Network Security

Takashi Mishina, Akiko Matsuhashi, Takemi Nisase, and Hidehiro Shito

Abstract

Events that attract worldwide attention, such as the Olympic and Paralympic Games and international exhibitions, have become easy targets for cyber attacks, and it is no longer rare to hear of reports of damage from such attacks. The Olympic and Paralympic Games Tokyo 2020 was held in 2021 after a one-year delay due to the novel coronavirus (COVID-19), and NTT, as a Gold Partner (Telecommunications Services), had the responsibility of managing the network infrastructure supporting the Tokyo 2020 Games, thus dealing with the threat of cyber attacks. This article describes how NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) of NTT Social Informatics Laboratories faced cyber attacks as the representative computer security incident response team of the NTT Group.

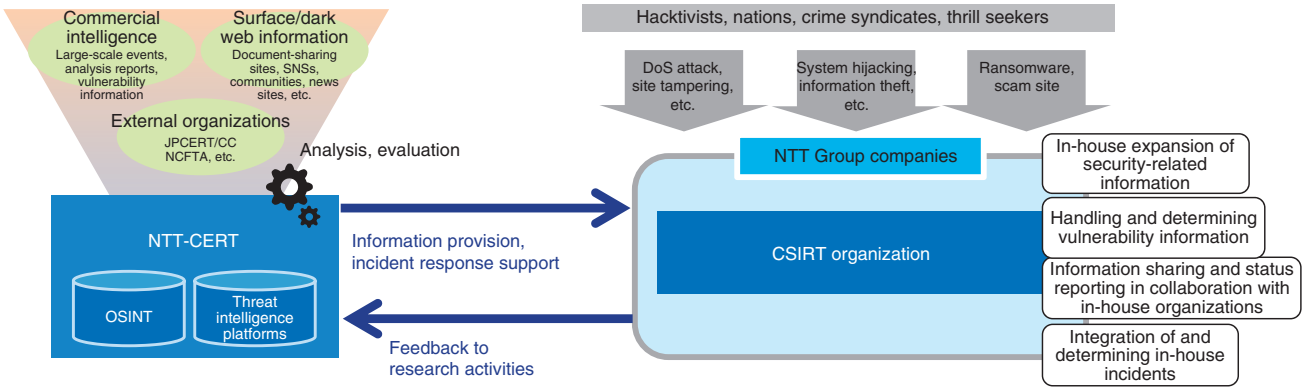
Keywords: information security, cyber attack, CSIRT

1. Olympic and Paralympic Games and cyber attacks

The Olympic and Paralympic Games is an international event with a long history. It attracts worldwide attention, therefore, it can become a target of many parties with a variety of malicious intentions. The event can be misused as a site for advancing political agendas, swindling money, or generating a loss of confidence in the host nation by inducing failure. The *modus operandi* of attackers having such malicious intentions have begun to spread to cyberspace beyond physical activities. In past Olympic and Paralympic Games, a variety of attacks having the potential of impacting their operations and management have been confirmed. These include disruptive acts caused by denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, the breaching of systems belonging to organizations related to the Games, and targeted attacks toward malware infections. To obtain results at a single international event, attackers have been watching for opportunities and refining their techniques. Organizations related to the Olympic and Paralympic Games must therefore implement extensive and reliable systems to protect the Games from such advanced attacks. As a Gold Partner (Telecommunications Services) of the Olympic and Paralympic Games Tokyo 2020, NTT had the important responsibility of managing the network infrastructure supporting the Tokyo 2020 Games, thus having to deal with the threat of cyber attacks. This article introduces the activities of NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) of NTT Social Informatics Laboratories at the Olympic and Paralympic Games Tokyo 2020.

2. NTT-CERT activities at Olympic and Paralympic Games Tokyo 2020

NTT-CERT, a research group operating within NTT Social Informatics Laboratories, acts as the representative computer security incident response team (CSIRT) of the NTT Group (**Fig. 1**). NTT-CERT activities, which do not include the operation of equipment, have two major objectives: (i) collect information and share that information seamlessly with NTT Group companies to prevent cyber attacks from occurring, and (ii) provide support to minimize the damage caused by actual incidents and prevent their reoccurrence. NTT-CERT also feeds back the knowledge gained from such activities to research



NTT-CERT main activities
(1) Information collection & analysis
(2) Incident response support
(3) Technology surveys, product evaluation/education

JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
NCFTA: National Cyber-Forensics and Training Alliance
SNSs: social networking services

Fig. 1. Role of NTT-CERT.

activities and promotes research toward more advanced and robust security technologies.

As described above, the NTT Group had the responsibility of creating and maintaining a safe and secure network infrastructure in support of the Tokyo 2020 Games. Therefore, it was essential that NTT-CERT functions be enhanced to protect the NTT Group and network infrastructure from a diverse array of attackers from around the world. As an organization related to the Tokyo 2020 Games, we drafted a policy of preventing the possibility of a cyber attack before it occurs, and if an incident should occur, of minimizing any damage and impact on the Tokyo 2020 Games. We focused our efforts on enhancing our information collection and analysis functions.

Since NTT-CERT possesses no network facilities that it directly operates, the target of its information collection is mainly external open source intelligence (OSINT). However, collecting such a large volume of randomly arranged OSINT information would be nearly impossible no matter how many people are assigned to the task. We decided to prioritize the type of threat analysis to be conducted for the Tokyo 2020 Games and the information that should be collected. We analyzed cyber attacks that would seem likely to occur at the Tokyo 2020 Games by analyzing threats from the following four viewpoints: 1) What kind of attacker or organization using 2) what type of attack technique and having 3) what purpose would mount an attack on 4) what attack target? On the basis of these four viewpoints, it became possible to organize information in terms of what attack target should be prioritized and protected by NTT-CERT and what information on attack techniques should be prioritized and detected, and on the whole, to classify with good efficiency the information that should be prioritized and collected. It was first necessary to list and analyze as many cyber attacks as possible that could occur at the Tokyo 2020 Games.

With this in mind, we began by collecting information on cyber attacks that occurred in the past. Ranging from the Olympic Games London 2012, during which full-fledged cyber attacks occurred, to the Olympic Winter Games PyeongChang 2018, during which targeted attacks were confirmed, we analyzed both Japanese and overseas news articles on past Olympic Games, reports issued by security vendors, etc. To obtain a comprehensive understanding of attacks that should be expected, we broadened our survey range to attacks that targeted personnel related to the Olympic Games and spectators and prepared a list of damages that occurred and damages that could be assumed. To carry out the threat analysis described above, we classified these data into "attacker," "purpose," "technique," and "target."

After using that list to determine "attacker," "purpose," and "technique" for which an attack could be detected from outside sources, NTT-CERT prioritized

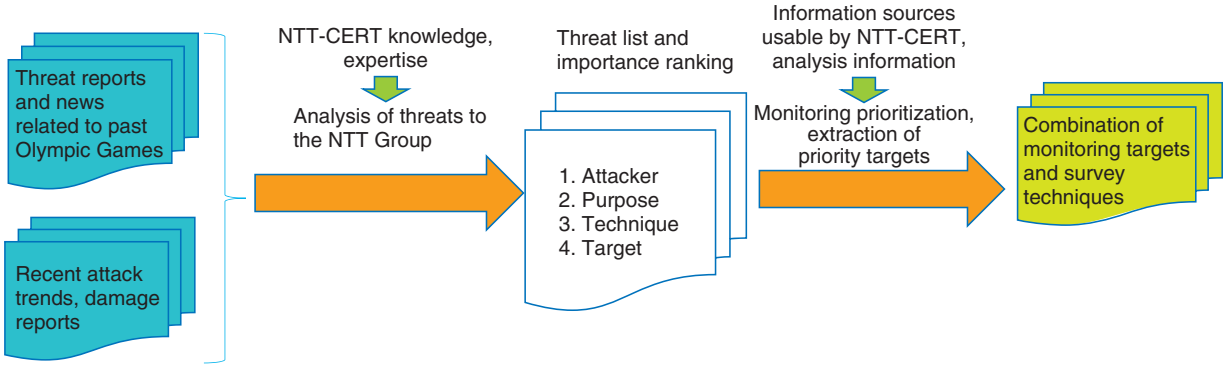


Fig. 2. Analysis toward enhanced monitoring.

the information that should be collected from the viewpoint of "target." Specifically, attacks for which the NTT Group would be the direct attack target were set as top priority followed by attacks on personnel related to the Tokyo 2020 Games that could have an impact on the NTT Group and attacks on spectators in that order. "Technique" and "purpose" were prioritized on the basis of what NTT-CERT could detect from OSINT information. For example, while the threat level of a targeted mail attack targeting the NTT Group was high, it would be difficult to directly detect the receiving of such mail at NTT-CERT, so devoting resources there would be inefficient. We therefore studied how the NTT Group could be protected from such threats on the basis of information that could be detected from the outside. We considered, for example, detecting phishing sites having domains similar to those of NTT that might act as an inducement, determining whether stolen information is being sold on the dark web, and checking for the existence of hacktivists (persons engaged in hacking activities to advance their social or political agendas) who warn of politically oriented attacks. In short, we investigated a variety of attacks that could be detected from NTT-CERT's position (**Fig. 2**).

After prioritizing the information that should be collected, the next step was to enhance the range and volume of information collection. Until recently, NTT-CERT's main target of information collection had been the surface web as well as dark web information from intelligence vendors with survey languages being Japanese and English. However, as described above, it was considered insufficient to detect as much information as possible on information for sale on the dark web or on hacktivists' agendas, so we used machine translation to add two survey languages for which there were many past cases. Dark web surveys developed by NTT-CERT were also launched. Though we had been conducting surveys of domains similar to those of the NTT Group, we decided to simultaneously conduct surveys of domains similar to those of the Olympic and Paralympic Games Tokyo 2020 that were predicted to increase while the Tokyo 2020 Games were being held (including the preparatory period) and collected information on phishing sites in detected domains. These activities can be regarded as surveys that introduced new tools and applied accumulated knowledge as functional enhancements making use of research results in the automation of CSIRT functions.

No matter how much a single company's functions can be enhanced through such efforts, there is a limit to how much information a company can collect. Therefore, NTT-CERT proactively shared information in collaboration with a variety of communities that it had thus far fostered. It participated, for example, in the Japan Cybersecurity Information Sharing Platform (JISP), an information-sharing tool of the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), and the information sharing platform for the Olympic and Paralympic Games Tokyo 2020 set up by the ICT Information Sharing and Analysis Center (ICT-ISAC). These activities created a state in which NTT-CERT could access unreleased or original information. Collaboration with NTT Security's Global Threat Intelligence Center also created a state of detailed information sharing from overseas sites with respect to cyber attacks on the Tokyo 2020 Games. This information obtained through such external collaborations was distributed to NTT Group companies along with additional surveys and analysis results from NTT-CERT. These efforts

Table 1. Monitoring results: Information sources and examples of detection results.

Information source	Information source details	Examples of detection results
Public organizations	JPCERT/CC, IPA, etc.	Vulnerability information, general attack information, etc.
SNSs	Twitter, blogs, message board	Posts encouraging attacks on Tokyo 2020 Games personnel, information on discovered phishing sites, etc.
News sites	Newspaper companies, broadcast stations, information technology-related news sites	News on fake sites posing as deliverers of Tokyo 2020 Games videos, news on cyber attacks on past Olympic Games-related organizations, articles on malware pretending to be Tokyo 2020 Games-related, etc.
Dark web	Hacker forums, black-market trading sites, etc.	Information on credential selling/buying thought to be Tokyo 2020 Games-related.
Fake site information	Domain abuse, Google search results, etc.	Information on new domains that can be mistaken as Tokyo 2020 Games-related (some of which are confirmed to be phishing sites)
Other	Manually prepared reports, vendor reports, etc.	Analysis information on assumed attackers, malware, etc.

could be seen as boosting the role of NTT-CERT as a hub between external organizations and the NTT Group.

To prepare for the discovery of information on vulnerabilities that could impact the network infrastructure and operating systems, NTT-CERT strengthened its vulnerability-information collection system as well as its test system for cases in which attack code came to be released.

Preparations for the activities described above were made right up to the beginning of the Tokyo 2020 Games, and cyber exercises were finally held within the NTT Group in anticipation of attacks. In these exercises, NTT-CERT was in charge of creating attack scenarios in which information on attacks presumed to have occurred or actually detected was to be shared within the NTT Group. Each company was to check their contact system and response procedure for any problems and confirm whether appropriate measures could be taken. Thus, the NTT Group worked together in its preparations for the opening of the Olympic and Paralympic Games Tokyo 2020.

3. Results of activities for the Olympic and Paralympic Games Tokyo 2020

As a result of the functional enhancements taken for the Tokyo 2020 Games, NTT-CERT collected and analyzed information from a variety of sources and passed on information for review to each company in the NTT Group (**Table 1**). In this information for review, NTT-CERT shared detection details that if ignored could allow an attack to gain a foothold, e.g., warnings of attacks due to growing geopolitical tensions in Southeast Asia and information on the buying and selling of credential information thought to be related to the Tokyo 2020 Games, although no small-scale DDoS attacks or damage actually occurred. By repeatedly providing information in this manner, we were able to prevent major damage from being done and provide each company in the NTT Group with a feeling of security. It was reported after the Tokyo 2020 Games that Japan's National Police Agency had declared that "No Acts of Terrorism or Cyber Attacks Occurred during the Olympic and Paralympic Games" [1], which agreed with our detection results.

4. Comparison with past Olympic Games

The largest difference between the Tokyo 2020 Games and past Olympic Games is that most of the venues held events with no spectators due to the novel coronavirus (COVID-19) pandemic. It was probably for this reason that no sites selling fake tickets or cyber attacks on the venue admission system as seen in past Olympic Games were observed, and sites selling fake goods were likewise hardly seen. While DDoS attacks carried out by hacktivists as in past Olympic Games are regarded to be dangerous, there has recently been a drop in the frequency of such attacks that push a political agenda. There were also very few organizations in Japan that were greatly opposed to the Tokyo 2020 Games. We consider that this is why no DDoS attacks of this kind occurred.

In summary, the enhancing of NTT-CERT functions and nurturing of collaborations enabled the detection of information not previously available and, while small in scale, the sharing of information on a number of attacks that had the potential of gaining a foothold. The network infrastructure supporting the Tokyo 2020 Games suffered no incidents due to cyber

attacks and the closing ceremony was reached without problem. We feel that all of these results testify to the significance of our activities in protecting the Tokyo 2020 Games.

5. Future outlook

We consider that the threat analysis we conducted for the first time on cyber attacks against the Tokyo 2020 Games was effective. We feel that this threat analysis, which included related parties on the outside while considering the impact on the NTT Group and our ability to detect information and threats not previously detectable, should enable us to conduct flexible surveys on future large-scale events that the NTT Group will participate in as a provider of a network infrastructure. As an effort to strengthen NTT-CERT functions, we expanded our survey range by increasing our survey languages and dark-web surveys, analyzing the actors involved in attacks, etc. Now that the Tokyo 2020 Games are over, we should be able to collect information of even higher quality by applying these achievements to our survey range in normal situations. Once this knowledge becomes formalized, it is our intention to distribute it to NTT Group companies to help improve the security of the entire NTT Group.

NTT is an Olympic and Paralympic Games Tokyo 2020 Gold Partner (Telecommunication Services).

Reference

[1] The Sankei Shimbun news, Sept. 9, 2021 (in Japanese). https://www.sankei.com/article/20210909-KOK2GCDO3JK2LPIBAJOBHBRW6Y/

Takashi Mishina
Research Engineer, Social Innovation Research Project, NTT Social Informatics Laboratories.
He joined NTT EAST in 2011 and engaged in network design, network operation, and system construction. He is currently with NTT Social Informatics Laboratories, where he is in charge of research and development (R&D) of information-leakage detection using intelligence services.

Akiko Matsuhashi
Senior Research Engineer, Social Innovation Research Project, NTT Social Informatics Laboratories.
She joined NTT Communications in 2003 and engaged in the maintenance of web servers. In 2016, she joined NTT Security Platform Laboratories, where she was in charge of handling security incidents. She was also a member of the Tokyo Organising Committee of the Olympic and Paralympic Games from 2019 to 2021. She is currently with NTT Social Informatics Laboratories and engaged in NTT-CERT activities.

Takemi Nisase
Vice Director, Social Innovation Research Project, NTT Social Informatics Laboratories.
He joined NTT in 1987 and engaged in the R&D of an asynchronous transfer mode network service, OCN service, Next Generation Network service, etc. He joined NTT Security Platform Laboratories, where he was in charge of handling security incidents. He is currently with NTT Social Informatics Laboratories, where he is in charge of security incident response support and research on risk-analysis techniques.

Hidehiro Shito
Director, Social Innovation Research Project, NTT Social Informatics Laboratories.
He received a B.E. and M.E. in mechanical and system engineering from Yamanashi University in 1994 and 1996. He joined NTT in 1997. After several years of experience in R&D, operation, and construction of communications infrastructure, he began his career as a member of CSIRTs at NTT EAST and NTT DATA. He joined NTT laboratories in 2018, and his current position is a director of NTT-CERT, the representative CSIRT of the NTT Group.