Executive Summary

Conventional DDoS attacks primarily used botnets consisting of a large number of malware-infected PCs to flood the attack target with connections. Then from around 2013, we began to observe large-scale DDoS attacks where the attacker had taken advantage of poorly configured IoT devices, such as home routers and internet cameras, exploiting their vulnerabilities to infect them with malware.

We expect the number of internet-connected IoT devices to continue rising strongly ahead, and preventing them from being used in DDoS attacks will be crucial to keeping the internet safe. In response to such threats, on February 1, 2019, Japan's Ministry of Internal Affairs and Communications, the National Institute of Information Communications and Technology (NICT), and telecommunications carriers unveiled a project to survey IoT devices and alert users called "NOTICE (National Operation Towards IoT Clean Environment)".

Through the NOTICE project, the NICT will survey IoT devices on the internet to identify devices vulnerable to cyberattacks and pass information about relevant devices onto the telecommunications carriers. The carriers will then identify the users of those devices and alert them to the issue. This is a collaboration between government and the private sector aimed at enhancing the safety of internet-connected IoT devices, and IIJ is an active participant.

The IIR introduces the wide range of technology that IIJ researches and develops, comprising periodic observation reports that provide an outline of various data IIJ obtains through the daily operation of services, as well as focused research examining specific areas of technology.

As our periodic observation report for this edition, Chapter 1 discusses our SOC Report. IIJ's SOC collates and analyzes a range of logs, including those from security devices provided as IIJ services, on its Data Analytics Platform, and we release up-to-date information on threats observed in blog format via wizSafe Security Signal. In this edition, we draw from past wizSafe Security Signal posts and look at three types of notable activity revealed using our Data Analytics Platform and also describe the use of our Data Analytics Platform for machine learning.

Our first focused research report in Chapter 2, titled "Deep-Learning Analysis of Logs to Detect Malicious Communications", is a restructured version of the content of a presentation given by IIJ staff at Black Hat Europe 2018. The report looks at general-purpose methods for detecting threats using logs from commonly available servers and network devices, rather than using specialized equipment or security devices. These huge logs require complex processing, but our research has confirmed there is potential to make effective use of them if they are properly optimized for deep learning.

Our second focused research report in Chapter 3 discusses the overhaul of IIJ Secure MX Service, the email gateway service that IIJ provides. More than 10 years have passed since the service was first launched. It remains a key service for IIJ and continues to see strong growth in subscriptions to this day. That said, with the changes in the landscape over those 10 years, the system had grown obsolete and was saddled by various issues. The chapter presents a report from one of the engineers involved in development process, which included revising system architecture to solve those issues and the decision to develop the system in-house, and we hope this serves as a good reference.

Through activities such as these, IIJ strives to improve and develop its services on a daily basis while maintaining the stability of the Internet. We will continue to provide a variety of services and solutions that our customers can take full advantage of as infrastructure for their corporate activities.

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.