also report in details about when they found new virus infections (Figure 6).

3. DNS based Detection of Security Incidents in the Campus Network

After working out the campus information security policy, we started to develop several DNS based detection technologies of security incidents in the campus network, like a virus/worm infection activity, or bot activity, especially, random spam bot (RSB), a targeted denial of service (DoS) attack against the DNS cache server, and the host search (HS) activity from the Internet.

3.1 DNS based detection

Firstly, we can briefly explain on the DNS based detection system. The DNS based detection watches only the DNS query request packet traffic between the DNS cache server and the DNS client

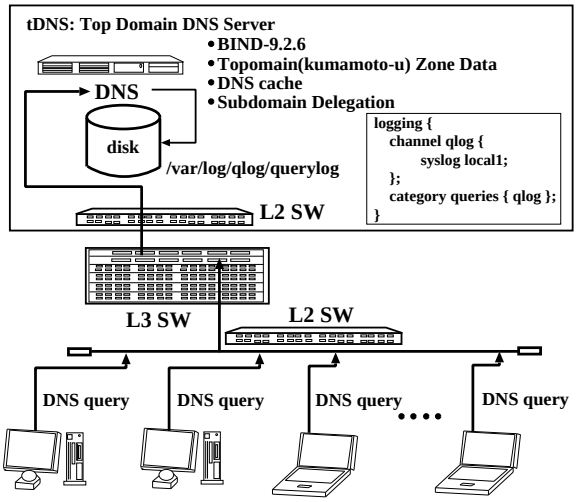

Figure 7. The observed network system.

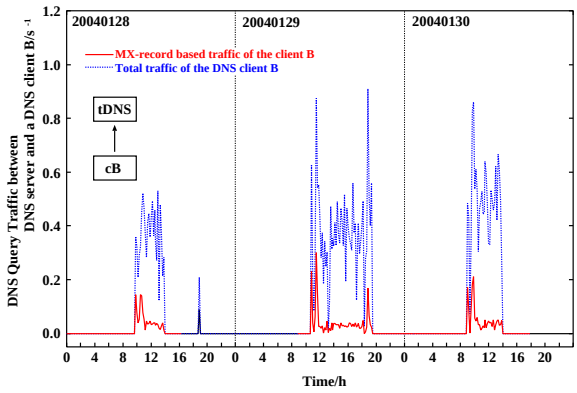

Figure 8. Traffic of the DNS query access between the top domain DNS server and the DNS client B through January 28th to 30th, 2004. The dotted line shows the total DNS traffic and the solid line indicates the MX-record based DNS traffic (s^{-1} unit).

hosts like servers and PC terminals. The E-mail server, for example, send a lot of DNS resolution traffic including the A, PTR, and MX RR based DNS query request packet traffic.

Usually, the normal PC hosts transmit only the A RR based DNS query request packet traffic generated by the Web browser. However, the MMW infected PC can send the A and MX RR based DNS query request packet traffic. This is because the MMW infected PC has a built-in SMTP engine that directly sends the E-mail including the worm as an attachment file.

But, interestingly, we can find no PTR RR based DNS query request packets in the DNS resolution traffic from the MMW infected PC hosts.

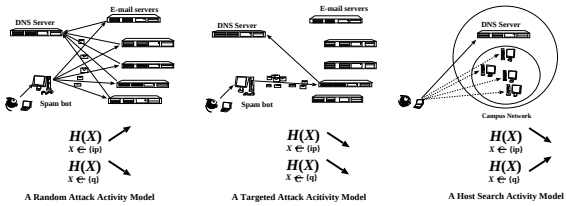

Figure 9. RSB(random spam bots), TSB(targeted spam bots), and HS(host searches) activity models.

From this result, we can detect the MMW infected PC hosts by checking whether or not the DNS resolution traffic includes the MX RR based DNS query request packets but no PTR RR based DNS query one.

3.2 Detection of Random Spam Bots and Host Search Activity

Currently, we started to develop detection of a random spam bot (RSB) and a host search (HS) activity models.

Recently, we noticed that the unique source IP address- and the unique DNS query keyword based entropies changed in three patterns shown in Figure 9.

We illustrate the calculated unique source IP address and unique DNS query keyword based entropies for the PTR resource records (RRs) based DNS query request packet traffic from the Internet to the top domain DNS (**tDNS**) server through January 1st to December 31st, as shown in Figure 10.

As shown in Figure 10, we can observe thirty seven peaks and they can be categorized into three groups, as: {(1)-(4), (6)-(11), (14), (16), (18)-(19), (21)-(22), (25)-(30), (32)-(35)}, {(5), (12)-(13), (15), (17), (20), (31), (36)-(37)}, and {(23), (24)} in which the first, the second, and the last groups take twenty six, nine, and two peaks, respectively.

In the first peak group, all the peaks show an increase in the unique source IP address based entropy and a decrease in the unique DNS query keyword based one, showing the RSB activity.

In the peak (3), (4), (6), and (7), for instance,

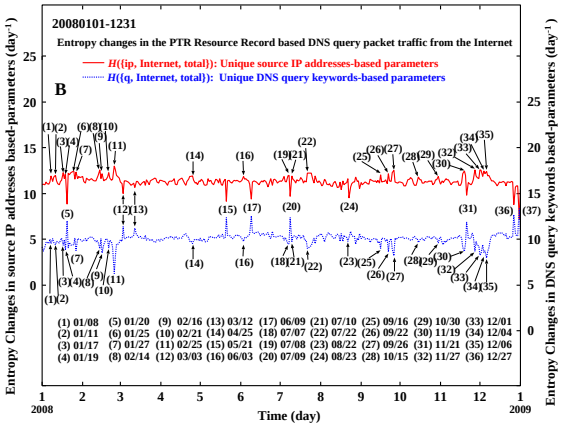

Figure 10. Entropy changes in the total PTR resource record (RR) based DNS query request packet traffic from the Internet to the top domain DNS (**tDNS**) server through January 1st to December 31st, 2008. The solid and dotted lines show the unique source IP addresses and unique DNS query keywords based entropies, respectively (day^{-1} unit).

we investigated the detected PC hosts which are PC room terminals and administrated by a computer center, however, no evidence can be directly found in the PC hosts. Fortunately, we successfully interviewed an account holder and finally, we detected an *auto.inf* file, a Win32/Agent.BUL Trojan Horse (TH), in the USB stick type disk storage for the account holder. In the peak (16), we detected the IP address for a broadband router in the campus laboratory in which there were three Windows XP PCs. We investigated all the PCs by the typical anti-virus software but no virus infection could be found. Then, we checked the SMTP activity in the PC by executing a netstat command on the DOS window and we could detected a lot of SMTP connections. Therefore, we could conclude that the PC hosts was hijacked to be a random spam bot (RSB).

In the second peak group, nine peaks can be found. The unique source IP addresses based entropy decreases while the unique DNS query keywords based one increases. This feature indicates the host search (HS) activity. It is very important to detect the HS activity because the HS activity is mainly performed as pre-investigation on the campus network for the next cyber attack.

In the last peak group, we can observe two peaks (23) and (24). The peaks can be assigned to Au-

gust 22nd and 23rd, 2008, respectively. This is because we had a half-day blackout through August 22nd to 23rd, 2008, because of inspection of electrical defects, affecting the entropy changes.

4. Conclusions

We reported how to smoothly install a security policy into a national university corporation and how to use the security policy efficiently to take countermeasures to fix the security incidents in the campus network system.

In Kumamoto University, we created policies and standards through August 2001 to February 2003, and procedures through March 2003 to March 2004 for the campus information security policy. Subsequently, the information security policy has been taken effect since September 2004.

Since the security policy had been already installed in 2004, we can easily implement the prototype detection system, we can get friendly support from the users of the campus network.

From this reason, on the other hand, we can be keeping to detect efficiently the security incidents in the campus network by observing the DNS query request packet traffic since 2004 and can also easily take various incident responses.

Acknowledgement

All the studies were carried out in CMIT of Kumamoto University. We thank all the members of Kumamoto University.

References and Notes

1) 政府機関統一基準について:
http://www.nisc.go.jp/conference/seisaku/dai2/pdf/2siryou03.pdf

2) 高等教育機関の情報セキュリティ対策のためのサンプル規定集:
http://www.nii.ac.jp/csi/sp/
http://www.nii.ac.jp/csi/sp/doc/sp-sample-fy2007.pdf

3) 長谷川・伊藤・井上・八巻，実践 ISMS 講座，静岡学術出版，ISBN-978-4-903859-08-8

4) 武蔵，熊本大学における情報セキュリティポリシーの策定事例，文部科学省・平成 16 年度情報セキュリティセミナー:
http://www.nii.ac.jp/hrd/ja/security/h16sec_seminar.html

5) (a) Musashi, Y., and Rannenberg, K. : Detection of Mass Mailing Worm-infected PC terminals by Observing DNS Query Access, *IPSJ SIG Technical Reports, Computer Security 27th (CSEC27),*, Vol. 2004, No.129, pp.39-44 (2004). (b) Musashi, Y., Matusba, R. and Sugitani, K., Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners *Proceedings for the 3rd International Conference on Emerging Telecommunications Technologies and Applicatications (ICETA2004),* Košice, Slovakia, 2004, pp.233-237. (c) Matsuba, R., Musashi, Y., and Sugitani, K. : Detection of Mass Mailing Worm-infected IP address by Analysis of DNS Server Syslog, *IPSJ SIG Technical Reports, Distributed System and Mangement 32nd (DSM32)*, Vol. 2004, No.37, pp.67-72 (2004).

6) Musashi, Y., Matsuba, R., Sugitani, K., and Moriyama, T. : Workaround for Welchia and Sasser Internet Worms in Kumamoto University, *Journal for Academic Computing and Networking*, Vol. 8, No.1, pp.5-8 (2004).

7) 岡部，情報セキュリティポリシー（対策）を浸透させるには，文部科学省 平成 20 年度情報セキュリティセミナー
http://www.nii.ac.jp/csi/upki/secsem/2009/secsem2009/seminar_02.pdf

8) 第 3 回国立大学法人情報系センター ISMS 研究会
http://www.cc.yamaguchi-u.ac.jp/osirase/isms_ com.phtml

9) 大学における情報セキュリティポリシーの考え方
http://www.nii.ac.jp/csi/sp/doc/toshin2001.pdf