Remarks for Special Issue on Information Security in Enterprises

Let me start by expressing our gratitude for your patronage of NEC solutions and products. During the 1990's in which companies really began full-scale use of the Internet, we saw the spread of email and Web usage into every corner of corporate activity. As a result of information exchange through email, as well as internal and external Web-based business activities, in recent years the Internet has revolutionized corporate styles and business models on an unprecedented scale. At the same time, the ease with which digitized information can be transferred makes it susceptible to serious problems such as private information leakage, and strengthening information security has become a topic of utmost importance and urgency. This journal featured a Special Issue on Security (only in Japanese) back in 2003 which outlined our efforts in this area, but subsequently new situations and problems have come to light. In order to solve the security related issues that are in a continual state of change, it is important to address them with continued and comprehensive efforts as well as to boost our countermeasures.

Although people recognize that security is a necessity, it is also true that many of them are under the impression that security is complicated and difficult to understand. This is not because security technology is that difficult per se, but rather because security countermeasures are explained vis-à-vis potential threats and therefore it is difficult for the user to grasp the relationship between security and their day-to-day business activities. System and technological innovations in computing and networking have served to drive each other forward, leading to an IT environment that offers high speed, high capacity, wide coverage and ease of use. Security threats appear and attack the vulnerabilities that develop between these new technologies and management. What's more, as IT progresses toward high speed, threats also increase. For example, worms will be able to spread and find information more rapidly. The influences of threats keep changing as threats appear in different locations and situations, so countermeasures must also change according to changing threat (see **Table**). Unless security expert, threats that keep changing in a short period are difficult to understand its influence.

As the year 2000 and a new millennium arrived, we began to see a shift in focus from mainly countering threats from the outside - which was the common case in the 1990's - to the prevention of information leakage from the inside due to human error or by intention, from the standpoint of compliance. Actually, a study by the FBI has shown that

MARUYAMA Yoshikazu
Senior Vice President

80% of security problems occur internally for over a decade. Giving due consideration to this reality, we must be prepared for roughly 4 times the complexity and effort as was needed to remove security problems before by finding appropriate countermeasures.

When it comes to standardized security management at enterprises based on these wicked assumptions, unfortunately it is still deficient at most companies. A situation exists in which, despite taking measures such as encrypting entire PCs, many have found it impossible to completely stop information leakages during these last 2 or 3 years.

In Japan, the private information protection law, e-document law, and financial products transaction law (J-SOX) has taken effect in this day and age where the true nature of corporate compliance conformity is being increasingly scrutinized. We are at a juncture where it is essential to switch from patchwork of conventional incident-driven countermeasures to pursuing the realization of fundamental security measures that make it difficult to create loopholes on a mid- to long-term basis. By incorporating fundamental and comprehensive security measures into their corporate strategies, it will be possible for enterprises to complete their countermeasures quickly and at low cost whenever a

Table Information technology, security threats and countermeasures, correlated with changes in historical background.

Period	Computing technology	Networking technology	Typical threat	Main countermeasure	Background factors
70's	Terminal/Host	Dedicated cable, Dial-up line	Flaker		Industrial espionage
80's	Client/Server	LAN, Initial Internet	Unauthorized log-in, Virus, Virus evolution	User authntication, Vaccine	
Early 90's	3 layer client server	Wider ranging LAN			Joyriding
	Thin client	Online network	Spread of attack tools, DOS, Web Page altering, Worm, Worm evolution	Firewall, Server fortification, VPN, IDS	
Mid 90's	Web	Commercial Internet			
Late 90's	Streaming	Broadband			
Early 00's	P2P		Information leakage	Encryption	Compliance
	Mobile code	Wireless LAN	Phishing, Spyware	IPS, PC management	
Mid 00's	Shared space	Mobile	Bot, Internal crime	Surveillance, Forensics	
Future	Web2.0	Ubiquitous	Spear virus	Integration and coalition of countermeasures	Corporate responsibility
	Grid	NGN	Self-evolving virus	Safe infrastructure	Corporate strategy

threat arises, allowing them to continue regular business operations and offer uninterrupted services, thereby winning the trust of customers.

At NEC, we believe that the only way to eradicate these problems is to dig deep into the fundamentals of these new security issues and provide effective solutions based on that. These fundamentals include:

1) Unambiguous authentication and identity management

Applying constant authentication and prohibiting anonymous usage of the corporate IT assets is the starting point of security management.

2) Managing granular data units in which information is stored

Taking the unit of encrypted information management down to the file level, which is accessed by users on a daily basis, is the core concept.

3) Control through comprehensive management

Comprehensive management that controls and monitors the usage of the IT environment on the scale of user and file, and even audit trail for assurance of the control, will be a must.

4) Multi-layered countermeasures to close up loopholes

It is necessary to create systems that offer countermeasures at multiple layers, so that even if a threat could pass through one countermeasure it will be stopped by another.

5) Business system that verifies security in advance

It is crucial to prepare total systems where security products are integrated beforehand and the absence of vulnerabilities is verified.

6) Effective application of specialization

A system where specialists will assist in developing countermeasures is necessary to flexibly counter threats that are in an unstable state.

In this latest special issue, we will introduce our activities towards the comprehensive and fundamental security measures that will be essential in the future, through specific products, systems, trends such as system integration, as well as case studies. At NEC, we will be applying these products, systems, and system integration technologies to our own operations to further boost their usefulness. And the experience we gain through that will enhance our ability to provide high quality security measures, as well as realizing an environment that allows safe and secure information system usage, and contributes to our customers' business accomplishments.

Thank you for your attention, and your continued support in the future.