Summary of the Cybersecurity Policy for CIP (4th Edition)

April 18, 2017 Published
July 25, 2018 Revised

1．Purpose of the Cybersecurity Policy for CIP (4th Edition) (“this Cybersecurity Policy”)

◆ Promotion of activities for reduction of Critical Infrastructure Services (CISs) outage risk resulting from cyberattacks, natural disasters, etc. and ensuring resilience in order to provide CISs safely and continuously, based on active involvement of top management (Mission Assurance)

◆ Essential services for organizing the Olympic and Paralympic games shall be secured.

2．Challenges

◆ CI operators are gradually coming to take on voluntary activities, and still have some challenges on Check & Act in the PDCA cycle

◆ Improve information sharing not only IT but also OT (Operational Technology) and promote incident readiness

◆ Continue and improve provision of information to the nation through analysis and cooperation with various entities all over the world

3．Policy Priorities

(1) Promotion of Leading Activities (Classification)

- Enforcing and improving the leading activities of some sectors (such as Electric power supply, Information & Communication and Financial services), which are highly depended upon by other CISs and cause a big impact on society in the case of outages
- Encouraging other CI operators by expanding the leading activities

(2) Enhancement of Information Sharing System toward the Olympic and Paralympic Games

- Considering introduction of the severity schema on CISs outages
- Breaking the barrier of information sharing by diversifying the contact formation (Anonymization, sharing via the CEPTOAR* Secretariat, Cybersecurity related agencies) Study of gathering cross-sectoral information into the cabinet secretariat

  *Capability for Engineering of Protection, Technical Operation, Analysis and Response
- Development of information sharing system utilizing the hotline (Automation, Work saving, Expediting, Ensuring)
- Clarification of the scope of information sharing and provision including the OT, IoT, etc.
- Maintenance and improvement of CIP capability by improvement of exercises and penetration of the results
- Expanding the protection scope as “protection as plane” including the supply chain

(3) Promotion of Incident Readiness Based on Risk Management

- Dissemination of risk assessment by providing “the risk assessment guideline for mission assurance” and workshops
- Promotion of incident readiness of CI operators by establishing BCPs and contingency plans
- Enhancing the monitoring and review by providing the perspective of internal audit in risk management and incident readiness

4．Duration

◆ The 4th Edition will cover until the end of the Olympic and Paralympic games, and will be revised even within the period as necessary.

The Cybersecurity Policy for CIP (4th Edition)

Promoting CIP through public-private partnership

On the basis of the concept of mission assurance, in order to safely and continuously provide critical infrastructure services(CISs) and to avoid serious effects on the national life and socioeconomic activities from CISs outages resulting from cyber-attacks, natural disasters or other causes, all stakeholders should protect the critical infrastructures by reducing the occurrence of CISs outages as much as possible and by ensuring prompt recovery from outages.

Critical Infrastructures (14 sectors)

- Info. & comm.
- Finance
- Aviation
- Airport
- Railway
- Electric power supply
- Gas supply
- Gov. & admin. (incl. municipal government)
- Medical
- Water
- Logistics
- Chemical industries
- Credit card
- Petroleum industries

【NISC】 coordination & cooperation

Responsible ministries for critical infrastructure (5 ministries)

- FSA [Financial]
- MIC [Info & comm, Admin]
- MHLW [Medical, Water]
- METI [Electric power supply, Gas, Chemical, Credit card, Petroleum]
- MLIT [Aviation, Airport, Railway, Logistics]

Organizations concerned

- Cybersecurity related ministries [MIC, METI, etc.]
- Crisis management ministries [NPA, MOD, etc.]
- Disaster prevention related ministries [CAO, ministries, etc.]
- Cybersecurity related agencies [NICT, IPA, JPCERT, etc.]
- Cyberspace-related operators [Various vendors, etc.]

This Cybersecurity Policy

Maintenance and promotion of the safety principles

Promoting continual improvement of the "guidelines" of measures that are most necessary from a cross-sectoral perspective, and the "safety principles" in each sector.

Enhancement of information sharing system

Enhancing the public-private and cross-sectoral information sharing system by diversifying the contact formation, defining the sharing of information, etc.

Enhancement of incident response capability

Enhancing the overall CISs outages response system by the implementation of exercises and collaboration between exercises and trainings, etc. performed under public-private partnership

Risk management and preparation of incident readiness

Promoting comprehensive management including preparation of incident readiness such as risk assessment, establishment of contingency plans by CI operators, etc.

Enhancement of the basis for CIP

Review of the protection scope, promoting the public relations activities and international cooperation, appeal to top management, promotion of developing human resources

Basic Principles and Points of the Cybersecurity Policy for CIP (4th Edition)(1/2)

Purpose of "critical infrastructure protection"

In order to **safely and continuously provide** critical infrastructure services(CISs) and to avoid serious effects on the national life and socioeconomic activities from **CISs outages resulting from cyberattacks, natural disasters or other causes**, all stakeholders should protect the critical infrastructures by **reducing** the risk of CISs outages **as much as possible and by ensuring prompt recovery** from outages.

"Basic principles"

In the first place, critical infrastructure operators should implement cybersecurity measures on their own responsibility.

On the basis of the concept of mission assurance for all CIs, a sense of security should be nurtured among the public through CI protection activities in cooperation between Government and the private sector.

- The critical infrastructure operators should respectively take measures and make effort for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- **Government organizations** should **provide necessary support** for critical infrastructure operators' cybersecurity activities.
- Each critical infrastructure operator should **cooperate and coordinate with other stakeholders** due to the limit of each operator’s individual cybersecurity measures to address various threats.

Basic Principles and Points of the Cybersecurity Policy (4th Edition)(2/2)

Responsibility of stakeholders (critical infrastructure operators, government organizations, cybersecurity related agencies, etc.)

- All stakeholders should periodically check the progress of their own measures and policies as part of relevant efforts and **accurately recognize the current circumstances**, and **proactively determine the goals of relevant activities**. In addition, stakeholders should **enhance their cooperation with each other**, taking into account the status of other stakeholders' relevant activities.
- All stakeholders should understand the 5W1H (when, where, who, why, what and how) of responses to CISs outages depending on the scale thereof and should be able to calmly address signs or occurrence of any CISs outages. They should also be capable of cooperating with other stakeholders and **respond in a cooperative and concerted manner** in addition to **ensuring robust communication among various stakeholders** and taking proactive measures.

Responsibility of critical infrastructure operators’ executives and senior managers

- Recognize **their responsibility for ensuring cybersecurity** and exert their leadership in cybersecurity measures from the viewpoint of mission assurance
- With the awareness that their individual efforts also contribute to the development of society as a whole, take cybersecurity measures while **involving their supply chains (business partners, subsidiaries and affiliated companies, etc.)**
- Develop incident readiness even in normal times and **disclose information** on responses properly in the event of an incident from the perspective of **gaining trust and nurturing a sense of security among stakeholders**
- **Constantly secure management resources**, such as budgets, systems and personnel, necessary for the abovementioned measures and **devise risk-based allocation thereof**

Policy Group (1): Maintenance and Promotion of the Safety Principles

Look to continual improvement of the “guidelines" and “safety principles" under the PDCA cycle of security activities in order to maintain and strengthen the ability of critical infrastructure protection

* Safety principles: Generically refer to relevant laws, industry standards/guidelines, internal regulations (IR), etc.
* Guidelines: Contain items of measures that are most necessary from a cross-sectoral perspective, in order to contribute to preparation and revision of safety principles

Current Issues

- The PDCA cycle that allows CI operators to judge the necessity of review and improve independently is prevailing in the code of conduct of CI operators. However, the activities of “Check” and “Act” in the PDCA cycle are not established.

Activities during this Cybersecurity Policy term

(1) Continual improvement of the guidelines for safety principles

- Describing the details about the formation of cybersecurity culture and items and actions which top management who are responsible for carrying out the PDCA cycle must recognize.
- Describing the necessity of preparation of incident readiness by establishment of BCP, contingency plans, etc. on the basis of the mission assurance.

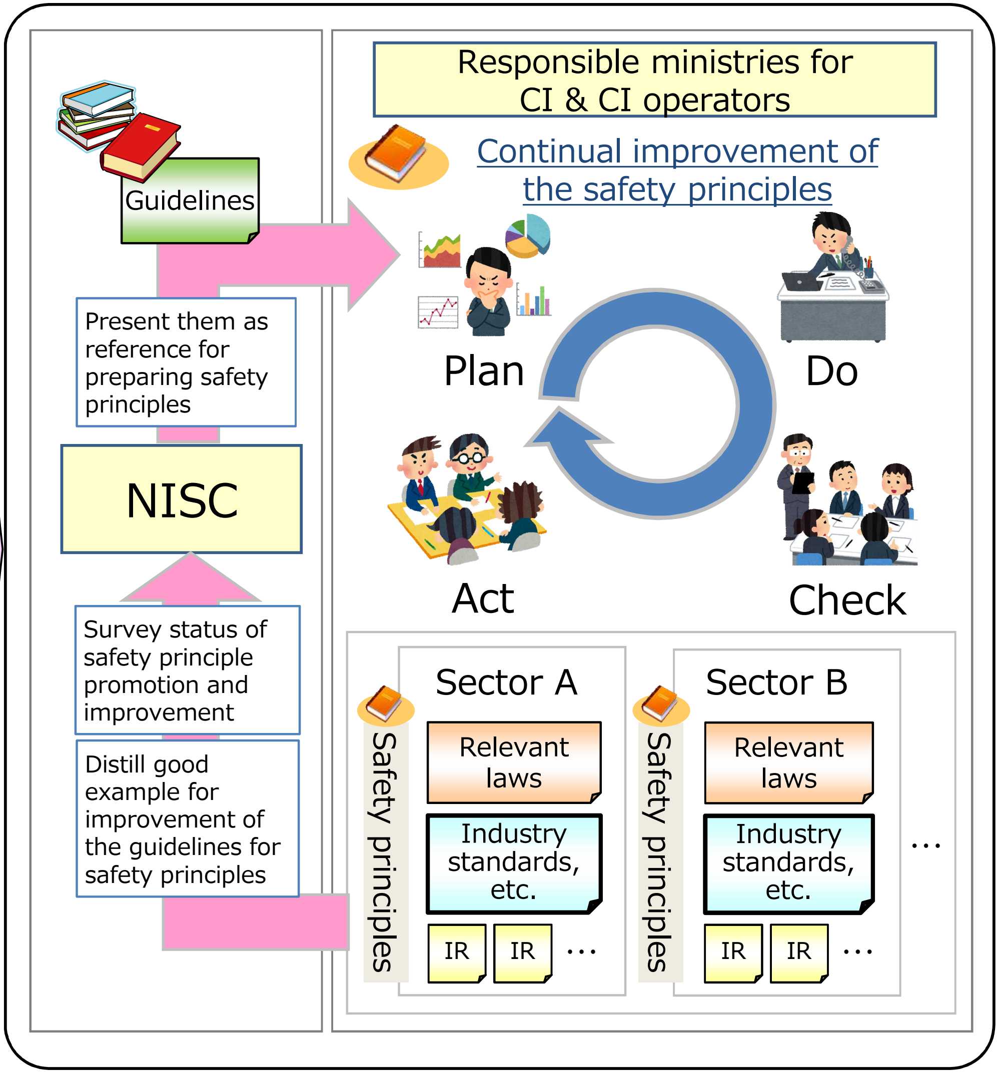
(2) Continual improvement of the safety principles

- Promotion of improvement process of standards and guidelines which reflects the PDCA cycle.
- Continual improvement of the institutional framework such as positioning the cybersecurity activities as safety regulation, embodiment of service maintenance level in relevant laws.

(3) Promotion of the safety principles

- Understanding the status of security measure through the annual questionnaire of CI operators, etc.
- Utilizing the answer of questionnaire, supporting CI operators to be able to recognize issues of measures, solutions, etc.

Activities based on this Cybersecurity Policy


Guidelines
Present them as reference for preparing safety principles
NISC
Survey status of safety principle promotion and improvement
Distill good example for improvement of the guidelines for safety principles
Responsible ministries for CI & CI operators
Continual improvement of the safety principles
Plan
Do
Act
Check
Safety principles
Sector A
Relevant laws
Industry standards, etc.
IR
IR
…
Safety principles
Sector B
Relevant laws
Industry standards, etc.
IR
IR
…
…

Policy Group (2): Enhancement of Information Sharing System

To rapidly address each CI operator's cybersecurity trends that change from day to day, further enhance information sharing between the public and private sectors, within a sector, and among sectors and/or outside sectors

Current Issues

- ➢ The understanding of the significance and necessity of information sharing is not sufficient in some CI operators.
- ➢ The lack of prompt and effective information sharing system in some CI operators.
- ➢ The understanding of information to be shared may not be sufficient.
- ➢ The dissemination and promotion of voluntary efforts by CI operators may not be sufficient.

Activities during this Cybersecurity Policy term

(1) Improvement of the information sharing system

- ➢ Adding new contact formation
- ➢ Preparation of the information sharing system for Olympic and Paralympic games.
- ➢ Positive cooperation with cybersecurity related agencies

(2) Further promotion of information sharing

- ➢ Consideration of introduction of the severity schema on CISs outages.
- ➢ Defining information to be shared

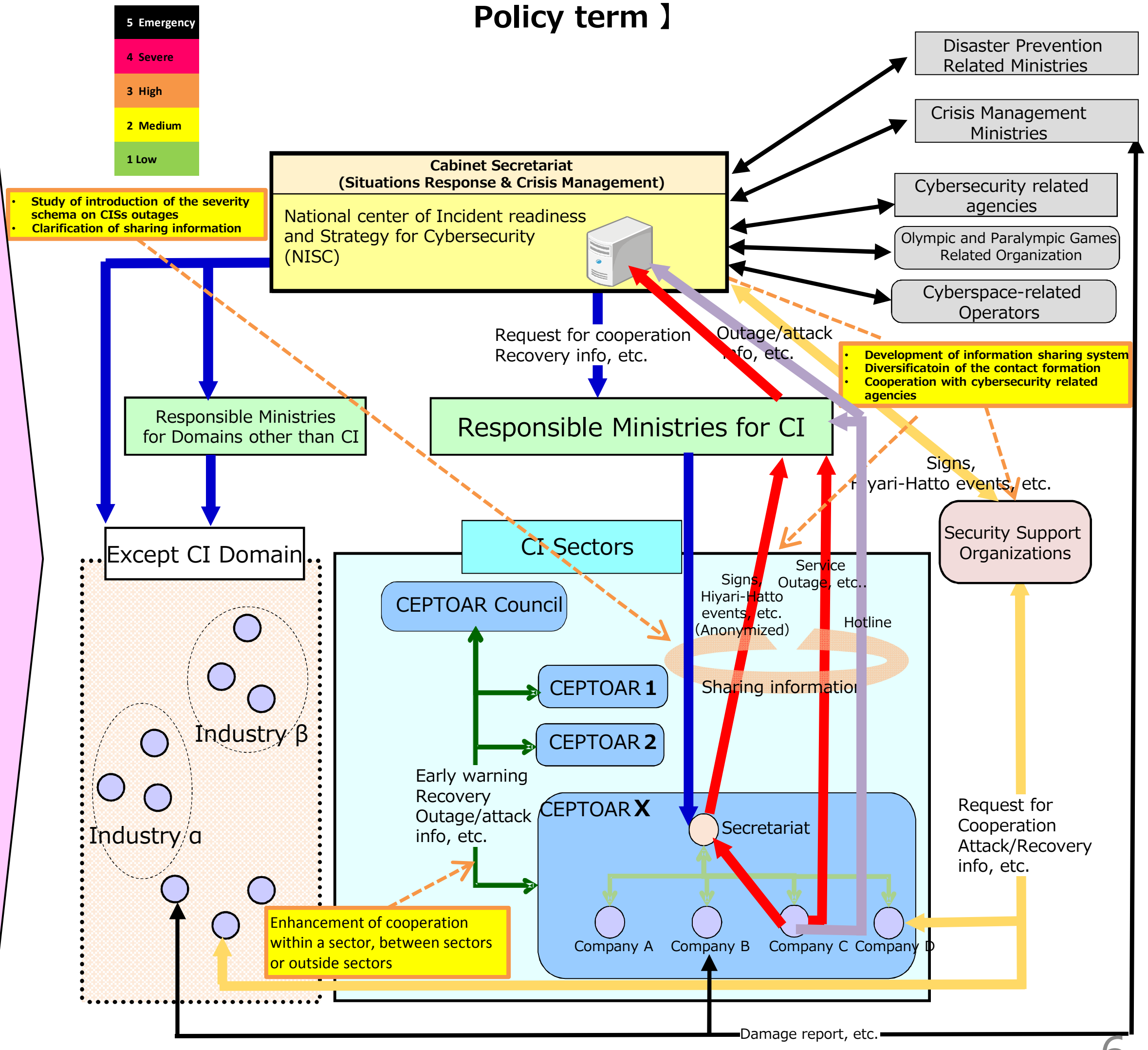
  Including the information of OT, IoT, etc. in the scope of information sharing and providing.

(3) Further activation of private activities

- ➢ Further improvement of information sharing within the CEPTOAR or among CEPTOARs
- ➢ Spreading the activities such as ISAC doing leading activities

Activities based on this Cybersecurity Policy

【Information sharing system Activities during this Cybersecurity Policy term】



5 Emergency
4 Severe
3 High
2 Medium
1 Low
Study of introduction of the severity schema on CISs outages
Clarification of sharing information
Cabinet Secretariat
(Situations Response & Crisis Management)
National center of Incident readiness and Strategy for Cybersecurity (NISC)
Disaster Prevention Related Ministries
Crisis Management Ministries
Cybersecurity related agencies
Olympic and Paralympic Games Related Organization
Cyberspace-related Operators
Request for cooperation
Recovery info, etc.
Outage/attack info, etc.
Development of information sharing system
Diversificatoin of the contact formation
Cooperation with cybersecurity related agencies
Responsible Ministries for Domains other than CI
Responsible Ministries for CI
Signs, Hiyari-Hatto events, etc.
Security Support Organizations
Except CI Domain
Industry β
Industry α
CI Sectors
CEPTOAR Council
CEPTOAR 1
CEPTOAR 2
Signs, Hiyari-Hatto events, etc. (Anonymized)
Service Outage, etc..
Hotline
Sharing information
Early warning
Recovery
Outage/attack info, etc.
CEPTOAR X
Secretariat
Company A
Company B
Company C
Company D
Enhancement of cooperation within a sector, between sectors or outside sectors
Request for Cooperation
Attack/Recovery info, etc.
Damage report, etc.

Policy Group (3): Enhancement of Incident Response Capability

Maintain and enhance the CIP capability through improvement of exercises and training which fit the actual state of response of CISs outages in operators and exercise needs.

Current Issues

- Planning and promotion of more effective and practical cross-sectoral exercises
- Spreading of participants in cross-sectoral exercises
- Spreading and promotion of lessons learned from cross-sectoral exercises fit for the roll of each stakeholder in service outage

Activities during this Cybersecurity Policy term

(1) Continuous improvement of cross-sectoral exercises

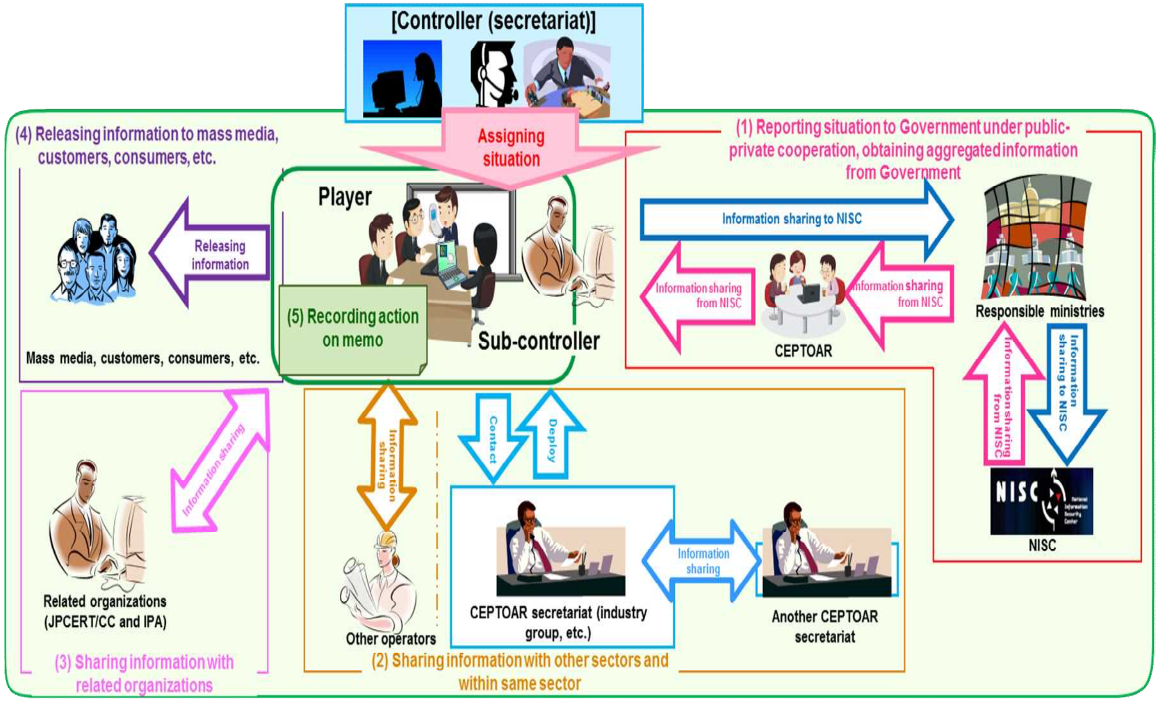
- Planning of exercises that fit the actual state of CI operators
  - Taking needs from CI operators in exercises
  - Maintenance of exercise scenarios reflecting the latest trends
  - Extending the scope of participants such as other operators except CI operators and those closely related to CI

(2) Increasing participants for more spreading of lessons learned

- Promotion for new participants
- Mutual cooperation with other exercises / training
- Planning exercises that are able to promote the understanding of top management
- Return the know-how of exercises that contribute to holding the exercises independently (provision of a virtual exercise environment)

Activities based on this Cybersecurity Policy

Summary of cross-sectoral exercises


[Controller (secretariat)]
Assigning situation
(4) Releasing information to mass media, customers, consumers, etc.
Releasing information
Mass media, customers, consumers, etc.
Player
(5) Recording action on memo
Sub-controller
(1) Reporting situation to Government under public-private cooperation, obtaining aggregated information from Government
Information sharing to NISC
Information sharing from NISC
CEPTOAR
Information sharing from NISC
Responsible ministries
Information sharing from NISC
Information sharing to NISC
NISC
Information sharing
Related organizations (JPCERT/CC and IPA)
(3) Sharing information with related organizations
Information sharing
Other operators
Contact
Deploy
CEPTOAR secretariat (industry group, etc.)
Information sharing
Another CEPTOAR secretariat
(2) Sharing information with other sectors and within same sector

Continuous improvement of cross-sectoral exercises

- Planning of exercises that fit the actual state of CI operators
- Promotion for new participants including operators except CI operators
- Mutual cooperation with other exercises / training
- Planning exercises that are able to promote the understanding of top management
- Return the know-how of exercises

Maintain and Improve the CIP capability

Policy Group (4): Risk Management and Preparation of Incident Readiness

Promote risk management that CI operators implement and the preparation of incident readiness to achieve safe and continuous CI service provision

Current Issues

- Recognition of the importance of risk assessment is spreading, but the concept and ways to implement it have not spread sufficiently.
- Needs for preparation of incident readiness are growing in case of CISs outages, but specific directions, supporting measures, etc. are not shown.

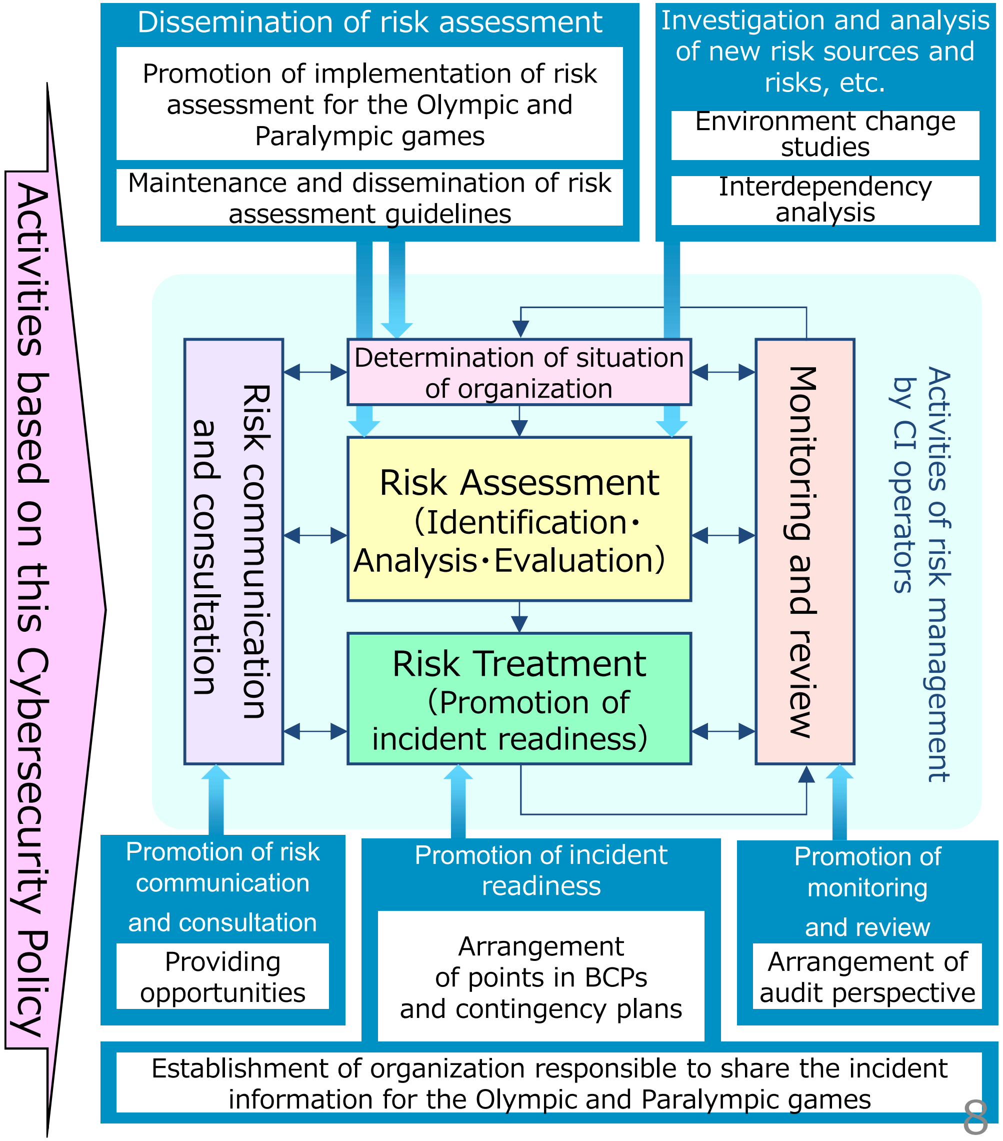
Activities during this Cybersecurity Policy term

(1) Basic view of risk management

(2) Promotion of risk management

- Dissemination of risk assessment
  - Promotion of implementation of risk assessment for Olympic and Paralympic games
  - Maintenance and dissemination of risk assessment guidelines based on the concept of mission assurance
- Investigation and analysis of new risk sources and risks, etc.
  - Environment change studies・Interdependency analysis
- Promotion of incident readiness
  - Arrangement of points in BCPs and contingency plans based on the concept of mission assurance
  - Establishment of organization responsible to share the incident information for the Olympic and Paralympic games
- Promotion of risk communication and consultation
  - Provision of opportunities for information and opinion sharing among stakeholders, including internal stakeholders
- Promotion of monitoring and review
  - Arrangement of audit perspective such as independent internal audit in CI operators.

(3) Establishment of process of reflection to and from other activities



Activities based on this Cybersecurity Policy

Dissemination of risk assessment

Promotion of implementation of risk assessment for the Olympic and Paralympic games

Maintenance and dissemination of risk assessment guidelines

Investigation and analysis of new risk sources and risks, etc.

Environment change studies

Interdependency analysis

Determination of situation of organization

Risk Assessment (Identification・Analysis・Evaluation)

Risk Treatment (Promotion of incident readiness)

Risk communication and consultation

Monitoring and review

Activities of risk management by CI operators

Promotion of risk communication and consultation

Providing opportunities

Promotion of incident readiness

Arrangement of points in BCPs and contingency plans

Promotion of monitoring and review

Arrangement of audit perspective

Establishment of organization responsible to share the incident information for the Olympic and Paralympic games

Policy Group (5): Enhancement of the Basis for CIP

Enhance common foundation activities that support the whole of this Cybersecurity Policy such as review of the protection scope of CI, public relations, international cooperation, appeal to top management and developing human resources, etc.

Current Issues

- “Protection as plane” for response to environment change
- Further promoting of public relations
- Improvement of international cybersecurity measure level
- Improvement of mindset of top management on cybersecurity
- Further quantitative and qualitative enhancing of human resources

Activities during this Cybersecurity Policy term

(1) Review of the protection scope of CI
- Activities towards “protection as plane” and from the perspective of securing national security

(2) Promotion of public relations activities
- Positive sending of frameworks of this Cybersecurity Policy, activities, etc. for the nation

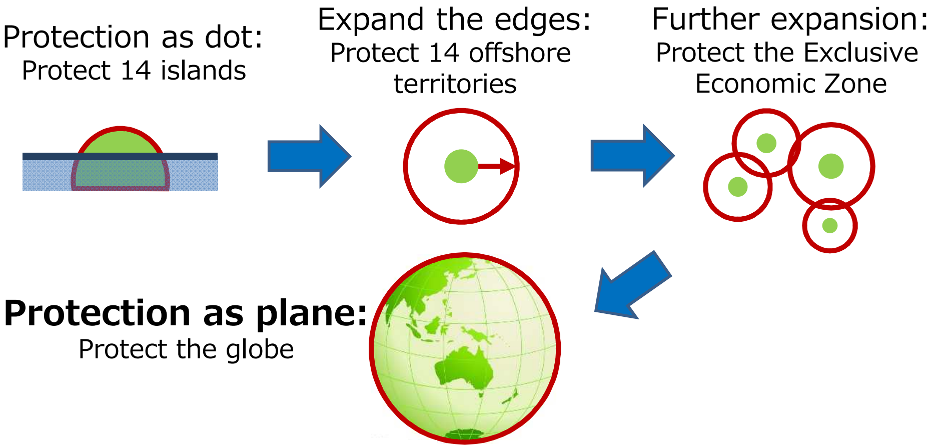
(3) Promotion of international cooperation
- Positive contribution to Improvement of international cybersecurity measure level

(4) Appeal to top management
- Appeal for improvement of awareness of top management on cybersecurity

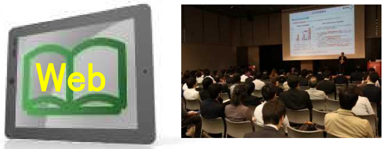
(5) Promotion of the development of human resources
- Promotion of development of bridge human resources, building of cross-sectoral system, exercises and qualification of cybersecurity, etc.

Activities based on this Cybersecurity Policy

Review of the protection scope of CI



Public relations activities



Promotion via Web, lecture, etc.

International cooperation

asean

MERIDIAN Connecting and Protecting

Cooperation of bilateral, inter-regional, and multilateral frameworks,

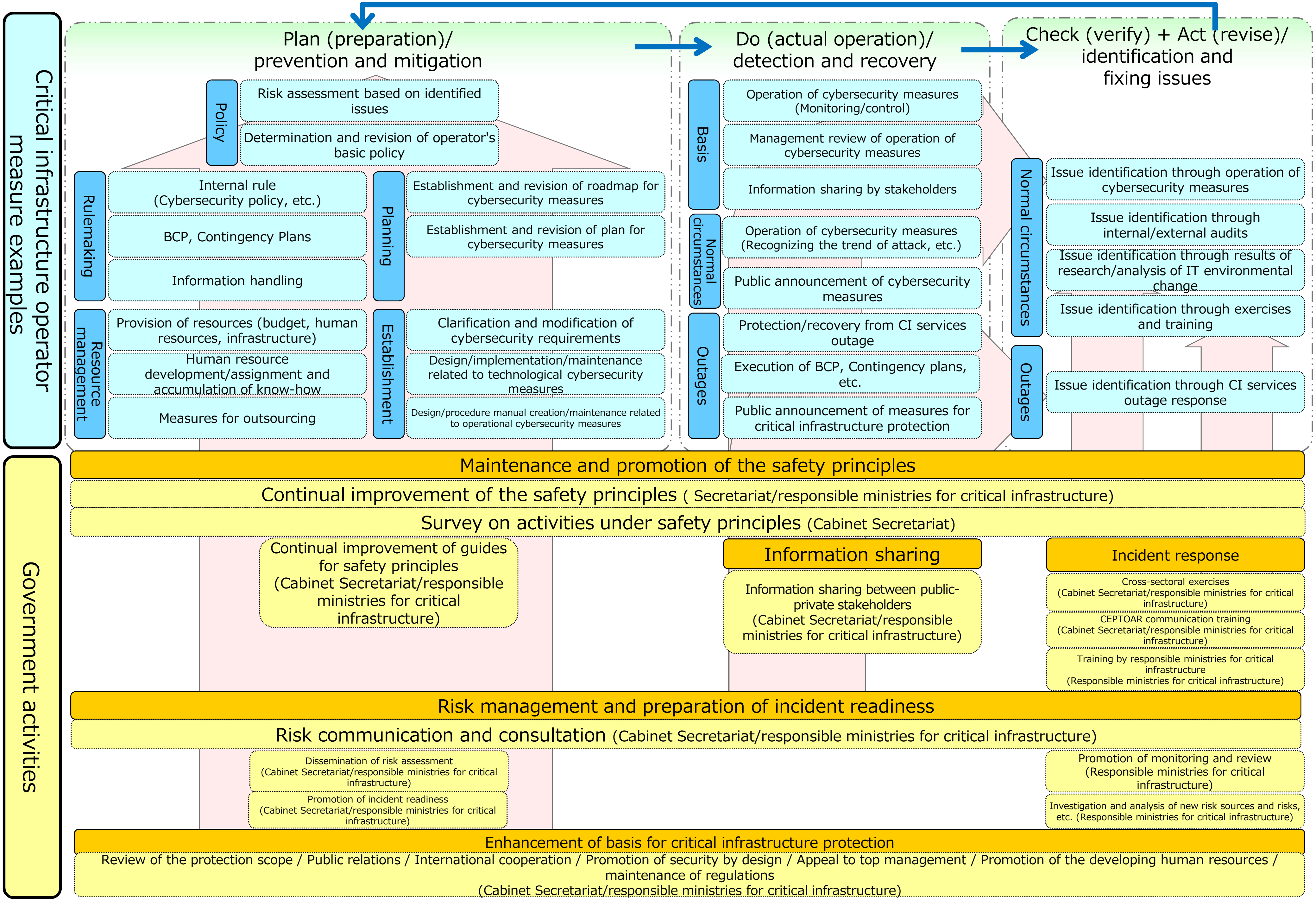
Appeal to top management

Improvement of awareness, improvement of activities of cybersecurity

Developing human resources

Promoting the activities based on the “Cybersecurity Experts Development Program”

"Critical Infrastructure Operator Measure Examples" and "Government Activities"



Critical infrastructure operator measure examples

Plan (preparation)/ prevention and mitigation

Policy
- Risk assessment based on identified issues
- Determination and revision of operator's basic policy

Rulemaking
- Internal rule (Cybersecurity policy, etc.)
- BCP, Contingency Plans
- Information handling

Planning
- Establishment and revision of roadmap for cybersecurity measures
- Establishment and revision of plan for cybersecurity measures

Resource management
- Provision of resources (budget, human resources, infrastructure)
- Human resource development/assignment and accumulation of know-how
- Measures for outsourcing

Establishment
- Clarification and modification of cybersecurity requirements
- Design/implementation/maintenance related to technological cybersecurity measures
- Design/procedure manual creation/maintenance related to operational cybersecurity measures

Do (actual operation)/ detection and recovery

Basis
- Operation of cybersecurity measures (Monitoring/control)
- Management review of operation of cybersecurity measures
- Information sharing by stakeholders

Normal circumstances
- Operation of cybersecurity measures (Recognizing the trend of attack, etc.)
- Public announcement of cybersecurity measures

Outages
- Protection/recovery from CI services outage
- Execution of BCP, Contingency plans, etc.
- Public announcement of measures for critical infrastructure protection

Check (verify) + Act (revise)/ identification and fixing issues

Normal circumstances
- Issue identification through operation of cybersecurity measures
- Issue identification through internal/external audits
- Issue identification through results of research/analysis of IT environmental change
- Issue identification through exercises and training

Outages
- Issue identification through CI services outage response

Government activities

Maintenance and promotion of the safety principles

Continual improvement of the safety principles (Secretariat/responsible ministries for critical infrastructure)

Survey on activities under safety principles (Cabinet Secretariat)

Continual improvement of guides for safety principles (Cabinet Secretariat/responsible ministries for critical infrastructure)

Information sharing

Information sharing between public-private stakeholders (Cabinet Secretariat/responsible ministries for critical infrastructure)

Incident response

- Cross-sectoral exercises (Cabinet Secretariat/responsible ministries for critical infrastructure)
- CEPTOAR communication training (Cabinet Secretariat/responsible ministries for critical infrastructure)
- Training by responsible ministries for critical infrastructure (Responsible ministries for critical infrastructure)

Risk management and preparation of incident readiness

Risk communication and consultation (Cabinet Secretariat/responsible ministries for critical infrastructure)

- Dissemination of risk assessment (Cabinet Secretariat/responsible ministries for critical infrastructure)
- Promotion of incident readiness (Cabinet Secretariat/responsible ministries for critical infrastructure)
- Promotion of monitoring and review (Responsible ministries for critical infrastructure)
- Investigation and analysis of new risk sources and risks, etc. (Responsible ministries for critical infrastructure)

Enhancement of basis for critical infrastructure protection

Review of the protection scope / Public relations / International cooperation / Promotion of security by design / Appeal to top management / Promotion of the developing human resources / maintenance of regulations (Cabinet Secretariat/responsible ministries for critical infrastructure)

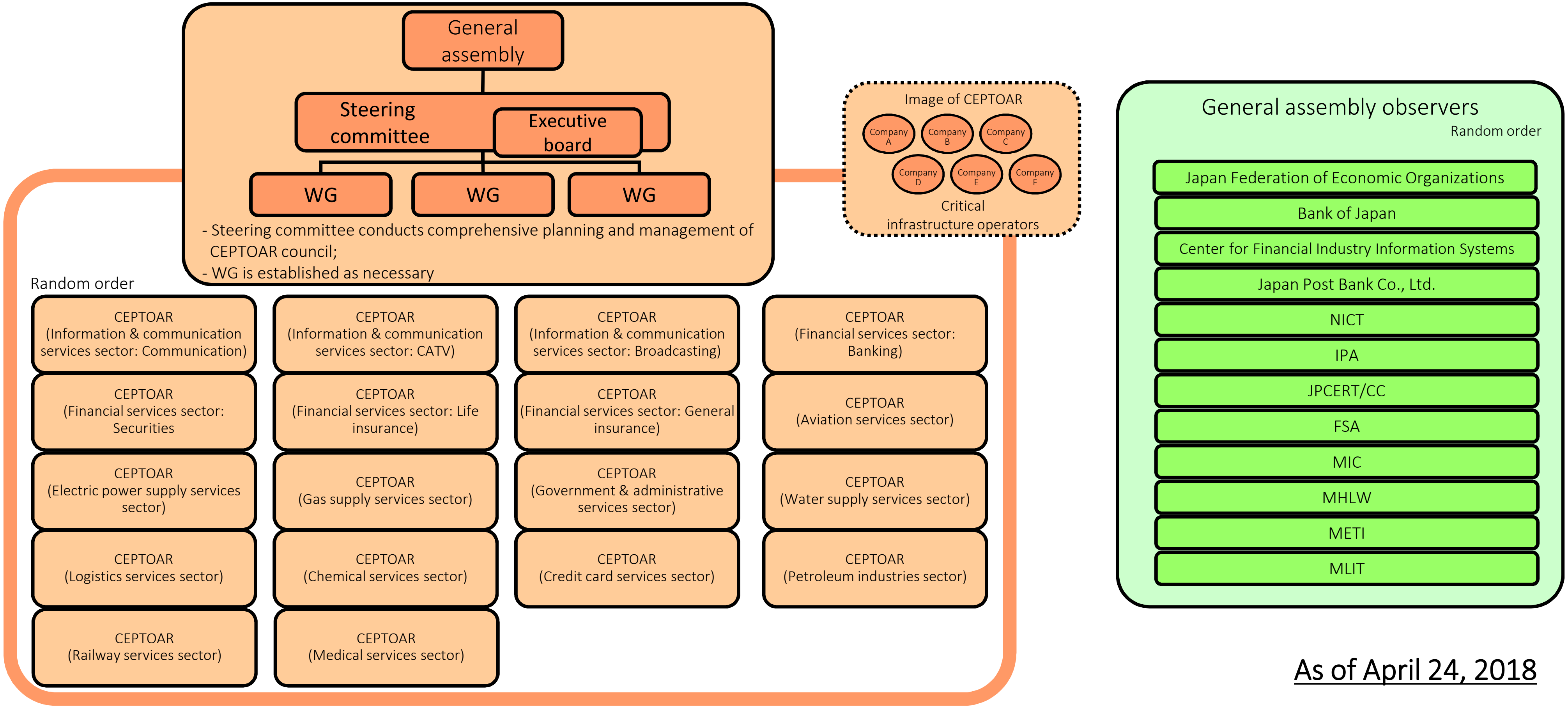
CEPTOAR and CEPTOAR Council

CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response

- Organization responsible for information sharing and analysis functions and relevant functions for critical infrastructure operators.
- For proactive prevention of CISs outages as well as prevention of the spread of damage, prompt recovery, and prevention of recurrence in the case of CISs outage, CEPTOARs appropriately provide information provided by the Government, etc. to critical infrastructure operators and share information with stakeholders. CEPTOARs hereby aim at activities that contribute to the improvement of the service maintenance and recovery capability of each critical infrastructure operator.

CEPTOAR council

- This is a council consisting of representatives from CEPTOARs developed in each critical infrastructure sector. It shares information between CEPTOARs. It is an independent meeting structure that is not positioned under any other organizations including government organizations.
- The council was founded on February 26, 2009, with the purpose of promoting cross-sectoral information sharing.



General assembly

Steering committee

Executive board

WG

WG

WG

- Steering committee conducts comprehensive planning and management of CEPTOAR council;
- WG is established as necessary

Image of CEPTOAR

Critical infrastructure operators

Random order

CEPTOAR (Information & communication services sector: Communication)

CEPTOAR (Information & communication services sector: CATV)

CEPTOAR (Information & communication services sector: Broadcasting)

CEPTOAR (Financial services sector: Banking)

CEPTOAR (Financial services sector: Securities)

CEPTOAR (Financial services sector: Life insurance)

CEPTOAR (Financial services sector: General insurance)

CEPTOAR (Aviation services sector)

CEPTOAR (Electric power supply services sector)

CEPTOAR (Gas supply services sector)

CEPTOAR (Government & administrative services sector)

CEPTOAR (Water supply services sector)

CEPTOAR (Logistics services sector)

CEPTOAR (Chemical services sector)

CEPTOAR (Credit card services sector)

CEPTOAR (Petroleum industries sector)

CEPTOAR (Railway services sector)

CEPTOAR (Medical services sector)

General assembly observers

Random order

- Japan Federation of Economic Organizations
- Bank of Japan
- Center for Financial Industry Information Systems
- Japan Post Bank Co., Ltd.
- NICT
- IPA
- JPCERT/CC
- FSA
- MIC
- MHLW
- METI
- MLIT

As of April 24, 2018

The list of CEPTOARs (14 sectors, 19 CEPTOARs)

As of July 25, 2018

■ CEPTOAR

CI Sectors	Information and communication			Financial				Aviation	Airport	Railway	Electric power supply	Gas supply	Government and administrative	Medical	Water	Logistics	Chemical	Credit card	Petroleum
Services	Electrical communication		Broadcasting	Banking	Securities	Life insurance	General insurance	Aviation	Airport	Railway	Electric power supply	Gas supply	Government and administrative	Medical	Water	Logistics	Chemical	Credit card	Petroleum
Name	T-CEPTOAR	Cable TV CEPTOAR	Broadcasting CEPTOAR	Financial service CEPTOAR Liaison Council				Aviation services CEPTOAR	Airport services CEPTOAR	Railway services CEPTOAR	Electric power supply services CEPTOAR	Gas supply services CEPTOAR	Local government	Medical services CEPTOAR	Water supply CEPTOAR	Logistics services CEPTOAR	Chemical industries CEPTOAR	Credit card services CEPTOAR	Petroleum industries CEPTOAR
				Banking services etc. CEPTOAR	Securities services CEPTOAR	Life insurance services CEPTOAR	General insurance services CEPTOAR												
Member	23 companies 1 community	335 companies 1 community	197 companies and community	1,411 companies	269 companies 7 organizations	41 companies	46 companies	14 companies 1 community	5 companies	22 companies 1 community	14 companies 3 organizations	10 companies and communities	47 states 1,741 local governments	1 group 9 organizations	8 business units	17 companies 6 communities	13 companies	51 companies	12 companies
Sharing Scope of info from NISC (Except member)	401 companies and communities	411 companies	12 companies	3 companies and communities							13 companies and organizations	170 companies and communities		381 companies and institutions	Spreading to 1341 business units as needed				
	Other (Nuclear material related office, building automation association, cyber defense Council, college)																		

Severity Schema on CISs Outages (draft version)

Summary

Considering that the affected area and incident response activities are different depending on the severity of Critical Infrastructure Services (CISs) outages and the importance of related information, aiming at enhancement of recognition sharing among stakeholders and quick decision making on incident response, Severity schema on CISs outages should be established and discussed in detail.

Purpose

1. To promote common understanding among stakeholders about the incident, objectivity and international coordination
2. To provide a standard for decision making concerning government activities on incident response
3. To provide a standard for structure and method of information sharing

Table 1: Severity Schema on CISs Outages (draft)

Severity	Definition
Level 5 Emergency	poses an imminent threat to wide-scale critical infrastructure services
Level 4 Severe	likely to result in a significant impact on critical infrastructure services
Level 3 High	likely to result in a demonstrable impact on critical infrastructure services
Level 2 Medium	may affect critical infrastructure services
Level 1 Low	unlikely to affect critical infrastructure services

(Source: The Cybersecurity Policy for CIP 4th edition)

Table 2: Draft version for discussion

Severity	Impact on People & Society	Impact on Systems	
		Emergency	24/365
Level 5 Emergency	poses an imminent significant threat to wide-range national life, etc.		
Level 4 Severe	likely to result in a significant impact on national life, etc.	Evaluate impact on safety and continuity of CISs	
Level 3 High	likely to result in a demonstrable impact on national life, etc.		Evaluate impact on provision of CISs
Level 2 Medium	may affect national life, etc.		
Level 1 Low	unlikely to affect national life, etc.		
Level 0 Baseline	will not affect national life, etc.		