## Executive Summary

The Constitution of Japan guarantees the secrecy of communications, so telecommunications carriers such as IIJ, and their employees, are forbidden from encroaching upon the secrecy of communications they handle by the Telecommunications Business Act. That said, in carrying out a telecommunications business, we infringe upon the secrecy of communications by referring to communication logs for billing purposes, and header information to deliver packets to their destination. As an ISP, some of the activities such as spam filtering, OP25B, and the blocking of child pornography that we perform on a daily basis to provide peace of mind when using the Internet also interfere with the secrecy of communications. For this reason, careful arrangements are made to provide justifiable cause for noncompliance with the law, such as by obtaining customer consent.

Given this background, it was a big surprise to ISPs such as IIJ, and lawyers and consumer organizations also expressed strong concern, when emergency measures against Internet-based piracy sites compiled by the Japanese government's Intellectual Property Strategy Headquarters in April suggested it would be appropriate for ISPs to block particularly malicious piracy sites as an urgent stopgap measure until judicial measures could be put in place. Going forward, the government plans to set up a task force to discuss this, so we will be keeping a close eye on how this matter develops.

IIJ aims to introduce the wide range of technology that it researches and develops in this IIR, which comprises periodic observation reports that provide an outline of various data we obtain through the daily operation of services, as well as focused research where we examine specific areas of technology. In this volume, Chapter 1 is our periodic observation report, while our first focused research report in Chapter 2 discusses the ROCA vulnerability in a key generation module for the RSA cryptographic algorithm. In Chapter 3, our second focused research report covers email issues.

In the first half of Chapter 1, we examine trends in incoming spam detected on IIJ's email services for the period of 500 weeks from 2008 to 2017, and also discuss notable changes in 2017. In the latter half, we report on trends in the adoption and standardization of DMARC sender authentication technology, an effective anti-spam measure. We also take a look at key legal matters to consider when implementing it in Japan.

Chapter 2 is our first focused research report, where we examine a flaw called ROCA in the implementation of a key generation module for the RSA cryptographic algorithm that leads to encryption not providing the expected level of security. We also analyze the cause of the vulnerability, and consider the future impact of these research results.

In Chapter 3, we discuss the construction of large-scale email systems that IIJ offers to service providers with millions of users, and look at the countermeasures against improper use that we have accumulated over the course of operating these services. Most of the work performed by email system administrators involves correspondence caused by improper use of the email system, as well as associated troubleshooting. For this reason, implementing countermeasures against improper use in email systems contributes greatly to reducing the operational and management workload and providing stable services to end users.

IIJ continues to strive towards improving and developing its services daily, while maintaining the stability of the ICT environment. We will continue to provide a variety of services and solutions that our customers can take full advantage of as infrastructure that supports their business.

**Junichi Shimagami**
Mr. Shimagami is a Senior Executive Officer and the CTO of IIJ. His interest in the Internet led to him joining IIJ in September 1996. After engaging in the design and construction of the A-Bone Asia region network spearheaded by IIJ, as well as IIJ's backbone network, he was put in charge of IIJ network services. Since 2015, he has been responsible for network, cloud, and security technology across the board as CTO. In April 2017, he became chairman of the Telecom Services Association of Japan MVNO Council.