NISC National center of Incident readiness and Strategy for Cybersecurity

Cybersecurity Law, Strategy, and Policy in Japan

September 2016

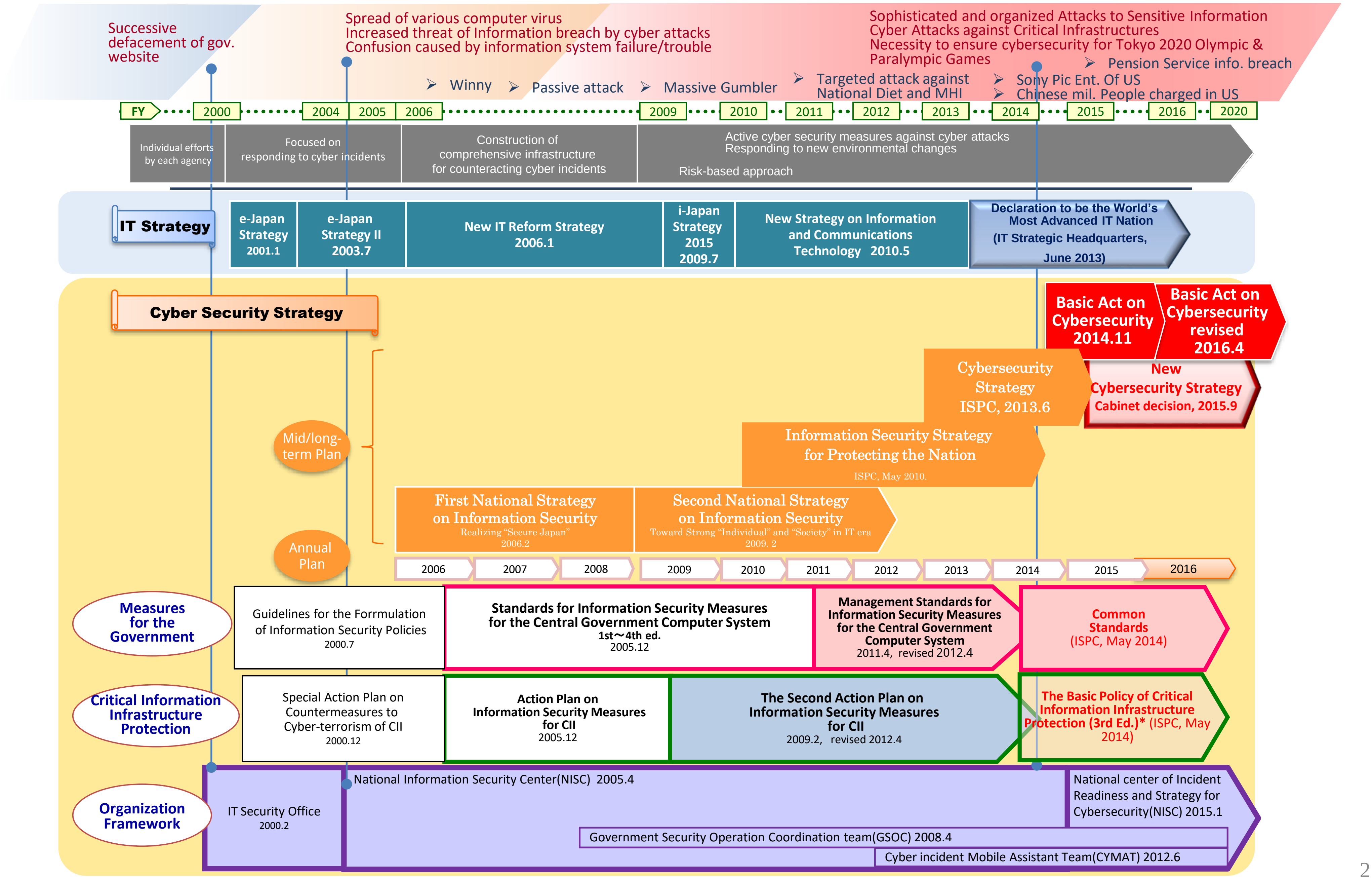
Masanori Sasaki

Deputy Counsellor
National center of Incident readiness and Strategy for Cybersecurity (NISC)
Cabinet Secretariat, Government of JAPAN

Legal & Policy Framework of Cybersecurity in Japan

Law	The Basic Act on Cybersecurity [Legal means of "Cybersecurity," basic principles, and position of the Cybersecurity Strategy, etc.]					
Cabinet Order	Order for Cybersecurity Headquarters [Matters pertaining to the Headquarters]					
Cabinet Decision	Cybersecurity Strategy [Understanding on Cyberspace, visions & objectives, basic principles, and policy approaches, etc.]					
Policy Measures & Documents						

History of Governmental Framework of Cybersecurity



Successive defacement of gov. website

Spread of various computer virus
Increased threat of Information breach by cyber attacks
Confusion caused by information system failure/trouble

Sophisticated and organized Attacks to Sensitive Information
Cyber Attacks against Critical Infrastructures
Necessity to ensure cybersecurity for Tokyo 2020 Olympic & Paralympic Games

- ➢ Winny
- ➢ Passive attack
- ➢ Massive Gumbler
- ➢ Targeted attack against National Diet and MHI
- ➢ Sony Pic Ent. Of US
- ➢ Chinese mil. People charged in US
- ➢ Pension Service info. breach

FY 2000 2004 2005 2006 2009 2010 2011 2012 2013 2014 2015 2016 2020

Individual efforts by each agency

Focused on responding to cyber incidents

Construction of comprehensive infrastructure for counteracting cyber incidents

Active cyber security measures against cyber attacks
Responding to new environmental changes

Risk-based approach

IT Strategy

- e-Japan Strategy 2001.1
- e-Japan Strategy II 2003.7
- New IT Reform Strategy 2006.1
- i-Japan Strategy 2015 2009.7
- New Strategy on Information and Communications Technology 2010.5
- Declaration to be the World's Most Advanced IT Nation (IT Strategic Headquarters, June 2013)

Cyber Security Strategy

- Basic Act on Cybersecurity 2014.11
- Basic Act on Cybersecurity revised 2016.4

Mid/long-term Plan

- First National Strategy on Information Security
  Realizing "Secure Japan"
  2006.2
- Second National Strategy on Information Security
  Toward Strong "Individual" and "Society" in IT era
  2009. 2
- Information Security Strategy for Protecting the Nation
  ISPC, May 2010.
- Cybersecurity Strategy
  ISPC, 2013.6
- New Cybersecurity Strategy
  Cabinet decision, 2015.9

Annual Plan

2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

Measures for the Government

- Guidelines for the Forrmulation of Information Security Policies
  2000.7
- **Standards for Information Security Measures for the Central Government Computer System**
  1st～4th ed.
  2005.12
- **Management Standards for Information Security Measures for the Central Government Computer System**
  2011.4, revised 2012.4
- Common Standards
  (ISPC, May 2014)

Critical Information Infrastructure Protection

- Special Action Plan on Countermeasures to Cyber-terrorism of CII
  2000.12
- **Action Plan on Information Security Measures for CII**
  2005.12
- **The Second Action Plan on Information Security Measures for CII**
  2009.2, revised 2012.4
- The Basic Policy of Critical Information Infrastructure Protection (3rd Ed.)* (ISPC, May 2014)

Organization Framework

- IT Security Office
  2000.2
- National Information Security Center(NISC) 2005.4
- National center of Incident Readiness and Strategy for Cybersecurity(NISC) 2015.1
- Government Security Operation Coordination team(GSOC) 2008.4
- Cyber incident Mobile Assistant Team(CYMAT) 2012.6

The Basic Act on Cybersecurity

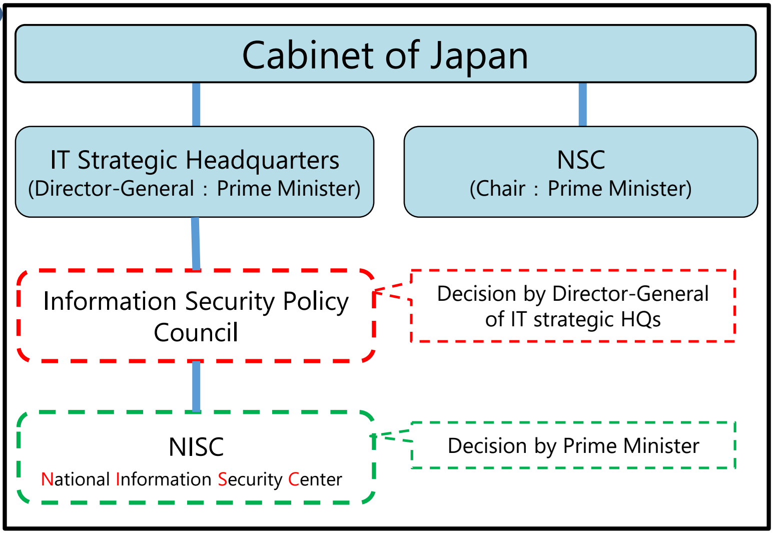
Enforced from 9th January 2015

The Basic Act on Cybersecurity [Enforced from 9th January 2015]

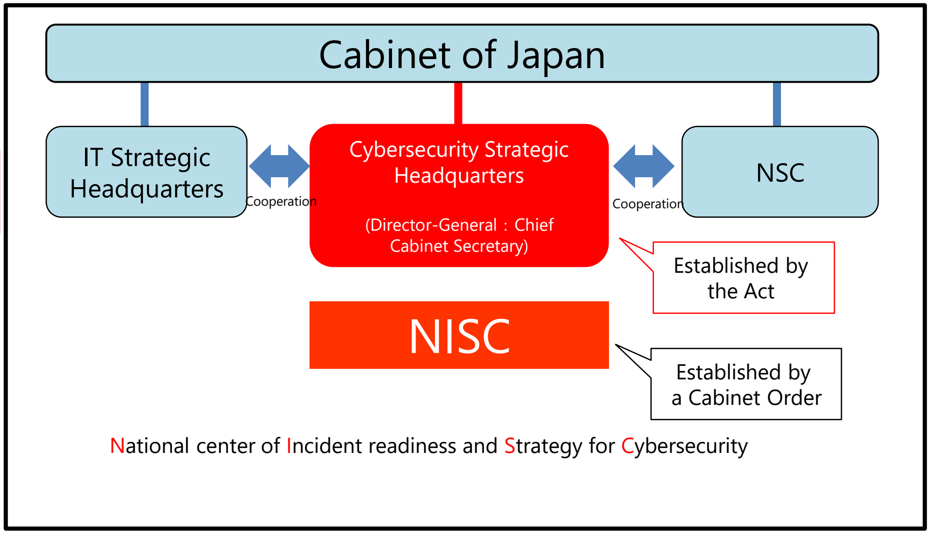
Before the Act

After the Act

Institutional Framework


Cabinet of Japan
IT Strategic Headquarters (Director-General : Prime Minister)
NSC (Chair : Prime Minister)
Information Security Policy Council
Decision by Director-General of IT strategic HQs
NISC
National Information Security Center
Decision by Prime Minister

Clear legislative backgrounds


Cabinet of Japan
IT Strategic Headquarters
Cooperation
Cybersecurity Strategic Headquarters
(Director-General : Chief Cabinet Secretary)
Cooperation
NSC
Established by the Act
NISC
Established by a Cabinet Order
National center of Incident readiness and Strategy for Cybersecurity

Authority to Governmental Bodies

Based on agreements with other governmental bodies

- Cybersecurity audit: self audit
- Incident analysis: NISC provides supports to other governmental bodies on request basis

Strengthened authority

Authority and mandate based on the Law

- Cybersecurity audit: 3rd Party audit by NISC
  - Management audit
  - Penetration test
- Incident analysis: NISC has authority to conduct cause investigation in serious incidents
  - Mandatory reports from other governmental bodies
  - Send formal recommendation to other governmental bodies

Strategy

"Cybersecurity Strategy" [June 2013]

Adopted by the Information Security Policy Council

Raised status

New "Cybersecurity Strategy" based on the Act [September 2015]

After accepting opinions from NSC and IT Strategic HQs, the strategy was adopted as a Cabinet Decision, and reported to the National Parliament

Definition of the term “Cybersecurity” in the act (Article 2)

- “Cybersecurity” means that necessary measures are taken:
  - to safely manage information, such as prevent against the leakage, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive function (hereinafter referred to as “electro-magnetic means”); and
  - to guarantee the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electro-magnetic means [hereinafter referred to as "electro-magnetic storage media"])
- and that those states are appropriately maintained.

Basic Principles for the Promotion of Cybersecurity Policy (Article 3)

- The act provides basic principles for the promotion of cybersecurity policy, such as:

  (1) … ensuring the free flow of information through the maintenance of advanced information and telecommunications networks … is critical to enjoying benefits from the freedom of expression, enabling the creation of innovation, improving economic and social vitality, and so on…

  (3) … with intent to positively implement the maintenance of the Internet and other advanced information and telecommunications networks and actions toward the establishment of a vital economy and society through the utilization of information and telecommunications technologies.

  (4) … with intent to play a leading role in an internationally-coordinated effort for the creation and development of an international normative framework for cybersecurity

  (6) … with intent to be careful not to wrongfully impinge upon citizens' rights

  etc.

The Basis of the Idea of the “Free Flow of Information”: The Constitution of Japan [November 3, 1946])

■ Article 21.

(1) Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed.

(2) No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

The Cybersecurity Strategy (Article 12)

- The act provides legislative backgrounds for the Cybersecurity Strategy:

(1) The Government shall be required to establish a basic plan for cybersecurity (hereinafter referred to as the "*Cybersecurity Strategy*") with the aim of the comprehensive and effective promotion of cybersecurity policy.

(2) The Cybersecurity Strategy shall address the following:

I. Basic objectives of cybersecurity policies;

II. Matters regarding cybersecurity assurance within administrative organs and related organs;

III. Matters regarding the promotion of cybersecurity assurance at critical infrastructure operators…;

etc.

(3) The Prime Minister shall request a cabinet decision on the proposed Cybersecurity Strategy.

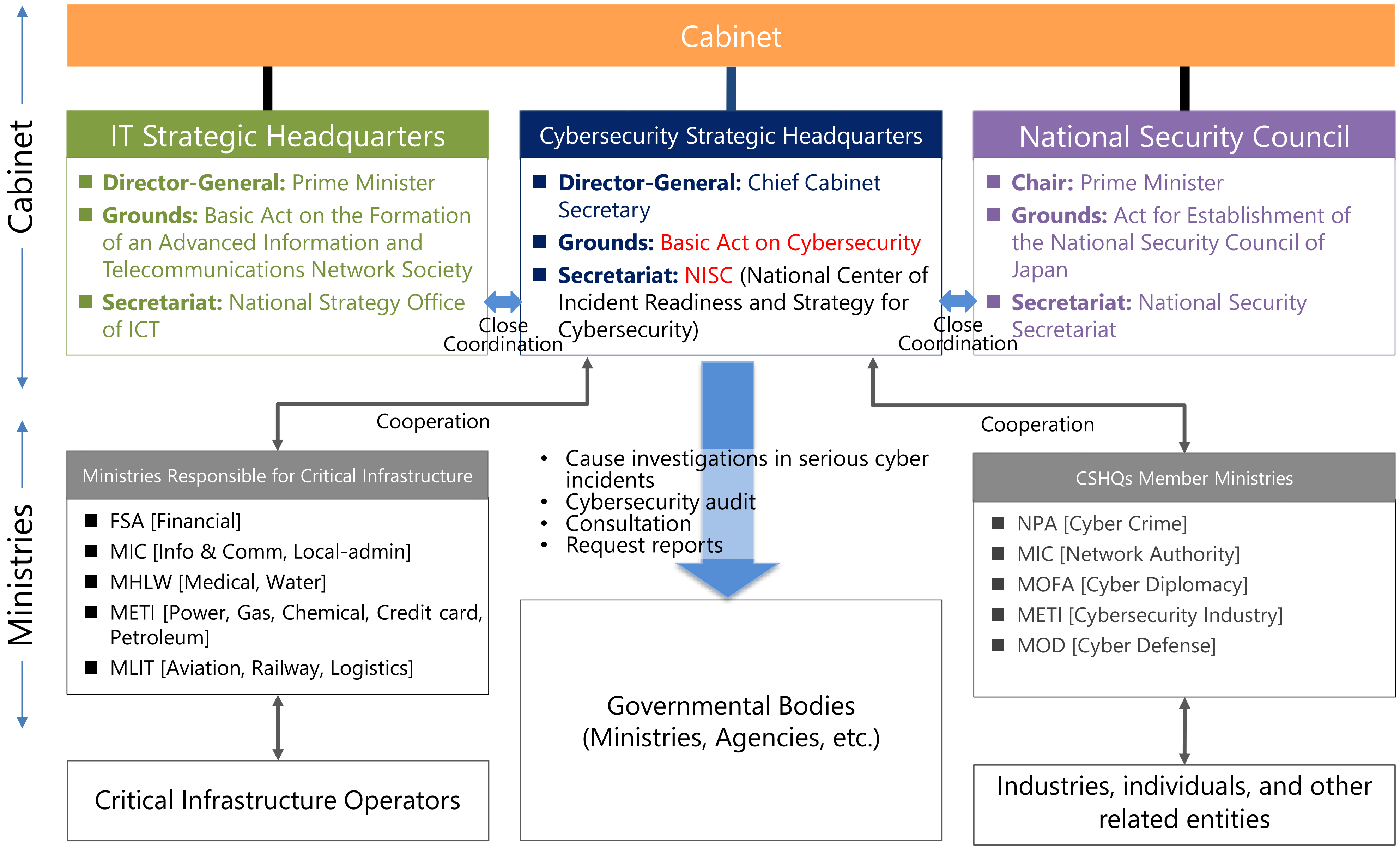
(4) When formulating the Cybersecurity Strategy, the Government shall, without delay, report it to the Diet and announce it publicly by using the Internet and other appropriate means.

etc.

Promotion of International Cooperation, and so forth (Article 23)

- To actively carry out Japan's role in the international community and to promote Japan's interests in the community, the Government shall promote:
  - active participation in international norm setting;
  - confidence building and the promotion of information sharing with foreign countries;
  - international technical cooperation such as active support for cybersecurity capacity building in developing countries;
  - international cooperation such as crackdowns on cybercrime; and
  - shall provide necessary measures to deepen other countries' understanding of Japan's cybersecurity.

Cybersecurity Framework (Article 25~30)



Cabinet

IT Strategic Headquarters

- **Director-General:** Prime Minister
- **Grounds:** Basic Act on the Formation of an Advanced Information and Telecommunications Network Society
- **Secretariat:** National Strategy Office of ICT

Cybersecurity Strategic Headquarters

- **Director-General:** Chief Cabinet Secretary
- **Grounds:** Basic Act on Cybersecurity
- **Secretariat:** NISC (National Center of Incident Readiness and Strategy for Cybersecurity)

National Security Council

- **Chair:** Prime Minister
- **Grounds:** Act for Establishment of the National Security Council of Japan
- **Secretariat:** National Security Secretariat

- Cause investigations in serious cyber incidents
- Cybersecurity audit
- Consultation
- Request reports

Ministries Responsible for Critical Infrastructure

- FSA [Financial]
- MIC [Info & Comm, Local-admin]
- MHLW [Medical, Water]
- METI [Power, Gas, Chemical, Credit card, Petroleum]
- MLIT [Aviation, Railway, Logistics]

Critical Infrastructure Operators

Governmental Bodies (Ministries, Agencies, etc.)

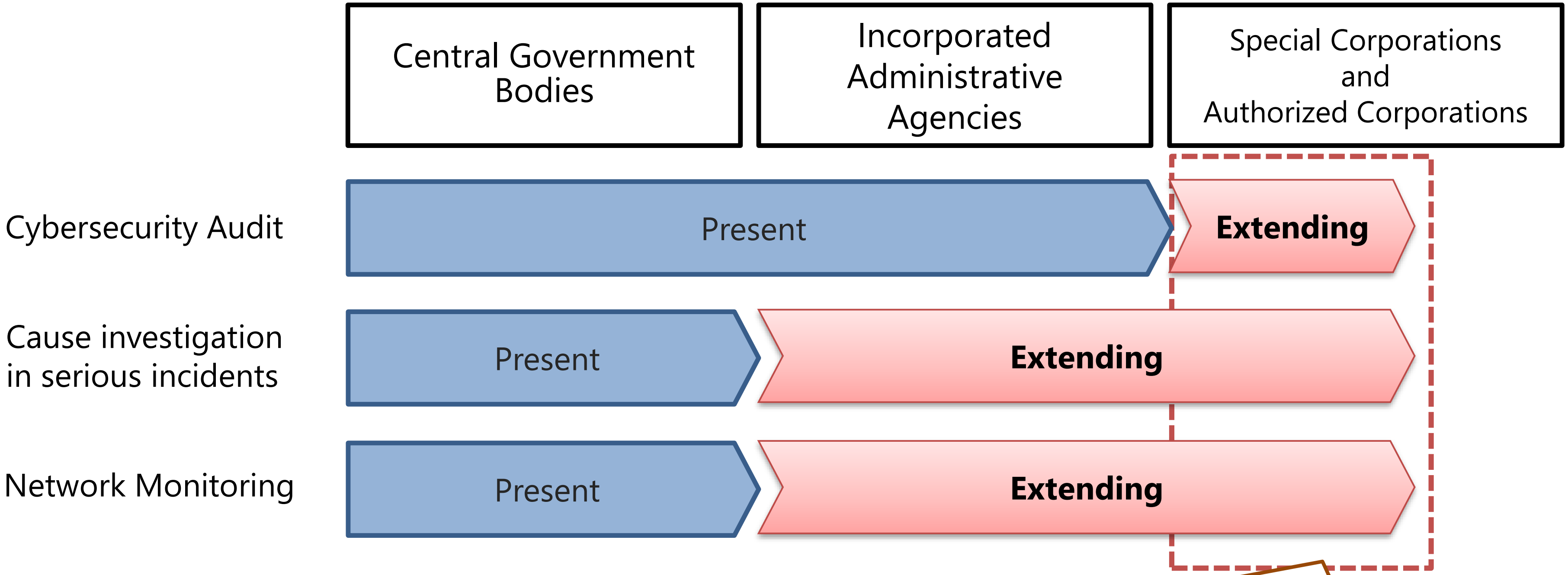
CSHQs Member Ministries

- NPA [Cyber Crime]
- MIC [Network Authority]
- MOFA [Cyber Diplomacy]
- METI [Cybersecurity Industry]
- MOD [Cyber Defense]

Industries, individuals, and other related entities

The Amendment to the Basic Act on Cybersecurity [Will be enforced no later than Oct. 22, 2016]

- Building upon the lessons learned from Japan Pension Service case, the National Diet passed the amendment of the Basic Act on Cybersecurity to extending Cybersecurity HQs'/NISC's mandate of network monitoring, cybersecurity audit, and investigation in serious incidents


Central Government Bodies
Incorporated Administrative Agencies
Special Corporations and Authorized Corporations
Cybersecurity Audit
Present
Extending
Cause investigation in serious incidents
Present
Extending
Network Monitoring
Present
Extending

CSHQ will identify Special Corporations and Authorized Corporations that should be subjects of audit, cause investigation, and monitoring etc.

- Japan Pension Service etc. will be expected as the subjects
- CSHQ will identify the subject entities considering the influence to national life and economy when the special corporation's cybersecurity is not assured

Cybersecurity Strategy

Cabinet Decision
September 24 2015

Outline of Cybersecurity Strategy

1 Understanding of Cyberspace

- ➢ Blessings of Cyberspace: Generating infinite values, essential foundation for our socio-economic activity
- ➢ "Hyper-connected and converged society" is coming
- ➢ Cyber threats are becoming more serious and being perceived as national security matters

2 Visions & Objective

- ➢ Develop and advance free, fair, and secure cyberspace subsequently contribute to:

1) Socio-economic vitalization 2) Safe and secure society 3) International Peace and stability, National security

3 Principles

1. Free Flow of Information 2. Rule of Law 3. Openness 4. Autonomy 5. Collaboration among Multi Stakeholders

4 Policy Approaches

Proactive / Initiative / Converged society

1) Socio-Economic Vitalization and Sustainable Development

~ From Cost to Investment ~

■Creating Secure IoT System
New industry creation by safe IoT

■Promoting Management with cybersecurity mindset
Awareness raising of senior executives

■Improving Business Environment
Promoting cybersecurity business

2) Realizing a Safe and Secure Society for the People

~ Foundation for 2020, further ~

■Protecting People and Society
Enhancing capability and countermeasure

■Protecting CII
Enhancing information sharing public with private

■Protecting Governmental Agencies
Strengthening defense and management audit

3) Peace and Stability of International Community and Japan's National Security

~ Proactive contribution to peace in cyberspace ~

■Ensure Japan's National Security
Improving Cyber capabilities

■International Peace and Stability
Rule of law in cyberspace, confidence building

■International Partnership
Cooperation in a wide range of area

Cross Cutting

■R&D
Improving detection and protection capabilities

■Human Resources
Developing multi-talent, practical training, promoting skill standard

5 Organization

- ➢ Enhancement cooperation with public and private sector, Institution building toward the Tokyo Olympic and Paralympic Games in 2020

1. Understanding of Cyberspace

■ Significant Benefits of Cyberspace…

- Exchanging ideas freely across national borders
- Generating infinite values from intellectual creations and innovations inspired by the ideas globally exchanged
- Essential foundation for Japan’s socio-economic activities

■ Cyber earthshaking changes…

- Things and People have become interconnected in multilayer without physical constraints
- “Hyper-connected and converged society” is coming

■ Increasing cyber threats…

- Cyber threats are becoming more serious and being perceived as national security matters

2. Visions and Objective

- To develop and advance free, fair, and secure cyberspace, and subsequently contribute to:
  - Socio-economic vitalization and sustainable development
  - Creation of a society where the people can enjoy safe and secure lives
  - Assuring international peace and stability as well as national security.

3. Basic Principles

- Japan affirms the following basic principles in policy planning and its implementation in cybersecurity, harmonized to perspectives of social and national security
  - Assurance of the Free Flow of Information
  - The Rule of Law
  - Openness
  - Autonomy (Self-governance)
  - Collaboration among Multi-stakeholders
- In line with these principles, Japan reserves, as options, all viable and effective measures in order to protect the people’s safety, security, and rights

1) Socio-Economic Vitalization and Sustainable Development

"Cybersecurity is not a cost, but an investment"

Creating Secured IoT (Internet of Things) Systems

- Promoting large scale projects related to secure IoT systems based on SBD (Security by Design)
- Guidelines and standards for cybersecurity of IoT systems
- R&D related to IoT systems

Promoting Enterprise Management with a Cybersecurity Mindset

- Evaluation framework for enterprise's efforts in cybersecurity
- Cybersecurity professionals, intermediators, senior executives
- Promoting cyber exercise, information sharing between the public and the private

Improving Cybersecurity Business Environment related to

- Promoting cybersecurity related business by using sovereign wealth funds, etc.
- Promoting security audit for cloud services for SMEs
- Reexamining the existing systems and institutional practices for new business opportunities
- Leading to set international security standards relating to IoT systems
- Realizing fair business environment such as preventing intellectual property leakage

2) Realizing a Safe and Secure Society for the People

”Developing cybersecurity infrastructure for 2020 and further”

■ Protecting People and Society

- Enhancing capability for information gathering on vulnerability
- Promoting awareness raising activities especially for local communities, local governments, and SMEs
- Enhancing countermeasures against cybercrimes e.g. storing traffic data by operators, etc.

■ Protecting Critical Information Infrastructure

- Continuous Review on the Scope of CII industries
- Enhancing information sharing between the public & the private in CII industries
- Offering tailored support for local governments with consideration of the upcoming Social Security and Tax Number System (“My Number” (national ID) System)
- Promoting international third-party certification schemes for smart meters and other industrial control systems

■ Protecting Governmental Agencies

- Conducting penetration tests, addressing supply chain risks, and strengthening defense capabilities
- Conducting management audit and risk based assessments
- Improving common and cross-governmental measures for cybersecurity with consideration of new ICT products and services

3) Peace and Stability of International Community and Japan’s National Security

“Proactive contribution to peace in cyberspace”

■ Ensuring Japan's National Security

- ● Improving cyber capabilities of NPA, SDF, and others in both quality and quantity
- ● Protecting Advanced Technologies
- ● Enhancing information sharing between public & private from the national security perspective

■ Building Peace and Stability of the International Community

- ● Contributing actively to international rule making processes for cyberspace at UN and other frameworks
- ● Taking measures to address malicious use of cyberspace by non-state actors
- ● Cooperating actively in capacity building efforts of other countries

■ Partnership with Countries around the World

- ● Asia & Pacific: Strengthening relationship with ASEAN, strengthening cooperative relations with regional partners who share basic values and strategic interest with Japan
- ● Cooperating with U.S. as an ally in all levels for cybersecurity
- ● Europe, Middle East, and other regions: Strengthening cooperation with countries sharing same basic values with Japan

Cross-Cutting Approaches to Cybersecurity

■ Advancement of Research and Development

- Improving detection and protection capabilities against cyber attacks
- Promoting interdisciplinary research on cybersecurity
- Promoting R&D in core technologies for national security like cryptographic technology
- Promoting international cooperation in R&D

■ Development and Assurance of Human Resources

- Developing multi-talented human resources
- Promoting industry-academia-public coordination for practical training
- Expanding elementary and secondary education
- Fostering world-class talent by international cybersecurity competitions, etc.
- Promoting skill standards, qualification frameworks, and evaluation systems for cybersecurity human resources

Cybersecurity Policy Examples

Policy Measures Based on the Cybersecurity Strategy

Improvement of Socio-Economic Vitality and Sustainable Development

■ Creation of Secure IoT Systems

- *General Framework for Secured IoT Systems [August 2016]*

■ Encouraging enterprises to report their cybersecurity efforts to the market

- *The Concept of Cybersecurity for Cooperate Management [August 2016]*

Building a Safe and Secure Society for the People

■ Conducting constant review on the scope of CIIP and enhancing information sharing on CII

- *Adopted the Roadmap for CIIP Policy Update [March 2016], which aims to enhance CII's cyber protection.*
- *Reviewing & renewing measures, such as public-private information sharing scheme and implementation [To be finished by March 2017]*

■ Improving cybersecurity measures for governmental bodies

- *Revising the Information Security Common Standards for Government [August 2016]*
- *Extended NISC's scope of network monitoring by amending the Basic Act on Cybersecurity [April 2016]*

Peace and Stability of International Community and Japan's National Security

■ Advancing cooperation on cybersecurity in bilateral cyber dialogues and multilateral frameworks

■ Contributing to the efforts to develop international rules and norms in cyberspace at various fora including UN Cyber GGE

- *Adopted G7 Ise-Shima Leaders' Declaration [May 2016], and established G7 Cyber WG*
- *2016-2017 UN GGE started [August 2016]*

■ Active contribution to the cybersecurity capacity building in developing countries, especially in ASEAN

Advancement of R&D and Development of Cybersecurity Human Resources

■ R&D of IoT security for critical infrastructure in the framework of SIP (Cross-Ministerial Strategic Innovation Promotion Program)

■ Promotion of human resources development by partnership between the public and the private sectors

- *Adopted the Cybersecurity Human Resources Development Plan [March 2016]*
- *Established a new national cybersecurity professional certification by a legislative amendment [April 2016]*
- *Built a national cyber range as a NICT's facility by a legislative amendment [April 2016]*

A policy example of implementation of the “Free Flow of Information”:

Information Security Common Standards for Government 2016

- To advance and improve efficiency of their business and IT systems, government bodies are anticipated to increase use of cloud services.
- In considering to use a cloud service as governmental business and IT systems, a government body need to review following items:

1. Information confidentiality and classification
2. Lex causae and legal jurisdiction of the cloud service
3. Credibility of the cloud service provider in case of terminating the service contract
4. Cybersecurity not only of the cloud service itself, but also of entire network path used for
5. Cybersecurity audit reports and certification of the cloud service

A policy example of implementation of the “Rule of Law”:

Convention on Cyber Crime (Budapest Convention)

- ■ Budapest Convention on Cyber Crime is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

✓	2001 Nov.	Signature Ceremony in Budapest (Japan signed with other 29 signatories)
✓	2004 Apr.	Approval of the Convention by the Diet
✓	2004 Jul.	Entry into force of the Convention
✓	2012 Nov.	Valid in Japan by completing the preparatory process

- ■ The Convention is an International framework for preventing cross-border cybercrime.
  - ● Definition of Crime: Illegal access, Interception, Disturbing computer systems, Creating Viruses
  - ● Procedure of Criminal Investigation: Procedure of Preservation of Data, Order of Submit, Search, Seizure
  - ● International Cooperation: Cooperation for Criminal Investigation, Extradition

- ■ Japan continuously encourages non-party countries to join the Budapest Convention on Cyber Crime to extend the Rule of Law in the Cyberspace

A policy example of implementation of the “Openness”:

Basic Principles of General Framework for Secured IoT Systems

- NISC brought up the General Framework for Secured IoT Systems to promote the interoperability of IoT systems and implementation of security requirements in August 2016.

- We consider to determine following items are essential to ensure IoT system security:

a. Definitions (including the applicability and the scope) of IoT systems should be determined and clarified. Also, those systems should be categorized based on system characteristics reflecting their inherent risks and properly addressing those risks;

b. Essential requirements for ensuring the users’ safety should be determined, as well as confidentiality, integrity and the availability of information on IoT systems, including functions of devices;

c. Requirements should be determined to ensure secured system operation and service resilience in case of a system failure, including mission assurance rules;

d. Safety assurance standards, including statutory and customary requirements, should be determined for connected things and networks;

e. Confidentiality, integrity, availability, and safety must be ensured in the case of mechanical failure or a cyber-attack, and swift service restoration in case of a system trouble should be clarified; and

f. Responsibilities, boundaries and information ownership of IoT systems should be clarified.

These items should be applied to the requirements for other cases such as interconnection of IoT systems.

“General Framework for Secured IoT Systems”, established on 26th Aug. 2016 by NISC

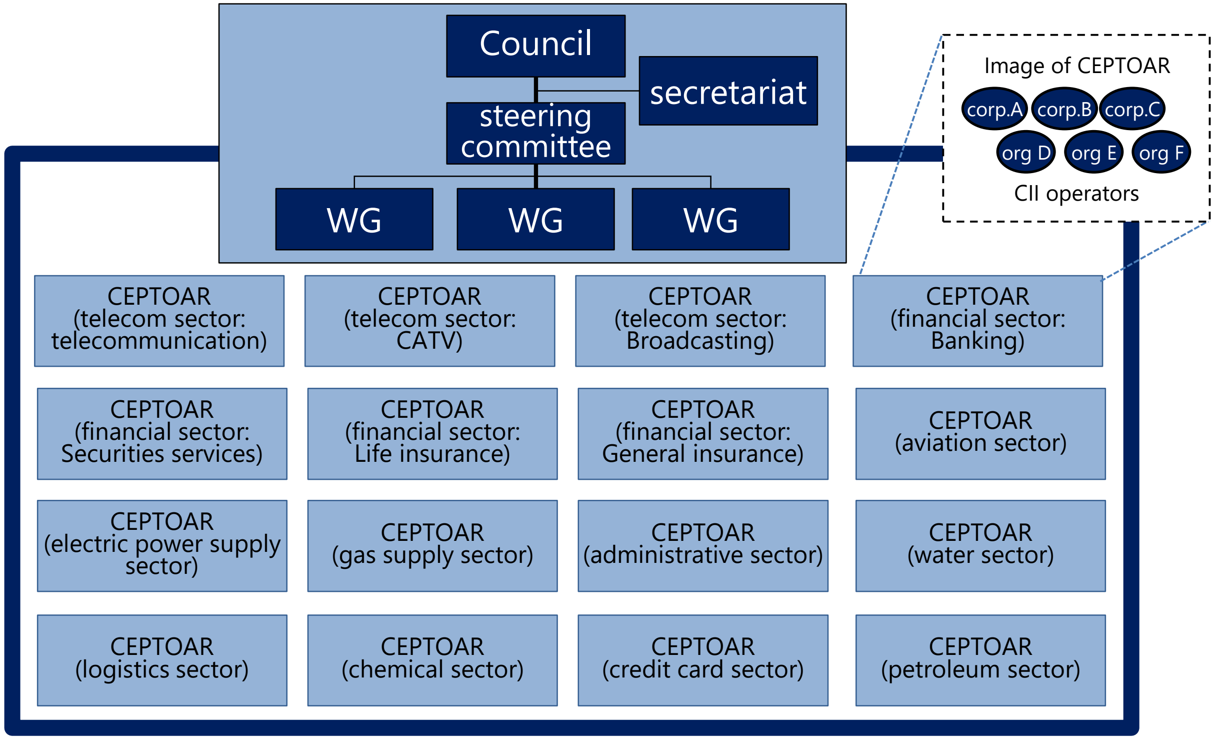
A policy example of implementation of the "Autonomy": Information Sharing Framework among CIIP Operators

CEPTOAR

- **C**apability for **E**ngineering of **P**rotection, **T**echnical **O**peration, **A**nalysis and **R**esponse.
- Functions which provide information sharing and analysis at CII operators, and organizations which serve as these functions.

CEPTOAR Council

- The council composed of representatives of each CEPTOAR which carries out information sharing between CEPTOARs.
- An independent body, not positioned under other agencies, including government organizations.



Council

secretariat

steering committee

WG

WG

WG

Image of CEPTOAR

corp.A corp.B corp.C

org D org E org F

CII operators

CEPTOAR (telecom sector: telecommunication)

CEPTOAR (telecom sector: CATV)

CEPTOAR (telecom sector: Broadcasting)

CEPTOAR (financial sector: Banking)

CEPTOAR (financial sector: Securities services)

CEPTOAR (financial sector: Life insurance)

CEPTOAR (financial sector: General insurance)

CEPTOAR (aviation sector)

CEPTOAR (electric power supply sector)

CEPTOAR (gas supply sector)

CEPTOAR (administrative sector)

CEPTOAR (water sector)

CEPTOAR (logistics sector)

CEPTOAR (chemical sector)

CEPTOAR (credit card sector)

CEPTOAR (petroleum sector)

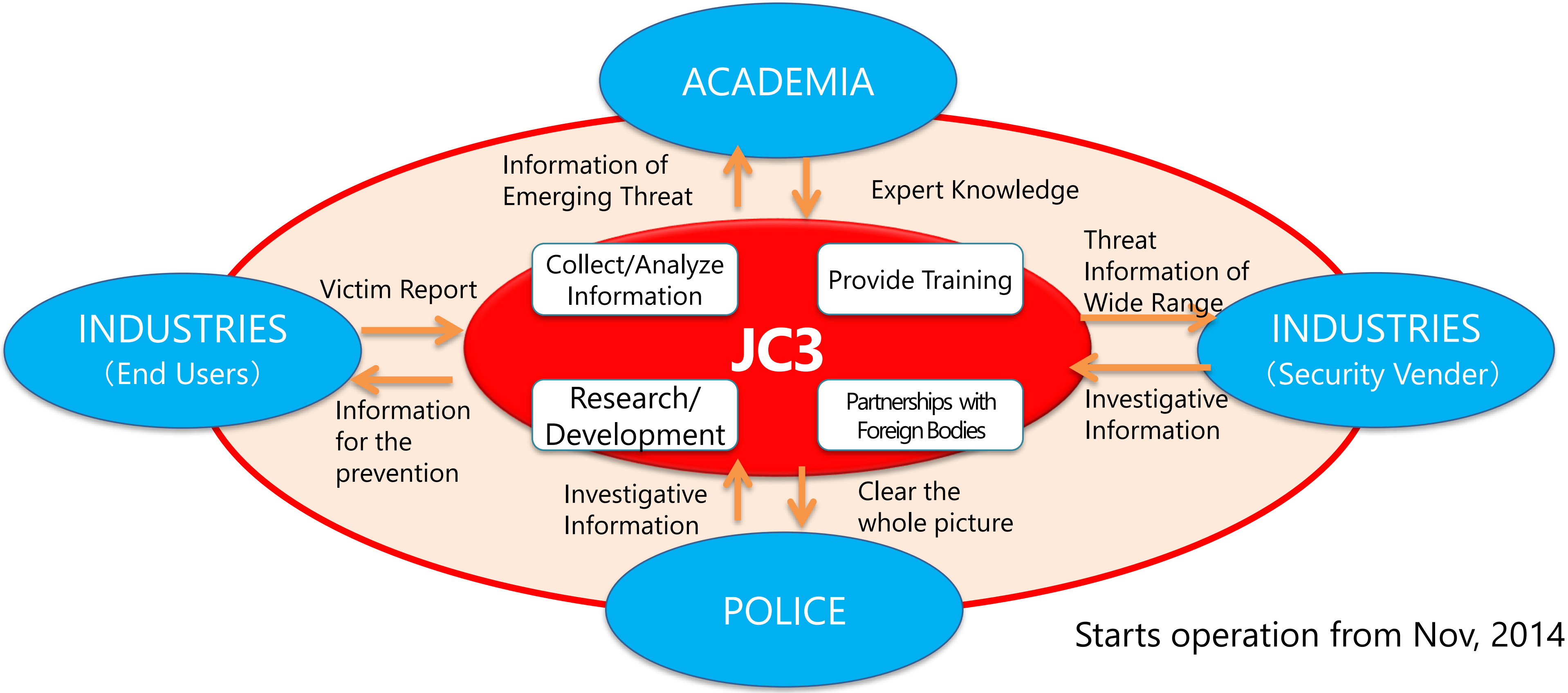
Observer of Council

CEPTOAR (railway sector)
CEPTOAR (medical sector)
Japan Business Federation / Keidanren
Bank of Japan
FISC
Japan Post Bank
NICT
IPA
JPCERT/CC
FSA
MIC
MHLW
METI
MLIT

A policy example of implementation of the "Collaboration among Multi Stakeholders":

The Overview of Japan Cybercrime Control Center（JC3）

■ Objective: to oversee the whole of cyberspace by sharing information gathered and analyzed, the knowledge and experiences of industry, academia and government, and contribute to the prevention of subsequent incidents by identifying, mitigating, and neutralizing the root of threats in cyberspace.


ACADEMIA
Information of Emerging Threat
Expert Knowledge
INDUSTRIES
(End Users)
Victim Report
Information for the prevention
Collect/Analyze Information
Provide Training
JC3
Research/ Development
Partnerships with Foreign Bodies
Threat Information of Wide Range
INDUSTRIES
(Security Vender)
Investigative Information
Investigative Information
Clear the whole picture
POLICE

Starts operation from Nov, 2014

International Commitment:
Actively Support Cybersecurity Capacity Building in ASEAN

- …we welcomed the progress made in the implementation of the "ASEAN-Japan Collaboration Framework on Information Security", and noted with appreciation Japan's determination to proactively support cybersecurity efforts of ASEAN member states through measures such as dispatching specialists and trainers, providing trainings and equipment, supporting the establishment of cybersecurity strategy and guideline, encouraging public-private partnerships, and promoting measures against cybercrime.

~ Chairman's Statement of the 19th ASEAN-Japan Summit (7 September 2016, Vientiane, Lao PDR)