Comprehensive Package of IoT Security Measures in Japan

October 9th, 2018

Taro Hashimoto

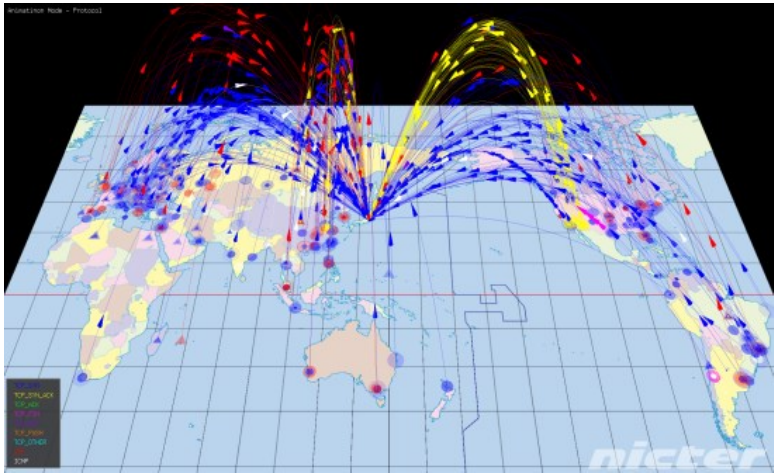
Deputy Director, Office of the Director-General for Cybersecurity,

Ministry of Internal Affairs and Communications (MIC)

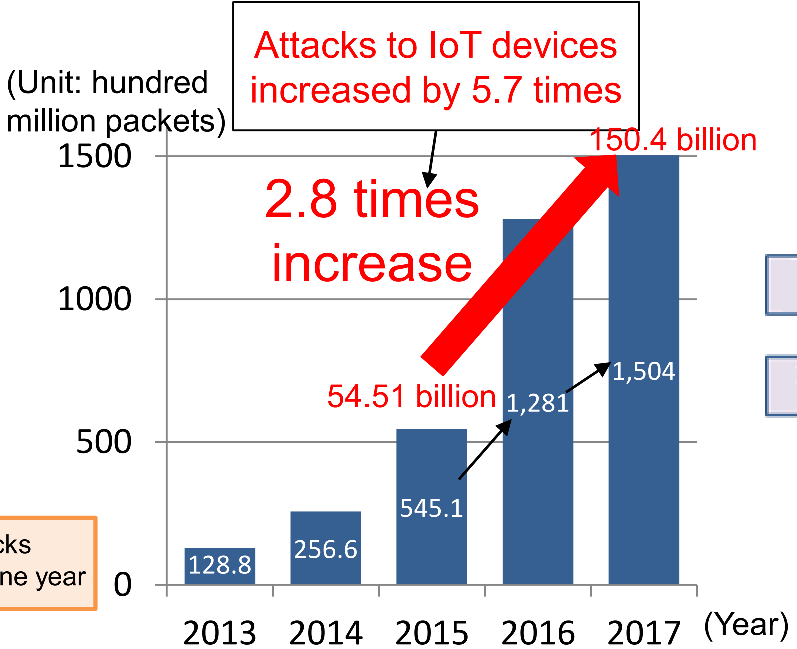
JAPAN

Attacks on IoT Devices (Observed by NICTER)

NICT(National Institute of Information and Communications Technology) is observing cyber attacks globally by monitoring 300,000+ unused IP addresses (darknet).

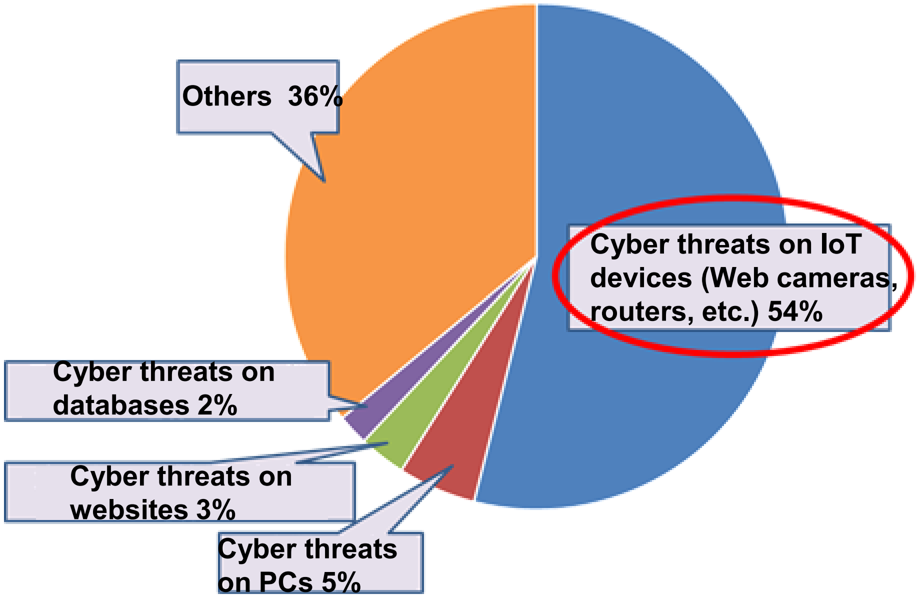


- 🟦 TCP SYN
- 🟨 TCP SYN/ACK
- 🟩 TCP ACK
- 🟪 TCP FIN
- 🟪 TCP RESET
- 🟧 TCP PUSH
- ⬜ TCP Other
- 🟥 UDP
- ⬜ ICMP



Number of cyberattacks observed by NITCER in one year

More than half were attacking on IoT devices!



Comprehensive Approach to Realize Secured IoT

(1) Establishment of systems to improve IoT vulnerability

(2) R&D

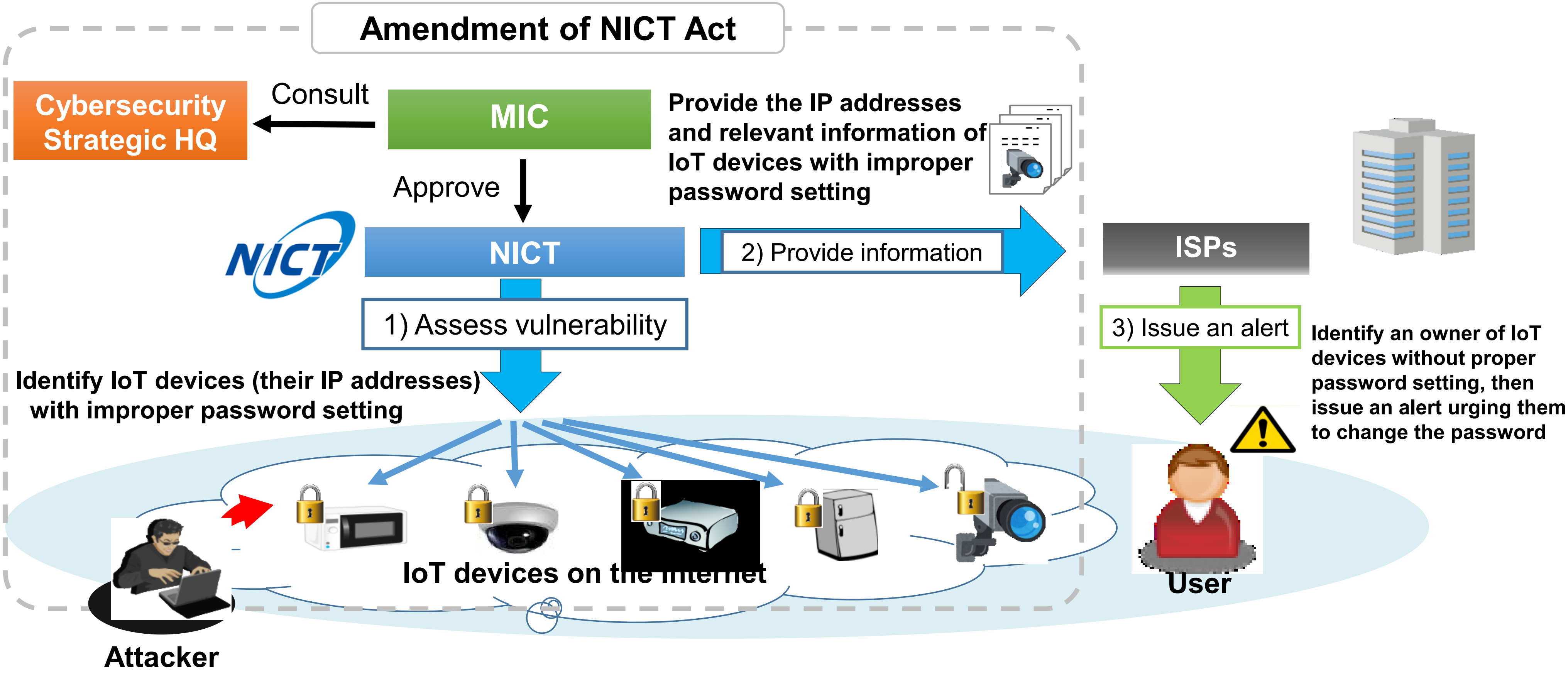
(3) Security measures in private sectors

(4) Human Resource Development

(5) International Collaboration

(1) Identify IoT Devices with Improper Password Settings

Due to the sophistication of cyber attacks using IoT devices, the amendment of the NICT act was passed in May 2018. The act enables NICT to scan IoT devices on the Internet and identify IoT devices with improper password setting (5-year temporary measure).



Amendment of NICT Act

Cybersecurity Strategic HQ

Consult

MIC

Approve

Provide the IP addresses and relevant information of IoT devices with improper password setting

NICT

1) Assess vulnerability

2) Provide information

Identify IoT devices (their IP addresses) with improper password setting

ISPs

3) Issue an alert

Identify an owner of IoT devices without proper password setting, then issue an alert urging them to change the password

IoT devices on the Internet

Attacker

User

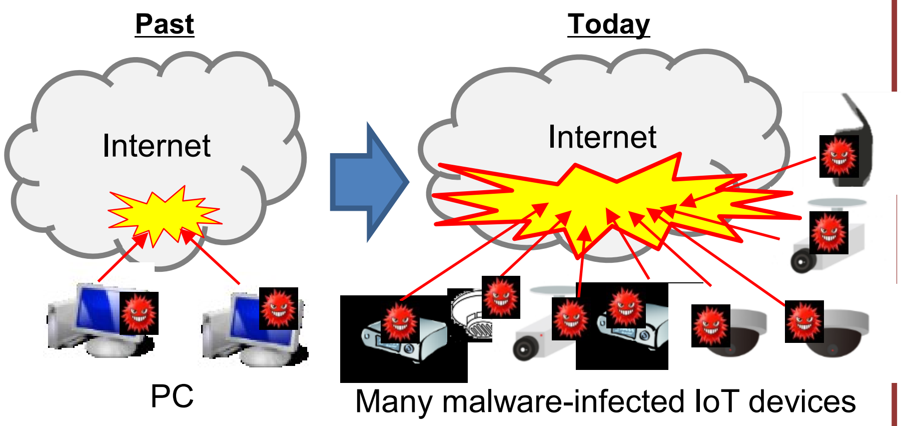
Information Sharing among Telecommunications Carriers

In May 2018, the national diet passed a bill(*) that establishes an information sharing system where a third party institution facilitates the exchange of necessary information among telecommunications carriers.

(*) Revision of Telecommunications Business Act

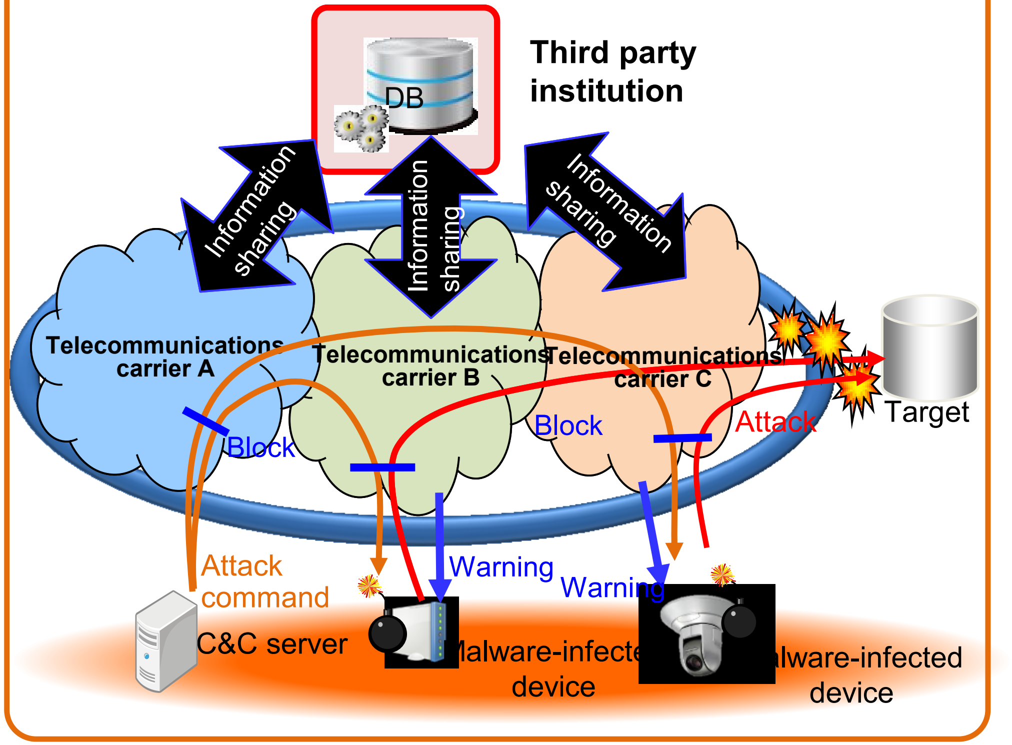
Serious internet outage increase (today)

- Cyber attacks cause internet outage.
- As IoT devices are increasing, malware-infected IoT devices which perform cyber attacks cause serious internet outage.
- A large-scale cyber attacks may take place during the 2020 Olympics and Paralympics.



Establish information-sharing system

Enabling telecom carriers to alert users and block harmful communications from C&C servers, malware-infected devices, etc by sharing information of them.

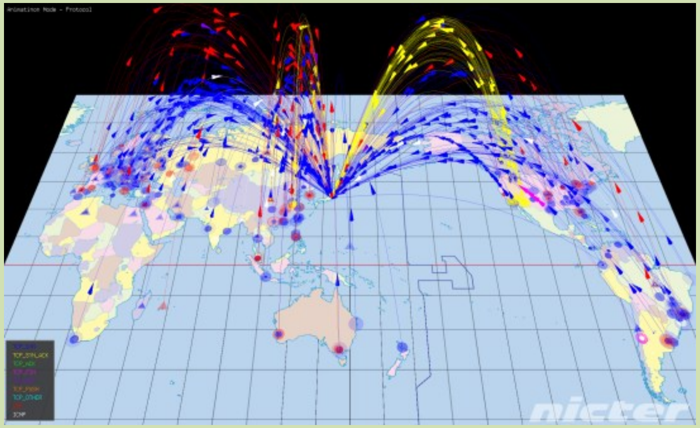


(2) R&D Activities against Indiscriminate/Targeted Attacks

NICT (National Institute of Information and Communications Technology) has been conducting R&D activities against indiscriminate and targeted cyberattacks.

(1) **NICTER** [Countermeasures against Indiscriminate attack]

- **Visualize geographical information, amount, and type of cyberattacks in real time** by observing communication in the darknet (unused IP addresses) with a sensor.
- The system based on this technology is introduced to **provide alerts to local governments infected with malware**.



Introduced to approx. 600 local governments (as of November 2017)

(2) **NIRVANA-Kai** [Countermeasures against targeted attacks]

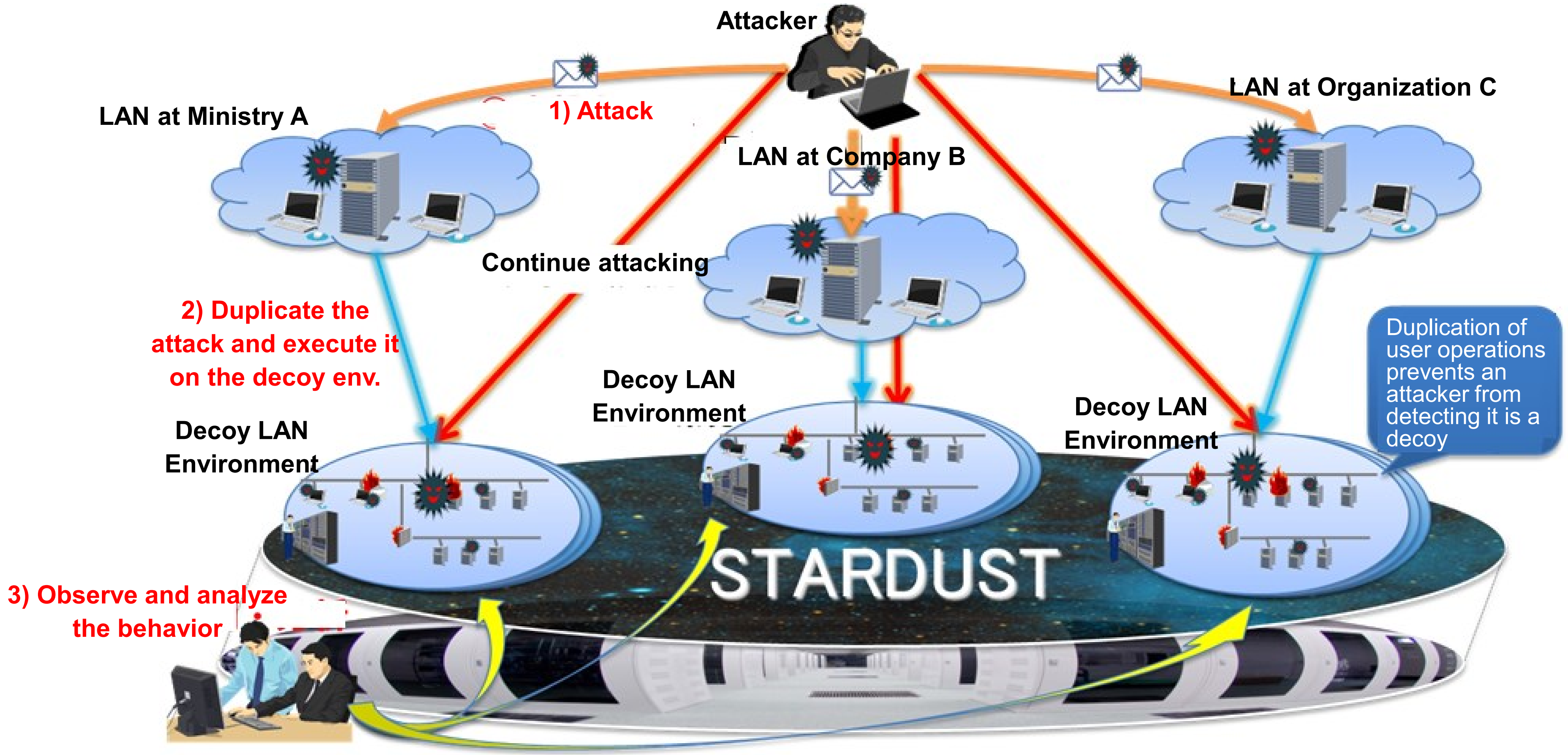
- **Visualize traffic occurred within the organization in real time** by installing the sensors in the environment.
- Further developments which enable **automatic block for abnormal communications once it is detected**

Started technology transfer (June 2015)

R&D Activities against Indiscriminate/Targeted Attacks

(3) **STAR DUST (Honeynet)**

STAR DUST is a honeynet to study targeted attacks in detail, lead by NICT. When an attacker sends malicious emails to a specific organization, the attached file is executed in “decoy environment implemented in advance" to observe and analyze the behavior.



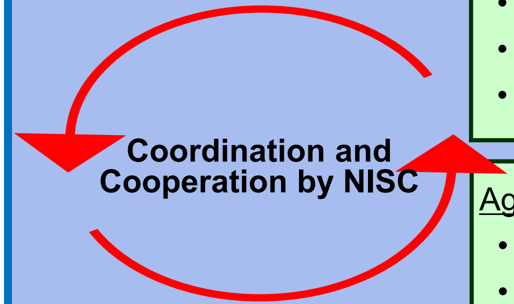
Duplication of user operations prevents an attacker from detecting it is a decoy

(3) CIIP Action Plan 4th Edition

Promotion of Critical Information Infrastructure Protection through public-private partnership

Critical infrastructure (14 fields)

- Information and Communications
- Finance
- Aviation
- Airport
- Railways
- Electricity
- Gas
- Government and Administrative Services (including local government services)
- Medical Services
- Water
- Logistics
- Chemistry
- Credit Card
- Petroleum



Coordination and Cooperation by NISC

Critical Infrastructure Sector-Specific Ministries

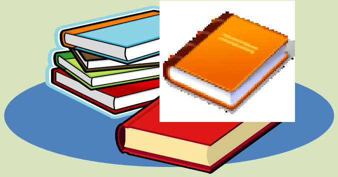
- FSA
- MIC
- MHLW
- METI
- MLIT

Agencies concerned

- Information Security Related Ministries
- Ministries Concerned with Countermeasures
- Disaster Management Ministries
- Information Security Related Organizations
- Cyberspace Related Operators

CIIP Action Plan 4th Edition

Safety standards



Information sharing system

Incident response system

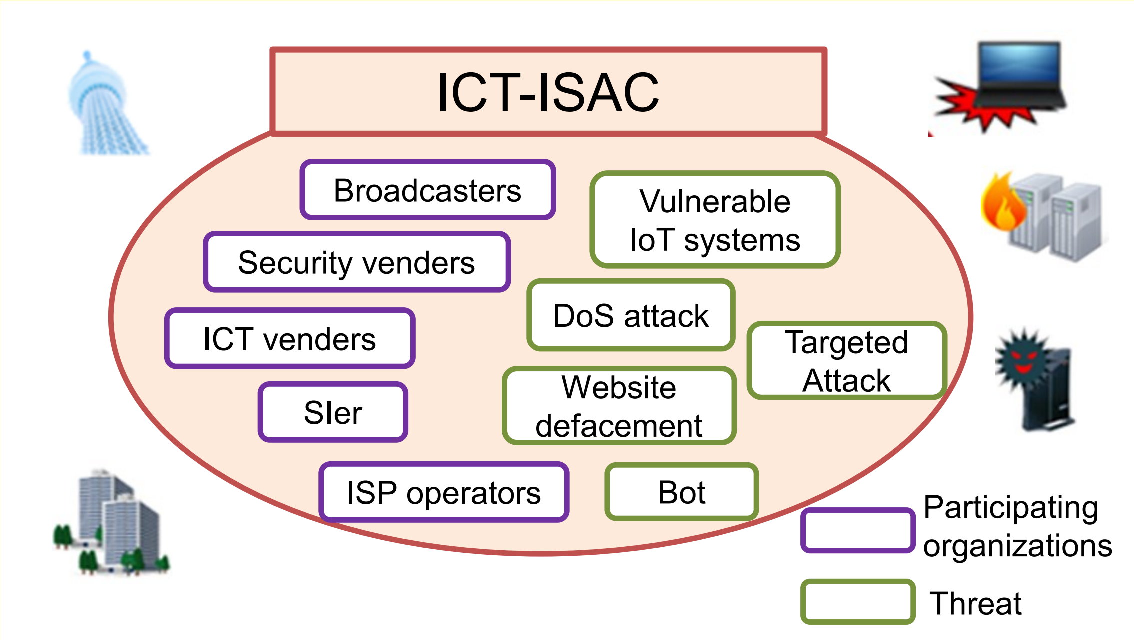
Risk management and countermeasures

Infrastructure Protection

Cooperation through ISAC

- **<u>ISAC (Information Sharing and Analysis Center)</u>** has established in each industry for the purpose of collecting, analyzing, and sharing the incident information on cyberattacks.
- **<u>Telecom-ISAC Japan has established in 2002, as the ISAC for telecom industry.</u>**
- Financial ISAC has established in 2014.
- Electricity ISAC and J-AUTO-ISAC have established in 2017.
- Broadcasters, ICT vendors, and cybersecurity vendors have participated in Telecom-ISAC Japan, which was renamed as **<u>ICT-ISAC</u>** Japan since March 2016, in order to reinforce information sharing function throughout the ICT field.

Overview of ICT-ISAC Japan



President:
Tadao Saito

Members:
38 companies, including telecommunications carriers, broadcasters, ICT vendors, security vendors, etc.

(4) Human Resource Development (National Cyber Training Center)

In order to develop cybersecurity human resource capable of practically handling sophisticated and complex cyberattacks, MIC has started the following hands-on training programs since April 2017 in the National Cyber Training Center, which is organized under the NICT.

(1) CYDER

A **CY**ber **D**efense **E**xercise with **R**ecurrence (**CYDER**) program for governmental administrations, local governments, independent administrative agencies, and critical infrastructure providers, etc.

(2) Cyber Colosseo

A cyber defense exercise for those who are in charge of cybersecurity in the organizations related to the Tokyo 2020 Olympic and Paralympic Games. (**Cyber Colosseo**)

(3) SecHack365

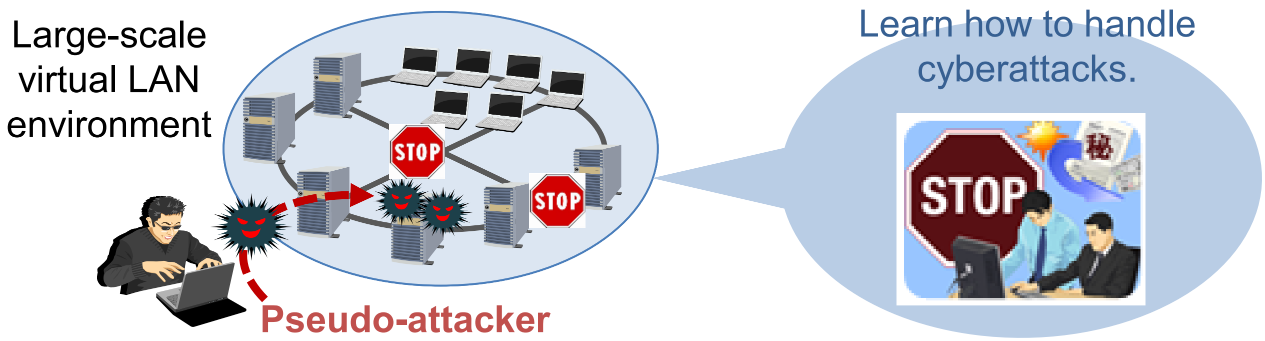
Training program for young cybersecurity innovators. (**SecHack365**)

CYber Defense Exercise with Recurrence (CYDER)

National Cyber Training Center

- ○ MIC provides **CYDER exercises**, which is conducted by NICT, **for those who are in charge of information systems in administrative organizations and critical infrastructure providers**.
- ○ **The participants are able to experience a series of incident handing** against cyberattacks, **by hands-on operation of real machines in the large-scale virtual LAN environment simulating the organizations network**.
- ○ In FY 2017, CYDER exercises were held **100 times** and a total of **3,009 trainees** were attended.

Image of exercise


Large-scale virtual LAN environment
STOP
STOP
Pseudo-attacker
Learn how to handle cyberattacks.
STOP
秘

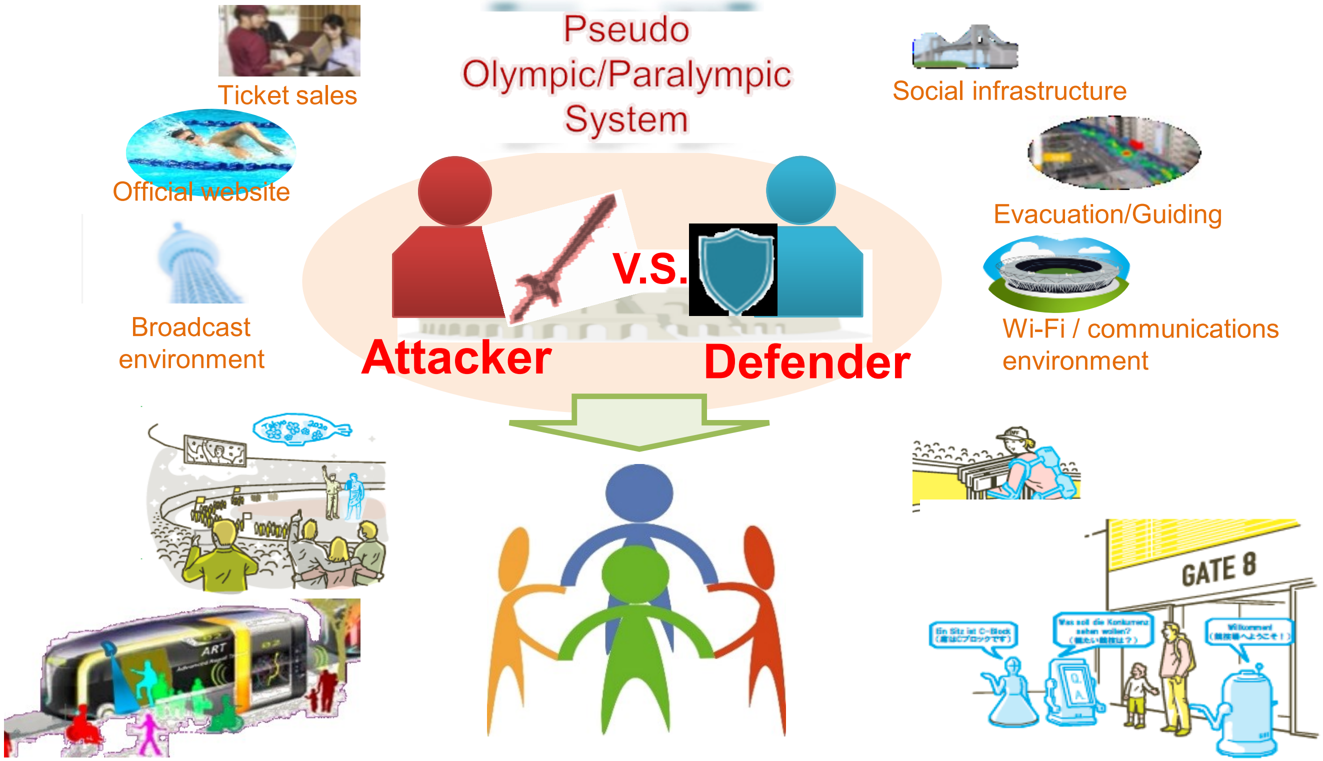
Exercise Plan for 2018

Course	Target organizations	Venue	Number of courses
Course A (Beginner)	(For all organizations)	47 prefectures	60 times
Course B-1 (Intermediate)	For local governments	11 regions	20 times
Course B-2 (Intermediate)	For governmental organizations	Tokyo	10 times
Course B-3 (Intermediate)	For critical infrastructure providers	Tokyo	10 times

Practical Cyber Exercise for the Tokyo 2020 (Cyber Colosseo)

National Cyber Training Center

- **Cyber Colosseo** exercise started February 2018 to develop human resources capable of handling advanced cyberattacks, which is conducted for those who are in charge of cybersecurity in the organizations related to Tokyo 2020 Olympic and Paralympic Games.
- At the exercise venue of the Cyber Coliseum (NICT Innovation Center at Tokyo), battle-style (attacker v.s. defender) exercise is conducted in the virtual network environment with physical machines and software.

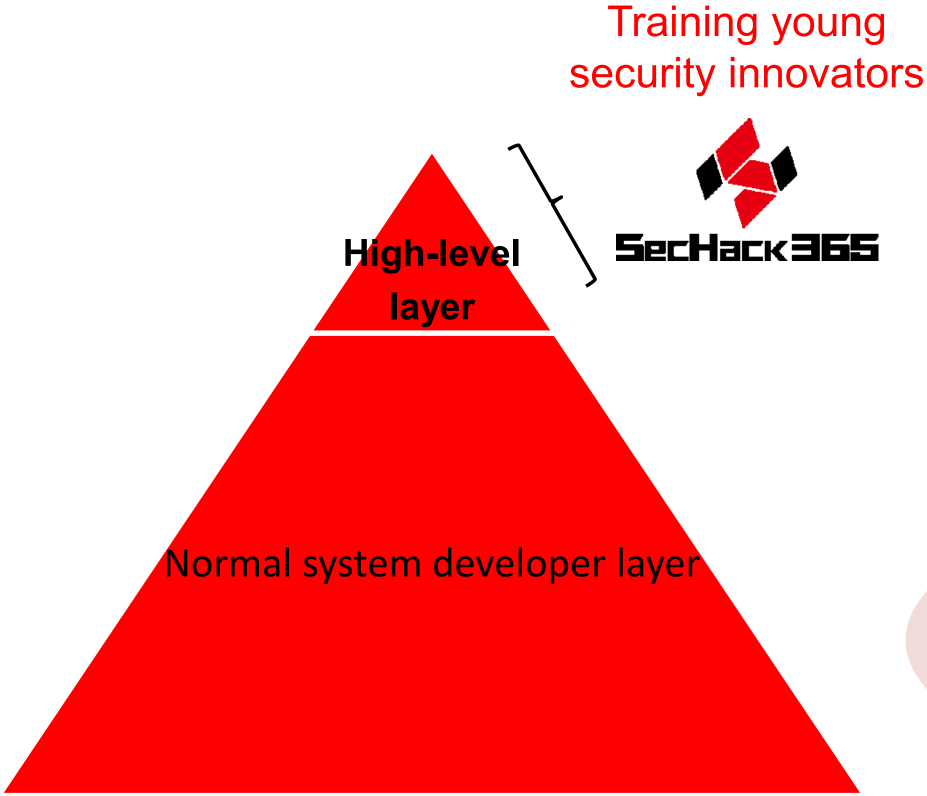


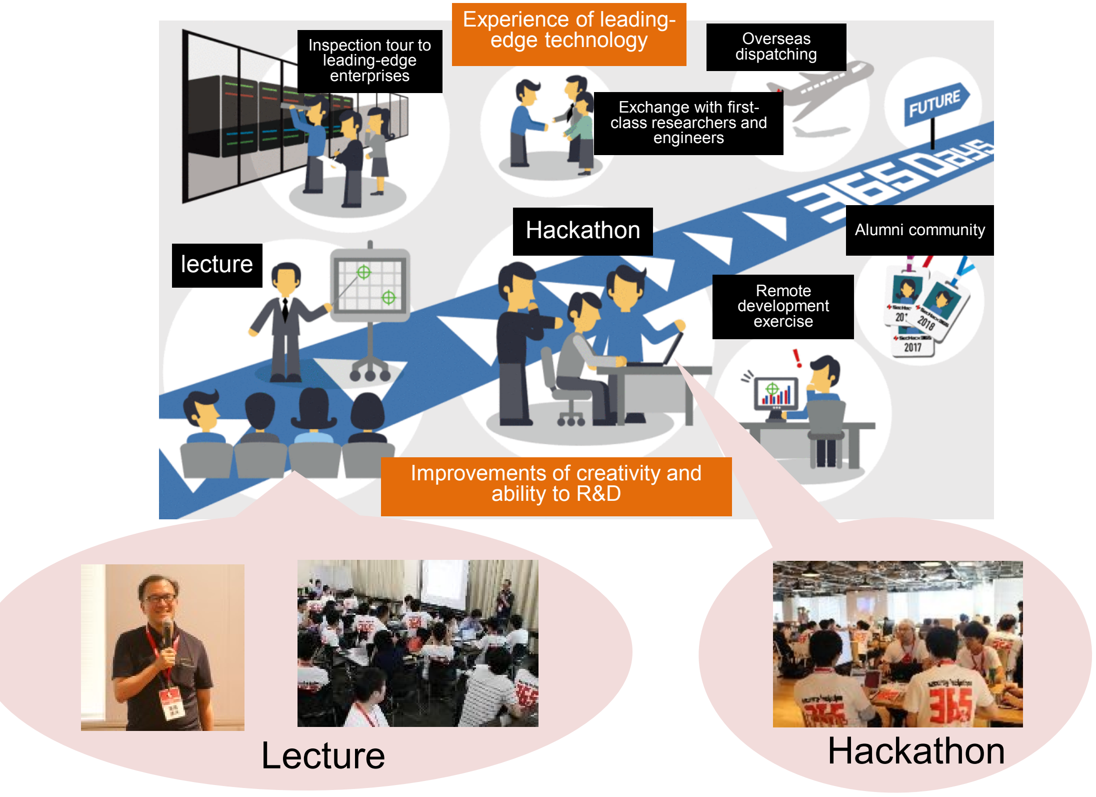
Training Young Security Innovators (SecHack365)

National Cyber Training Center

- In order to increase advanced cybersecurity researchers and entrepreneurs in the future, NICT provides a one-year cybersecurity training program with hands-on training and remote software development training for young talents, utilizing its own cybersecurity research assets.

- Participants are ICT engineers who are 25 years old or younger, living in Japan (39 trainees have completed the one-year program in FY2017).


Training young security innovators
SecHack365
High-level layer
Normal system developer layer


Inspection tour to leading-edge enterprises
Experience of leading-edge technology
Overseas dispatching
Exchange with first-class researchers and engineers
FUTURE
365 Days
lecture
Hackathon
Alumni community
Remote development exercise
Improvements of creativity and ability to R&D
Lecture
Hackathon

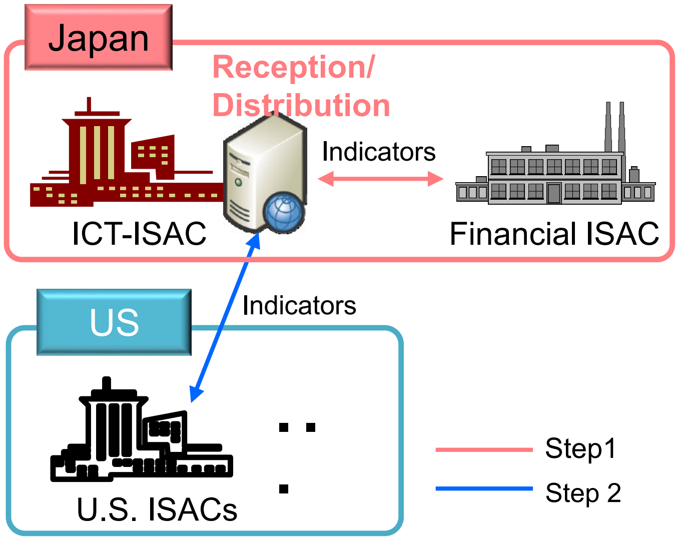
(5) International Collaboration

1. Information sharing

- Promote international collaboration in private sectors (mainly ICT industry), including ISAC
  - Share information, such as threat intelligence and indicators, with US ISACs
  - Hold the International Workshop on ISAC Collaboration on a regular basis (Tokyo, Nov 2017)

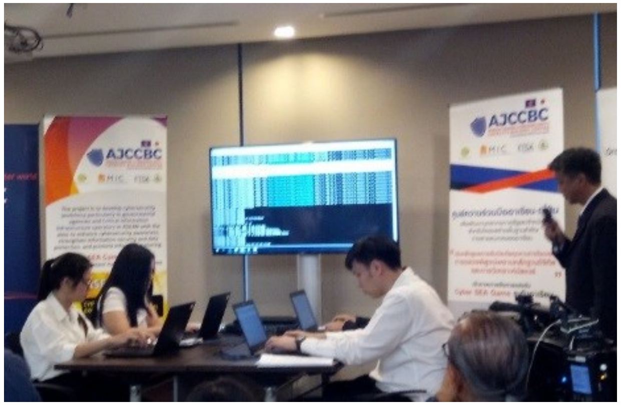
- Promote information sharing among government officials
  - Bilateral cyber dialogues (US, UK, France, Estonia etc.)
- Japan-EU ICT Policy Dialogue (Oct 2017) and Japan-France ICT Policy Dialogue (Mar 2018)
  - Japan-ASEAN Information Security Policy Conference (Oct 2017)

[Example]



2. Capacity building

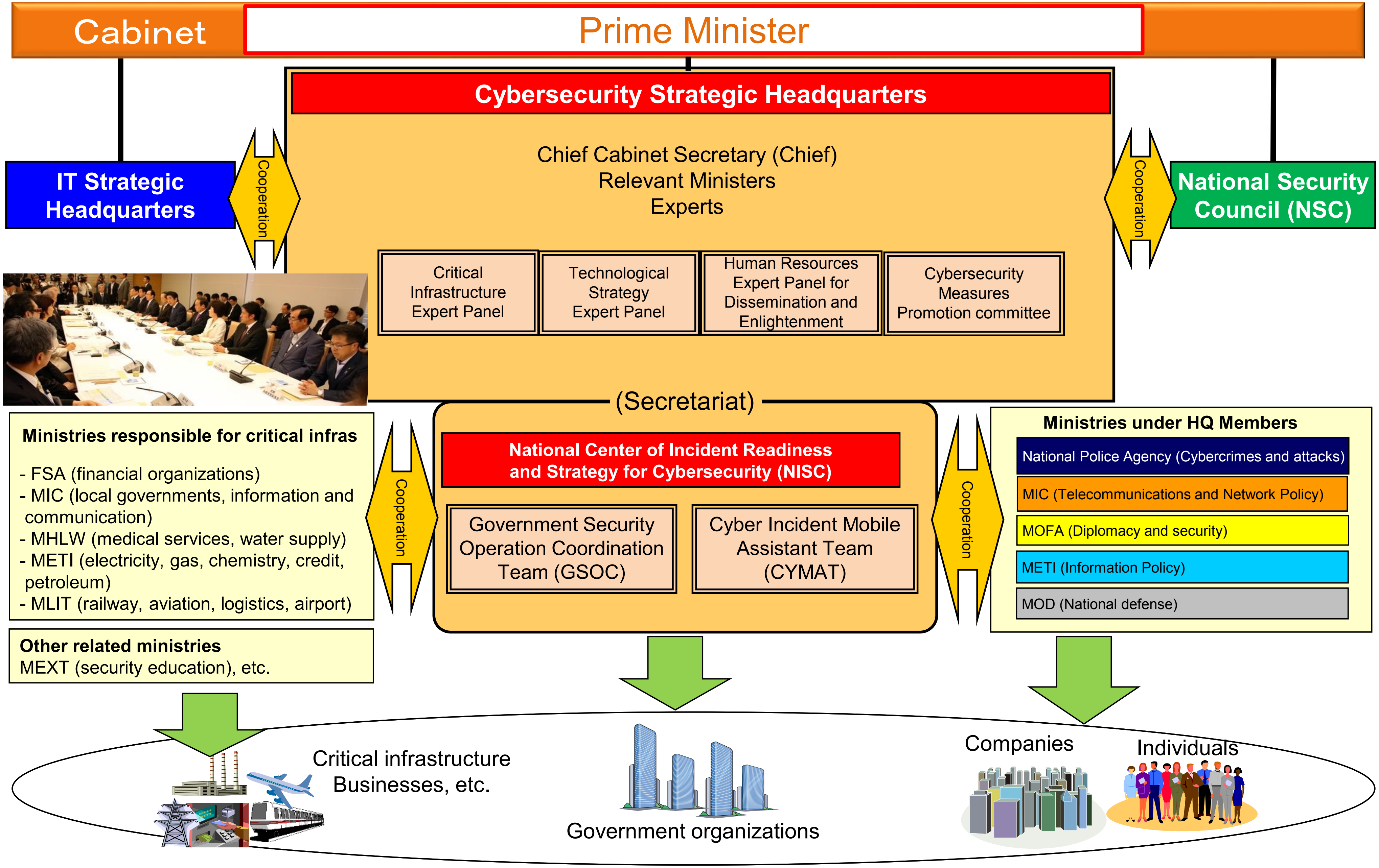
- Support the development of security human resources in other countries, such as ASEAN, by expanding CYDER program globally
- Moreover, promote to expand Japanese security businesses globally, such as SOC development and security operations, through the human resource development
  - Thailand (Nov 2015 and Feb 2017), Malaysia (Jan 2017), and India (Jan 2018)
  - Training programs in ASEAN (FY2016 through FY2018)



Thank you for your kind attention

Ministry of Internal Affairs and Communications (MIC)
http://www.soumu.go.jp/english/index.html

Cybersecurity Structure of Japanese Government



Cabinet

Prime Minister

IT Strategic Headquarters

Cooperation

Cybersecurity Strategic Headquarters

Chief Cabinet Secretary (Chief)
Relevant Ministers
Experts

Critical Infrastructure Expert Panel

Technological Strategy Expert Panel

Human Resources Expert Panel for Dissemination and Enlightenment

Cybersecurity Measures Promotion committee

Cooperation

National Security Council (NSC)

(Secretariat)

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

Government Security Operation Coordination Team (GSOC)

Cyber Incident Mobile Assistant Team (CYMAT)

Ministries responsible for critical infras

- FSA (financial organizations)
- MIC (local governments, information and communication)
- MHLW (medical services, water supply)
- METI (electricity, gas, chemistry, credit, petroleum)
- MLIT (railway, aviation, logistics, airport)

Other related ministries
MEXT (security education), etc.

Cooperation

Cooperation

Ministries under HQ Members

- National Police Agency (Cybercrimes and attacks)
- MIC (Telecommunications and Network Policy)
- MOFA (Diplomacy and security)
- METI (Information Policy)
- MOD (National defense)

Critical infrastructure Businesses, etc.

Government organizations

Companies

Individuals

Reasons why IoT Devices are Targeted by Cyberattacks

(1) The extent and degree of impact by attacks is severe.

(2) The life cycle of IoT devices is long-term.

(3) IoT devices are not well-monitored.

(4) Interoperability of IoT devices and network is not sufficient.

(5) Functions and performance of IoT devices are limited.

(6) IoT devices can be connected in a way that the developers have never expected.

[Reference] Cases of Threats to IoT Devices 1)

1) Web Camera

Video and audio of the web camera was accessible to anyone over the Internet.

2) Multifunction Printer (MFP)

Data stored in MFPs of Japanese universities were accessible to anyone over the Internet.

3) Water Supply System

Data loggers of the water supply system in hospitals were accessible over the Internet, which allowed anyone to view the operational status and switch the operational mode (run/stop).

4) Power Monitoring System

Power monitoring systems installed in factories were accessible over the Internet, which allowed anyone to change alert threshold, disable alert, configure proxy, and restart the system.

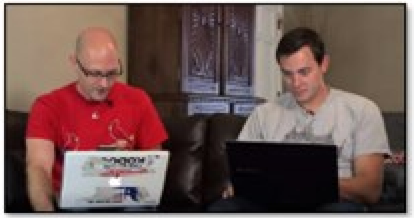
[Reference] Cases of Threats to IoT devices 2)

5) Automobiles

- A security researcher found vulnerabilities in the automobiles made in 2014, which allowed remote control over the Internet. The researcher successfully controlled the car remotely at home over the Internet.
- The car company announced recalls of 1.4 million cars, as a response to the vulnerabilities.

The target is 2014-type Jeep Cherokee

The attackers were several miles away at home.



Controlled the wiper

Controlled the air conditioner

Unlocked the door

Disabled the brake

Controlled the handle

Stopped the engine while running.

Succeeded in overwriting the firmware of the on-vehicle multimedia equipment connected to the Internet, which resulted in the recalling of 1.4 million cars.

Source: Black Hat USA (August 2015)