



**National center of Incident readiness and  
Strategy for Cybersecurity**

# Cybersecurity Strategy in Japan

April 24, 2017

Tomoo YAMAUCHI

Counsellor

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

# 3 Words to Bring Back from Today's Presentation

1. “2015”

2. The Cybersecurity Strategy

3. “2020”

# Overview of Today's Presentation

1. Historic Framework of Cybersecurity Policy:  
Before the Legislation of the Basic Act

2. The Legislation of the Basic Act on Cybersecurity:  
Explaining the Current Framework

3. Cybersecurity Strategy

4. Current Issues in Individual Topics

# 1. Historic Framework of Cybersecurity Policy: Before the Legislation of the Basic Act

- History of Cybersecurity Policy
- Recent Notable Cyberattacks/incidents

# 2. The Legislation of the Basic Act on Cybersecurity: Explaining the Current Framework

# 3. Cybersecurity Strategy

# 4. Current Issues in Individual Topics

# History of Cybersecurity Policy

## 2000: Dawn

- ☐ Defacement of Government Website (Jan. 2000)
- IT Security Office (Feb. 2000-)

## 2005: Launch

- National Information Security Center (Apr. 2005-)
- Information Security Policy Council (May 2005-)

## 2015: Institutionalization

- The Basic Act on Cybersecurity (Jan. 2015)
- The Cybersecurity Strategy (Sep. 2015)

## 2016: We Are Here

Basic Framework

Individual Measures

Basic Strategy

Annual Plan

Gov.

CII



# Recent Notable Cyberattacks/incidents

- ❑ Complicated and sophisticated threat: both domestically and internationally
- ❑ Call for heightened level of cybersecurity framework

## Domestic

- Mitsubishi Heavy Industries (Sep. 2011)
- Benesse Corp. (Jul. 2014)
- Japan Pension Service (Jun. 2015):  
Targeted Attack
- Several Gov. Agencies (Nov. 2015-):  
DDoS Attack
- JTB (Jun. 2016)

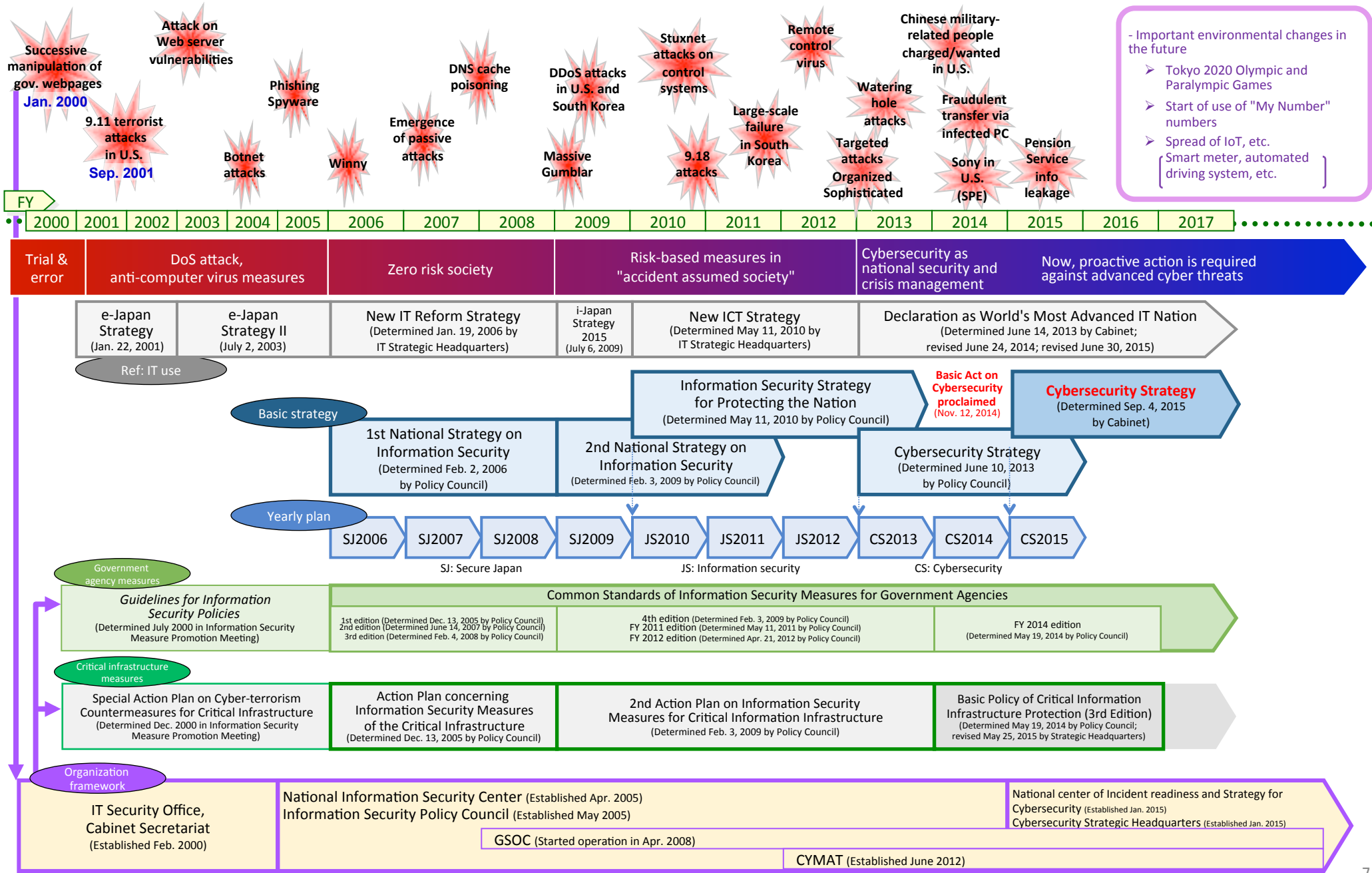
And more...

## International

- Sony Pictures Entertainment (Nov. 2014)
- German Parliament (May 2015)
- U.S. Office of Personnel  
Management(OPM) (Jun. 2015)
- Ukraine Power Grid (Mar. 2016)
- World Anti-Doping Agency (WADA) (July  
2016)

And more...

# History of Cybersecurity Measures



## Increased IT dependency

PC



Spread in many workplaces and homes connecting Internet.

(end of 2014: diffusion rate PC:78.0% Internet 82.8%)  
※2015 ICT White paper (MIC)

smartphone



Penetration rate increases 6.6 times  
 (end of 2010: 9.7% → end of 2014:64.2%)

※2015 ICT White paper (MIC)

Vehicle



Each vehicle has 100 or more computers and operated by more than 10 million lines of software code

Smartmeter

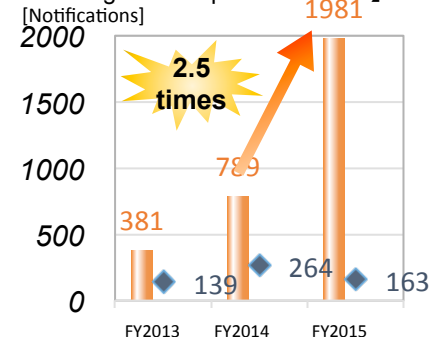


Electric power industries have started installation

- Tokyo area: planned to install 27 millions of smart meters by FY 2020
- Kansai area: planned to install 13 millions of smart meters by FY2022

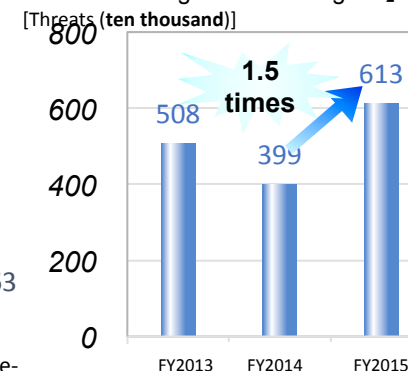
## trend of Cyber attacks

【Number of notifications against suspicious e-mails】



# of notification against suspicious e-mails  
 # of notification issued by GSOC sensor

【Number of threats to government organs】



# of threats to government organizations observed by GSOC sensor

## Cyber attacks that might be state-sponsored



Korea (Apr. 2013)

Occurred major cyber attacks to CII (Finance and broadcasting)  
 Korean authority announced that the attack was conducted by North Korea.



US (Dec. 2014)

Occurred cyber attack to Sony Pictures Entertainment.  
 US government blamed North Korea for the attack, and treated this as national security issue.

## Toward Tokyo 2020

- Festival amid attention of the world, NO Down time must be guaranteed.
- During 2012 Olympic Paralympics games in London, 200 million cyber attack observed
- UK government started the preparation for Cyber attacks 6 years prior to the 2012 games

**For the response of cyber threat and more resilient cybersecurity,  
 the Basic Act on Cybersecurity is enacted and put into effect.**

(Promulgated on 12<sup>th</sup> of Nov, 2014. Put into effect on the 9<sup>th</sup> of Jan. 2015)



1. Historic Framework of Cybersecurity Policy: Before the Legislation of the Basic Act

2. The Legislation of the Basic Act on Cybersecurity: Explaining the Current Framework

- Summary of the Basic Act
- Cybersecurity Headquarters
- Summary of NISC: Organization Chart; GSOC, Standards for Government, etc

3. Cybersecurity Strategy

4. Current Issues in Individual Topics

# Overview of the Basic Act on Cybersecurity

## What is in the Provisions of the Basic Act?

- LEGAL definition of “Cybersecurity”

- ✓ Aims to describe common understanding of cybersecurity in legal language

- Basic Principle of Cybersecurity Policy

- Responsibilities of the Stakeholders

- ✓ National Gov.; Local Gov.; CII Operators; Business Entities; Educational/research organizations.

- The Cybersecurity Strategy

- ✓ The structure of the strategy
- ✓ Subject to Cabinet decision

- Basic Policy

- ✓ Security measures for National Gov.; CII Operators
- ✓ Governing policy in individual areas

- Cybersecurity Strategic Headquarters

- ✓ Composition of HQ
- ✓ Authorities of HQ
- ✓ Relation with other agencies

# Overview of the Basic Act on Cybersecurity

What has changed with the Basic Act?

(1) Clear and Strengthened Legal Background of the Organization

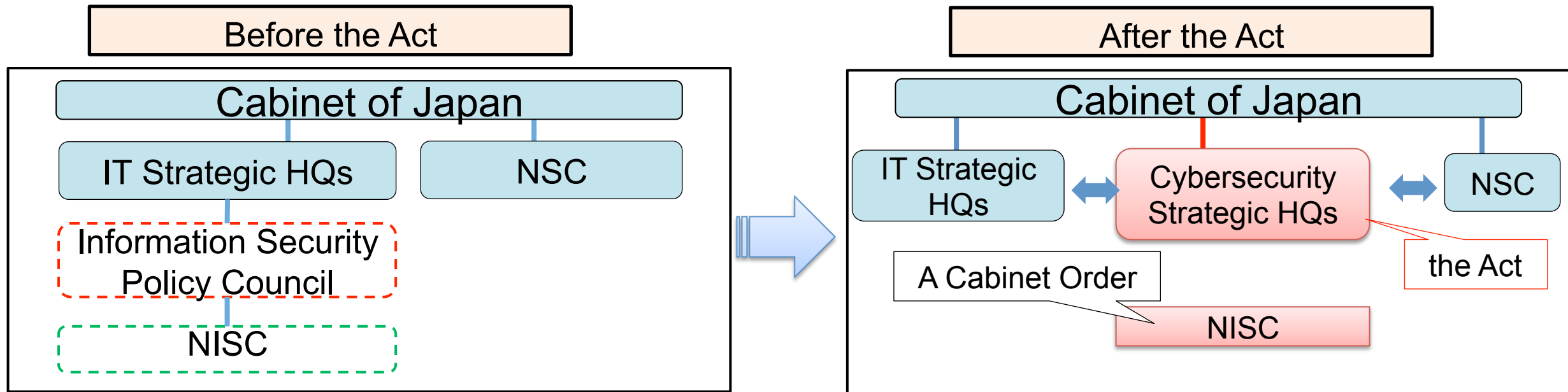
(2) Strengthened Authority of HQ

(3) Status of the Cybersecurity Strategy

# Overview of the Basic Act on Cybersecurity

What has changed with the Basic Act?

## (1) Clear and Strengthened Legal Background of the Organization



✓ Cybersecurity Strategic HQs as independent HQ

# Overview of the Basic Act on Cybersecurity

What has changed with the Basic Act?

## (2) Strengthened Authorities of the HQ

Before the Act

◆ All the activities based on agreements with other governmental bodies

✓ Cybersecurity audit: Self Audit

✓ Incident analysis: NISC provides supports to other governmental bodies on request basis



After the Act

◆ Mandatory reports from other governmental bodies  
◆ Send formal recommendation to other governmental bodies

✓ Cybersecurity audit: 3rd Party Audit by NISC  
• Management audit  
• Penetration test

✓ Incident analysis: NISC has authority to conduct cause investigation in serious incidents

# Overview of the Basic Act on Cybersecurity

What has changed with the Basic Act?

## (3) The Cybersecurity Strategy

Before the Act

The Cybersecurity Strategy (June 2013)

- ◆ Adopted by the Information Security Policy Council

- ✓ Binds only the member of the Council
- ✓ No authority to enforce the execution of the Strategy

After the Act

The Cybersecurity Strategy (Sep. 2015)

- ◆ Adopted as a Cabinet Decision
- ◆ Reported to the National Parliament

- ✓ Binds ALL the Gov. Agencies
- ✓ The HQs may enforce the Strategy via authorities of mandatory reporting and formal recommendations

# Current Framework of Cybersecurity Policy

Cabinet

IT Strategic HQs

Cybersecurity Strategic Headquarters

NSC

Chair:	Chief Cabinet Secretary
Deputy Chair:	Minister in charge of the Cybersecurity Strategic Headquarters
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
	Minister in charge of Information Technology (IT) Policy
	Minister in charge of the Tokyo Olympic and Paralympic Games
	Experts (7 persons)

Relevant Org.

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

Government Organizations

Ministries responsible for  
Critical Infrastructure

Ministries Participating in the  
HQs

Local Gov.

Close Cooperation

Close Cooperation

Submit Infos.

Request Cooperation

Recommendation

Cooperation

# Establishment of National center of Incident readiness and Strategy for Cybersecurity (NISC): Jan 9, 2015

## Cybersecurity Strategic Headquarters

(General Manager: Chief Cabinet Secretary)

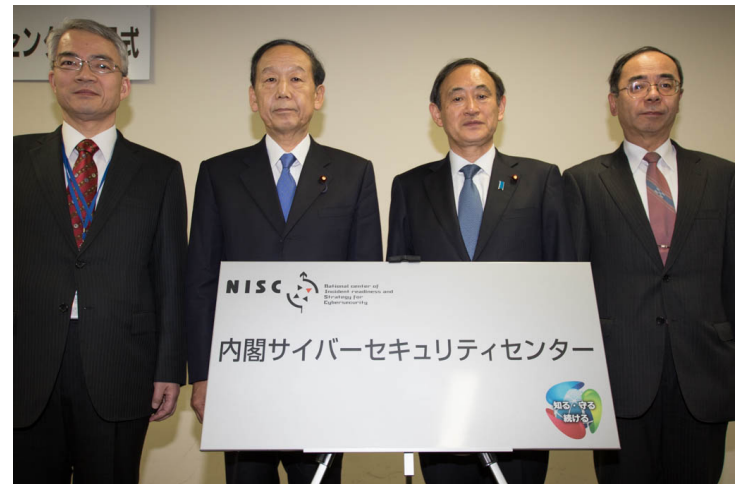
Assistant Chief Cabinet Secretary takes charge of clerical work associated with the Cybersecurity Strategic Headquarters

Secretariat

## National center of Incident readiness and Strategy for Cybersecurity

(Manager: Assistant Chief Cabinet Secretary (Responsible for SR&CM))

- National center of Incident readiness and Strategy for Cybersecurity is placed in charge of cleric work relating to:
  1. Management of GSOC (\*1)
  2. Cause investigations
  3. Auditing and others
  4. Cybersecurity related projects, planning, and general coordination



(\*1) Government Security Operation Coordination team



# 3 Words to Bring Back from Today's Presentation

## 1. “2015”

- ✓ “2015” is the year launching the current framework under The Basic Act on Cybersecurity

## 2. The Cybersecurity Strategy

## 3. “2020”

1. Historic Framework of Cybersecurity Policy: Before the Legislation of the Basic Act

2. The Legislation of the Basic Act on Cybersecurity: Explaining the Current Framework

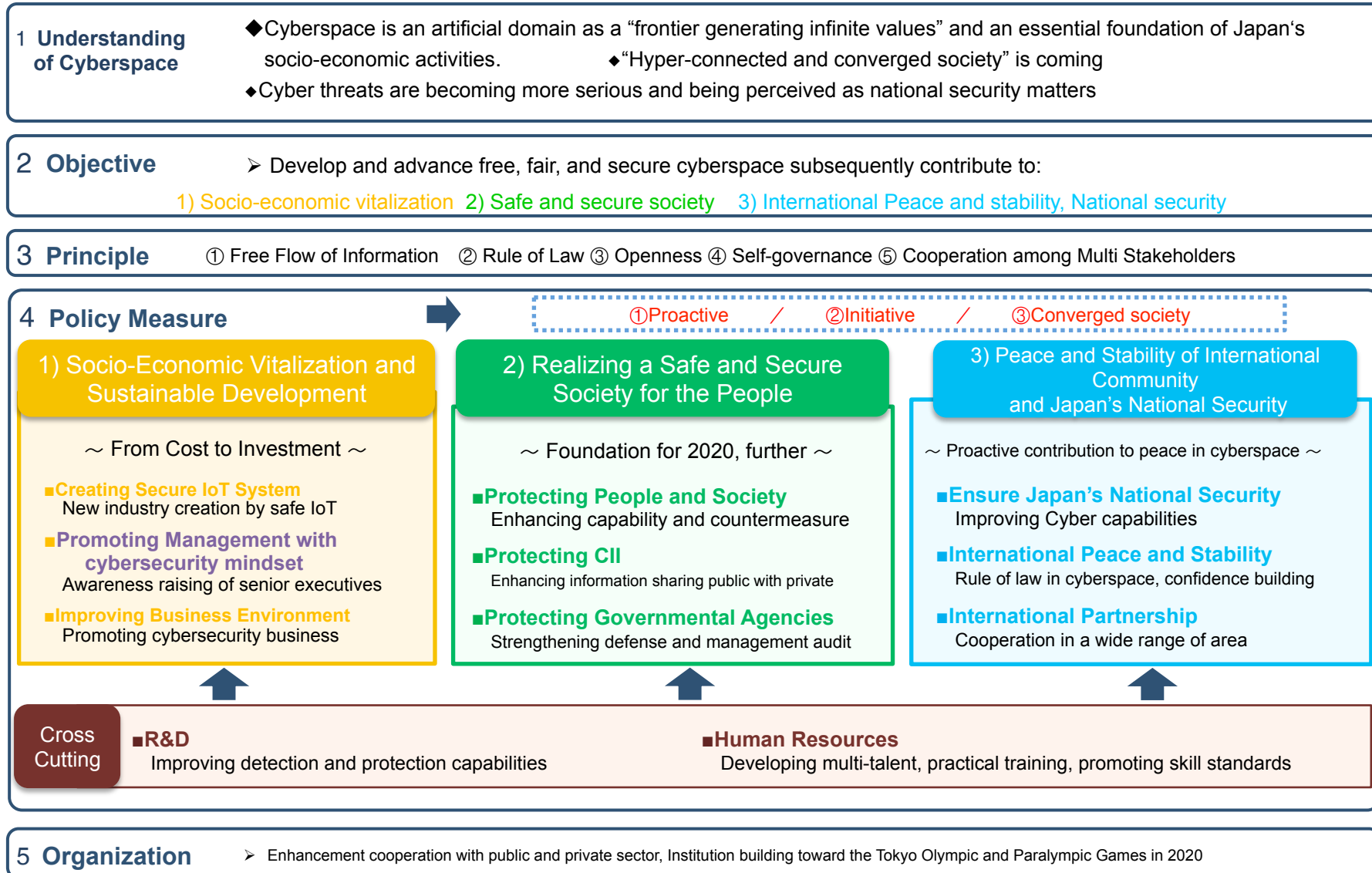
3. Cybersecurity Strategy

- Framework of the Strategy
- Annual Plan for FY2016

4. Current Issues in Individual Topics

# Cybersecurity Strategy

Below is the summary of the Cybersecurity Strategy. However, it is too SMALL to see...



# Cybersecurity Strategy [Cabinet Decision, September 2015]

## 1 Understanding of Cyberspace

- ◆ Cyberspace is an artificial domain as a “frontier generating infinite values” and an essential foundation of Japan’s socio-economic activities.
- ◆ “Hyper-connected and converged society” is coming
- ◆ Cyber threats are becoming more serious and being perceived as national security matters

## 2 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 Principle

- ① Free Flow of Information; ② Rule of Law; ③ Openness; ④ Self-governance; and ⑤ Cooperation among Multi Stakeholders



These sections established governing principle of cybersecurity policy

# Cybersecurity Strategy [Cabinet Decision, September 2015]

## 4 Policy Measure

Approachs: ①Proactive / ②Initiative / ③Converged society

1) Socio-Economic Vitalization and Sustainable Development

2) Realizing a Safe and Secure Society for the People

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

Cross Cutting

■R&D

■Human Resources

## 5 Organization

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



These sections established comprehensive map of individual measures

# 3 Words to Bring Back from Today's Presentation

1. “2015”

2. The Cybersecurity Strategy

- ✓ Japanese government adopted the Cybersecurity Strategy
- ✓ This strategy is setting leading policy and comprehensive framework

3. “2020”

1. Historic Framework of Cybersecurity Policy: Before the Legislation of the Basic Act

2. The Legislation of the Basic Act on Cybersecurity: Explaining the Current Framework

3. Cybersecurity Strategy

4. Current Issues in Individual Topics

- IoT: General Framework
- Expanding Scope of NISC: Pension case; Revision of the Basic Act; expand to Government Affiliated Agencies
- CIIP: Current Action Plan; Revision
- International Coordination: G7 WG, GGE
- Workforce/HR
- Toward Tokyo 2020

# Socio-Economic Vitalization and Sustainable Development

## Governing Principle: From Cost to Investment

### ■ **Creating Secure IoT System**

- New industry creation by safe IoT

### ■ **Promoting Management with cybersecurity mindset**

- Awareness raising of senior executives
  - ✓ Encouraging enterprises to report their cybersecurity efforts to the market
  - ✓ Supporting information sharing between the private and the public sectors, and within the private sector

### ■ **Improving Business Environment**

- Promoting cybersecurity business



# “General Framework for Secured IoT Systems”, Aug. 2016 by

NISC

## ■ Determination of 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 26<sup>th</sup> Aug. 2016 by NISC

# Realizing a Safe and Secure Society for the People

Governing Principle: Foundation for 2020, further

## ■ **Protecting People and Society**

- Enhancing capability and countermeasure

## ■ **Protecting CII**

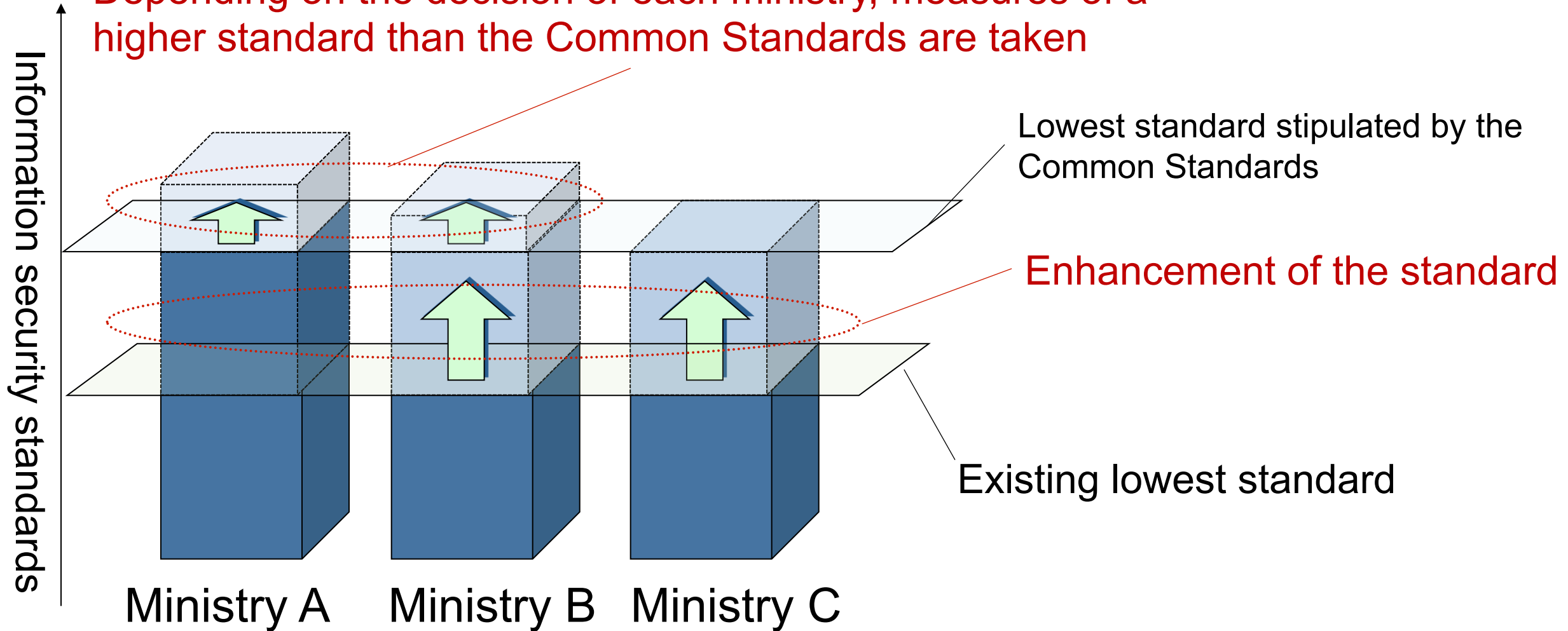
- Enhancing information sharing public with private

## ■ **Protecting Governmental Agencies**

- Strengthening defense and management audit

# Common Standards (base line for governmental body security policies)

Depending on the decision of each ministry, measures of a higher standard than the Common Standards are taken



# Cyberattack against Japan Pension Service (May 2015)

- Personal data of 1.25 million people leaked following cyberattack
- Targeted attack was the method of cyberattack
- Cybersecurity Strategic Headquarters issued analysis of the incident in August 2015



## Incident Handling Process and Procedures

- ✓ Improving incident handling process and procedures

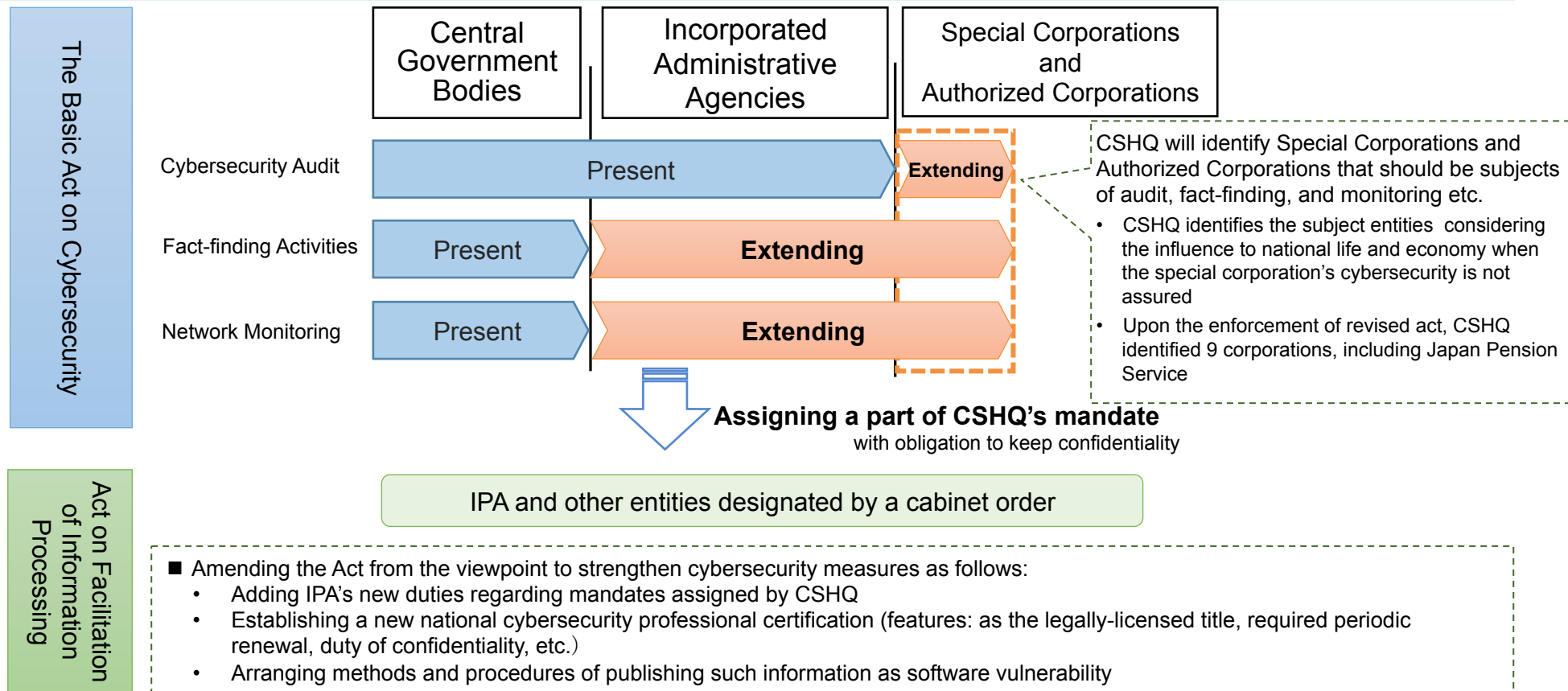
## Strengthening cybersecurity of the System

- ✓ Separation of system containing critical information from the Internet
- ✓ Aggregation of the Internet Access

# Amendment of the Basic Act on Cybersecurity Basic Act

Based on the lessons learned in such cases as Japan Pension Service case, the Diet passed the draft amendment of the Basic Act on Cybersecurity and other related laws in order to drastically strengthen cybersecurity measures of government bodies & related organizations

- Extending the scope of network monitoring, cybersecurity audit, and fact-finding activities
- Assigning a part of CSHQ's mandate to IPA and other entities

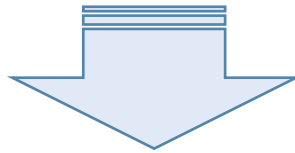


# Ideas behind the Revision of the Basic Act

## Government Agencies

- ✓ Government will take direct measures to ensure cybersecurity  
e.g. Network monitoring; audit

Expanded



## Government Agencies

+

## Government Affiliated Organizations<sup>(\*)</sup>

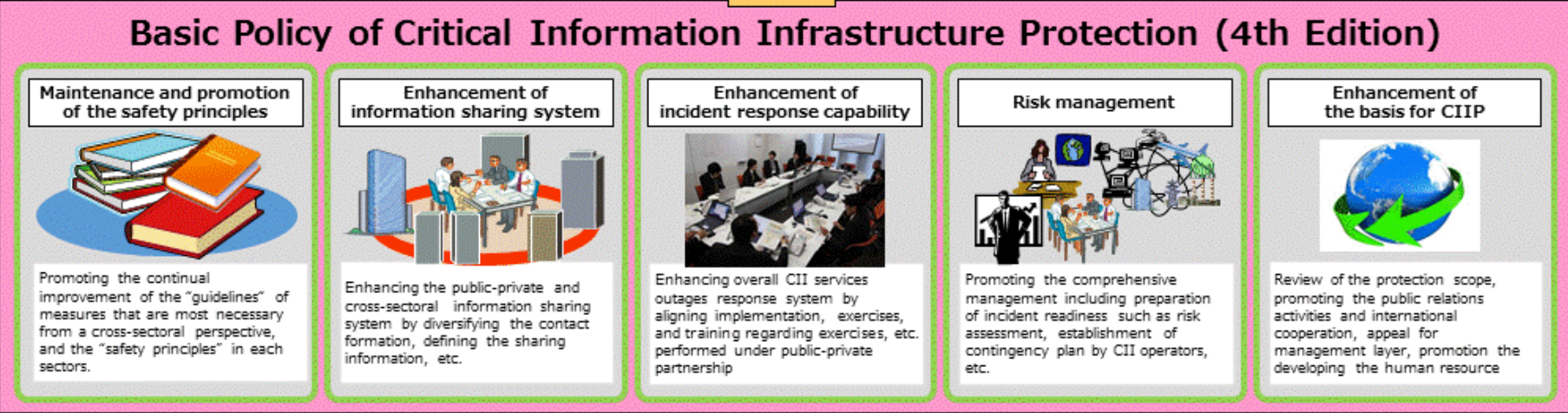
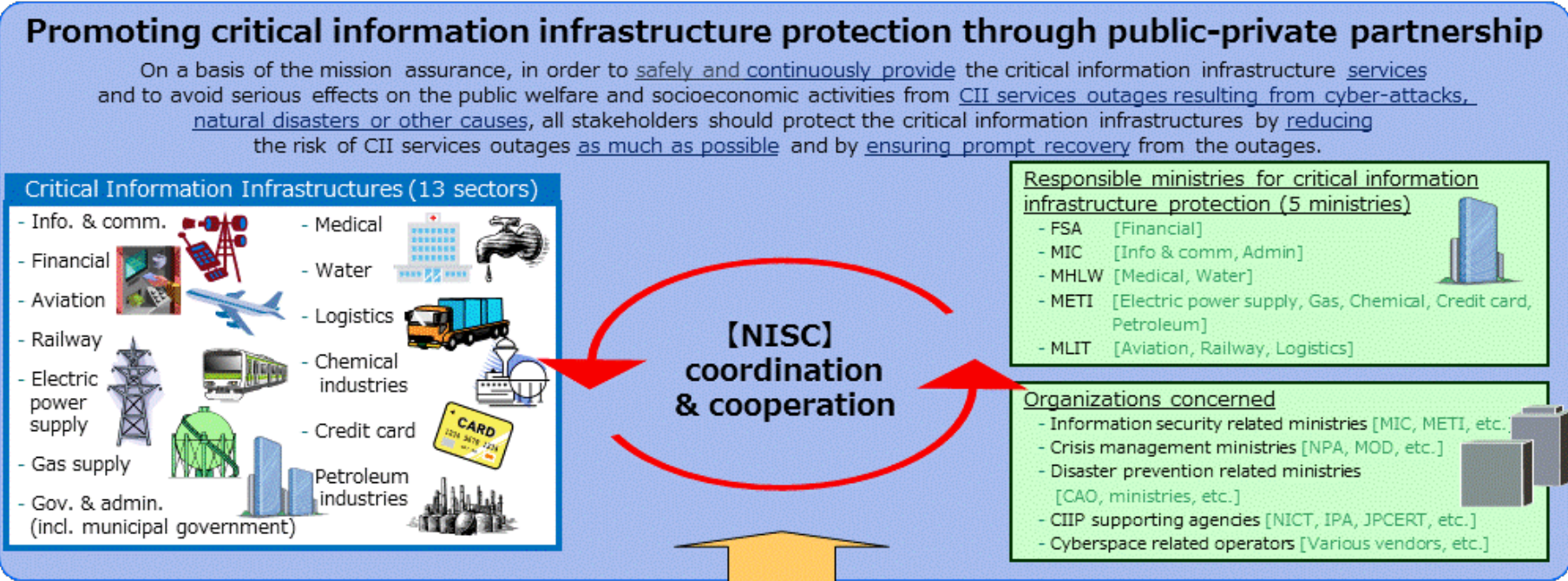
(\*)Incorporated Administrative Agencies; Special Corporations; and Authorized Corporations

## Other Organizations

- ✓ Each organizations are expected take actions to ensure cybersecurity on a voluntary basis
- ✓ Government will assist them
- ✓ CII operators will be in a special framework

# Basic Policy of Critical Information Infrastructure Protection (4th Edition)

Below is the summary of the CII Protection Framework. Again, it is too SMALL to see...



# Points of Basic Policy of Critical Information Infrastructure Protection

## Critical Information Infrastructures: 13 Sectors

1. Information and Communications
2. Financial
3. Aviation
4. Railway
5. Electric Power
6. Gas
7. Government and Administrative Services  
(including municipal government)
8. Medical
9. Water
10. Logistics
11. Chemical
12. Credit Card
13. Petroleum

## Role of NISC

- ✓ Coordination and Cooperation among stakeholders (Operators; Government agencies; industry organizations)

## Basic Policy

- Maintenance and promotion of safety principles
- Enhancement of information sharing system
- Enhancement of incident response capability
- Risk management
- Enhancement of basis for critical information infrastructure protection



## 2. Major Points of The Basic Policy of CIIP (1/2)

### Purpose of "critical information infrastructure protection"

In order to **safely and continuously provide** the critical information infrastructure services and to avoid serious effects on the public welfare and socioeconomic activities from **CII services outages resulting from cyber-attacks, natural disasters or other causes**, all stakeholders should protect the critical information infrastructures by **reducing** the risk of CII services outages **as much as possible and by ensuring prompt recovery** from the outages.

### "Basic principles"

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

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

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

## 2. Major Points of The Basic Policy of CIIP (2/2)

### 3 . Three Main Points of Review

Review 5 Activities based on the Basic Policy from 3 Main Points below

#### ①Promotion of Leading Activities of some CII Operators (Classification)

- Promotion of the leading activities of some operators in domains such as electricity, ICT and finance that are depended by other CII Operators and cause a big impact on the society even if short IT outages occur
- Ensuring the mission assurance of entire CII operators by expanding the leading activities for other operators

#### ②Enhancement of the Information Sharing Structure Looking Toward The Olympic and Paralympic Games

- Promotion of the information sharing by diversifying the contact formation, creating the level classification of incident severity, preparing the information sharing platform, and expanding the provision of information
- Expansion of the scope of information sharing in CII domain
- Sharing the information regarding operational technology and IoT etc.
- Enhancement of the incident response capability by continuing and Improving of exercises

#### ③Promoting the Incident Readiness Based on Risk Management

Promotion of the penetration of risk management into CII operators and preparation of incident readiness including preparation of CSIRT and contingency plan in order to ensure the safe and continuous provision of CII services.

Maintenance and Promotion of The Safety Principles



Enhancement of Information Sharing System



◆ Activities based on Basic Policy

Enhancement of Incident Response Capability



Risk Management



Enhancement of The Basis for CIIP



### 4 . Duration

➤ Until 2020 Tokyo Games (Review will be summarized after the Games)

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

Governing Principle: 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

## Cyber space and International Law (GGE, June 2015)

---

*“In their use of ICTs, **States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful measures, and non-intervention in the internal affairs of States.**”*

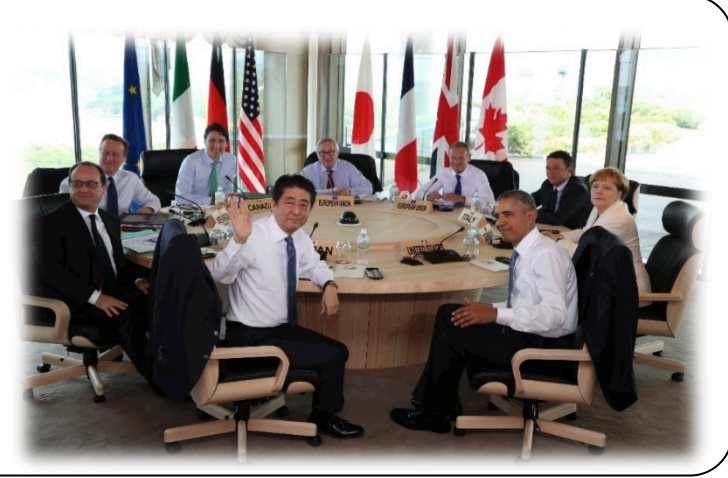
*“**Existing obligations under international law are applicable to State use of ICTs** and States must comply with their obligations to respect and protect human rights and fundamental freedoms.”*

*“**States must not use proxies to commit internationally wrongful acts using ICTs**, and should seek to ensure that their territory is not used by non-State actors to commit such acts.”*

*“**The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States**, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behavior.”*

# G7 Ise-Shima Summit (May 2016)

- G7 leaders **reaffirmed basic principles on cyberspace** and **endorsed the *G7 Principles and Actions on Cyber*** as an annex document to promote and protect an open, interoperable, reliable and secure cyberspace.
- G7 leaders **decided to establish a new G7 working group on cyber** to enhance policy coordination and practical cooperation among G7 countries to promote security and stability in cyberspace.



## G7 Ise-Shima Leaders' Declaration on Cyber (summary)

- ✓ To take decisive and robust measures in close cooperation against malicious use of cyberspace
- ✓ To reaffirm that no country should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information
- ✓ To reaffirm that international law is applicable in cyberspace.
- ✓ To promote a strategic framework of international cyber stability consisting of:
  - The applicability of existing international law to state behavior in cyberspace,
  - The promotion of voluntary norms of responsible state behavior during peacetime, and
  - The development and the implementation of practical cyber CBMs
- ✓ To promote a multi-stakeholder approach to Internet governance

# Overview of Tokyo 2020 and its circumstances

Asset owners  
(≈ prime responsibility holders)

Mission owners  
(≈ prime responsible coordinator)

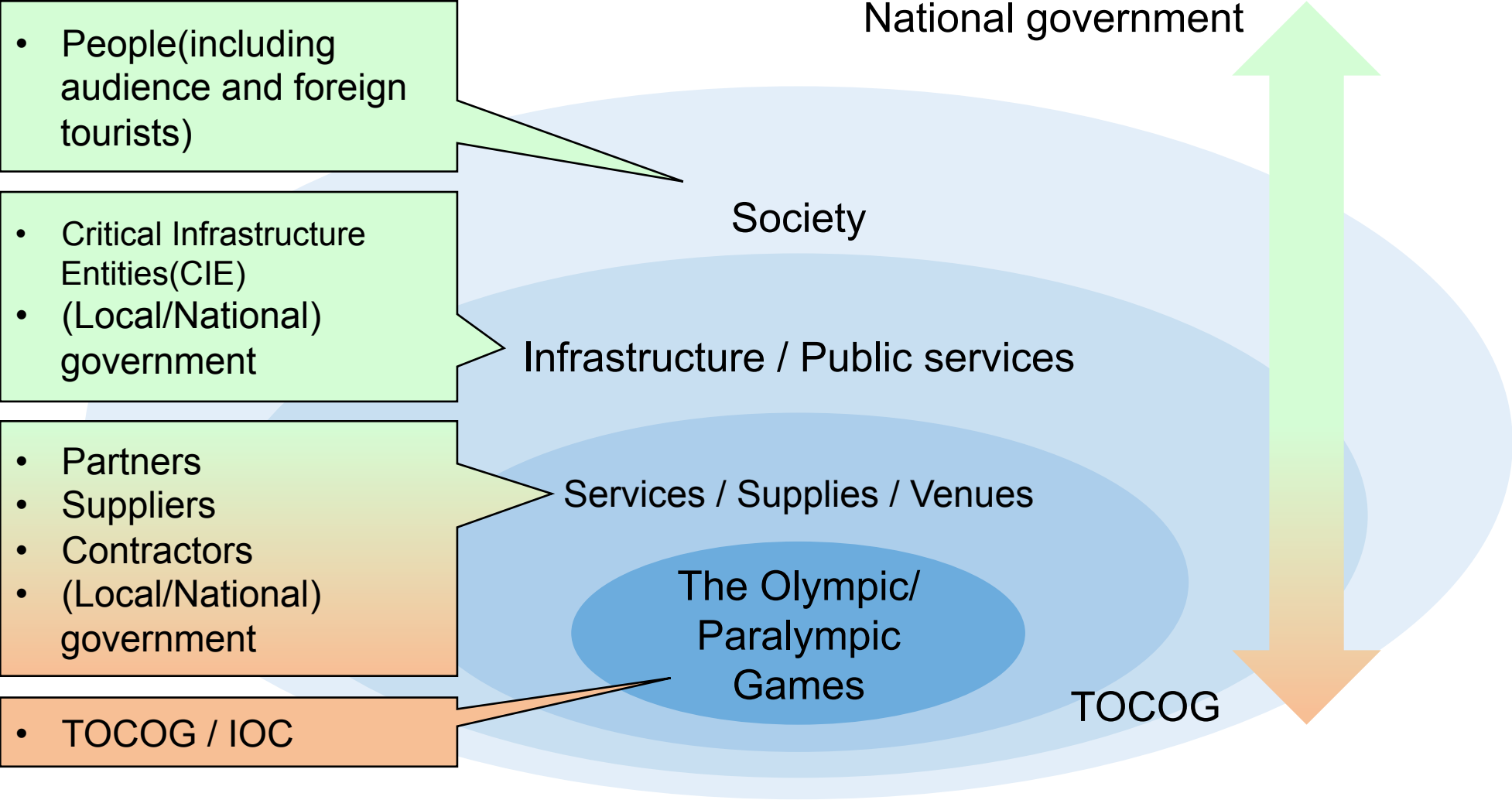
- People(including audience and foreign tourists)

- Critical Infrastructure Entities(CIE)
- (Local/National) government

- Partners
- Suppliers
- Contractors
- (Local/National) government

- TOCOG / IOC

National government



Society

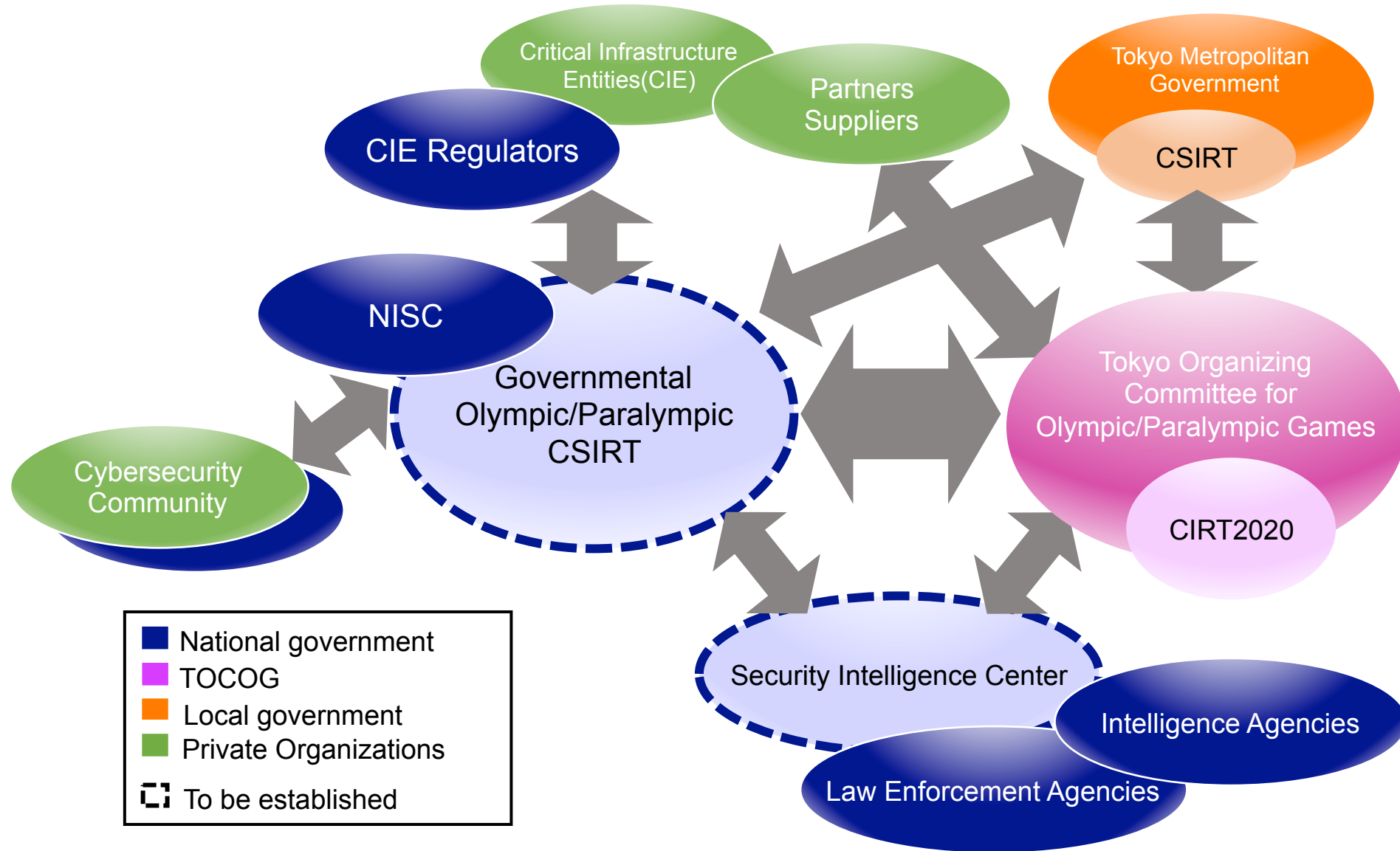
Infrastructure / Public services

Services / Supplies / Venues

The Olympic/  
Paralympic  
Games

TOCOG

# Cybersecurity stakeholders of Tokyo 2020



# Cybersecurity Measures for Tokyo 2020 Olympic/Paralympic Games

Government of Japan promotes cybersecurity measures of essential service providers for the Games based on risk assessment and discusses to establish Governmental Olympic/Paralympic CSIRT as a core organization of information sharing among stake holders.

## Summary of measures

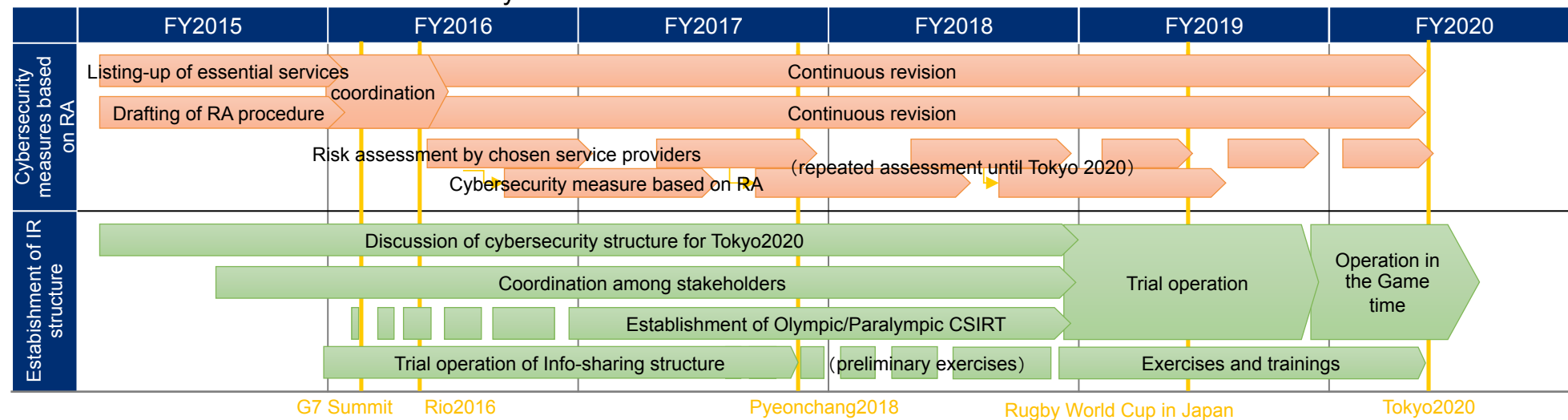
**Promotion of cybersecurity measures based on risk assessment(RA)**  
(for appropriate preparation)

**Establishment of incident response(IR) structure**  
(for quick and precise responses against incidents)

- Listing-up of essential service providers that can affect Games operation.
- Preparation of the procedure for the chosen providers' self risk assessment to promote their cybersecurity measures.

- Establishment a discussion group for Tokyo 2020 cyber security structure among the members of cybersecurity community of Japan to discuss the details.
- Trial operation of information sharing structure consist of the group members during G7 Ise-Shima Summit and Rio 2016 Olympic/Paralympic Games.

## Schedule for Tokyo 2020



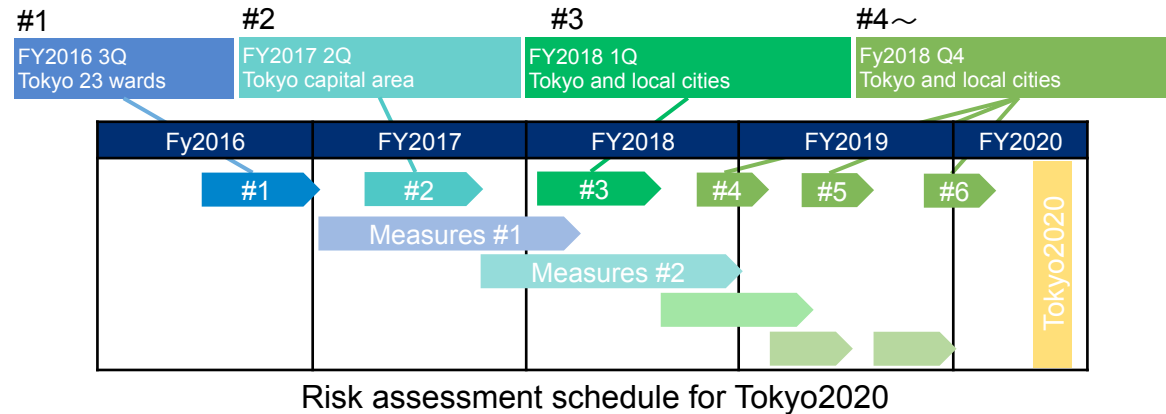


# Risk assessment for Tokyo 2020 Olympic/Paralympic Games

- Based on London2012's practices, NISC promotes risk assessment for continuous and safe provision of essential services for Tokyo 2020.
- NISC requested service providers that can affect the Games' operation to perform their self assessment in the explanation meeting.

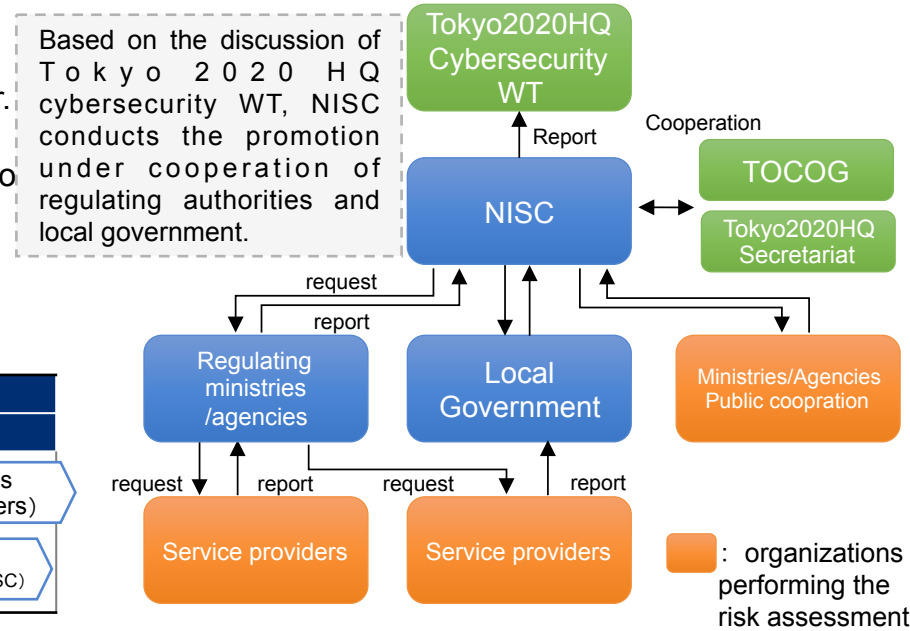
## Abstract

- NISC provided the procedure to identify, analyze and assess security risks to promote risk management.
- Based on regulators' cooperation, NISC identified essential service providers that can affect Games operation, and requested them to perform the assessment.
- Several assessments are planned until 2020.
  - Expanding of service providers
  - Brushing-up of the procedure and risk scenarios

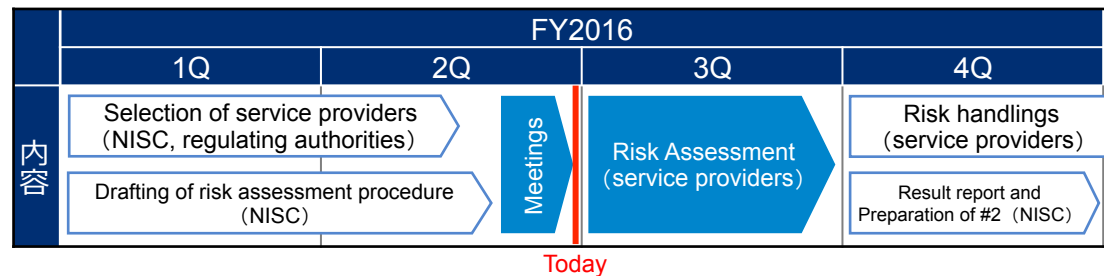


## Risk Assessment #1

- Risk Assessment #1 targets service providers in Tokyo 23 wards.
- NISC invited service providers to the explanation meeting in September. The providers were requested to perform their self-assessment until December. NISC will receive their result reports and draft the summary of the results until March 2017.
- Service providers were requested to address the identified risks by themselves



### Schedule of Risk Assessment #1



# 3 Words to Bring Back from Today's Presentation

1. “2015”

2. The Cybersecurity Strategy

3. “2020”

- ✓ “2020” is the target year for each policy
- ✓ Human resource, CII protection is important issues in FY2016

# Fishing using “Kakkoi!!” contents

“Kakkoi!!” means “Wow it’s cool!!” in Japanese.

An important factor for young people to decide their future direction

- In our “New information security public awareness raising program”
- Utilization of media familiar to the public
- As a way to appeal to every citizen, attention should be paid to the influence of media (**comics, songs etc.**) familiar to the public, and efforts in collaboration with businesses and creators dealing with these are also expected to be effective .

# Raising Awareness is important, too.

Annual Cybersecurity Month 2017 (2/1-3/18)

Enjoying Pokémon GO Safely!



2017 Cybersecurity Campaign.

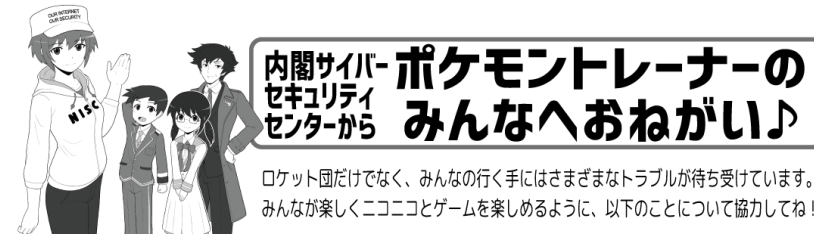
"Sword Art Online the Movie"

Story of security and VR/AR death game. Story of hero and heroine who rescue prisoners.

There are many fans in young generation and gamers.

Slogans in posters are

"We protect this world(Internet)!"  
"Be a guardian of the future!"



**1. 個人情報を守ろう**  
トレーナー登録するときは、本名とは違う、いかしたニックネームを付けましょう。ニックネームに本名がわかるものを使うと、あなたを追いかけようとする人が出てくるかも。SNSに写真を投稿するときは、家の近くのものやめておきましょう。家が特定されます。また写真にはGPS情報が付かないように設定しましょう。

**2. 偽アプリ、チートツール注意**  
人が多く集まるコンテンツは、悪いハッカーには絶好のターゲット! マルウェア(ウイルス)入りの偽アプリがあったり、攻撃のいどぐちになるチートツールも登場するでしょう。「裏技があるからこを見て!」というも民かも。また、アプリは公式ストアから正規のものを利用しましょう。

**3. お天気アプリは必ず入れよう**  
外で遊ぶゲームだからこそ、天候には十分注意しましょう! 警報を受信できるお天気アプリを必ず入れて、警報などが出た場合はハンディングはお休みしましょう。特に「特別警報」は「ただちに命を守る行動」が求められます。また海岸沿いの探索は、常に避難場所を気にかけよう。

**4. 熱中症を警戒しよう**  
炎天下を歩き回るときは「熱中症」を警戒しましょう。熱中症の症状をよく勉強して理解し、定期的に日陰での休憩や、塩分を含む水分摂取を行いましょう。水だけを飲んではダメです。帽子や日傘などは有効です。汗をかくときスマホを服の中に入れておくと湿気が入ってしまいますが、みなさんはスマホを手を持つので大丈夫です。

**5. 予備の電池を持とう**  
位置情報ゲームは常にGPS情報を利用するので、大量に電池を消費します。そのためいつもよりかなり早く電池切れになってしまいます。スマホはゲームだけでなく重要な連絡手段でもあるので、電池切れで電話ができなくなったたりしないように、予備の電池(モバイルバッテリー)や充電器を持ち歩きましょう。休憩時にコンセントを使わせてもらえるなら、きちんと許可を取ってこまめに充電を行います。無断利用はダメです。

**6. 予備の連絡手段を準備しよう**  
スマホの電池がなくなって、電話をかけられなくなった時のために、テレフォカードを持ち、公衆電話の使い方を調べておきましょう。子供たちだけで出かけるときは、迷子になってしまった時のため、出発前にパパママに全身の写真を撮ってもらっておきましょう。探しても見つからない時は、特徴を伝えてもらったりしてください。

**7. 危険な場所には立ち入らない**  
すでに開始されている国では、ゲームをやりながら歩いていて、車にひかれたり、池に落ちたり、蛇にかまれたり、強盗にあつたりという事件が起きます。地形や治安が危険な場所には立ち入らないようにしましょう。国によっては発砲事件も起きていますし、カメラを向けただけで拘束される場所もあるので海外では注意しましょう。

**8. 会おうという人を警戒しよう**  
ゲームにかこつけて会おうという人には十分に警戒してください。どうしても会わないといけないときは、おとなと一緒に行きましょう。また人気のない場所での探索は避けましょう。別の意味でのモンスターがいてもいいかもしれません。

**9. 歩きスマホは×ですよ**  
歩きスマホをしていてたくさん事故が起っています。駅のホームでは電車に接触してけがをした例もあります。歩きスマホは大変危険なのです。ゲームにはモンスターが現れるとスマホが震えるモードもあるそうですから有効活用して、震えたら立ち止まり、周囲を確認してから見るようにしましょう。自転車に乗りながらのプレイももちろんダメですよ。

Attention Reminding of "Pokémon GO"

Published just before the release of the game!

In order to enjoy the games safely especially during summer vacation

Sensational response just after the release (No.1 "♡" @twitter in JAPAN)

このチラシは改変をしない範囲で、印刷配布などに自由にお使いください。

NISC 内閣サイバーセキュリティセンター  
National Center for Cyber Security Agency  
Ministry for Digital Governance

2016/07/20 発行  
2016/07/21 修正

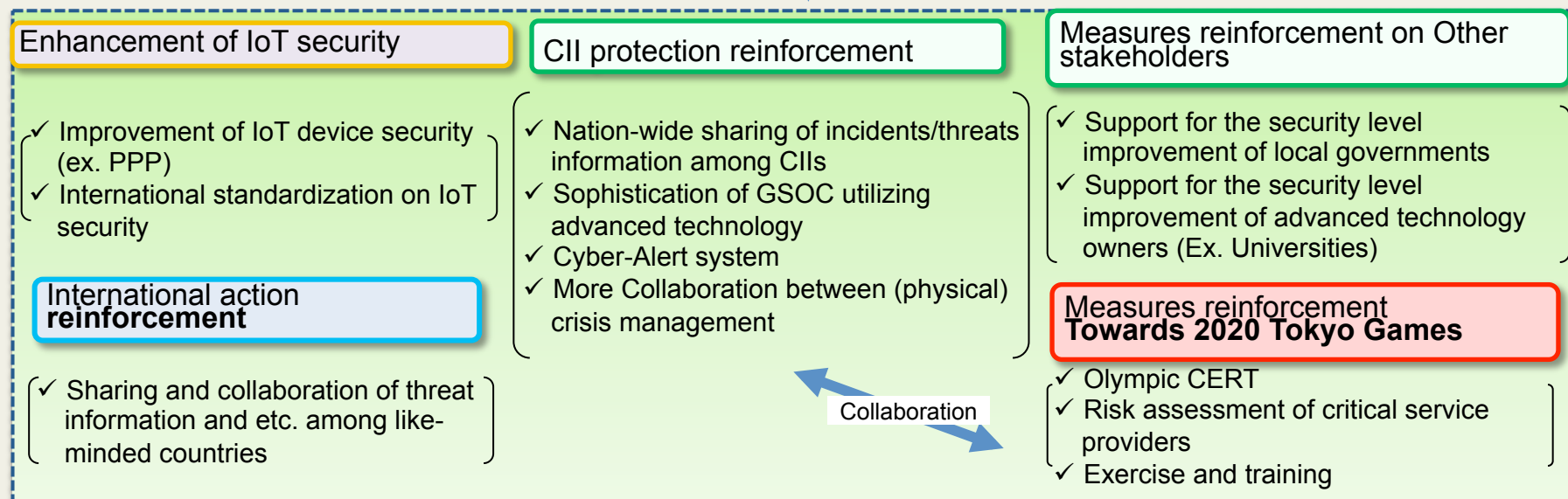
# Consideration on Cybersecurity Policy towards 2020 and beyond

[Changes]



**Reinforcement of measures required towards 2020 and beyond**

[Agendas and major consideration items]



# End of Presentation

Thank you for listening !

Please ask me if you have any questions.



**National center of Incident readiness and  
Strategy for Cybersecurity**