Internet Topics: An Introduction to the Managed Security Service (MSS) Selection Guidelines

Here we present an overview of the Information Security Operation providers Group Japan (ISOG-J)*[1], and the “Managed Security Service (MSS) Selection Guidelines”*[2] that they have recently published.

■ About the Information Security Operation providers Group Japan

ISOG-J is an association of security service providers. It was established in June 2008 by a group of service providers that help ensure corporate security as a forum to share information about security operation and resolve common issues. Its diverse membership is comprised of information security vendors, security product vendors, manufacturers, system integration vendors, anti-virus product vendors, and ISPs.

One of the reasons ISOG-J was established was to foster common understanding regarding security operation. Currently, different companies use their own unique terminology for the services they provide, which makes it difficult for customers to select an appropriate service that meets their requirements. Additionally, security operation cannot be accomplished by the service provider unilaterally, as security is improved through a collaborative effort between customers and providers. This means that trouble may occur if there are any differences in perception between them. To remedy these issues and minimize the occurrence of trouble, it was decided that guidelines should be established.

■ Service Map

The “Managed Security Service (MSS) Selection Guidelines” were produced by an ISOG-J working group over the course of two years*[3]. During the first year the security services provided by each company were listed up and categorized, and the results were summarized as a service map*[4]. Because of the differences in approaches to security and service characteristics among the providers that belong to ISOG-J, it was necessary to define the service space covered by the guidelines.

In the service map, services were categorized based on their contribution to IT security over the lifecycle (planning, implementation, normal operation, emergency operation) of the IT system to be protected*[5].

■ Managed Security Service (MSS) Selection Guidelines

By establishing a service map, it was possible for ISOG-J members to exchange knowledge regarding the scope of applicable services and security operation with each other. The Managed Security Service (MSS) Selection Guidelines are a compilation of security service utilization methods based on this knowledge.

The guidelines are comprised of three sections. The first section contains definitions and descriptions of terminology and concepts. The second section explains each stage of the IT system lifecycle (implementation planning, design/construction, normal operation, emergency operation) that was also used for classification of the service map. “Implementation planning” covers the organization of implementation goals and the systems to be protected, methods for determining requirements, and points for selecting services and providers. “Design/construction” presents procedures and points to take note of in order to realize requirements together with providers. “Normal operation” covers the day-to-day dealings that occur between customers and providers such as periodic reporting and changes to configuration. “Emergency operation” contains information about checkpoints, decision making, and implementation of countermeasures to be carried out by both customers and providers when a security incident occurs. Last of all, the appendix presents a number of security incidents as case studies for situations where security services are being used, explaining communication between customers and providers. This gives a concrete picture of what support is available when a service is actually used.

As detailed above, these guidelines contain information about the preparations a customer can carry out before selecting a security service. Through the use of these guidelines, it is possible to compare the services of multiple providers in a fair manner, and avoid the trouble that occurs when both customers and providers make incorrect assumptions. They would be of value both to those who are currently considering the adoption of security services and those who are already using one.

■ Future Activities

ISOG-J is involved in a variety of activities in addition to those presented here, such as studying laws related to managed security services, sharing technical information, training operators, and fostering community among operators. IIJ will continue to actively participate in the activities of ISOG-J to contribute to improvements in security services and the security of our customers.

Author:
Mamoru Saito
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

*1 The Information Security Operation providers Group Japan is also known by the acronym ISOG-J, which is pronounced "ee-sog-jay"(the meaning is “Got to hurry, Japan!”). The owl in the center of the logo symbolizes both wisdom and intelligence, as well as the operators that stand watch through the late hours every day (http://www.jnsa.org/isog-j/e/index.html).

*2 Managed Security Service Selection Guidelines (http://www.jnsa.org/isog-j/activities/result.html)(in Japanese). As services that provide managed security are often called Managed Security Services (MSS), the notation "MSS" is also used in the guidelines.

*3 The following presentation contains details regarding the sequence of events leading to the formulation of the guidelines and their content (http://www.jnsa.org/seminar/2010/0611/data/1-A_2.pdf) (in Japanese).

*4 The service map has also been published on (http://www.jnsa.org/isog-j/activities/result.html)(in Japanese).

*5 In this map, many distinct services and features such as anti-spam measures, secure file-sharing methods, and physical security measures such as those using IC cards are classified as "other." This is due to the objectives behind the creation of the map, and it must be noted that this does not mean that the role they play in security is small.