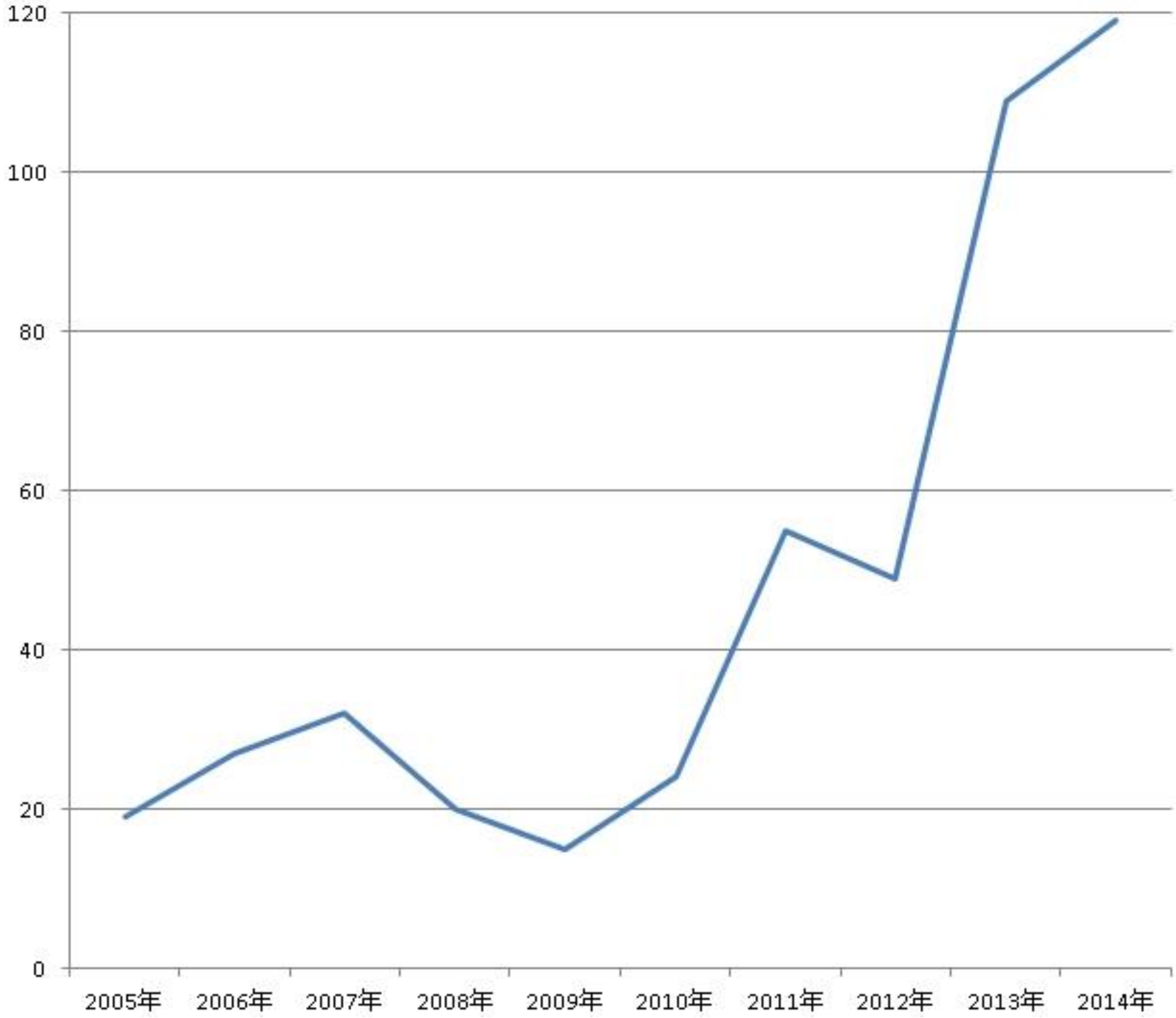
Cybersecurity Strategy in Japan

Jan 21, 2015

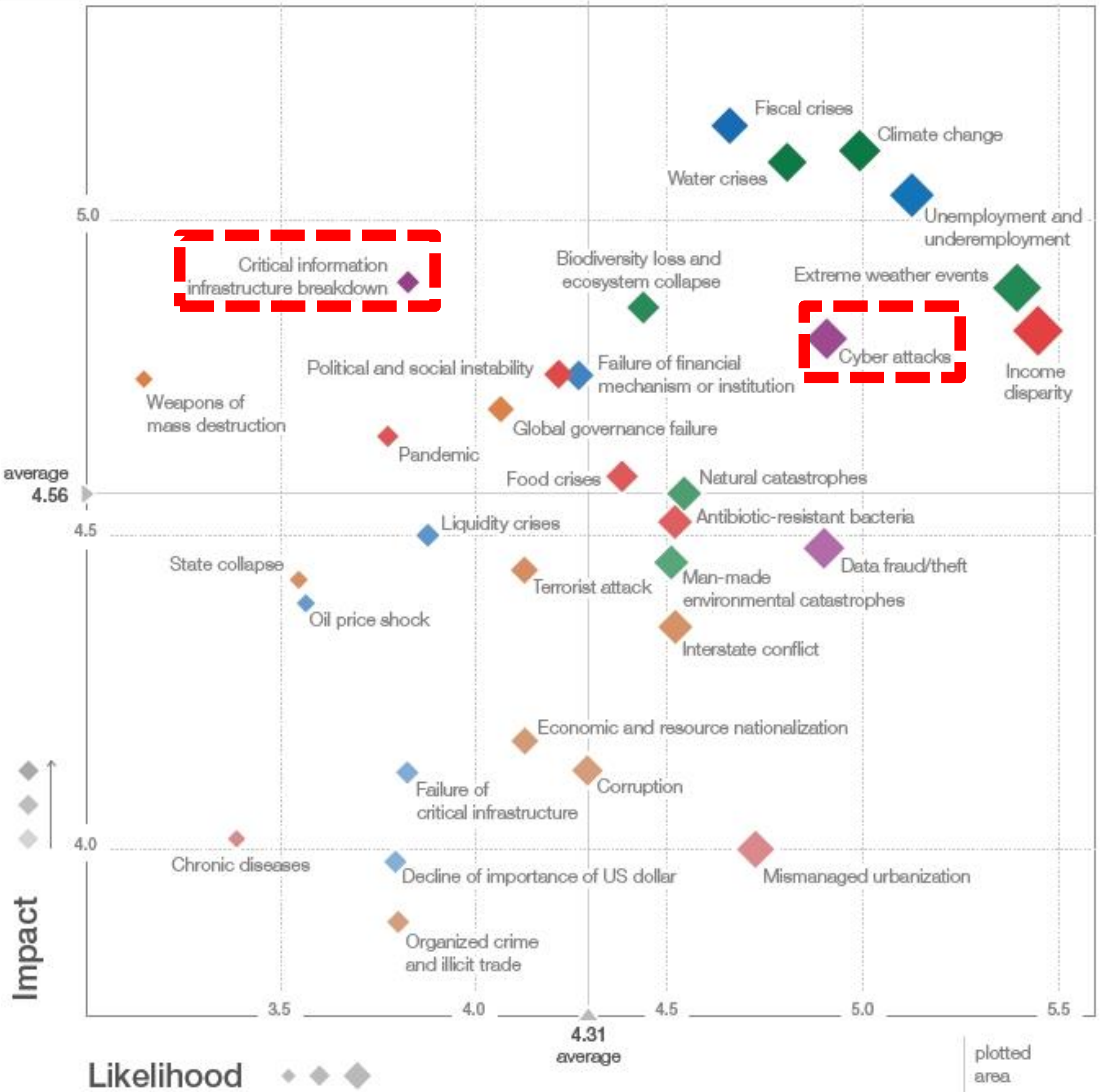
Hiroshi Kawaguchi, CISSP
Little eArth Corporation Co., Ltd.
Chief Evangelist
hiroshi.kawaguchi @ lac.co.jp

JSOC JAPAN SECURITY OPERATION CENTER

What is this?

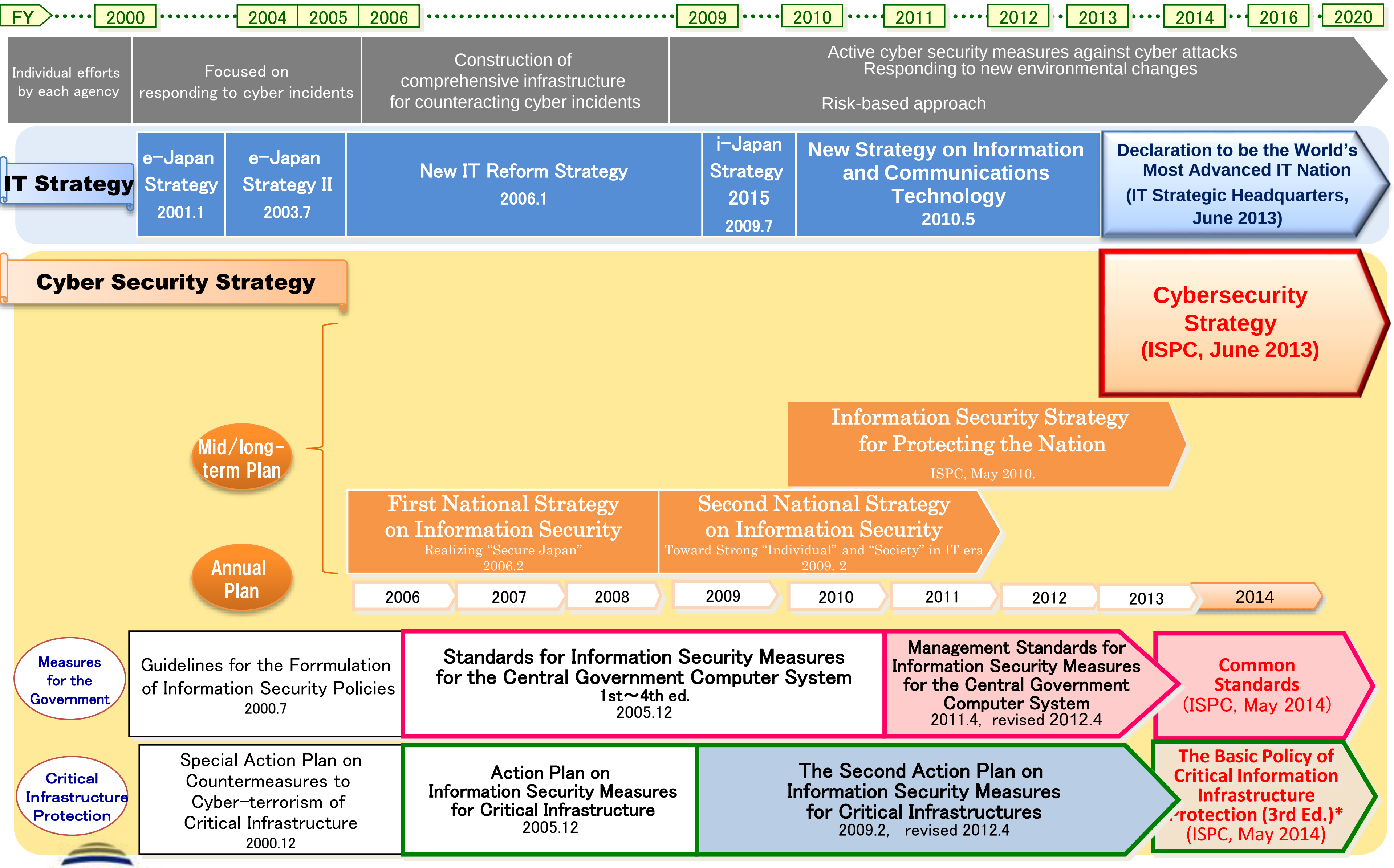

120
100
80
60
40
20
0
2005年
2006年
2007年
2008年
2009年
2010年
2011年
2012年
2013年
2014年

Global Risks 2014



http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

History of Cybersecurity Strategy



FY 2000 2004 2005 2006 2009 2010 2011 2012 2013 2014 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

Cybersecurity Strategy (ISPC, June 2013)

Mid/long-term Plan

Information Security Strategy for Protecting the Nation
ISPC, May 2010.

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

Annual Plan

2006 2007 2008 2009 2010 2011 2012 2013 2014

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 Infrastructure Protection

Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure
2000.12

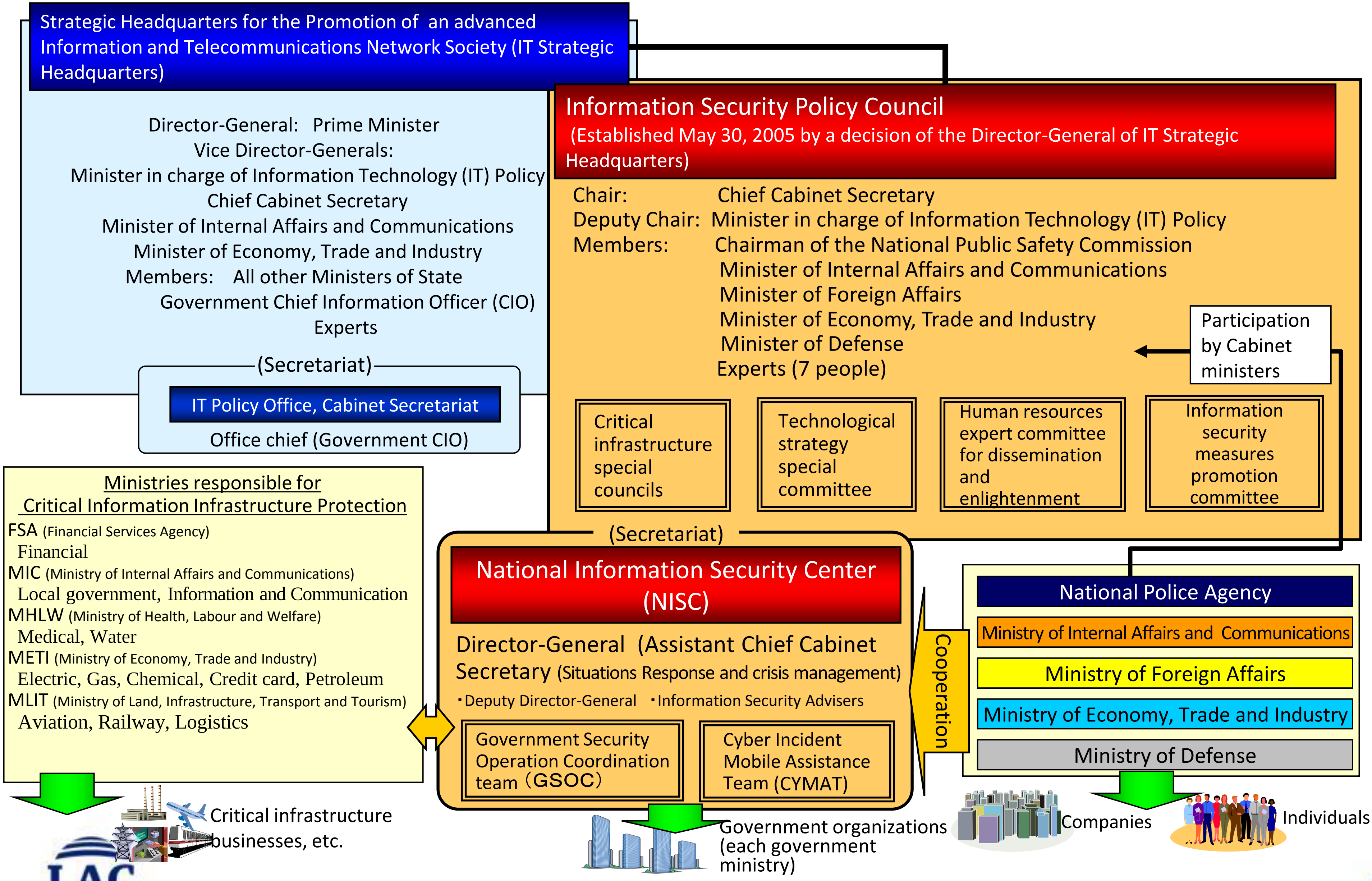
Action Plan on Information Security Measures for Critical Infrastructure
2005.12

The Second Action Plan on Information Security Measures for Critical Infrastructures
2009.2, revised 2012.4

The Basic Policy of Critical Information Infrastructure Protection (3rd Ed.)*
(ISPC, May 2014)

*The document title was changed.

Framework for Information Security Policies



Strategic Headquarters for the Promotion of an advanced Information and Telecommunications Network Society (IT Strategic Headquarters)

Director-General: Prime Minister
Vice Director-Generals:
Minister in charge of Information Technology (IT) Policy
Chief Cabinet Secretary
Minister of Internal Affairs and Communications
Minister of Economy, Trade and Industry
Members: All other Ministers of State
Government Chief Information Officer (CIO)
Experts

(Secretariat)

IT Policy Office, Cabinet Secretariat

Office chief (Government CIO)

Information Security Policy Council
(Established May 30, 2005 by a decision of the Director-General of IT Strategic Headquarters)

Chair: Chief Cabinet Secretary
Deputy Chair: Minister in charge of Information Technology (IT) Policy
Members: Chairman of the National Public Safety Commission
Minister of Internal Affairs and Communications
Minister of Foreign Affairs
Minister of Economy, Trade and Industry
Minister of Defense
Experts (7 people)

Participation by Cabinet ministers

Critical infrastructure special councils

Technological strategy special committee

Human resources expert committee for dissemination and enlightenment

Information security measures promotion committee

Ministries responsible for Critical Information Infrastructure Protection

FSA (Financial Services Agency)
Financial
MIC (Ministry of Internal Affairs and Communications)
Local government, Information and Communication
MHLW (Ministry of Health, Labour and Welfare)
Medical, Water
METI (Ministry of Economy, Trade and Industry)
Electric, Gas, Chemical, Credit card, Petroleum
MLIT (Ministry of Land, Infrastructure, Transport and Tourism)
Aviation, Railway, Logistics

(Secretariat)

National Information Security Center (NISC)

Director-General (Assistant Chief Cabinet Secretary (Situations Response and crisis management)
・Deputy Director-General ・Information Security Advisers

Government Security Operation Coordination team（GSOC）

Cyber Incident Mobile Assistance Team (CYMAT)

Cooperation

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

Critical infrastructure businesses, etc.

Government organizations (each government ministry)

Companies

Individuals

Sophisticated Attacks to Sensitive Information

[Recent major cases]

2011.9 ～	[Mitsubishi Heavy Industries, Ltd. (MHI), House of Representative (HR) etc.] **Found virus infection by targeted attacks**
2012.5	[Japan Nuclear Energy Safety Organization (JNES)] **Found possibility of information leakage over previous months**
2013.1	[Ministry of Agriculture, Forestry and Fisheries of Japan (MAFF)] **Announced attack case on TPP-related information leakage**
2013.4	[Japan Aerospace Exploration Agency (JAXA)] **Found unauthorized access to servers from outside**
2013 autumn	[Government agencies etc.] **Found zero-day attack* causing particular entities to be infected by web browsing**
2014.1	[Japan Atomic Energy Agency (JAEA)] **Found possibility of information leakage by virus infection**

* Zero-day attack: Attack misuses unpatched or undisclosed security holes in software.

[Threats to government's organizations]

	FY 2011	FY 2012	FY 2013
No. of threats detected through monitoring by sensors, etc.**	Approx. 660,000	Approx. 1,080,000	Approx. 5,080,000
No. of notices issued through monitoring by sensors, etc.	139	175	139
No. of warnings issued on suspicious e-mails	209	415	381

24 hrs & 365 days
(10 times in a min.)

** No. of no normal accesses or communications among events detected by sensors installed in the ministries by the GSOC（abbreviation for Government Security Operation Coordination team) etc.

Attacks on Critical Infrastructures

[No. of attacks on critical infrastructures]

	FY 2012	FY 2013	Main Details
No. of info. Messages or reports* from critical infrastructures areas	110 (76)**	153 (133)	Unauthorized access,Dos **121** Virus infection **7** Other intentional factors **5**

* Reports from the critical infrastructure operators to the NISC

** Reports concerning Cyber Attacks

	FY 2012	FY 2013
No. of received info. Messages*** about targeted attack e-mail, etc.	246	385

Increasing crisis

*** Reports from the five industries (45 organizations), or critical infrastructure equipment manufacture, power, gas, chemistry and petroleum to Information-Technology Promotion Agency (IPA), Japan

[Area of the Critical infrastructure]

(1)Information and Communications

(2) Finance

(3) Aviation

(4) Railways

(5) Electricity

(6) Gas

(7) Gov't and Admin. Services

(8) Medical Services

(9) Water

(10) Logistics

(11) Chemistry

(12) Credit Card

(13) Petroleum

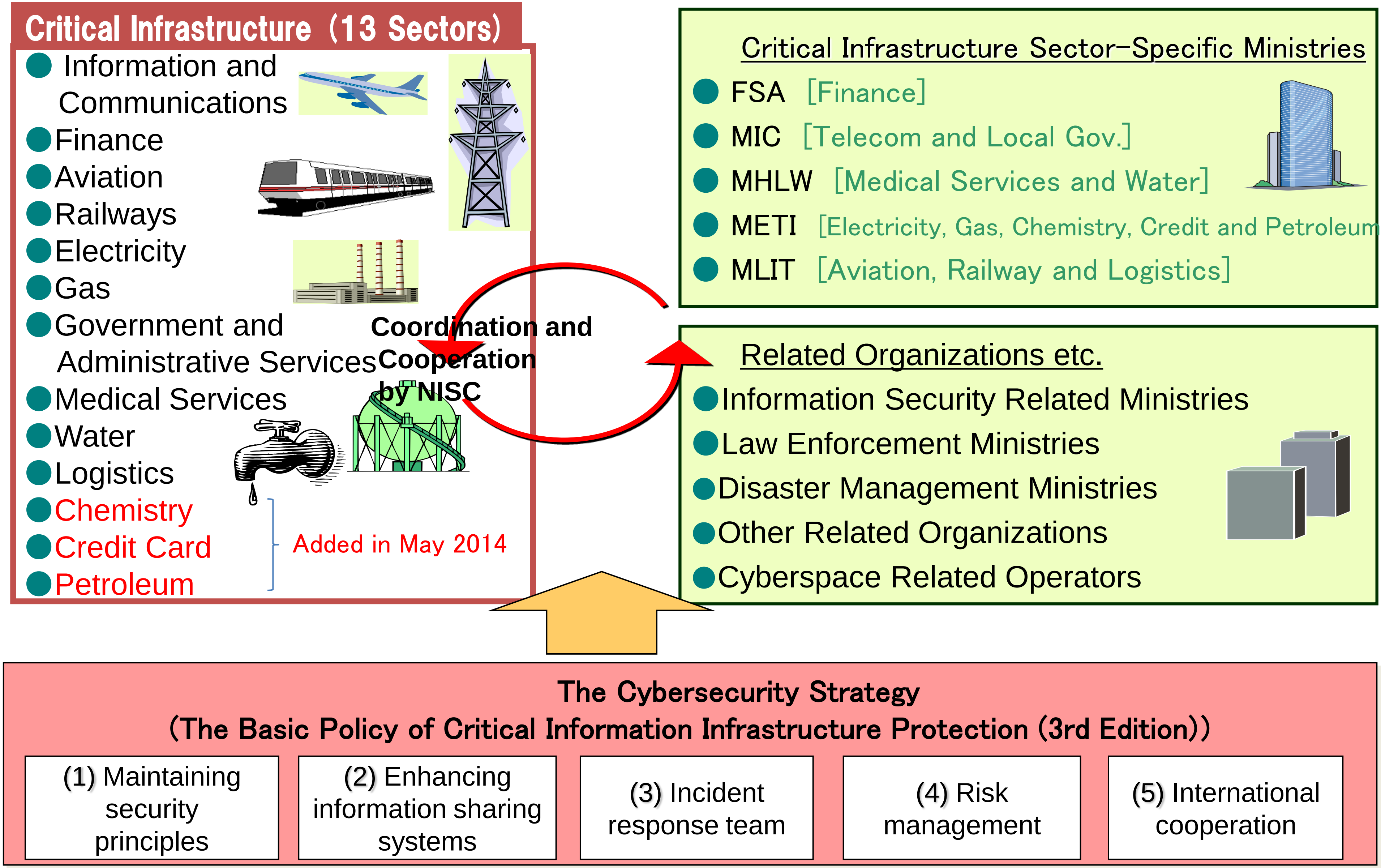
Diversification of areas to be protected

**** These three sectors were added to the third action plan to security measures for critical infrastructures decided by the Information Security Policy Council (ISPC) on 19th May 2014.

Main Efforts based on the “Cybersecurity Strategy”(June 2013)

	Government Organizations, Independent Administrative Organizations, etc.	Critical Infrastructure Industries	Enterprises, Individuals
Resilient Cyberspace (Strengthening protection)	● **Common Standards for Information Security Measures for the Government Agencies (2014 edition) (Information Security Policy Council, 2014)** ● Strengthening GSOC, accurate and quick response through cooperation with CYMAT and CSIRT ● Conducting incident response drills, specifying roles of related organizations such as the police and the Self Defense Forces ● Measures for new threats pursuant to new services, including SNS and group mail	● **The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (Information Security Policy Council, 2014)** ● Strengthening information sharing with government organizations and system vendors, etc. ● Cross-sector exercises for ensuring business continuity ● Building a platform for evaluation and authentication of such systems as control systems used by critical infrastructure, in compliance with international standards	● Measures for malicious smartphone applications ● Information Security Awareness Month 【**February**】, Founding a Cyber Security Day ● **New Information Security Outreach and Awareness Program (Information Security Policy Council, 2014)** ● Promotion of investment in security by small and medium-sized businesses, through incentives such as tax systems ● Measures by IT-related businesses including notifying malware infection to individuals by ISPs ● Ensuring the traceability of cyber crimes, such as by examining the way to store logs
Vigorous Cyberspace (Fundamentals)	● **New Information Security Human Resource Development Program** (Information Security Policy Council, 2014) ● **Information Security Research and Development Strategy (Revised)** (Information Security Policy Council, 2014)		
World-leading Cyberspace (international strategy)	● Japan-US ● Japan-UK ● Japan-India ● Japan-ASEAN ● Japan-EU ● Japan-China-Korea		*1 Promoting international measures related to vulnerabilities, threats, and attacks in cyberspace. Participation by government organizations and CSIRTs from countries such as the US, Germany, the UK, and Japan. *2 Sharing best practices for the protection of critical infrastructure, exchanging information on measures such as international cooperation. Participated by government officials in charge of protecting critical infrastructure from countries such as the US, the UK, Germany, and Japan
	● **International Strategy on Cybersecurity** (Information Security Policy Council, 2013)		
	● Conferences on International Rulemaking in Cyberspace		
	● IWWN (*1)	● MERIDIAN (*2) *(2014 in Japan)*	●Joint awareness raising activities【**October**】
Organizational Reform	● **Strengthening NISC functions**		

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



Critical Infrastructure（13 Sectors）

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

Added in May 2014

Coordination and Cooperation by NISC

Critical Infrastructure Sector-Specific Ministries

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

Related Organizations etc.

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

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

- (1) Maintaining security principles
- (2) Enhancing information sharing systems
- (3) Incident response team
- (4) Risk management
- (5) International cooperation

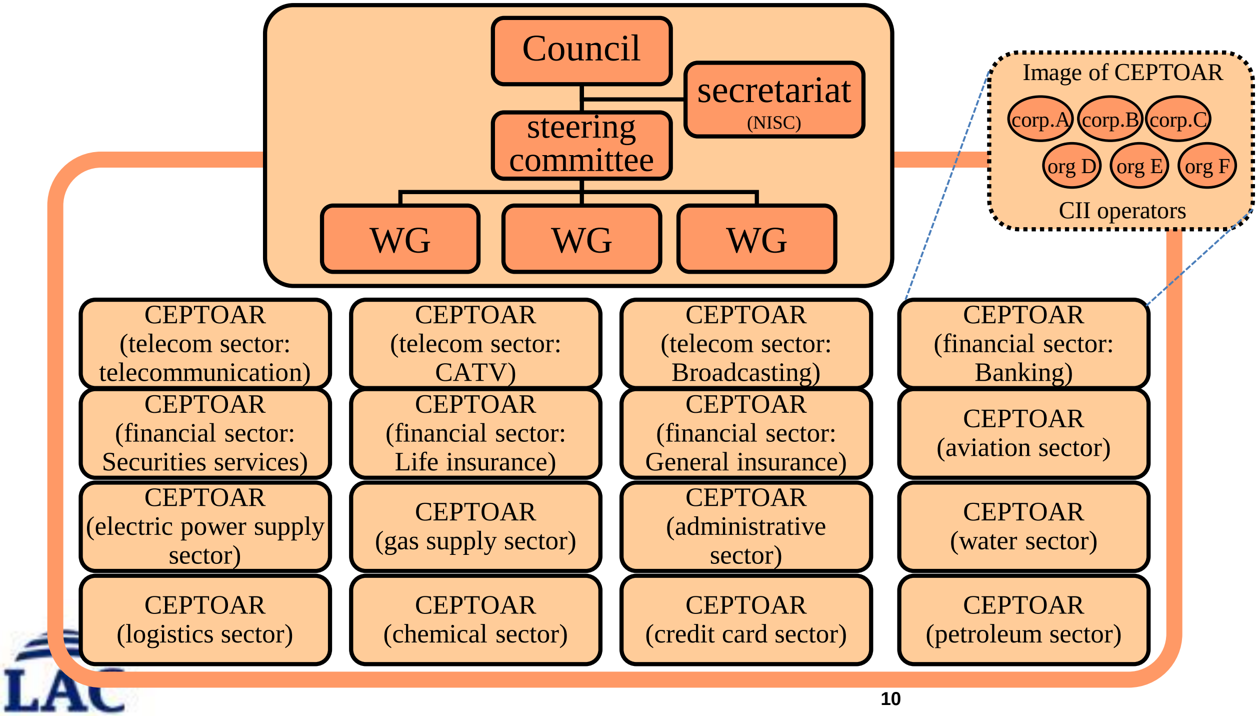
Information Sharing among CIIP Players

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
(NISC)
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

International Strategy on Cybersecurity Cooperation (October 2013)

[Priority Areas]

1. Implementation of dynamic responses to cyber incidents

Building a mechanism for international cooperation and partnership for global response to expanding cyberspace

1) Enhancing multi-layered mechanism for information sharing

2) Appropriate response to cybercrime

2. Building up "fundamentals" for dynamic response

Raising the cybersecurity standard of basic capability and response mechanisms at the global level

1) Support for building a global framework for cyber hygiene

2) Promotion of awareness-raising activities

3) Enhanced research and development through international cooperation

3. International rulemaking for cybersecurity

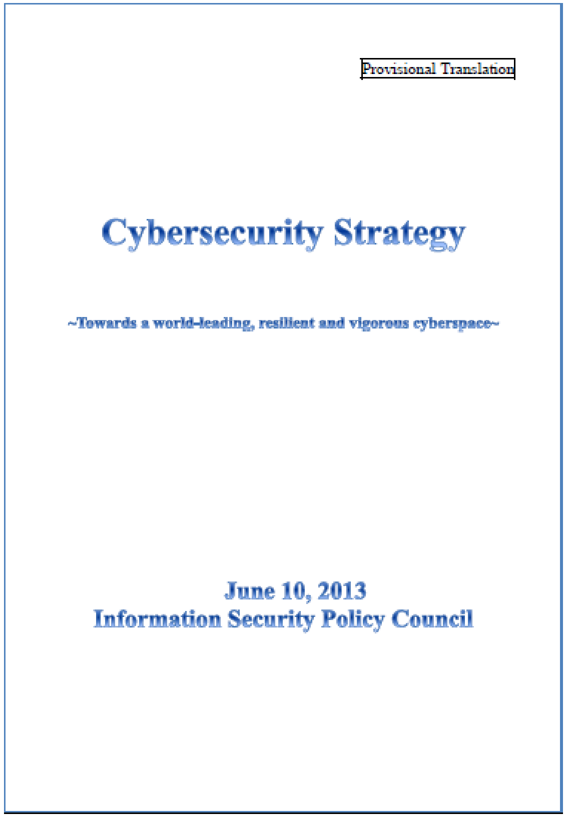
Promoting international rulemaking for ensuring stable use of cyberspace

1) Formulation of international standards of technology

2) International rulemaking

Recent Efforts on Cybersecurity Strategy (Summary)

" Cybersecurity Strategy "
(June 2013)



Provisional Translation

Cybersecurity Strategy

~Towards a world-leading, resilient and vigorous cyberspace~

June 10, 2013
Information Security Policy Council

"Resilient" Cyberspace
- Strengthening protection -

- Issued Common Standards for Information Security Measures for the Government Agencies (2014 edition) (May 2014)
- Issued The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (May 2014)

"Vigorous" Cyberspace
- Building fundamentals -

- Issued New Information Security Human Resource Development Program (May 2014)
- Issued Information Security Research and Development Strategy (Revised) (July 2014)

"World-leading" Cyberspace
- International Strategy -

- Issued "International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity (October 2013)
- ASEAN-Japan Commemorative Summit Meeting (held in December 2013)

Organizational Reform

- Issued Annual Report on Cybersecurity (July 2014)
- Strengthening the function of NISC

Main Points of “CYBERSECURITY BASIC ACT” (Outline)

1. General Provisions

1 Objectives

2 Definitions: Cybersecurity

For the purposes of this Act, the term “Cybersecurity” shall mean that necessary measures are taken: for safety management of information, such as prevention against the leakage, disappearance, or damage of information which is stored, sent, transmitted, or received by electronic, magnetic, or other means unrecognizable by natural perceptive function (hereinafter referred to as “electro-magnetic means”); and for guarantee of the safety and reliability of information systems and information communication networks (including necessary preventive measures against unlawful activities toward electronic computers through information network or storage media for information created by electro-magnetic means), and that those states are appropriately maintained.

3 Basic principles

① From the aspect of ensuring the free flow of information through the maintenance of the Internet and other advanced information communication networks and the utilization of Information and Communications Technology is critical to enjoying benefit from the freedom of expression, enabling the creation of innovation, improving economic and social vitality, and so on; the promotion of the cybersecurity policy shall be carried out with intent to produce active responses to cyber threats through cooperation among multiple stakeholders, including the Central and local governments and critical infrastructure providers .

② The promotion of the cybersecurity policy shall be carried out with intent to raise awareness of each citizen about cybersecurity and invite his/her voluntary action, to prevent any damage caused by cyber threats, and to positively and steadily promote actions to establish resilient systems which can quickly recover from damage or failure.

③ The promotion of the cybersecurity policy shall be carried out with intent to positively promote the maintenance of the Internet and other advanced information and communication networks and the establishment of a vital economy and society through the utilization of information communication technology.

④ From the aspect of combatting cyber threats, a common concern of the international community, and with recognition that our national economic and social activities are conducted in close international interdependence, the promotion of the cybersecurity policy shall be carried out with intent to play a leading role in an internationally coordinated effort for the creation and development of an international normative framework for cybersecurity.

⑤ The policy shall be carried out in consideration of the basic principles of the IT Basic Law.

2. Cybersecurity Strategy

1 The Government shall decide the Cybersecurity Strategy(CSS)

2 The Prime Minister shall request a cabinet decision on the proposed CSS.

3 The Government shall report the CSS to the Diet and endeavor to take necessary measures including a budget, within the national fiscal limits

etc.

3. General Policy

1 Assurance of cybersecurity at national administrative organs

2 Promotion of voluntary measures of cybersecurity at critical infrastructure providers

3 Promotion of voluntary activities of private enterprises and educational organizations

4 Cooperation with multiple stakeholders, and so forth

5 Cybercrime control and prevention of damage spread

6 Response to matters of great concern to national security

⑥ The promotion of the cybersecurity policy shall be carried out with intent to be careful not to wrongfully violate citizen’s rights.

4-8 Responsibilities of the central gov., local gov.,critical infrastructure providers etc.

9 Endeavors of citizen

10 Legal measures

11 Development of administrative organs

3. General Policy (continued)

7 Enhancement of industrial development and international competitiveness

8 Promotion of R&D

9 Reservation of human resources

10 Promotion and development of Education/ learning

11 Promotion of international cooperation

4. Cybersecurity Strategic Headquarters

1 For the purpose of executing the policies concerning cybersecurity effectively and comprehensively, Cybersecurity Strategic Headquarters (hereinafter Headquarters) shall be established under the Cabinet.

⇒ for other matters stipulated, including HQs tasks, organization, and authority, please see the next page.

5. Miscellaneous

1 Effective date

This act shall come into effect on the day of its promulgation. 2 (Cybersecurity Strategy) and 4 (Cybersecurity Strategic HQs) shall come into effect on the date stipulated by a cabinet order, which shall not exceed a year from the promulgation date.

2 Preparation of legislative measures required for appropriate assignment of the HQ administrative affairs to the Cabinet Secretariat

① The Government shall take necessary measures including legislation of the National Information Security Center (NISC) as part of the Cabinet secretariat.

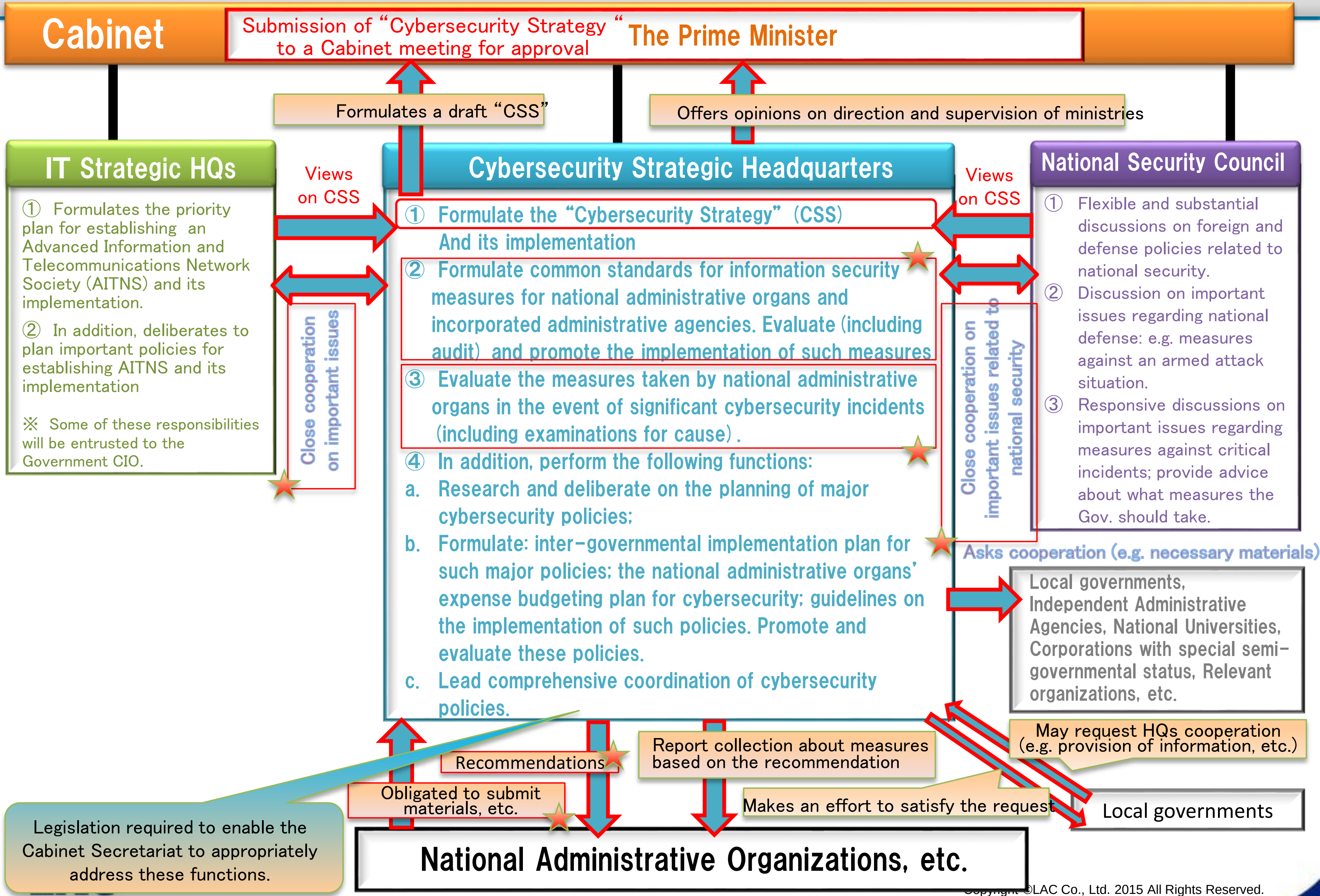
② The Government shall consider and take necessary legal and financial measures for fixed term appointments of specialists in the Cabinet secretariat, monitoring and analysis of illegal activities against governmental information systems through IC networks, the full preparation of a workforce system and equipment necessary for liaison with domestic and international organizations for cybersecurity issues.

3 Consideration

The Government shall broadly consider measures for strengthening the capability to protect critical infrastructure in the event of cybersecurity incident correspond to a state of emergency .

4 Partial revision of the IT Basic Law

Cybersecurity Basic Act



Cabinet

Submission of "Cybersecurity Strategy " to a Cabinet meeting for approval

The Prime Minister

Formulates a draft "CSS"

Offers opinions on direction and supervision of ministries

IT Strategic HQs

① Formulates the priority plan for establishing an Advanced Information and Telecommunications Network Society (AITNS) and its implementation.

② In addition, deliberates to plan important policies for establishing AITNS and its implementation

※ Some of these responsibilities will be entrusted to the Government CIO.

Views on CSS

Close cooperation on important issues

Cybersecurity Strategic Headquarters

① Formulate the "Cybersecurity Strategy" (CSS) And its implementation

② Formulate common standards for information security measures for national administrative organs and incorporated administrative agencies. Evaluate (including audit) and promote the implementation of such measures

③ Evaluate the measures taken by national administrative organs in the event of significant cybersecurity incidents (including examinations for cause) .

④ In addition, perform the following functions:

a. Research and deliberate on the planning of major cybersecurity policies;

b. Formulate: inter-governmental implementation plan for such major policies; the national administrative organs' expense budgeting plan for cybersecurity; guidelines on the implementation of such policies. Promote and evaluate these policies.

c. Lead comprehensive coordination of cybersecurity policies.

Views on CSS

Close cooperation on important issues related to national security

National Security Council

① Flexible and substantial discussions on foreign and defense policies related to national security.

② Discussion on important issues regarding national defense: e.g. measures against an armed attack situation.

③ Responsive discussions on important issues regarding measures against critical incidents; provide advice about what measures the Gov. should take.

Asks cooperation (e.g. necessary materials)

Local governments, Independent Administrative Agencies, National Universities, Corporations with special semi-governmental status, Relevant organizations, etc.

May request HQs cooperation (e.g. provision of information, etc.)

Local governments

Makes an effort to satisfy the request

Report collection about measures based on the recommendation

Recommendations

Obligated to submit materials, etc.

National Administrative Organizations, etc.

Legislation required to enable the Cabinet Secretariat to appropriately address these functions.

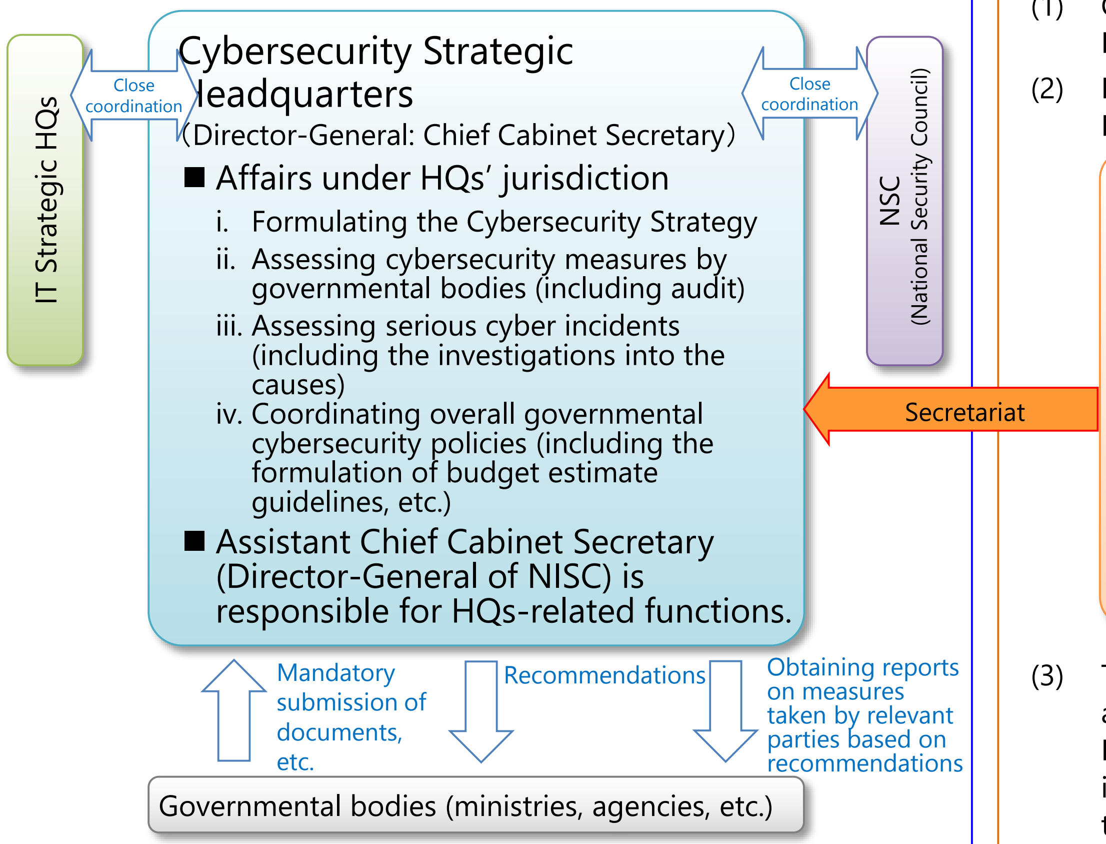
Policy Directions on the Functional Enhancement for Japan’s Cybersecurity (Summary)

1 Context

Considering the following conditions, Japan need to enhance governmental functions for cybersecurity assurance:

- As entire socio-economic activities are getting dependent on cyberspace, cyber risks have become growingly serious.
- Japan is building “the world’s most advanced IT use-based society” as one of the major pillars of the Growth Strategy of Japan.
- Japan’s international partner countries have been also actively enhancing governmental functions for cybersecurity assurance.
- Japan must strengthen cybersecurity for the Tokyo Olympic and Paralympic Games in 2020.

2 Enactment of the Basic Act on Cybersecurity



IT Strategic HQs

Close coordination

Cybersecurity Strategic Headquarters
(Director-General: Chief Cabinet Secretary)

- Affairs under HQs’ jurisdiction
  - i. Formulating the Cybersecurity Strategy
  - ii. Assessing cybersecurity measures by governmental bodies (including audit)
  - iii. Assessing serious cyber incidents (including the investigations into the causes)
  - iv. Coordinating overall governmental cybersecurity policies (including the formulation of budget estimate guidelines, etc.)
- Assistant Chief Cabinet Secretary (Director-General of NISC) is responsible for HQs-related functions.

Close coordination

NSC
(National Security Council)

Secretariat

Mandatory submission of documents, etc.

Recommendations

Obtaining reports on measures taken by relevant parties based on recommendations

Governmental bodies (ministries, agencies, etc.)

3 Policy for the functional enhancement of Japan’s promotion system

(1) Cybersecurity Strategic HQs replaces Information Security Policy Council’s functions.

(2) By the Order for Organization of the Cabinet Secretariat, NISC is legislated as an organization as follows:

National Center of **I**ncident Readiness and **S**trategy for **C**ybersecurity (NISC)

- Affairs under NISC’s jurisdiction
  - i. GSOC* functions
  - ii. Investigations into the causes of serious cyber incidents
  - iii. Audit, consultation, etc., to governmental bodies for cybersecurity assurance
  - iv. Program planning and overall coordination

* Government Security Operation Coordination team

- Assistant Chief Cabinet Secretary is designated as Director-General of NISC

(3) Taking into account the operational status of the HQs affairs, the preparation for the Tokyo Olympic and Paralympic Games, and cyber-related situations, e.g. increasing cyber threats, etc., the Government continues to examine necessary measures such as supplemental legislative provisions.

Issues under consideration regarding NISC in line with the legislative organizational arrangements

In line with the legislative organizational arrangements by the Act, and in view of the Tokyo Olympic and Paralympic Games in 2020, the Government shall consider necessary measures for the following issues regarding NISC as soon as possible.

(1) Upgrading GSOC functions

- Upgrading its organizational structure, equipment, and facilities for the new GSOC systems

(2) Enhancing comprehensive analysis capabilities

- Enhancing comprehensive analysis capabilities on the cybersecurity policies of foreign countries, the trends in cyber threats, and the technologies used in cyber attacks
- Quantitative and qualitative improvement of highly skilled cybersecurity experts with profound knowledge/experiences

(3) Increasing domestic and overseas information gathering capacity

For providing advanced incident information gathering function and advisory functions for the governmental bodies, the incorporated administrative agencies, and CII operators, etc.,

- Developing and expanding public-private partnerships
- Making NISC's internal organizational arrangement and capacity building

(4) Advancing international collaboration

- Improving functions as the national contact point for international cybersecurity issues by building close partnership with emergency response organizations

(5) Developing and recruiting human resources

- Sharing cybersecurity knowledge and experiences from NISC to other governmental ministries/agencies through the intergovernmental personnel exchanges, etc.
- Appointing highly skilled experts in the private sector as NISC officials by promoting fixed term assignments & personnel exchanges, etc.

JSOC (Japan Security Operation Center)