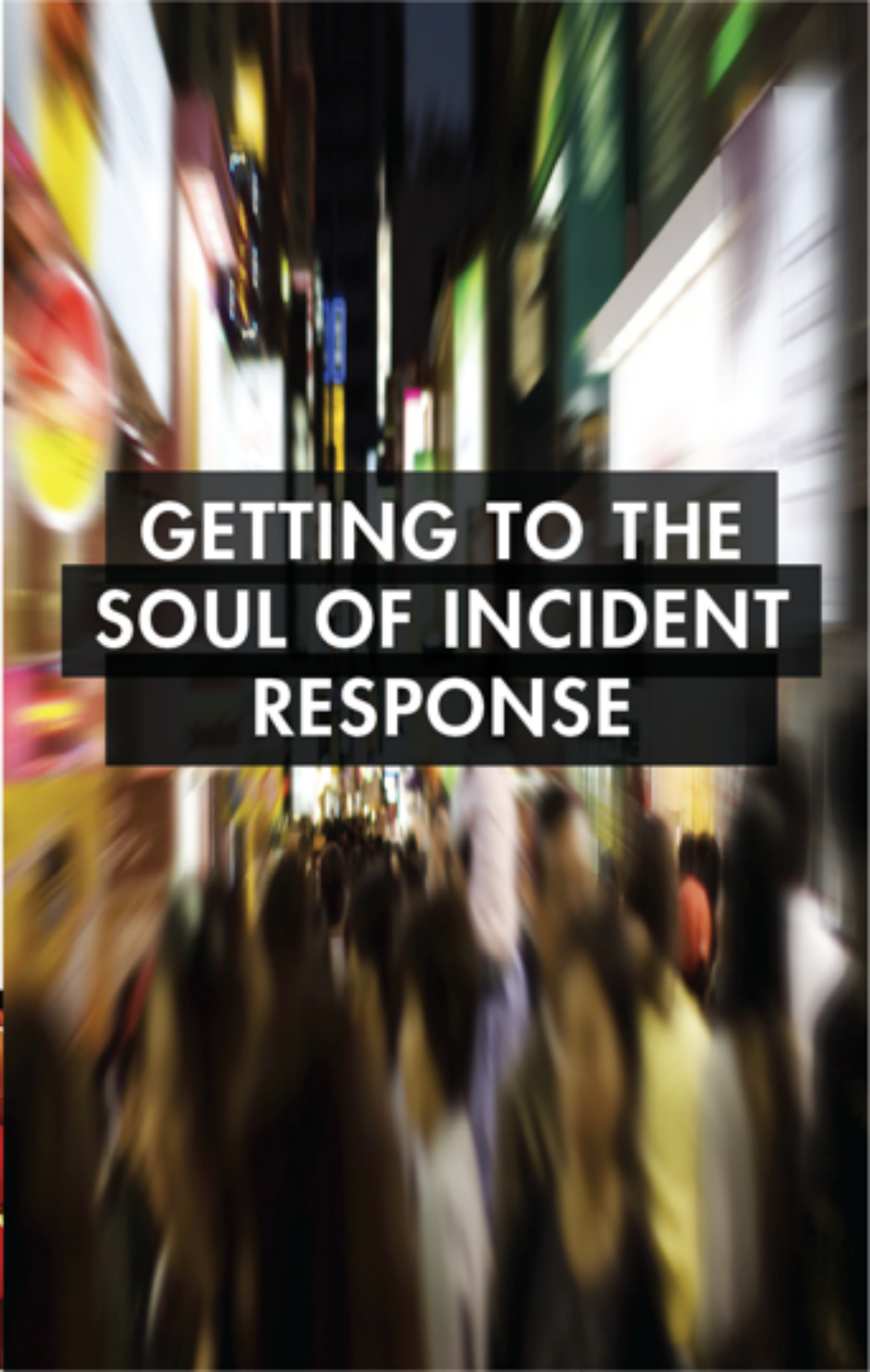
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



GETTING TO THE SOUL OF INCIDENT RESPONSE

Cybersecurity Readiness for Tokyo 2020 Olympic/Paralympic Games

Ko IKAI
Counsellor,
National center for Incident readiness and Strategy for Cybersecurity(NISC),
Government of Japan

NISC

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

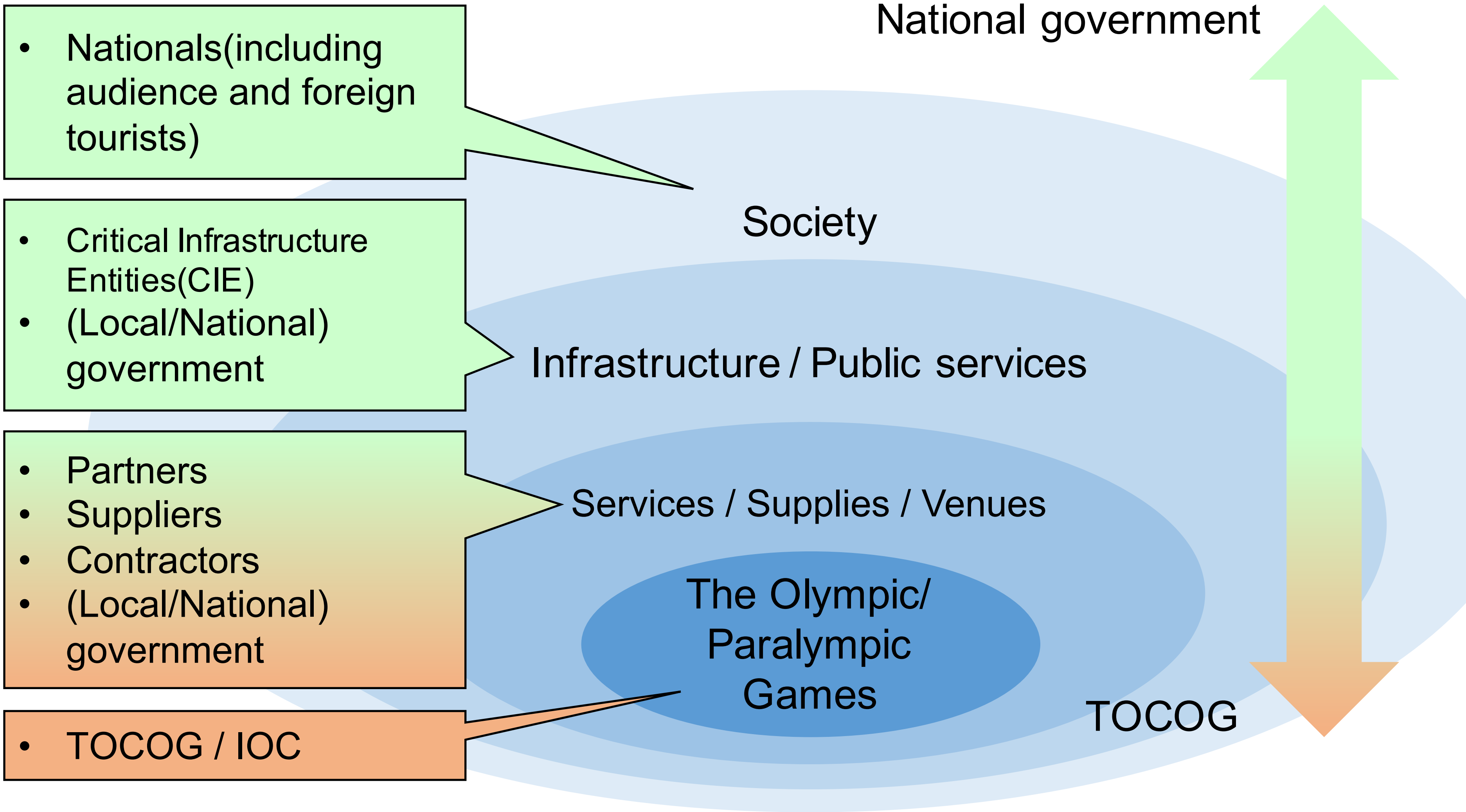
Contents

- Overview of Tokyo 2020 and its circumstances
- Cybersecurity stakeholders of Tokyo 2020
- The Government's role for cybersecurity
- Overview of Critical Information Infrastructure Protection (CIIP) measures in Japan
- Cybersecurity measures taken by the Government for Tokyo 2020
- Timetable for Tokyo 2020
- Challenges

Overview of Tokyo 2020 and its circumstances

Asset owners
(≈ prime responsibility holders)

Mission owners
(≈ prime responsible coordinator)



- Nationals(including audience and foreign tourists)

- Critical Infrastructure Entities(CIE)
- (Local/National) government

- Partners
- Suppliers
- Contractors
- (Local/National) government

- TOCOG / IOC

National government
Society
Infrastructure / Public services
Services / Supplies / Venues
The Olympic/ Paralympic Games
TOCOG

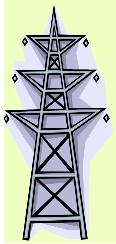
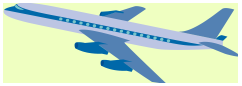
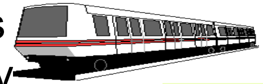
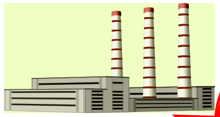
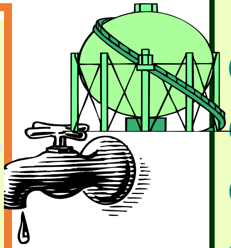
Overview of Cybersecurity Measures for CII in Japan

CII (13 Sectors)

- Information and Communications
- Finance
- Aviation
- Railways
- Electricity
- Gas
- Government and Administrative Services
- Medical Services
- Water
- Logistics
- Chemistry
- Credit Card
- Petroleum

Added in 2005 (Medical Services, Water, Logistics)

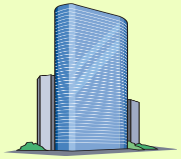
Added in 2014 (Chemistry, Credit Card, Petroleum)

Coordination and Cooperation by NISC

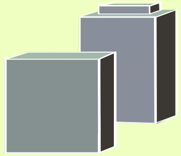
CII Sector-Specific Ministries

- FSA [Finance]
- MIC [Telecom and Local Gov.]
- MHLW [Medical Services and Water]
- METI [Electricity, Gas, Chemistry, Credit and Petroleum]
- MLIT [Aviation, Railway and Logistics]



Related Organizations, etc.

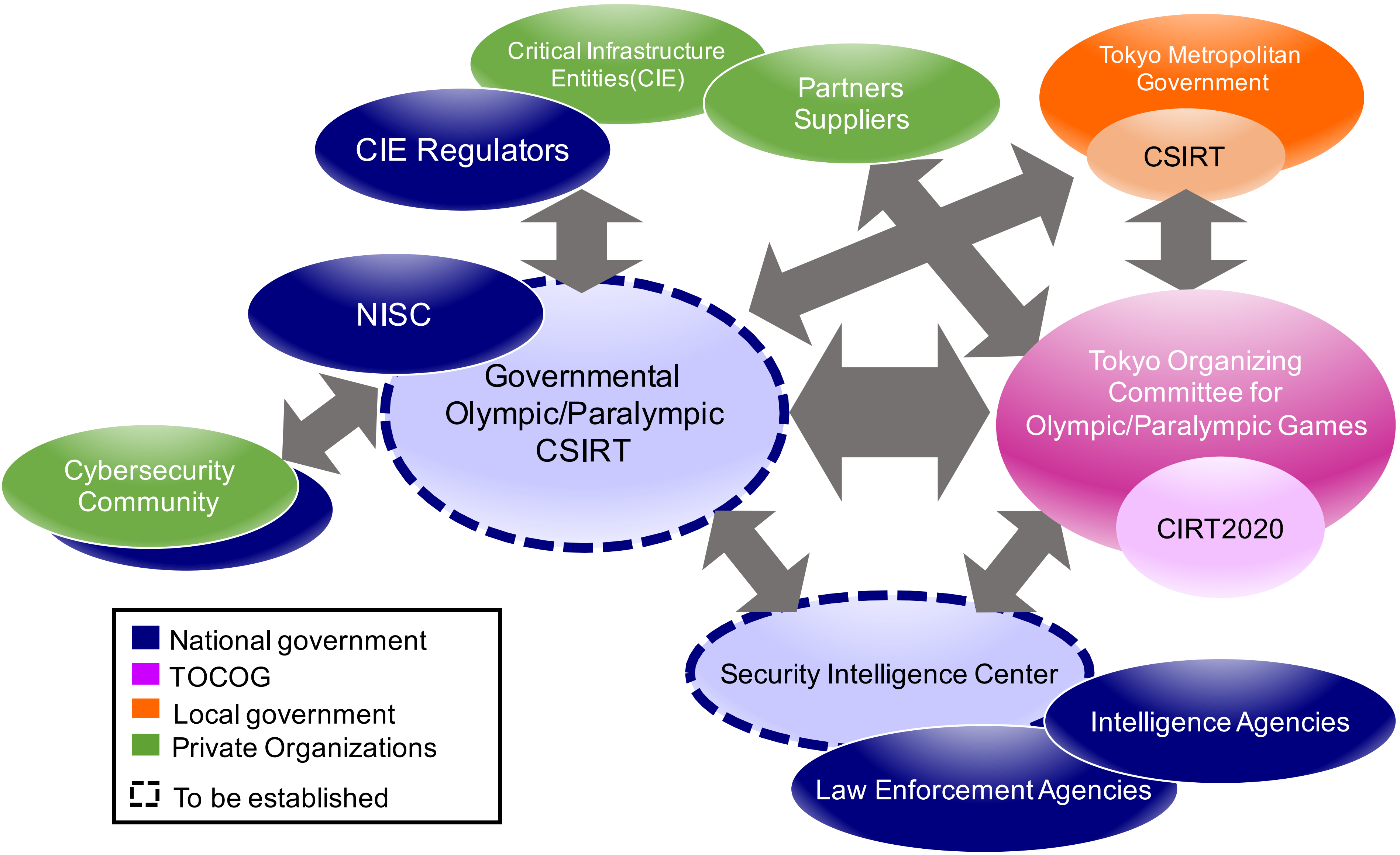
- Information Security Related Ministries
- Law Enforcement Ministries
- Disaster Management Ministries
- Other Related Organizations
- Cyberspace Related Operators



The Cybersecurity Strategy
(The Basic Policy of Critical Information Infrastructure Protection, 3rd Edition)

(1) Maintaining security principles	(2) Enhancing information sharing systems	(3) Enhancing Incident response capability	(4) Risk management	(5) Enhancing basis for CIIP

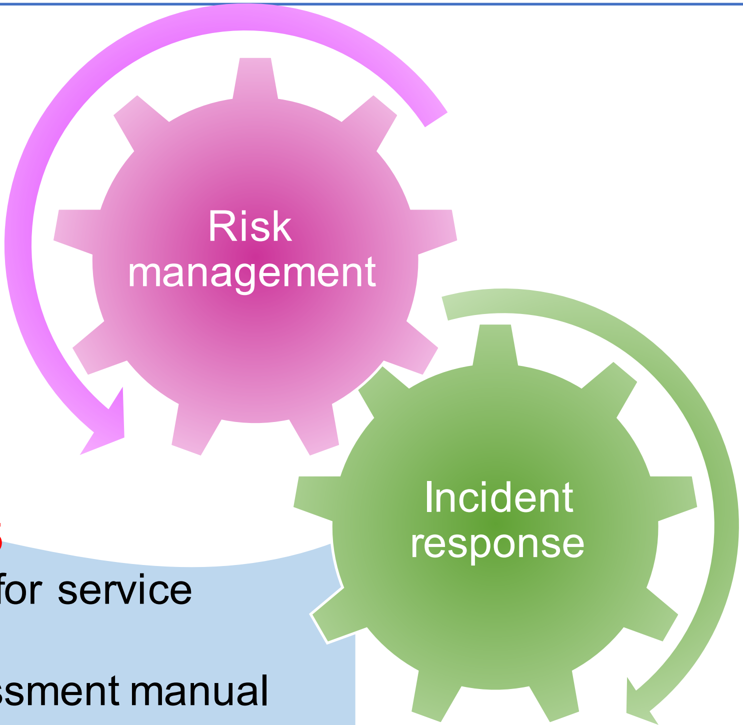
Cybersecurity stakeholders of Tokyo 2020


Critical Infrastructure Entities(CIE)
Partners Suppliers
Tokyo Metropolitan Government
CSIRT
CIE Regulators
NISC
Governmental Olympic/Paralympic CSIRT
Tokyo Organizing Committee for Olympic/Paralympic Games
CIRT2020
Cybersecurity Community
Security Intelligence Center
Intelligence Agencies
Law Enforcement Agencies

- 🟦 National government
- 🟪 TOCOG
- 🟧 Local government
- 🟩 Private Organizations
- ⬚ To be established

Cybersecurity Measures taken by the Government for Tokyo 2020

- It is critical to secure stable services supporting Tokyo 2020 by cybersecurity for its successful operation.
- To realize it, it is necessary to let critical service providers of the Games understand/address their own cybersecurity risks, and to establish and strengthen the structure for appropriate responses by timely information sharing among them.



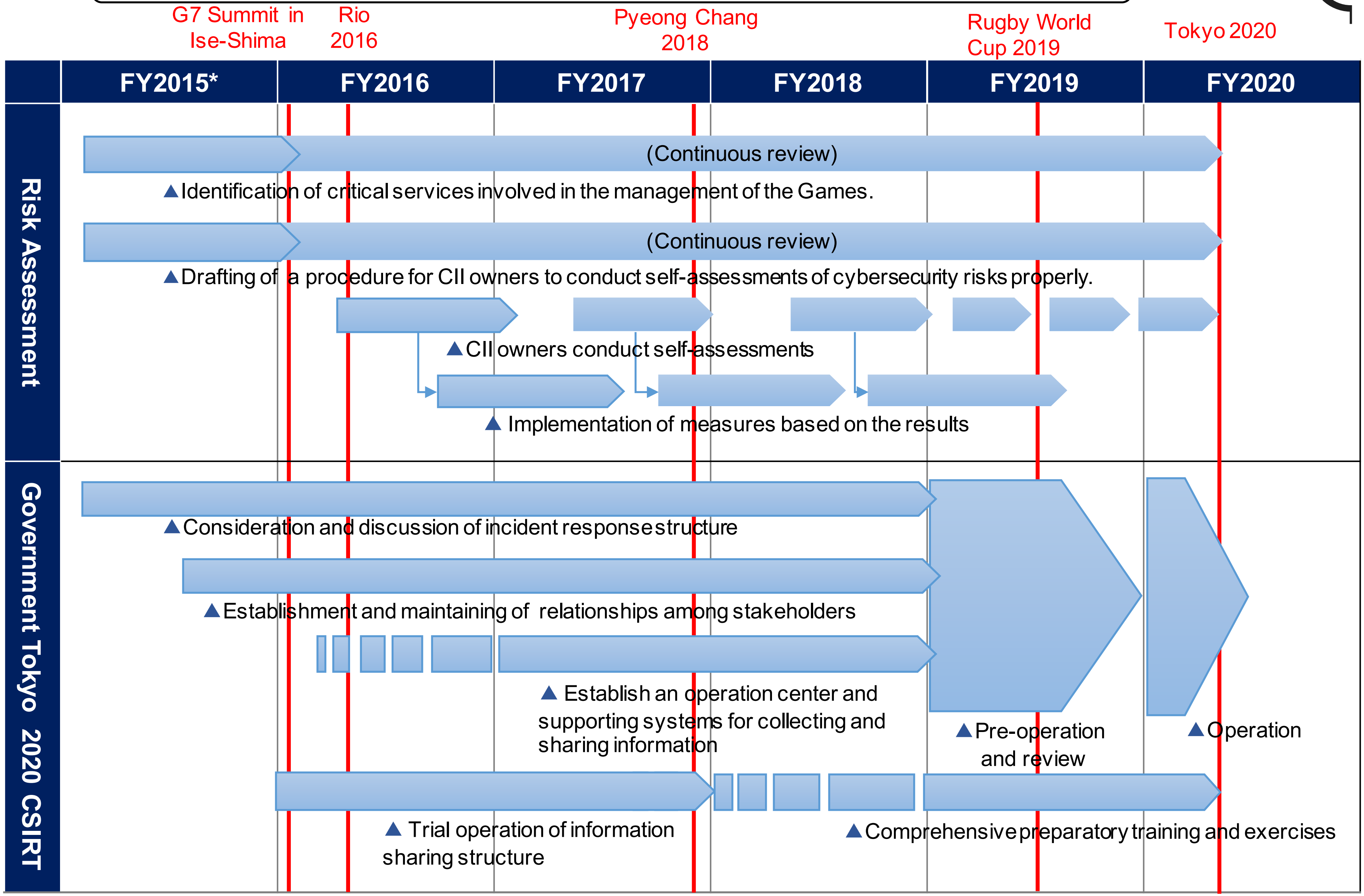
- Pick up critical service providers for the Games by criticality metrics
- Facilitate risk management by chosen providers with a manual of risk identification, analysis and evaluation

- Establish the Governmental Tokyo 2020 CSIRT as a core organization of information sharing among stakeholders
- Discuss details by demarcation between the roles of the public and private sectors in the Discussion Group for Cybersecurity Structure of Tokyo 2020

Outcomes of FY2015

- Criticality metrics for service providers
- Draft of risk assessment manual
- Agreement of information sharing with the domestic cybersecurity community

Timetable for Tokyo 2020 (draft)



G7 Summit in Ise-Shima

Rio 2016

Pyeong Chang 2018

Rugby World Cup 2019

Tokyo 2020

FY2015* | FY2016 | FY2017 | FY2018 | FY2019 | FY2020

Risk Assessment

(Continuous review)

▲Identification of critical services involved in the management of the Games.

(Continuous review)

▲Drafting of a procedure for CII owners to conduct self-assessments of cybersecurity risks properly.

▲CII owners conduct self-assessments

▲ Implementation of measures based on the results

Government Tokyo 2020 CSIRT

▲Consideration and discussion of incident response structure

▲Establishment and maintaining of relationships among stakeholders

▲ Establish an operation center and supporting systems for collecting and sharing information

▲Pre-operation and review

▲Operation

▲ Trial operation of information sharing structure

▲Comprehensive preparatory training and exercises

* Fiscal Year of Japan starts on April 1st.

Challenges

- Unpredictability
  No one can accurately predict future changes of cyber threat trends. Keep flexibility.
- Complexity
  Many stakeholders works simultaneously with a lot of interoperations. Avoid combinational problem.
- Broadness
  No organization, not even the Government of Japan, can be a “Big Brother.” Keep cooperative relationships domestically and internationally.
- Reputation-oriented big bosses

Thank you for your attention!

We absolutely welcome your kind comments and supports for our preparation for Tokyo 2020.

NISC

National center of Incident readiness and Strategy for Cybersecurity

Contact : ikai-k6i5@cyber.go.jp