Remarks for Special Issue on Security for Network Society

By Koichi IKUMI*

*Senior Vice President

RECENT TRENDS

Cyber attacks by means of viruses and worms are not only increasing in number but infection rates are also speeding up year by year with a consequent aggravation of the effects. This trend sometimes results in the infected systems being incapable of continuing operations over an extensive period of time. Personal information leakage incidents are also tending to be on the increase. The issue has clearly become one of the biggest threats to effective management with average payments for damages currently reaching 550 million yen. This figure represents an average for the 51 cases whose claim damages are able to be estimated out of the 57 cases for the year 2003 reported from the JNSA (Japan Network Security Association).

On the other hand, new network systems are being introduced as a result of an expansion of services using broadband and also because of the dissemination and application of the 'ubiquitous' concept. Network safety and convenience are also posing issues that are related to security.

IN-HOUSE EFFORTS AT NEC

At NEC, we have long been protecting our in-house systems against the various threats.

First of all, we have defined the threats based on IT infrastructures and assets and have in consequence applied the following procedures:

1) Security policy preparation.
2) Thorough promotion of the prepared security policy.
3) Construction of a security management system.
4) Provision of security countermeasures to support the information infrastructures.

With regard to the issue of cyber attack, a security infrastructure called the Cyber Attack Protection System (CAPS) has been developed. This system identifies the status of the information assets in our 200,000 PCs and servers and is used to manage the application of patches and vaccines specifically for clients' PCs and servers. When a PC is discovered to be unprotected, an application of vaccines and patches is recommended. Furthermore, those PCs that apply old patches or ones that are not registered have their connections interrupted.

In the sphere of information leakage countermeasures, we have introduced a system in which the corporate PCs are completely encrypted and even the transference of data to client's PCs is prohibited. The information leakage countermeasures of NEC are referred to as the InfoCage Suite, which is organized based on the concept that it is impossible to transfer the confidential information that is stored in the server, even into clients' PCs. The divisions of NEC introduce the InfoCage components selectively on a case-by-case basis and the circumstances of introduction for each division are identified by using the management function of CAPS as described above.

Preparation of the intranet administration/management system is another key issue. NEC has 4,000 site administrators employed in its in-house departments besides operating the Security

Management Center. They are at all times, ready to apply the emergency system. Surveillance by the Security Management System is performed 24 hours a day, 365 days a year including holidays.

In addition to the Security Management Center, NEC has prepared the inward/outward access management systems based on fingerprints and non-contact IC cards. We believe that this system permits us to manage security more conveniently, more securely and with the support of reliable records.

Moreover, a management cycle consisting of maintenance, administration, education, and promotion and auditing is applied continuously to the above described security countermeasure systems, which are thus protected against new threats.

SECURITY SOLUTIONS PROVIDED BY NEC

By proposing i-BestSolutions/Security as the security solution, NEC is responding to the customer needs by considering the security issue at the following four levels.

(1) Security Management
Security diagnosis, monitoring and handling to reduce customer TCO.

(2) Integrated ID Management
Integration of network authentication to construct a safe and convenient environment.

(3) Cyber Attack Prevention
Countermeasures against cyber attack by viruses, worms or illegal connections.

(4) Prevention of Information Leakage
Countermeasures against information leakages due to the theft or loss of a PC or as a result of an illegal action by an insider.

We also consider issues involving every process from introductory studies to post operation maintenance/administration by responding to the need to protect our business by adopting various viewpoints including: consulting, design & construction, operation, outsourcing and education.

With regard to the need for solutions against the “cyber attacks” that have been increasing recently, we provide CapsSuite, a product that is implemented based on the CAPS used inside NEC. Together with the InfoCage Suite, which is a countermeasure aimed at “information leakage” this product helps meet any urgent needs of customers.

With regard to security management, a Personal Information Protection Law is soon to be enforced in Japan and we are currently holding consultations and developing strategies on how to coordinate the new system with existing IT systems.

EXPANSION OF SECURITY NEEDS

Advancements in information technology have been leading to the creation of various IT devices and services. However, every time a new device or service is created, it is necessary to overcome security holes that may be hidden within it. It is often said that security and ease of operation form a contradictory relationship. However, we are currently solving problems associated with this issue by applying new technologies.

NEC considers that security trends should consist of the following four points:

(1) Advancement of Attack Techniques
Skimming, Phishing, Spyware, Stealth technology, An accelerated development in attack techniques, The consequent increase in aggravation caused by infections

(2) Advancement of Services
Presence tie-up services, Dynamic value chain, Inter-business collaboration

(3) Changes in the IT Environment
Mobile PC, Wireless LAN, Cellular phone mail, Cellular debit phones, The dynamic workplace

(4) Compliance
Personal Information Protection Law, E-documentation

SECURITY EFFORTS BY NEC

At NEC, we are unremittingly identifying current trends based on the above concerns and developing basic and applied technologies in order that we may continue to provide solutions in advance of needs.

With regard to authentication and encryption, we are preparing anonymous signature and multiple signature technologies as well as the PKI.

Fingerprints are used not only for authentication but are also useful for identification in police work and we are also developing face authentication as another biometric technology. The technology for real-time detection of suspicious or irregular behavior is expected to be applicable in countermeasures against cyber attacks and information leakages. Quantum encryption with a bugging detection capability is a technology that is useful in the sphere of highly confidential communications.

NEC's intention is to gain experience of the construction, maintenance and administration of systems and to consider them in the context of solutions to the security of customer issues, so that optimum solutions can be provided . This strategy will be based on the in-house performance of the entire NEC group.

Our technical development is of course not limited to the field of technology, we are also pursuing the most advanced applications of information technology as a corporate commitment.