Executive Summary

You will no doubt be aware of the extensive global disruption sparked on July 19 (US time) due to an error in a channel file distributed by CrowdStrike. The error affected Windows devices (PCs, servers, etc.) that use CrowdStrike's Falcon sensor, and according to Microsoft (in a post titled "Helping our customers through the CrowdStrike outage" on the Official Microsoft Blog), the incident affected 8.5 million Windows devices, or less than one percent of all Windows machines.

That there was a huge impact on financial, aviation, medical, and other systems that underpin our society despite only one percent of all Windows devices being affected may seem surprising, but this is evidence of how widely CrowdStrike's security products were deployed on devices used in critical operations.

According to the Root Cause Analysis published by CrowdStrike (Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf (crowdstrike.com)), there were, broadly speaking, two problems. First, insufficient checks were performed. As it is not realistically possible to reduce human error to zero, it goes without saying that it is crucial to perform multi-stage checks to prevent errors being missed, thereby minimizing their impact. Second, there is a need for staged deployment, or canary releases. Our observations also indicate that the malfunctions occurred in sequence starting with the devices that received the new channel file first. So if the problem had been detected early via a staged deployment—by limiting the number of devices the file was initially deployed to, for example—then it may have been possible to take countermeasures of some kind before it had such a large impact.

As an additional mitigation, CrowdStrike noted that it has engaged independent third-party reviewers. Multi-stage checks, canary releases, and third-party reviews are something that we always strive for when developing and operating our own systems as well.

Today's computer systems continue to grow in complexity. This incident has reminded us that it is becoming increasingly important for us to be mindful that errors can and will happen, and to think about how to prevent them from being missed and how to reduce the scope of their impact when designing systems and operations.

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.

The periodic observation report in Chapter 1 is our broadband traffic report for the year, providing our analysis of IIJ's fixed broadband and mobile traffic. Our observations indicate that overall traffic volume on both broadband and mobile services continues to grow steadily, and that the proportion of traffic accounted for by TCP port 443 (HTTPS) and UDP port 443 (QUIC) is rising, consistent with the trends we observed over the past few years. In this edition, we also take another look back at the past five years. While the changes observed from year to year are not all that notable, the data reaffirm that the cumulative changes over that past five years have been large enough to have a decent impact on the infrastructure.

Chapter 2 presents a focused research report on the evolution of virtualization technology and IIJ initiatives in this area over the years. Virtualization technology has a long history, but the technology has made significant advances alongside the spread of Intel Architecture servers and cloud computing since 2000, resulting in explosive growth in its use. The report traces the history of virtualization technology, which underpins today's cloud computing systems, back to the 1960s, and also looks at what sort of virtualization technologies are used on IIJ's cloud services and the features that IIJ has implemented.

Through activities such as these, IIJ continues striving 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 Director and Senior Managing 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, stepping down from that post in May 2023. In June 2021, he also became a vice-chairman of the association.