1 Introduction: The Research of the Information Security Research Center

TAKAHASHI Yukio

In today's society where the Internet has become widely used and a new social change is beginning to take place utilizing information and communications technologies (ICT), information and communications have become one of the essential lifelines. Further, with the emergence of new ICT such as cloud computing and smartphones, information society is about to go through a rapid and significant change, and the gap between those who can keep up with the changes in ICT and freely use related equipment and those who cannot is widening.

Is life today truly convenient and fulfilling as a result of information and communications? Many challenges still remain, and we have yet to achieve a truly advanced information society. In particular, threats to information security are increasing daily, demanding that cost and efforts are spent on them. The damage from security breaches is becoming more serious and widespread. Balancing safety and convenience, information security is taking on growing significance in our ICT society.

With an aim to "creating a safe and secure society" and "enabling truly rich communication," the Information Security Research Center of National Institute of Information and Communications Technology (NICT) has carried out research and development activities for information security including network security, cryptography and authentication technologies that form the basis of network security, and information and communications technologies in emergency situations or for disaster management and mitigation, mainly with a focus on the following four challenges.

1. Conducting research and development regarding the monitoring and analysis of and countermeasure technologies against malicious human-induced events (incidents) that occur on the network such as cyber attacks, through the assessment of the situation on the entire network.
2. Conducting research and development of spatiotemporal tracing and reproduction technologies of cyber attacks and incidents to detect and reveal their source addresses and to clarify the details of packet transition.
3. Conducting research and development of technologies such as cryptography and authentication technologies, algorithms, cryptographic protocols, and the electromagnetic emanation security, and conducting research and support related to cryptography evaluation.
4. Conducting research and development of network technologies in emergency situations and technologies for disaster management and mitigation utilizing ICT.

In order to advance these researches, when our medium-term plan in the second term was launched in April 2006, the Information Security Research Center was established, which is comprised of the four research groups: Network Security Incident Response Group; Traceable Secure Network Group; Security Fundamentals Group; and Disaster Management and Mitigation Group, and the Project Promotion Office that provides supports for research activities.

In this special issue, the results related to network security from the research conducted by the Information Security Research Center during the five-year period of the medium-

term plan in the second term are reported. We consider this report as a reference to our research technologies and their utilization. The contents, significance and contribution of the main achieved technologies as part of the many results of our medium-term plan in the second term are introduced as topics. We believe that we have been able to achieve the goals of the medium-term plan in the second term as described in each chapter. The results of the research activities related to disaster management and mitigation technologies were reported in the Special issue of NICT Journal (Vol. 58 Nos. 1/2).

As following these results, the Network Security Research Institute has been newly carrying out network security research in the third medium-term plan since April 2011. The Network Security Research Institute is promoting research and development activities to provide every user with a safe and secure information communication environment by working on the following three research issues comprehensively: cyber-security technology to provide observing, and analyzing against cyber attacks in real time, and implementing appropriate countermeasures and preventing against them; security architecture technology that offers flexible, secure and continuously advanced network architecture in correspondence with diverse network environments and user environments; security fundamentals technology that establishes new cryptographic technologies as well as quantum security technology, which is a combination of modern cryptography and quantum communication.

Regarding researches of disaster management and mitigation, because the research aims of our medium-term plan in the second term have been achieved and the developed technologies have been transferred to the actual field situation, it has been decided that the research of the Disaster Management and Mitigation Group would be terminated following the completion of the second medium-term plan and the whole NICT would examine and promote their research activities.

We hope that those who are working or interested in the field of information security research and development will find this special issue useful for their activities. We intend to continue promoting advanced research activities at the newly started Network Security Research Institute through the dual approaches of practical continuous countermeasures and cutting-edge research against cyber attacks to ensure that they will contribute to the safety and true security of the society. We would appreciate your continued support and cooperation.

Finally, we would like to express our deep appreciation to Dr. Yoichi Shinoda, who had served as the Executive Director of the Information Security Research Center till July 2010, and now is a professor at the Japan Advanced Institute of Science and Technology and an R&D Advisor of NICT, Mr. Hiroshi Ooya, Mr. Hirohisa Sekiguchi, Mr. Tetsuya Yasui, Mr. Fusanobu Yonago, who had served as the Vice Executive Director of the Research Center, as well as to the staffs of the Project Promotion Office and NICT who have supported the research of the Research Center, and many others from a number of relevant institutions who have cooperated with the Research Center, who all helped us achieve many research results.

TAKAHASHI Yukio, *Ph.D.*

Director General, Network Security Research Institute

Space Positioning Measurement, Radio Astrometry, Position and Time Authentication, Space and Time Information