Secure Technology

Tomoo Fukazawa†

Abstract

This article describes technological trends related to cyber security for achieving safe and secure communication network environments in the broadband/ubiquitous era and introduces our research and development efforts on subjects such as countermeasures against distributed denial of service (DDoS) attacks, encryption/authentication techniques, and NTT-CERT security management.

1. Growth of security awareness

The number of broadband subscribers is continuing to grow and reached approximately 17.6 million as of September 2004. In particular, subscriptions to optical fiber services exhibited a sharp increase over the previous year and now account for more than 10% of all broadband subscriptions. At the same time, the scope of broadband usage has also broadened, with the pattern of Internet usage in households showing a sharp increase in personal finance activities such as online shopping, auctions, and banking in addition to ordinary activities such as data acquisition and email.

So what sorts of concerns do ordinary users have concerning the forthcoming ubiquitous society? Although one might expect viruses to appear at the top of the list, it turns out that most concerns are related to security issues such as damage caused by fraud and scams and by the misappropriation and illegal use of personal information. Meanwhile, security-related issues such as personal data protection and network security risks are also viewed by businesses as being more important than cost. This reflects the social background of rising hi-tech crime, especially problems associated with emails containing fictitious demands, which have grown rapidly since 2003.

Under these circumstances, it goes without saying that businesses must all concentrate on strengthening various security measures. Popular tools for this purpose include firewalls for preventing unauthorized access from the Internet, anti-virus systems, authentication servers, and authentication devices for client systems. There is also a growing incidence of activities such as “phishing” (obtaining personal information by masquerading as a legitimate company) and website forgery, which has led to a growing demand for other forms of filtering software besides anti-virus software. In addition to introducing these individual products, it is also rapidly becoming more important to manage overall security strategies, including vulnerability testing and policy testing.

Looking at the state of introduction of these tools, we can see that although essential products like firewalls and anti-virus systems have been widely adopted, products related to security management have still only been partially introduced. Moreover, this field is expected to become even more important in the future (**Fig. 1**).

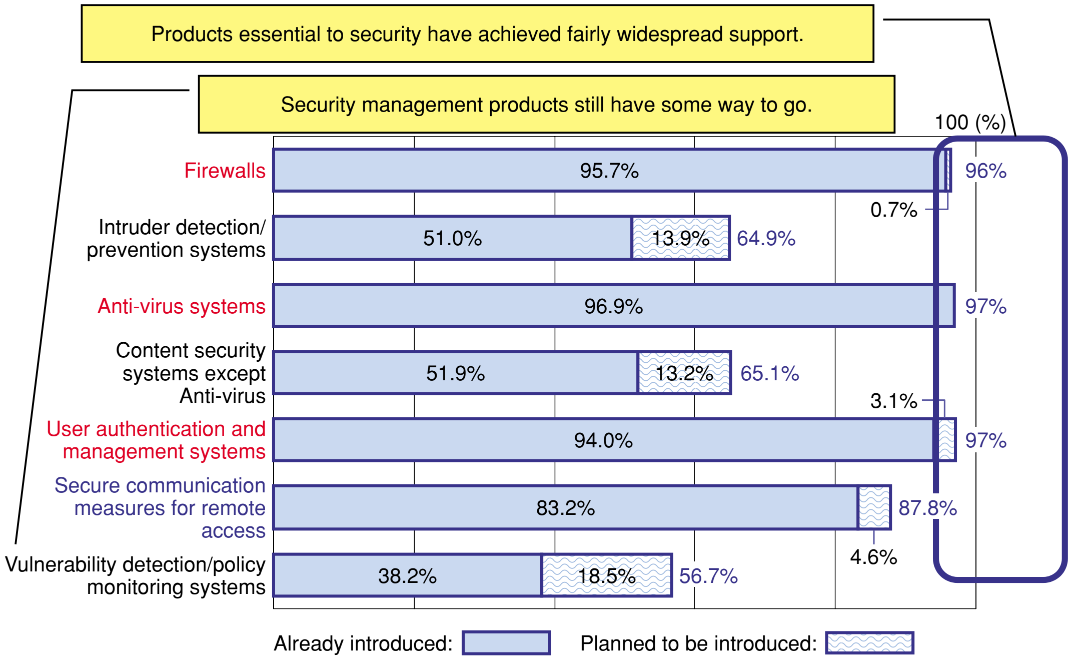
2. Some recent examples of security issues

The mechanisms employed in the main forms of hi-tech crime are briefly reviewed here.

(1) Phishing

In a phishing attack, the perpetrator sends out an email containing a link to a fake website. This fake

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: fukazawa.tomoo@lab.ntt.co.jp



(Source: JNSA survey "Introduction and implementation of IT security measures and their satisfaction levels," 2005)

Fig. 1. State of introduction of security tools.

website, which is designed to resemble the website of a legitimate organization, instructs users to enter personal information such as bank account details. Since phishing relies on a combination of several elements such as emails and websites, it must be dealt with by a comprehensive set of countermeasures. Countermeasures taken at the user end are the most important in this respect.

Countermeasures for users

- Do not divulge personal information
- Identify incoming mail
- Confirm URLs

Countermeasures for service providers

- Use a screen configuration that is difficult to counterfeit
- Eliminate vulnerabilities
- Use server authentication
- Collect information about phishing sites
- Adopt a comprehensive strategy including continuous monitoring, adaptation and cooperation

(2) Distributed denial of service (DDoS) attacks

In this form of attack, the attacker sets a virus which starts sending abnormal packets to a target server at a predetermined time. This virus continues to infect other systems all over the world until the attack starts. When the attacking time is reached, the infected systems start sending malicious packets to the target server, which goes down under the huge amount of abnormal traffic received simultaneously from all over the world.

Network countermeasures

- Network monitoring
- Manual investigation of cause
- Manual network control
- Collaboration between ISPs

(3) Leakage of information

Information can leak out in any number of ways. Electronic leakage can result from human activities such as eavesdropping or impersonation, from system failures caused by virus infections, or from the copying of data from terminal equipment or external media, for example. Physical leakage can be caused by theft, illegal break-ins, and so on. It could thus be argued that recent security issues involve many different factors, and it is no longer possible to address them with a single tool or system. Instead, a comprehensive set of countermeasures must be employed (**Fig. 2**). Also, whereas the bulk of hi-tech crime used to be perpetrated largely as a way of attracting attention, these days it is tending to shift towards crimes that cause financial loss or economic damage. It should be remembered that new problems may still arise even after all the countermeasures currently available have been taken, so continuous monitoring, updating, and management are essential.

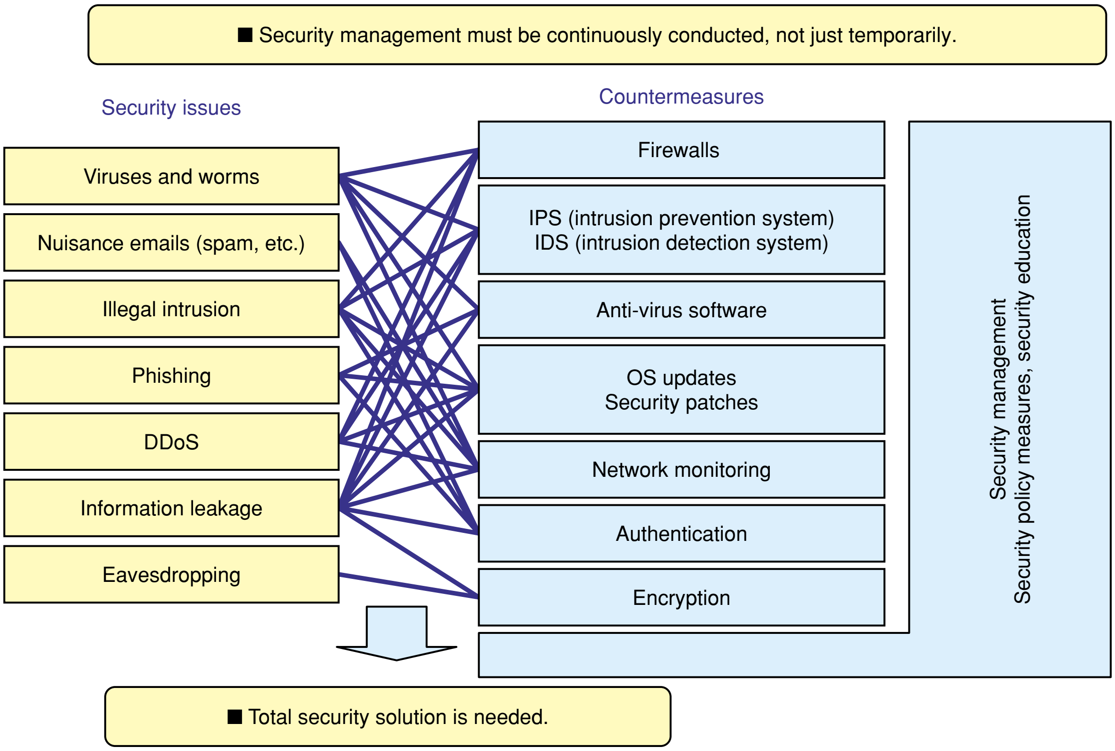

■ Security management must be continuously conducted, not just temporarily.
Security issues
Countermeasures
Viruses and worms
Nuisance emails (spam, etc.)
Illegal intrusion
Phishing
DDoS
Information leakage
Eavesdropping
Firewalls
IPS (intrusion prevention system)
IDS (intrusion detection system)
Anti-virus software
OS updates
Security patches
Network monitoring
Authentication
Encryption
Security management
Security policy measures, security education
■ Total security solution is needed.

Fig. 2. Countermeasures to security issues.

3. NTT's R&D activities

With the imminent arrival of the broadband/ubiquitous era, it is no longer possible to avoid security issues. At NTT, we are therefore working on various security-related issues. These are introduced below.

- Bearing in mind that security is an issue of far-reaching importance, we are conducting comprehensive security research and development at all levels ranging from security core technology to secure content and applications.
- We are developing total security countermeasures that include security management strategies as well as secure systems.
- In addition to defensive security measures, we are also developing technologies for advanced security services that will stimulate demand for ubiquitous network-based services.

Specifically, the following technologies and activities are introduced in this article: an application security system called Privango, network security systems such as MovingFirewall and SCN (storage centric network), technology platforms for authentication and encryption, and security management activity of NTT-CERT team (**Fig. 3**).

(1) Privango mail system

This technology is aimed at preventing nuisance email. Users enter fixed usage conditions into the Privango mail system and are issued with an email address containing their Privango conditions in encrypted form. By using this email address for purposes such as website registration, they can avoid the risk of having their primary email address or personal information being misappropriated. When email is sent to a Privango email address, the mail server judges the correctness based on the conditions specified by the user, and the user only receives valid emails.

A Privango email address might look something like this:

fukazawa.ua4vwpfbtfzz2as@privango.ne.jp

Here, the part before the "@" symbol consists of a nickname followed by a dot "." and a string in which the mail usage conditions are encripted. The nickname is a unique identifier for each user, while the usage conditions contain information such as an expiry date and sender restrictions in the encrypted form. Only a pair of the identifier and the original email address are kept in a database and the mail usage conditions including the user's private information are not stored in the database. Accordingly, even if someone manages to work out how these

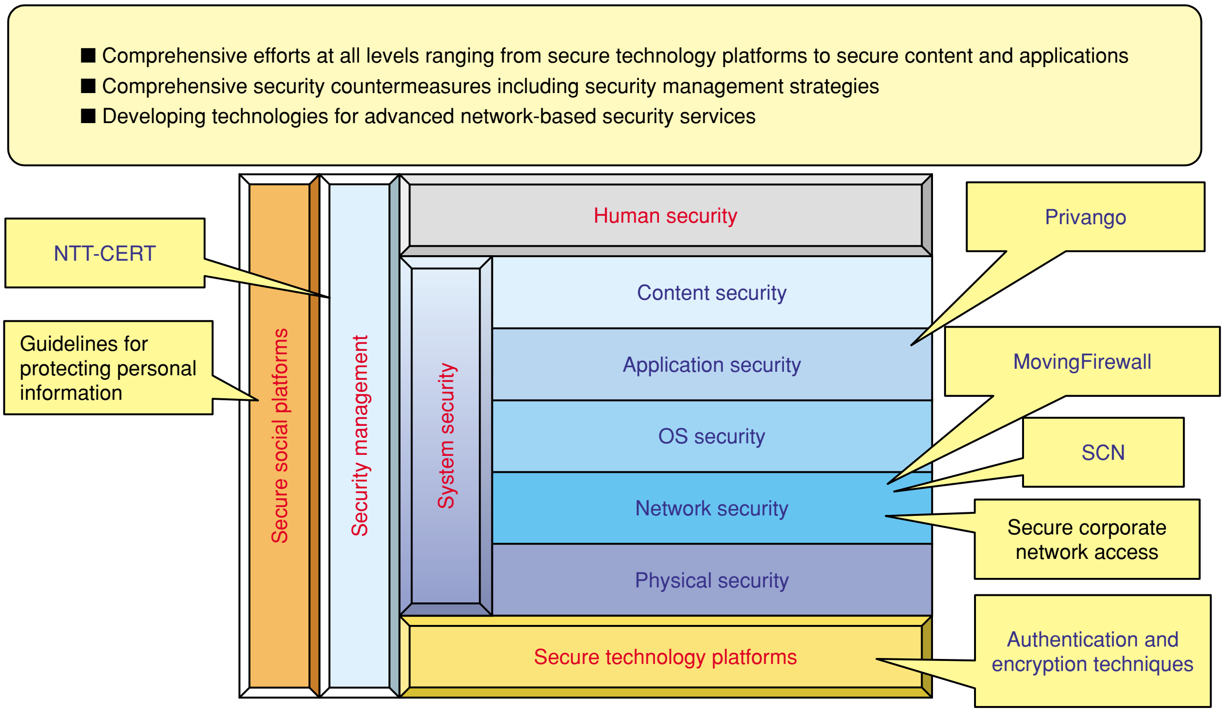

■ Comprehensive efforts at all levels ranging from secure technology platforms to secure content and applications
■ Comprehensive security countermeasures including security management strategies
■ Developing technologies for advanced network-based security services
NTT-CERT
Guidelines for protecting personal information
Secure social platforms
Security management
System security
Human security
Content security
Application security
OS security
Network security
Physical security
Secure technology platforms
Privango
MovingFirewall
SCN
Secure corporate network access
Authentication and encryption techniques

Fig. 3. NTT's R&D efforts.

email addresses are generated, no private information will be released.

For example, imagine you want to subscribe to an online competition on a website. Using the Privango service, you can register an email address that is set to expire in, say, one month, and use this email address when applying to the website. Any mail sent to this address during the next month will be redirected to your original email address, but any mail sent after the expiry date will be discarded by the Privango center instead of being delivered to you.

In the future, this technology could be extended to services such as the following:

- Cellular phone text messages (when exchanging text details with people for the first time)
- Preventing misappropriation of customer email addresses (any email addresses that leak out can be immediately invalidated)

To study the efficacy and convenience of the Privango mail system, we have been operating a public trial service. As a result, about 40% of the 614 respondents said that Privango mail had for the first time enabled them to use online services such as competitions, data banks, bulletin boards, and auctions that they had hitherto refrained from using due to fears about data safety. As this data shows, we have confirmed that providing a reliable means of online communication has a positive effect to increase the range of web application services that people are prepared to use. Furthermore, 98.05% of respondents said they would consider using a commercial service of this type (29.81% said they would be willing to pay for it, and 68.24% said they would use it if it was free), indicating a strong willingness to use the service.

(2) MovingFirewall

This technology offers countermeasures against DDoS attacks with the aim of defending networks. MovingFirewall equipment is installed at each edge of a network. When a data center is subjected to a DDoS attack, the MovingFirewall equipment (i) detects the DDoS attack at the targeted location, (ii) transfers the detected information upstream where defensive action can be taken, and (iii) traces back to the originating user to stop the DDoS attack with a MovingFirewall close to the source of the attack. In this way, traffic from regular users can be preserved and quickly put back to normal.

This technology also automates the collaboration between ISPs that has previously relied on human operators in most cases.

A number of practical trials of MovingFirewall technology have already been conducted. Since even in a DDoS attack, the protocols are relatively ordinary, the presence of an attack is detected based on abnormal traffic levels. This is currently performed by network operators monitoring the traffic, but we have confirmed that MovingFirewall technology is just as capable of detecting DDoS attacks as human operators. It can also be equipped with detection functions corresponding to known attack patterns and can dramatically reduce the time it takes to respond to a DDoS attack. This leads to a reduction in the server down time when a DDoS attack is made.

But having said that, it would not do to suddenly deploy this equipment on networks throughout the world. Instead, we envisage a gradual expansion of the service area based on the following sequence of steps:

Step 1: Services for protecting corporate networks at the edges between data centers and ISPs.
Step 2: DDoS defense services inside ISPs.
Step 3: DDoS defense services between ISPs.

At the same time, we are concentrating on improving the functions used to detect and control abnormal traffic.

(3) SCN (storage centric network)

The key idea of SCN is to move all the disk storage in PC (personal computer) to a centrally managed storage server deployed in a data center. With this structure, SCN performs two main functions:

- Consolidating all the PC environments (operating systems, applications, and data) into the remote storage using a broadband IP network.
- Eliminating the need for storage media in PCs and providing secure data access and total backup.

In current networks, businesses have various issues to consider in the office environment, such as preventing data leaks, reducing PC administration costs, and recovering from natural disasters. SCN technology does away with local disk storage. Instead, all the data is sent via a fast broadband IP network to a data center where the storage is centrally managed in the network. This has the effect of solving the conventional problems by providing benefits such as the following:

- The PCs have no local storage, which prevents data leaks even if a PC is stolen.
- Security updates can be implemented more reliably through centralized administration of the PC environment.
- Entire systems can be easily backed up to facilitate disaster recovery.

(4) Single sign-on

This technology provides an authentication system that works as a security platform. As web services diversify, users end up having to set IDs and passwords for the authentication systems of each individual service provider, and in many cases these IDs and passwords are different each time. This situation is exacerbated by the need for different IDs and passwords in different environments—e.g., at work, at home, and outdoors on mobile terminals—and as a result users can become overwhelmed by a number of IDs and passwords they have to memorize.

This situation can be addressed by an authentication platform that authenticates users with a single sign-on procedure. With this technology, users simply log in to a dedicated authenticating organization with a single ID/password combination. Thereafter, the authorized ID is linked between this authenticating organization and each service provider. This eliminates the need for users to log in to and out from each service provider, leaving them free to use a succession of other services without having to bother about authentication procedures each time (**Fig. 4**).

Secure techniques are also employed when information is exchanged to link IDs. The authenticating organization and service provider organizations do not exchange actual IDs; instead, they swap information by substituting them with aliases (random character sequences) so that the true ID information cannot be misappropriated. If there are multiple service provider organizations, then they will all use completely different aliases, which has the advantage of preventing information leakage between these organizations and making them highly independent from each other.

Since this ID linking technique will not function without the support of many service provider organizations, it is essential to get others to cooperate. Standardizing the system is another important theme and we are also working on this.

(5) Encryption techniques

We have a long history, more than 20 years, of research into cryptography. During this period, the technology has evolved from 64-bit block ciphers to 128-bit block ciphers, and two new encryption techniques called Camellia and PSEC-KEM have been under development and are almost ready to use (**Fig. 5**).

These two techniques use different types of encryption. Camellia is a common key encryption technique which is used for ordinary data. It requires a fast encryption algorithm and can be implemented in hardware to reduce processor overheads. On the other hand, PSEC-KEM is a public key encryption technique in which the cryptographic keys of common key encryption are themselves encrypted during

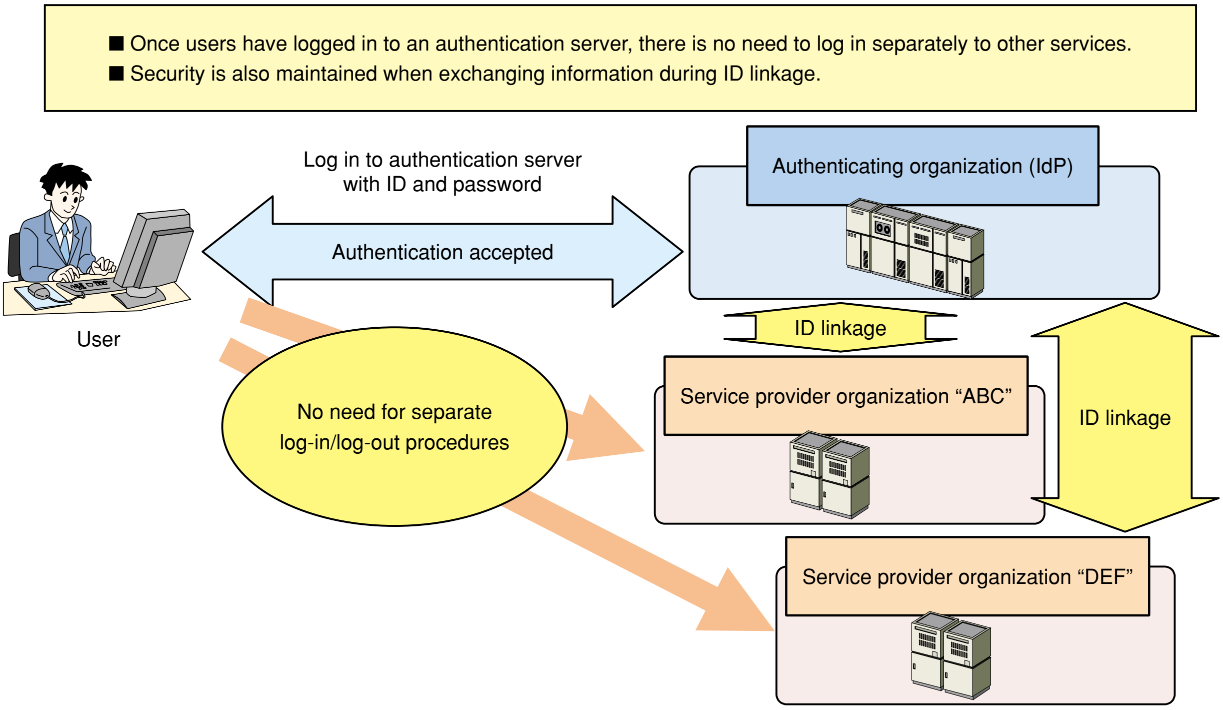

■ Once users have logged in to an authentication server, there is no need to log in separately to other services.
■ Security is also maintained when exchanging information during ID linkage.
Log in to authentication server with ID and password
Authentication accepted
Authenticating organization (IdP)
User
ID linkage
No need for separate log-in/log-out procedures
Service provider organization "ABC"
ID linkage
Service provider organization "DEF"

Fig. 4. ID-linked single sign-on technology.

Encryption technique	Main applications	NTT's encryption scheme	Features	Other useful schemes
Common-key encryption	Encrypting data (faster than public-key encryption)	**Camellia**	• A next-generation 128-bit block cipher that strikes a balance between security and performance • A unique form of encryption developed in Japan, equivalent to AES	**AES**
Public-key encryption (key delivery)	Secure delivery of encrypted public keys	**PSEC**-KEM	• Public-key encryption based on an elliptical curve algorithm with proven security • Faster than RSA-KEM	**RSA**-OAEP **RSA**-KEM

■ In the future, we aim to further improve the popularity and brand awareness by promoting open licensing and applications to software packages, IC cards, etc.

■ We are working on next-generation techniques such as public-key encryption schemes with greater security based on completely new principles.

AES (Advanced Encryption Standard) is a symmetric key encryption technique that will replace the commonly used Data Encryption Standard (DES).

Fig. 5. Characteristics of Camellia and PSEC-KEM.

transmission. This is a technique for performing public key encryption on elliptical curves; the security of this technique has been proved by experts.

In the future, we will work towards open licensing and promote the use of encryption in software applications, IC (integrated circuit) cards, and the like, while at the same time we will begin work on developing completely new encryption principles that differ from existing encryption techniques.

(6) NTT-CERT

This is a CSIRT (Computer Security Incident Response Team) activity related to security management. CSIRT is an organization that gathers, investigates, and acts upon reports of computer security incidents. The mission of NTT-CERT is to minimize and if possible completely prevent damage by promptly gathering and disseminating information about security issues (including the discovery of vulnerabilities and the appearance of viruses). At the same time, it has functions for implementing the successive countermeasures and reviewing security policies which lead to preventative maintenance.

NTT-CERT operates by maintaining constant links with other domestic or foreign CSIRT teams and obtains the up-to-date security information. Specifically, its activities include:

- Providing a reliable point of contact
- Supporting the CSIRT structure
- Gathering, analyzing, and supplying security information
- Providing training and educational support
- Conducting research and development on security issues

It would of course be very difficult for NTT Group to maintain security by itself, so establishing links with outside communities is highly important. We have already joined FIRST (Forum of Incident Response Security Team, the world most authoritative forum of CSIRT organizations), and we are continuing to gather information while strengthening our international connections.

In this way, the NTT-CERT team is cooperating with security experts both here and abroad and will continue to perform security management in order to provide safe and secure communication services.

Profile

■ Career highlights

He received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo in 1980, 1982, and 1985, respectively. In 1985, he joined NTT Atsugi Electrical Communications Laboratories. He became a Senior Research Engineer in 1989 at NTT LSI Laboratories. From 1989 to 1990, he was a Visiting Scholar at Stanford University, USA. In 1995, he became a Senior Research Engineer, Supervisor at NTT LSI Laboratories. He moved to NTT Optical Network System Laboratories as a Senior Research Engineer, Supervisor, in 1997. In 1998, he moved to NTT Phoenix Communications Network, Inc. as the Director of Service and Network Operations. He became Executive Vice President of NTT Phoenix Communications Network, Inc. (now NTT BizLink), in 1999. In 2003, he became Chief Technical Officer of NTT BiZLink. In 2004 he moved to NTT Information Sharing Platform Laboratories as the Executive Manager of the Secure Communication Project.