03 OKI's Information Security as a Leader in the Information Society

Enhancing Information Security Systems and Implementing Effective Security Measures

OKI Group's Efforts for Information Security

As the integration, networking and mobility of information systems have become indispensable for corporate activities, there has been a growing focus on the importance of dealing with new risks. According to the Information Technology Promotion Agency, cases of illegal access and attacks on web vulnerabilities have been increasing although the number of viruses detected has been decreasing. Under these circumstances, we need to take appropriate measures against them.

The OKI Group has been long committed to the promotion of information security. While offering its customers various security products and services, it has also been active in enhancing its internal systems to manage information security. For example, we have implemented our security measures from three perspectives as shown in the following diagram since the enactment of the OKI Group Security Policy in fiscal 2002. It is also notable that the divisions responsible for the development and operation of in-house information systems obtained ISMS* certification.

Furthermore, the OKI Group established the Information Security Committee in fiscal 2007 in order to strengthen measures against information leaks. Since then, each business unit of the group has designed its systems to promote information security, developed security plans and taken necessary measures under the supervision of the committee.

*ISMS stands for Information Security Management System.

Establishing Information Security Measures and Disseminating Them to Overseas Business Sites

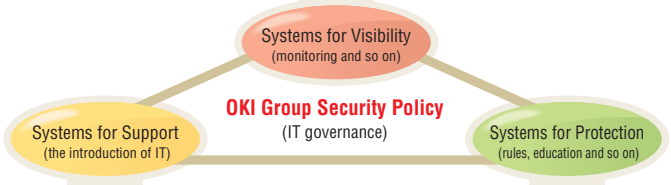
Our activities for information security in fiscal 2008 focused on establishing the measures planned and implemented in fiscal 2007. We put special emphasis on on-site monitoring by the secretariat of the Information Security Committee. The eight business sites

● Information Security Systems Based on Three Perspectives

Monitoring at the security center
Observing how various systems are being implemented and detecting the use of unauthorized software

Protection from computer viruses
Monitoring computer viruses at around-the-clock support centers and providing up-to-date information

Automatic updating of virus pattern files
Automatically updating virus pattern files at every PC/server



Management of confidential data using a shared server
Installing a special server to be shared across the group for storing confidential data and managing access

Development of IT infrastructure
● Restricting data copying from PCs to portable storage mediums such as USB thumb drives ● Encryption of mobile PCs ● Restricting network access to PCs belonging to individual employees ● Enhancing password management

Clarification and definition of data and business processes
Clarifying the distinction between data offered by customers and data to be processed within the company, and defining business processes to obtain, generate or discard such data as rules, and establishing related regulations

Implementation of information security education
● Group training sessions ● e-learning

Tetsuya Izaki

Tetsuya Izaki
General Manager
Information Planning Division

Commitment

The OKI Group has considered and introduced the most appropriate information security measures for its activities in response to changes and breakthroughs in IT through careful examination. On the other hand, we have built a security framework based on the understanding that information security is ultimately ensured by individual employees. We are convinced that the security awareness of each employee has been improved through various efforts made thus far. We will continue to provide security education, and conduct effective inspections and monitoring at each business frontline.

monitored during fiscal 2008 included some branch offices in remote locations, small-scale sites and group companies. During each monitoring session, the implementation of the measures in question was checked while the latest security issues were explained directly to employees in order to improve their security awareness.

We have also started to disseminate our information security measures to business sites in China. Since the IT environment in China is different from that in Japan, we have started adopting an antivirus software program designed for computer viruses detected in China. We have also improved the local help desk function, enhanced support for damage caused by computer viruses, and thus improved the virus elimination rate there.

Improving Security Awareness of Business Partners

In order to provide security to our customers, the improvement of information security of our business partners is also necessary. For this purpose, we have asked the business partners handling important confidential information to self-check their information security using an information security check list designed by us. The 47 check items covering six categories are to be reviewed and revised in response to changes in the information security environment. The utilization of this check list has allowed the OKI Group to share the same security issues with its business partners and thus develop further measures for information security.

Information security check list

Establishing OKI-CSIRT for Prompt Response to Increasingly Complex Security Accidents

In order to enhance our preventive measures against threats to computer security and improve our capacity to respond to them, we established OKI-CSIRT (Computer Security Incident Response Team) as an organization specializing in responding to security accidents in September 2008, and then became a member of the Nippon CSIRT Association. The purpose of the association is to promote information sharing and cooperation between different in-house CSIRTs and help them improve their capacities to respond to security accidents. OKI-CSIRT publishes a report on computer viruses every month and offers technical assistance within the OKI Group while contributing to the Nippon CSIRT Association by promoting the sharing and resolution of security issues among its members through its involvement in the development of guidelines for measures against computer viruses. We will continue to live up to the expectations of our customers, provide them security, and make efforts to build a system to offer technical support for our customers' security accidents.

Voice — Yi Yang

Yi Yang

Assistant General Manager
(in charge of information security)
Sales Division SI Unit
OKI Software Technology

As the types of computer viruses detected in China are different from those found in Japan, we have implemented a set of antivirus measures designed specifically for China since 2008.

In order to promote communication among in-house users, we have our help desk in China, share information on viruses detected with the IT manager at each site, and make various efforts to decrease virus detections. However, we still detect a considerable number of virus infections via USB thumb drives. In order to restrict the use of external storage devices and enhance our internal oversight, we have been working to introduce a system that can be used in Chinese.

We will continue to make our utmost efforts to maintain a robust and safe IT environment as a member of the OKI Group.

Column — Information Security-conscious Products that Protect Customers

A3 Color Multifunctional Printer with Security Functions

The MC860dtn and MC860dn A3 color multifunctional printers launched in October 2008 feature a variety of security functions. Among them are "Access Restriction" which allows the restriction of functions accessible to each user, "Job Erase" that automatically erases printed data saved on the hard disk, "Encrypted Authentication Printing," and "Forcible Printing of Logon Information." In addition, the printer is very friendly to users with a voice navigation function and a touch panel.

Robust LAN System with a Firewall Function

OKI Networks, a provider of global products for telecom networks, also offers solutions for increased communication security. One of them is the ARUBA Series, wireless mobility controllers with a firewall function manufactured by Aruba Networks that allow the control of the access right of each user, the flexible restriction of access depending on the characteristics of each employee, and the provision of internet services to guest users. They ensure the highest level of security and mobility in the world.