Summary of Cyber Security Activities at the Tokyo 2020 Games

SAKA Akira　IBAYASHI Hiroaki

Abstract

The Olympic and Paralympic Games are the focus of worldwide attention and are subject to a wide variety of cyber attacks at every Games. On the other hand, the increasing use of various IT technologies, such as the expansion of cloud computing environments is progressing year by year, making it difficult to control cyber security risks. This article introduce how Cyber Security Team of the Organising Committee managed the cyber security risks for the entire system related to the Olympic and Paralympic Games Tokyo 2020 including the environment of the Games officials and how the government and related parties contribute to the future legacy of the Games for Japan.

Keywords：Tokyo 2020 Games, Cyber attacks, Security governance

1. Foreword

The Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as “Tokyo 2020 Games”) had to be held without spectators at most venues due to the effects of the coronavirus disease 2019 (COVID-19). However, as announced by the IOC (International Olympic Committee), 3.05 billion unique viewers worldwide watched the Games on TV and digital platforms, and new technologies and digital innovations enabled more fans to “interact” with the games. The Game was the most engaged Game to date[1]. Cyber security was indispensable for the Games to be held with participation from all over the world via digital platforms in the COVID-19. There were many cyber attacks for the past games which could affect the operations, and the Tokyo 2020 Games got a total of 450 million security events and blocked them during the Games.

The Organising Committee had considered cyber security measures to be an important issue since its establishment, it formed the Cyber Security Department, an independent division with dedicated members, and established the Security Operation Centre (SOC), headed by the CISO, which coordinates the various bureaus of the Organising Committee across the board. In this and following articles the Cyber Security Department and SOC are referred to as the Cyber Security Team.

As attack methods become more sophisticated and their objectives more diverse, and attackers are said to be dominant, it is important to surpass attackers’ activities in order to protect systems and ensure the success of the Games. As a challenge for the Tokyo 2020 Games, we had worked on the implementation of appropriate risk controls with proper understanding of the characteristics of the Games, and on the construction and maturation of the system operation for these risk controls. This article and this special issue “5-2 Cyber Security Governance of the Tokyo 2020 Games”[2], “5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games”[3], “5-4 Cyber Security Operations for the Tokyo 2020 Games”[4], and “5-5 Responding to Cyber Attacks during the Tokyo 2020 Games”[5] will introduce the approach of how the Cyber Security Team thought

SAKA Akira
The Tokyo Organising Committee of the Olympic and Paralympic Games
IBAYASHI Hiroaki
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.249-253, August 2022

about, prepared for, and organized the system.

In addition, a list of terms used in the chapter five (5-1 to 5-9) of this special issue and their explanations are provided after this article (page …) for your reference when reading the chapters 5.

2. Cyber Threats to the Games

Before introducing our efforts, we introduce the cyber threats related to the Games.

First, cyber crimes targeting economic interests are mentioned. Fake tickets, unauthorized websites selling related goods, phishing through fake websites, and information theft through fake access points had been frequently observed in the past Games. The Organising Committee could not ignore these activities, so it had to constantly gather information and take action as soon as it found them. In addition, targeted ransomware attacks became active in 2020, requiring thorough protection including the supply chain as well.

Another example is the obstructive activities for the purpose of political propaganda. In the past, most of these attacks were access interference and falsification for the official websites of the Games, sponsors, host cities, and other related organizations. However, as attack methods have become more sophisticated, they have changed and evolved to include system and data destruction through intrusion and hijacking of Games systems, as was the case at the PyeongChang 2018 Games. In terms of intrusion routes, there is an increasing number of methods that target the supply chain, first compromising the systems of parties, and then using them as foothold to attack the main systems. To protect the systems from these attacks, zero trust designs and thorough protections that include the Organising Committee's systems and related critical infrastructure environments are demanded.

In addition to the above, attention must also be paid to attacks on new technologies introduced in recent Games, such as those aimed at tampering with IoT devices (drones, robots, facial recognition, surveillance cameras, etc.). The methods and objectives of attacks are constantly changing, and various new types of attacks, such as Emotet and PetitPotam, were launched during the preparation period for the Games. It is essential for security operations to keep up with new risks and continuously add appropriate countermeasures.

3. Approach to the Tokyo 2020 Games

Based on these threats, we the Cyber Security Team decided approaches to security measures.

First, we clarified the targets to be protected. There were very large and diverse targets including the environment managed by the Organising Committee, which was the core of the Games operations, the environment of partners and suppliers related to the Games operations, and the critical infrastructure environment that supported the Games. It was necessary to clarify who protect where and how to ensure that all environments were protected properly in each of these environments. Second, we thoroughly established governance system to ensure that security measures were implemented without fail and that a quick response for the incidents were enabled at the Games time.

For the environment managed by the Organising Committee, which was the core of the Games operation, we analyzed threats and selected various security solutions that utilized advanced technologies to prevent advanced attacks. Furthermore, we established security operation team early and trained them to maximize the use of the solutions and matured the operational quality through practical exercises and daily incident response to the wide variety of incidents. The following is a summary of these efforts.

3.1 Thorough Governance

To protect the Games from cyber attacks, not only the systems built by the Organising Committee, but also the environment of the related parties and the critical infrastructure supporting the Games must be comprehensively protected. The Organising Committee itself was a large organization consisting of a total of 52 Games management functions, and the systems used by each of these functions were becoming increasingly complex due to the diverse use of IT, such as cloud computing environments. So penetration of security were very important. In addition, as attacks became more sophisticated, countermeasures based on the zero-trust security design became essential for a wide range of targets without omission. To address this issue, the Cyber Security Team had developed a number of security policies and standards to ensure a certain level of security quality. Furthermore, the team had established a governance structure to ensure that security measures were implemented without omissions by making application of security policies and standards mandatory at various phases of system development and by providing security checks and security reviews to confirm their application status. Details are presented in this special issue "5-2 Cyber Security Governance of the Tokyo 2020 Games"[2].

3.2 Selection of Security Solutions

The environment managed by the Organising Committee, which is central to the operation of the Games, had a special and complex configuration, there were 4 domains known as Backoffice Network (hereinafter referred to as "BON") used by the Organising Committee members for their work, Competition Network (hereinafter referred to as "CPN") connecting the venues, Olympic Technology Network (hereinafter referred to as "OTN") that accommodated various services such as the dedicated VLANs of the people involved in the Games, and a group of Web sites located on the Internet. Based on the characteristics of each domain, optimal security solutions were selected and implemented.

In the BON and CPN domains, important systems directly related to the Games operation were located and many PCs of related parties were connected. Therefore, many solutions were implemented from the viewpoint of sophisticated communication control inside the network and defense in depth design. In addition to them, based on the zero-trust approach, we implemented thorough authority hierarchization and minimization, systematic blocking of attacker behavior and malicious operations, installing EDR (Endpoint Detection and Response) and NDR (Network Detection and Response) to detect suspicious behavior, and SIEM (Security Information and Event Management) to correlate and analyze those logs.

In the OTN, the balance between convenience and security was necessary because various devices brought in by the parties concerned.

For the network, we adopted a blocking list method that blocks known malicious communications, rather than a permission list method that allows the minimum necessary communications. For endpoints, we focused on promptly detection and response rather than blocking.

For the Web site domain, we adopted a policy of ensuring uniform security by utilizing a CDN (Content Delivery Network) and its optional functions such as WAF (Web Application Firewall), while each site would implement security measures tailored to its own needs. The details of this policy are introduced in this special issue "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games"[3].

3.3 Maturity of Security Operations

Security solutions are not meaningful if they are merely implemented. It is also essential to set up a mechanism to appropriately coordinate each solution, optimize the settings to maximize the performance of each solution, and mature the operation team to master the use of each solution.

As a mechanism to link solutions, we had utilized SIEM and other means and set up the environment that could detect the signs of the attack immediately. This enabled real-time monitoring and visualization of risks and cyber attacks, and also enabled prompt response to any incidents that might occur during the Games. In addition, an operational infrastructure was created to enable the smooth deployment of IoC (Indicator of Compromise) obtained from the partner organizations to operation teams.

In order to mature the operation team, we improved the technical capabilities of team and sophisticated our security solutions through a combination of actual operations and practical exercises during the Pre-Games period. One example of the actual operations is a phishing campaign targeting Games officials occurred in January 2020, which was a preparatory activity of the attackers. This was a very useful experience in reaffirming the effectiveness of the solutions implemented and reaffirming the awareness of the operation team for the Games. It was important to be aware that attack methods are constantly becoming more sophisticated and brushed up the security measures and operations of the Games operating environment by keeping up with global incident cases and the latest attack methods. The breaches of enterprises and cloud service providers were often reported. By learning from such incidents and repeatedly evaluating how each solution would react to a similar attack on the Organising Committee and whether the current configuration would be sufficient to protect us, we were able to improve our ability to detect new threats and keep the risk under control. By repeating these evaluations, we improved our ability to detect new threats and kept controlling risks. In addition, we used practical exercises to mature the system for events that would not occur on a daily operation. Cyber war games were conducted to simulate possible attacks on the Tokyo 2020 IT systems during the Games, disaster recovery exercises were conducted to confirm recovery procedures under the assumption of a large-scale failure, and technology rehearsals were conducted to simulate actual Games operations through various scenarios. The participants were able to confirm their preparedness for a large-scale security incident.

At Tokyo 2020 Games, 450 million security events from external network were detected, but these preparations enabled us to successfully protect the Games environment. Details are presented in this special issue "5-4 Cyber Security Operations for the Tokyo 2020 Games"[4] and "5-5 Responding to Cyber Attacks during the Tokyo 2020 Games"[5].

4. Review of the Tokyo 2020 Games

The Cyber Security Team prepared utmost for the cyber threats and approached the Games with minimal assumed risks through thorough governance, implementation of optimal solutions based on the characteristics of the Games environment, and efforts to enhance operational maturity.

During the Games, various events occurred, including website attacks, receipt of suspicious e-mails, zero-day vulnerabilities, large numbers of login attempt to Organising Committee staff accounts, suspicion of related organization's account breaches, suspicious websites distributing competition recordings, websites selling counterfeit goods, and the publication of entrance websites leading to suspicious websites. However, we were able to successfully complete the Games without any incidents that would have affected the operation of it.

The biggest success factor was the early establishment of a security governance system and the preparation based on the zero-trust design for a wide range of environments related to the Games. Governance is based on three basic principles : visualization of risks, minimization of uncontrollable risks and elimination of unexpected risks, and assurance of business continuity when faced with imminent risk. In addition to these principles, the Cyber Security Team paid close attention to confirming that what was designed to protect the Games was correctly implemented. This policy was based on the fact that the dependencies between systems were becoming less visible due to the use of cloud environments and other factors, which were increasing risks that could not be controlled. This careful confirmation increased awareness among the parties involved and promoted maturity of security operations.

Although there was a seven-year preparation period between the establishment of the Cyber Security Department and the Tokyo 2020 Games, the time and resources were always limited due to cost constraints. Even in such a situation, the success of the Games was due to the fact that we aimed to control cyber security risks within the expected range, developed a threat information sharing structure over the extensive ICT environment for the Games, constantly addressed the early signs of attack, and made maximum preparations to surpass the attackers, who evolve every day.

5. Japan's Efforts and Legacy

The IOC took an unprecedentedly high level of interest in cybersecurity and provided a variety of support in response to concerns that the systems of the Organising Committee and partner companies were disrupted at the PyeongChang 2018 Winter Games. This includes Cyber Assurance Programme which covered the domains that were assessed due to their criticality to the delivery of the Games, such as Energy, CATV, Website/Mobile App, OMS/ODS, Omega Systems, Transportation, IoT and Autonomous vehicles.

In 2013, the Japanese Government also held the "Liaison Conference of the Ministries and Agencies concerned with the Tokyo 2020 Olympic and Paralympic Games"[Note 1], chaired by the Deputy Chief Cabinet Secretary (Administrative Affairs), and in 2015, the "The Headquarters for the Tokyo 2020 Olympic and Paralympic Games"[Note 2] chaired by the Prime Minister, was established. In 2014, a Security Executive Committee chaired by the Deputy Chief Cabinet Secretary for Crisis Management was established, and a Cyber Security Working Team chaired by the Councillor, Cabinet Secretariat (Deputy Director General of NISC[Note 3]) was set up under the Security Executive Committee to ensure cyber security of the Games in cooperation with relevant ministries and agencies. In 2017, the Security Information Center was established in

(Note 1) Based on the decision of the Chief Cabinet Secretary on October 11, 2013.

(Note 2) Basis for establishment is Article 2 of the Act on Special Measures for the Olympic Games Tokyo 2020 and the Paralympic Games 2020 Tokyo (Act No. 33 of 2015).

(Note 3) Cabinet Cyber Security Center. The English name is National center of Incident readiness and Strategy for Cybersecurity.

(Note 4) "Basic Security Strategy for the Tokyo 2020 Games," Decision of the Security Executive Committee, March 21, 2017.

the National Police Agency to provide necessary information to relevant organizations including the Organising Committee(Note 4). In April 2019, the Cyber Security Response Coordination Center, which was operated by the NISC, was established in the Cabinet Secretariat and it was decided that threats and incidents related to cybersecurity at the Games would be shared, incident response, etc. would be carried out in cooperation among the relevant organizations in cooperation with each other. And they conducted the monitoring to handle incidents for the public infrastructure and related environment around the Games to cooperate with other related organizations(6). The Cyber Security Response Coordination Center coordinated support for response to incidents, conducted cyber incident response exercises, shared cyber threat information, and provided an information sharing platform (JISP : Japan cyber-security Information Sharing Platform). The Organising Committee also participated in these efforts, and promptly shared information with government agencies, security-related organizations, critical service providers, sports-related organizations, and others through JISP. (For details, see "3.3 Organising Roles with Government Agencies" in this special issue "5-2 Cyber Security Governance of the Tokyo 2020 Games"(2)).

The Cyber Security Strategy approved by the Cabinet on September 28, 2021, describes the efforts of information sharing and collaboration by the public and private sectors in cooperation as part of the framework development of the National CSIRT (CSIRT/CERT). The strategy aimed to raise the overall level of Japan's cyber security not only during large-scale international events but also during normal times by utilizing the knowledge and know-how gained from the operational experience and risk management activities for the Tokyo 2020 Games. It also included the sharing of knowledge gained from the Tokyo 2020 Games to contribute to the international community(7). The cyber security measures taken at the Tokyo 2020 Games will be utilized throughout Japan in the future.

References

(1) International Olympic Committee, "Olympic Games Tokyo 2020 watched by more than 300 million people," December 8, 2021. https://olympics.com/ioc/news/olympic-games-tokyo-2020-watched-by-more-than-3-billion-people (viewed January 31, 2022)

(2) H. Ibayashi, K. Tamai, M. Onishi, and Y. Nojiri, "5-2 Cyber Security Governance of the Tokyo2020 Games," Journal of IEICE, vol. 105, no. 8, supplement, pp. 255-263, Aug. 2022.

(3) K. Tamai, Y. Nojiri, N. Hosoda, and H. Ibayashi, "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games," Journal of IEICE, vol. 105, no. 8, supplement, pp. 264-271, Aug. 2022.

(4) M. Onishi, N. Hosoda, K. Nakanishi, and H. Ibayashi, "5-4 Cyber Security Operations for the Tokyo 2020 Games," Journal of IEICE, vol. 105, no. 8, supplement, pp. 272-278, Aug. 2022.

(5) M. Onishi, N. Hosoda, K. Nakanishi, and H. Ibayashi, "5-5 Responding to Cyber Attacks during the Tokyo 2020 Games," Journal of IEICE, vol. 105, no. 8, supplement, pp. 279-284, Aug. 2022.

(6) NISC Tokyo 2020 Group, "Cyber Security Measures for the Tokyo Games and Future Action Policies." https://www.nisc.go.jp/active/2020/index.html (viewed February 2, 2021)

(7) "Cyber Security Strategy," Cabinet Decision on September 28, 2021. https://www.nisc.go.jp/materials/index.html (viewed February 2, 2022)

(Received February 9, 2022 ; Revised March 23, 2022)

SAKA Akira

Akira SAKA joined the National Police Agency in 1981. He was a visiting fellow at WCFIA, Harvard University, and a professor at Graduate School of Media and Governance, Keio University from 2008 to 2010. He served as CISO of the Tokyo 2020 Olympic and Paralympic Games Organising Committee. He is CISO of the Digital Agency, Director of the Japan Cybercrime Center (JC3), and Executive Director of the Public Policy Research Institute (CPP).

IBAYASHI Hiroaki

Hiroaki IBAYASHI 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 will be responsible for the overall security operations in the SOC.