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
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)

### 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...
Current situation of cybersecurity

Increased IT dependency

- Spread in many workplaces and homes connecting Internet.
  (end of 2014: diffusion rate PC: 78.0% Internet 82.8%)
- Penetration rate increases 6.6 times
  (end of 2010: 9.7% → end of 2014: 64.2%)

- Smartphone
- Vehicle
- Smartmeter

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 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 12th of Nov, 2014. Put into effect on the 9th 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

Before the Act
- Cabinet of Japan
  - IT Strategic HQs
  - NSC
  - Information Security Policy Council
  - NISC

After the Act
- Cabinet of Japan
  - IT Strategic HQs
  - Cybersecurity Strategic HQs
  - NSC
  - A Cabinet Order
  - NISC

✓ 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

Cybersecurity Strategic Headquarters

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)

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

Government Organizations

Ministries responsible for Critical Infrastructure

Ministries Participating in the HQs

IT Strategic HQs

NSC

Close Cooperation

Submit Infos.

Recommendation

Local Gov.

Relevant Org.

Cooperation

Request 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

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 clerical 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...

| 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 ⑤ Cooperation among Multi Stakeholders |
| 5 Organization | Enhancement cooperation with public and private sector, Institution building toward the Tokyo Olympic and Paralympic Games in 2020 |

Cross Cutting
- R&D Improving detection and protection capabilities
- Human Resources Developing multi-talent, practical training, promoting skill standards
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

Approaches: ① Proactive / ② Initiative / ③ Converged 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
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 26th 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.

- Ministry A
- Ministry B
- Ministry C

Lowest standard stipulated by the Common Standards

Enhancement of the standard

Existing lowest standard
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

### The Basic Act on Cybersecurity

- **Central Government Bodies**
  - Cybersecurity Audit: Present
  - Fact-finding Activities: Present
  - Network Monitoring: Present

- **Incorporated Administrative Agencies**
  - Cybersecurity Audit: Present
  - Fact-finding Activities: Extending
  - Network Monitoring: Extending

- **Special Corporations and Authorized Corporations**
  - CSHQ will identify Special Corporations and Authorized Corporations that should be subjects of audit, fact-finding, and monitoring etc.
    - CSHQ identifies the subject entities considering the influence to national life and economy when the special corporation’s cybersecurity is not assured
    - Upon the enforcement of revised act, CSHQ identified 9 corporations, including Japan Pension Service

### Act on Facilitation of Information Processing

- Assigning a part of CSHQ’s mandate with obligation to keep confidentiality

#### IPA and other entities designated by a cabinet order

- Amending the Act from the viewpoint to strengthen cybersecurity measures as follows:
  - Adding IPA’s new duties regarding mandates assigned by CSHQ
  - Establishing a new national cybersecurity professional certification (features: as the legally-licensed title, required periodic renewal, duty of confidentiality, etc.)
  - Arranging methods and procedures of publishing such information as software vulnerability
Ideas behind the Revision of the Basic Act

Government Agencies

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

Other Organizations

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

Expanded

+ Government Affiliated Organizations(*)

(*) Incorporated Administrative Agencies; Special Corporations; and Authorized Corporations
Promoting critical information infrastructure protection through public-private partnership

On a basis of the mission assurance, 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 outage resulting from cyber-attacks, natural disasters or other causes, all stakeholders should protect the critical information infrastructures by reducing the risk of CII services outage as much as possible and by ensuring prompt recovery from the outage.


Promoting the continual improvement of the “Guidelines” of measures that are most necessary from a cross-sectoral perspective and the “safety principles” in each sector.

- Maintenance and promotion of the safety principles
  - Enhancing the public-private and cross-sectoral information sharing system
  - Enhancing overall CII services outage response system by diversifying the contact formation, defining the sharing information, etc.

- Enhancement of information sharing system
  - Enhancing public-private and cross-sectoral information sharing system by diversifying the contact formation, defining the sharing information, etc.

- Enhancement of incident response capability
  - Enhancing overall CII services outage response system by diversifying the contact formation, defining the sharing information, etc.

- Risk management
  - Promoting the comprehensive management including preparation of incident readiness, such as risk assessment, establishment of contingency plan by CII operators, etc.

- Enhancement of the basis for CIIP
  - Review of the protection scope, promoting the public relations activities and international cooperation, appeal for management layer, promotion the developing the human resource
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
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

<table>
<thead>
<tr>
<th>① Promotion of Leading Activities of some CII Operators (Classification)</th>
<th>② Enhancement of the Information Sharing Structure Looking Toward The Olympic and Paralympic Games</th>
<th>③ Promoting the Incident Readiness Based on Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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</td>
<td>• 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</td>
<td>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.</td>
</tr>
<tr>
<td>• Ensuring the mission assurance of entire CII operators by expanding the leading activities for other operators</td>
<td>• Expansion of the scope of information sharing in CII domain</td>
<td>• Sharing the information regarding operational technology and IoT etc.</td>
</tr>
<tr>
<td></td>
<td>• Sharing the information regarding operational technology and IoT etc.</td>
<td>• Enhancement of the incident response capability by continuing and Improving of exercises</td>
</tr>
</tbody>
</table>

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
“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.”

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2015)
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)
- People (including audience and foreign tourists)
- Critical Infrastructure Entities (CIE)
- (Local/National) government
- Partners
  - Suppliers
  - Contractors
  - (Local/National) government
- TOCOG / IOC

Mission owners
(≈ prime responsible coordinator)
- National government

Society

Infrastructure / Public services

Services / Supplies / Venues

The Olympic/Paralympic Games

TOCOG
Cybersecurity stakeholders of Tokyo 2020

- Critical Infrastructure Entities (CIE)
- NISC
- Cybersecurity Community
- CIE Regulators
- Partners Suppliers
- Tokyo Metropolitan Government
- CSIRT
- Tokyo Organizing Committee for Olympic/Paralympic Games
- CIRT2020
- Security Intelligence Center
- Law Enforcement Agencies
- Intelligence Agencies

Labels:
- National government
- TOCOG
- Local government
- Private Organizations
- To be established
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 stakeholders.

### 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)

<table>
<thead>
<tr>
<th>Schedule for Tokyo 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FY2015</strong></td>
</tr>
<tr>
<td>Cybersecurity measures based on RA</td>
</tr>
<tr>
<td>Risk assessment by chosen service providers</td>
</tr>
<tr>
<td>(repeated assessment until Tokyo 2020)</td>
</tr>
<tr>
<td>Establishment of IR structure</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>G7 Summit</td>
</tr>
</tbody>
</table>

- 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 cybersecurity 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.
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

<table>
<thead>
<tr>
<th>FY2016</th>
<th>1Q</th>
<th>2Q</th>
<th>3Q</th>
<th>4Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>内容</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1Q</td>
<td>Selection of service providers (NISC, regulating authorities)</td>
<td>Meeting</td>
<td>Risk Assessment (service providers)</td>
<td>Risk handlings (service providers)</td>
</tr>
<tr>
<td>2Q</td>
<td>Drafting of risk assessment procedure (NISC)</td>
<td></td>
<td></td>
<td>Result report and Preparation of #2 (NISC)</td>
</tr>
</tbody>
</table>

Today

### Risk assessment schedule for Tokyo2020

- FY2016
  - #1: FY2016 3Q
  - #2: FY2017 2Q
  - #3: FY2018 1Q
  - #4~: FY2018 Q4

- FY2017
  - #1: FY2017
  - #2: Measures #1
  - #3: Measures #2
  - #4: #4
  - #5: #5
  - #6: #6

- FY2018
  - #1: Tokyo 23 wards
  - #2: Tokyo capital area
  - #3: Tokyo and local cities

- FY2019
  - #4: Tokyo and local cities

- FY2020
  - #5: Tokyo and local cities

- #6: Tokyo and local cities

Based on the discussion of Tokyo 2020 HQ cybersecurity WT, NISC conducts the promotion under cooperation of regulating authorities and local government.

**Report**

Cooperation

TOKOCG

NISC

Regulating ministries/agencies

Local Government

Service providers

Ministries/Agencies

Public cooperation

Tokyo2020HQ Secretariat

Cybersecurity

WT

Report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

report

request

model

risk assessment

organizations

performing the

risk assessment

...
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 “Kakkoii!!” contents

“Kakkoii!!” 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)

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!”

Enjoying Pokémon GO Safely!

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 “retty” @twitter in JAPAN)
Consideration on Cybersecurity Policy towards 2020 and beyond

[Changes]
- Complexity
  - "Servitization" of Cyber attack
  - Increased dependence on IT in CIIs
- Coverage Expansion
  - Increase of threats on local Govs.
  - Increase of threats on advanced Technology Owners
- Globalization
  - Exponential increase and diffusion of IoT devices
  - Increase of simultaneous global cyber attacks

Reinforcement of measures required towards 2020 and beyond

[Agendas and major consideration items]
- Enhancement of IoT security
  - Improvement of IoT device security (ex. PPP)
  - International standardization on IoT security
- CII protection reinforcement
  - Nation-wide sharing of incidents/threats information among CIIs
  - Sophistication of GSOC utilizing advanced technology
  - Cyber-Alert system
  - More Collaboration between (physical) crisis management
- Measures reinforcement on Other stakeholders
  - Support for the security level improvement of local governments
  - Support for the security level improvement of advanced technology owners (Ex. Universities)
- Collaboration
  - Olympic CERT
  - Risk assessment of critical service providers
  - Exercise and training

[Schedule]
- This summer
  - Work Policy decided at Cybersecurity HQ
- by Next summer
  - Measures implementation
End of Presentation

Thank you for listening!

Please ask me if you have any questions.