Cyber Security Cooperation of National Institute to Support the Tokyo 2020 Games

INOUE Daisuke KUBO Masaki TERADA Kenjiro MORI Yoshiki ENDO Yukiko JINGU Masato MATSUMOTO Takashi ISHIHARA Shota MAKITA Daisuke

Abstract

For the Olympic and Paralympic Games Tokyo 2020, the key issue was to ensure the security of systems related to the Games, at the same time, the security of organizations involved in the Games in various ways, such as Japanese government agencies, local governments, and critical service providers were also necessary during the Games. This article provides an overview of the cyberattack observations conducted by the National Institute of Information and Communications Technology (NICT) in cooperation with the Tokyo 2020 Games, and the results of the observations during the Games.

Keywords : Tokyo 2020 Games, DAEDALUS, AmpMon, STARDUST, Threat Intelligence

1. Introduction

For the Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games"), the key issue was to ensure the security of systems related to the Games, at the same time, the security of organizations involved in the Tokyo 2020 Games in various ways, such as Japanese government agencies, local governments, and critical service providers (hereinafter referred to as "Games-related organizations") were also necessary during the Games.

This article provides an overview of the efforts by the National center of Incident readiness and Strategy for Cybersecurity (NISC) and other organizations for securing the Games-related organizations, as well as the observations on cyberattacks conducted by the National Institute of Information and Communications Technology (NICT) in cooperation with the security operations of the Tokyo 2020 Games.

Note that the observations in this article were made by NICT, independent of the monitoring and analysis conducted by the Organising Committee described in other articles in this special issue. The events detected by NICT were also shared with and compiled by the Organising Committee. As a result, it was carefully confirmed that there was no impact on the Games' operations even from a different perspective.

INOUE Daisuke (IEICE Member)
National Institute of Information and Communications Technology
KUBO Masaki (IEICE Member)
National Institute of Information and Communications Technology
TERADA Kenjiro
National Institute of Information and Communications Technology
MORI Yoshiki
National Institute of Information and Communications Technology
ENDO Yukiko
National Institute of Information and Communications Technology
JINGU Masato
National Institute of Information and Communications Technology
MATSUMOTO Takashi
National Institute of Information and Communications Technology
ISHIHARA Shota
National Institute of Information and Communications Technology
MAKITA Daisuke (IEICE Member)
National Institute of Information and Communications Technology
The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.294-300, August 2022

2. Discussion Group for IR Structure and Cyber Security IR Coordination Center

2.1 Discussion Group for IR Structure

In 2015, the "Discussion Group for Incident Response Structure for the 2020 Tokyo Olympic and Paralympic Games" (hereinafter called "Discussion Group for IR Structure") was established, chaired by the councillor of NISC. In the group, a study of a structure to promote comprehensive security measures to ensure a stable supply of critical services (Note 1), (1) in Japan was initiated.

From the beginning, organizations such as NICT, Information-technology Promotion Agency (IPA), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), and Japan Cybercrime Control Center (JC3) participated as observers in the Discussion Group for IR Structure. Since then, cyberattack observation and information sharing have been conducted by the Group for each high-profile international event, such as the G7 Ise-Shima Summit (2016), the PyeongChang Olympics (2018), the coronation ceremony (2019), the Rugby World Cup (2019), and the G20 Osaka Summit (2019).

2.2 Cyber Security IR Coordination Center

In 2021, after a one-year postponement of the Games due to the coronavirus disease 2019 (COVID-19) pandemic, the Cyber Security Incident Response Coordination Center (hereinafter called Cyber Security IR Coordination Center) was established as a national organization to coordinate the cooperation among the Games-related organizations, based on discussions at the Discussion Group for IR Structure. NICT, IPA, JPCERT/CC, and JC3 were positioned as "Information Security Related Institutions" to cooperate with the Cyber Security IR Coordination Center and observed and shared information on cyberattacks regarding the Games-related organizations.

During the Games, information sharing among NISC, Information Security Related Institutions, and Games-related organizations was conducted around the clock on the JISP (Note 2), which has been in operation since April 2019, and ultimately 330 organizations and approximately 1,800 people used this platform. Finally, about 8,000 topics was posted on the JISP.

As a result, no cyberattacks that could affect the operations of the Games were confirmed, although some malicious communications, DDoS attacks, problems with website browsing, phishing, etc., were detected.

3. Initiatives by NICT

NICT observed IP addresses and URLs of the Games-related organizations (including the Games-related networks provided by the Organising Committee) from July 9 to September 5, 2021, provided observation information to the Cyber Security IR Coordination Center, and cooperated in analysis when incidents occurred (Figure 1).

- DAEDALUS : Detection of malicious communications, backscatter, etc. originating from IP addresses of the Games-related organizations
- AmpMon : Detection of DRDoS attacks against URLs and IP addresses of the Games-related organizations
- STARDUST : Artifact analysis of malware targeting the Games-related organizations, including dynamic and static analysis
- Threat Intelligence : Detection of threats to the Games-related organizations based on various types of threat intelligence

The following sections, 3.1 to 3.5, outline each of the initiatives by NICT.

3.1 DAEDALUS

NICT has a large-scale darknet monitoring system that observes packets arriving at about 300,000 reachable and unused IP addresses on the Internet. The darknet monitoring system is used to detect scan packets sent by malware-infected hosts, attack packets containing exploit code, and backscatter (i.e., SYN-ACK packets caused by a TCP SYN flooding with spoofed source IP addresses).

Direct Alert Environment for Darknet And Livenet Unified Security (DAEDALUS) is a darknet-based alert system that detects malicious activities regarding organizations registered as alert targets. The system can detect malware infection inside organizations,

(Note 1) Communications, broadcasting, finance, aviation, railroads, electric power, gas, water supply, logistics, credit, administrative services (local governments), sewerage, airports, roads, marine and air traffic control, emergency reporting, weather and disaster information, immigration control, highways, heat supply, buses, security, travel, hospitals (to the extent of not interfering with on-site hospital operations), and venues.

(Note 2) Japan cyber security Information Sharing Platform.

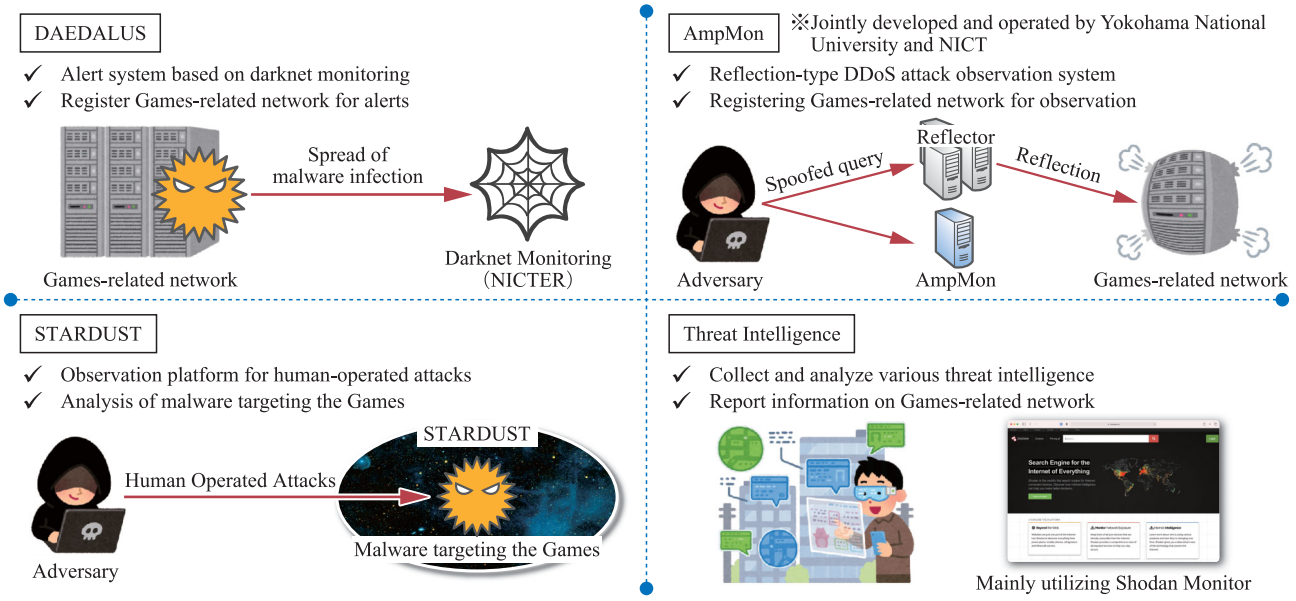

Figure 1 Overview of NICT's Cooperation During the Games

activities spreading infection outside the organizations, and DDoS attacks on the organizations and promptly send alerts to the relevant organizations[2].

For the Tokyo 2020 Games, the IP addresses of the Games-related organizations were registered with DAEDALUS as alert targets, and the status of detection regarding the organizations was notified to the Cyber Security IR Coordination Center in real time.

3.2 AmpMon

A DDoS attack is a cyberattack that overloads the target server or network and disrupts its services. A DRDoS attack is a DDoS attacks that exploits DNS, NTP, and other servers that are inappropriately exposed on the Internet as reflectors, and send a large volumes of traffic to the attack target via the reflectors. It is also called an amplifier attack because it amplifies the traffic during the reflection.

NICT, in collaboration with Yokohama National University, has proposed and operated AmpPot[3], a honeypot for observing DRDoS attacks, and is conducting research and development of AmpMon[4], a platform for observation of, analysis, and sending alert of DRDoS attacks based on this honeypot.

AmpMon is capable of real-time notification of DRDoS attacks based on registered IP addresses, networks, and other information. During the Tokyo 2020 Games, it notified the DRDoS attack status regarding the Games-related organizations to the Cyber Security IR Coordination Center.

3.3 STARDUST

STARDUST is a cyberattack inducement platform that lures attackers, such as targeted attacks, and enables long-term observation of their attack activities[5]. STARDUST generates a "parallel network", which is a network that elaborately simulates organizations such as governments and companies. In this parallel network, various servers (Web servers, mail servers, file servers, DNS servers, authentication servers, proxy servers, etc.) and tens to hundreds of PCs are in actual operation, and in addition, dummy information that imitates information assets of an organization is placed on the servers and PCs, making them behave as if they were a real organization. When a malware sample is executed on a PC called "dummy node" in the parallel network, an attacker connects from the outside via a backdoor installed by the malware and infiltrates the dummy node. STARDUST enables detailed analysis of human-operated attacks by observing the behavior of such attackers in real time.

For the Tokyo 2020 Games, NICT prepared for the emergence of malware such as Olympic Destroyer, which targeted the Pyeongchang Winter Olympics in 2018, so as to conduct artifact analysis centered on STARDUST.

3.4 Threat Intelligence

Looking back on past Olympic and Paralympic Games, there have been phishing campaigns related to sponsor companies, hacktivist activities such as DDoS attacks against the host and participating countries that had human rights issues, and attacks on the IT infrastructure of the competition venues and related facilities.

To detect signs of such attacks, NICT collected and analyzed Games-related threat information transmitted daily via social media such as Twitter. In addition, to grasp the status of IT infrastructure of the Games-related organizations, NICT utilized threat intelligence from sources such as Shodan [6], and routinely observed whether or not devices and services with vulnerabilities were unintentionally exposed to the Internet.

3.5 Establishment of Analysis Team

The cooperation described above was carried out by setting up an analysis team within the NICT around 2015, and during the Games, we established a response structure consisted of analysts in the analysis team and some researchers.

During the Games, a shift system was introduced to enable each member to balance their regular work with the Tokyo 2020 Games. One analyst covered from 10 : 00 a.m. to 5 : 00 p.m. outside the Games period, and two analysts covered from the start of the Games to the end during the Games period, triaging and analyzing various alerts that occurred during the shift and sharing information with the Cyber Security IR Coordination Center via the JISP and telephone calls. To enable off-shift members to quickly grasp alerts, we used Slack, a team communication tool, to notify members of alerts, and implemented a bot for various observation systems on Slack to link alert information with relevant information and to automate the primary triage/response for alerts.

Furthermore, on the days of the opening and closing ceremonies of the Olympic and Paralympic Games, special arrangements were made to prepare for incidents, and NICT dispatched liaison personnel to the Cyber Security IR Coordination Center.

4. Observation and Detection Results during the Games

This section describes the observation and detection results by DAEDALUS, AmpMon, STARDUST, and Threat Intelligence during the Games.

4.1 DAEDALUS Results

Figure 2 shows the number of hosts detected by DAEDALUS during the Games period. DAEDALUS detected anomalous communications from a total of 36 IP addresses during the period, and notified approximately 300 alerts in real time. Of the approximately 300 alerts, 22 required response. For these, the details of the abnormal communication were reported to the Cyber Security IR Coordination Center via JISP, and the source hosts were requested to investigate and take action. Other alerts, such as packets suspected of spoofing the source IP address (only one or two packets were observed) and packets observed due to the use of BitTorrent (a P2P file transfer protocol), were handled quietly after consultation with the Coordination Center.

Figure 2 shows that the most significant number of hosts were detected during the period from the start of the Olympic Games to the closing ceremony of the

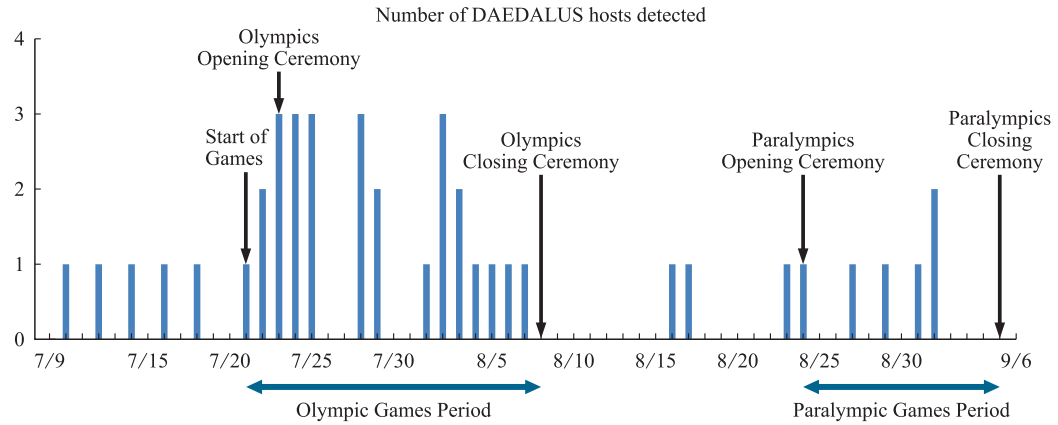

Figure 2 DAEDALUS Detection Results

Olympic Games. In some cases, the spread of infection was prevented by initializing the infected PC immediately based on the DAEDALUS alerts.

4.2 AmpMon Results

Figure 3 shows the daily number of target IP addresses of DRDoS attacks detected by AmpMon against the Games-related organizations during the Games period. AmpMon detected 1,030 DRDoS events in total that targeted 365 unique IP addresses. The figure shows that a relatively large number of attacks were observed during the Olympic period.

As an example of AmpMon observation, DRDoS attacks that appeared to be part of OpBoycottOlympic campaign by Anonymous were detected around the opening and closing ceremonies of the Olympics. Regarding alerts of large-scale attacks, the target organizations were notified the alerts, and appropriate measures were taken.

4.3 STARDUST Results

A malware suspected to be targeted to the Tokyo 2020 Games was posted on VirusTotal[7] during the Games[8]. NICT obtained and analyzed the malware, however, it was mere a simple wiper program. No advanced malware attacks targeting the Games-related organizations that would require analysis by STARDUST were observed.

4.4 Threat Intelligence Results

Using an external threat intelligence service such as Shodan, NICT monitored approximately 50,000 IP

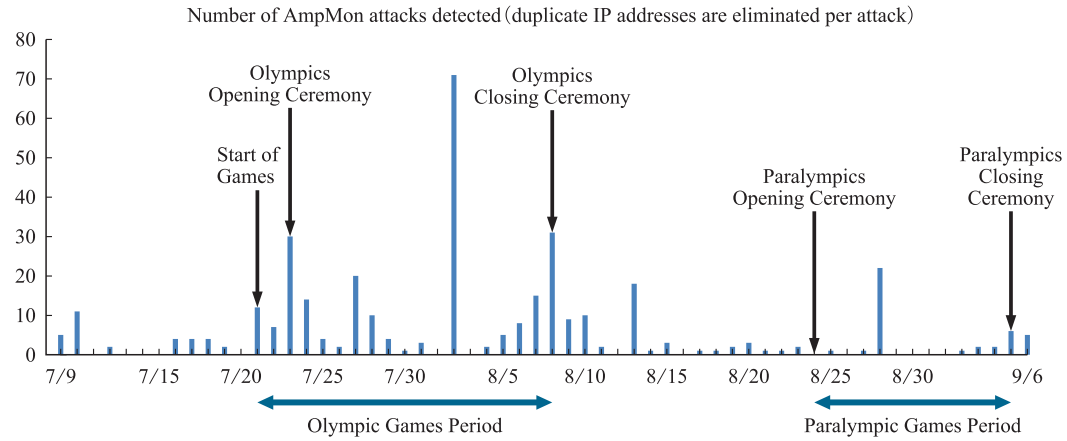

Figure 3 AmpMon Detection Results

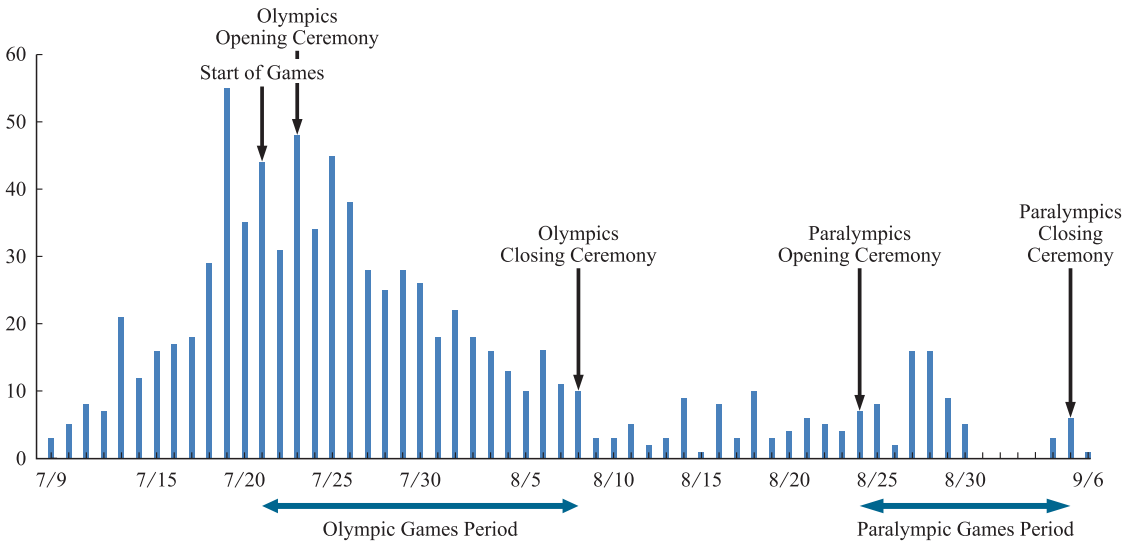

Figure 4 Threat Intelligence Detection Results

addresses of the Games-related organizations. As Figure 4 shows, 843 cases (213 unique IP addresses) were detected during the Games period. The figure shows that the number of detections peaked a few days before the start of the Olympic games and gradually decreased from there.

Among the detected devices were video equipment for domestic and foreign TV stations, professional audio equipment, printers, wireless access points, and security appliance, many of which had management user interface accessible from the Internet without authentication. Information regarding problematic devices was shared with the Games-related organizations, and appropriate action was taken.

NICT also paid attention to anti-Olympics posts (OpBoycottOlympics, etc.) on SNS, and shared information on attack statements and attack targets with the Cyber Security IR Coordination Center. Although AmpMon alerts coincided with the attack targets in some of the attack statements directed at Games-related organizations, there was no impact on the Games operations.

5. Conclusion

The cyberattack observation and analysis technologies researched and developed by NICT over many years functioned effectively during the Tokyo 2020 Games. We believe that the careful examination of observation targets and careful training in advance between the public and private sectors, led by the Cyber Security IR Coordination Center were significant factors in the effective functioning of the technologies.

The legacy of the Tokyo 2020 Games is being reviewed and shared in various fields. However, the legacy of cyberattack response is the trust among the stakeholders that was enhanced by handling various events during the Games.

NICT will continue to contribute to improving Japan's cybersecurity by sharing the knowledge gained from the Tokyo 2020 Games and continue to conduct our research and development to provide Japan's cybersecurity measures even after the Games are over.

Acknowledgements We would like to thank Mr. Shuichiro Takeuchi (Clwit Corporation) and Mr. Yuhei Chiba (NTT Advanced Technology Corporation) for their assistance with the operations of the NICT analysis team during the Tokyo 2020 Games.

References

(1) NISC, "Cyber Security Measures and Future Action Policies of the Tokyo 2020 Games," 2022. https://www.nisc.go.jp/pdf/policy/2020/Tokyo2020houkoku.pdf
(2) D. Inoue, M. Eto, K. Suzuki, M. Suzuki and K. Nakao, "DAEDALUS-VIZ : Novel Real-Time 3D Visualization for Darknet Monitoring-Based Alert System," 9th Int. Symp. Visualization for Cyber Security (VizSec "12), 2012.
(3) L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka and C. Rossow, "AmpPot : Monitoring and Defending Amplification DDoS Attacks," 18th Int. Symp. Research in Attacks, Intrusions and Defenses (RAID '15), 2015.
(4) D. Makita, T. Nishizoe, K. Yoshioka, T. Matsumoto, D. Inoue, and K. Nakao, "DRDoS Attack Alert System for Early Incident Response," Transactions of Information Processing Society of Japan, vol. 57, no. 9, pp. 1974-1985, 2016.
(5) Y. Tsuda, T. Tohmine, N. Kanaya, D. Makita, H. Ushimaru, M. Jingu, Y. Takano, S. Yasuda, R. Miura, S. Ota, T. Miyachi, M. Kamizono, M. Eto, D. Inoue and K. Nakao, "STARDUST : Large-scale Infrastructure for Luring Cyber Adversaries," Computer Security Symposium (CSS2017), 2017.
(6) Shodan, https://www.shodan.io/
(7) VirusTotal, https://www.virustotal.com/
(8) MBSD, "Analysis of Malware (Wiper) with Japanese File Names Related to the Tokyo Olympics," 2021. https://www.mbsd.jp/research/20210721/blog/

(Received April 15, 2022 ; Revised May 23, 2022)

INOUE Daisuke (IEICE Member)
Director General, Cybersecurity Nexus, Cybersecurity Research Institute, NICT. He is also the Director of the Cybersecurity Laboratory at the same institute, where he is engaged in research and development of cyber-security, including DAEDALUS and STARDUST. He is setting up an analysis team in NICT for the Tokyo 2020 Games. Ph.D. in Engineering.

KUBO Masaki (IEICE Member)
Executive Research Engineer, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. He is also a member of Cybersecurity Nexus of the same institute, and an expert member of JPCERT/CC. He is the leader of the analysis team.

TERADA Kenjiro
Planning Manager, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. He is also a member of Cybersecurity Nexus of the same institute, where he is engaged in DRDoS attack observation and analysis. During the Games, he performed alert analysis and reporting using various observation systems.

MORI Yoshiki
Research Engineer, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. He is also a member of Cybersecurity Nexus of the same institute. He is involved in darknet monitoring and analysis, and is the leader of NICT's response to the Tokyo 2020 Games. During the Games, he is responsible for analyzing and reporting alerts from various observation systems. Especially, during the opening and closing ceremonies, he is in charge of liaison between NICT and NISC.

ENDO Yukiko

Senior Research Engineer, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. She is also a member of Cybersecurity Nexus of the same institute. She engaged in darknet monitoring and analysis. During the Games, she performed alert analysis and reporting using various observation systems.

JINGU Masato

Senior Research Engineer, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. He is also a member of Cybersecurity Nexus of the same institute. He engaged in livenet monitoring and analysis. During the Games, he performed alert analysis and reporting using various observation systems.

MATSUMOTO Takashi

Research Engineer, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. He is also a member of Cybersecurity Nexus of the same institute. He engaged in malware analysis. During the Games, he performed alert analysis and reporting using various observation systems, and artifact analysis.

ISHIHARA Shota

Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT (seconded from Hitachi Systems, Ltd.). He is also a member of Cybersecurity Nexus of the same institute. He engaged in livenet monitoring and analysis. During the Games, he performed alert analysis and reporting using various observation systems, and information collection and analysis using public information and threat intelligence.

MAKITA Daisuke (IEICE Member)

Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute, NICT. Visiting Researcher, Advanced Institute for Advanced Studies (IAS), Yokohama National University. He is engaged in research and development of cyber-attack observation systems such as AmpMon. Ph. D. in Engineering.