Executive Summary

2017 has begun, and as usual the first few months have flown by. With the Trump administration constantly in the news, and events like something out of a spy movie taking place, all eyes are fixed on overseas matters. Although the political situation in Japan is seemingly calm, recent incidents related to security intelligence are also important issues that concern the Internet, so I cannot help but feel that we will be called upon more and more to respond to events that cannot be resolved through technological theory alone.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ, as a service provider, carries out to support the Internet and cloud infrastructure, and enable our customers to continue to use them safely and securely. We also regularly present summaries of technological development as well as important technical information.

In Chapter 1, we provide a summary of Internet security over the past three months, discussing the many DDoS attacks targeting servers that have been observed, and the increase in attacks that saturate the upstream bandwidth of housing equipment. Many of these attacks use a composite approach, and attack techniques are also becoming more elaborate. In our focused research for this period, we examined the anti-analysis techniques of the Ursnif malware and ways to bypass them. We cover the cunning techniques that malware uses to impede its own analysis and connect to C&C servers, giving actual examples to explain methods to avoid this.

In Chapter 2, we discuss Library OSes. OSes have developed along with the evolution of computers, becoming extremely sophisticated. On the other hand, some source code has been made public, enabling everyone from students to researchers to participate in development through collaborative work on a global level. Library OSes are slightly different from OSes like these, as they support the design of OSes that can withstand flexible use, by stripping the kernel down to only the minimum necessary functions, and providing others in the form of libraries. In this chapter, a developer actually participating in development introduces the Linux Kernel Library and its content, so it is well worth a look.

As mentioned in press releases and other media, we launched the “wizSafe” brand that we announced last year under the concept of “making safety a matter of course,” and we are pouring our efforts into bolstering our security business.

Up until now, IIJ has integrated security operations into our regular operational structure, utilizing operational technologies in a unified manner across all our technology departments. Going forward, we will overhaul our Security Operations Center, and use it to offer solutions such as the C-SOC Service to customers, enabling security intelligence information based on these operational technologies and IIJ’s unique analytics platform to be utilized from the perspective of protecting customer systems.

As part of these initiatives, we will continue striving toward a better Internet, maintaining its stability and making it safer under the “wizSafe” banner, through this IIR and various other outlets for information.

Yoshikazu Yamai

Mr. Yamai is an Executive Managing Officer of IIJ and Director of the Service Infrastructure Division.
Upon joining IIJ in June 1999, he was temporarily transferred to Crosswave Communications, Inc., where he was engaged in WDM and SONET network construction, wide-area LAN service planning, and data center construction, before returning to his post in June 2004. After his return he was in charge of IIJ’s Service Operation Division. From April 2016 he joined the Infrastructure Operation Division, and now oversees the overall operation of corporate IT services at IIJ. He also heads IIJ’s data center operations, and he played a key role in the establishment of the modular “Matsue Data Center Park,” which was the first in Japan to use outside-air cooling.