

Study Group on Next-Generation Information Security Policies—2nd Meeting

Summary of Minutes

1. Date and Time

Wednesday, December 5, 2007; 10:00–12:00

2. Location

Special Conference Room 4, Mita Kaigisho

3. Attendees (honorifics omitted)

1) Study Group Members (in order of Japanese alphabet)

Yu Arai (LAC Co., Ltd.), Koichi Arimura (Telecom-ISAC Japan), Yasuo Ayazuka (NTT DoCoMo), Hisao Iizuka (NEC BIGLOBE, Ltd.), Takashi Suga (Mitsubishi Electric Corporation), Takashi Kimura (NIFTY), Shingo Koya (Trend Micro Incorporated), Satoru Koyama (NTTPC Communications Inc), Mamoru Saito (Internet Initiative Japan Inc.), Masahiro Sata (WILLCOM, Inc.), Yoichi Shinoda (Japan Advanced Institute of Science and Technology), Masahiro Shimomura (Japan Network Security Association), Satoru Tezuka (Hitachi, Ltd.), Hirofumi Tokuda (IBM Japan, Ltd.), Koji Nakao (KDDI Corporation), Masaya Norifusa (NEC Corporation), Michikazu Fukuchi (SOFTBANK BB Corp), Toshiro Fujii (Matsushita Electric Industrial Co., Ltd.), Ichiro Mizukoshi (Nippon Telegraph and Telephone East Corporation), Hiroshi Yasuda (Tokyo Denki University), Suguru Yamaguchi (Nara Institute of Science and Technology), Masashi Yamauchi (Symantec Japan Research Institute, Inc.), Takahiro Yokota (KDDI Corporation)

(2) Secretariat

Nakata (Director-General for Policy Planning), Matsui (Deputy Director-General), Yanagishima (Director for Policy Planning, Computer Communications Division), Kawauchi (Director, IT Security Office), Murakami (Deputy Director, IT Security Office), Tanabe (Security Measures Chief, IT Security Office)

4. Agenda

(1) Opening

(2) Agenda

(i) Threats to and issues in information security

(ii) Direction and organization of study group discussions

(iii) General discussion

(3) Others

(4) Closing

5. Summary of meeting

(1) Opening

Nakata, who was absent from the last meeting due to business obligations, made a short speech.

The Secretariat reviewed the minutes of the 1st meeting.

(2) Agenda

(i) Threats to and issues in information security

a. Recent security trends (Yamauchi)

Yamauchi gave an explanation based on Document 2-2.

Summary of the question-and-answer session

- What do you think of risk evaluations?

→ Risk evaluation is the process of quantifying how much impact a range of threats would have on assets if they were to eventuate. It involves subjective concepts such as probability of occurrence and amount of damage. Then, considering the amount of resources that can be allocated to address the problem, the risks are prioritized. Every company faces some risks; how well they are addressing the potential risks is important.

- Regarding the “Global Intelligent Network” on page 19, what is the relationship with other organizations and how the networks are protected?

→ We are exchanging information with public organizations, such as CERT, that are collecting vulnerability information. We are also discussing the technology for analyzing the information with members of other communities. We have divided the network into several zones with different levels of protective measures. Once a personal computer is brought into the deepest zone, its disk is completely destroyed before the computer is taken back outside the zone.

b. Current situation regarding malware (Arai)

Arai gave an explanation based on Document 2-3.

Summary of the question-and-answer session

- A proposal on page 18 refers to ISPs as the leading players. What are your expectations of

them?

→ Some personal blog services provided by ISPs are included on the blacklist. We also have to take a look at this.

- A breakdown of computer viruses that have been successfully collected is given on pages 5 and 6. What are the specific behaviors of those described as “UNKNOWN”?

→ Most of them are “downloaders.” Downloaders are simple malware that download viruses. Software that makes it easy to create downloaders can be bought. Because many downloaders have been created with such software, we have a series of “UNKOWN” items.

- There is a description of code-signed malware on page 19. How could they do such a thing?

→ They established a dummy company and acquired a certificate via the proper procedures. This is what is happening in the world of personal computers. I assume that the same thing will be done with smart phones.

- If what is finally downloaded is conventional malware, it can be addressed with anti-malware. Therefore, I think we should emphasize the role of the “information security product vendors.”

→ There are various measures. You have referred to one of them.

c. Next-generation information security measures (Koyama)

Koyama gave an explanation based on Document 2-4.

Summary of the question-and-answer session

- One thing we agree on is that it is necessary to collect and analyze a wide range of information on risks. Are there any specific plans on how to do this?

→ How about starting with establishing a partnership between database creators, gathering related information into one place, analyzing the data and coming up with ideas?

- Do you mean to reflect the contents of the reputation database in the DNS of each company and operate the DNS to redirect access?

→ We haven't thought of specific methods but I think the method you describe would be effective.

- Creating a blacklist and using filters works for a short time, but I don't think it is a fundamental solution.

→ We think it is necessary to take measures that address both the symptoms and the underlying cause.

Along with activities to raise awareness, ISP and other carriers also need to take countermeasures.

(ii) Direction and organization of study group discussions

The Secretariat gave an explanation based on Document 2-5.

(iii) General discussion

The members discussed the direction and organization of discussions of this study group.

(A summary of the discussion is provided separately.)

(3) Others

The Chair asked that a table of Point 5 in Document 2-5 be created.

(4) Closing

6. Summary of the general discussion

A summary of the general discussion follows.

- What is the scope of the discussion?

→ In the first place, we would like to have a broad discussion about threats and issues. As specific issues emerge, we will define the respective roles of MIC and the private sector.

- ISPs have been spending a significant amount on information security infrastructure, which we would like you to consider.

- In Point 4 in Document 2-5, companies and individuals are collectively called the users who carry out information security measures. Shouldn't they be considered on a separate basis, because companies and individuals differ in terms of assets to be protected and measures needed?

- Isn't it necessary to discuss the issues from the viewpoints of both sides: those who implement measures and those who are protected against threats?

- Point 1 in Document 2-5 indicates the target of consideration. I think we should put more emphasis on addressing the expected changes in the social and industrial domains such as terrestrial digital TV broadcasting, the NGN and 4G mobile phones, and the changes in the environment that are certain to eventuate in around 2011. In other words, wouldn't it be better to discuss (2) first?

→ In terms of the outcomes of the study group, an analysis of the current state is required, so we would like to consider (1) first.

- Concerns are rising that there is a growing number of individuals with very high information literacy who actively access various information using tools and crossing

borders.

- Telecommunications carriers are very hesitant to cut off communications. I would like to know, why are you resisting implementing filters to protect users?
- Bandwidth control to protect operators' facilities follows the Telecommunications Business Law and the Radio Law in most cases, while filtering to protect users is not easy to implement from the viewpoint of the legal definitions.
- Since the legal system is behind the progress of technology and the changes in threats, it is difficult to judge whether it is really legal, which I think causes some hesitation to implement even a single filter.
- Issues related to the neutrality of the Internet and the fair cost burden are not the intended subjects of a general discussion on security. However, they are also discussed by other MIC study groups.
- When we compile a table based on Point 5 in Document 2-5, we would appreciate your opinion on the positioning of the measures in the business model and any legal issues.
- For Point 4 in Document 2-5, I would like you to include the issue of incident response and specify with whom we should cooperate and how we should act when something happens.
- If we were to include that topic, the table on Point 4 in Document 2-5 would require a new perspective describing time.
- It is important that we know what we can depend on in an incident response situation.