Study Group on ASP/SaaS Information Security Measures—2nd Meeting

Summary of Minutes

1. Date and Time

Wednesday, Aug 08, 2007; 10:00–12:00

2. Location

Room A & B, 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.), Yasuo Iwashita (Osaka Excellent iDC KK), 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), Yoshiki Matsuhashi (Sansui Co., Ltd.), Hajime Miyasaka (NTT Data Corporation)

Absent: Satoshi Hayashi (Miroku Jyoho Service Co., Ltd.)

(2) MIC Representatives

Kawachi (Director, Office of IT Security Policy), Murakami (Deputy Director, Office of IT Security Policy), Yoshida (Deputy Director, Computer Communications Division), Yamashita (Deputy Director, Telecommunication Systems Division, represented by Yamanaka, Chief, Security and Reliability Measure Unit), Tanabe (Policy Unit Chief, Office of IT Security Policy)

4. Agenda

(1) Opening

(2) Confirmation of Distributed Documents

(3) Meeting Proceedings

1) Confirmation of Meeting Summary of the Previous Meeting

2) Introduction of Group Members (Change in Secretariat Members)

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

As described in Document 2-2, Mr. Miyasaka presented the CO_2 Navigator by NTT Data as an example of ASP services (details explained by Mr. Moriya).

Questions and answers concerning this issue were as follows:

- NTT Data has established a corporate-wide security policy and implementation measures concerning ASP services in accordance with this security policy.
- To integrate operational procedures across the company, we have an operational management implementation procedure as a corporate standard, utilizing ITIL and CMMI, both internationally recognized standards.

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

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

Questions and answers concerning this issue were as follows:

- For effective improvement of security levels, it is important to equally improve: physical security; software security; and security concerning persons or corporation as operators; taking account of achieving a balance with costs.
- Our users are all corporate users, and they are very sensitive about the information security. Thus, we are keen to get the ISO PrivacyMark and update security hole information.

5) Issues Presented by the Secretariat

The Secretariat provided information concerning the following issues using the documents listed below:

- *Current Status and Challenges concerning the Standards and Guidelines of Information Security Measures* (Document 2-4)
- *Clarifying the Issues for Discussion in Order to Establish the ASP/SaaS Information Security Guidelines* (Document 2-5)
- *How to Establish the ASP/SaaS Information Security Guidelines* (Document 2-6)

6) Free Discussion

Members exchanged opinions concerning the above issues raised by the Secretariat.

Comments are summarized below:

- The following lines need to be added in pages 3, 13, and 16 of Document 2-5.
  - Dialogues concerning risk must be held between ASP/SaaS vendors and users.
  - The Guidelines must be established in a language understood both by ASP/SaaS vendors and users. We should share and retain this viewpoint.
- The following three points are important in establishing the Guidelines.
  - The compliance with the Guidelines must be ensured by providing/obtaining a certificate.
  - The coverage of the Guidelines must be easily understandable by users.
  - Utilize the Guidelines as the criteria to assess security levels.
- The Guidelines are expected to be utilized within the ASP/SaaS industry, rather than the certification criteria that a public body uses. Another purpose of having the Guidelines is to present the minimum requirements concerning information security measures.
- The Information Security Conference for Telecommunications (ISeCT) (MIC is involved as an observer) is currently discussing the Information Security Management Guidelines for Telecommunications (ISM-TG) and is working towards establishing a new system that gives a “T” mark to a telecommunication carrier that is certified to be compliant with ISM-TG, in addition to the ISMS certificate. In the same way, it would be possible to give some kind of approval mark to an ASP/SaaS vendor that has been certified as compliant with the Guidelines, again in addition to the existing ISMS certificate.
- As the information security measures between ISPs are not specified in ISO/IEC27001; we must clarify the requirements for inter-ISP security measures to be included in these Guidelines.
- The Council on Economic and Fiscal Policy discussed promoting ASP/SaaS in order to improve the productivity of small-to-medium-sized companies; however, there has been no discussion about promoting small-to-medium-sized ASP/SaaS vendors. When discussing the certification system, we should keep in our mind that the ASP industry is an infrastructural industry and therefore small and medium vendors will be gradually shaken out or merged.
- The requirements provided in the Guidelines must specify the security level that the industry should have as its foundation, rather than merely an indication for the

minimum security measures required.

- Clarify the minimum security measures required (the level that must be achieved) first, and on top of that, we should clarify the level that users would demand of ASP/SaaS vendors. This level should be quantified so as to be visible, in the same way as an SLA provided by vendors to users.
- As for MICTS, described on page 2 of Document 2-6, a part of MICTS-1 has been implemented as ISO/IEC 27000 (Fundamentals and vocabulary) and MICTS-2 has become the final draft of ISO/IEC 27005 (Information security risk management). It is possible to provide these drafts as far as they are not distributed beyond this Study Group. Under the same conditions, it would also be possible to provide the revised X.1051 recommendations that reflect the above-mentioned ISM-TG, as suggested by Japan to the ITU.

(4) Others

The secretariat presented the schedule for the next meeting.

(5) Close of Meeting