NISC

National center of Incident readiness and
Strategy for Cybersecurity

Cybersecurity Strategy in Japan

- Present Situation and Challenges -

July 4, 2019
Tomoo YAMAUCHI
Deputy Director-General
NISC, Cabinet Secretariat

Japan’s Cybersecurity Framework and NISC

- The **Basic Act on Cybersecurity** provides:
  - Definition of “Cybersecurity” in legal context
  - Position of Cybersecurity Strategy
  - Authority and mandate of **Cybersecurity Strategic HQ**, which consists of Ministers and notable experts
- As the secretariat of Cybersecurity HQ, **NISC** (Cabinet Secretariat) works for the HQ’s mandate such as:
  - Integrating and advancing cybersecurity policies crossing over governmental bodies
    - **Cybersecurity Strategy**
    - Cybersecurity Policy for Critical Infrastructure Protection
    - Common Standard on Information Security Measures of Government Entities
    - Cybersecurity HRD Plan
    - Cybersecurity R&D Strategy etc.
  - Monitoring, analyzing, and handling cyber attacks to governmental bodies on 24/7 basis as a governmental CSIRT
  - Assisting governmental bodies in case of severe cyber incidents with CYMAT

Cybersecurity Strategic Headquarters

Cabinet

Prime Minister

IT Strategic Headquarters

IT Strategic Headquarters swiftly and thoroughly introduces the measures for the formation of an advanced information and telecommunications network society.

Cooperation

Cybersecurity Strategic Headquarters

Established in accordance with the Basic Act on Cybersecurity, 9 January, 2015

Chair:	Chief Cabinet Secretary
Deputy Chair:	Minister in charge of the Tokyo Olympic and Paralympic Games
Members:	Chairman of the National Public Safety Commission
	Minister for Internal Affairs and Communications
	Minister for Foreign Affairs
	Minister of Economy, Trade and Industry
	Minister of Defense
	Minister in charge of Information Technology Policy
	Experts (8 persons)

- Critical Infrastructure Expert Panel
- Technological Strategy Expert Panel
- Human Resources Expert Panel for Dissemination and Enlightenment
- Cybersecurity Measures Promotion committee

Cooperation

National Security Council（NSC）

NSC deliberates on important issues regarding national defense.

(Secretariat)

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

Established by Cabinet Order, 9 January, 2015

Director-General
(Assistant CCS (Sit. Response and crisis mgt.))
(Secretary General of NSS)

･Deputy Director-General ･Cybersecurity Assistant

- Government Security Operation Coordination team（GSOC）
- Cyber Incident Mobile Assistant Team **(CYMAT)**

Government organizations (Ministries, IAAs, Designated Special Corporations)

Competent Ministries of Critical Infrastructures

Financial Services Agency
【bank, security, insurance】
Ministry of Internal Affairs and Communications
【local governments, infor. and comm.】
Ministry of Health, Labour and Welfare
【medical service, water supply】
Ministry of Economy, Trade and Industry
【electricity, gas, chemistry, credit card, petroleum 】
Ministry of Land, Infra., Transport and Tourism
【railway, aviation, logistics】

Cooperation

Critical infrastructure businesses, etc.

Ministries under HQ Members

- National Police Agency
- Ministry of Internal Affairs and Communications
- Ministry of Foreign Affairs
- Ministry of Economy, Trade and Industry
- Ministry of Defense

Cooperation

Companies

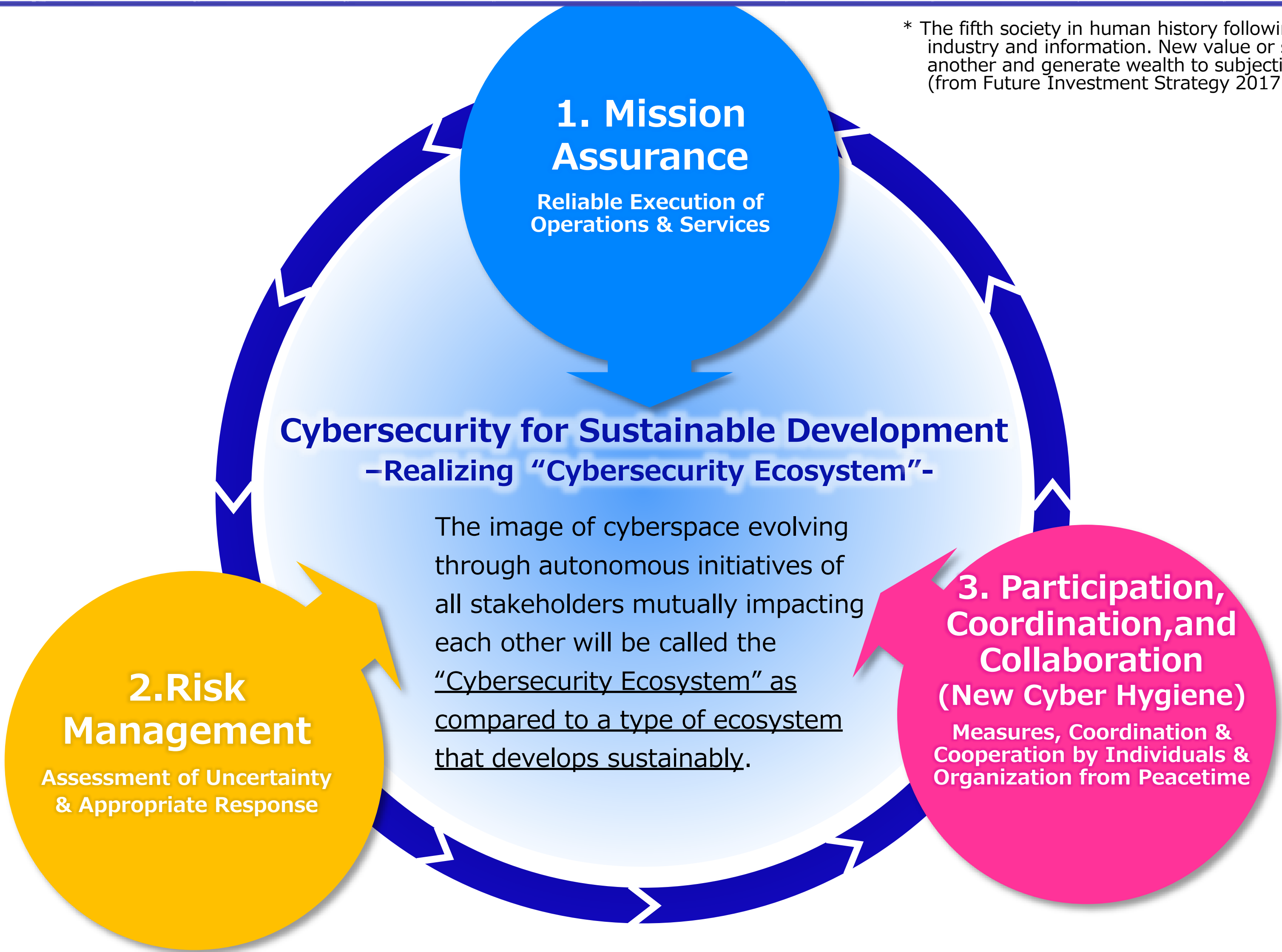
Individuals

Basic Vision and Approaches for Cybersecurity

○ Aims for sustainable development of cyberspace to realize a new-generation society(Society5.0*).

○ Adhering to its basic position presented in the Strategy 2015 and promoting initiatives based on 3 approaches.

* The fifth society in human history following hunting, agriculture, industry and information. New value or service emerge one after another and generate wealth to subjective people of the society (from Future Investment Strategy 2017)



1. Mission Assurance

Reliable Execution of Operations & Services

2.Risk Management

Assessment of Uncertainty & Appropriate Response

3. Participation, Coordination,and Collaboration (New Cyber Hygiene)

Measures, Coordination & Cooperation by Individuals & Organization from Peacetime

Cybersecurity for Sustainable Development

–Realizing "Cybersecurity Ecosystem"-

The image of cyberspace evolving through autonomous initiatives of all stakeholders mutually impacting each other will be called the "Cybersecurity Ecosystem" as compared to a type of ecosystem that develops sustainably.

Summary of the Cybersecurity Strategy (July 28, 2018 Cabinet Decision)

◆ Basic position and vision on Cybersecurity, and objectives and implementation policies in next 3 years (2018~2021) .

1 Introduction

- An unprecedented paradigm shift by cyberspace (Society5.0)
- Increasing seriousness of threats with cyberspace and real space unification

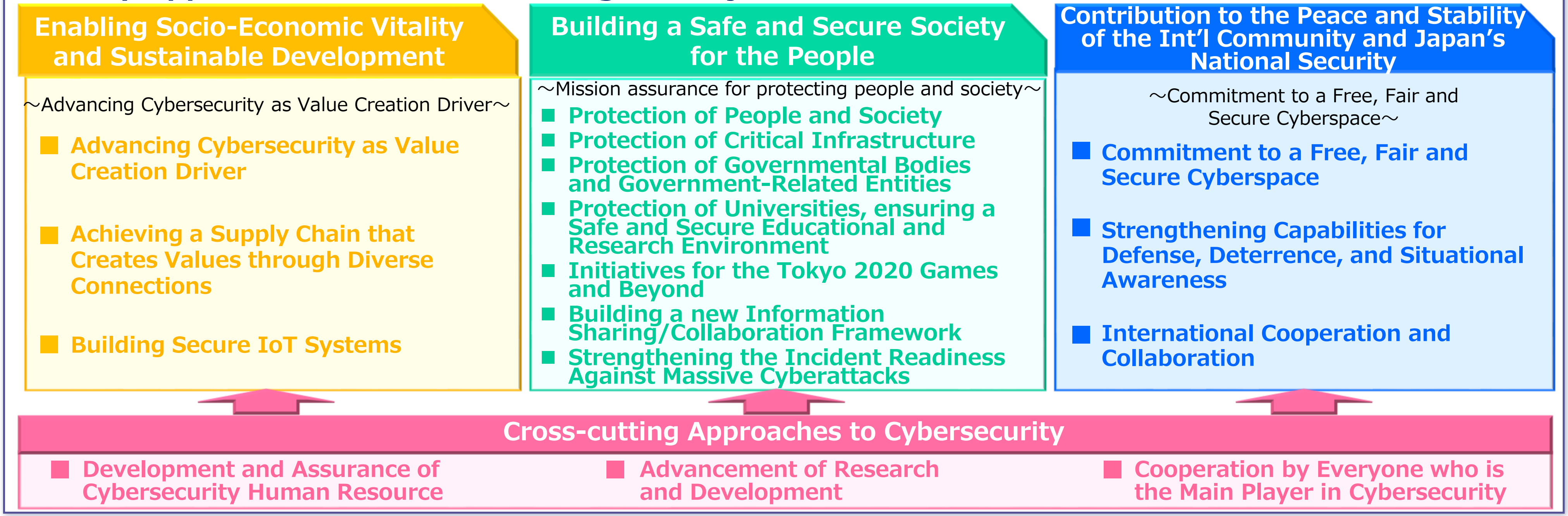
2 Understanding on Cyberspace

- Knowledge/technologies/services in cyberspace bringing about abundance.
- Risk - loss of the ability to control system/service.
  Attacks - socio-economic losses increasing exponentially.

3 Visions and Objective of this Strategy

- Adherence to the Basic Position on Cybersecurity (“free, fair and secure cyberspace”)
- Basic Vision (Promotion of “Cybersecurity Ecosystem”); Three Approaches

4 Policy Approaches towards Achieving the Objective



Enabling Socio-Economic Vitality and Sustainable Development

～Advancing Cybersecurity as Value Creation Driver～

- ■ Advancing Cybersecurity as Value Creation Driver
- ■ Achieving a Supply Chain that Creates Values through Diverse Connections
- ■ Building Secure IoT Systems

Building a Safe and Secure Society for the People

～Mission assurance for protecting people and society～

- ■ Protection of People and Society
- ■ Protection of Critical Infrastructure
- ■ Protection of Governmental Bodies and Government-Related Entities
- ■ Protection of Universities, ensuring a Safe and Secure Educational and Research Environment
- ■ Initiatives for the Tokyo 2020 Games and Beyond
- ■ Building a new Information Sharing/Collaboration Framework
- ■ Strengthening the Incident Readiness Against Massive Cyberattacks

Contribution to the Peace and Stability of the Int’l Community and Japan’s National Security

～Commitment to a Free, Fair and Secure Cyberspace～

- ■ Commitment to a Free, Fair and Secure Cyberspace
- ■ Strengthening Capabilities for Defense, Deterrence, and Situational Awareness
- ■ International Cooperation and Collaboration

Cross-cutting Approaches to Cybersecurity

- ■ Development and Assurance of Cybersecurity Human Resource
- ■ Advancement of Research and Development
- ■ Cooperation by Everyone who is the Main Player in Cybersecurity

5 Promotion and Implementation of Cybersecurity

- ● Government bodies keep working on improving their capabilities under the leadership of NISC
- ● NISC plays its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships among stakeholders.

Establishment of the Cybersecurity Council

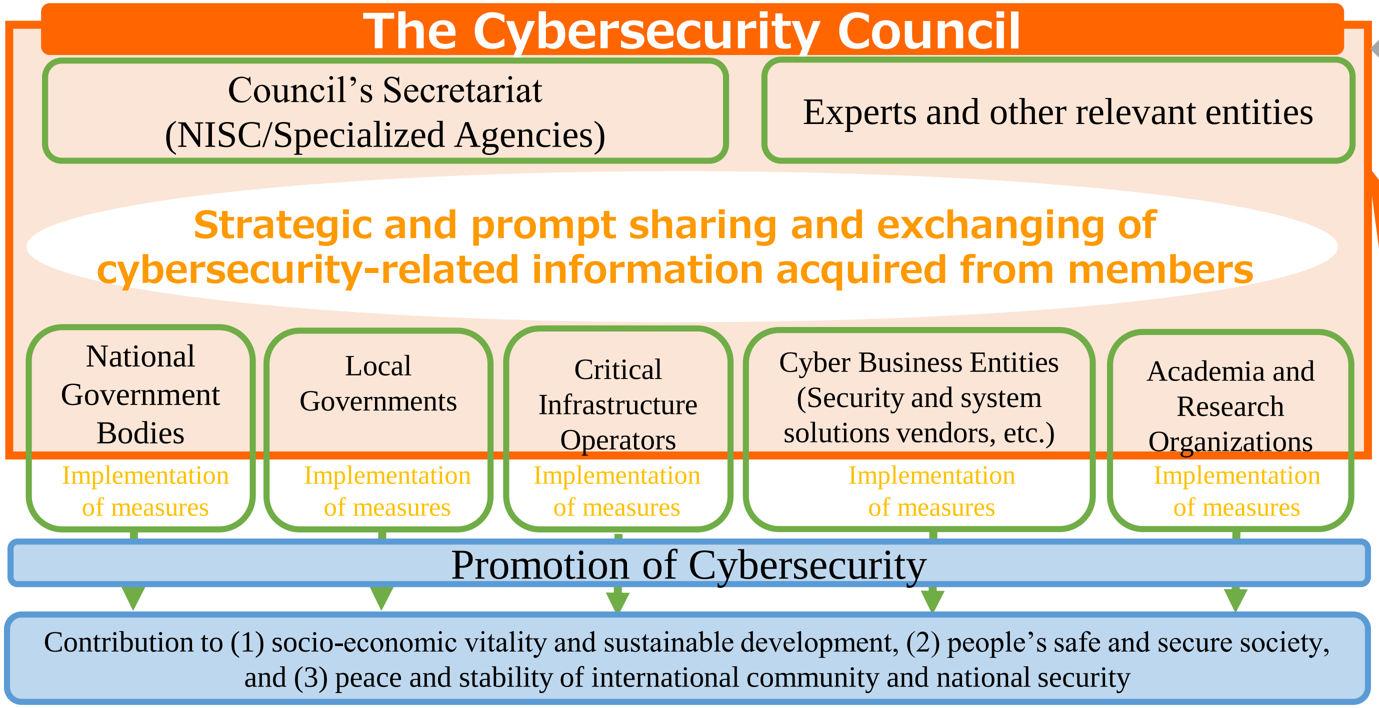
NISC

Second Amendment of the Basic Act on Cybersecurity was enacted on December 2018.

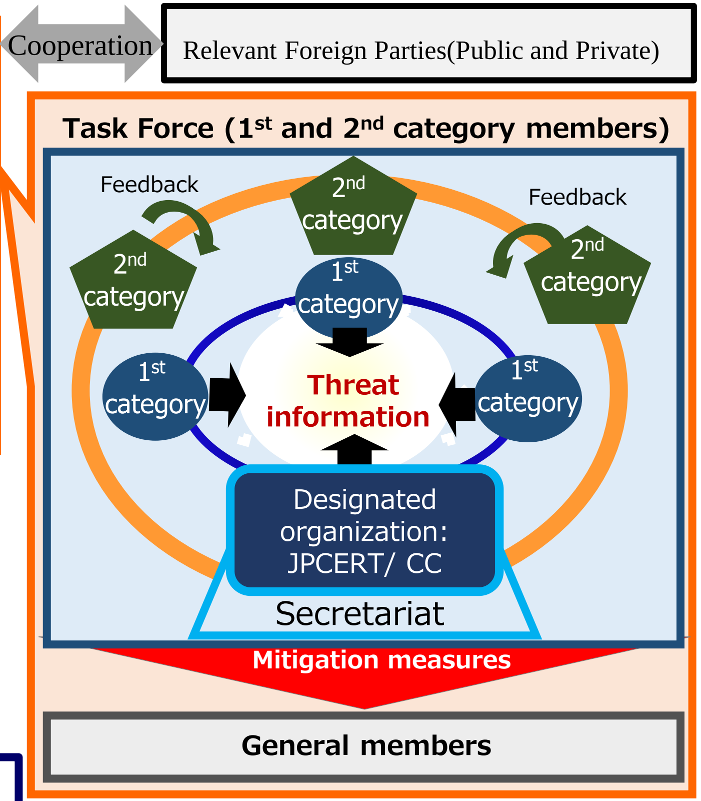
Overview

※ Effective on April 1,2019

- The Cybersecurity Council was established to enhance the discussion among relevant stakeholders in public and private sector to promote cybersecurity.
- The Act imposes **obligation** on **confidentiality** and **information sharing** against members of the Cybersecurity Council.



The Cybersecurity Council
Council's Secretariat (NISC/Specialized Agencies)
Experts and other relevant entities
Strategic and prompt sharing and exchanging of cybersecurity-related information acquired from members
National Government Bodies
Implementation of measures
Local Governments
Implementation of measures
Critical Infrastructure Operators
Implementation of measures
Cyber Business Entities (Security and system solutions vendors, etc.)
Implementation of measures
Academia and Research Organizations
Implementation of measures
Promotion of Cybersecurity
Contribution to (1) socio-economic vitality and sustainable development, (2) people's safe and secure society, and (3) peace and stability of international community and national security

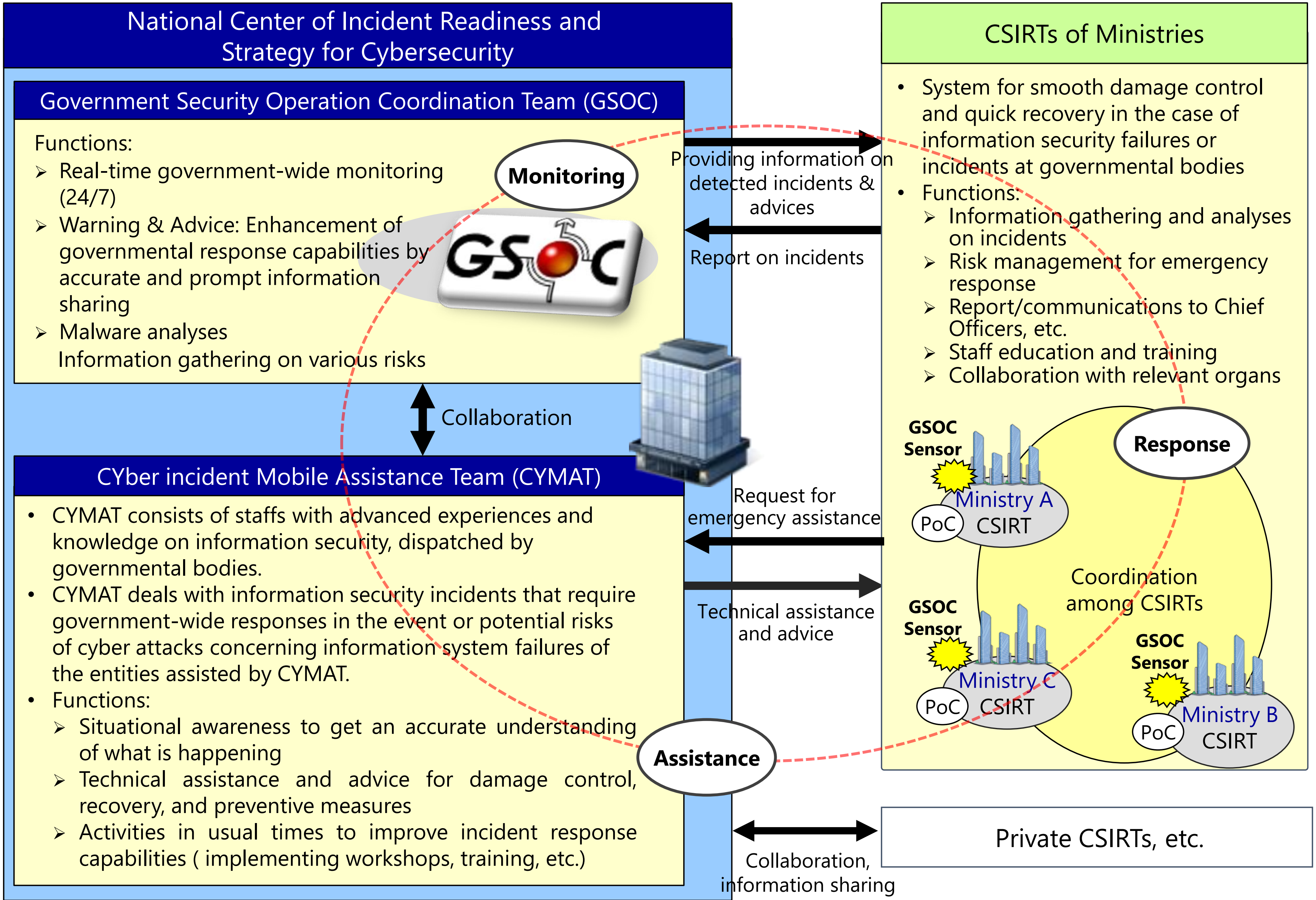


- ✓ 1st category members (specialized agencies and security vendors) cross-check threat information
- ✓ 2nd category members give feedback to 1st category members
- ✓ Mitigation measures are provided to general members

Operational rules of the Cybersecurity Council

Back Ground	・Need to enhance information sharing in addition to removing barrier information sharing through amendment of the act
Solution	・Establishing a Task Force (TF) composed of members who have ability and willingness for active information sharing
Merit to be a Task Force member	・Increasing accuracy of threat information through the cross-check and feedback among members ・Enabling TF members to obtain information shared only within the TF by ensuring give-and-take principle

Cybersecurity Operation for Government Organizations



National Center of Incident Readiness and Strategy for Cybersecurity

Government Security Operation Coordination Team (GSOC)

Functions:

- ➢ Real-time government-wide monitoring (24/7)
- ➢ Warning & Advice: Enhancement of governmental response capabilities by accurate and prompt information sharing
- ➢ Malware analyses

Information gathering on various risks

Collaboration

CYber incident Mobile Assistance Team (CYMAT)

- CYMAT consists of staffs with advanced experiences and knowledge on information security, dispatched by governmental bodies.
- CYMAT deals with information security incidents that require government-wide responses in the event or potential risks of cyber attacks concerning information system failures of the entities assisted by CYMAT.
- Functions:
  - ➢ Situational awareness to get an accurate understanding of what is happening
  - ➢ Technical assistance and advice for damage control, recovery, and preventive measures
  - ➢ Activities in usual times to improve incident response capabilities (implementing workshops, training, etc.)

Providing information on detected incidents & advices

Report on incidents

Request for emergency assistance

Technical assistance and advice

Collaboration, information sharing

CSIRTs of Ministries

- System for smooth damage control and quick recovery in the case of information security failures or incidents at governmental bodies
- Functions:
  - ➢ Information gathering and analyses on incidents
  - ➢ Risk management for emergency response
  - ➢ Report/communications to Chief Officers, etc.
  - ➢ Staff education and training
  - ➢ Collaboration with relevant organs

Private CSIRTs, etc.

Overview of Interagency Agreement for Government Procurement of IT system, Equipment, and Services and Procurement Procedure

1．Scope

The IT system, equipment, and services judged to fall into following categories by each ministry through the consultation with NISC and National Strategy Office of IT

a. The system that deals with information regarding national security and public safety

b. The system treating confidential information or sensitive information, the breach of which causes social or economic loss

c. The system dealing with a large volume of personal information such as social security number

d. The foundation system such as LAN, the disruption of which causes serious effect on the ministry’s operation

e. The system with high running cost

2．Effectuation

From April 1st 2019

3．Procurement Process

Above systems will be procured through the process such as comprehensive scoring auction which takes various factors into consideration as well as price. Each ministry should obtain necessary information by issuing RFI (Request for Information) or RFP (Request for Proposal).

4．Advice by NISC and National Strategy Office of IT

Each ministry should consult with NISC and National Strategy Office of IT about appropriate measures to ensure cybersecurity of its system through the procurement process.

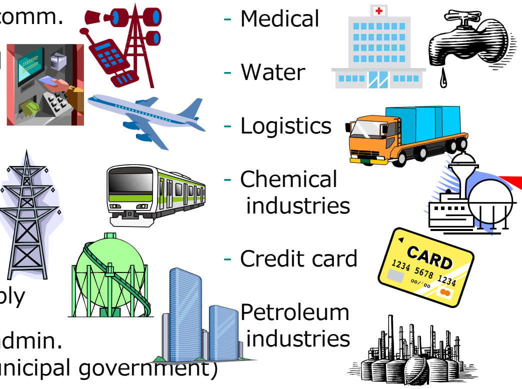
Critical Infrastructure Protection

Basic Policy of CIP (4th Edition)

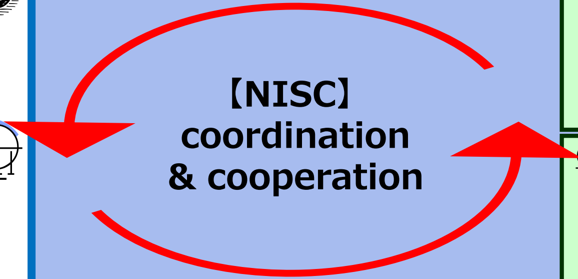
Promoting CIP through public-private partnership

On the basis of the concept of mission assurance, in order to safely and continuously provide critical infrastructure services 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 (13 sectors)



- Info. & comm.
- Financial
- Aviation
- 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 protection (5 ministries)

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

Organizations concerned

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

This Basic 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 CII operators, etc.

Enhancement of the basis for CIIP

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