NISC National center of Incident readiness and Strategy for Cybersecurity

A Look Back on Cybersecurity for the Tokyo 2020 Games

January 2022

Tokyo 2020 Group

National center of Incident readiness and Strategy for Cybersecurity (NISC)

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

Overview of Risk Management Promotion Activities for the Tokyo 2020 Games

●Risk assessment

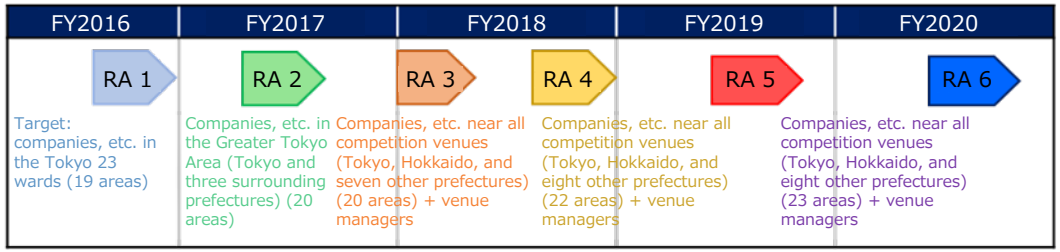
In order to prevent/reduce the impact of cyberattacks on preparations and the running of the Tokyo 2020 Games, the NISC promoted measures against possible cybersecurity risks by strengthening risk management by peripheral essential service providers (ESPs) that supported the Games. In Risk Assessment ("RA") 6, the NISC not only reconsidered risks of postponement or environmental changes due to the spread of coronavirus infection but also comprehensively examined measures against risks requiring actions and strengthened the system to handle residual risks that may arise.

○ To promote risk management, the NISC created a cybersecurity risk identification, analysis, and evaluation procedure.

○ From the important service areas that could influence preparations and the running of the Games, important ESPs were chosen through consultation with relevant management parties.

Important service areas + venues (competition and non-competition venues)

(Communications, broadcasting, finance, airlines, railways, electricity, gas, water system, logistics, credit, administrative service (local public agencies), sewage system, airports, road, maritime, and traffic control, emergency reporting, weather and disaster information, border control, highways, heat supply, buses, security, travel, hospitals, and venues)



○ The NISC created based on its assumption "model cases for business, important services, and management resources (information assets) (for each important service area)" and "events (threats) and sources of risks that may lead to negative consequences in the case of an event that disrupts business operation." It provided feedback to ESPs on the possibility of undetected management resources and risk sources to promote more comprehensive RA.

○ The NISC provided feedback to ESPs on their cybersecurity measure management status and offered advice as necessary.

●Cross-sectional risk assessment

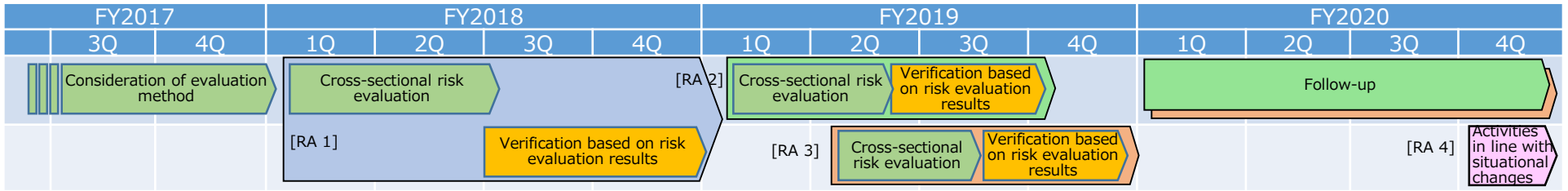
Based on the cybersecurity risks predicted for the important ESPs, the NISC checked their cybersecurity measure implementation status. Doing so confirmed uninterrupted supply of functions essential for the success of the Games. In the case of insufficient implementation, the NISC sent feedback to the subject important ESP to increase the certainty that said important functions would be provided continuously.

○ A scenario in which Games-related risks arise was created and used as a risk scenario to examine the validity and effectiveness of the rules set by the important ESPs.

○ In RA 1, an onsite inspection of about five ESPs was carried out in the areas of electricity, communications, water, railways, broadcasting, and so on. From all important service areas, document inspection was carried out for about 20 ESPs.

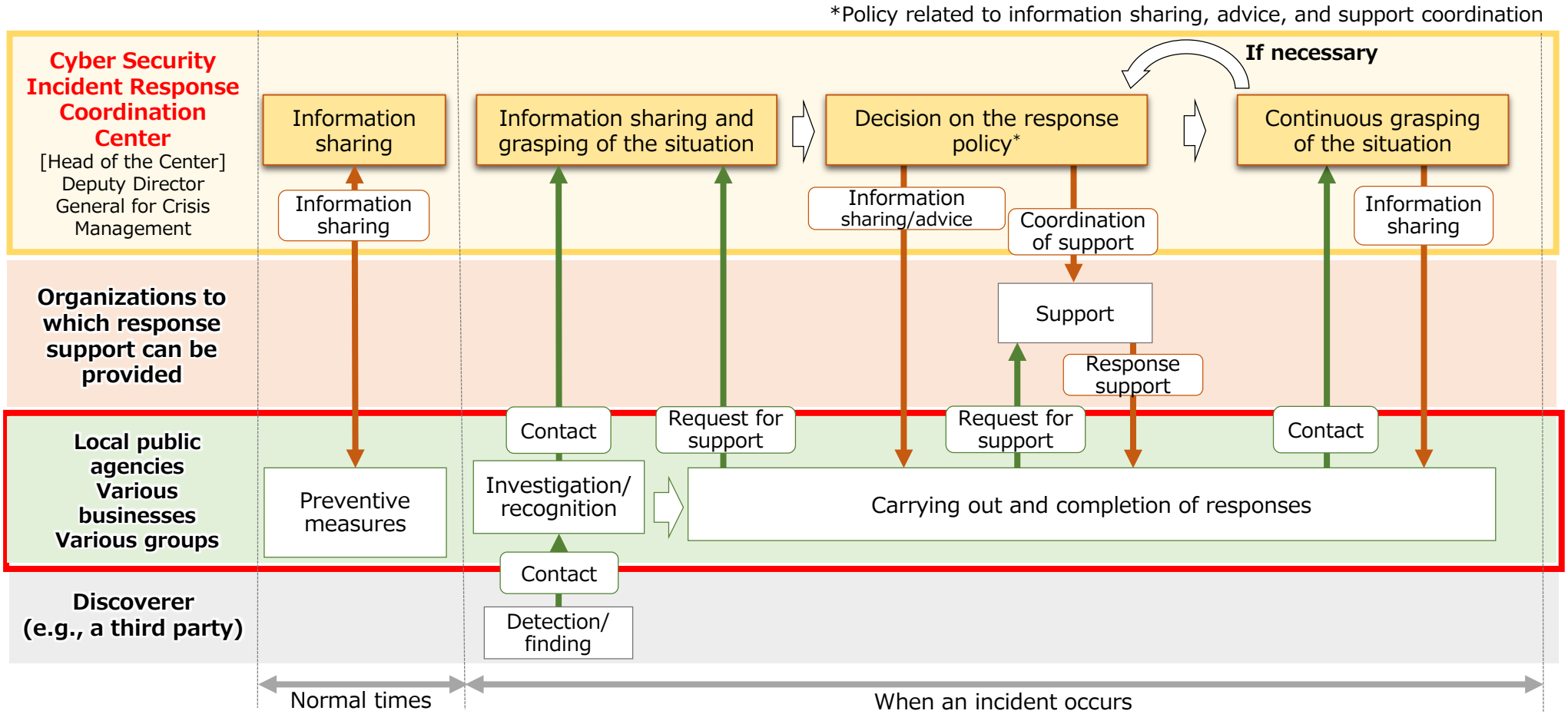
○ In RA 2 and 3, an (onsite/document) inspection was carried out for the important ESPs (including venue (including legacy sites)).
Note that, for the state of improvement and supervision of the measures for overlays at venues, the Tokyo Organising Committee of the Olympic and Paralympic Games (TOCOG) was subject to an onsite inspection.

○ In FY2020, RA 4 was carried out in line with situational changes due to the spread of coronavirus infections.



Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

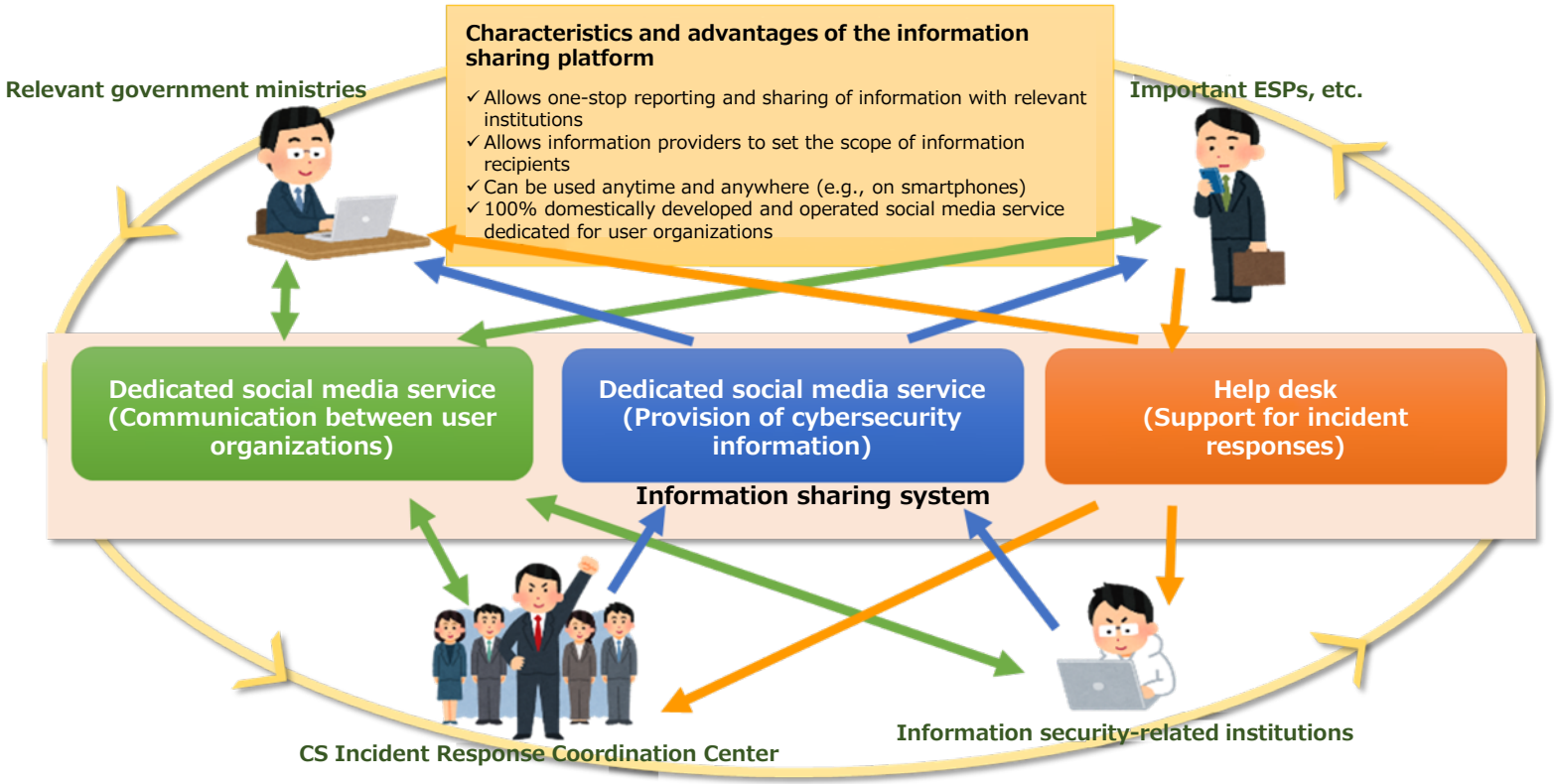
➢It collects threat and incident information related to cybersecurity of the Tokyo 2020 Olympic and Paralympic Games, provides such information to relevant institutions including the TOCOG, and if necessary, **coordinates support** for incident responses by a relevant agency. (The Cyber Security Incident Response Coordination Center will be closed down on March 31, 2022, but the activities the Center promotes will continue.)



Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

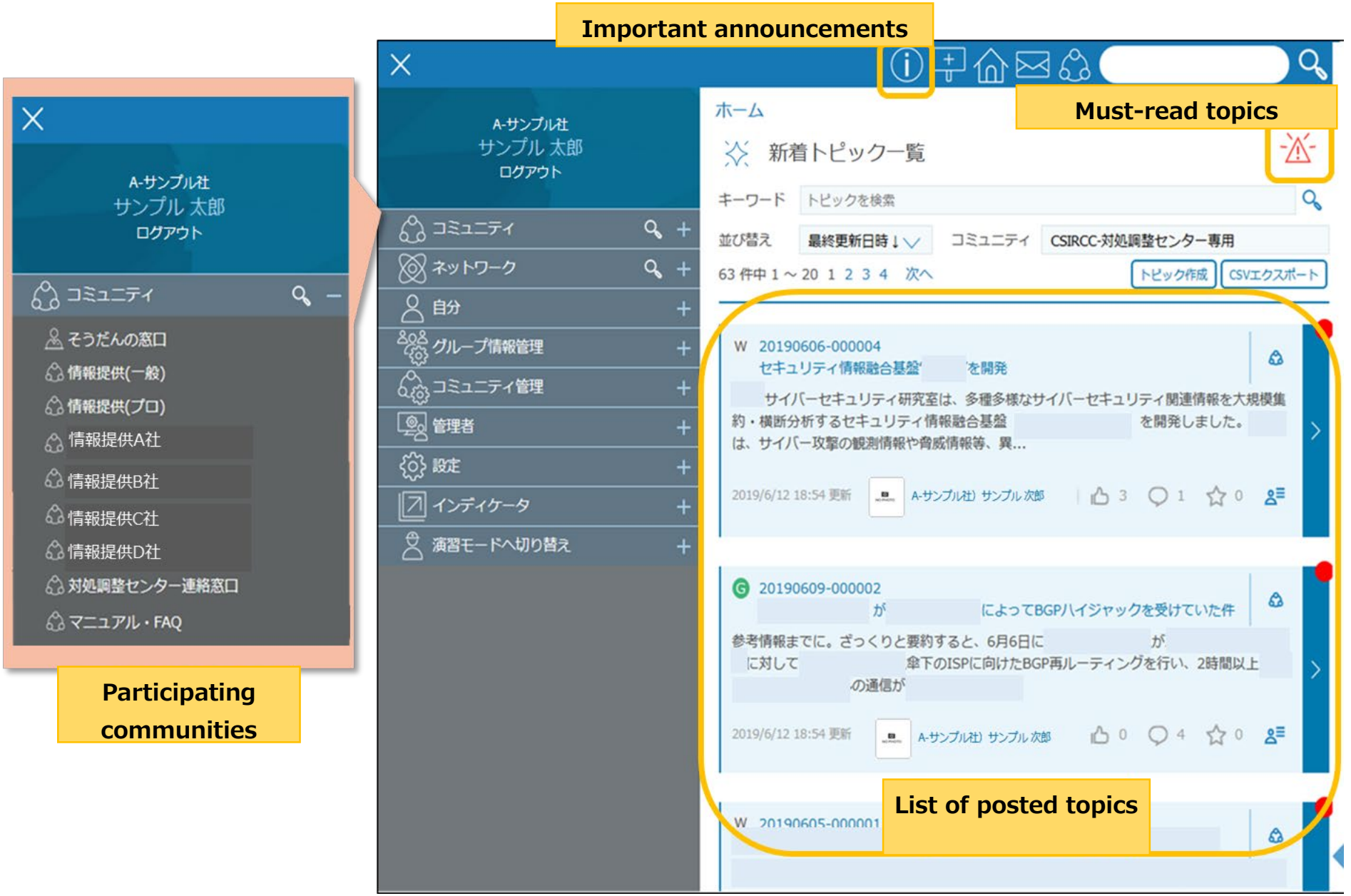
Overview of the Japan cybersecurity Information Sharing Platform (JISP)

- It is an information sharing platform to share threat information between relevant organizations, provide advice to an organization affected by an incident, and coordinate incident responses.
- The service began in April 2019.
- Users can access the platform via a PC or smartphone, and there are about 350 member organizations (as of the end of August 2021).



*JISP member organizations
The TOCOG, venue managers, the Tokyo Metropolitan Government, local public agencies of areas where venues are located, important ESPs, sports associations, information security-related institutions, government agencies, police, and so on

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity



Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

Promotion of risk management

○ **Number of organizations that carried out self-RA**

RA 1: 75 (Oct.–Dec. 2016) → RA 2: 115 (Aug.–Oct. 2017) → RA 3: 191 (Jun.–Aug. 2018) → RA 4: 273 (Feb.–Apr. 2019) → RA 5: 279 (Sept.–Dec. 2019) → RA 6: 270 (Nov. 2020–Jan. 2021)

○ **Explanatory meetings**

In 10 prefectures, 53 meetings were held, and a total of about 2,000 individuals participated.

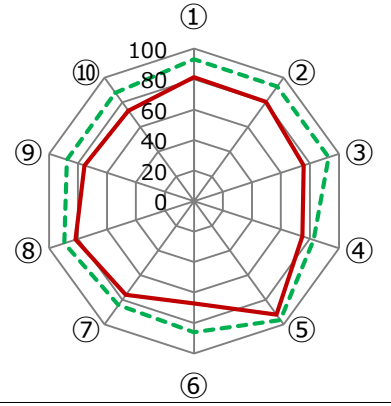
○ **State of cybersecurity measure implementation**

- It was confirmed that more RA led to better risk management measure implementation status (see the figure on the right).
- The organizations that participated in RA from RA 1 seemed to have carried out their own exercises and training after each round of assessment to prepare for the Games and considered corrective measures.

○ **Study sessions for sports associations**

The NISC held 17 study sessions and a total of about 500 individuals attended.

State of cybersecurity measure implementation (RA 6)



Plan	①	Formulation of the basic policy
	②	Creation of internal documents
	③	Creation of a plan for measures
	④	Holding of training
	⑤	Strengthening of internal control
Do	⑥	Creation of a contingency plan
	⑦	Creation of a business continuity plan
	⑧	Holding of exercises and training
Check	⑨	Auditing
Act	⑩	Examination of measures that need correction

Overall

Organizations that participated in RA from RA 1

Preparation of an incident response system (e.g., creation of the Cyber Security Incident Response Coordination Center)

○ **The number of participants in the information sharing scheme**

Member organizations: 353
(Breakdown: 153 important ESPs, 40 sponsors, 67 sports associations, 30 relevant ministries, and 63 other organizations)
The number of participating individuals: 3,944

○ **The number of participants in drills to prepare for the Games (four times by May 2021*)**

Total number of organizations that participated: 512 (Breakdown: 140 in the 1st drill, 149 in the 2nd drill, 108 in the 3rd drill, and 115 in the 4th drill) *The 5th drill was carried out in June.

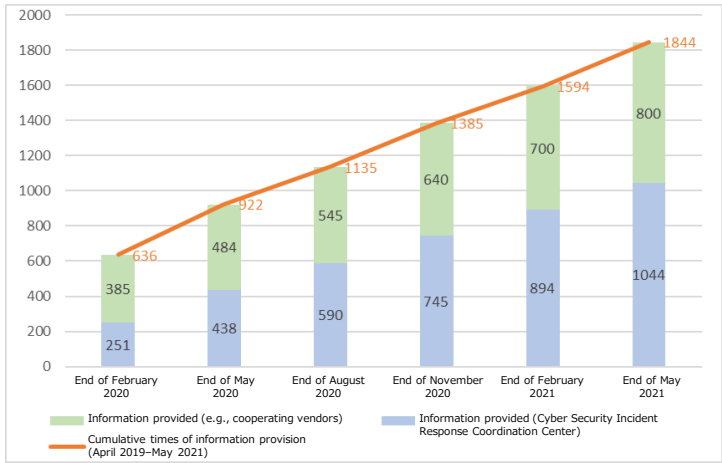
○ **Threat information reports**

The cumulative number of reports: 1,844 (Breakdown: 1,044 from the Cyber Security Incident Response Coordination Center and 800 from cooperating vendors (see the figure on the right)

○ **Use of the JISP** (as of the end of May 2021)

The cumulative number of logins: 175,000; views: 443,000; posts: 7,000; and comments: 29,000
(Monthly average logins: 6,722; views: 17,020; posts: 277; comments: 1,106)

Threat information reports



Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

Damage status due to cyberattacks on the Tokyo 2020 Games

No cyberattacks that would influence management of the Games were confirmed.

Main topics during the Games (no influence on management of the Games)

○ **TOCOG observed suspicious communication**

TOCOG, Tokyo Organizing Committee of the Olympic and Paralympic Games, observed suspicious communication to PC that connected the internet environment used by stakeholders and official websites.
During the Game competition period, TOCOG blocked communication in 450 million security events.

○ **Social media posts about cyberattacks**

There were no social media posts calling for cyberattacks against Games-related organizations.

○ **Service outage at an American content streaming service provider**

An American content streaming service provider had a system failure resulting in a service outage. Websites of Games-related organizations, including the official Games site, became unavailable temporarily (for about an hour on July 23).
The subject company announced that this incident was not due to a cyberattack.

○ **Fraudulent video streaming website**

There were multiple fraudulent websites disguised as streaming services for the opening ceremony as well as various competitions.

Fraudulent account registration screen that appeared after connecting to the site

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

There were no incidents during the Games that would influence its management.

[Activity outline]

- The NISC, well before the Games, collected information on events at organizations in the information sharing scheme that would or may influence the management of the Games. It then reported to the Security Coordination Center the events, among those collected, that would influence the Games or that would require responses to third parties.
- The NISC sent out information to relevant institutions (e.g., organizations that are considering joining the information sharing scheme, ESPs who are in the information sharing scheme) about the Games and activities of the Cyber Security Incident Response Coordination Center.

[Number of responses]

There were a total of 19 reports from organizations in the information sharing scheme. Among them, 7 were reported to the Security Coordination Center.

[Main activities]

◆ Information provided from organizations in the information sharing scheme

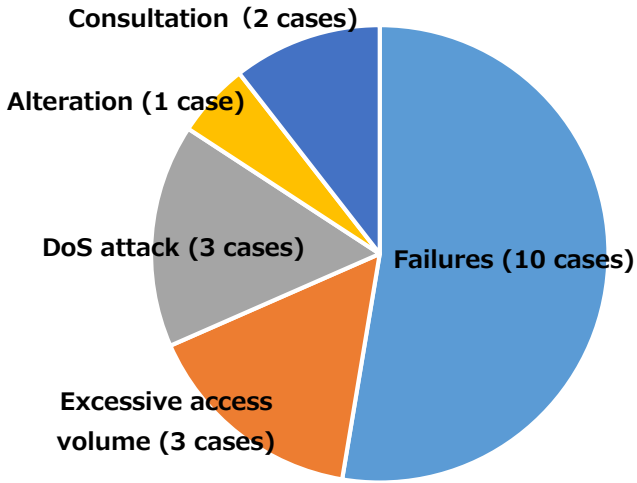
- A total of 19 reports were made. Of which, 17 were received by the JISP, and 2 were received through collaboration within the NISC.
- **Among the total of 19 reports, 17 were incident reports and 2 were consultations about security measures.**
- Among the 17 incident reports, system failure accounted for the most. **There were 7 cloud service failures and 3 system failures (10 in total).**
- **The official online store had a loading problem for a few days after the opening ceremony and also on the day of the closing ceremony due to too many access attempts.**
- As for cyberattacks, **there were 3 reports of a DoS attack and 1 report of website alteration (4 in total).**

◆ Security Coordination Center report (AM/PM)

- Among the events reported by the organizations in the information sharing scheme, **events that would influence the Games (including events in Games-related websites) and events that may be recognized by the public (including events reported by the media) were reported.** There were no reports of events that would influence the Games.
- There were **7 events in total** that were reported: **4 website loading problems and 3 system failures.**

◆ Information sharing with relevant institutions

- The NISC shared an overview of the Security Coordination Center reports with the contact person of the Information Sharing Scheme Committee (AM/PM).
- The NISC sent out information to ESPs in the information sharing scheme about the Games and activities of the Cyber Security Incident Response Coordination Center (once a day).



Categories of incident reports and consultations
(Jul. 21–Sept. 5)

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

Observation and Threat Information Provided during the Tokyo 2020 Games

[Activity outline]
- With the cooperation of information security-related institutions, the NISC observed systems running for the Tokyo 2020 Games, and when abnormal observation results or attack predictions were detected, the Cyber Security Incident Response Coordination Center sent information to each applicable organization.
- The NISC conducted a dark web study to detect phishing sites and information on attack campaigns by attacker groups.
- The NISC sent Games-related cybersecurity threat information collected by the Cyber Security Incident Response Coordination Center to the organizations in the information sharing scheme.
- With the possibility of adverse impacts on the Games in mind, the NISC identified and investigated major attacker groups, analyzed attack methods, and warned relevant parties.

[Number of cases]
During the subject period, 75 cases of observation information and 32 cases of threat information were sent to the organizations in the information sharing scheme.

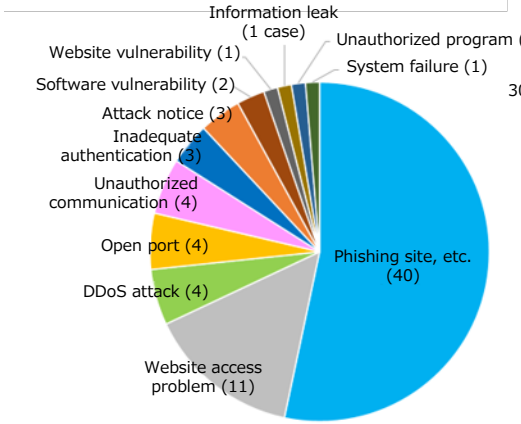
[Main activities]

◆ Observation information provided by the Cyber Security Incident Response Coordination Center

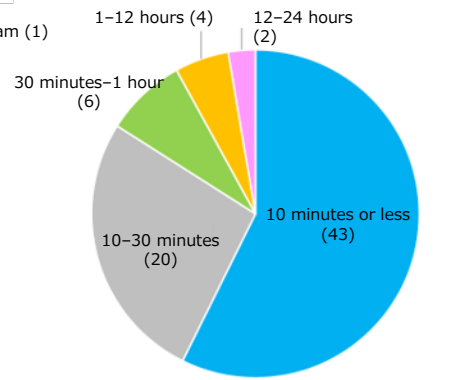
- Information on 75 events that would or may influence important ESPs was provided to each subject organization.
  - Many **fake opening ceremony, closing ceremony, and competition live streaming sites** (e.g., phishing sites) were observed in the dark web study, and the study result was reported to the TOCOG.
  - On the first day (July 21) and the next day of the competition, **attack notices and DDoS attacks targeting three organizations** were observed. Later, **DDoS attacks** were also observed **on the opening and closing ceremony days among others.** None had any impact on the Games management.
  - In addition to the above, issues such as **inadequate authentication, open RDP ports, and open information on devices with Microsoft Exchange server vulnerabilities** were observed, and relevant organizations were notified of the issues and were requested to address them.

◆ Threat information provided by the Cyber Security Incident Response Coordination Center

- A total of 32 cases of threat information were reported.
- Warnings were issued to all organizations in the information sharing scheme about **the confirmed existence of an unauthorized program faking a Games-related damage report** and **a Tokyo 2020 Games scam program** as well as **DDoS attack campaigns**.



Categories of events for which observation reports were issued (Jul. 21–Sept. 5)



Time between issuance of observation reports and viewing of them (Jul. 21–Sept. 5)

Threat information frequently viewed (July 21-Sept 5)

Ranking	Provided threat information *Brief description of reports for the top 3 places	Issuance date
1	Confirmed existence of an unauthorized program faking a Games-related damage report	July 21
2	DDoS attack campaign (#OpBoycottOlympics)	July 23
3	Tokyo 2020 Games scam program	July 30
4	Zero-day vulnerability in iOS and iPad OS (Apple)	July 24
5	Zero-day vulnerability in Windows OS that allows privilege escalation	July 21

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

[Activity outline]
The JISP was launched on April 2019 as a one-stop information sharing platform for relevant organizations. Information related to and unique to the Games was shared during the event period. Logins increased by 1.5 times from normal times, and topic views, 2.5 times. The platform was most actively used from the first day of competition (July 21) to the opening ceremony (July 23) of the Olympic Games.

[Number of cases] (as of the time of the Paralympic Games closing ceremony (September 5))
・Approximately 1,800 users from 330 organizations used the system.
・Cumulative logins: about 198,000 times; cumulative topic views: about 559,000 times; topic posting: 8,000 times

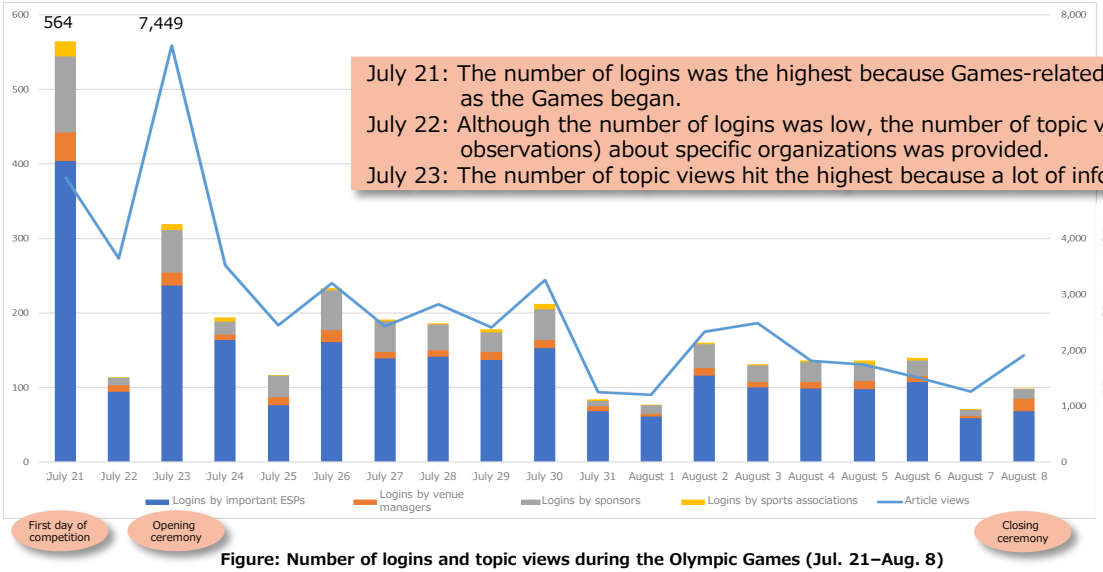


Figure: Number of logins and topic views during the Olympic Games (Jul. 21–Aug. 8)

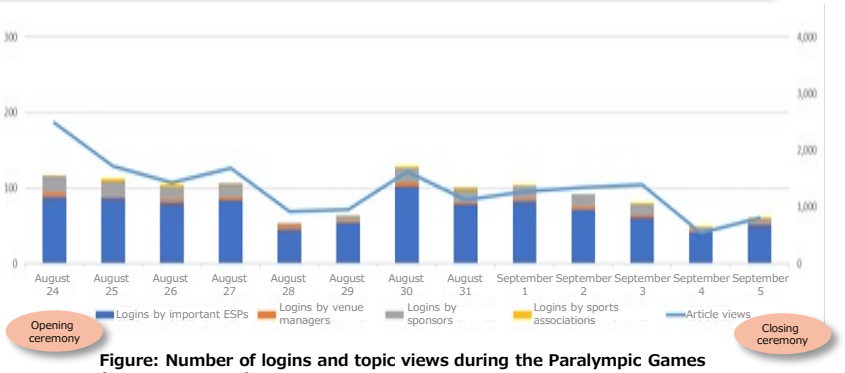


Figure: Number of logins and topic views during the Paralympic Games (Aug. 24–Sept. 5)

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity