Executive Summary

IIR Vol.54 (https://www.iij.ad.jp/en/dev/iir/054.html), published March 2022, offered a focused research report analyzing the changes in Internet connectivity that occurred when Russia annexed Crimea in 2014. That report appeared during Russia's contemporary invasion of Ukraine, which began on February 24, and a month or so after it was published, NetBlocks reported[*1] that on May 1, after a blackout of several hours, Internet connectivity in Russia-controlled areas had been restored but was being routed via Russian telecom providers.

It was surprising to see this happen immediately after our report on the Crimean case appeared in the IIR, and doubly surprising that, unlike what happened in 2014, the change of network happened at such an early juncture. Perhaps this is proof that control over the information flowing across the Internet is even more important than it was some eight years ago.

That this is happening now after the period of war and conflict that was the 20th century is behind us is quite shocking. Some observers have been highly vocal about the need to review the use of technology in the context of security, and the same goes for the information and communications technology that we are responsible for. I pray in earnest that the technologies available to humanity are used to enrich our lives, and I hope we can continue to move forward in that vein.

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.

Our periodic observation report in Chapter 1 looks at messaging. In our periodic observation report about messaging a year ago, we described how the Emotet virus was encrypting itself in ZIP files and thus running rampant. A widespread practice in Japan when attaching files to an email is to encrypt them in a ZIP archive and send the password to that archive in a separate email. This practice has made it difficult for companies to prevent Emotent infections. As of January 2022, IIJ adopted a policy of generally rejecting emails to which an encrypted ZIP file is attached. IIJ also tightened its DMARC policy for sender authentication in December 2021. The in this edition report discusses the background to IIJ adopting these security enhancements for its own email systems along with the issues it faced, and we hope this serves as a valuable reference for anyone managing an email system in their own organization.

The focused research report in Chapter 2 is the second part of our two-part series on mac_apt, a forensic analysis framework being developed for macOS. This installment explains how mac_apt plugins are created. It goes into the details of the data stored by mac_apt and discusses the actual design and implementation of a plugin. We encourage you to read through both installments.

Our second focused research report in Chapter 3 looks at challenges and solutions to do with storage on IIJ's service infrastructure. The amount of data generated and processed around the world is growing at an astounding pace, supported by advances in computer processing power and network data transfer speeds. All of that data is essentially amassed on what we call storage systems, and just like computers and networks, storage systems have also been evolving in a significant way. We at IIJ also operate a lot of storage systems designed to ensure that data is kept safe and sound. The report here provides a basic explanation of storage and discusses the FC-SAN and storage operation technologies that IIJ makes extensive use of.

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's MVNO Council, and in June 2021, he became a vice-chairman of the association.

[*1] NetBlocks (https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K).