Cyber Security Operations for the Tokyo 2020 Games

ONISHI Masaki HOSODA Naofumi
NAKANISHI Katsuhiko IBAYASHI Hiroaki

Abstract

The Olympic and Paralympic Games Tokyo 2020 established a robust security environment through security governance and the use of many security solutions. However, without the mature security operations that enabled full utilization of the security solutions, the security measures provided would be meaningless. This article describes how the security operations were designed, implemented, and matured for the Tokyo 2020 Olympic and Paralympic Games.
Keywords : Tokyo 2020 Games, Cyberattacks, Security operations

1. Preface

As described in this special issue "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games", The Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games") implemented many security solutions from the perspective of defense in depth. However, to prepare for unpredictable cyberattacks that evade these solutions, or to prevent them from interfering with the proper operation of the system, the maturity of the security operations is the key.

It is difficult to achieve a sufficient level of the security operations in a day, and it is necessary to mature them over time. On the other hand, there are cost constraints. For the Tokyo 2020 Games, the master plan was to start preliminary operations in 2016 and full-scale operations in March 2019, in time for the transition of the network from the Games preparation to Games production, and then the number of security operators were to be gradually increased for the Games.

As of March 2019, there were 15 full-time weekday and day shift operators, but during the Olympic Games, the Security Operations Centre (SOC) was established within the Technology Operations Centre (TOC) and operated 24 hours a day by approximately 130 operators in 44 positions in three teams : the Security Solutions Team, the Security Incident Response Team, and the Security Intelligence Team.

The following sections describe how the security operations were prepared and matured for the Games.

ONISHI Masaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
HOSODA Naofumi
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
NAKANISHI Katsuhiko
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
IBAYASHI Hiroaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.272-278, August 2022

2. Basic Design of the Security Operations

2.1 Basic Design

In designing the security operations, we referred to the security operation design documents of the past Games and the "Textbook for Security Response Organizations, Version 2.1"[(1)] issued by the Information Security Operation providers Group Japan to efficiently design the overall security operations required for the Tokyo 2020 Games, the relationship between each

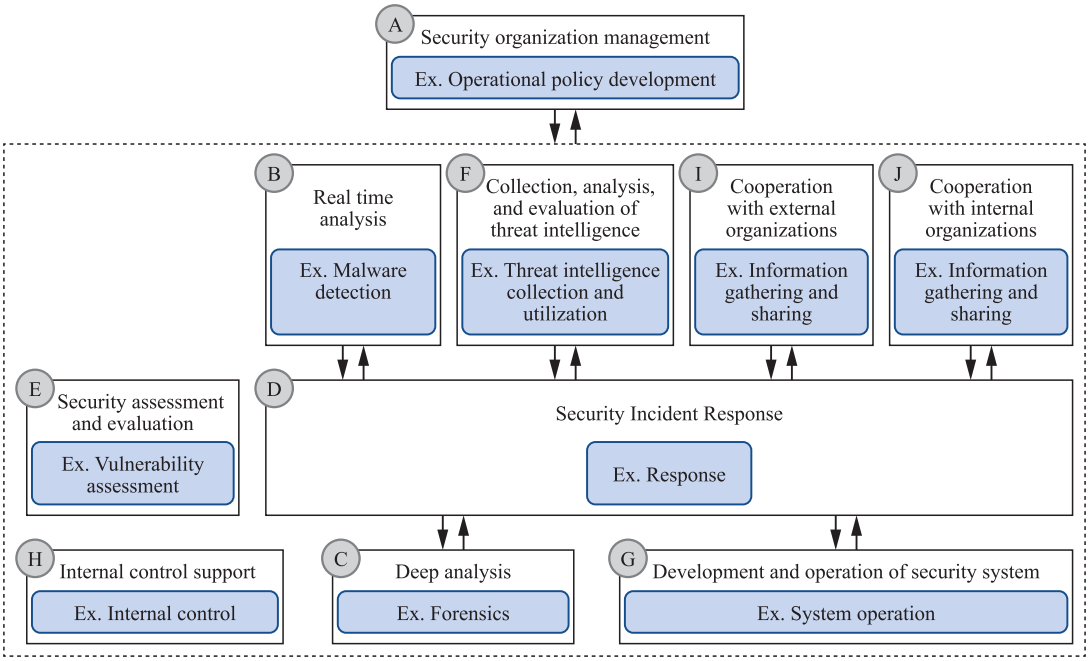

Figure 1　Overall Security Operations and the Relationship between Each Operation

operation, and the operations to be performed in cooperation with the Tokyo 2020 Games stakeholders (Figure 1). The basic design was also effective as a common language when cooperating with staff and relevant departments.

2.2　Detailed Design

Due to cost constraints, the required number of the security operators could only be allocated approximately one month before the Games time. On the other hand, because many security solutions were implemented based on defense in depth, the information that operators needed to understand covered a wide range of fields. Based on these premises, to train new operators in a short period of time, we developed policies and procedures (PnP) in detail for each solution and standardized operations. We also developed a detailed PnP for security incident response, including what to identify, how to prioritize, what actions to take, and how to recover from user inquiries and alerts from each security solution.

In addition, we set up a management indicator to measure whether the incident was handled in accordance with the PnP for operational refinement. This enabled us to continuously improve the scope and content of the PnPs by feeding back the knowledge obtained from daily operations.

3.　Security Operations during the Preparation Period

When security solutions are put into operation, there are many cases where the detection capability against new cyberattacks is insufficient, or where the solution reacts more excessively than expected and interferes with the operation of legitimate services. Therefore, it is important for the security operations to review the solution and the operation method itself each time, and to promote optimization and improvement.

3.1　SIEM Operation

For the Tokyo 2020 Games, Security Information and Event Management (SIEM) was introduced to collect and correlate server and PC logs, alerts from security devices, etc., and thereby to detect cyberattacks that were difficult to detect by each security solution alone. Since the attack detection rules to be developed on the SIEM vary depending on the security solutions and environment, it is necessary to develop the detection rules suitable for each organization. For the Tokyo 2020 Games, we established the operational system that allowed the security operators to develop and modify the detection rules themselves to continuously utilize the SIEM.

For the start of the SIEM operation, the detection rules were developed with reference to MITRE ATT &

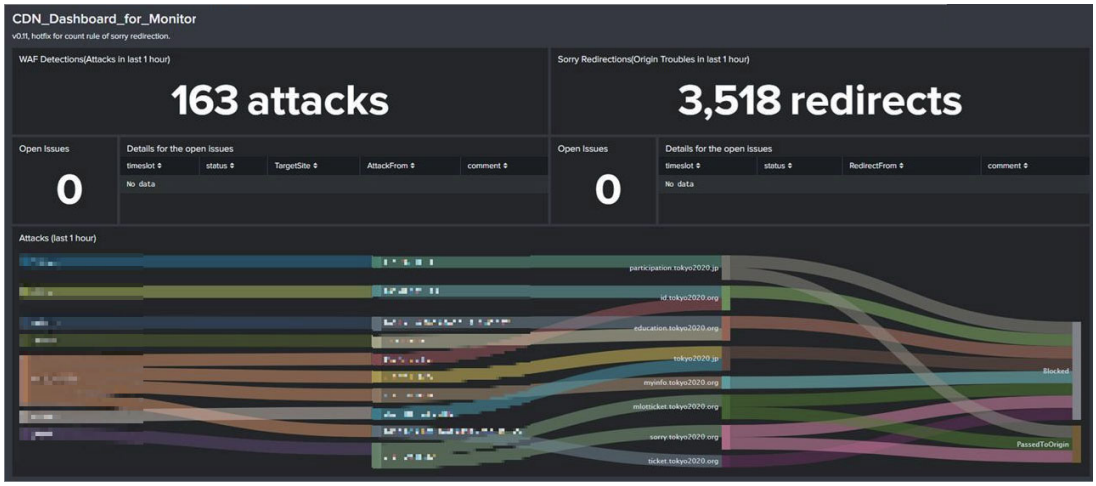

Figure 2　Dashboard Utilizing CDN Logs

CK [2]. When developing the detection rules, we focused on operational feasibility. We conducted actual cyberattacks to verify whether our detection rules could adequately detect the attacks, and we used past logs to ensure that false positives were eliminated as much as possible. When we conducted tests, we found cases where our detection rules failed to detect cyberattacks, because the behavior of the security solutions was very different from our expectations, and cases where the security operations were difficult due to many false positives. This initiative was extremely useful in terms of improving the quality of our detection rules as well as the skills of the security operators.

After the start of the SIEM operation, we added and modified our detection rules mainly to detect actions prohibited by our regulations (e.g., interactive logon using a service account). Since these actions were often used in cyberattacks and were useful for attack detection, we continuously implemented the detection rule whenever new regulation was added. The detection rules developed based on our regulations sometimes resulted in more false positives than expected. This was because the configuration of the system was changing dynamically in preparation for the Games, and each time this happened, we analyzed the causes, and continually improved the detection rule and operated the permission list. In addition, continuous development of the detection rules by analyzing the signs of cyberattacks observed and the cyberattacks methods used during the Cyber War Games (to be described later), as well as other cyberattack methods disclosed to the world, resulted in the advancement of both the detection rules and the skills of the security operators, which enabled us to keep up with the latest cyberattacks.

This preparation was put to great use during the Games. When PetitPotam, an attack method against Windows domain controllers, was disclosed during the Games time, the security operators themselves developed the detection rule to detect PetitPotam, enabling them to promptly detect and immediately respond to the attack.

3.2　Visualization and Dashboard

Visualization is very important to quickly grasp the situation when a cyberattack occurs and to take appropriate initial actions.

As an example of visualization, we introduce one of the dashboards used in the security operations. Figure 2 shows the number of attacks detected by the Content Delivery Network (CDN) at the top, and the attack source and destination at the bottom. This was created with an emphasis on information sharing between the security operators and website operators rather than a detailed analysis of attacks. The dashboard visualized which websites were being attacked and which attacks were slipping through the CDN filters. Cyberattacks are often misunderstood as a cause of system trouble. However, by utilizing this dashboard, it was possible to show the state that there were no cyberattacks or there were attacks but they did not affect the system. This enabled each team to understand the effects of attacks and to respond promptly and appropriately.

In Figure 2, the attack source information is hidden to avoid misunderstanding. Visualization can cause a great deal of misunderstanding if it is used for unexpected purposes. It is very important for dashboards to clarify

to whom and what the information is intended to be shown, and to appropriately limit the scope of disclosure.

3.3 CDN Operation

As described in this special issue "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games" our websites were hosted in a CDN. It was a countermeasure against Distributed Denial of Service (DDoS) attacks and unauthorized access, but it also caused serious false positives which blocked legitimate user connections. 3.3 will focus on countermeasures against false positives.

The Tokyo 2020 Games website delivered not only static contents such as documents and images, but also accepted information uploads from related parties or related systems. These connections may be misidentified as attacks and blocked. For example, the format of uploaded data may resemble an attack code, or the hash value in a cookie may look like an attack command, which will be blocked by a rule-based filter. In other cases, related system connections suddenly become frequent and they would be misidentified as DoS attacks and were blocked by the rate-based filter. False positives are not rare cases. They occur frequently and require daily response. If legitimate connections were blocked, they could interfere with the operation of the website and, in the worst case, might affect the operation of the Games. Responding to false positives is as important as responding to attacks. For the Tokyo 2020 Games, we worked to minimize the number of false positives by combining pre-tuning before the site was released with tuning after the service was launched.

In pre-tuning, a dedicated period of time is defined to generate traffics that simulate legitimate connections and evaluate filters. This is done in a staging environment with limited access. When deploying CDN to existing services, the filters are often activated as detection-only mode to eliminate the risk of false blocking, and tuning is performed while using actual user communications. However, for the Tokyo 2020 Games, almost all sites had access peaks immediately after the release, therefore filtering protection needed be put in place from the beginning. Based on this, we ruled that sites needed to start their services with block mode filters after reducing the risk of false positives as much as possible by pre-tuning, and then start using the filter in blocking mode. Nevertheless, false positives were remained in many cases because it was difficult to prepare enough test patterns. For this reason, it was important to keep on tuning in the security monitoring phase.

In the security monitoring phase, false positives are found in a mixture connections of legitimate user accesses and attacks. False positives are difficult to detect because they are hidden in low-risk attacks detections. They are always too many low-risk attacks and often ignored. To detect false positives, it was important to implement monitoring rules that focus not only on the characteristics of attacks, but also on the characteristics of false positives. By maturing these rules based on actual cases, we established a system that detected and responded to even small false positives without omission. Although we could have wait for users to report false positives, we decided to proactively detect false positives because there was a risk that they would be left unreported and become a major problem during a critical period of time.

After finding false positives, it is necessary to optimize the detection settings. Understanding the specifications and behavior of the website is essential for this, and cooperation with the system developer is also important. By establishing a cooperative system with the developers and deepening the CDN operation team's understanding of the site, we were able to determine the optimal settings, prevent attacks, and maintain legitimate connections without interfering with the Game.

3.4 Security Intelligence Activities

The Security Intelligence Team began its activities in October 2019. The team detected signs of cyberattacks, information leaks, fake websites, fake mobile applications, spoofing of official SNS, fake news, and so on, using the information provided by multiple security intelligence services and the government agencies, as well as information collected from Internet forums, SNS, and the dark web.

As an example, we detected the leakage of credential information such as authentication IDs and passwords used for the Tokyo 2020 Games ticket site and official online store. Upon detection, we promptly reset the password for the account before any unauthorized intrusion occurred. In this case, it was assumed that the service provided by the Tokyo 2020 Games was not compromised by the attacker, but rather the user's private device was infected with information-stealing malware.

In addition, we built the security intelligence platform that automatically collected the Indicators of Compro-

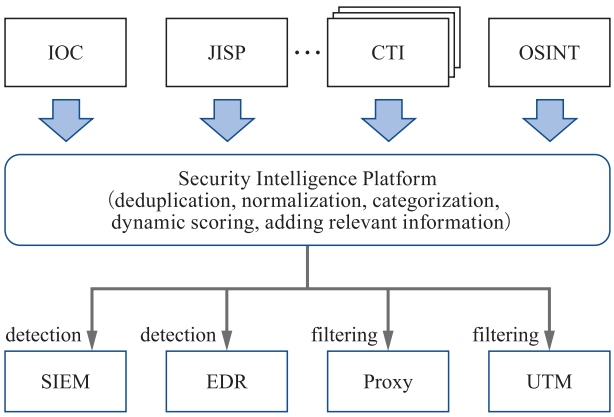

Figure 3 Security Intelligence Platform

mise from the International Olympic Committee (IOC), security intelligence services, Japan cyber security Information Sharing Platform (JISP), Open Source Intelligence (OSINT), and automatically distributed the collected Indicators of Compromise to network security devices, SIEM, and Endpoint Detection and Response (EDR) (Figure 3).

Security intelligence was also used as a countermeasure against reputation risk and ambush marketing. Using the PyeongChang 2018 Games and the 2018 FIFA World Cup as case studies, we worked with the relevant departments to improve the maturity of monitoring methods and responses to detection.

3.5 Threat Hunting

While promoting the maturity of the security operations, it is also important to prepare for cyberattacks that cannot be detected by current security measures. For this purpose, we conducted Threat Hunting, which was a research activity to proactively detect signs of attacks and attacks that were missed by current security measures. Details are described in this special issue "5-6 Find Evil-Know Normal : Tokyo 2020 Games Threat Hunting from Internal and External Perspectives".

4. Security Operation Test

The capabilities of the security operations can be improved by responding to cyberattacks that occur on a daily basis. On the other hand, for a one-time major event such as the Olympic and Paralympic Games, the ability to respond quickly and accurately to infrequent or unexpected security incidents is also required. We conducted various tests to sufficiently enhance the ability to respond to these security incidents.

4.1 Cyber War Games

The Cyber War Games (CWGs) are practical cyberattack exercises to evaluate staff, the implementation of the IT system and network, and operation processes from a cyber security perspective by conducting cyberattacks that may occur on the IT systems used for the Tokyo 2020 Games during the Games.

The CWGs consisted of three teams : the Green Team, which coordinated and evaluated the exercise ; the Red Team, which launched the cyberattacks ; and the Blue Team, which defended against the Red Team's attack. For the Tokyo 2020 Games, the CWGs were conducted four times : two exercises at the Back Office Network, the network used by the Tokyo Organising Committee staffs in their work (BON), one exercise at the Competition Network, the network for competitions connecting venues (CPN), and one exercise at the Core Hosting Network, the network for Olympic and Paralympic Games related system (CHN) The following major issues were identified and resolved :

(1) Rule Violation
- Credentials were recorded in plain text in the log.
- Accounts were assigned more privileges than necessary, etc.

(2) Improper System and Network Configurations
- The configurations for servers, network devices differed from the design documents.

(3) Response to Unexpected Cyberattacks
- Failed to detect cyberattacks using standard Windows tools (Living Off The Land Binaries and Scripts) and undisclosed vulnerability attacks, etc.

Some of these issues were known before the CWGs. For example, we were aware that some of the accounts that had existed since the inception of the Tokyo Organising Committee had higher privileges than necessary, but we could not correct them because we did not know the impact of changing the privileges, etc. The successful attacks on these accounts by the CWGs raised awareness of cyberattacks among the people involved and resulted in the remediation of the situation.

The CWGs were useful in that they allowed the security operators to experience security incidents that did not occur in daily security operations and to make use of them for improvement, and to objectively evaluate

the current security level by being subjected to actual cyberattacks.

4.2 Disaster Recovery Rehearsals

At every Olympic and Paralympic Games, Disaster Recovery Rehearsals (DRRs) are held for switching from a primary to a secondary data centre in an overseas data centre and from a primary to a secondary data centre in the host country's data centre.

For the Tokyo 2020 Games, based on the security incident that occurred during the PyeongChang 2018 Games, we enhanced the DRR scenarios from a cyber security perspective in addition to the scenarios conducted for each Games. Specifically, the scenario assumed that Active Directory (AD), which had authentication and other functions, was stopped due to unauthorized access. The purpose of the scenario was to confirm the effectiveness of the provisional operation procedures and the roles of each team to ensure that the systems (single sign-on system, proxy, etc.) linked with AD resume service within the target recovery time.

The scenario allowed us to confirm the feasibility of recovery by alternative means in the event of an AD outage in an actual environment. In addition, it was possible to check the actual operation based on the dependencies between systems and parameter settings, such as the fact that logging in to the PC and using a file server were possible if the PC's authentication cache was enabled, while network and VPN connections were disabled if the PC was logged off. This was also useful for improving the business continuity plan with an awareness of resilience in the event of cyberattacks.

Although we conducted a rehearsal for AD and systems that were linked to AD, we also established appropriate procedures for the systems that might have a significant impact on the operation of the Tokyo 2020 Games such as network authentication systems, software distribution systems, and operation management systems, etc.

4.3 Technology Rehearsals

Technology Rehearsals simulate technology operations through various normal and abnormal scenarios during the Games time. They were conducted twice (each time for three days) to evaluate systems, staff, and operational procedures, and were attended by staff from the Technology Services Department of the Tokyo Organising Committee, the IOC, vendors including technology partners, and others.

A total of 29 cyber security scenarios were conducted, including suspicious behavior in the network, infection with unknown malware, file server encryption by ransomware, social engineering, website defacement, and government collaboration. As a result, a total of 22 issues were identified, including inadequacies in operation procedures and shift handover methods, and improvements to the dashboard for security monitoring, which were promptly resolved before the Games.

5. Examples of Security Incident Response during the Game Preparation Period

5.1 Zero-day Vulnerability Response

We describe an example of a zero-day vulnerability that we responded to just before the Game times when our concerns became a reality.

"PrinterNightmare" is a vulnerability, that was disclosed at the end of June 2021 and assigned CVE-2021-34527. Because it was approximately one month before the opening ceremony of the Olympic Games, we had to be very careful in changing the systems, and difficult decisions were required. First, we promptly collected detailed information on the vulnerability and proceeded to verify the Proof of Concept (PoC) code. In addition, to confirm the extent of the impact, we quickly checked all servers whether the print spooler service affected by the vulnerability was running on each server by using the vulnerability tracking tool.

As a result of the check, we confirmed that many servers and PCs had the print spooler service enabled and were affected by the vulnerability. We explained the impact of the vulnerability, workarounds, and the impact of implementing the workarounds to the server administrators. Then, we sequentially disabled the print spooler service on the server approved by the server administrator using group policy. On the other hand, since PCs were unable to print if the print spooler service was disabled, which had a significant impact on business operations, we disabled Inbound Remote Printing according to the guidance issued by Microsoft on July 1, 2021. Subsequently, an emergent security update was released, and we applied it to PCs and all critical servers, including AD, to complete the response. In this way, we were able to quickly make decisions and respond to zero-day vulnerabilities that occurred immediately before and during the Games time in accordance with the vulnerability response process that had been prepared in advance.

5.2 Phishing E-mail Disguised as the Chief of the Tokyo Organising Committee

In daily security operations, we analyzed reports from staff and alerts notified by each solution, and identified the extent of the impact and causes, which were then addressed. In addition, we took action in cooperation with related organizations as necessary.

As an example, we describe how to respond to phishing e-mails disguised as the chief of the Tokyo Organising Committee. In the example, attackers sent phishing e-mails to an unspecified number of people, spoofing the e-mail address of the chief of the Tokyo Organising Committee. The phishing e-mails were sent intermittently seven times in two weeks from January 24 to February 6, 2020. For our analysis, we used undeliverable e-mails received in the e-mail account of the chief of the Tokyo Organising Committee.

The phishing e-mails were also sent to three staff members of the Tokyo Organising Committee, but we were not affected because the spam filter handled them properly. The phishing site, which illegally used the Olympic symbol, was designed to induce e-mail recipients to log in to view documents. We identified a total of six phishing sites, none of which were accessed by the Tokyo Organising Committee staff members.

We analyzed the undeliverable e-mails that were sent in the early stages of the phishing e-mails and found a high probability that they were phishing campaigns targeting the Tokyo 2020 Games stakeholders. Therefore, we regarded it as preparing activities for cyberattacks by attackers and alerted the Tokyo 2020 Games stakeholders. In addition, we cooperated with external organizations such as security vendors to register the sites with the anti-phishing function of the browsers and to take down the sites.

6. Conclusion

This article has described the security operations. The security operations and their improvement activities accumulated since the early stage of the Games preparation period, as well as various training and exercises such as the CWGs, steadily improved the capability of the security operations. In addition, we responded promptly to security incidents, such as the website defacements and the compromised e-mail accounts, that targeted the Tokyo 2020 Games stakeholders, in cooperation with related organizations during daily security operations, so as not to miss any early signs of cyber attacks.

The security operations during the Games time, which were the result of these efforts, are described in this special issue "5-5 Responding to Cyber Attacks during the Tokyo 2020 Games", but it can be said that the security operations matured during the Games preparation period protected the Games from cyberattacks and contributed to the success of the Tokyo 2020 Games.

References

(1) Information Security Operation providers Group Japan, Textbook for Security Response Organizations, Version 2.1. https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

(2) MITRE ATT & CK https://attack.mitre.org/

(Received February 28, 2022 ; Revised March 16, 2022)

ONISHI Masaki

ONISHI Masaki was engaged in security management at NTT Communications Corporation. He has been seconded to the Tokyo 2020 Organising Committee as the Director of Security Operation, Cyber Security Department, Technology Services Bureau since 2018. During the Games, he was responsible for the security incident response at the SOC.

HOSODA Naofumi

HOSODA Naofumi has been working for ISP backbone operation and analysis of cyber threats at NTT Communications Corporation. He was seconded to the Tokyo 2020 Organising Committee as Security Operations Manager of the Cyber Security Department, Technology Services Bureau since 2014. During the Games, he was in charge of web security operations at the SOC.

NAKANISHI Katsuhiko

NAKANISHI Katsuhiko was engaged in security incident response and cyber exercise at NEC Nexsolutions, Ltd. and has been seconded to the Tokyo 2020 Organising Committee as the Director of Cyber Attack Response Department, Security Bureau, and Cyber Security Department, Technology Services Bureau since 2015. During the Games, he was responsible for the overall security operations at the SOC.

IBAYASHI Hiroaki

IBAYASHI Hiroaki has been working in the service development of cloud and security businesses at NTT Communications Corporation since 2014, and has been seconded to the Tokyo 2020 Organising Committee as the Director of Cyber Security Department, Technology Services Bureau. During the Games, he was responsible for the overall security operations in the SOC.