ISSN 1349-3531

NiCT NEWS

7
JUL. 2006
No.364

National Institute of Information and Communications Technology

nicter: the Network Incident Analysis Center for Tactical Emergency Response — Toward a Safer and More Secure Internet Environment —

The Era of Safety and Security

The Internet has become an integral part of our social infrastructure in recent years. Services vital to our daily lives—such as online banking and government and municipal public services—have turned the Internet into a convenient tool. On the other hand, we now see crimes associated with the Internet publicized in the news every day, such as the spread of viruses through software like Winny, unauthorized access to servers, and obstruction of services provided at specific sites.

Until now, the Internet was generally designed and implemented with a priority on being connected at all times, otherwise known as "best-effort services." Today, however, merely being connected no longer has any special appeal, and strategies for the Internet have switched direction toward the development of services that may be accessed with guaranteed security.

The nicter Project

In response to such changes in user demands, NICT has launched the nicter (Network Incident Analysis Center for Tactical Emergency Response) project. The term "network incident" here refers to activities such as unauthorized use of server programs, service obstruction (DoS attacks), data destruction or tampering, unauthorized publication of internal information, and actions leading to such activities (such as scanning). These activities may be carried out by users with malicious intent or by computers that have been infected with malware (such as viruses or worms). The purpose of nicter is to enable the early detection of such incidents, which are detrimental to networks, and to determine the quickest and most effective countermeasures.

Technologies to Support nicter

Figure 1 shows the overall plan of the nicter project. The project consists of a macro-analysis phase, visualization processing, a micro-analysis phase, and an incident handling system. The functions of each will be briefly summarized below.

The Macro-Analysis Phase

In this network monitoring phase, various events that occur on the Internet (identified from records such as traffic data and firewall logs) are regularly collected. In this phase, automatic real-time detection of incidents is performed using algorithms such as behavior analysis and change point analysis on the acquired data.

Visualization Processing

To support the intuitive detection of incidents by a human analyst, visualizations of the events are made. Figure 2 shows one example of such a visualization, in which the network traffic is displayed in a three-dimensional representation. Here, the scanning behavior conducted as a preliminary step in the attack appears with a characteristic traffic feature, and it can be used to judge the initiation of an incident and trigger the launch of detailed analysis.

Micro-Analysis Phase

In this phase, code analysis using reverse assembly and behavior analysis in the virtual environment is performed on samples of viruses and worms obtained in the malware sample acquisition phase to determine the behavior pattern. The information is accumulated in a database, and vaccines to create resistance to the detected malware are also produced.

The Incident Handling System (IHS)

As stated above, the macro-analysis phase detects events associated with incidents occurring on the network, and the micro-analysis phase determines the behavior of the malware believed to be the cause of such incidents. By comparing the results of the analyses, it is possible for the incident handling system to identify the cause of an ongoing incident and thus to determine the most effective countermeasure against the detected malware.

The incident handling system provides statistical data derived from the network monitoring function and issues detailed reports on the incident's cause and effective countermeasures to the government, public offices, communication companies such as Internet service providers (ISPs), and general users.

Life and Technology

Q: What countermeasures are currently taken in response to network or security incidents? And what are the limits of the present method for blocking unauthorized access?

A: Currently, public offices and info-communication-related industry organizations are operating a number of network monitoring projects. However, while past studies have been effective in incident detection, they have generally been unable to track the cause of the incidents. Thus a more detailed event analysis method was required. That is precisely why the nicter project launched by NICT has come into the spotlight. In the nicter project, a method has been proposed for identifying the cause of an incident by comparing the results of event analysis over a wide-area network with the results of the micro-analysis for malware identification, and research and development are currently being conducted to fulfill this goal.

Future Efforts

The R&D efforts up to the present have enabled the launch of the nicter system operation with the above function, although part of the system still needs to be developed. A prototype operation room (upper right-hand photo in Fig. 1) has been installed to enable traffic monitoring and development of novel analysis techniques. A test run of a part of this system was made at the Interop 2006 exhibition for network-associated instruments held at the Makuhari Messe in June 2006. The test run not only proved that the incident detection and visualization processing capacity of the system was on a level sufficient to handle the massive volumes of traffic concentrated on the Interop network, but also received high evaluations from the network operators and all those who attended the exhibition.

During this fiscal year, we plan to develop modules that have yet to be implemented, especially for the correlation analysis mechanism for micro/macro phases and malware sample collection, and to conduct studies on how to operate the nicter system effectively overall.

Figure 1 Overall design of the nicter project

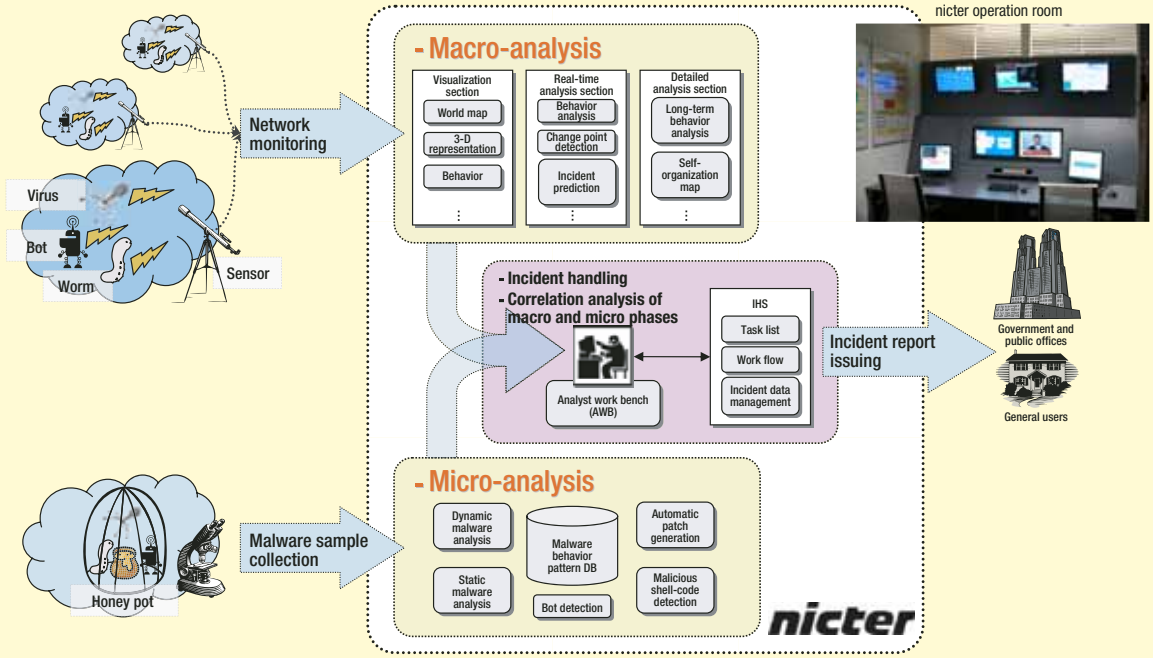
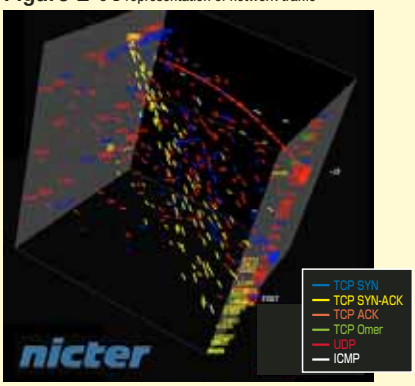


Figure 2 3-D representation of network traffic



Researcher

Masashi Eto

Researcher
Network Security Incident Response Group
Information Security Research Center

After completing his graduate course, Masashi Eto joined NICT in 2005. He is currently involved in research on technologies for Internet routing, incident analysis, and malware sample collection. His hobbies are playing musical instruments and scuba diving, which he has recently taken up. Ph.D (engineering).

This month's key concept

[Best-Effort Service]

The term "best-effort" in the field of communication networks refers to a form of communication in which the quality and performance of a given service are not guaranteed. For example, a best-effort service offering by a provider for DSL connection having a rate of "1.5 Mbps downwards" means that the maximum volume of data that can be received per second is 1.5 Mb. In other words, the performance and quality of transmission is affected by the traffic conditions, and no lower boundaries in performance or quality are guaranteed. In general, such services are cheaper to maintain, so they are offered at lower prices. However, these services are not suitable for video distribution services that require full-time appropriation of certain bands or for network backbones of businesses that will incur losses with connection interruptions. Since the Internet suffers from data loss, transmission delays, and reduction in communication bands when the number of machines and communication volume are increased, it can be regarded as a "best-effort" type service on the whole. In contrast, a communication network service with guaranteed quality and performance, such as minimum transmission speed and maximum annual transmission interruption time, is called a "guaranteed service."

"Seeing" Winds Invisible to the Eye — An eye-safe laser beam: 2 mm coherent Doppler LIDAR —

Aerosols Carried Along With the Winds

Lately a growing number of people are asking questions such as "Why do the weather forecasts seem to be off more frequently?" or "Why are there more incidents of natural disasters involving localized torrential rainstorms?" or "How serious is global warming?" In order to conduct numerical weather prediction and climate models, we require data such as the three-dimensional distribution of temperature, ground surface pressure, and wind velocity. There are wide gaps in wind data (especially over the oceans) that, if available, especially for the troposphere, would significantly improve the precision of numerical weather predictions, and climate models, and make it possible to answer the questions above. Some of the important substances that may assist us in answering such questions are particles suspended in the air around us, called aerosols. Aerosols are carried by winds into all parts of the atmosphere and contribute to various phenomena there. For example, they affect the radiation balance by scattering and absorbing light, they become nuclei during cloud formation, and they trigger chemical reactions on cloud surfaces.

The Development of Radars Using Laser Beams

Aerosols have been made the target of observation at NICT, and various LIDAR (LIght Detection and Ranging) systems have been developed so far. The LIDAR is a type of radar that uses laser beams and makes the observation of aerosol distributions possible. The coherent Doppler LIDAR developed by NICT uses a laser beam with a stable frequency and a wavelength of 2 mm, which is safe for the eye, to make wind measurements through aerosol observation. This laser beam is emitted at an elevation angle from the ground, and the light backscattered by the aerosols moving with the wind is received by the telescope. The frequency of the received light is shifted from the original beam due to the Doppler effect, and a beat signal can be created by mixing the received signal with a part of the original emission. This beat signal is analyzed to detect the Doppler frequency component, which is then used to calculate the wind speed in the direction of the original beam to obtain information on wind speed distribution.

The following is an example of actual observation made on the Kiyokawa dashi, a local wind that blows in the Shonai plain of Yamagata prefecture. The Kiyokawa dashi is one of the three most hazardous winds in Japan (the other two being the Yamaji kaze in Ehime prefecture and the Hiroto kaze in Okayama prefecture) and mainly blows easterly when there are high pressure to the east and low pressure to the west. This wind has caused heavy damage to rice and other crops in the region dating back to ancient times. However, the mechanism by which the Kiyokawa dashi is generated long remained unresolved, and the survey carried out to obtain a 3-D wind distribution at the location of its generation aroused interest among researchers. Figure 1 shows the temporal changes in wind speed and direction from the ground to an altitude of 3 km, represented by the length and direction of the arrows, respectively. At altitudes below approximately 1 km, easterly winds of 5–10 m/s are observed, while near the altitude of 1 km, the wind speed falls to nearly zero. At altitudes above 1 km, westerly winds prevail. Furthermore, downward flow was observed before noon, but it switched to a strong upward flow in the afternoon. Figure 2 shows the results of wind measurements taken in the Shonai plain at an elevation angle of 2∞, and it can be seen that the winds blew from the Mogami valley towards the Shonai plain. The figure also shows how the wind speed and area of strong winds (blue circle) change. Numerical simulations have not yet been able to fully reproduce the features seen in this observation, but we believe that the measurement results will contribute to the improvement of the numerical model and eventually contribute to the stability of agricultural production and supply, thus creating safe and secure conditions for human living.

Contributions to Solving Global Warming

We are currently faced with a host of environmental issues, such as localized torrential rainstorms, heat island phenomena, air pollution, and more. NICT believes that wind measurements, especially in urban areas, are important in solving these problems. In urban areas, various regulations and complex conditions place severe restrictions on wind measurements using radar. However, by constructing a multi-point observation network using the Doppler LIDAR, it should be possible to develop a novel urban environment monitoring system.

Furthermore, the technologies developed for the coherent Doppler LIDAR can be applied to the development of a CO2-measuring coherent LIDAR. We believe that we can contribute to finding a solution for global warming by developing ground-based and airborne systems for measuring CO2 concentrations using such a LIDAR.

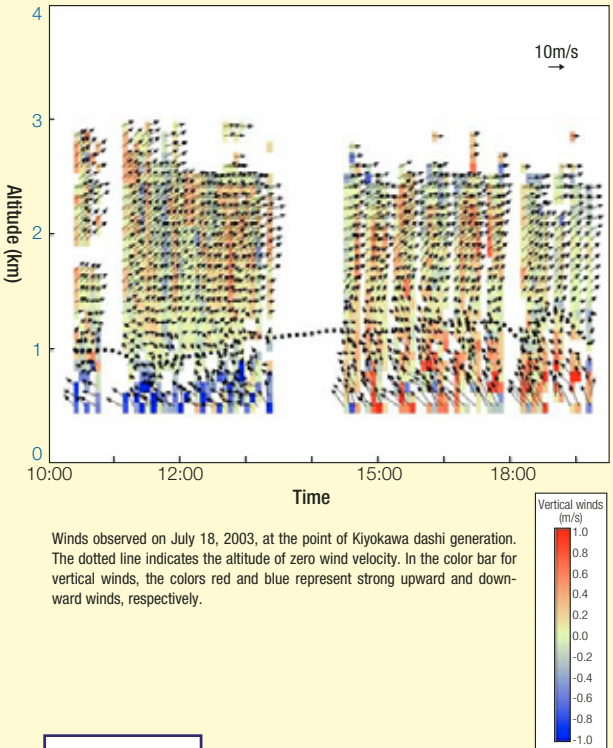
Life and Technology

Q: The present technology can be used in future weather forecast systems, but how is it different from radars that are used in current systems?

A: The biggest difference between radars used presently and LIDARs used for wind measurements is the media; the former uses radio waves, while the latter uses light. Laser beams have extremely low divergence, unlike radio waves. Near ground-level observations that cannot be made by radar due to the presence of side lobes can be made using the LIDAR. Also, radars require large antennas, while the telescope for the LIDAR, which corresponds to the antenna of the radar, is not required to have large apertures. This enables the production of a compact system that may be placed aboard cars, aircraft or satellite.

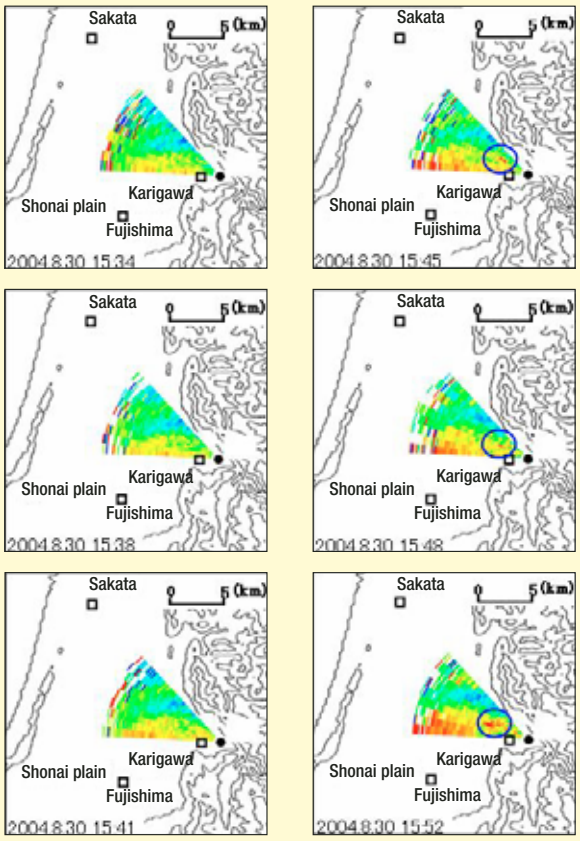
Photos from the Kiyokawa dashi observation experiment: cargo transporter for observation (top left); inside the cargo space with the main body of the LIDAR colored blue (top right); and the two-axis scanning unit (left). The two-axis scanning unit is stored inside the cargo space.

Figure 1



Winds observed on July 18, 2003, at the point of Kiyokawa dashi generation. The dotted line indicates the altitude of zero wind velocity. In the color bar for vertical winds, the colors red and blue represent strong upward and downward winds, respectively.

Figure 2



The horizontal wind distribution observed on August 30, 2004, at the point of Kiyokawa dashi generation by horizontal scanning from the west to the southeast at an elevation angle of 2∞. In the color bar, the color red shows stronger winds.

Researcher

Shoken Ishii

Shoken Ishii joined NICT in 2002 (at the time called CRL) and mainly takes part in the R&D on coherent Doppler LIDAR. Ph.D (science).

This month's key concept

[Local Winds]

Winds that blow only in a certain region are called local winds, and distinct names are given to these winds at various locations in Japan. Local winds are mainly generated by the unique geographical features of a region, and have threatened the agriculture and lives of the people in such regions throughout history. Although conventional measurement systems are not capable of determining the mechanism of their generation, the LIDAR developed in the present study can perform detailed observations of winds at high spatial resolutions within a short time. The understanding of local winds should assist us in developing wind measurement systems for urban regions.

Participation Report on the Fifth Conference for the Promotion of Collaboration Among Business, Academia, and Government

Masahiro Kiyokawa, Group Leader, Outcome Promotion Group, Research Promotion Department

On June 10 and 11, 2006, "the Fifth Conference for the Promotion of Collaboration Among Business, Academia, and Government" was held in the Kyoto International Conference Hall, hosted by the Cabinet Office, the Ministry of Internal Affairs and Communications, the Ministry of Education, Culture, Sports, Science and Technology; the Ministry of Economy, Trade and Industry; the Nippon Keidanren; and the Science Council of Japan. NICT participated as one of the co-sponsoring organizations. This conference has been held since 2002 to achieve a real and steady development among the Business, Academia, and Government. The theme of the conference this year was "Concentrated Efforts to Accelerate Innovation," and over 3,900 participants attended the meeting. It was an impressive conference in which leaders and experienced specialists pioneering their fields came together to promote collaboration among their respective sectors.

On Day 1, after Prime Minister Koizumi's message was broadcast, Science and Technology Policy State Minister Matsuda ,gave a keynote speech on the general strategy for creating innovation, listeners to generate a new wave of business-academia-government collaboration, to help promote Japan-originated innovation throughout the world. This was followed by special lectures from Mr. Mitarai, Chairperson of the Nippon Keidanren, and Mr. Jean-Jacques Gagnepain, Director of Technology at the French Ministry of Research and New Technologies, and a special report by Mr. Shimizu, Chairperson of the National Center for Industrial Property Information and Training.

In the afternoon, panel discussions were held in five subcommittees on themes such as international expansion of business-academia-government collaboration, business-academia-government collaboration (hereinafter referred to as "collaboration"), "collaboration" in regional areas and small-to-middle-scale businesses, fostering of human resources, "collaboration" centered on intellectual property, and the current status of "collaboration." At a general assembly led by the conference convener, Dr. Kurokawa (President of the Science Council of Japan) and three commentators, Dr. Abe (a member of the Council for Science and Technology Policy), Mr. Omi (former Minister of State for Science and Technology Policy), and Mr. Nomaguchi (President of the Mitsubishi Electric Corporation), the project general manager of each subcommittee presented report of the discussions and further exchange of opinions were made.

On Day 2, awards of merit in business-academia-government collaboration were presented, and Minister for Internal Affairs and Communications Awards were given to Mr. Iue (Chief Director of the Keihanna Info-Communication Open Laboratory), Mr. Akiyama (Chairperson of the Kansai Economic Federation), and Mr. Tateishi (Chairperson of the Kansai Science City Promotion Office Planning and Environment Department), for their efforts in the promotion of research and development at the Keihanna Info-Communication Open Laboratory.

In a special lecture given by Dr. Yoshikawa, President of the National Institute of Advanced Industrial Science and Technology, some efforts in "full research" that integrate basic research and product commercialization research, stressing the importance of a national effort to construct a broad system of innovation.

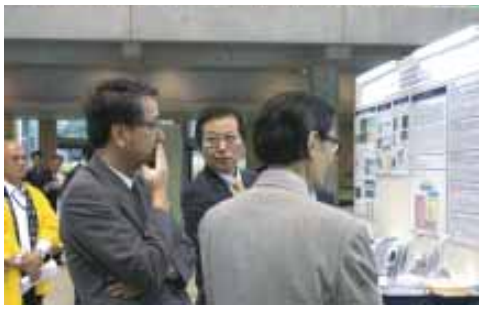
Exhibitions were held in the event hall and lobby adjacent to the main conference hall, consisting of 221 booths presented by 11 award recipients, 12 co-sponsoring organizations, and 197 participating organizations.

At the Minister for Internal Affairs and Communications Award booth, an experiment for driving a compact car–type robot on a public road was introduced by the Knowledge Creating Communication Research Center, and a demonstration of the GMPLS experiment was given for the audience by the New Generation Network Research Center. At NICT's booth in the co-sponsoring organization section, presentations and demonstrations were given on four themes—the real-time asbestos monitor, numerical whole-body voxel models, broadband portable wireless terminals, and quantum encryption technology—by the Public Relations Office and associated research centers and departments. The exhibitions were a great success, and were visited by Mr. Matsuda, Minister of State for Science and Technology Policy, and Mr. Matsumoto, Director-General for Technology Policy Coordination of the Ministry of Internal Affairs and Communications.

The meeting provided a precious opportunity to glimpse the present state and trends of business-academia-government collaboration efforts in Japan as well as overseas.

We would like to thank all those who were associated with participating in the Fifth Conference for the Promotion of Collaboration Among Business, Academia, and Government.

Visit by Mr. Matsuda, Minister of State for Science and Technology Policy (left)



Visit by Mr. Matsumoto, Director-General for Technology Policy Coordination of the Ministry of Internal Affairs and Communications (at the Minister for Internal Affairs and Communications Award booth)

The Fifth Conference for the Promotion of Collaboration Among Business, Academia, and Government
Date: June 10–11, 2006
Venue: Kyoto International Conference Hall (Sakyo-Ku, Kyoto)

NICT Symposium on Basic Technologies for Photonic Network

Takao Morikawa, Research Manager, Project Promotion Office of the New Generation Network Research Center

On June 21, 2006, the NICT Symposium on Basic Technologies for Photonic Network was held at the Meiji Kinenkan by New Generation Network Research Center and the Collaborative Research Department of NICT, with the support by the Ministry of Internal Affairs and Communication.

The main purpose of the present symposium was to introduce research activities led by NICT to realize interdisciplinary industry-academia-government collaboration—in particular, R&D in photonic networks and basic technologies in four info-communication technology fields: photonic network technologies, quantum communication technologies, terahertz technologies, and nanotechnologies.

The symposium opened with a keynote lecture from Dr. Reona Esaki, the president of the Yokohama College of Pharmacy, on "Research on Basic ICT Technologies: A Message for Semiconductor Quantum Structure Research and the Four ICT fields, Quantum Mechanics and Info-Communication." This was followed by speeches from invited speakers Prof. Hiroyuki Sakaki of the University of Tokyo and Prof. Yoshihisa Yamamoto of Stanford University, on nano-ICT and quantum ICT. The themes of all three speeches were closely related, and the audience had an opportunity to grasp a sense of how basic concepts in quantum mechanics are deeply associated with state-of-the-art info-communication technologies.

The latter part of the symposium consisted of presentations of results of original and commissioned researches on related fields at NICT. At the end, NICT's program director, Dr. Kamiya, gave an overview on how NICT plans to proceed with its R&D efforts, with an emphasis on the societal demands on the new generation network and the role of NICT, which was followed by valuable comments and advices from the experts present.

The symposium was attended by over 300 participants, consisting not only of researchers from industry, academia, and government leading the pioneering R&D in the field, but also of those involved with research management and project planning. Enthusiastic discussions were heard not only during the Q&A sessions after the speeches but also during coffee breaks and at the poster sessions.

We would like to thank all those who worked to make the symposium a success.

Keynote lecture by Dr. Reona Esaki, the president of the Yokohama College of Pharmacy


Scenes from the poster sessions


NICT's program director, Dr. Kamiya, during a discussion with a commentator

NICT Symposium on Basic Technologies for Photonic Network
Date: June 21, 2006
Venue: Meiji Kinenkan (Minato-ku, Tokyo)

Winner of the Twentieth Awards for High Technology

Dr. Fumito Kubota (Director of the New Generation Network Research Center of NICT), Dr. Tetsuya Miyazaki (Group Leader, Photonic-Network Group, New Generation Network Research Center of NICT), and Dr. Itsuro Morita (KDDI R&D Laboratories) received the Minister for Internal Affairs and Communications Award at the twentieth Awards for High Technology sponsored by FujiSankei Business i. for their research paper titled "Research and Development of the 160-Gbps Ultra-Fast Photonic Transmission Technology." The awards ceremony was held on July 4, 2006, at the Tokyo Prince Hotel (Minato-Ku, Tokyo), attended by Her Imperial Highness, Princess Takamado. Besides Dr. Kubota, the ceremony was also attended by Dr. Yuichi Matsushima and Dr. Shingo Omori (Vice Presidents of NICT).

The Award for High Technology is presented to students of science and technology and young researchers in the industry who will become leaders of the next generation, and is supported by the Ministry of Education, Culture, Sports, Science and Technology; the Ministry of Economy, Trade and Industry; Fuji Television Network; the Sankei Shimbun; and the Nippon Broadcasting System.

The award-winning paper was a compilation of the results of a series of ultra-fast photonic transmission demonstration experiments at a basic rate of 160 Gbps per wavelength, conducted in 2004 and 2005 on the JGN II optical testbed (having a total extension of 200 km forward and back between Otemachi and Tsukuba) as a collaborative research with the KDDI R&D Laboratories. In 2005, 1.28 Tbps transmission was achieved, and the outcome was presented in post deadline sessions and guest speeches of various international conferences, as well as in journals, and press releases.

This honor could not have been achieved without the cooperation of all those who have contributed to the study. NICT promises to continue our pursuit of further progress in innovative technologies.

At center in the first row is Princess Takamado; to her right are Dr. Morita of KDDI R&D Laboratories and Dr. Kubota (Director of the New Generation Network Research Center)

At center in the first row is Princess Takamado; to her right are Dr. Morita of KDDI R&D Laboratories and Dr. Kubota (Director of the New Generation Network Research Center)

NiCT NEWS

Published by:
Public Relations Division, General Affairs Department
National Institute of Information and Communications Technology

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
■ Tel: (042) 327-5392 ■ Fax: (042) 327-7587
■ e-mail: publicity@nict.go.jp
■ URL: http://www.nict.go.jp/

July 2006 No. 364

NICT NEWS at: http://www.nict.go.jp/overview/news/nict-news.html