Cyber Security Project for Safe and Secure Network Services

Yoshitaka Kagei, Kazuyuki Nakagawa, Takeshi Tachi†, Masao Takeda, and Tetsuya Nakagawa

Abstract

To respond to various security-related topics for our information-technology-driven society, the Cyber Security Project, which is composed of security producers, is performing a broad range of activities. For example, it is promoting the development of products that take advantage of the latest security technology from NTT Laboratories and Group corporations. It is also supporting the deployment of such products and technical know-how across the Group and studying the types of security technology that will be needed in the future, including performing analyses that go beyond sociological studies.

1. Role of the Project

The Cyber Security Project, which was set up in 2003, consists of a team of security producers who perform a broad range of activities related to security for the entire NTT Group. An overview of the prevailing external environment that is relevant to the Cyber Security Project is shown in **Fig. 1**. Activities

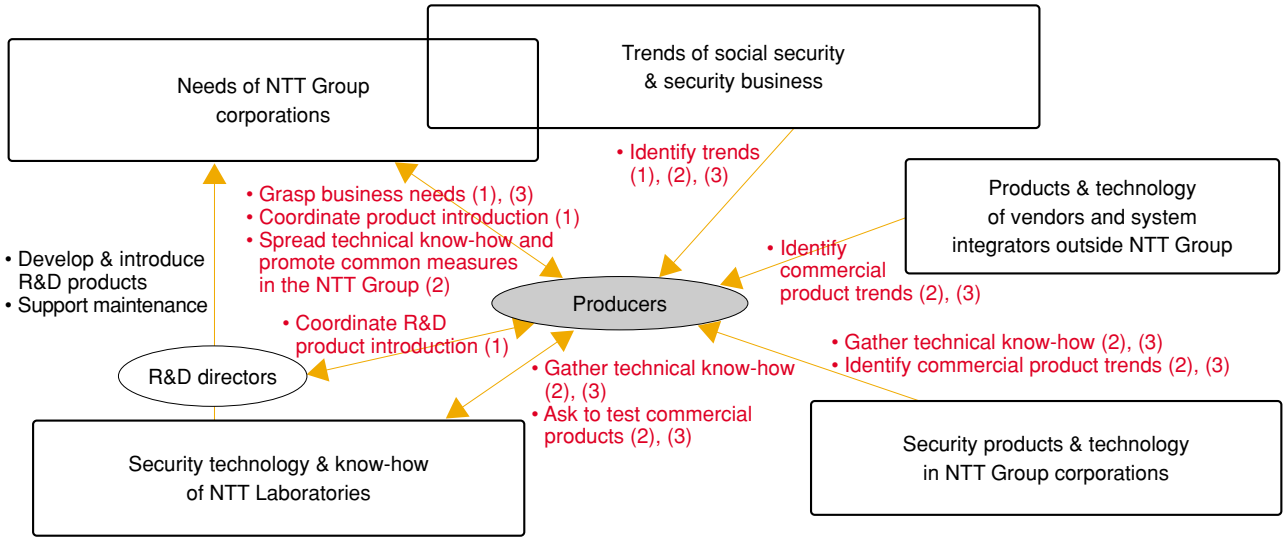

Fig. 1. External environment relevant to the Cyber Security Project.

† NTT Department III
Chiyoda-ku, Tokyo, 100-8116 Japan
E-mail: security-p@ml.hco.ntt.co.jp

include matching the needs of Group corporations to the seeds of NTT Laboratories and promoting measures to cope with security-related issues common to the entire NTT Group. The main needs are for security technology and know-how about IP networks that will help system operators manage the system stably. The project's main activities and results are described in Section 2. By continually observing trends in the world at large from a sociological perspective, the Project works to ascertain the types of security-related businesses that will be in demand in the future and understand the direction of current technological development. Section 3 explains some achievements up to FY 2004.

2. Security development coordination activities

Common patterns in coordination activities can be organized according to their purpose. There are three patterns: (1) commercializing technology seeds in NTT Laboratories, (2) organizing and implementing security know-how within NTT Group, and (3) promoting security measures for NTT Group businesses. Typical activities for each pattern are described below.

Pattern (1): Cultivating and commercializing applications of security technologies created in NTT Laboratories

Pattern (1-1) Applying technology for centralized network profile management to business

In recent years, the computing environment has changed due to an increase in remote access and mobile terminals and the severe damage caused by viruses from terminals connected to the Internet (especially via corporate local area networks (LANs)). The security management and surveillance systems needed to manage terminals and LAN connections are also growing more and more complex and sophisticated. Along with these changes, hidden problems have come to light, such as the difficulty of managing user registration and updates for systems individually introduced to the network and the significant complexity of system settings that needed to be made by the users themselves.

To respond to such issues, NTT Laboratories developed technology for centrally managing profile settings for each of the user terminals and different access networks (e.g., wired LAN, wireless LAN, RAS (remote access server), and Internet VPN (virtual private network)). This secure enterprise network access control system is called SENACS. It lets system administrators perform centralized user management spanning multiple access networks and lets users connect to the internal corporate LAN safely without changing complicated terminal settings (**Fig. 2**). It has three main features: 1) Regardless of the location from which an employee connects to the intranet, SENACS automatically selects the optimum communication protocol; 2) no manual setup is required for network profiles (layer 2/3) for each different terminal or access line, except for an initial installation of terminal software and user profile; and 3) by interlinking to a commercial quarantine system, infected or untested terminals are isolated from the intranet.

To let corporate customers use such advanced technology without confusion, security producers integrate it with complementary systems that are commercially available, such as a quarantine system and an authentication VLAN (virtual LAN). Moreover, this integrated solution is provided to enterprises along with the know-how needed to introduce the system while keeping any changes to customers' legacy infrastructures to the absolute minimum.

Pattern (1-2) Commercializing time authentication and time delivery technologies

The so-called E-Document Law was ratified by the Diet in autumn 2004 and took effect in April 2005. This law allows companies to store tax-related and other official documents in digital format, instead of only being allowed to use paper documents as in the past. *Keidanren* (Japan Business Federation) expects the economic effects of this change to be as high as 300 billion yen. However, in order to store documents electronically under the E-Document Law, it is necessary to construct an infrastructure including document management applications and additional functions, such as a time authentication (timestamp) function and a traceable time delivery function. A time authentication function associates a specific time with each digital document and can prove that the document has not been changed after storage. A traceable time delivery function announces the correct time to the entire network and can be used to confirm the precision with which time announcements were transmitted in the past. To enable each NTT Group company to efficiently develop the document storage management and other related businesses, security producers coordinate activities among

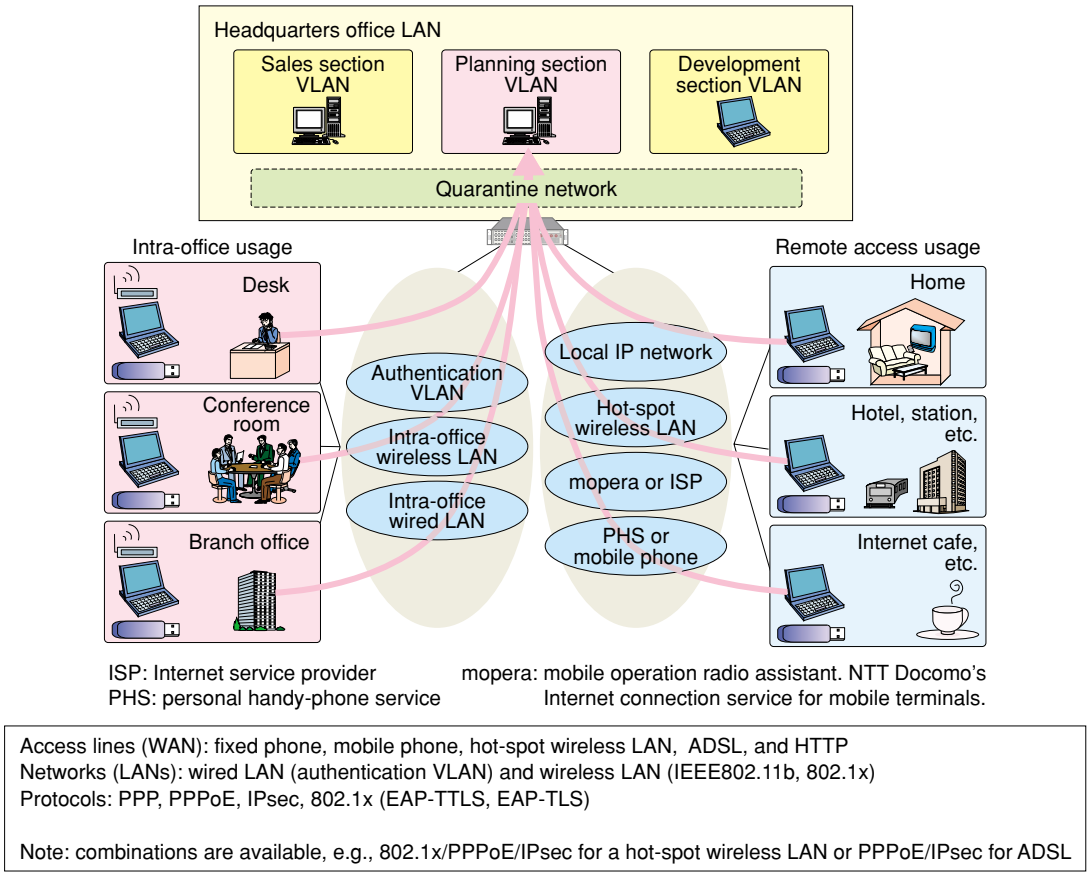

Fig. 2. Overview of the secure enterprise network access control system (SENACS).

Group companies. They promote cooperation between Group companies and the division of responsibilities with regard to the construction of the requisite time authentication and time delivery infrastructure by using technologies developed by NTT Laboratories.

Pattern (2): Organizing security technology and know-how from the community and implementing them within the Group

Pattern (2-1) Systematizing knowledge about information leakage countermeasures

The Personal Information Protection Law, which came into effect in April 2005, enforces a course of actions on companies, municipalities, and in particular divisions within the NTT Group. These organizations need to review their management and security systems, for example those concerning customer data, homeowner data, and employee data, and strengthen measures to prevent the leakage of such information.

Along with the spread of the Internet and personal computers, technologies intended to protect against information leakage have become widespread such as user authentication, encryption of communications, and firewalls. Nevertheless, as new technologies appeared, such as wireless LANs and P2P file sharing software, new risks became visible. Consequently, products and services that provide the technical expertise to deal with these issues have appeared. Recently, these issues have been viewed from a more human perspective, such as the need to monitor terminal operation logs to guard against input errors and unauthorized operation (**Table 1**).

As the complexity and sophistication of measures against information leakage increase, it is growing more and more difficult to make decisions such as which technology or product to use for a specific organization and to what extent protective measures should be implemented. Based on the insights of the NTT Laboratories, security producers have worked to systematize knowledge about the commercialized information security solutions, the lat-

Table 1. Transition of information security management.

Period[*1]		1995–1999	2000–2002	2003–2004	2005–(projected)
Risk #	Major events, social trend / Risk	-Information security risks of IT[*2] became apparent. -Web page interpolations increased.	-Virus infections drastically increased. -Security risks of wireless LAN became apparent.	-Personal Information Protection Law took partial effect. -Phishing damage increased. -P2P software risks became apparent.	-Incident response know-how becomes generalized. -IPR[*5] leakage risks become apparent. -The E-Document Law takes effect.
1	Tapping over network	-email encryption	-countermeasures against wireless LAN		
2	Spoofing over network	-periodical renewal of IDs & passwords	-biometrics -one-time passwords	-electronic certificate -single sign on	
3	Illegal transfer/address error/wrong address over network	-email monitoring -URL access monitoring	-training employees -providing security policy	-document security management -P2P software monitoring -illegal operation monitoring -network forensics	-document originality assurance -information lifecycle management -computer forensics -privacy protection
4	Software weakness of network nodes, servers, and PCs	-countermeasures against Web application weakness -firewall	-desktop management system -IDS[*3], IPS[*4]	-quarantine system	
5	Virus infection of network nodes, servers, and PCs		-access log monitoring		
6	Inappropriate copying of information over mobile PCs or external memory devices		-training employees -providing security policy	-document security management -illegal operation monitoring	-thin client -information lifecycle management
7	Electromagnetic leakage		-cable shielding	-TEMPEST (transient electromagnetic pulse surveillance technology)	
8	Careless printing or taking pictures		-training employees -providing security policy	-document security management	-information lifecycle management
9	Physical intrusion		-biometrics		
10	Inappropriate incident responses (increase the damage)			-network forensics	-document originality assurance -information lifecycle management -computer forensics

Countermeasures against leakage through outside intrusion
Countermeasures against leakage by insiders

*1 "Period" indicates the approximate time of media attention to each countermeasure, not necessarily when they became widely used in enterprises.
*2 IT: information technology
*3 IDS: intrusion detection system
*4 IPS: intrusion protection system
*5 IPR: intellectual property rights

est technologies, and the rules and organizational structures for corporate compliance (**Table 2**). This knowledge base is being used to inspect and strengthen the information management systems of the NTT Group and also as a way to recommend tools to customers. Based on the results of these activities, efforts are also being made to develop educational programs, inspection check sheets and other resources to strengthen the information security infrastructure within the NTT Group.

Pattern (2-2) Creating encryption usage guidelines

Encryption is now used frequently by Internet users. For example, SSL (secure socket layer) connections are used to protect personal information

Table 2. Knowledge base of information security management.

Title	Content	Target readers
Volume 1: Solution map of information security management, 2004	Commercial products and technologies are systematized comprehensively in this map.	1) Sales staff of enterprise security solution business 2) Intra-company security managers
Volume 2: Technology guidebook of information security management	Technical know-how of current countermeasures for information security management is systematized.	1) System designers and operators 2) Sales staff of enterprise security solution business
Volume 3: Guidebook for providing personal information protection rules	Things to be done before the Personal Information Protection Law takes effect are systematized.	1) Staff with the mission of providing intra-company rules 2) Intra-company inspectors 3) Consultants who propose intra-company security management

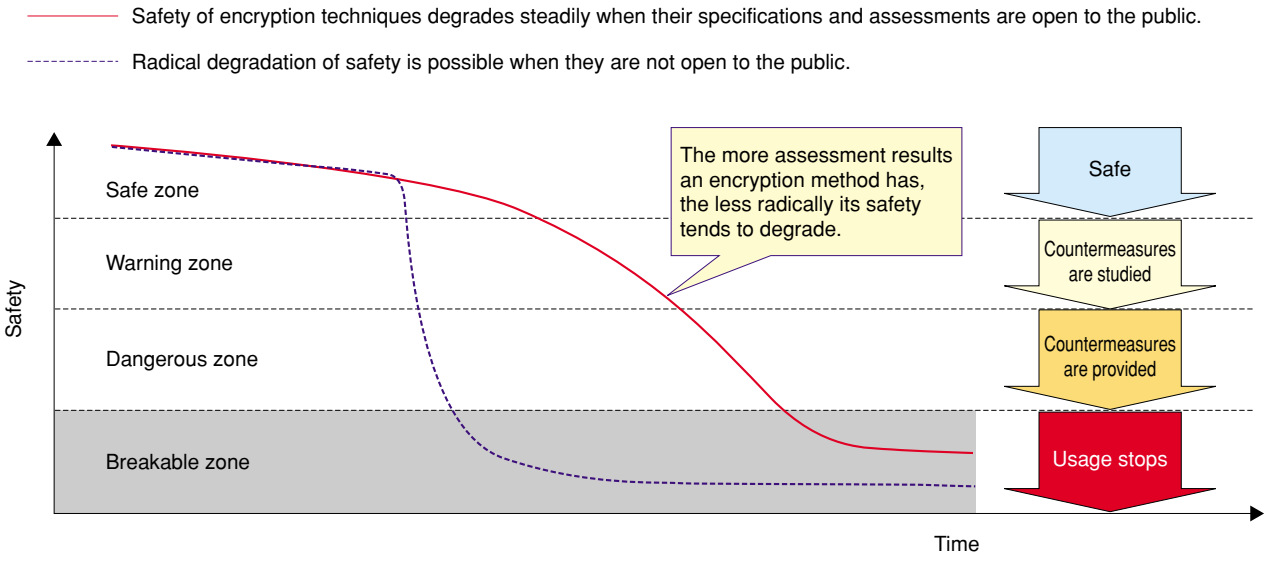

Fig. 3. Degradation of safety of encryption and digital signature.

when making online transactions or when encrypting electronic documents. NTT Laboratories started research into encryption algorithms a long time ago. And algorithms proposed by NTT such as Camellia and PSEC-KEM have been selected for Japan's e-government recommended encryption algorithm list. They have also been designated as selected encryption algorithms in Europe's NESSIE project (new European schemes for signatures, integrity and encryption).

However, improvements in computing performance and the appearance of new decryption technologies may sometimes make it possible to break encryption schemes. In that case, to prolong the safety of products and services, system designers must replace the encryption algorithm or system with a more advanced or secure one (**Fig. 3**). For example, the DES algorithm, which is well known for its use over many years, is not among those on Japan's e-government recommended encryption algorithm list.

To deal with this challenge, security producers have developed comprehensive guidelines based on the insights of the NTT Laboratories specifying procedures for the selection of appropriate encryption algorithms. By referring to these guidelines, all technologists in the NTT Group using encryption technology and related products can accurately understand the safety level of their system and properly select and use encryption technology. At the same time, these guidelines help security managers anticipate how current encryption methods could endanger a service on offer and implement protective measures before failures occur (**Fig. 4**).

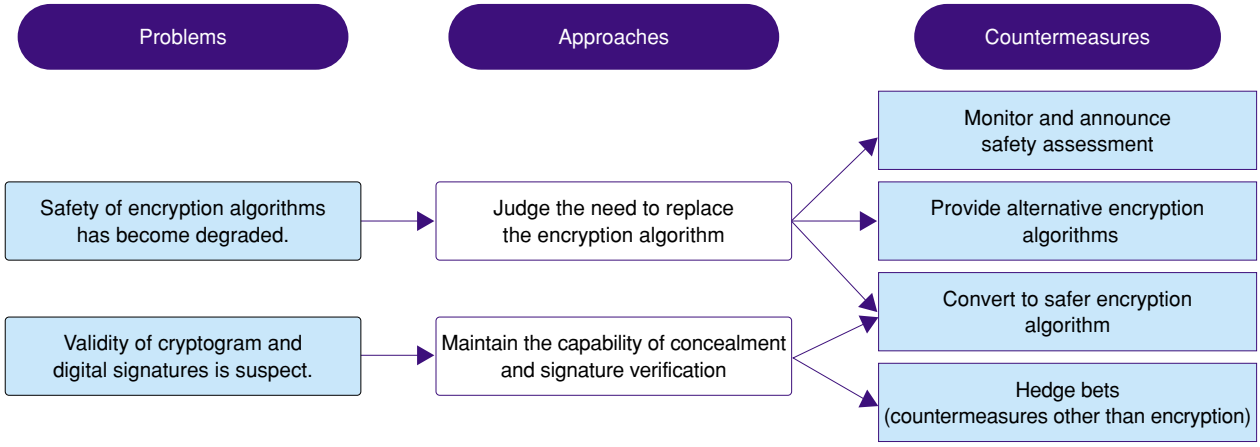

Fig. 4. Countermeasures against endangered encryption and digital signature techniques.

Pattern (3): Promoting measures concerning security topics common to NTT Group businesses

Pattern (3-1) Countering DDoS attacks

To counter the damage caused by distributed denial of service (DDoS) attacks, NTT Laboratories developed a technology for detecting and blocking them called MovingFirewall [1]. When the system detects an attack, it traces the attack back up the Internet to multiple sources and intercepts the attacking packets at points in the network close to the sources. In order to expand the use of this technology, security producers must negotiate with domestic and overseas vendors of the routers and switches that make up the Internet so that the key technology will be built into these devices and in this way operate globally to further improve the reliability and safety of the network.

Pattern (3-2) Countering spam and other undesired email

These days massive volumes of unsolicited commercial email are being sent to end users and various illegal scams are being conducted via email. In response, NTT Laboratories developed the privango mail system [2], which allows only the receipt of email that meets certain conditions such as sender name and expiry date. To promote its use, security producers conducted a live demonstration of its safety and convenience. Opinions and feedback from users are currently being examined and will be incorporated into future products to promote the use of safer and securer electronic mail systems.

3. Sociological approach toward security

Security is a problem that arises from the interaction between social structures and people. In this sense, focusing on social structures and the human beings that form them, analyzing their modes of activity, and considering the potential effects on them of newly introduced technologies and services are all critical to the development of a healthy networked society of the future. This section reviews the state of responses to various issues related to security producer activities from this perspective.

3.1 FY2004 & 2005 activities

In FY2004, emphasis was placed on social structures and their relation to human beings and studies were performed to understand phenomena that may effect security. Advice was sought from university professors and various Internet experts concerning a number of perspectives: 1) the trustworthiness of information on the Internet, 2) community and well-ordered networks, 3) educational issues related to adaptation to network society, 4) legal systems, 5) the balance between regulations and voluntary management, and 6) trends in technical measures and related points. Several discussions of these issues were held in the course of this research.

For FY2005, two general goals have been planned based on the results of the previous year's work. The first goal is to analyze the functionality, structure, and systems necessary to build a stable social infrastructure given the vulnerability and frailness of IP networks through a comparison with the history of the automobile from its introduction on up to the current

automobile-based society. Our automobile-based society experiences approximately 10,000 vehicle-related fatalities per year and many times that number of injuries; nevertheless, the automobile is regarded as being necessary and various safety-related technologies, organizational structures, and systems having sprung up around it. Research on IP networks will be conducted based on this analogy in order to compile necessary preventive measures.

The second goal is to survey the state of security in the U.S. and Europe and grasp the situation facing Japan. If security is a reflection of society, then its implementation ought to differ depending on local cultural differences. For example, a great deal of damage due to DDoS attacks and spam mail is known to have occurred in the English-speaking world. It is thought that by studying how the environmental conditions (such as the state of security, opinions about it, and social structures) differ from region to region based on historical and current examples, it should be possible to hypothesize the risks that Japan will face in the future. In addition, by clarifying the differences in the security and legal measures found necessary in different regions, it should be possible to find pointers indicating the level of security that NTT Group should attain as a global corporation.

3.2 Three important issues

Based on the sociological research approach initiated in the latter half of FY2004, the following three issues are thought to be most important ones among those found to date concerning security of information communication technology (ICT).

1. Guaranteeing the integrity and completeness of data and the disclosure/display of this information: What measures should be implemented toward use of the latest ICT concerning antisocial acts and breaches of trust such as the falsification or concealment of information inside and outside a company? What kind of ICT should exist and how should it be operated in order to prevent wrongdoing?
2. Guaranteeing the continuity of social infrastructure functions: How should the infrastructure be protected and functionality be maintained in the event of natural disasters such as earthquakes and typhoons and man-made disasters such as terrorist attacks?
3. Preventing information from spreading over time and space: Looking towards the future digital society, what kinds of preparations are necessary so that the usability of information will be not degraded, even as systems or applications change from one region to another or evolve from one era to the next?

To tackle these issues, we must always react sensitively to changes in the world at large and we intend to continue this work in the future.

4. Conclusion

The activities of security producers take into account the results of research conducted from a sociological approach, designate technical goals for the future, and promote R&D activities to support these initiatives. Through these activities, security producers will contribute to the business of the NTT Group by proposing and promoting all security measures.

References

[1] N. Wada, “Ushering in a New Networked Society,” NTT Technical Review, Vol. 2, No. 4, pp. 6-13, 2004.
[2] K. Takahashi, T. Abe, and M. Kawashima, “Stopping Junk Email by Using Conditional ID Technology: privango,” NTT Technical Review, Vol. 3, No. 3, pp. 52-56, 2005.

Yoshitaka Kagei
Senior Manager, Chief Producer, Cyber Security Project, NTT Department III (R&D Strategy Department).

He received the B.E. degree in electrical engineering from Yokohama National University, Yokohama, Kanagawa in 1978. In 1978, he joined Nippon Telegraph and Telephone Public Corporation (now NTT), Tokyo, Japan and engaged in the development of digital data transmission and switching systems. After that, he moved to NTT DATA Corporation and engaged in the development of products and systems applying security technologies at R&D Headquarters and in the development of new businesses at Corporate Strategy Division. In 2003, he moved to his present post in NTT.

Kazuyuki Nakagawa
Senior Manager, Cyber Security Project, NTT Department III (R&D Strategy Department).

He received the B.E. and M.E. degrees in electro-communications engineering from the University of Electro-Communications, Chofu, Tokyo in 1980 and 1982, respectively. In 1982, he joined the Yokosuka Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT). He has been engaged in the development of integrated business communication systems and intelligent transport systems and the planning of R&D strategy in the field of information sharing platforms. In 2003, he moved to his present post in NTT. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Takeshi Tachi
Senior Research Engineer, Supervisor, Cyber Security Project, NTT Department III (R&D Strategy Department).

He received the B.E. and M.E. degrees in electrical engineering from Osaka University, Suita, Osaka in 1987 and 1989, respectively. In 1989, he joined NTT Telecommunication Networks Laboratories. In 1997, he received the M.S. degree in industrial engineering and operations research from the University of California, Berkeley. He has been engaged in the development of IP network systems and banking systems and the planning of R&D strategy in the field of information sharing platforms. In 2004, he moved to his present post in NTT.

Masao Takeda
Producer, Cyber Security Project, NTT Department III (R&D Strategy Department).

He received the B.E. and M.E. degrees in electrical engineering from Yamagata University, Yonezawa, Yamagata in 1993 and 1995, respectively. In 1995, he joined NTT Tohoku Branch Office. He has been engaged in the planning of multimedia services, the development of advanced intelligent network systems, and the planning of R&D strategy for information sharing platforms. In 2003, he moved to his present post in NTT.

Tetsuya Nakagawa
Senior Research Engineer, Supervisor, Planning Section, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electrical engineering from Waseda University, Tokyo in 1986 and 1988, respectively. In 1988, he joined NTT Transmission System Laboratories. He has been engaged in system development for Internet service providers and Internet portal services and the planning of R&D strategy in NTT Information Sharing Platform Laboratories. In 2003, he moved to his present post in NTT.