Study Group for Next-Generation Information Security Policies—7th Meeting

Summary of Minutes

1. Date and Time

Thursday, May 1, 2008, 10:00–12:00

2. Location

Special Conference Room 1, Ministry of Internal Affairs and Communications

3. Attendees (honorifics omitted)

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

Koichi Arimura (Telecom-ISAC Japan), Yasuo Ayazuka (NTT DoCoMo, Inc.), Hisao Iizuka (NEC BIGLOBE, Ltd.), Hiroyuki Ogura (Mitsubishi Electric Corporation), Akira Kato (Keio University Graduate School), Takashi Kimura (NIFTY Corporation), Shingo Koya (Trend Micro Incorporated), Satoru Koyama (NTTPC Communications Inc.), Mamoru Saito (Internet Initiative Japan Inc.), Masahiro Sata (WILLCOM, Inc.), Masahiro Shimomura (Japan Network Security Association), Hiroki Takakura (Kyoto University), Ikuo Takahashi (Lawyer), Masakazu Takahashi (Microsoft Corporation), Satoru Tezuka (Hitachi, Ltd.), Koji Nakao (KDDI Corporation), Michikazu Fukuchi (SOFTBANK BB Corp.), Masayo Fujimoto (Fuji Xerox 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), Suzuki (Director, General Policy Division), Yanagishima (Director for Policy Planning, Computer Communications Division), Kawauchi (Director, IT Security Office), Murakami (Deputy Director, IT Security Office), Nakamura (Deputy Director, IT Security Office), Nagaya (Security Measures Chief, IT Security Office)

4. Agenda

(1) Opening

(2) Agenda

(i) International cooperation for information security

(ii) General discussion

(3) Others

(4) Closing

5. Summary of meeting

(1) Opening

The Chair introduced a new member who joined the Study Group starting with this meeting.

New member: Ikuo Takahashi (Lawyer)

The Secretariat reviewed the minutes of the 6th meeting.

(2) Agenda

(i) International cooperation for information security

a. International cooperation/collaboration (Nakao)

Nakao gave an explanation based on Document 7-2.

Summary of the question and answer session

- It is suggested that as a future course, “cooperation with neighboring countries be promoted” with “focus placed on the CJK meeting.” Is it feasible for Japan, China, and Korea to cooperate together in a security related market?

→Japan, China and Korea have good relationships at ITU-T and share a high level of motivation. However, there is a certain issue in dealing with what has been decided due to various factors, such as the environment in each country. It is, however, obviously impossible to ask countries to all of a sudden cooperate with one another. Though it is impossible to know whether things will go well or not, I think that it would be a good option to start talking with motivated neighboring countries.

- As a future direction, the description says “security information sharing framework (to be reviewed).” Which part specifically do you think should be reviewed?

→In the current information sharing scheme, we cannot expect effective measures even if we contact the PoC. Consequently, the scheme is not activated and does not effectively function. It is necessary to clarify the issues of the current scheme and reorganize players.

- People think that standardization has two aspects; one where everyone promotes it and the other where everyone hinders each other. In my opinion, security has the latter aspect because it is better to have better security than others.

→It used to be argued that security is not in a category suited for standardization. However, as is represented by encryption algorithms, the current trend is that security is not something that should be concealed but rather used actively to increase the nation's benefit. If it is difficult for certain countries to adopt a certain technology or the technology is sweeping the world, some countries may be opposed to or compete against the technology. But, if technology can be used by anyone on a common platform, it is usually supported by everyone.

- The definition of damage is not clarified on an international basis. For example, if there are criteria for DoS and for the degree of DDoS, people will be able to declare that they certainly have damage without any misunderstanding. Are there any such standardization movements?

→It is considerably difficult to establish standards because indices to measure threats vary, depending on, for example, the size of ISPs and the legal systems of individual countries.

b. International issues from the viewpoint of an ISP and collaborative measures for such issues (Saito)

Saito gave an explanation based on Document 7-3.

Summary of the question and answer session

- It is difficult for a simple national PoC to function well. Now, we are in the process of dividing it into three layers, namely: policy, operation, and legal enforcement. With the policy layer of the PoC at the National Information Security Center (NISC), the operation layer of the PoC related to the government at the NISC with other general parts to the JPCERT/CC, and the legal enforcement layer at the National Police Agency; this set of layers will act as a national PoC. In the future, it will be necessary to prepare a PoC for industry concerning business and to develop mutual cooperation among the PoCs.
- When ISPs conduct certain activities in implementing international cooperation, the secrecy of communications will become a great obstacle. Since some countries handle the secrecy of communications quite differently from Japan, it is necessary to carefully find and clarify what laws and regulations are observed internationally and how the secrecy of communications is handled.
- Eventually, it is essential to properly deal with domestic issues. The reality in Japan is that no one can take any action unless those who suffered damage report the damage. There are also many cases in which action cannot be taken even if damage is declared. A legal

system has been established, for example, for offensive or defaming cases, and things are moving more smoothly. Concerning these matters, I hope that discussions are held to facilitate taking specific action.

- An example is given in which attacks from Country C are made via Country A and Country B. There can be cases where Japan is Country A. In such cases, the network may be deemed to be participating in crime.

→Such problems may possibly occur, however, nothing has been discussed on such matters yet. It is essentially impossible to identify what role the network played unless the content of the communications is investigated.

→In the United States, legal regulations are quite different for domestic communications and for communications transmitted across borders. A sovereignty matter is involved once communications are transmitted across borders. Sovereignty of telecommunications has rarely been argued in Japan.

c. Direction of measures for international cooperation for information security

The Secretariat gave an explanation based on Document 7-4.

(ii) General discussion

- It will be better not to make ciphers or the like available to the public. Even if they are not standardized, everyone will use them if they are used by the government and not deciphered.

→I do not know whether this is an appropriate expression, but ciphers should be discussed separately in the cases of the national defense and disaster prevention, respectively. National defense and business in the private sector are quite different from one another. My understanding is that this study group is discussing matters closer to the private sector.

- We will be in trouble if the country's security is just in accordance with the standards. It should exceed the standards. We should stop arguing that the country's security can be in accordance with the standards.

→"Country" is not really a good expression. In the USA and Europe, "national security related computing and communication" that pertains to security is also distinguished from other "civil computing and communication," and the respective information management classifications are different from one another. Coordination is now in progress in the government to review the classifications accordingly.

-People talk about international standardization in joint activities. In Japan, activities are conducted to promote international standardization. One example is the Information Technology Standard Committee of the Information Processing Society of Japan. However, while there is usually only one relevant major manufacturer in each country in Europe, there are many manufacturers in Japan, making it difficult to compile a common consensus here. We may need a scheme to compile domestic opinions before we attempt ones on an international basis.

- In the registration system of encryption algorithms specified in ISO/IEC 18033, ciphers in Japan accounted for more than 60% of the total of 20 or so cases that have been registered. It is difficult for an organization, such as an academic society, to determine a single standard in Japan's environment. A political decision will be necessary with the involvement of the relevant ministries and agencies.

(3) Others

The Secretariat explained the future schedule.

(4) Closing