Study Group on ASP/SaaS Information Security Measures—3rd Meeting

Summary of Minutes

1. Date and Time

Wednesday, Oct 17, 2007; 15:00–17:00

2. Location

Room C, D, & E, 3rd floor, Mita Common Meeting Place

3. Attendees (as seated, honorifics omitted)

(1) Group Members

Chair: Ryoichi Sasaki (Tokyo Denki University)

Vice Chair: Koji Nakao (KDDI Corporation) and Masayo Fujimoto (Institute of Information Security)

Eiji Aoki (NEC Corporation), Masami Imada (Fujitsu Business Systems Ltd.), Inekazu Uehara (Okinawa Electric Power Company, Incorporated), Yoshiyuki Oikawa (salesforce.com Co., Ltd.), Hiroyuki Ogura (Mitsubishi Electric Corporation), Takashi Kimura (Blayn Co., Ltd), Shintaro Kobayashi (Nomura Research Institute, Ltd.), Kunikazu Tsuda (ASP Industry Consortium Japan), Toshio Nishiyama (NTT Communications), Shunsuke Hanato (TRICORN Corporation), Hajime Miyasaka (NTT Data Corporation)

Absent: Yoshiki Matsuhashi (Sansui Co., Ltd.), Satoshi Hayashi (Miroku Jyoho Service Co., Ltd.), Yasuo Iwashita (Osaka Excellent iDC KK),

(2) MIC Representatives

Kawachi (Director, Office of IT Security Policy), Murakami (Deputy Director, Office of IT Security Policy), Nakamura (Deputy Director, Office of IT Security Policy), Yamashita (Deputy Director, Telecommunication Systems Division), Tanabe (Policy Unit Chief, Office of IT Security Policy), Nakao (International Policy Unit Chief, Office of IT Security Policy)

4. Agenda

(1) Opening

(2) Confirmation of Distributed Documents

(3) Confirmation of Meeting Summary of the Previous Meeting

As described in Document 3-1, a summary of the previous meeting was presented.

(4) Attendee Roll Call

(5) Meeting Proceedings

1) Current Status and Challenges in Information Security Measures concerning ASP/SaaS

As described in Document 3-2, Mr. Ogura presented the current status and challenges in information security measures concerning ASP/SaaS within Mitsubishi Electric Corporation.

2) Current Status and Challenges in Information Security Measures concerning ASP/SaaS

As described in Document 3-3, Mr. Kimura presented the current status and challenges in information security measures concerning ASP/SaaS within Blayn Co., Ltd.

3) Discussion about the ASP/SaaS Information Security Policy Guidelines Draft

As described in Document 3-4, 3-5, 3-6-1, and 3-6-2, the Secretariat provided information concerning the ASP/SaaS Information Security Policy Guidelines and the other issues. Details are summarized below:

- ASP and SaaS services were classified into the 12 patterns from the viewpoints of confidentiality, integrity, and availability. In order for classification according to these viewpoints, the handling of private information was used for confidentiality. In the same way, financial/accounting information was used for integrity, and recovery time for availability.
- In the Organization and Operations section of the Guidelines, we wonder if the Guidelines can be made applicable to all 12 patterns, taking account of the characteristics of PDCA, B2B relationships, and SLAs.
- In the Physical and Technological Measures section of the Guidelines, a risk analysis was performed with focuses on confidentiality, integrity, and availability in order to identify the correspondence between each measure and the associated type of risk.
- Further, each measure was assessed as to whether it was a “basic” measure for which implementation is essential, or a “recommended” measure that may be implemented additionally.
- In order to establish the level of requirement in terms of confidentiality, integrity, and availability for each measure in the 12 patterns, such requirement levels should be quantified for use as criteria.

Also, the Secretariat suggested a plan to establish a voluntary working group to work out the

details of the ASP/SaaS Information Security Measures, and this was approved by the members.

4) Free Discussion

The Secretariat presented the following issues to discuss and members expressed their opinions concerning each issue:

Issue 1: Security measures were now classified according to three viewpoints, i.e. judgment criteria (confidentiality, integrity, and availability), but is this classification adequate? Are there any other viewpoints that should be added?

Issue 2: Are the 12 patterns appropriate? Should they be merged into a smaller number of patterns?

Issue 3: Is it adequate to divide each measure into “basic” and “recommended?”

Issue 4: Is it adequate to use an “Item to Assess” and its “Criterion” to indicate the level of requirement within one measure?

Issue 5: Is it adequate to organize the Guidelines that comprise an Organization and Operations section, and a Physical and Technological Measures section?

Issue 6: Other issues (Volume of information, contents, and ease of understanding the structure of the Guidelines, etc.)

Comments, questions, and answers were as follows:

<Comments on Purpose of the Guideline>

- The purpose of the Guidelines is to provide patterns of information security measures for ASP/SaaS vendors who do not have information security expertise so that they can choose suitable security measures according to the contents of their business.
- It is also important to disseminate the concept of information security to users, not just to ASP/SaaS vendors.
- For small-to-medium ASP/SaaS vendors, the words and contents of the Guideline are too complicated. Revision is necessary to make it easier to understand.
- We agree with having two sections, the Organization and Operations section and the Physical and Technological Measures section, in the Guidelines.

<Comments on the Organization & Operation section (Issue 5 related)>

- ISO/IEC27001 is requirement, not the Guidelines. ISO/IEC27001’s contents should not be altered.
- The problem in ISMS is having so many implementation guidelines across 133 controls, making implementation costly due to the requirement for external consultants to

undertake such work.

- ASP/SaaS vendors are not required to implement all the measures specified in ISMS. It is possible for the Guidelines to specify a conceptual framework and a procedure to simplify ISMS for ASP/SaaS vendors.

<Comments on the Physical & Technological Measure section (Issue 1 to 4 related)>

- The number of patterns should be reduced.
- Chapter 3 (page 3) in Document 3-6-2 concerns the Internet Data Center, which is actually beyond the range of ASP/SaaS vendors' responsibility. Areas for which ASP/SaaS vendors have no way other than outsourcing must be noted as such.

(6) The secretariat presented the schedule for the next meeting.

(7) Close of Meeting