Establishing and continuously enhancing information security systems living up to the corporate vision, "OKI, Network Solutions for a Global Society"

Masayoshi Matsushita

CIO
Executive Managing Director
(Chairman of Information Security Committee)

There cannot be perfect information security no matter how hard we work to improve our security systems. What ultimately matters is how each individual recognizes the importance of security. As the capacity of personal computers used for day-to-day business processes has dramatically increased, people are able to store vast amounts of information in their PCs. In order to help each employee of the OKI Group realize that information itself is an "asset," we make constant efforts to increase security awareness and sensitivity. We have also reexamined the role and necessity of personal computers, and are considering introducing a thin client* system in which individual users do not store data in their PCs.

* The term "thin client" here means a system architecture in which client computers have only minimum capability and all significant processing occurs on a remote server.

The Importance of Information Security in the IT society

As the integration, networking and mobility of business processes have become indispensable for corporate activities, some new risks have come to the fore, such as unauthorized access through security holes and damage by computer viruses. According to the Information Technology Promotion Agency, more than 34,000 cases of computer virus damage are reported every year although the number of viruses detected has been decreasing. Furthermore, there have been many leaks of personal or business information through P2P*1 file-sharing software in the last few years. Under these circumstances, dealing with such security risks has become increasingly important for firms.

The OKI Group, as a provider of network solutions for a global society, has been committed to the promotion of information security for a long time. 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, the group defined the OKI Group Security Policy in 2002, and the division responsible for the establishment and operation of in-house information systems obtained ISMS*2 certification.

However, in September 2006 it came to light that some personal and business information belonging to a group of customers had leaked out to the Internet through a PC owned by an employee of the OKI Group. The employee was using the Winny file- sharing software with his PC. The OKI Group took this incident seriously and formalized a group-wide policy for preventing further information leaks. The entire group will continue to enhance its security systems to ensure safe, secure information management.

*1 P2P (peer-to-peer) communication is a style of direct communication between two personal computers.
*2 ISMS, that stands for Information Security Management System, is a standard commonly known as ISO27001 (ISO/IEC27001 2005). It was published in October 2005 by the International Organization for Standardization.

OKI 's Efforts for Information Security

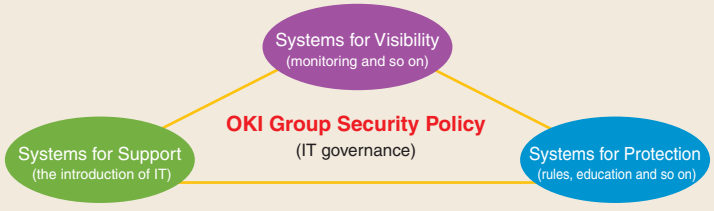
Believing that a comprehensive approach is necessary to ensure information security, the OKI Group makes various efforts based on the three perspectives shown in the following diagram in accordance with its OKI Group Security Policy for Information Security.

● 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

The Information Security Committee and Strict Security Management Across the Group

The OKI Group was very active in preventing information leaks during the fiscal year ended March 2008 in accordance with its plan for the entire group shown in the following table.

In order to disseminate the systems to prevent information leaks among all people using the group's information infrastructure (including the executives, permanent employees, part-time employees, and temporary staff of each member company), the group established the Information Security Committee in May 2007. After briefing sessions were held at all business units, each business unit designed a system to promote information security and developed its security plan (See Page 22).

The entire OKI Group will continue to make every effort to ensure information security and build trust.

● Main Activities for Information Security in the fiscal year ended March 2008

Main Activities	Description	4	5	6	7	8	9	10	11	12	1	2	3
Establishment of the Information Security Committee	·Approving the security policy and activity plan for 1H of 2007		▼										
Development of security measures for the entire group	·Determining related regulations, a work flow to be followed, and IT to be used		→										
Holding briefing sessions at all business units	·Explaining procedures for preventing information leaks and other tasks common to all business units			→	→								
Establishment and implementation of each business unit's plan	·Developing plans to promote security and making a schedule for the plan				→	→	→	→	→	→	→	→	
Establishment of an information security portal	·Disclosing security measures to be carried out across the group				▼								
Information security education	·Disseminating security measures to be carried out across the group through e-learning							→	→	→			
General checkup across the group	·Inspecting how security measures are being carried out							→					
Meeting of the Information Security Committee for 2H of 2007	·Reporting the activities in 1H / approving the activity plan for 2H							▼					
Information Security Audit	·Conducting an information security audit by Internal Auditing Division									▼			

Employee Perspective

Tae Nabeyama

Enterprise Solutions Division
System Solutions Company

Since our main job is to offer IT solutions to various customers in various industry sectors such as transportation, tourism, distribution and manufacturing, we handle a large amount of diverse information. In order to carry out security measures, we first carefully examined which information was subject to our information security management, and then held briefing sessions for the entire division.

As some of our security measures involve inconvenience, such as restrictions on data copying from PCs to portable storage mediums, they cannot be effectively implemented and disseminated unless each member of the division understands their importance. As we went through repeated briefings, each member of the division became more conscious of the significance of information security, thus helping us promote our security measures. We will continue to improve our systems to further promote information security.

Column

Security Products That Protect Customers

Color LED Printer with enhanced security features

The OKI C8800dn color LED printer features various security functions such as authenticated secure printing using a contactless smart card that prevents information leaks from printed data or documents. An optional security kit Type A for the printer allows the encryption of print data stored in the hard drive.

The C8800dn module with this security kit has been certified ISO/IEC 15408 (EAL3).

Iris Recognition Middleware for Mobile Devices

OKI's iris recognition middleware for mobile devices is designed to incorporate an iris recognition* function in cell phones or laptop computers. It prevents the improper use of lost or stolen mobile devices, and enables secure authentication for remote access and electronic payment.

* Iris recognition is a biometric system to authenticate the identities of individuals based on the iris patterns of their eyes. The false-acceptance rate of this system is one in 100,000 (one in 1,200,000 if used with an infrared camera).