



Communications News

Vol. 19 No. 4
June 6, 2008

Biweekly Newsletter of the Ministry of Internal Affairs and Communications (MIC), Japan

ISSN 1349-7987

Please feel free to use the articles in this publication, with proper credits.

Formulation of Guidelines for Information Security Measures for ASP/SaaS - From the Report from the Study Group on ASP/SaaS Information Security Measures -

MIC set up the Study Group on ASP/SaaS Information Security Measures (Chair: Prof. SASAKI Ryoichi, Tokyo Denki University) in June 2007 in order to investigate information security measures for ASP/SaaS which are showing rapid penetration as ICT services that provide application and related functions over networks.

The following is an outline of the report compiled by the study group in January 2008, as well as guidelines for information security measures.

Background

(1) The development of the broadband environment

Japan's Internet users now account for over 68% of the total population, and in fact, two out of three citizens are now using the Internet. Also, there were 26.44 million broadband users as of the end of fiscal year 2006, and with the penetration of broadband, the distribution of high volume contents such as music and movies has become possible, turning the Internet into a major infrastructure supporting people's lives and the economic activities of society.

(2) The promotion of penetration of ASP/SaaS

There is no denying that Japan is facing a declining population and that the existing economic model is

nearing its limits. In order to put the economic back on track for growth in the current conditions, it is vital to use ICT to improve productivity and strengthen international competitiveness.

Under such conditions, ASP (Application Service Provider) and SaaS (Software as a Service) which provide applications and related functions through networks have attracted attention as easy-to-use new ICT services for small and medium sized companies, and having been mentioned in the likes of the Program for Enhancing Growth Potential (Council on Economic and Fiscal Policy) and the final compilation by the Panel on ICT International Competitiveness (MIC), the government as a whole is working towards promoting the penetration of ASP/SaaS as trump cards to

CONTENTS



Formulation of Guidelines for Information Security Measures for ASP/SaaS
- From the Report from the Study Group on ASP/SaaS Information Security Measures -

..... 1



**International Policy Division,
International Affairs Department,
Telecommunications Bureau,
Ministry of Internal Affairs and
Communications (MIC)**

1-2, Kasumigaseki 2-chome, Chiyoda-ku, Tokyo 100-8926, Japan
Fax: +81-3-5253-5924
Tel: +81-3-5253-5920

We welcome your comments via:
http://www.soumu.go.jp/joho_tsusin/eng/contact.html

MIC Communications News is available at:
http://www.soumu.go.jp/joho_tsusin/eng/newsletter.html

Presentation materials of MIC are available at:
http://www.soumu.go.jp/joho_tsusin/eng/presentation.html

E-mail distribution of this newsletter is possible if desired.

improving productivity and strengthening global competitiveness.

(3) Goals of setting up study group

The corporate usage of ASP/SaaS offers enormous advantages from the point of view of costs and ICT literacy, including the ability to build and operate systems in a short time rather than developing them separately, plus the reduction in the

burden related to system maintenance, operation and management. This is why the use of ASP/SaaS seriously contributes to improvements in productivity in small and medium-sized companies where both human and financial resources are limited. On the other hand, given that ASP/SaaS operators accumulate large-scale confidential information and customer information from the corporations that are their users,

the implementation of appropriate security measures is important.

This is why the Study Group on ASP/SaaS Information Security Measures was established in order to investigate information security measures that ASP/SaaS operators should implement, having grasped the actual condition of ASP/SaaS, the current status of information security measures, and future

Figure 1: What are ASP/SaaS?

Definition of ASP/SaaS

"To make available for use application software and related services through networks, or business models that provide such services." (from the 2004 "ASP White Paper")

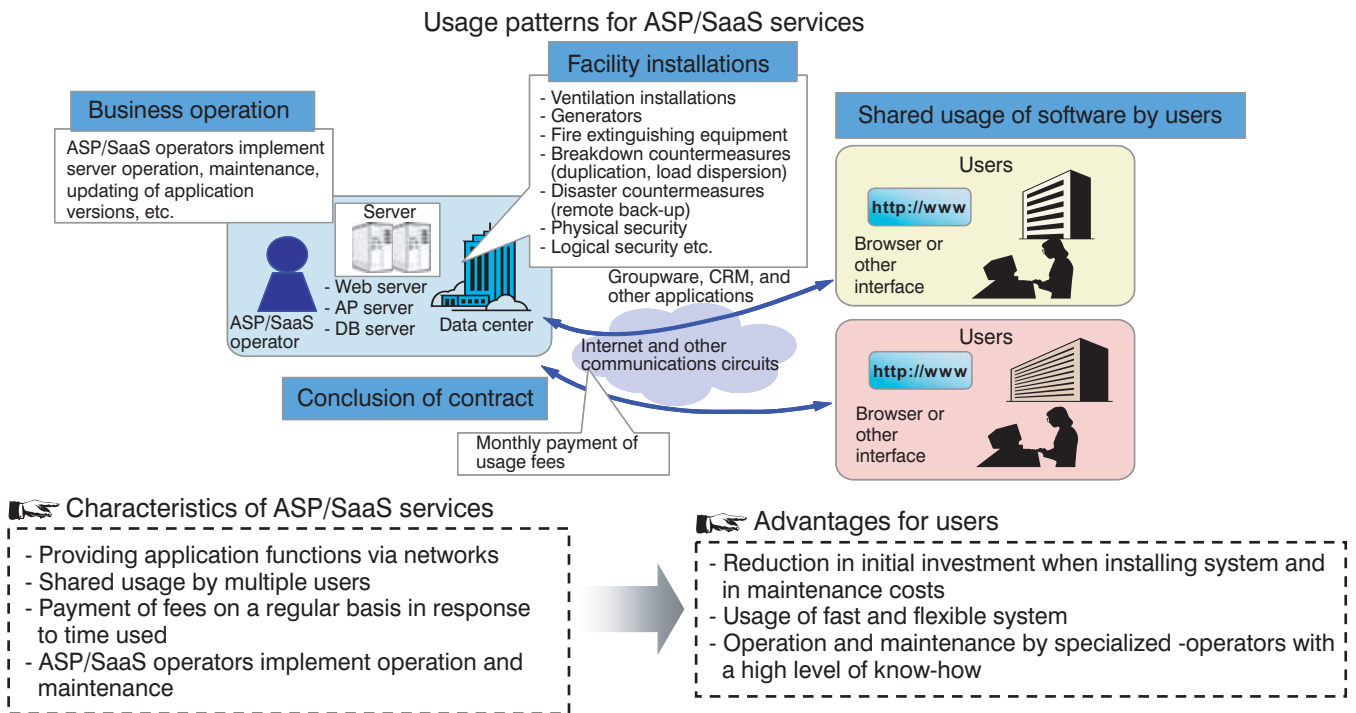
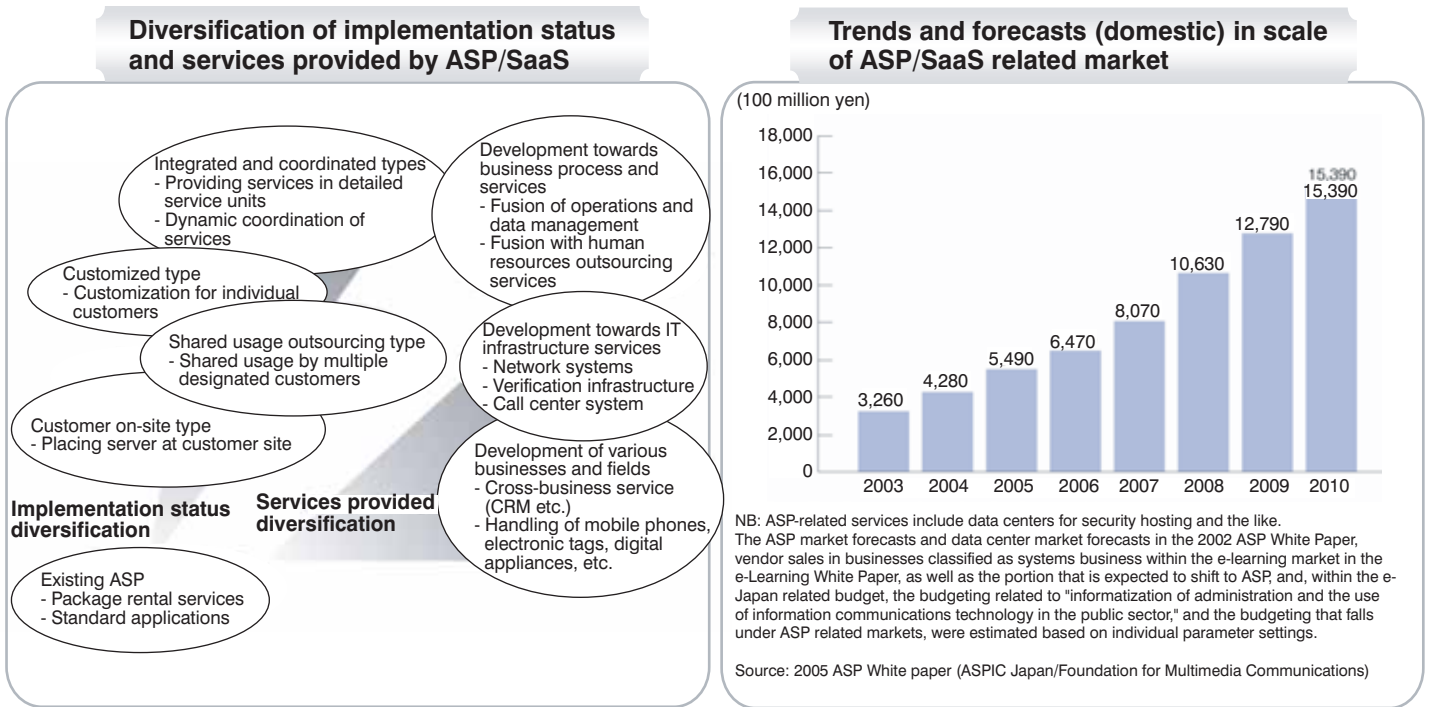


Figure 2: Diversification of ASP/SaaS services and increase in scale of market

- Rapid development in diversification of ASP/SaaS services from the two viewpoints of implementation status and contents of services provided.
- In response to the diversification of ASP/SaaS services, the user base is also expanding to a wider range of industrial sectors.
- The scale of the ASP/SaaS market is continuing to grow at a pace of approximately 1.3 times a year since its value of 326 billion yen in 2003, and is expected to reach 1,539 billion yen by the 2010, which is just under five times the 2003 figure.



Current Status and Issues Related to ASP/SaaS Information Security Measures

The two major characteristic of ASP/SaaS services can be said to be that the majority of providers are small and medium-sized operators, and that there is a wide diversity in the services on offer. Taking these characteristics into consideration, the results of interviews implemented with ASP/SaaS operators revealed the following issues in relation to the implementation of information security measures:

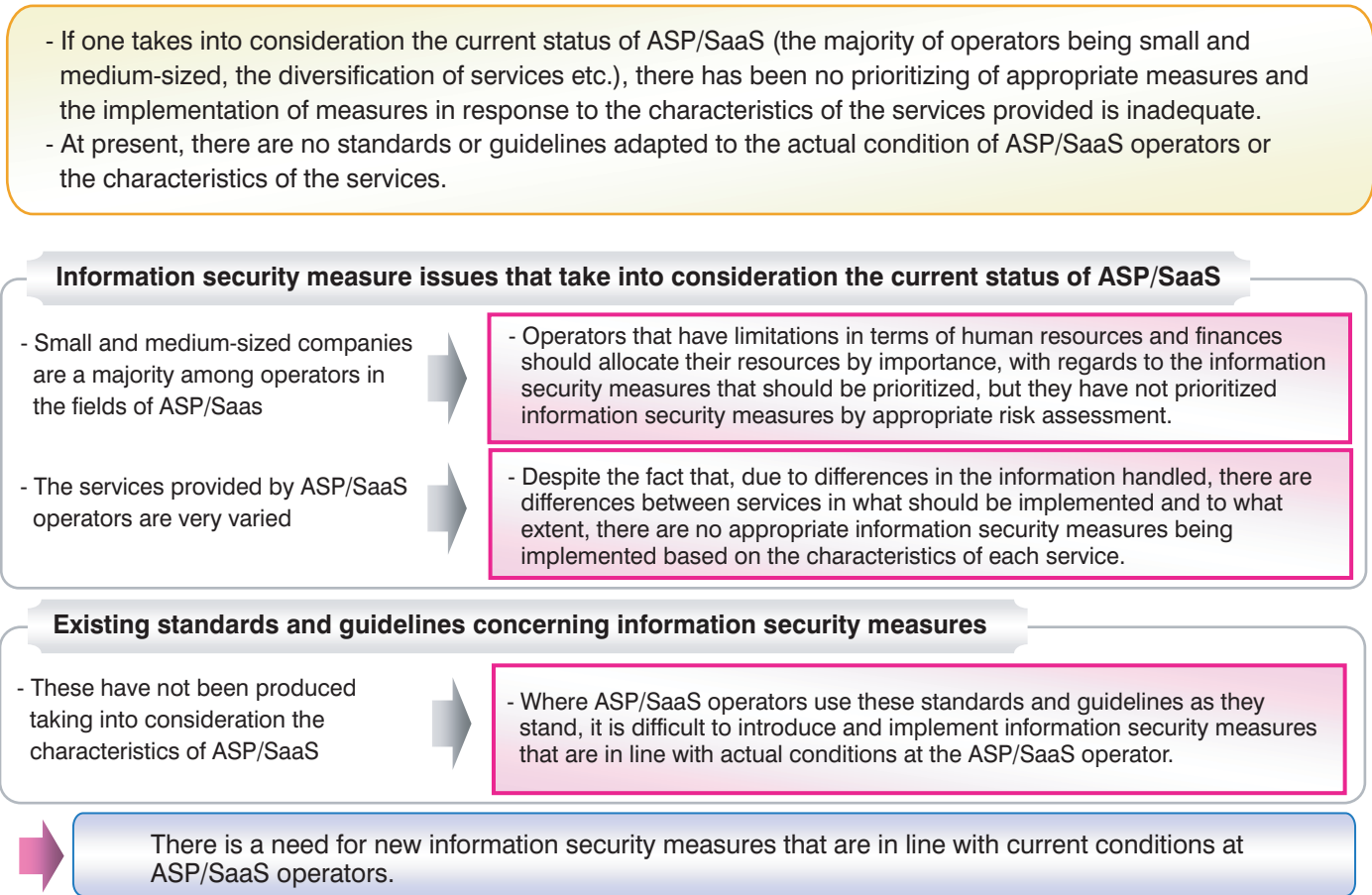
- o There has been no prioritization of information security measures.
- o The most appropriate information security measures based on the characteristics of the ASP/SaaS services provided have not been developed.

On the one hand, in terms of existing standards and guidelines for information security measures, there are a variety of things out there that can serve as guidelines in implementing measures, such as the JIS Q 27001 (ISO/IEC 27001) and the JIS Q 27002 (ISO/IEC 27002). Since, however, these were not necessarily formulated with the

particular characteristics of ASP/SaaS in mind, if ASP/SaaS business operators make use of such standards and guidelines as they stand, there will be a problem in introducing and operating information security guidelines that are in line with actual conditions.

From the results of the above analysis, the study group came to the conclusion that there is a need to produce new information security guidelines that reflect the characteristics of ASP/SaaS, and are in line with the current conditions of ASP/SaaS operators.

Figure 3: Current ASP/SaaS information security status and issues



The Formulation of Guidelines for Information Security Measures

(1) Basic outlook concerning the guidelines

In order to work towards solving the issues related to information security measures for ASP/SaaS, "Concrete guidelines for ASP/SaaS service operators when investigating the implementation of appropriate information security measures based on the characteristics of the services provided" should be the basic positioning of the guidelines, and in producing them, the following important points were kept in mind.

- o To pinpoint the information security guidelines that should be given priority, and that reflect the characteristics of the ASP/SaaS operators and their services.

- o Making it possible to relatively easily implement information

security measures which take into account the services each provides, by having the ASP/SaaS business operator use the guidelines as they stand.

- o Offering concrete information security guidelines that are easy for ASP/SaaS business operators to understand and implement.

Furthermore, investigations took place to consider the facts of the guidelines being used as reference by the ASP/SaaS service providers, but these have also been produced keeping in mind that they should be easy to understand for users of ASP/SaaS services.

(2) Investigations ahead of formulation of guidelines

In order to work towards ongoing operation and revisions of the information security guidelines for ASP/SaaS operators, there is a need for putting in place an

operation management system within the internal organization of the ASP/SaaS business operators, for measures for the organizational and operational sides of the matters for consideration in contracts with external organizations. In parallel, physical and technical measures will be needed that apply to the hardware and software that makes up the systems, as well as housing such as buildings, power sources, etc. in order to preserve the information resources of the ASP/SaaS services.

With regard to the information security measures for the organizational and operational sides, ASP/SaaS stakeholders (those with interests) were taken into consideration and measure items were obtained using the information security detailed management measures shown in appendix A of the JIS Q 27001.

On the other hand, with

regard to physical and operational security, measure items were obtained by categorizing the widely varied ASP/SaaS services into 6 patterns, specifying the elements that make up ASP/SaaS, clarifying information resources and conducting an analysis of dangers facing information resources, and then referring to existing standards and guidelines such as Appendix A of the JIS Q 27001 and the guidelines concerning outsourcing in public IT (MIC). In addition, with regard to the deriving of each measure item, the fact that a large proportion of ASP/SaaS business operators are small and medium-sized companies was taken into consideration, investigations are focused on measures that are easy to understand as well as prioritizing the order in which they should be applied, and similar measure items are being grouped together and re-written so as to reduce the number of measure items.

Following on from that, a two-level priority system was established regarding the necessity and importance of each measure item, with measure items that should be given priority implementation, regardless of ease of implementation or cost, classified as "basic," and measure items that could be applied selectively when working to differentiate oneself from other companies or responding to high-level user demands classified as "recommended."

In addition, in order to deepen the understanding of ASP/SaaS business operators concerning measure items, an

explanatory document for a best practice addendum of concrete implementation methods and warnings relating to implementing the measures was produced, referring to the JIS Q 27002 as well as "Security Guidelines and Explanations for Financial Institution Computer Systems" (The Center for Financial Industry Information Systems), and attached to the measure items.

Furthermore, with regard to physical and technical measures, as there are differences in the information resources depending on the type of ASP/SaaS service, it is necessary to put in place a measure implementation level that complies with the pattern, while keeping in mind that different levels of information security are required. Consequently, it was decided to establish a "measure reference value" that is attached to each pattern as a value for gauging implementation levels, and an "evaluation item" that works as an indicator for evaluating the implementation level of each measure item quantitatively or concretely, so as to obtain easily the measure implementation level that should be aimed for.

Also, in terms of investigating best practices, valuation items and measure reference values, by including the opinions of experts in relevant fields (ASP/SaaS business operators, information equipment manufacturers, ISPs and data center business operators), attention was paid to the extent possible to consistency with the actual condition of ASP/SaaS services, for example with regard

to attention to difficulties relating to the actual implementation of measures by ASP/SaaS business operators.

(3) Composition of the guidelines

The guidelines that were completed according to the process described above were composed out of the three parts shown below.

- o Prologue: Introduction including the guideline objectives, range covered, usage methods, warnings and definition of terms

- o Organization and Operation: A collection of information security measures related to organization and operations such as operation management systems to secure information security, points to consider in contracts with outside organizations, and responsibilities towards users. This will probably mainly be used as reference material by organizational managers such as executives.

- o Physical and Technical Measures: Information security measures for operations, failure surveillance, virus countermeasures, back-ups and damage measures, taking into consideration the variety of ASP/SaaS services as well as structural elements (applications, networks, and also buildings and power sources etc.). This will probably be mainly used as reference by on-site engineers.

Figure 4: Derivations of necessary information security measures

- Focusing on the organizational elements of ASP/SaaS, investigating the necessary information security measures, and turning these into guidelines.
- Deriving organizational and operational measures relating to the putting in place of an internal operational management system within ASP/SaaS business operators, as well as physical and technical measures applying to the hardware and software that make up the ASP/SaaS services.

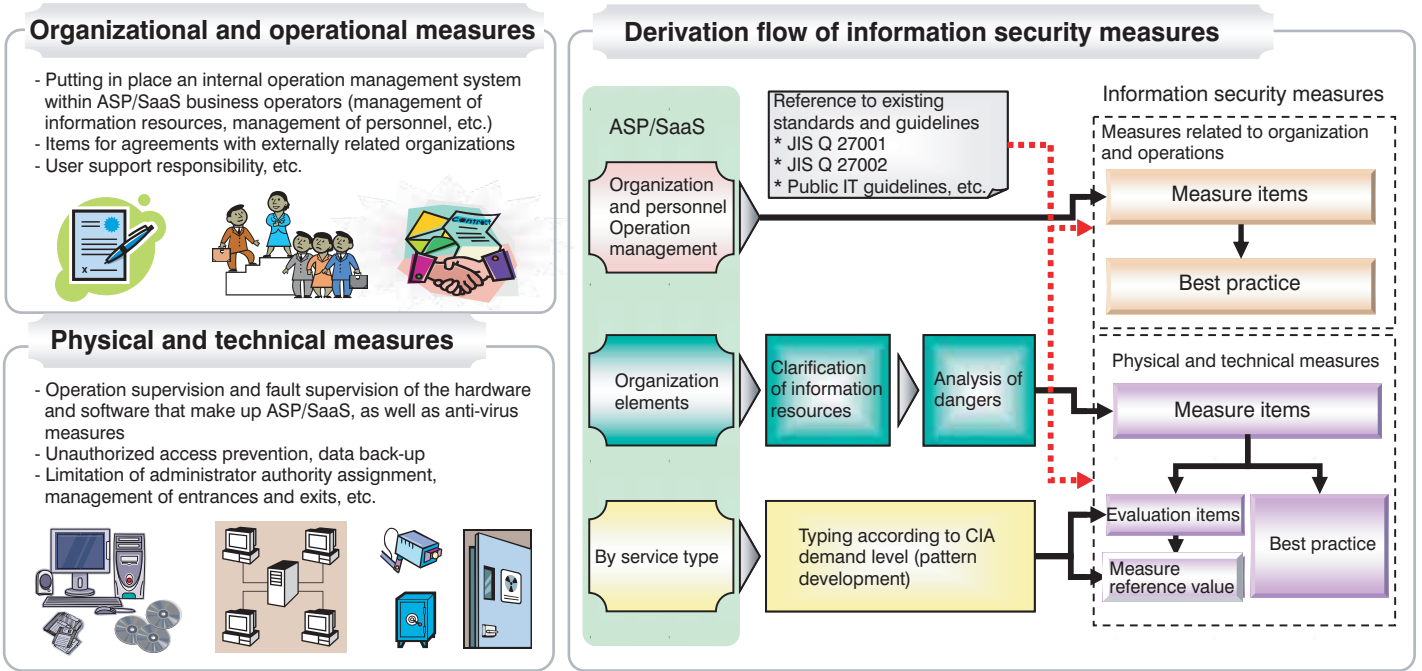
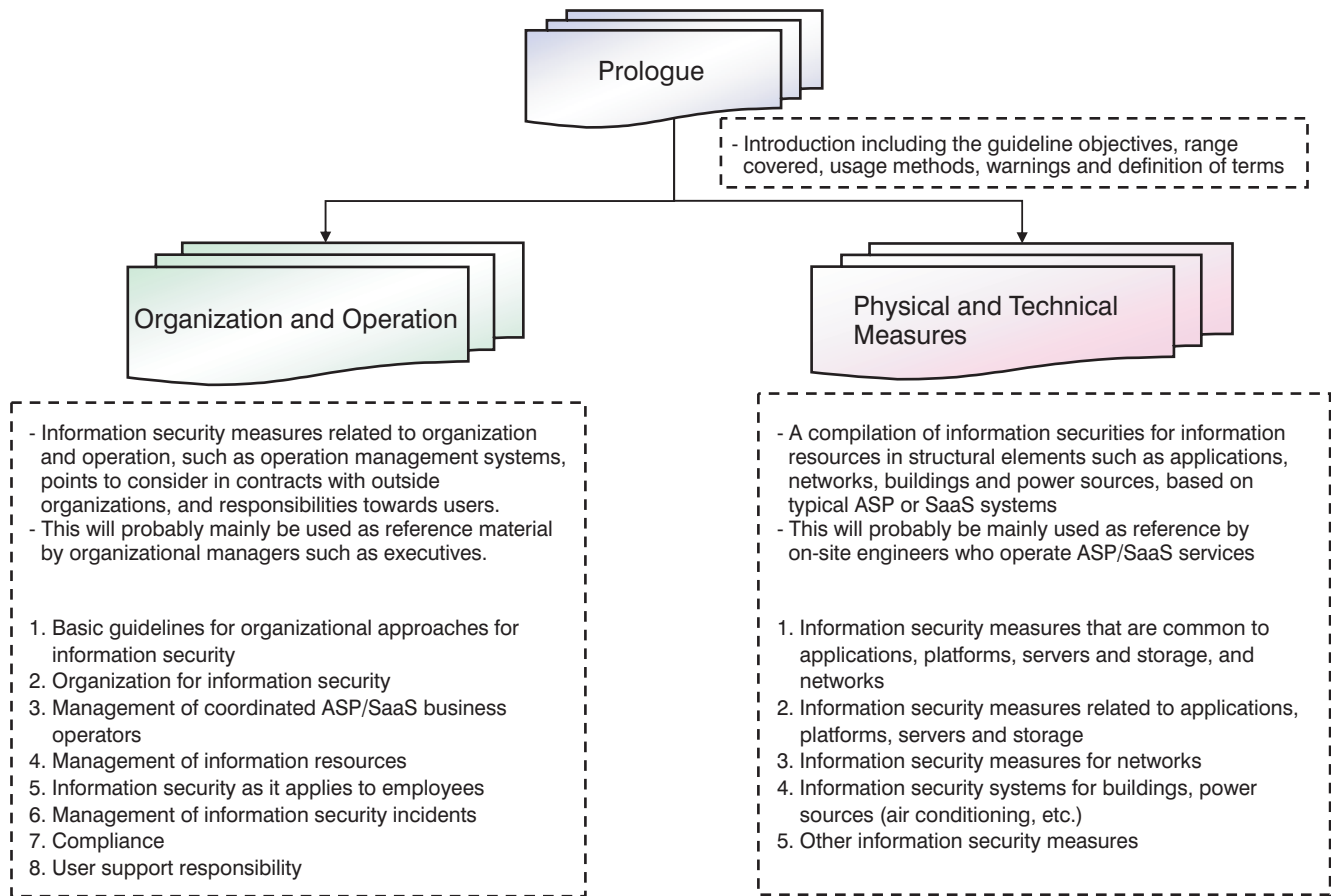


Figure 5: Structure and outline of guidelines

- Overall target of information security measures that should be implemented when ASP/SaaS business operators provide services.
- In order to encourage pro-active and wide-ranging use, produced while taking care to make them as easily understandable and as easy to use as possible, and divided into three parts, the "prologue," the "organization and operation," and the "physical and technical measures."



The Effects of Proper Use of the Guidelines and Future Topics

(1) The effects of proper use of the guidelines

By using these guidelines effectively, the following results can be expected both for the ASP/SaaS business operators and for the service users.

- o The promotion of the implementation of appropriate information security measures that are in line with the characteristics of the services provided, and the development of approaches for small and medium-sized operators as well as new entrant business operators (ASP/SaaS business

operators).

- o They can be used as guidelines for desirable information security items with regard to business operators that coordinate to offer services (ASP/SaaS business operators).

- o They can be used as guidelines for the contents of the information security measures implementation status that is provided to users (ASP/SaaS business operators).

- o They can be used as guidelines when evaluating the appropriateness of the state of implementation of information security measures by ASP/SaaS

business operators (service users).

- o Overall information security levels can be improved by receiving a service in which appropriate information security measures have been implemented (service users).

With these results of effective usage, there is a move towards the improvement of information security levels for the ASP/SaaS industry as a whole, as well as an increase in awareness of information security, including among users, with the expectation of vitalization and a healthy development for the ASP/SaaS industry.

Figure 6: Results of effective usage of guidelines and future topics

- The vitalization and healthy development of the ASP/SaaS industry can be expected as a result of effective use of the guidelines.
- Therefore, the wide-ranging penetration of the guidelines and their ongoing revision and amendment in response to changes in the ASP/SaaS usage environment are necessary.

The results expected from the effective use of the guidelines

- The promotion of the implementation of appropriate information security measures by ASP/SaaS business operators (promotion of the development of approaches for small and medium-sized operators as well as new entrants)
- Usage as guidelines for desirable items for information security for coordinated ASP/SaaS business operators
- Usage as guidelines for proposed contents for the state of implementation of information security measures for users
- Usage as guidelines for when users evaluate the appropriateness of the state of implementation of information security measures by ASP/SaaS business operators



- Increasing the information security level of the ASP/SaaS industry as a whole, and increasing awareness of information security, including among users

The vitalization and healthy development of the ASP/SaaS industry can be expected

Future Topics

- Wide-ranging promotion of the guidelines
Proactive usage within the industry as well as a greater awareness of the guidelines are expected, not just as guidelines for implementing measures by ASP/SaaS business operators, but as standards for setting SLA in contracts with users, or announcing the state of implementation to users

- Revisions and amendments in response to changes in the ASP/SaaS usage environment
In conjunction with changes in the environment surrounding ASP/SaaS, such as technological advances, there is the fear that the contents of the guidelines will become dated and will no longer be relevant to current conditions
A structure is expected for a system of ongoing revisions and amendments

Expectation of promotion of penetration through the ASP/SaaS industry and ongoing revisions and amendments

Conclusion

By making proactive effective usage of these guidelines in the future, centering on the ASP/SaaS industry, the provision of ASP/SaaS services with appropriate

information security measures will be promoted, leading to expectations of the even greater growth as one of the ICT services that lead Japan's economic growth. MIC will continue to provide the

necessary support in looking towards further promoting the penetration of ASP/SaaS as well as improving the level of information security.