Study Group on ASP/SaaS Information Security Measures—4th Meeting

Summary of Minutes (Draft)

1. Date and Time

Tuesday, Dec 18, 2007; 10:00–11:00

2. Location

Special Meeting Room No. 3, 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), 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.), Inekazu Uehara (Okinawa Electric Power Company, Incorporated),

(2) MIC Representatives

Nakata (Director-General for Policies), Matsui (Deputy Director General), Suzuki (Director, General Policy Division), Kawachi (Director, Office of IT Security Policy), Murakami (Deputy Director, Office of IT Security Policy), Nakamura (Deputy Director, Office of IT Security Policy), Nakazato (Deputy Director, Information Policy Division) Yoshida (Deputy Director, Computer Communications Division), Watanabe (Head, 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) Opening Speech by Nakata Director-General for Policies

Greetings were extended by Mr. Nakata.

(3) Confirmation of Distributed Documents

(4) Confirmation of Meeting Summary of the Previous Meeting

As described in Document 4-1, a summary of the previous meeting was presented.

(5) Attendee Roll Call

(6) Meeting Proceedings

1) As described in Document 4-2, *ASP/SaaS Information Security Policy Guidelines (Draft)*, the Secretariat provided information concerning the Guidelines. Members agreed to send out these Guidelines for public review after amending them according to the questions and answers that took place in this meeting.

2) As described in Document 4-3, *Summary Report of the Study Group on ASP/SaaS Information Security Measures (Draft),* the Secretariat explained Document 4-4, *Report of the Study Group on ASP/SaaS Information Security Measures (Draft)*. Members agreed to send out this draft report for public review after amending it according to the questions and answers that took place in this meeting.

● A summary of the Secretariat's explanation concerning Document 4-2, *ASP/SaaS Information Security Policy Guidelines (Draft)* is as follows:

- The Guidelines specify the Information Security Measures that ASP/SaaS vendors need to implement, and comprise: *I. Introduction; II. Organization and Operation;* and *III. Physical and Technological Measures*.
- The Guidelines are expected to provide the following benefits:

  1) Reducing the burden for small-to-medium size ASP/SaaS vendors who may not have sufficient financial resources, to perform their own security analyses by presenting a prioritized set of the most important information security measures to be implemented.

  2) Represent a standard for information security measure requirements to be shared among ASP/SaaS vendors, especially when they are affiliated.

  3) Provide selection criteria to help users to select the most appropriate ASP/SaaS vendor.
- *I. Introduction* provides basic information, including the purpose of the Guidelines, coverage, usage, notes, and glossary.

- *II. Organization and Operations* presents measures for organization managers, including optimizing the management system, notes on concluding contracts with outsourcers, and responsibilities towards users.
- *III. Physical and Technological Measures* is mainly for ASP/SaaS service operators and engineers and lists information security measures to protect the information assets of ASP/SaaS vendors.
- ASP/SaaS services have been classified into six patterns from the viewpoints of confidentiality, integrity, and availability. The level of information security measures required for each type is also indicated.
- Information security measures are also classified into *Basic* and *Recommended*. The implementation priority for each measure is presented along with a sample of best practice.
- In the *Physical and Technological Measures* section, an assessment list has been added to evaluate the implementation level of each measure quantitatively and concretely. Also each item in the list is indicated with the standard value for the required level of implementation for each pattern. An asterisk (*) shown with the standard value indicates the level that must be achieved in order to deliver reliable information security.

Questions and answers concerning issues are listed below:

- The *Access Authorization* section on page 53 and some other sections have two values as the standard value. Do both of these values need to be achieved, or just either one? This should be indicated clearly.

  (Secretariat's Answer) We will check whether both of them or either of them need to be achieved, and will add either "and" or "or," accordingly.
- In the *Glossary*, some terms refer to JIS Q 13335-1. However, the referenced standard is currently integrated and reorganized with the other standards and the standard number may either be changed or become obsolete. Isn't referring to JIS Q 27001 solely sufficient in order to avoid confusion?

  (Secretariat's Answer) We will amend those references as commented.
- *I. Introduction* describes the overall structure of the Guidelines and it refers to the Introduction section itself. This is a little strange to read and I think the explanation of the structure of the Guidelines should be placed before the Introduction.

  (Secretariat's Answer) For the ease of understanding of readers, we would like to keep the structure of the Guidelines as simple as possible. Therefore we would like to retain the same structure.

● The summary of the Secretariat's explanation concerning Document 4-3, *Summary Report of the Study Group on ASP/SaaS Information Security Measures* is as follows.

- ASP/SaaS services naturally accumulate a massive amount of confidential information and personal information concerning their corporate customers. Therefore information security is essential for the sound growth of the industry.
- Some concerns include: there is no indication for ASP/SaaS vendors with limited personnel and limited financial resources to prioritize the necessary information security measures; there is no indication about appropriate information security measures to suit each of the various types of ASP/SaaS services; and the explanations and information for users seems insufficient.
- The existing standards and guidelines are not made for ASP/SaaS services. Therefore it is necessary to create information security measure guidelines specifically for ASP/SaaS vendors.
- The Guidelines were made with an emphasis on the following four points:
  1) Limited to high-priority information security measures for ASP/SaaS vendors
  2) Implementation of suitable information security measures should be simple
  3) Present easy-to-understand and easy-to-implement information security measures
  4) The measures should be easy to understand for users as well
- The following six approaches were taken in creating the Guidelines:
  1) Establish information security measures particularly suitable for ASP/SaaS services based on typical ASP/SaaS system configurations
  2) Classify the measures into basic ones, which are mandatory, and recommended ones
  3) Present easy-to-understand descriptions and provide quantitative and concrete levels for implementation of measures (ones that must be achieved are clearly marked)
  4) Provide security measures concerning organizational operations that need to be specifically addressed by ASP/SaaS vendors
  5) Measures are classified into different patterns of security requirements according to the type of services, delivering inclusiveness and adaptability
  6) Provide methods whereby a vendor can easily choose the most appropriate measures using the above-mentioned patterns
  - The next challenge is promotion of the Guidelines so that they become widely recognized and utilized. Also, the Guidelines must be regularly reviewed in order to keep the contents up to date with advances in technology and ASP/SaaS service styles,

and a coherent system of revision and update must be established.

Questions and answers regarding the explanation of Document 4-3 are as follows:

- Which documents will be submitted for public review?

  (Answer from Secretariat) They will be Document 4-2, *Guidelines (Draft),* and Document 4-4, *Report (Draft)*. Document 4-3, *Summary of Report (Draft)* will be attached to the press release as reference material.
- Is it possible to add a paragraph that states, "Usage of the Guidelines should improve the overall information security environment for users by implementing suitable information security measures among ASP/SaaS services?"

  (Answer from Secretariat) Such a paragraph is already in the introductory chapter and Chapter 1 of *Report (Draft)*, but we are considering adding a similar paragraph in Chapter 4, *Effects of Utilizing the Guidelines*.
- The coloring of the legend in *Existing Laws, Standards, and Guidelines* on page 6 in Document 4-3 is incorrect. Please correct it.

  (Answer from Secretariat) We will check and make amendments.
- There was a discussion that the Guidelines may refer to some parts (related to IT services) of the JIS Q 20000 series. Was this idea reflected in the current *Guidelines (Draft)*?

  (Answer from Secretariat) After a detailed study concerning the issue involving experts, we found that the reference to the JIS Q 20000 series can be replaced by a reference to the description concerning concluding contracts with outsourcers listed in ISO/IEC 27001 and 27002. As a result, there is no longer a reference to the JIS Q 20000 series.

(4) Others

The Secretariat explained that the public review would take place from December 19, 2007, to January 18, 2008. It was also announced that the next meeting (5th) would be held sometime between late January and early February, depending upon the results of the public review.

(5) Close of Meeting