

---

# 1 Researches on Information Security in NICT

MATSUSHIMA Yuichi

With the recent rapid increase in the number of Internet users and the widespread use of broadband access environments such as ADSL and FTTH, we are now about to enter a ubiquitous communications age in which it will be possible to exchange information with anyone at anytime, anywhere. As a result, information and communications services are becoming an essential element of our daily societal infrastructure. Today, information and communications technology—involving, for example, fixed and mobile phones, Internet search and information exchange, and electronic payment—is already deeply woven into society, mirroring the historical integration of electricity, water and sewerage, gas, and public transport into our daily lives. Unfortunately, as a result of this integration, computer viruses and other malicious data operations are now capable of breaking into PCs and databases and causing significant disruptions. Given the increasing scale of cyber attacks, wide-area information network infrastructures are growing more vulnerable.

Under these circumstances, it is urgent that we ensure a safe and secure worldwide environment in which to deploy our information and communications infrastructures. Information security technology is thus of pressing importance. Accordingly, the National Institute of Information and Communications Technology (NICT) has been continuing a range of relevant R&D activities and state-level research support, efforts that began with the organization's predecessors, the Communications Research Laboratory (CRL) and the Telecommunications Advancement Organiza-

tion of Japan (TAO). The CRL recognized the importance of information security ahead of most others, initiating a special "Emergency Communications Group" project to pursue independent R&D from 2001 to 2003. The R&D subjects included Internet vulnerabilities, methods of ensuring communications in the event of an emergency such as an earthquake, and an Internet-based system to confirm the safety of residents in disaster areas. In January 2004, the CRL established the "Information Security Center" to address this important issue. Meanwhile, the TAO also placed a great deal of emphasis on information security, providing continuous state-level support for research on Internet security as well as on cryptographic and other technologies to prevent the leakage of information.

NICT, established through the consolidation of these two organizations, is now entrusted with the task of strategically and efficiently carrying out R&D at all stages, from basic research to technology development and practical use within societal infrastructures. Information security R&D demands no less than such a comprehensive approach, and calls an increasing for the creation of a nationwide framework to address this issue. To enhance the effectiveness of the merger between the CRL and the TAO, NICT has created an internal system of cross-departmental units. The Information Security Unit is one of these units, functioning effectively within the overall system.

This special issue covers a wide range of specialized fields based mainly on CRL research results, reports on R&D activities

---

supported by the TAO, and recent NICT activities. I hope this issue will be of some help to researchers engaged in information security

R&D as well as all those with an interest in this field.



**MATSUSHIMA Yuichi**, *Dr. Eng.*  
*Executive Director, Information and  
Network Systems Department*  
*Optical Network Systems*