

---

## Executive Summary

The year 2020 was to be the second time Tokyo hosted the Olympic and Paralympic Games. As preparations for the games were entering their final stages, the world was rocked by news of the novel coronavirus. The daily stream of media reports brings home just how hard it is to prevent the rapid spread of a virus like this in our modern world, where people and goods are constantly moving across the globe. Despite the efforts of WHO and government bodies around the world to stem the outbreak, the number of infections continues to rise daily.

Viral infections are not the only thing to propagate rapidly. Huge amounts of information spread through the Internet like wildfire, and we are constantly bombarded with all sorts of information about the coronavirus. That information is not always accurate. Some of it is partial to a particular perspective, some of it is geared to the interests of specific people, and some of it is even deliberately crafted to mislead. The great advances in information and communications technology we enjoy in our modern world afford us the freedom to obtain myriad information, yet at the same time, these recent world events have reaffirmed the need for individuals to verify the truthfulness of the vast sea of information available, and to think and act accordingly.

The IIR introduces the wide range of technology that IJ researches and develops, comprising periodic observation reports that provide an outline of various data IJ 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 contains our SOC Report. IJ's SOC analyzes huge amounts of log data, including those from security devices provided as IJ services, on its Data Analytics Platform, and we release up-to-date information on threats in blog format via wizSafe Security Signal. In this edition, we list the key security topics in 2019 that our SOC was focused on and look at three notable types of activity revealed by the Data Analytics Platform: information leaks via Elasticsearch servers, DDoS attacks, and Emotet. Our discussion incorporates IJ's own observational data throughout, which we hope will be of keen interest.

The focused research report in Chapter 2 follows on from the forensic memory imaging discussion in Vol. 45. In that edition, we looked at acquiring memory images on Linux. This time around, we focus on Windows memory images. We go beyond simply introducing memory imaging tools and also discuss key points to be aware of when capturing and analyzing memory images. We also suggest methods of reliably dumping individual processes.

The focused research report in Chapter 3 looks at the IJ Innovation Institute's research into binary program analysis technology that requires no special assumptions to be made about the program being analyzed. Program analysis technology is built into integrated development environments and helps to streamline development and reduce bugs. Investigating the behavior of suspected malware programs, meanwhile, at times requires us to analyze in-the-wild binary programs of unknown origins. Chapter 3 discusses research efforts to develop technology for the static analysis of binary programs that requires no prior knowledge or assumptions about the program's origins.

Through activities such as these, IJ 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 IJ. His interest in the Internet led to him joining IJ in September 1996. After engaging in the design and construction of the A-Bone Asia region network spearheaded by IJ, as well as IJ's backbone network, he was put in charge of IJ 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.