Overview of Cybersecurity Policy for CIP

Promotion of critical infrastructure protection through public-private partnerships

- Achieve **safe and sustainable provision of critical infrastructure services** based on the concept of **mission assurance**
- Promote **public-private partnership activities** to **ensure cybersecurity of critical infrastructure.**

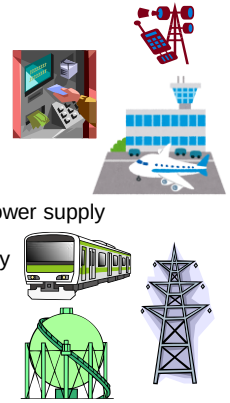
Comprehensive coordination by NISC

Responsible ministries for CIP

- Financial Services Agency
  [Finance]
- Ministry of Internal Affairs and Communications
  [Information and communication, Administration]
- Ministry of Health, Labour and Welfare
  [Medical, Water]
- Ministry of Economy, Trade and Industry
  [Electric power supply, Gas supply, Chemical inductries, Credit card, Petroleum industries]
- Ministry of Land, Infrastructure, Transport and Tourism
  [Aviation, Airport, Railway, Logistics]

Critical Infrastructure (14 sectors in total)

- Information & communication
- Finance
- Aviation
- Airport
- Railway
- Electric power supply
- Gas supply
- Government & administration
- Medical
- Water
- Logistics
- Chemical industries
- Credit card
- Petroleum industries



Related organizations, etc.

- Cybersecurity related ministries
  [Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, etc.]
- Crisis management ministries
  [National Police Agency, Ministry of Defense, etc.]
- Disaster prevention related ministries
  [Cabinet Office, ministries and agencies, etc.]
- Cybersecurity related agencies
  [NICT, IPA, JPCERT/CC, etc.]
- Cyberspace-related business entities
  [Vendors and others involved in the supply chain, etc.]

Main activities in the Cybersecurity Policy for CIP

Enhancement of Incident Response Capability

Promote the enhancement of incident response capability as part of the organizational governance so that the entire organization, including top management, CISO, strategic management, and system staff, etc. are involved in the activities.

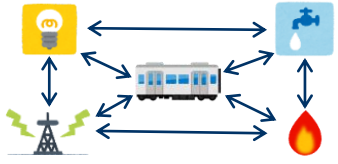
Maintenance and Promotion of the Safety Principles

Promote continuous improvement of guidelines for necessary cross-sectoral measures in critical infrastructure protection and safety principles, etc. in each sector.

Enhancement of Information Sharing System

Further enhance the public-private and internal-external sectorial information sharing system.

Utilization of Risk Management



Identify the characteristics of own organization and use risk management to ensure that appropriate protection measures are continuously implemented.

Enhancement of the Basis for CIP

Raise the overall level of cybersecurity by promoting cross-field exercises, international cooperation, and public relations and public information activities.

Executive Summary of Cybersecurity Policy for CIP

1. Purpose of CIP

Based on the concept of mission assurance, the purpose of CI protection (CIP) is to maintain safe and continuous provision of CISs by ensuring resilience and preventing serious impact on national life and socioeconomic activities from the dual aspects of below;

- Limit risk to acceptable levels taking the view that natural disasters, mismanagement, cyberattacks, and changes in the environment surrounding CI constitute risks that make the continuous provision of CISs uncertain.
- Take appropriate action in the event of outages and ensure rapid restoration of services in terms of preparing for CISs outages.

2. Responsibilities of stakeholders

- Responsibilities of stakeholders are based on the Basic Act on Cybersecurity (Act No. 104 of 2014).
- The national government is responsible for formulating and implementing comprehensive cybersecurity policies.
- Local governments bear the responsibility to formulate and implement independent cybersecurity policies.
- CI operators (excl. related entities) bear the responsibility to deepen their interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, in order to stably and properly provide its services.
- Cyberspace-related business entities and other business entities shall endeavor independently and actively to ensure cybersecurity in the course of their business activities.

3. Basic concept

- In response to the increasingly sophisticated and complex usage of systems and the rapidly increasing threats in cyberspace, CI operators will further promote organization-wide responses, involving top management, CISOs, strategic management, and system personnel. Particular measures will be taken towards promoting cybersecurity as an important priority for management.
- CI operators will clarify the specific characteristics of their organization and implement the most appropriate CIP policies by utilizing risk management that organically combines the perspectives of all organizational levels, from top management through to system personnel.
- In order to respond precisely to changes to threats relating to CI, a comprehensive response is implemented capable of anticipating future changes in the environment, including in the supply chain, etc.

4. Enhancement of incident response capability

- Enhance incident response capability through a combination of preemptive risk management and crisis management.
- Clarify the relationship between top management and experts for ensuring organizational cybersecurity.
- Based on the definition stipulated in Article 2 of the Basic Act on Cybersecurity, to ensure cybersecurity develop and operate an incident response system capable of responding not only to external attacks, but also to events related to system procurement, design, and operation.

Policy Group (1): Enhancement of Incident Response Capability

Critical infrastructure operators, etc. will promote the enhancement of their incident response capabilities through close mutual cooperation between the public and private sectors, after making their organization-wide efforts to ensure cybersecurity.

Key points of activities

- ✓ Development of incident response capability as part of the organizational governance
- ✓ Comprehensive response, including supply chain

Activities during this Cybersecurity Policy term

(1) Incident response capability as part of organizational governance

- Promote the enhancement of incident response capability of the entire organization, including top management, CISO, strategic management, and system personnel, etc., and operators involved in the supply chain, etc.

(2) Activities to enhance incident response capability

- Promote effective activities for BCP/IT-BCP, CSIRT, audit system, etc. to enhance the incident response capability

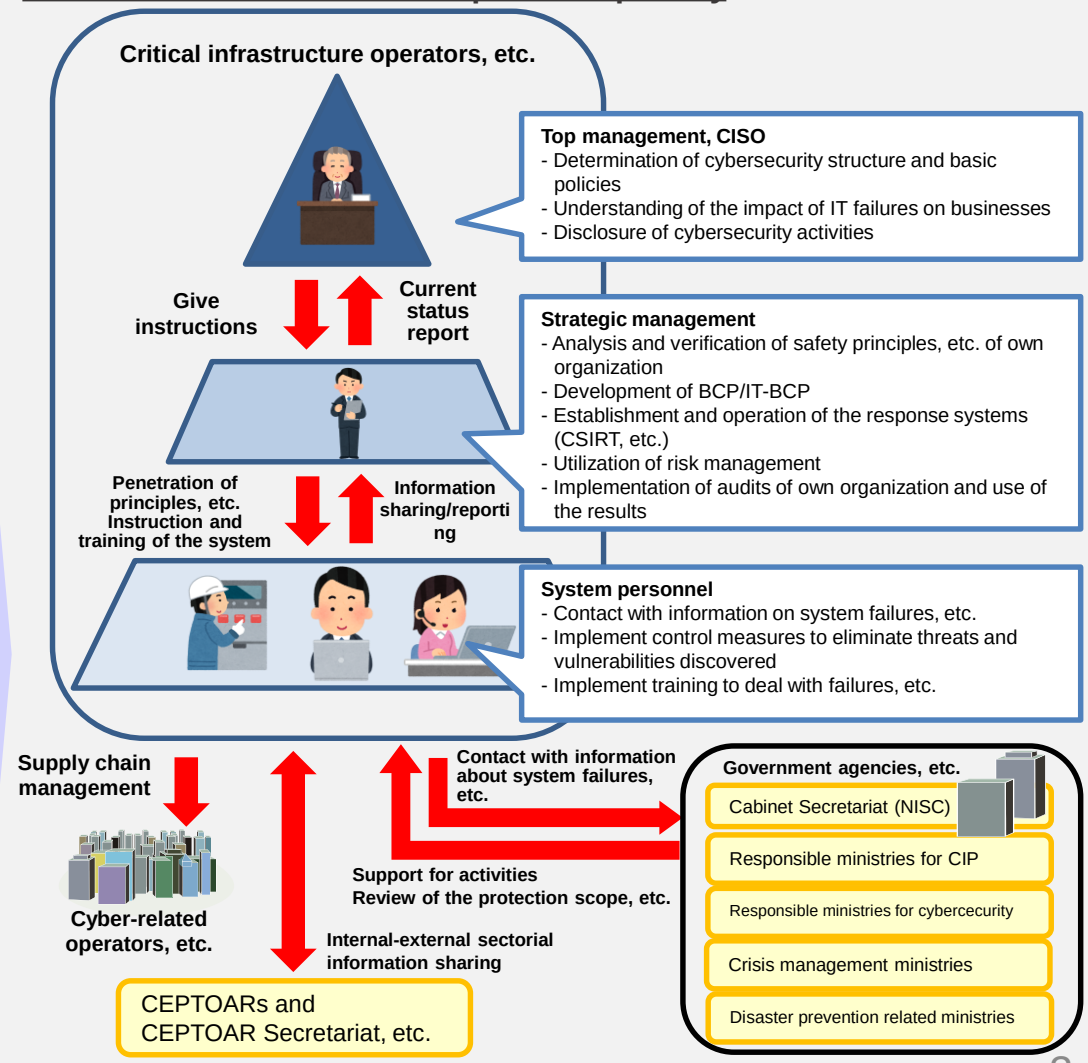
(3) Integrated public-private efforts to enhance incident response capability

- Consider integrated public-private efforts with close mutual cooperation between the government and critical infrastructure operators, etc.

(4) Review of the protection scope of CI

- Ensure "protection as plane" including the supply chain and from a security perspective in order to respond to changes in the environment

Enhancement of Incident Response Capability



Policy Group (2): Maintenance and Promotion of the Safety Principles

In order to implement the most appropriate protection measures for own organizations, promote activities for the maintenance and promotion of the "safety principles, etc." by the stakeholders such as critical infrastructure operators.

* Safety principles, etc.: General term for relevant laws, industry standards/guidelines, internal regulations, etc.

Key points of activities

- ✓ Develop safety principles, etc. appropriate to own organization, adapting to social trends and changes in the surrounding environment.
- ✓ Make continuous improvement of safety principles, etc. through risk assessment by audits, exercises, etc.

Activities during this Cybersecurity Policy term

(1) Continual improvement of the Guidelines for Safety Principles

- Enhance measures to **incorporate cybersecurity as part of organizational governance** and develop principles for supply chain
- Develop principles for continuous improvement optimized to own organization

(2) Continuous improvement of the safety principles

- Continuous improvement of safety principles, etc. through **risk assessment** by **internal and external audits**, participation in exercises, etc.
- Survey on the status of improvement of safety principles, etc. by responsible ministries for CIP

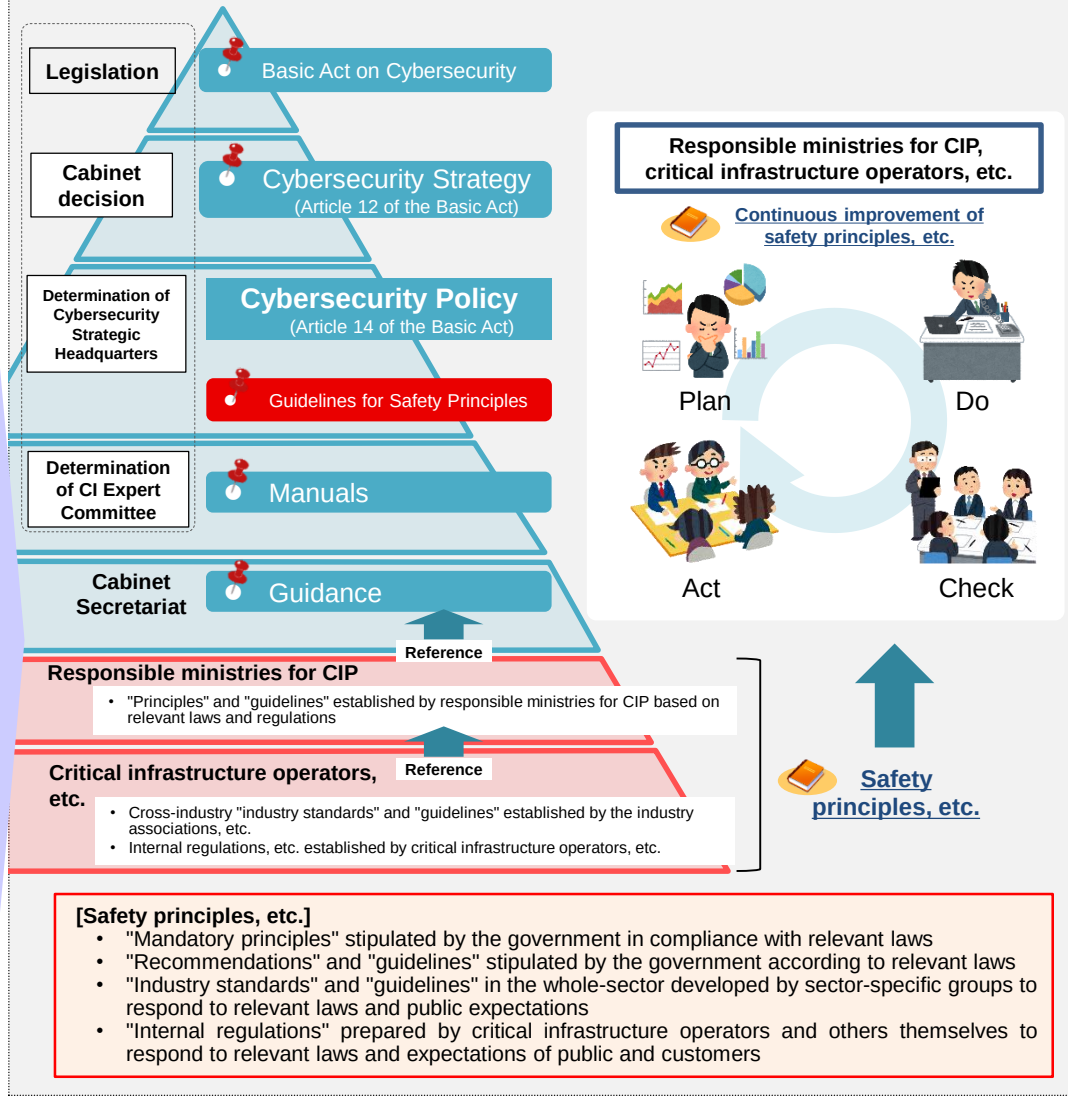
(3) Penetration of the safety principles

- Survey to ascertain the actual status of activities to ensure cybersecurity by the critical infrastructure operators, etc.

(4) Clarification of documentation relating to the safety principles

- Listing of documents and clarification of relationships between documents to promote understanding of the Guidelines for Safety Principles, safety principles, etc.

Continuous improvement of Safety Principles, etc.



[Safety principles, etc.]

- "Mandatory principles" stipulated by the government in compliance with relevant laws
- "Recommendations" and "guidelines" stipulated by the government according to relevant laws
- "Industry standards" and "guidelines" in the whole-sector developed by sector-specific groups to respond to relevant laws and public expectations
- "Internal regulations" prepared by critical infrastructure operators and others themselves to respond to relevant laws and expectations of public and customers

Policy Group (3): Enhancement of Information Sharing System

Work to enhance public-private and internal-external sectoral information sharing systems further so that individual critical infrastructure operators, etc. can respond to cybersecurity trends that change on a daily basis.

Key points of activities

- ✓ Develop and disseminate the information sharing systems built under the previous policies.
- ✓ Activate voluntary efforts by critical infrastructure operators, etc.

Activities during this Cybersecurity Policy term

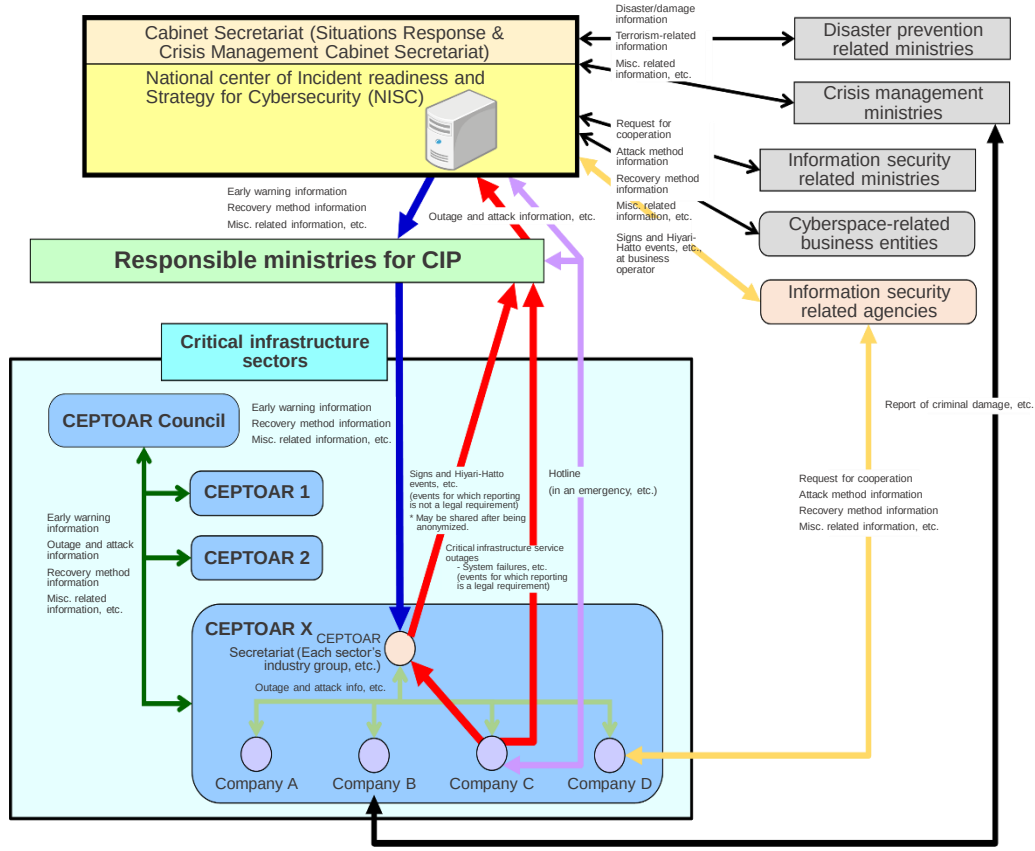
(1) Further promotion of information sharing

- Proactive utilization for risk management of shared information
- Aggregation, analysis and sharing of information related to critical infrastructure service outages and threat and vulnerability information
- Clarification of what information should be shared (Clarify that not only information systems but also control systems and IoT systems should be covered, and so on.)
- Timely and appropriate review in the event of environmental changes, etc.

(2) Promotion of CI operators' activities

- Establishment and enhancement of the incident response capability under the leadership of top management
- Further enhancement of information sharing within and between CEPTOARs
- Promotion of participation in ISACs and information sharing among ISACs
- Implementation of CEPTOAR training in a more realistic manner

Information Sharing Systems in the Critical Infrastructure



Policy Group (4): Utilization of Risk Management

Aiming to ensure resilience in the continual provision of critical infrastructure services, promote continuous efforts in repeated PDCA cycles of protection measures optimized to individual organizations.

Key points of activities

- ✓ Realization of protection measures optimized to individual organizations
- ✓ Identification of new risks and risk sources due to environmental changes
- ✓ Analysis of interdependency among critical infrastructure sectors

Activities during this Cybersecurity Policy term

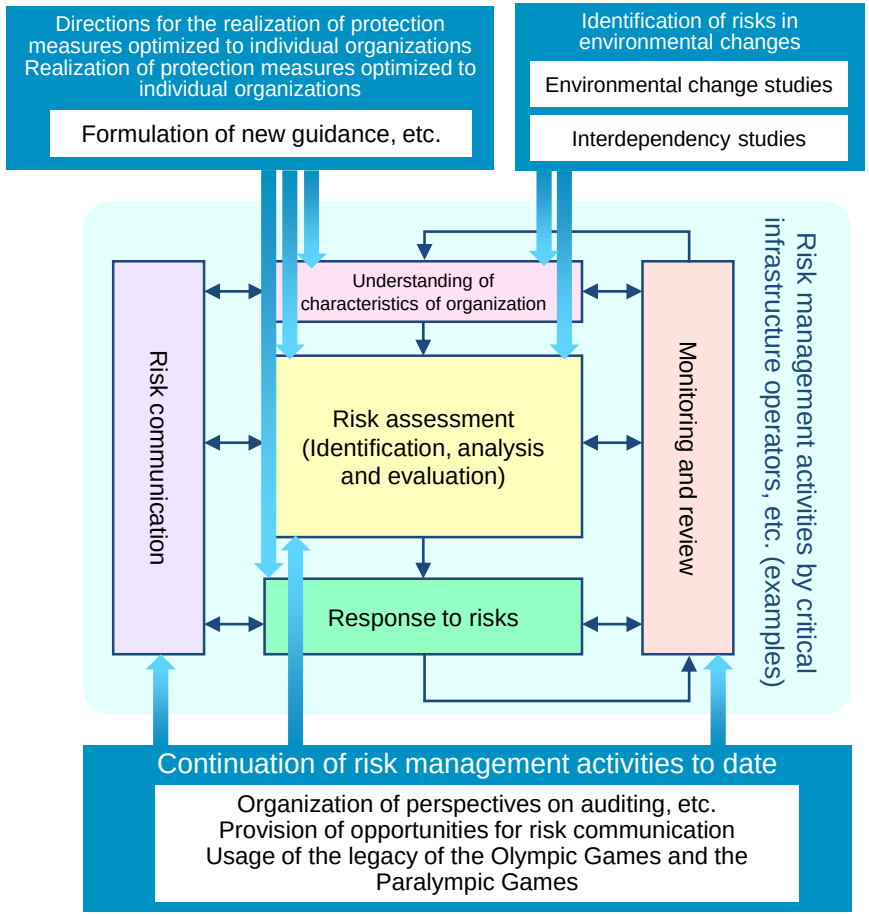
(1) Promotion of risk management

- Clarification of the profile of own organization and promotion of efforts to realize protection measures optimized to individual organizations
- Review of the effective measures and usage of existing principles, review of manuals and development of new guidance, etc.

(2) Studies and analysis of risks

- Implementation of environmental change studies to address risks due to the transformation of cyberspace as a result of the advancement of DX with digitalization, etc.
- Implementation of interdependency studies of which other critical infrastructure sectors would be affected in the event of a critical infrastructure service outage

Utilization of Risk Management



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

In order to strengthen the basis for CIP, promote activities which support the entirety of the policy, such as verification of the effectiveness of the incident response capability, human resources development, cooperation with related agencies, international cooperation, public relations activities.

Key points of activities

- ✓ Implementation of effectiveness verification of incident response capability
- ✓ Development of human resources not only in the IT sector but also in a wide range of other sectors
- ✓ Information dissemination through effective PR channels, etc.

Activities during this Cybersecurity Policy term

(1) Verification of effectiveness of incident response capability
- Verification of incident response capability through cross-sectoral exercise
- Improvement of incident response capability by using the issues from the exercise

(2) Promotion of the development of human resources
- Develop strategic management personnel to work closely with top management
- Raise awareness throughout the organization, not just in the IT department

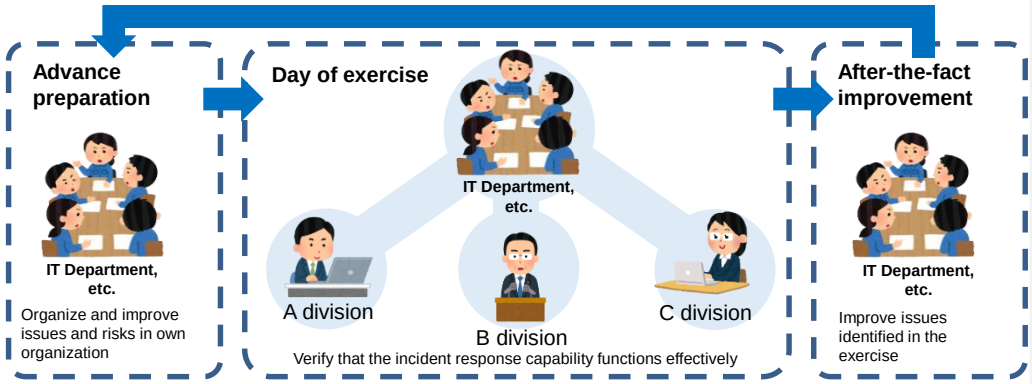
(3) Promotion of international cooperation
- Promote diversified and multilateral international cooperation by using various frameworks between the government and businesses

(4) Strengthening of cooperation with the National PoliceAgency and the Digital Agency
- Promote overall security by raising awareness of cybercrime and new technologies associated with DX

(5) Promotion of public relations activities
- Making the framework and activities of the policies easy to understand for the public
- Maintenance of relevant documents and standards

Activities for the Enhancement of Basis for Critical Infrastructure Protection

Verification of effectiveness of incident response capability



Development of Human resources.

- Develop strategic management
- Raise awareness throughout the organization

International cooperation

ASEAN

MERIDIAN Connecting and Protecting

Cooperation between two countries and regions and among countries

Strengthening of cooperation with the National Police Agency and the Digital Agency

警察庁 National Police Agency

デジタル庁

- Reporting cybercrimes to the police, etc.
- Securing of cyberspace security through raising the awareness for new technologies associated with DX

Public relations activities

Dissemination through website, social media, newsletter, lectures, etc.

“Critical Infrastructure Operator Measure Examples” and “Government Activities”

Understanding of the responsibilities of stakeholders under the Basic Act on Cybersecurity

Critical infrastructure operator measure examples

Plan
Identification and prevention

Policy
- Positioning cybersecurity as management priority
- Determination and revision of operator’s basic policy
- Utilization of risk management
  ・Clarification of organizational profile ・Analyze differences between requirements and actual situation・ Identify items for improvement・ Consider and set priorities for prevention measures

Resource management
- Development of monitoring, information sharing and CSIRT structures, etc.
- Securing of budget / personnel
- Human Resource development / assignment, and accumulation of know-how
- Measures for outsourcing

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

Planning
- Establishment / revision of roadmap for cybersecurity
- Establishment / revision of plan for cybersecurity

Establishment
- Design/implementation/maintenance related to technological measures for cybersecurity
- Design/procedure manual creation/maintenance related to operational cybersecurity measures

Do
Detection and recovery

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

Normal circumstances
- Operation of cybersecurity measures (recognizing attack trends, etc.)
- Public announcement of the status of cybersecurity measures

Outages
- Protection/recovery from CISs outages
- Execution of BCP / contingency plans,etc.
- Public announcement of the status of measures to respond to CISs outages

Check / 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 environmental changes
- Issue identification through exercises and training

Outages
- Issue identification through CISs outage responses (detection and recovery)

Government activities

Enhancement of incident response capabilities
- Promotion of incident response capabilities as part of organizational governance / Support for formulation of BCPs, CSIRT operation and audits at operators (Cabinet Secretariat/ Responsible ministries for CIIP)
- Integrated public-private efforts to enhance incident response capabilities (Cabinet Secretariat/ Responsible ministries for CIIP / Crisis management ministries, etc.)

Maintenance and promotion of the safety principles
- Continual improvement of the safety principles (Cabinet Secretariat/ Responsible ministries for CIIP)
- Promotion of the safety principles (Cabinet Secretariat/ Responsible ministries for CIIP)
- Continual improvement of the Guidelines for Safety Principles (Cabinet Secretariat/ Responsible ministries for CIIP)

Enhancement of information sharing
- Information sharing among public-private stakeholders (Cabinet Secretariat/ Responsible ministries for CIIP)
- CEPTOAR exercises (Cabinet Secretariat/ Responsible ministries for CIIP)

Utilization of risk management
- Realization of protection measures optimized for individual organizations / promotion of risk communication (Cabinet Secretariat/ Responsible ministries for CIIP)
- Dissemination of risk assessment (Cabinet Secretariat/ Responsible ministries for CIIP)
- Awareness of risks arising due to environmental change (Cabinet Secretariat/ Responsible ministries for CIIP)

Enhancement of basis for CIIP
- Promotion of the developing of human resources, etc. / Promotion of security by design / International cooperation / Cooperation with Digital Agency / Public relations (Cabinet Secretariat/ Responsible ministries for CIIP)
- Verifying effectiveness of incident response capabilities (Cabinet Secretariat/ Responsible ministries for CIIP)
- Exercises run by responsible ministries for CIIP (Responsible ministries for CIIP) ）

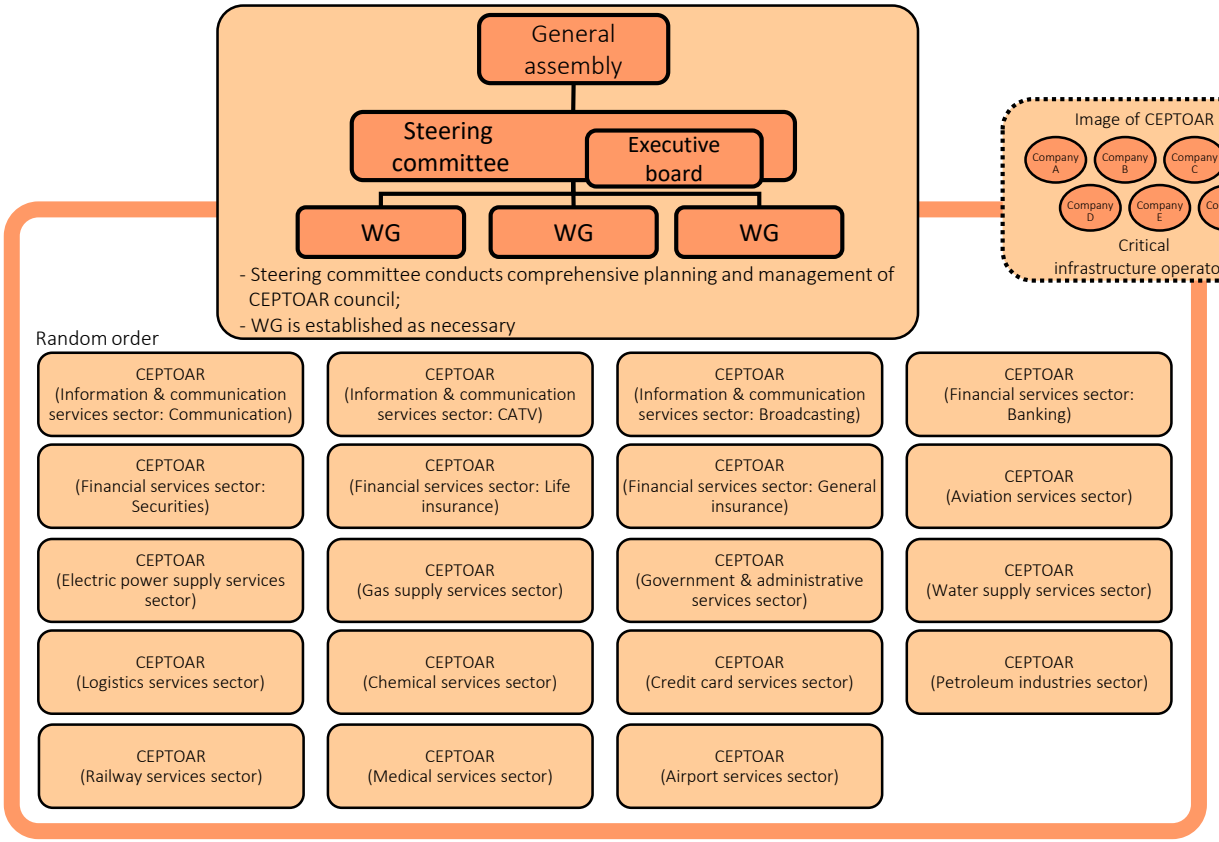
CEPTOAR and CEPTOAR Council

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.



As of September 30, 2022

The list of CEPTOARs

As of September 30, 2022

■ 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	Telecommunication		Broadcasting	Banking	Securities	Life insurance	General insurance	Payment	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	Payment services CEPTOAR												
Member	**28** companies **1** community	**310** companies **1** community	**194** companies **2** communities	**1,285** companies	**282** companies **7** organizations	**42** companies	**47** companies	**217** companies	**14** companies **1** community	**8** companies	**22** companies **1** community	**24** companies **4** organizations	**12** companies **1** community	**47** States **1,741** local governments	**1** group **21** organizations	**8** business units	**17** companies **6** communities	**13** companies	**51** companies	**11** companies
Sharing Scope of info from NISC (Except member)	**412** companies and communities	**340** companies	**11** companies	**2** companies and communities	—	—	—	**9** companies	—	—	—	**15** companies and organizations	**196** companies and communities	—	**391** companies and institutions	Spreading to **1,324** business units as needed	—	—	—	—
	Other (Nuclear material related office, building automation association, cyber defense Council, college)																			