Cyber Security Governance of the Tokyo 2020 Games

IBAYASHI Hiroaki TAMAI Kuniharu ONISHI Masaki
NOJIRI Yasuhiro

Abstract

In the Olympic and Paralympic Games Tokyo 2020, each of the 52 Games management organization constructed and operated the wide variety of systems in cooperation with various Games stakeholders. Comprehensive risk control needed to be implemented for these wide-ranging targets, while thorough security measures based on the zero-trust premise were required. Based on this issue, we introduce the security governance implemented by the Organising Committee.
Keywords : Tokyo 2020 Games, Security governance, Security policy, Security architecture

1. Preface

The nature of the Olympic and Paralympic Games made it difficult to control security policies at an appropriate level, and security incidents had occurred frequently in the past Games. In addition, as the IT system environment became more advanced and was more widely used, Functional Areas (FAs) actively selected cloud environment, making it even more difficult to control risks due to the wide range and variety of objects to be protected. The governance based on organizational collaboration was being increasingly important to protect a complex and wide-ranging environment.

In this report, the cyber security team introduces the security governance efforts that were implemented horizontally to the Organising Committee and the Games stakeholders.

IBAYASHI Hiroaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
TAMAI Kuniharu
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
ONISHI Masaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
NOJIRI Yasuhiro
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.255-263, August 2022

2. Characteristics of the Olympic and Paralympic Games

Before introducing the governance efforts, the characteristics of the Games are summarized as a precondition.

First of all, as the world's largest sporting event, the Games are the target of various cyberattacks and crimes. As described in this special issue, "5-1 Summary of Cyber Security Activities at the Tokyo 2020 Games, Part 2 : Cyber Threats to the Games"[(1)], the Games must be appropriately prepared not only for cyberattacks that directly affect the operation of the Games, but also for attacks that indirectly affect the reputation of the Games by destroying its credibility and value (reputation risk), and for crimes targeting economic benefits. In particular, when dealing with the attacks intended to disrupt the operation of the Games, it is important to gather background information on the attack activities, and it is always necessary to consider peripheral information such as anti-doping issues and the national prestige. In some cases, a message such as, "We are fully prepared for the Games and have a complete security defense system in place", may trigger the attack.

Having the large number of the Games stakeholders is also one of major characteristics of the Games. In the current attack trend, the attackers often target those stakeholders who have weak security measures first, and then attack the main target in a chain reaction starting from there. We need the protection that included all stakeholders involved to successfully lead the Games. About the situation of cyberattacks at the PyeongChang 2018 Games was announced by the U.S. in October 2020. There were reported cases of attacks that originated from companies with weak security measures, and it can be said that this supply chain risk had indeed turned out to be a reality.

In addition to the diversification of the IT system environment, the Tokyo 2020 Games saw the progress a more global operation and a wider range of venues for the Games, so it was the important and significant challenge to establish how to ensure the thorough governance and protection against the diversity of organization and environment.

This diversity of IT system environment was also the same situation within the Tokyo 2020 Organising Committee. The Organising Committee included employees seconded from various sponsor companies, staff hired by the Organising Committee, contractors, and many volunteers from different cultures in the 52 FAs, which resulted in the large variation in IT literacy. Furthermore, there was the special nature of the event in that several thousand people were recruited at once for the event from three months prior to the Games. In terms of the systems, the Back-Office Network (BON) used by the Organising Committee members for their work, the Competition Network (CPN) connecting the venues, and the Olympic Technology Network (OTN) connecting various services such as the dedicated VLANs assigned for the Games stakeholders, and the websites such as the official website, ticket sales website, and the Games information distribution system for the media, etc., located on the Internet, were existed as four domains to protect from cyberattacks. Each of the four domains required security measures based on completely different policies.

It was also characteristic that the Tokyo 2020 Games was the first Games to be held under the EU General Data Protection Regulation, which was also one of the characteristics of the Games and a sensitive matter. More than the past Games, we were required to clarify the confidential information held by the system and to manage it thoroughly.

Another unprecedented challenge was the drastic changes required to deal with the Games postponement and the need for no-spectators due to the coronavirus disease 2019 (COVID-19). In order to protect an environment of increased complexity for an additional year on a limited budget, more insight was required in terms of security measures.

Against this background, we had to protect the operation of the Games from cyberattacks and we had to lead the Games toward success.

3. Games-related Systems and Organization Structure

3.1 Games-related Systems and Development Structure

The systems supporting the Olympic and Paralympic Games Tokyo 2020 (hereinafter, referred to as "Tokyo 2020 Games") were in an extremely various environment. Each FA determined the system requirements needed for the Games, and were contracted out the development of these systems to various companies. Some systems were deployed in the data centre of the Organising Committee, while others were deployed in the cloud, and the domains that housed them varied. For these, appropriate governance needed to be implemented in cooperation with each FA and developer to ensure that the details of the system were fully understood and that security measures were implemented for them.

In addition, it was not only the systems developed by FAs that needed to be protected. The same security governance was also required for the systems managed by the Games stakeholders to prepare for attacks on the supply chain environment.

3.2 Complexity of Games-related Systems

In the Rio 2016 Games, all systems were constructed in the data centre of the Organising Committee, but in Tokyo 2020 Games, 70% of the systems were constructed by using cloud services and outsourcing services, Business Process Outsourcing (BPO) from the viewpoint of cost reduction. The optimal configuration differed for each system, so various external services were selected. In particular, in the case of BPO, the system environment was prepared by the BPO provider, making it difficult to grasp the details and increasing the number of uncontrollable risks.

The considering these situations, the cyber security

team expedited security check and review for all systems in the Organising Committee to comply with the IT security policies and architecture concurrently with the definition these policies and architecture that should be referred to for security implementation. Of course, these activities were included the aforementioned cloud services and BPO. The security checks consisted of a security review to confirm that the security functions were properly incorporated in compliance with the policy and architecture, based on detailed interviews according to the check sheets, and security tests to confirm that the finished system would function properly against the assumed threats. As the governance control, these were the important activities to ensure visibility of risk and a security baseline against cyberattacks.

In recent years, not only IT systems but also control systems such as central monitoring systems, power equipment, and air conditioning monitoring systems in the venues have become targets of cyberattacks. A penetration test was also conducted for control systems such as power and air-conditioning systems at key venues.

3.3 Organizing Roles with Government Agencies

With the roles of government agencies are described below. The Organising Committee was responsible for the environment procured and operated by the Organising Committee and the environment prepared by partners and suppliers related to the operation of the Games. For monitoring/incident handling of critical infrastructure, social infrastructure of the host city, and sports-related organizations, the government was responsible for promoting efforts to strengthen countermeasures in each entity, and for risk assessment and information coordination (Figure 1). Regarding venue facilities, it was decided that existing facilities would be treated as social infrastructure, but that additional facilities and systems to be constructed exclusively for the Tokyo 2020 Games would be managed by the Organising Committee.

The role of the government in cyber security measures for the Games varies by country. For the Tokyo 2020 Games, in addition to the role and responsibility mentioned above, we also shared threat information of the Internet space and exchanged indicator information, which was information on traces of cyberattacks. Recently, zero-day attacks, which target vulnerabilities of programs which have not been updated, occur frequently, so sharing threat and indicator information was extremely important.

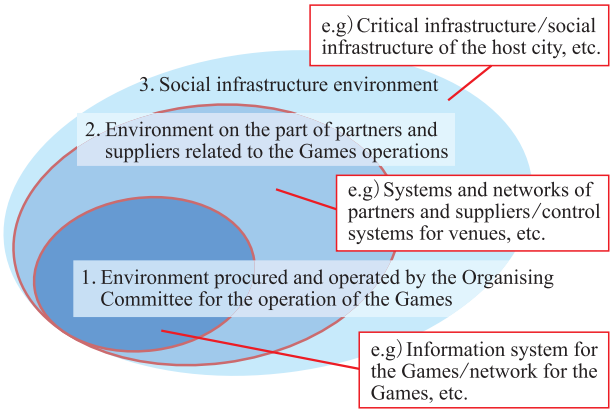

Figure 1 Organization of Roles with Government Agencies

4. Risk Control

The systems that supported the Games were diverse and large-scale, numbering more than 200 systems. The security risks associated with these systems needed to be controlled.

For risk control, it was needed to conduct : the visualization of risks based on assumed threats ; the minimization of uncontrollable risks and the elimination of unexpected risks ; the assurance of business continuity in the event that the risk become apparent.

There were a wide range of threats that needed to be assumed. The threats included : theft of confidential information by Advanced Persistent Threat ; PC terminal outage by ransomware attack ; malware infection via e-mail, Web, external storage media, etc. ; loss of availability by wiper-type malware ; service down by denial-of-service attack ; falsification of information assets ; information leakage by internal fraud, etc. ; phishing campaign by spoofed e-mails, etc. ; and data loss due to malware infection via e-mail, Web, external storage media, etc. ; confusion by fake website/fake mobile application/fake ticket-sales site, etc., and were too numerous to list. In response to these threats, it was necessary to implement appropriate security solution and system hardening.

It was not enough to simply implement a solution. It was essential to mature the security operation that could use these solutions. And, we needed to enhance the capability to triage quickly in the event of the various attacks.

However even with these efforts, there were still risks

that could not be controlled. These uncontrollable risks included zero-day vulnerabilities and attacks that targeted them, as well as cases caused by configuration mistakes and operational errors. It was also important to formulate and prepare the availability plan to ensure the continuity of the Games even if such risks happened. At the PyeongChang 2018 Games, a cyberattack just before the opening ceremony brought the consequence of many servers and PC terminals unavailable, but they were temporarily recovered overnight to avoid any impact on the next day's competition. This was made possible by the posture that the team had an appropriate understanding of the uncontrollable risks that an attack beyond expectations could occur and had prepared a recovery plan in advance. In addition to preventing cyberattacks, it was necessary to enhance resilience, such as the ability to recover quickly and maintain business continuity in the event of an attack.

Furthermore, the effective use of cloud services and BPO increased in the Tokyo 2020 environment, and the number of uncontrollable risks also increased. As the countermeasures against these risks, in addition to the three measures mentioned above, we had to periodically conduct Audit, Table Top Exercise, practical exercise by Red team called Cyber War Games, various Rehearsals such as Technology rehearsal, and vulnerability assessments as security check and test. Then, we took scrupulous care of the verification and confirmation that the security designs to secure the Games from assumed threats were correctly implemented and that security function worked as expected.

Through these efforts, we minimized the risks that could not be controlled, prepared the various plans to maintain business continuity against remaining risks, repeated improvements and remedial actions, and established the security system to overcome the Games in a perfect condition.

5. Security Governance of the Organising Committee

In section 5, we will introduce the governance efforts implemented by the appropriate cyber security team for the various systems supporting the Games.

5.1 IT Security Policy

Two security policies were issued : the Information System User's Guideline which served as a guideline of the Organising Committee, and the IT Security Policy which defined the security requirements to be followed by IT suppliers providing systems and services.

The Information System User's Guideline defined the policies that the members of the Organising Committee must follow in terms of security when using IT systems in their daily work. The Organising Committee members were a diverse group of people from different cultures, and their IT literacy varied widely. It was released in July 2015 with the aim of resolving this issue. It had been used until the end of the Games, with revisions made each time as the IT system expanded.

The IT Security Policy was a document that defined the requirements for risk controls to be implemented in the four domains for the Organising Committee systems. In the past Games, the system environment of the Organising Committee and the Games systems construct by Atos and Omega, were operated under different policies, and it made the governance difficult. To solve this problem, we worked with Atos, a sponsor in the IT integrator category, to define four domains (BON, CPN, OTN, and websites), and established baseline and specific policy followed by each domain. The IT security policy also formulated documents that provide detailed guidelines such as information classification policy, accounts and passwords policy, patch management policy, and security incident response policy. These policies were widely deployed not only within the Organising Committee, but also to IT suppliers who constructed and operated the system environment. Moreover, the Organising Committee conducted security reviews of all systems, and this brought increasing the awareness of IT system suppliers and reducing the variation in security quality.

5.2 IT Security Architecture

The IT security architecture was developed with Atos according to the requirements of each four domains, which were different in characteristic, in order to meet the IT security policy establishment, and further clarify the specific implementation image of the policy. However, even during the seven-years' examination period, the evolution of security technologies had made great progress, and effective solutions had changed fluidly. Catching up with these changes and updating the IT security architecture continued until just before the Games. Flexibility and continued technological and maturity enhancements were key factors in the success of the Games.

At the point of selecting solutions for the architecture,

the team also ensured to clarify the mapping for the identified security threats and the selected solutions. This was not only to prevent the omission and leak of solutions, but also made it easy to verify which solutions would work how, the attack would be successful if a similar one was to occur in the Organising Committee environment by using the compromised cases on other organizations. This was one of the factors that supported the maturation of security operations.

The basic concept of implementing solutions was multi-layered defense. Details are described in this special issue, "5-4 Cyber Security Operations for the Tokyo 2020 Games"[(2)].

From the perspective of cost efficiency and operational standardization, we also organized the implementation of common environment that could be shared by each domain. Regarding to BON, CPN and OTN, followings were examples that some core network sections and authentication functions were shared, a common endpoint security solution was adopted, and an integrated security information and event analysis environment called Security Information and Event Management (SIEM) were shared. However, shared implementation could also pose a security risk. Originally, the architecture was designed based on the assumption of zero-trust[(3)] and the BON, CPN, and OTN did not affect each other, even if the compromised event happened, but the PyeongChang 2018 Games allowed the internal spread of malware infection (Lateral Movement), which required a stronger awareness of network isolation. Although the shared points that were ultimately adopted were scrutinized based on these considerations, it was decided to manage them as the potential risk.

Unfortunately, there was the domain that had strayed on an application of the architecture. The OTN environment which was set up just before Games, had a risk to be connected by and the system devices with inadequate security measures, or in some cases PC terminals already infected with malware, as the Games stakeholders brought various systems. In fact, incidents occurred at every Games. To implement solution in view of this risk was considered, but the Director of Technology Service and the network team didn't make a decision to implement the solution due to cost reason. However, just before the Games, the IOC directed the policy change of this architecture and the firewall on the OTN was implemented to visualize and block unauthorized traffic in a hurry. Cost efficiency was also an important issue for the Tokyo 2020 Games, and the decision was always difficult.

5.3 Security Check

In order to maintain the security level of the entire Organising Committee system above a certain level, security checks were made mandatory at each milestone toward system implementation.

At critical points before planning, design, and operation, security reviews were conducted to ensure that the IT security policy and IT security architecture were applied without omissions.

After operation, IT security audit and IT configuration audit by the third-party perspective were conducted to confirm that the policy and architecture were properly implemented and operated. As mentioned above, the structure of the Tokyo 2020 Games system tended to be opaque due to the use of cloud services and BPO, making it difficult to control risks.

Therefore, it was important to visualize the results through the periodic audits.

5.3.1 Security Review

Security review was conducted not only for system service established or used by the Organising Committee, but also for cloud services and system services used by BPO as a concrete measure of the outsourcing management.

The review was conducted at each important milestone before operation as shown in Figure 2.

① Before RFP Distribution

Confirmation that security requirements were included in the RFP.

② Before Completion of Basic Design

Confirmation that security requirements were included in the basic design.

③ Release Judgement before the Operational Commencement

Confirm that security requirements were properly implemented in the system/service and that no security issues remained.

Security requirements were likely to be the first target in the cost reduction. It was particularly important to review the RFP at the time of ① in order to clearly state that the Organising Committee required solid design, implementation and operation. The checklist used in the review was an original version for the

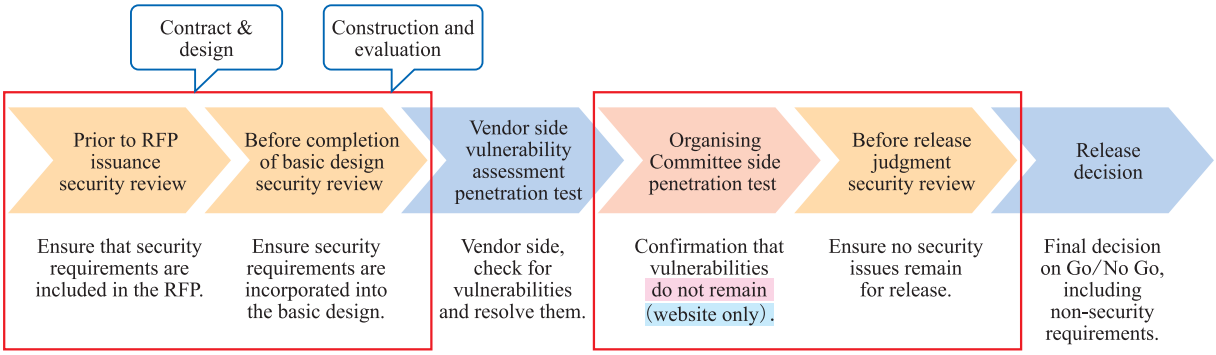

Figure 2　Key Milestones for Security

No. Item	Item	Compliance
1	Reporting and Auditing of Performance Status using Check Sheets	External service providers shall comply with domestic and foreign laws, regulations, and rules of the Corporation in their entrusted work. The external service provider shall comply with domestic and foreign laws and regulations, and the rules and regulations of KICR in the commissioned work. The external service provider shall fill in the check sheet for the information systems (including all information systems for data linkage) to be used in the entrusted work and information security measures to be taken in the implementation of the entrusted work, and submit it at the time of proposal. After the contract is concluded, the check sheet shall reflect the status of implementation of information security measures, including those of subcontractors, etc., and shall be reported to the Corporation periodically (at least once a year) at the time of release judgment as determined by the Corporation and after the release. Furthermore, the information security audit conducted by the Corporation shall be conducted at the request of the Corporation. If there are any findings in the report or audit results, corrective actions are to be taken.
2	Management System for Information Security	After the contract is concluded, the external service provider must designate one information handling manager who is in a position to supervise information handlers and information handlers including subcontractors (hereinafter referred to as "information handlers, etc."), and report the contact information, roles and responsibilities of information handlers, etc. to the Corporation. In addition, any changes in the information handlers, etc. must be promptly reported to the Corporation.
3	Information Security Training	After the contract is concluded, the external service provider shall formulate a plan for education and awareness of information handling and prevention of information leaks for information handlers, etc., record the results of such education and awareness, and submit the plan to the corporation at least once a year.
4	Incident Response Training	External service providers must comply with requests to participate in incident response training conducted by the corporation.
5	Establishment of Information Handling Rules and Management of Confidential Information	External service providers shall establish and comply with rules for handling information handled in information processing operations. In addition, the External Service Provider shall record the management status of confidential information in a ledger, etc., and submit the ledger upon request from the Corporation. In addition, when confidential information is to be disclosed or provided to a third party, or when equipment containing confidential information is to be taken out of the managed facility, prior permission must be obtained from the Corporation. However, this excludes cases in which the Corporation recognizes that confidential information can be mutually provided among multiple businesses that have signed a non-disclosure agreement (NDA) with the Corporation in advance, and in which confidential information labeled "For Project Use" is shared among such businesses.
OM : Measures for OS and middleware		
OM-01	Do not install or activate services that are not required for the operation or maintenance of the website	If services other than those originally required for website operation, maintenance, etc. are enabled, there is a possibility of an attack using those services. Also, since the administrator is not aware of security measures for services that are not used, patches are not applied and vulnerabilities may be exposed. Therefore, unless there is a special reason, it is important to stop all services other than those that are originally necessary.

Figure 3　Security Check Sheet

Tokyo 2020 Games which created by extracting the necessary elements to comply with the IT security policy and the IT security architecture from the National Institute of Standards and Technology (NIST) SP800 series, PCI DSS, and various guidelines issued by security organizations and groups in Japan. The checklist shown in Figure 3 was not only created once, but had to be continuously updated to meet the needs of each era and organization, as attack methods and security requirements changed with the times.

The security review was also very useful for the cyber security team to visualize the risk of each application. Especially, the Tokyo 2020 Games was the first Games to be held under the EU General Data Protection Regulation. Appropriately grasping possession situation of the personal information through this review and following up with compliance officers based on this information, helped us to ensure proper information management.

The number of reviews was 838 in total as a formal meeting, and more than 1,000 including informal pre-conferences. The fact that the review functioned as the standard process of the Organising Committee helped to increase the security level.

5.3.2 Security Testing

It was very important to verify that the security measures specified in the design are properly implemented and that the implemented functions worked as expected. Cases frequently occur are that implemented security functions do not work properly, or unintended security bugs (vulnerabilities) remain. Security testing was a very effective way to check these issues.

The Organising Committee made it mandatory to conduct penetration test (pen test) and vulnerability assessments, and conducted web pen test, platform and application vulnerability assessment, and infrastructure pen test (including brute-force test) to meet the domain and system. These tests were supposed to be conducted by the vendor before site release as a part of system development. In addition to these vendor-side test, the Organising Committee decided to conduct thorough the inspection by adding web pen test before site release to control the risks. For the servers located in the BON and CPN, the Organising Committee conducted post-release vulnerability assessment on a quarterly basis, and carried out the cycle of taking necessary remediation actions.

In the pen test and vulnerability assessment conducted by the Organising Committee, test items in accordance with the OWASP Testing Guide[4] were implemented to keep test quality. Moreover, tests and the improvement following-up of all systems were conducted, as the policy of presenting detailed procedures (reproduction methods) for finding vulnerabilities Corrective measures based on vendor test results varied between vendors, but the addition of testing by the Organising Committee achieved a uniform baseline.

Tests by the Organising Committee were required the implementation to a very large number of systems. In order to conduct tests agility and with mobility to a large number of test targets, we decided as our policy to establish a permanent test team within the Organising Committee. This structure enabled parallel testing to be carried out even during peak testing periods, such as when many systems were released at the same time.

Due to the wide variety of systems in each FA, the total number of hours spent by the testing team was 59,840 for the pen test and 8,320 for the vulnerability assessment. (The total number of hours for the pen test was 7.5 times that of the Rio 2016 Games (8,000 hours) ; no comparable figures were available for vulnerability assessment.) The success of these testing teams was one of the factors that contributed to the success of the Games, as they were the last line of defense before the release to ensure the security of the systems and services.

In addition to the above-mentioned security tests, DoS simulation test to verify and enhance DDoS resistance, and Cyber War Games which was the practical exercise were conducted. The former is introduced in this special issue, "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games, 5.2 : DoS Simulation"[5], and the latter in "5-4 Cyber Security Operations for the Tokyo 2020 Games, 4.1 : Cyber War Games"[2].

5.3.3 Audit

As attack methods were constantly evolving, it was necessary to keep up with them and continue to enhance solutions and operations even after the system was released. In order to confirm that this approach was functioning properly, and to confirm that there were no omissions in the risk identification by a perspective different from the security testing, IT security audit by the third-party was conducted to visualize the risks even after operation. However, same as the security test, the audit required a large number of operations. Therefore, the audit was conducted in order of priority

for significant assets, such as those that could affect human lives, the operation of the Games, economic impact, and confidential information.

IT Configuration audit were also conducted for the BON and CPN environments, which housed a large number of considerable systems and were prone to cause slack of setting by frequent configuration changes. On the other hand, since each system shared the same basic configuration following the common architecture, it was possible to verify the configuration collectively by auditing the IT Configuration at one time. Considering these characteristics, we conducted a follow-up to remediate any problems that were detected and confirmation by audit. This activity was conducted on the regular basis and continued until just before the Games. Especially this audit was very useful to detect uncovering problems such as the failure to disable unnecessary applications and loose hardening on the server, leaving unnecessary communication permissions on the network, and leaving accounts with excessive authority, which greatly contributed to the correction of loose architectural implementation.

5.4 Strict Security Settings and Checks of Exception Handling

The Organising Committee was characterized by the fact that it was an assembly of various members from widely different cultures, and also it was an organization which was constantly changing with the number of members increasing rapidly just before the Games. In the busiest situation just before the Games, education and training for the increased members were not provided enough, and there was the risk that compliance with the IT security policy could not be expected. With this in mind, the security settings of the system were meticulously configured, and our system was created and implemented to thoroughly visualize and detected suspicious behavior, thereby creating the environment that did not rely solely on the efforts of cyber security team members and the literacy of the Organising Committee members. User's behavior was one of the most difficult risks to control, but the implementation of strict security settings and the visualization structure were the success factors of the Games because we were able to achieve the minimization of risks.

Particularly, the use of the free cloud environment had been a target of attacks in past Games. To protect the Organising Committee's information and minimize the risk of information leakage, the use of free e-mail including forwarding to such e-mail accounts, and free storage were prohibited in both the policy and the system settings.

Followings were also restricted in detail : the use of executable files ; scripts ; commands, macro files ; etc. As they were often used for cyberattacks, the function of browser extensions, tethering, Bluetooth, communication between terminals, USB connection, and so on. These restrictions provided the environment which prevented the incident even if an unauthorized operation was performed by the mistake.

Software installed on PC terminals was also prohibited by both the policy and the security settings to prevent the adding of suspicious software. However, the installation of additional software was often essential for the work of each FA. For such cases, we set up a flow called "exception request" to allow the installation of such software after the review by the cyber security team. The number of sponsors of the Tokyo 2020 Games was the largest ever, and we had to cover many different topics of the system requirements, so the number of "exception request" from each FA was more than 1,000, resulting in a large number of reviews. And also, the process did not end with the approval of the software installation. As with existing standard software, vulnerability management was required. For vulnerability management, we collected and analyzed information from multiple sources in addition to open source information, and reinforced the monitoring of update application status by using a vulnerability tracking tool to ensure prompt update response.

5.5 Security Awareness

Although we mentioned in 5.4 that human behavior should not be expected, it was important to enhance the level of maturity in order to prepare utmost for the success of the Games. It was also important to observe it at a fixed point. These meant that we conducted to raise security awareness for three perspectives : ① the user (staff/executives) perspective ; ② the business owner perspective of each FA ; and ③ the operator perspective of the Security Operation Centre (SOC).

The three main efforts are as follows :

① User perspective

Targeted e-mail training, e-learning by using incident cases of the global and the Organising Committee, and user hearing through alert detection.

② Business owner perspective

Periodic IT security audit, table top exercises, DoS testing of important web sites.

③ Operator's perspective

Table top exercise, Cyber War Games, Disaster Recovery Rehearsals, Technology Rehearsals, periodic vulnerability assessment (check preparations for zero-day).

Activities to enhance security awareness from the operator perspective are described in detail within "5-4 Cyber Security Operations for the Tokyo 2020 Games"[2].

The activities described in ① were widely deployed not only to the staff of the Organising Committee, but also to the Games stakeholders, and were conducted repeatedly and continuously. The activities in ② and ③ enhanced the maturity of the operation and helped to build a face-to-face relationship with the cyber security team in terms of information collaboration.

6. Conclusion

In this article, we have described how we promoted the security governance activities to appropriate risk control for the object to be protected from cyberattacks.

The sequent sections, "5-3 Solutions for Cyber Security Challenges of the Tokyo 2020 Games"[5] and "5-4 Cyber Security Operations for the Tokyo 2020 Games"[2], will be described in detail how we implemented Defense in depth solution, enhanced operational maturity, and dealt with various cyber events.

References

(1) A. Saka and H. Ibayashi, "5-1 Summary of Cyber Security Activities at the Tokyo 2020 Games," Journal of IEICE, vol. 105, no. 8 supplement, pp. 249-253, Aug. 2022.

(2) M. Onishi, H. 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.

(3) Special Issue : Technology and Innovation in the Olympic and Paralympic Games Tokyo 2020, "5. 'Terminology' Zero trust," Journal of IEICE, vol. 105, no. 8 supplement, p. 254, Aug. 2022.

(4) Special Issue on Technology and Innovation in the Olympic and Paralympic Games Tokyo 2020, "5. 'Terminology' OWAST Testing Guide," Journal of IEICE, vol. 105, no. 8 supplement, p. 254, Aug. 2022.

(5) 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.

(Received 28 February 2022 ; Revised 18 March 2022)

IBAYASHI Hiroaki

Hiroaki IBAYASHI has been working on cloud computing and security business 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 in charge of overall security operations at the SOC.

TAMAI Kuniharu

Mr. Kuniharu TAMAI is a Director of Cyber Security Department, Technology Services Bureau, seconded to the Tokyo 2020 Organising Committee in 2018. During the Games, he was in charge of security solution operations at the SOC.

ONISHI Masaki

Masaki Onishi is a security manager at NTT Communications Corporation, and has been seconded to the Tokyo 2020 Organising Committee since 2018. He has been seconded to the Tokyo 2020 Organising Committee since 2018, where he was the Security Operations Section Chief of the Cyber Security Department of the Technology Services Bureau. During the Games, he was in charge of security incident response at the SOC.

NOJIRI Yasuhiro

Mr. Yasuhiro Nojiri is engaged in CSIRT establishment support and education at NEC Solution Innovators. He was seconded to the Tokyo 2020 Organising Committee, where he was in charge of security solutions in the Cyber Security Department of the Technology Services Bureau. During the Games, he oversaw the operation of security solutions at the SOC.