NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

Cybersecurity Measures for Tokyo 2020 Olympic/Paralympic Games

April 25, 2019

Yoichi KUMOTA, Counsellor

National center of Incident Readiness and Strategy for Cybersecurity(NISC),

Cabinet Secretariat, Government of Japan

Upcoming Major Events

- **Rugby World Cup 2019**
  September 20 to November 2, 2019

- **Games of the XXXII Olympiad**
  July 24 to August 9, 2020

- **XVI Paralympic Games**
  August 25 to September 5, 2020

Tokyo was selected to the host city of the XXXII Olympiad at the 125th IOC Session in Buenos Aires on September 7, 2013

Cybersecurity Situations in Rio2016 Olympic/Paralympic Games

In spite of a lot of cyber-attacks against related sites, there were NO incidents affecting Games operation.

NISC's activities during Games time

NISC sent two liaisons to Technical Operation Center(TOC) of Rio 2016 Organizing Committee of Olympic/Paralympic Games(ROCOG) HQ. They watched the actual situations with shadowing TOC's information security managers, and provided threat intelligence found by NISC and cybersecurity community of Japan.

Situations in Rio2016

✓ A lot of cyber attacks, such as DDoS and web scan, against official and related websites were identified. Information of some websites was bleached.
- Targets moved from Games relates websites to surrounding websites such as federal/local government's ones.
- Most of identified attacks were noticed and announced in SNS and other media.
- Just after the opening ceremony, the peak of attacks came, but it didn't affect operations because of good preparation.

<Transition of targets during Games time>

- ✓ Rio2016 Official websites
- ✓ BOC/BPC websites
- ✓ Rio2016 portal website of Federal Government
- ✓ The website of Federal Ministry of Sports
- ✓ Websites of Rio State/City government
- ✓ Websites of constructor of Games' venue

<TOC, Rio2016 HQ>

Lessons learned from Rio2016 and Brazilian government will be reflected in the cybersecurity preparations of Tokyo2020

Situations in Rio Olympic/Paralympic Games

While cyber attacks against several sites related to the games were detected, the incident influencing the game operation was not happened.

○Attacks in cyber space expected before Rio Games

- ✓ Various hacker groups such as “OpOlympicHacking”
- ✓ Warning about physical terrorism in cyber space
- ✓ Cyber attacks by using botnet (large number of malware infection)

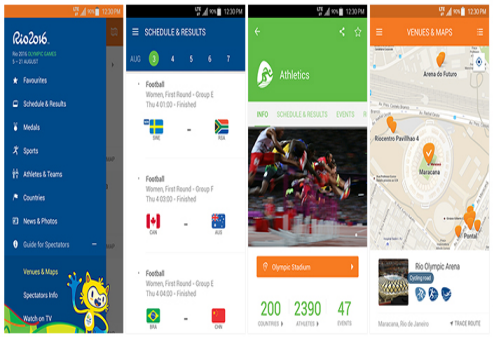
○Situation during Rio Games

- ✓ Access congestion by unexpected number of users in official application
- ✓ Active activities in Brazilian hacker groups, also supported by foreign groups
- ✓ Connecting to Wifi systems the malware infected PCs brought by players and press

○Major incidents during Rio Games

- ✓Attacks/vulnerability searches against the official Rio Games sites
- ✓Attacks/Information leakage in government sites including Brazilian Federal Government and Rio State Government
- ✓Attacks against the sites in the Rio Game related organizations
- ✓Information leakage in OBS(Olympic Broadcasting Services) site
- ✓Phishing sites fraudly imitating the official Rio Games sites

Activities by hacker groups



Rio2016 official application

Major incidents during Rio Games

Incident 1: Web site attacks

Warning of attacks against various sports association sites, Browsing problems caused by DDoS attacks, Leakage of database information in parts of the sites

Countdown site for the expected attacks

DDoS attack tools publicized by hacker groups

International Olympic Committee
International Paralympic Committee
Brazilian Paralympic Committee
Ministry of Sports in Brazil
World Anti-Doping Agency
Court of Arbitration for Sports

International Association of Athletics Federation
International Weightlifting Federation
International Federation of Association Football
Brazilian Handball Association
Brazilian Modern Pentathlon
Brazilian Boxing Association

Official site for Michael Phillips

Examples of sports related sites that suffered damage or received warnings of attacks

Incident 2: Information leakage

13/8/2016
WADA (World Anti-Doping Agency) announced that accounts of whistle-blowers about Russian organizational doping was hacked and the hackers unlawfully used their accounts with their passwords.
13/9/2016
Some players' medical information leaked from WADA was publicized in internet. At a later date, WADA conceded the leakage of the information. The information about Japanese player was also publicized.

Web site publicized by the hacker group

NISC's activities

1． Outline

Cyber threat information, detected and collected by Japanese relevant cyber organizations, was provided to Kr POC.

Information gathering on Korea's cyber security measures and the actual situation of cyber attacks.

2． Period

・Sharing information

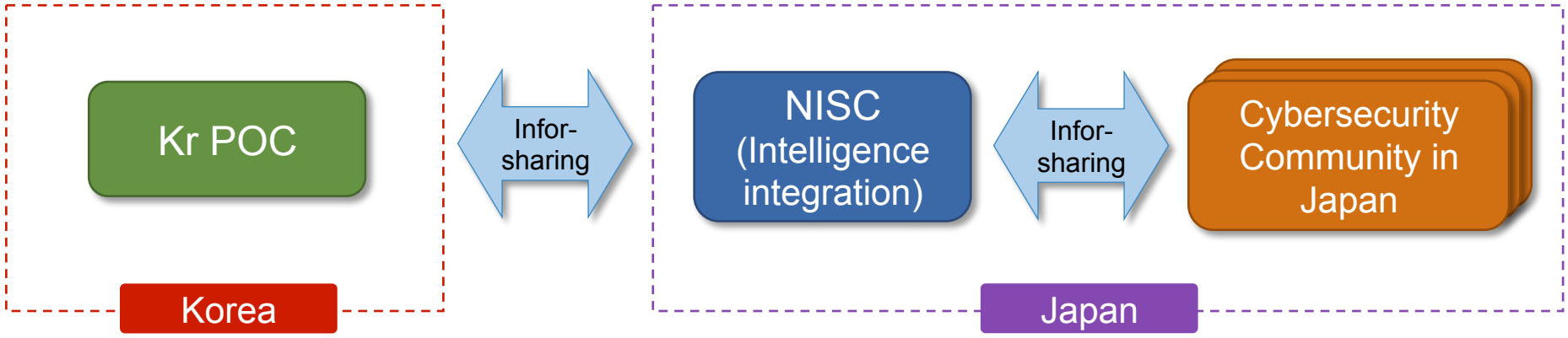
Feb 5 – Feb 25 (Olympic Games Period)

March 9 – March 18 (Paralympic Games Period)

・Meeting

Feb 19 – Feb 23 (Olympic Games Period)

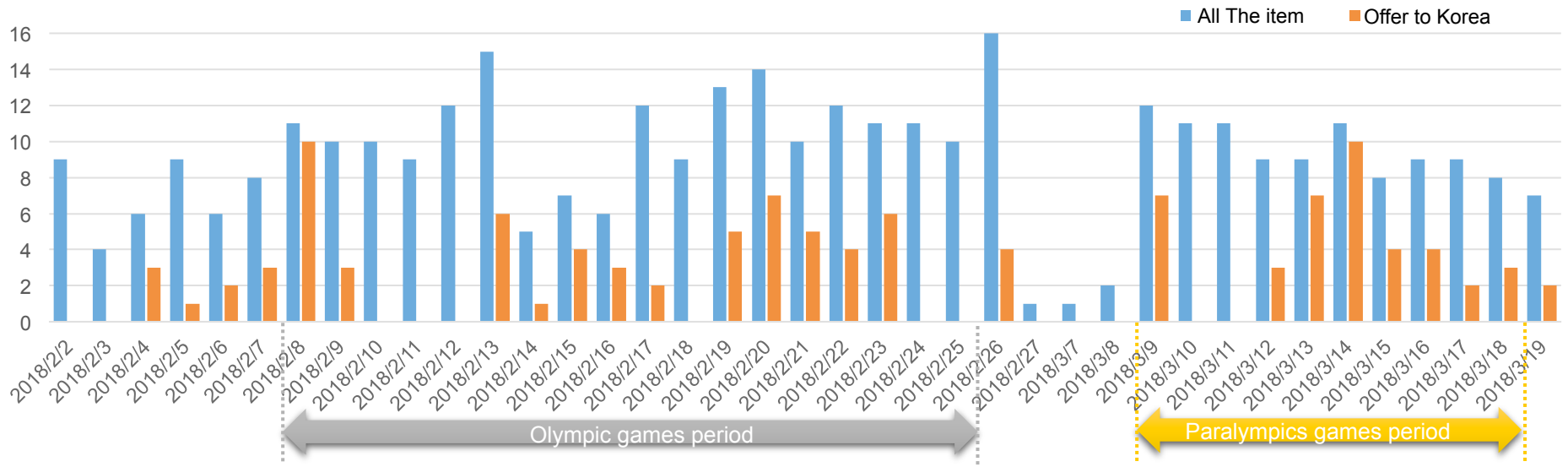
March 25 – Match 28 (After Games)



About the NISC's activities in PyeongChang 2018 Olympic/Paralympic Games

Statistics of the sharing information

The item	Number
(1) Live/Death monitoring for the sites related to PyeongChang 2018	**138**
(2) Open Source Intelligence (SNS BBS etc.)	**200**
Cyber security related	69
Other information	131
(3) Information on DRDoS attacks	**8**
PyeongChang 2018 Official sites	2
Official Sponsor sites.	6
(4) Others	**9**
Total	**355**



The cyber threat information recognized in Japan was gathered and sent to Korea POC in every weekday at noon. However, suitable dissemination of information also planned to be performed in case of emergency.

Structure for Governmental Security Policy Decision Making

The HQ for the Tokyo 2020 Olympic/Paralympic Games
Chair - Prime Minister
Member - all ministers

Vice Ministers Meeting
Chair - Deputy Chief Cabinet Secretary
Member - all vice-ministers

Security Board Meeting

Chair – Deputy Chief Cabinet Secretary for Crisis
Co-chair – Secretary General of HQ for TOKYO2020, Assistant Chief Cabinet Secretary(interior), Assistant Chief Cabinet Secretary(Crisis), Deputy Commissioner General of National Police Agency
Member – Director Generals of relevant ministries/agencies
Observer – Tokyo Metropolitan Government, Tokyo Metropolitan Police Department, Tokyo Metropolitan Fire Department, Tokyo 2020 Organizing Committee
Secretariat – Cabinet Secretariat(including NISC)

Counter-terrorism measure WT

Chair – Councillor, Cabinet Secretariat(Crisis, Interior)
Councillor, Cabinet Secretariat(Tokyo2020)
Co-chair – Councillor, Cabinet Secretariat(Interior),
Councillor, Cabinet Office(Dissaster Prevention)
Councillor, NPA(Security)
Member – Directors of relevant ministries/Agencies
Secretariat – Cabinet Secretariat(Crisis, Interior)

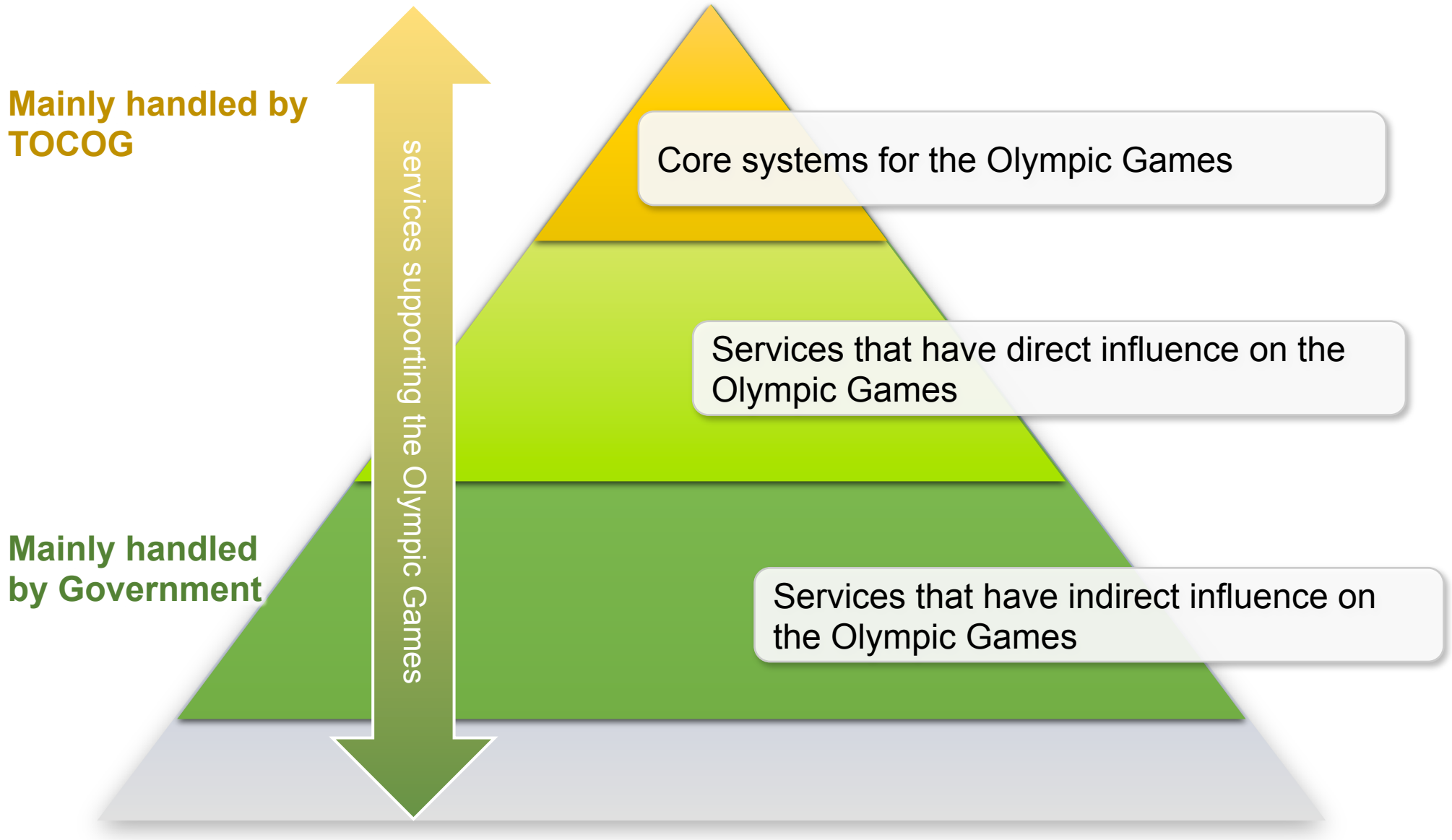
Cybersecurity WT

Chair – Councillor, Cabinet Secretariat(NISC)
Co-Chair – Councillor, Cabinet Secretariat(Tokyo2020)
Councillor, NPA(Security)
Member – Directors of relevant ministries/agencies
Observer – Tokyo 2020 Organizing Committee
Secretariat - NISC

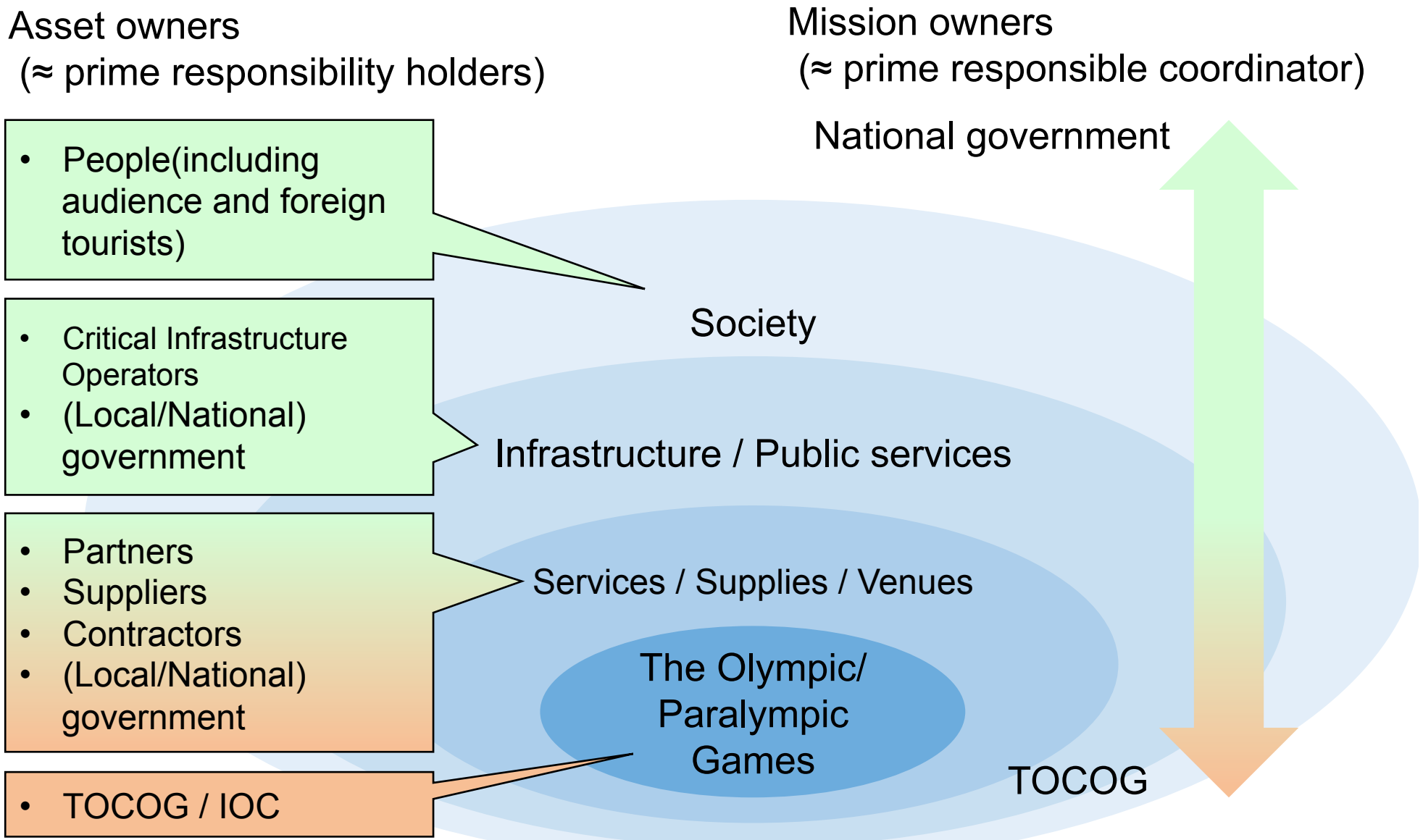
Discussion Group for IR Structure

Member – Directors of relevant ministries/agencies and Tokyo 2020 Organizing Committee
Secretariat - NISC

Image of essential services supporting the Olympic Games



Overview of Tokyo 2020 and its circumstances

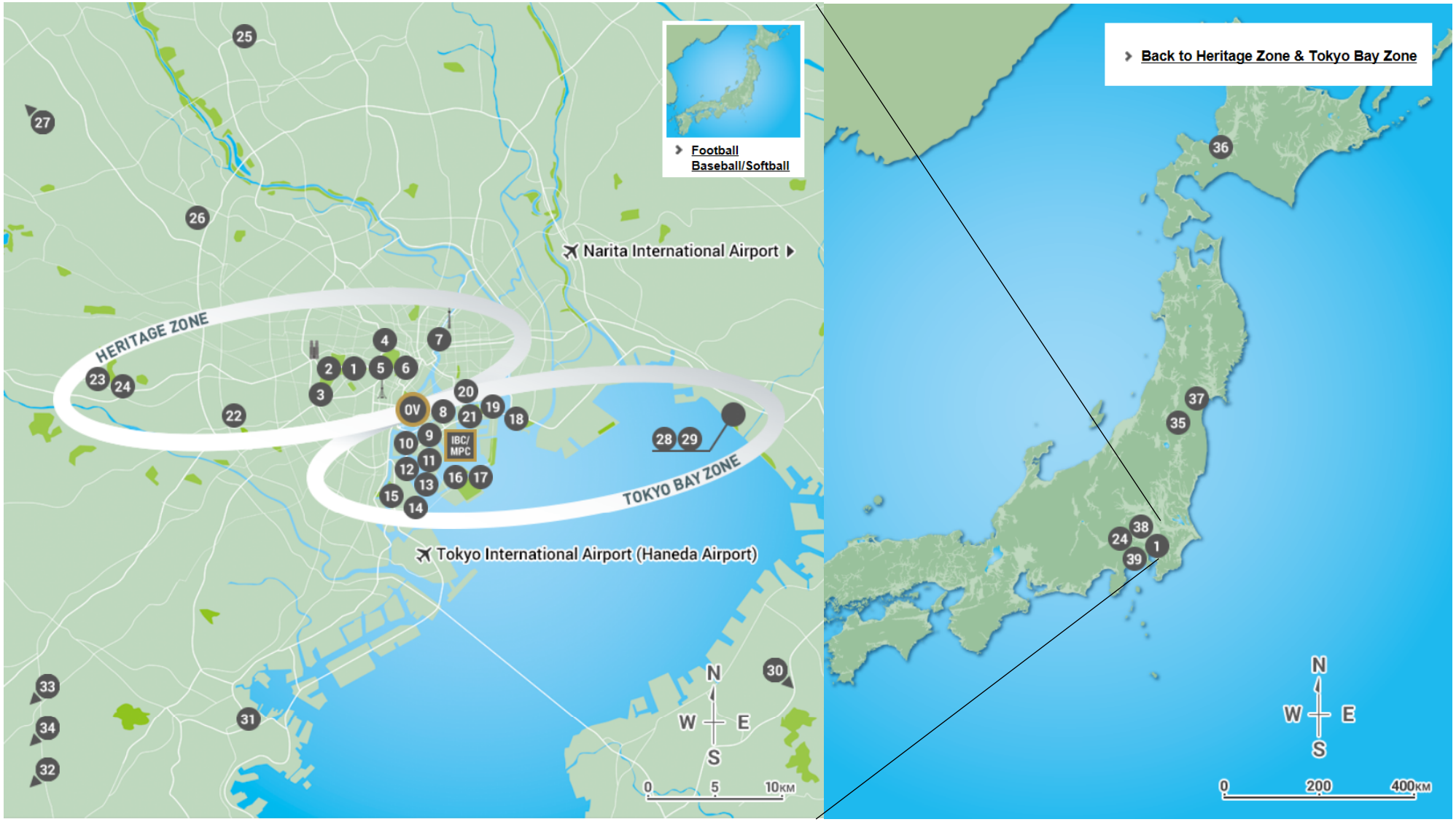


Critical Infrastructures vs. Essential Services

Critical Infrastructures (14) (identified in 4th Basic Policy for CIIP)	**Essential Services (22)** (for operation of Olympic/ Paralympic Games)
Information & Communication	Telecommunication
	Broadcasting
Financial	Financial
Aviation	Aviation
Railroad	Railway
Electric power supply	Electric power
Gas supply	Gas
Gov't & Admin services (incl. municipal gov'ts)	Local Government
Medical	
Water	Water System
Logistics	Logistics
Chemical Industries	
Credit Card	Credit Card
Petroleum industries	
	Sewerage
Airport	Airport
	Traffic Control (Air, Vessel, Road)
	Emergency Call (Police, Ambulance, Fire defense)
	Weather forecast
	CIQ
	Expressway (esp. Shuto expwy)
	Heat supply
	Bus
	Security
	Tourism

About 200 service providers(private companies, public companies, local governments, nat'l government)

Tokyo 2020 Olympic/Paralympic Games



From Olympic Committee

Cybersecurity Measures for Tokyo 2020 Olympic and Paralympic Games

Government of Japan promotes cybersecurity measures of Essential Service Providers (ESPs) for the Games based on risk assessment and discusses to establish Cyber Security Incident Response Coordination Center as a core organization of information sharing among stake holders.

Summary of measures

Promotion of cybersecurity measures based on risk assessment(RA) (for appropriate preparation)

- ○ Establishment of guidance for self-RA to secure safe and continuous provision of services.
- ○ Listing-up of Essential Service Providers (ESPs) that can affect Games operation.
- ○ Request for ESPs to conduct self-RA to promote their cybersecurity measures.
- ○ ESPs conducted their self-RA during Oct.-Dec. 2016. About 70 ESPs reported their result.
- ○ NISC requested the 2nd self-RA during Jul.-Oct. 2017, and about 130 ESPs reported their results. NISC started cross-sectional-RA for some particularly important ESPs.
- ○ NISC requested the 3rd self-RA during Jun.-Aug. 2018, and about 200 ESPs reported their results. NISC gave the feedback report to each ESP.

Establishment of incident response(IR) structure (for quick and precise responses against incidents)

- ○ “Discussion Group for Cybersecurity Structure of Tokyo 2020” discusses the details of information sharing and agrees the fundamental policy.
- ○ Sent liaisons for G7 Ise-Shima Summit and Rio2016 Olympic/Paralympic Games as large-scale test events and conducted trial operation of the information sharing structure.
- ○ Continuous discussion of creating Japan cyber security Information Sharing Platform (JISP) for more streamlined information sharing among stakeholders

Risk assessment for Tokyo 2020 Olympic/Paralympic Games

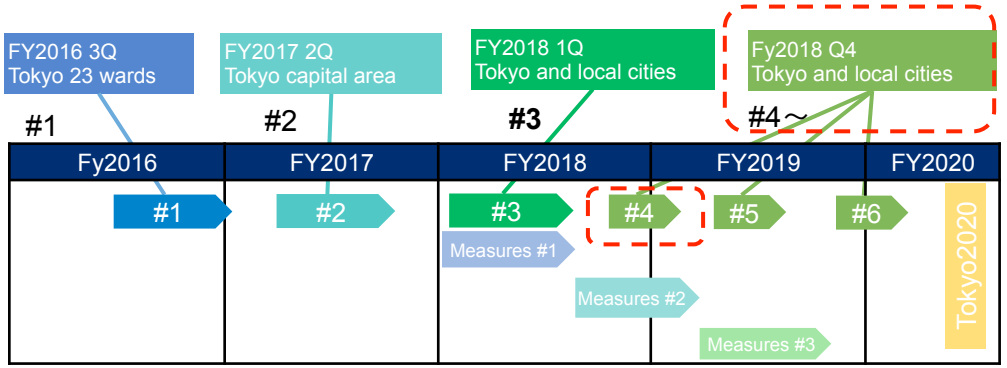
●Risk Assessment

- Based on the London 2012 Game's practices, NISC promotes risk assessment for safe and continuous provision of essential services for Tokyo 2020 Olympic/Paralympic Games.
- NISC requested service providers, which can affect the Game's operation, to perform their self assessment.

Risk Assessment #3

- Expand Essential Service Providers(ESPs) +Venues
  - Expand area (Tokyo+Capital area+Local cities)
- Analyze every report and feedback to each ESP
- Follow up the status of ESP's risk measures

ESPs:20 areas + Venue (Telecommunication, Broadcasting, Financial, Water System, Aviation, Railway, electric power, Gas, Local Government, Credit, Bus card, Logistics, Sewerage, Airport, Traffic control, Emergency call, Weather forecast, Custom/ Immigration/Quarantine, Expressway, Heat supply)



Risk assessment schedule for Tokyo2020

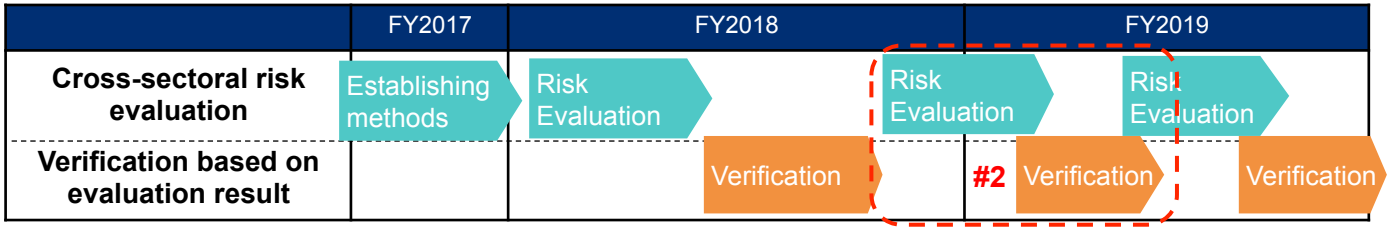
●Cross-sectoral risk assessment

- NISC identifies the services in a cross-sectoral manner, which would have big impacts on Games in the suspension. NISC verifies the operators' service level to be satisfied, as a result of their risk assessment.
- The validity of the result of the assessment by operators is checked, and verified results will be used for excises for Games.

Cross-sectoral risk assessment #1

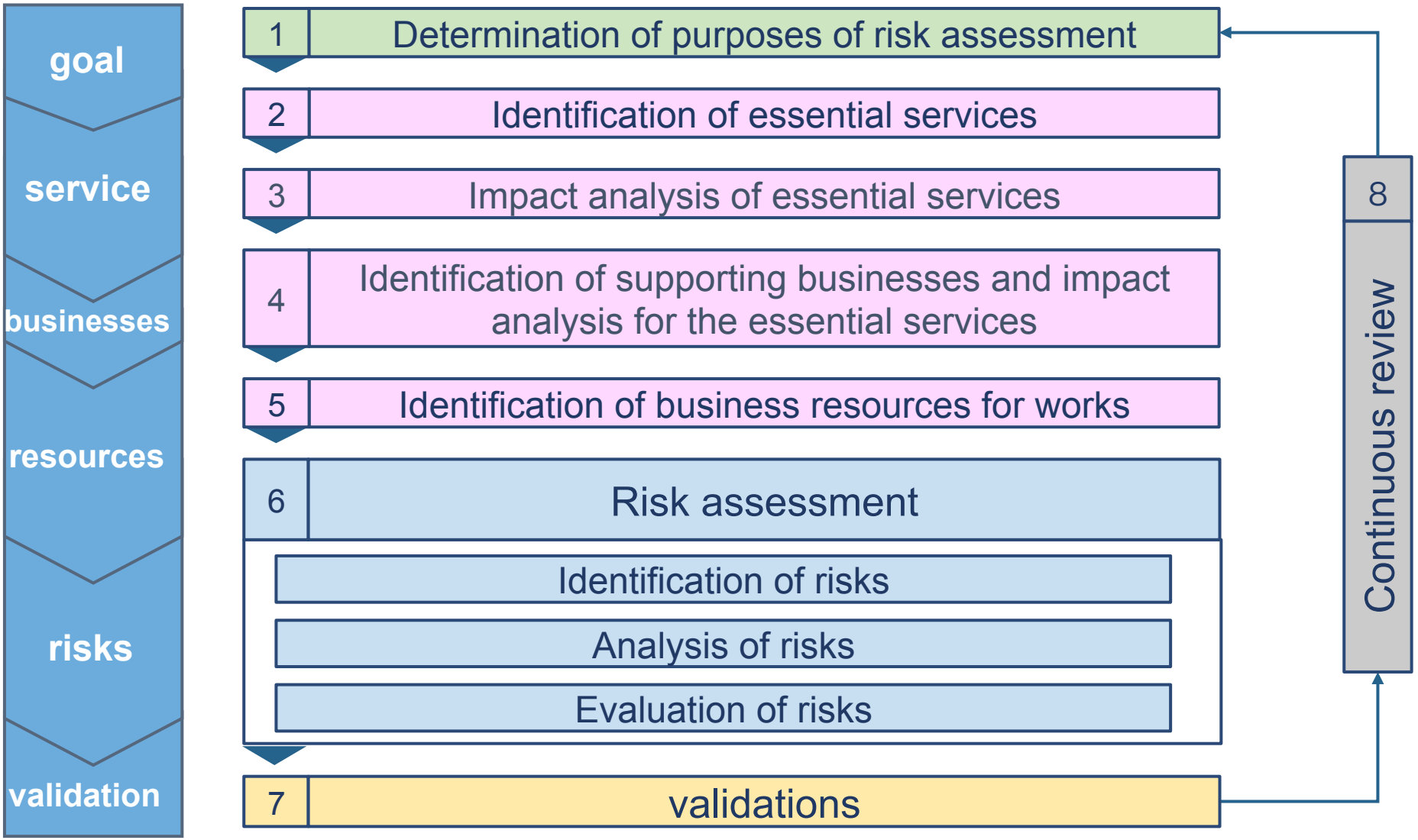
- Develop risk scenarios when risks materializes and check validity/effectiveness of rules prescribed by ESPs
- Identify dependencies between ESPs and verify the service level
- Verify integrity of service level by utilizing risk scenario which tests dependency between services

On-site verification: 5 providers
(Telecommunication, Broadcasting, Railway, Electric energy supply, Water)
Verification in writing forms: 20 providers



Cross-sectoral risk assessment schedule

Overview of Risk Assessment Guidance



Information Exchange Meetings for Essential Service Providers (ESPs)

Overview of Information Exchange Meetings (IEMs)

ESPs including newly participating ones could get information necessary for effective/ efficient risk assessment, and communicate with the persons in charge in the same industries at the meetings.

Date　2nd Risk Assessment: Sep. 19, 2017 (Tokyo)
3rd Risk Assessment: Jul. 25, 27, 31, Aug. 2, 7 (Tokyo & 4 other prefectures)

Examples of the agenda：

- **Explanation about Transportation Operation Plan (2nd Risk Assessment)**
  (by Tokyo Organizing Committee of the Olympic and Paralympic Games)
- **Workshop for Risk Assessment**　(by NISC)

Participants: 2nd RA IEMs：38 organizations(61 persons), 3rd RA IEMs: 46 organizations (52 persons)

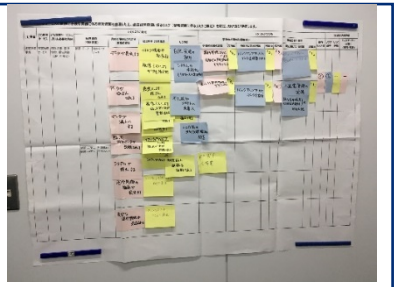
Overview of the Workshop for Risk Assessment

Purpose：Through discussion with the ESPs in the workshop,
① Deepening the risk assessment procedure
② Establishing/fostering the human network in the same industries

Method: Group work for identifying, analyzing and evaluating risks in virtual railroad company (2nd RA) and virtual stadium (3rd RA)

Contents：

- Overview explanation
- Group work
  - ・Identify risks ①(Considering results of phenomena causing service disruption)
  - ・Identify risks ②(Considering threats and risks)
  - ・Analyze risks
  - ・Evaluate risks
- Plenary meeting to share major risks recognized in each group
- Explanation and summary



Result of group work

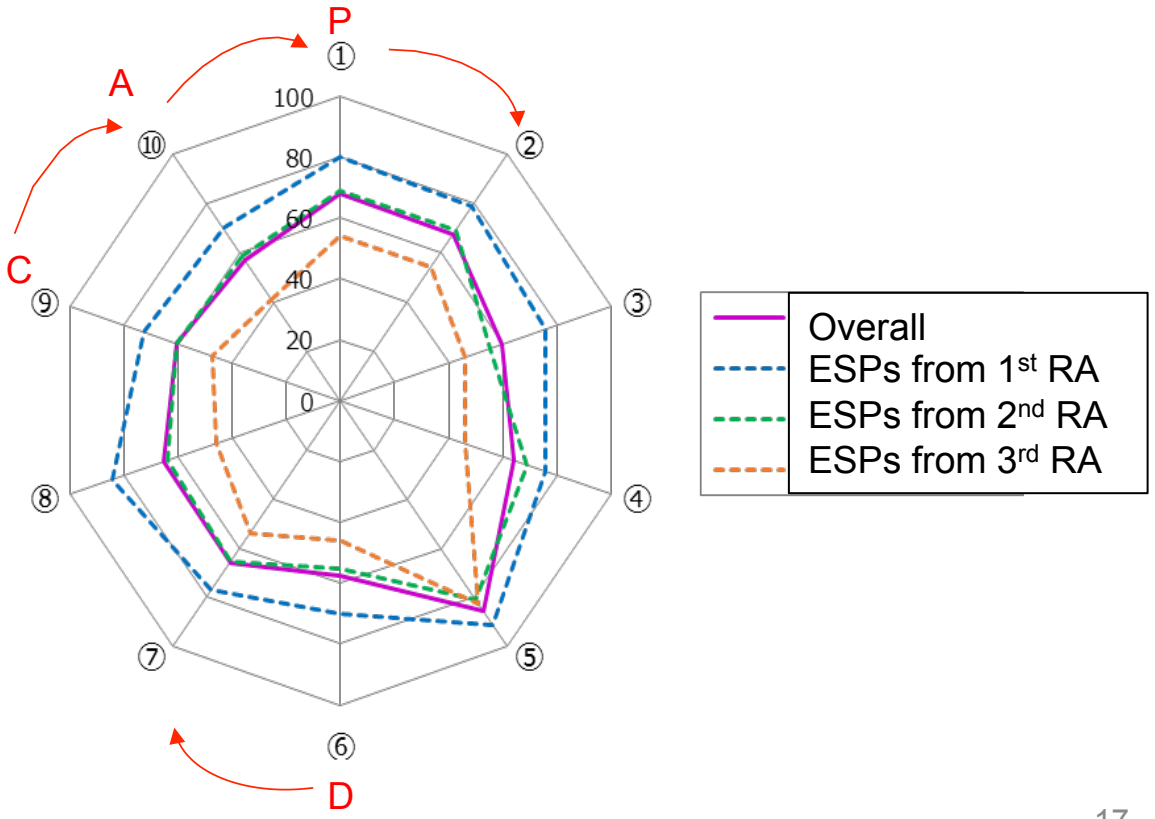
Plenary meeting

Feedback for implementation of CS measures in the ESPs

Overview of the submitted reports about the CS measure implementation

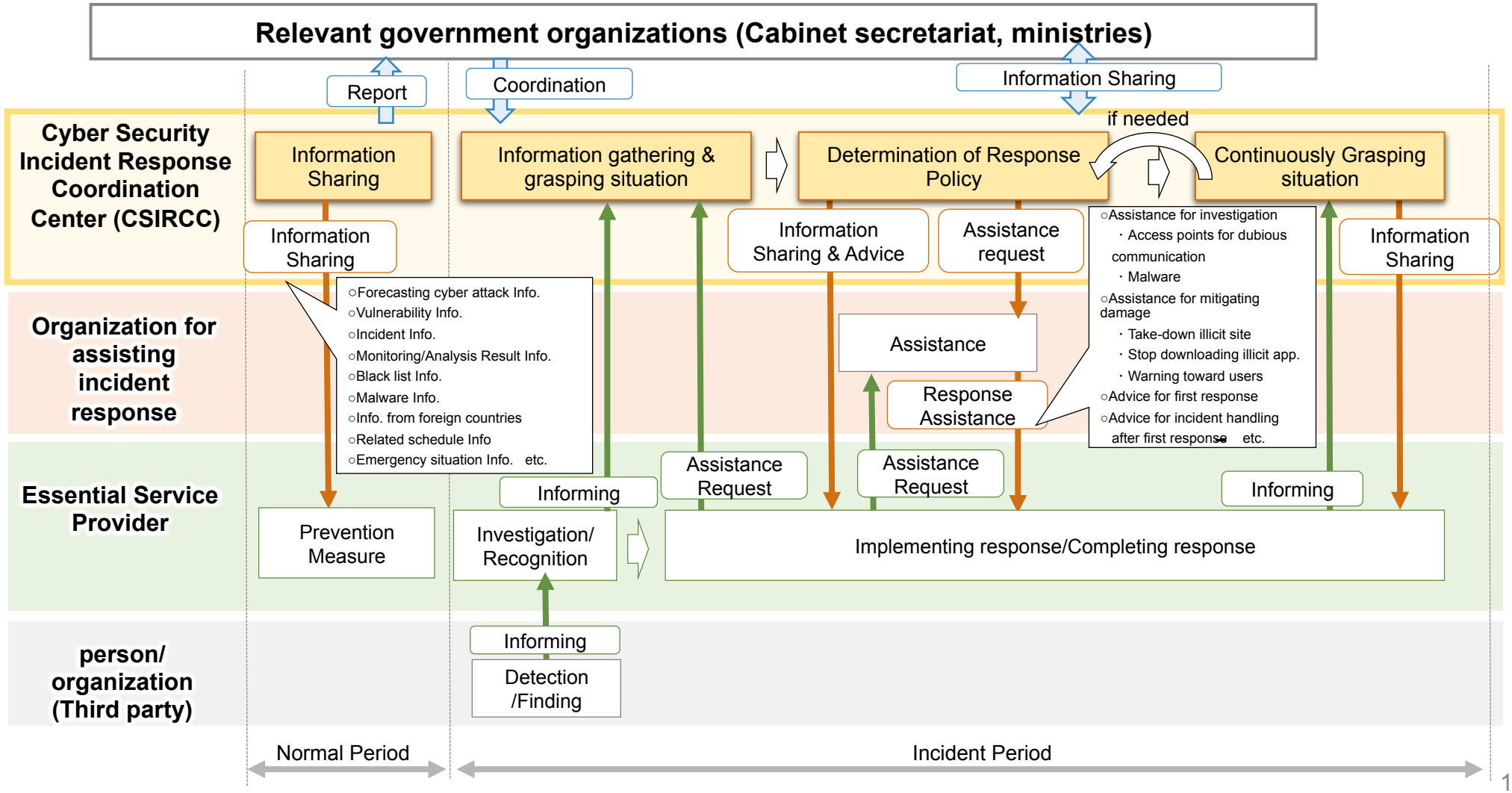
- Implementation rates in “Check” and “Act” are a little lower than those in “Plan” and “Do”
- Implementation rate in “Creation of Contingency Plan” is the lowest of all the 10 items
- Implementation rate in the ESPs that started participating in the 1st RA is the highest, those that started in the 2nd RA is the middle, and those that started in the 3rd RA is the lowest.

Plan (P)	①	Creation of basic policy
	②	Creation of internal rules
	③	Creation of CS measure plan
	④	Provision of training course
	⑤	Enhancement of internal control
Do (D)	⑥	Creation of contingency plan
	⑦	Creation of BCP
	⑧	Conduction of exercise and training
Check (C)	⑨	Conduction of audit
Act (A)	⑩	Consideration of CS measures to improve



Cyber Security Incident Response Coordination Center (CSIRCC)

- Core organization to share information regarding cyber security threats and incidents in close cooperation with the related organization
  - Gather and share information regarding the foreseeing cyber attacks, vulnerabilities, incidents and others in the relevant organizations through “Japan cyber security Information Sharing Platform (JISP)”,
  - Coordinate appropriate and swift response for organizations which require assistance in incident response



Services provided by CSIRCC (Plan)

- Established Cyber Security Incident Response Coordination Center (CSIRCC) in April 1, 2019
- CSIRCC provides with “Japan cyber security Information Sharing Platform (JISP)”, “incident response coordination function” and “exercise for communication with the relevant parties”.

Services provided by CSIRCC (Plan)

Provision of JISP

- ✓ Timely provision of information on vulnerabilities and cyber attacks
- ✓ Facilitation of communication among the users in the same industries as well as between the users and CSIRCC

Coordination of incident response

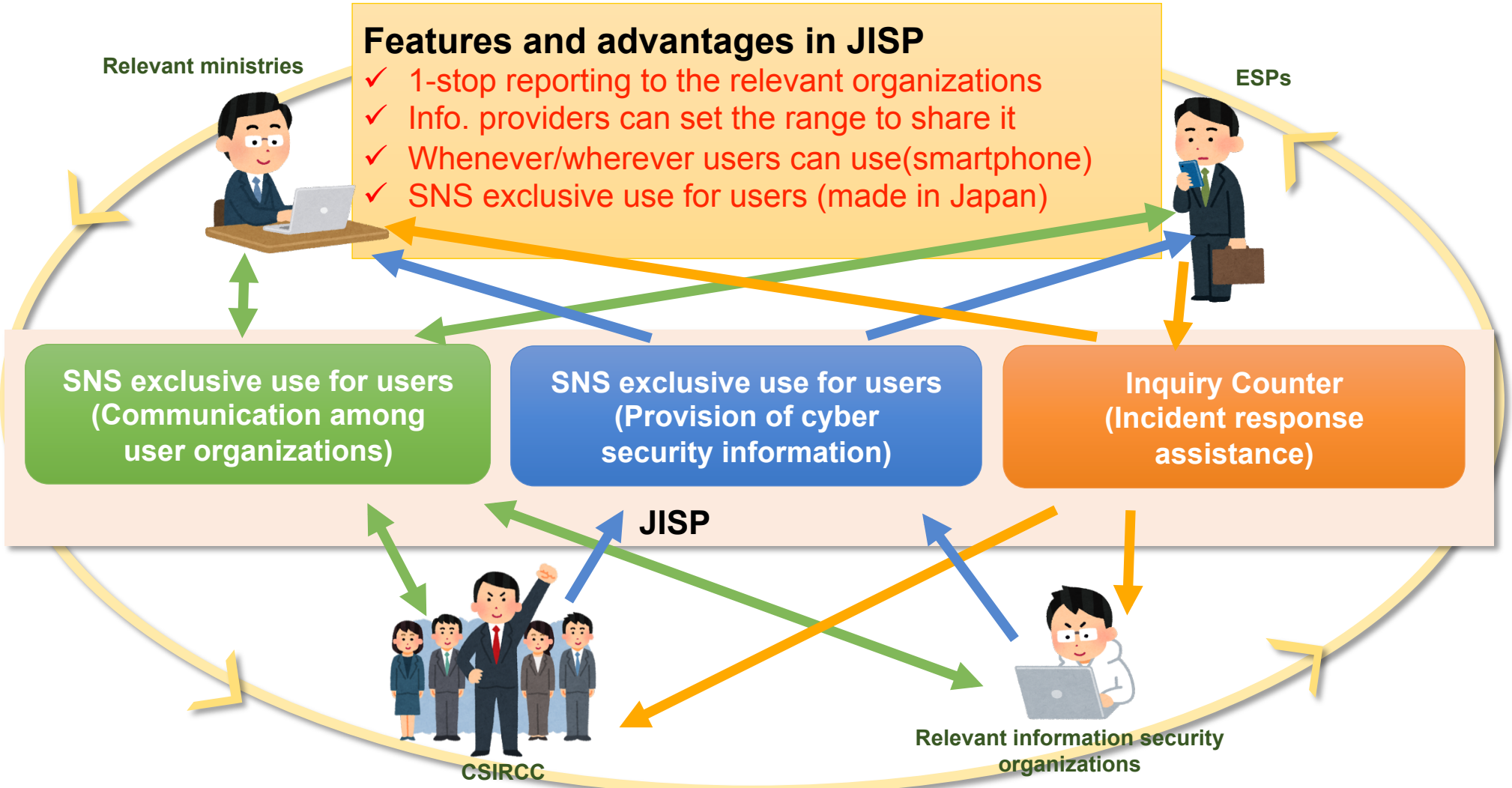
- ✓ Receipt of request for incident response assistance
- ✓ Consultation regardless of the occurrence of incident

Provision of exercise for communication with the relevant parties

- ✓ Conducting exercise to enhance incident response capability and confirm the information sharing procedure

Provision of Japan cyber security Information Sharing Platform (JISP)

- CSIRCC started to provide the relevant organizations※ with services through JISP
- CSIRCC plans to conduct exercises for the communication with the relevant parties



※TOCOG, Venue administrators, Tokyo Prefecture, Local governments, ESPs, Sports associations, Relevant information security organizations, national governments, police, etc.

Provision of Japan cyber security Information Sharing Platform (JISP)

➢ Usage scenes for each service

Communication among relevant organizations※

✓ Swiftly/securely communicate for the cooperation with the relevant organizations

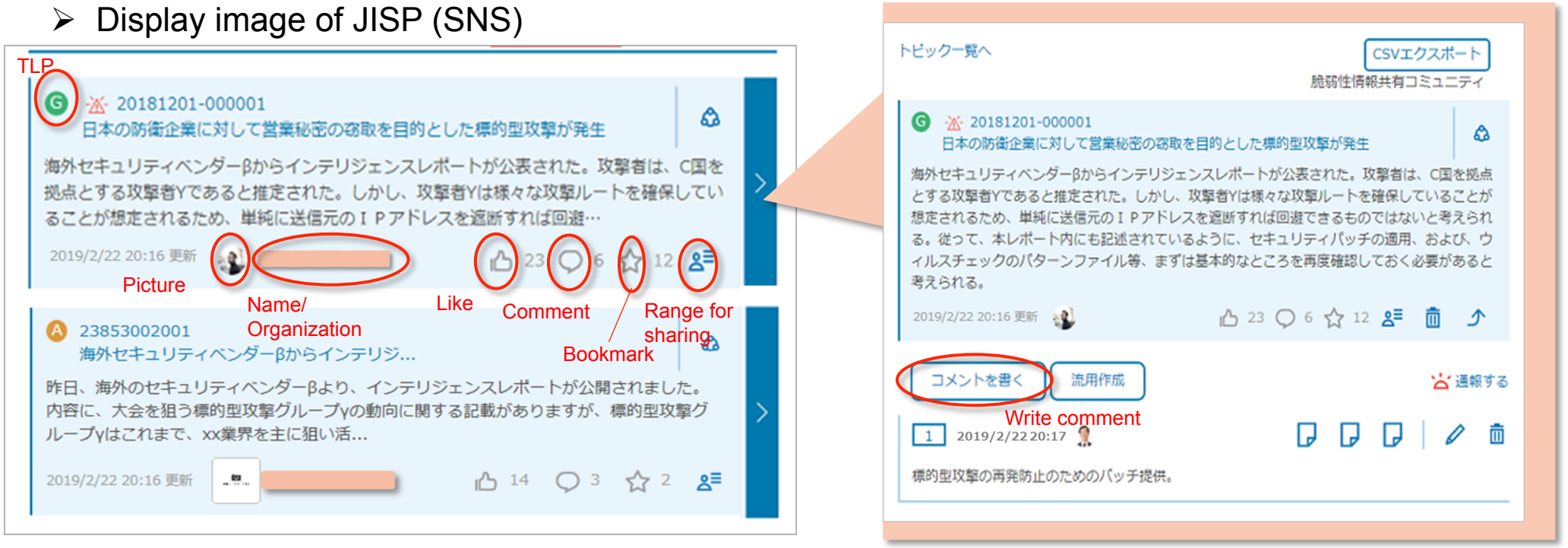
Provision of cyber security information

✓ Get vulnerability and cyber attack information in the use-friendly way

Inquiry counter

✓ Consult and receive advice in predictive or suspicious incidents and request the assistance in the incident

➢ Display image of JISP (SNS)



※TOCOG, Venue administrators, Tokyo Prefecture, Local governments, ESPs, Sports associations, Relevant information security organizations, national governments, police, etc.