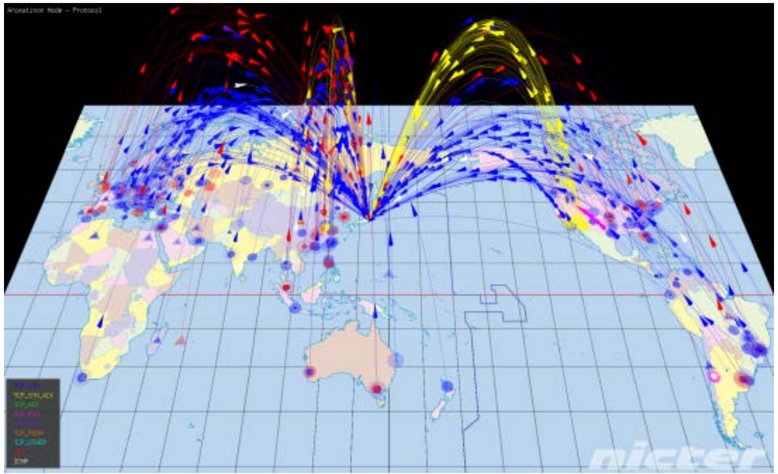
IoT Security Measures in Japan

January 24th, 2019

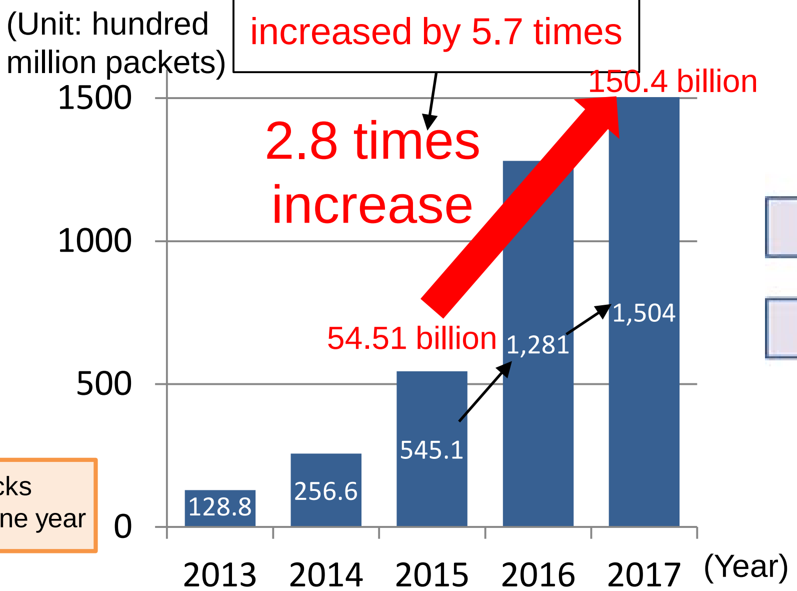
Reiko Kondo
Director
Office of the Director-General for Cybersecurity
Ministry of Internal Affairs and Communications (MIC)
JAPAN

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).



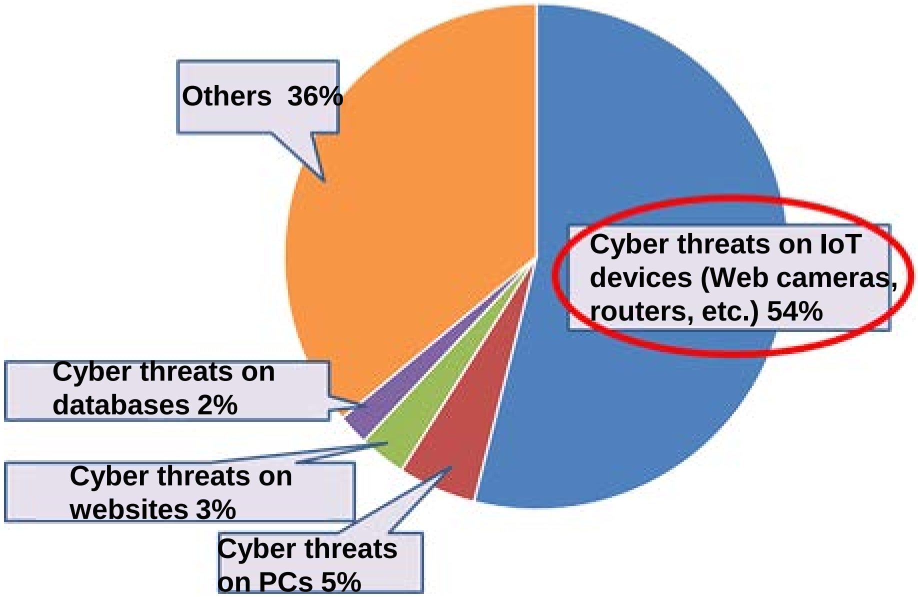
- 🟦 TCP SYN
- 🟨 TCP SYN/ACK
- 🟩 TCP ACK
- ■ TCP FIN
- 🟪 TCP RESET
- 🟧 TCP PUSH
- ■ TCP Other
- 🟥 UDP
- ■ ICMP



Attacks to IoT devices increased by 5.7 times

Number of cyberattacks observed by NITCER in one year

More than half were attacking on IoT devices!



Comprehensive Package of IoT Security Measures

The Cybersecurity Task Force administered by MIC published the comprehensive package of IoT security measures in October 2017. The progress made so far was reviewed this month. The progress report of this package has been published on 27th July 2018.

Measures on IoT devices vulnerabilities

- Necessary to implement measures on IoT devices vulnerabilities, covering the entire lifecycle (design, development, sale, installation, operation & maintenance and use)
- Necessary to organize the structure to conduct vulnerability assessment

Promotion of research & development

- Share security operation know-how and promote research and development in need

Acceleration of security measures in the private sector

- Accelerate cybersecurity investment in the private sector
- Encourage to share cyber attack/threat information to prevent damage or its spread

Strengthening of HR development

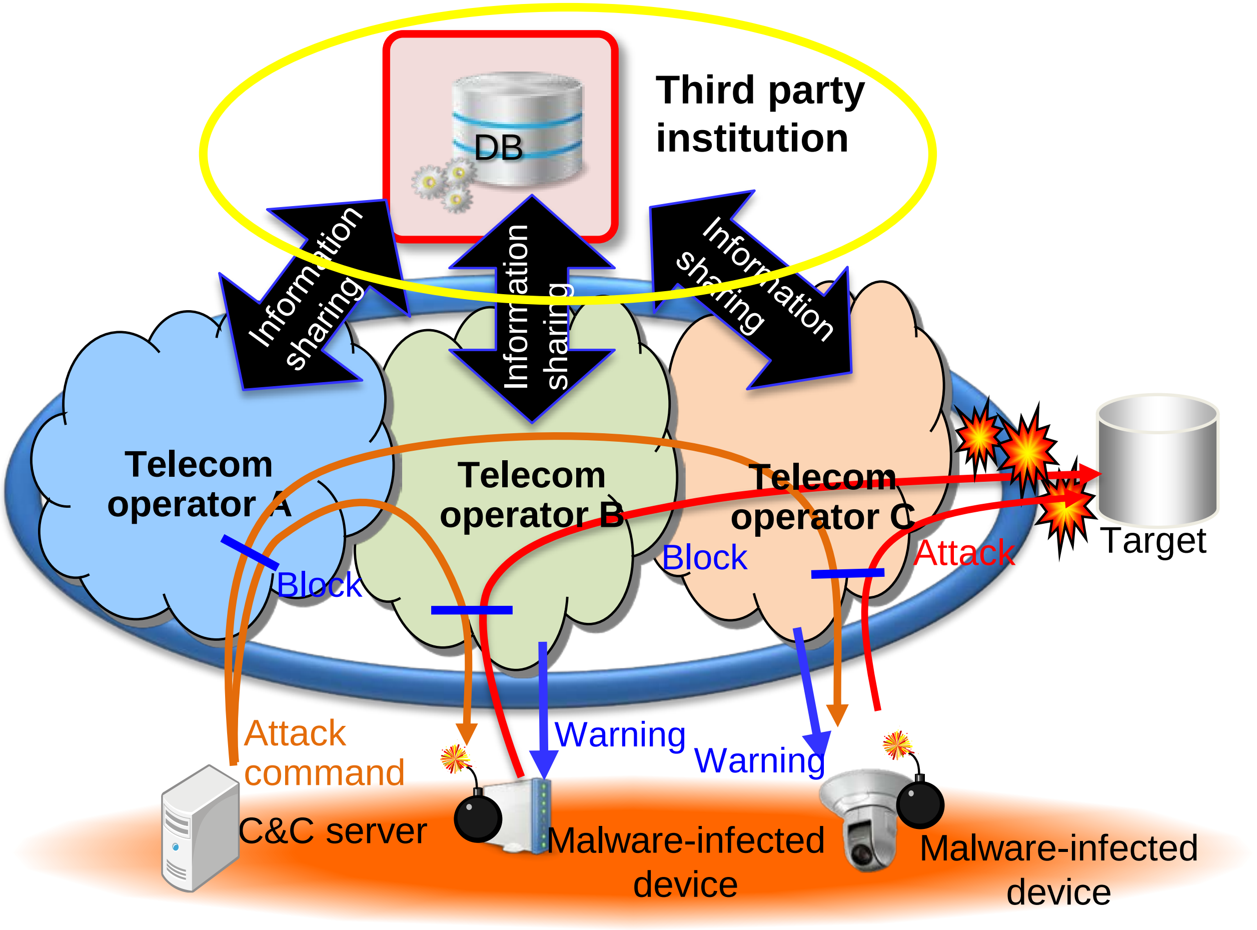
- Strengthen hands-on cyber defense exercise when predominantly lacking security experts

Promotion of international cooperation

- Promote information sharing, rulemaking, HR development and R&D bilaterally and multi-nationally

Information Gathering Hub with Firm Security Measures

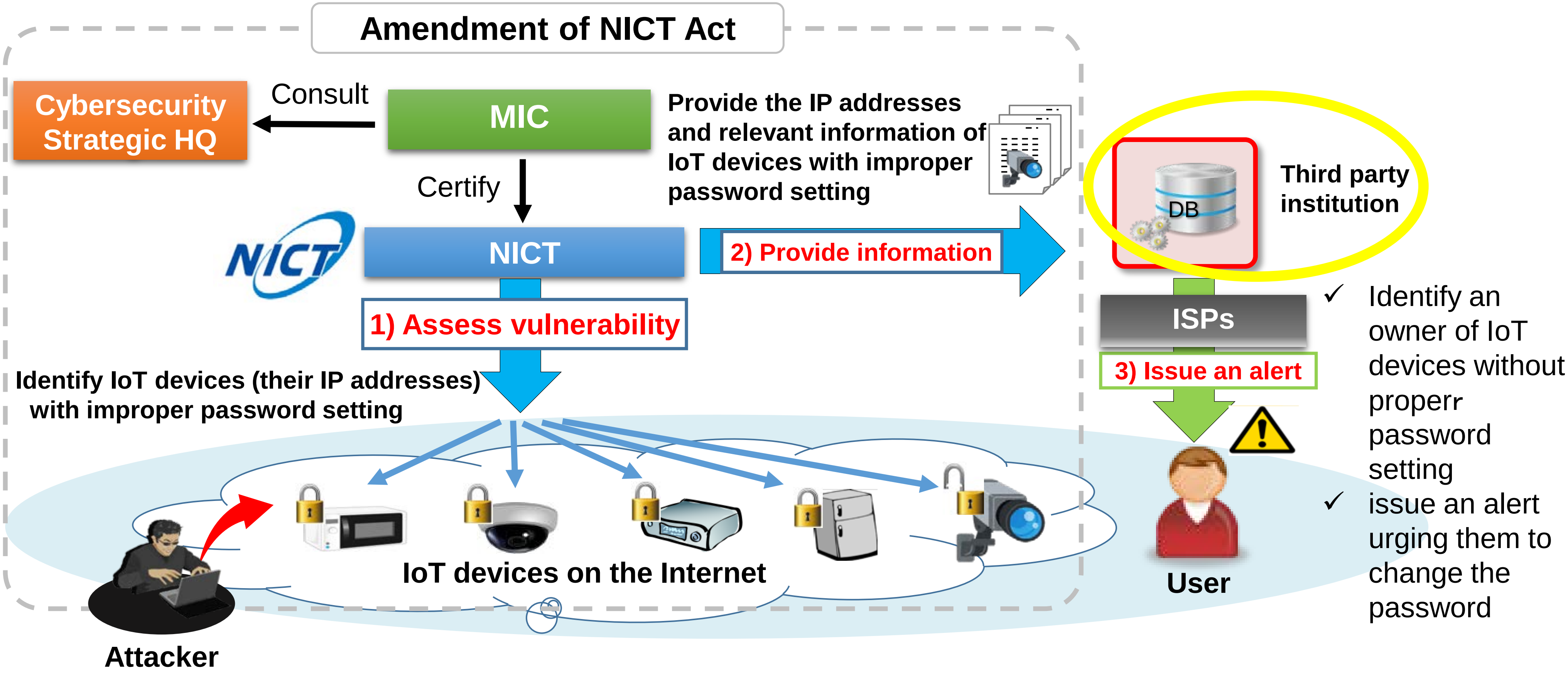
In May 2018, revised Telecommunications Business Act and NICT ACT were promulgated. By the revised Telecommunications Act, it is allowed to establish **the third party, working as an information gathering hub with firm security measures to manage sensitive information.**



- ✓ C&C server, through which the attacker gives instructions to infected terminals, is connected to the network of telecom operator A
- ✓ Infected terminals are connected to the networks of telecom operators B and C
- ✓ Telecom operators A, B, and C can share threats information such as IP addresses and time stamps through the third party institution without violating secrecy of information
- ✓ Telecom operator A blocks C&C server
- ✓ Telecom operators B and C can make alerts to their customers

Vulnerability Assessment of IoT Devices with Improper Password Settings

Revised ACT on National Institute of Information and Communications Technology (NICT) enables NICT to **actively scan** IoT devices over the Internet and **identify IoT devices with improper password settings**, of which actions had been prohibited by the Act on Prohibition of Unauthorized Computer Access.


Amendment of NICT Act
Cybersecurity Strategic HQ
Consult
MIC
Certify
NICT
Provide the IP addresses and relevant information of IoT devices with improper password setting
2) Provide information
1) Assess vulnerability
Identify IoT devices (their IP addresses) with improper password setting
DB
Third party institution
ISPs
3) Issue an alert
User
IoT devices on the Internet
Attacker

- ✓ Identify an owner of IoT devices without properr password setting
- ✓ issue an alert urging them to change the password

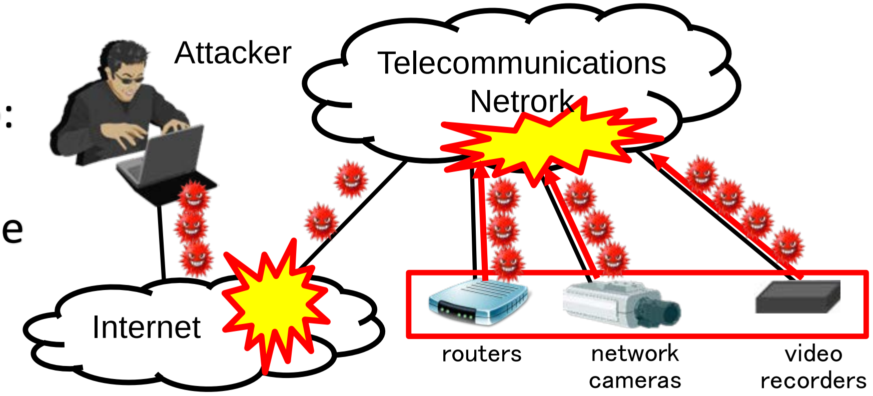
Amendment on the Technical Standard of Terminal Equipment for IoT Security Purpose（IoT Certification）

- In order to prevent massive malware infection on IoT devices, the Information and Communications Council in MIC discussed an addition of security measures to a technical standard of terminal equipment required by the Telecommunication Business Act and released a report on September 12, 2018 after public consultation.
- MIC is now preparing related ordinances, notifications, and guidelines for implementing the security measures, which will be enforced in April 2020.

Summary of the report

✓ Terminal equipment that has a remote control function to send/receive data through the internet is required to:
1) have access control on the remote control function,
2) have a mechanism to encourage its user to change the default IDs/passwords, if the access control uses IDs/passwords for the authentication and
3) have a feature to be able to update firmware,

or any equivalent/better security measures to/than above.



✓ The requirement does not apply to PCs or smartphones that are generally protected by other security measures such as anti-virus software.

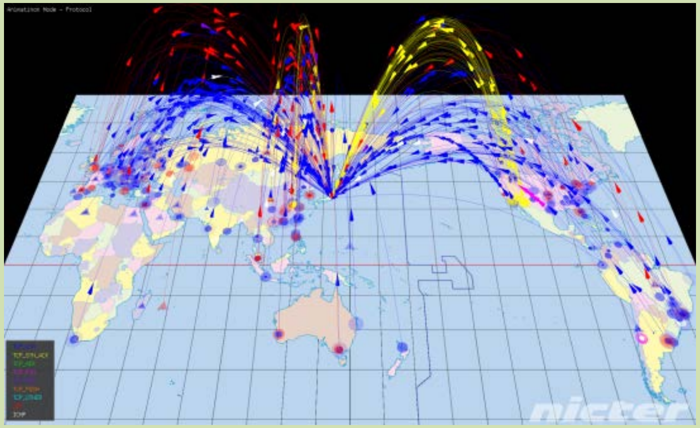
✓ These measures should be implemented after some period (one to two years) for allowing IoT device makers and certification bodies to prepare for adding new measures.

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 sensors.
- 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]

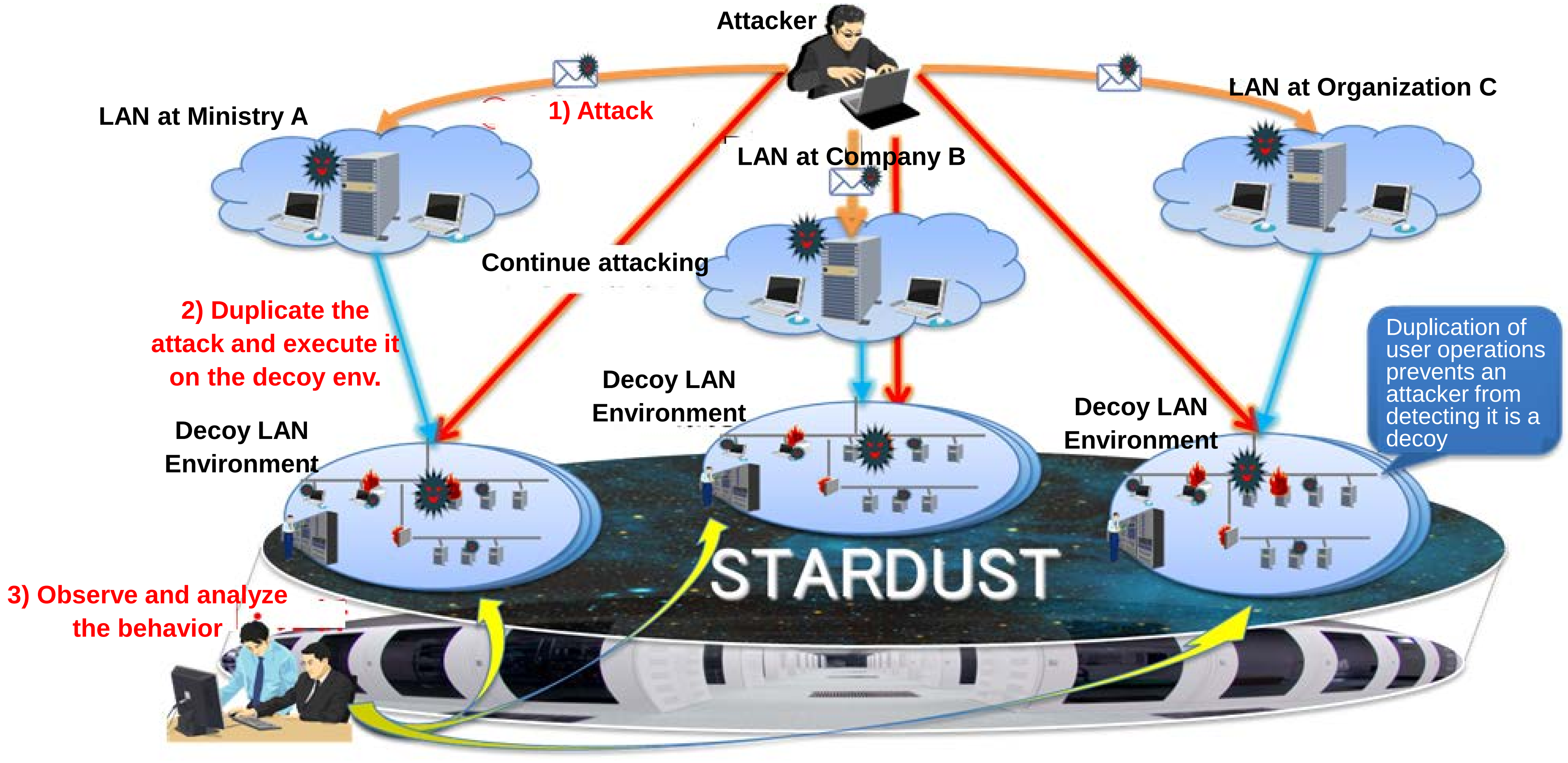
- **Visualize traffic occurred within the organization in real time** by installing the sensors in the environment.
- Further developments which enable **automatic block for abnormal communications once it is detected**

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

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 has been established 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

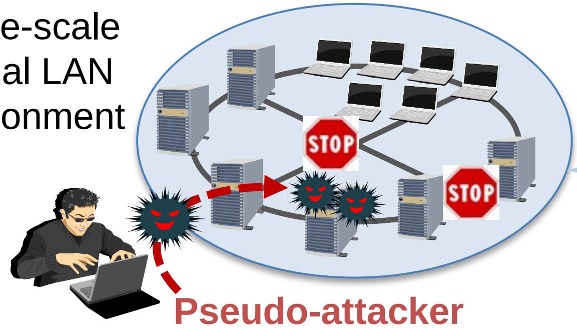
○ MIC provides **CYDER exercises**, which is conducted by NICT, **for those who are in charge of information systems in administrative organizations and critical infrastructure providers**.

○ **Participants can 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 CYDER

Large-scale
virtual LAN
environment



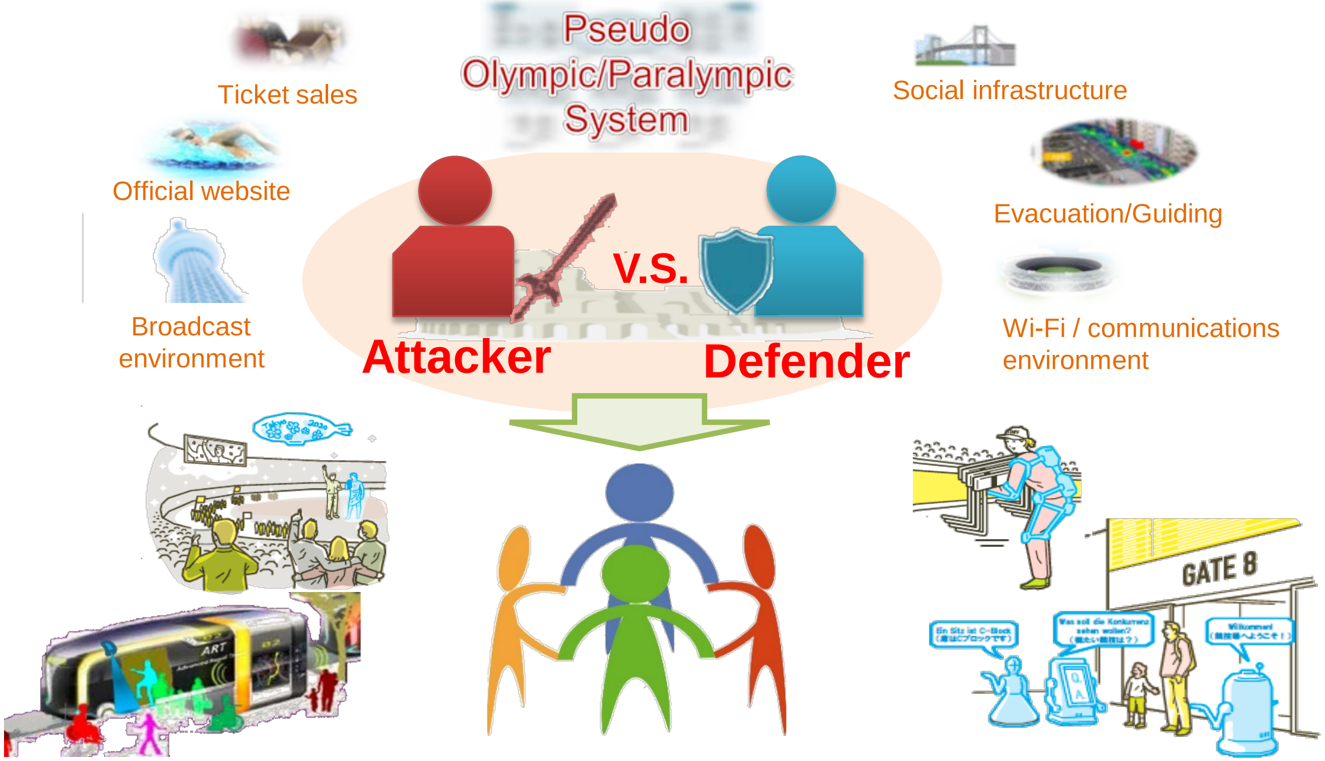
Exercise Plan for 2018

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

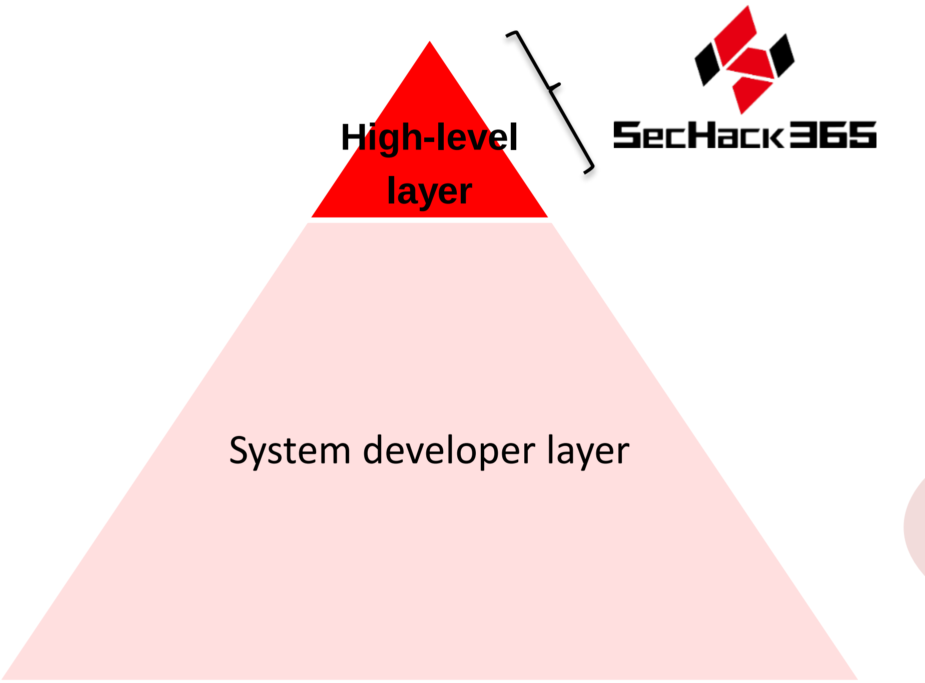
- **Cyber Colosseo** exercise started February 2018 to develop human resources capable of handling advanced cyberattacks, which is conducted for those who are in charge of cybersecurity in the organizations related to Tokyo 2020 Olympic and Paralympic Games.
- At the exercise venue of the Cyber Colosseo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



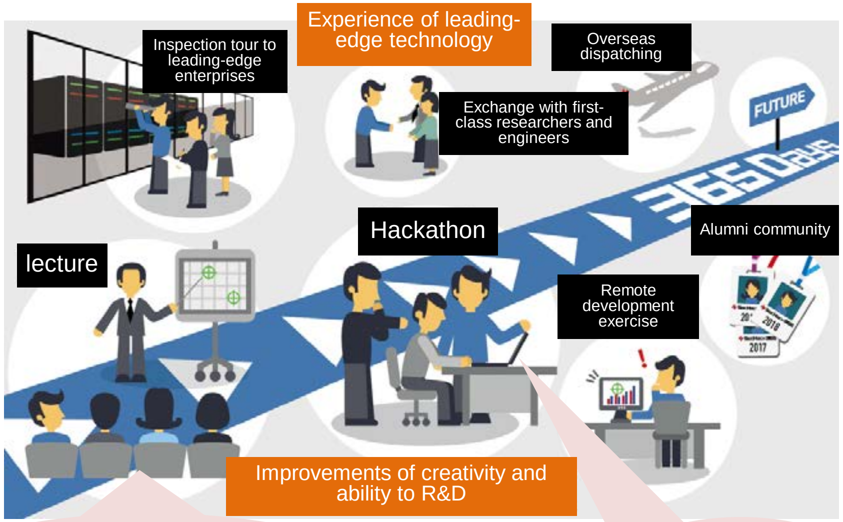
Training Young Security Innovators (SecHack365)

National Cyber Training Center

- In order to increase the number of advanced cybersecurity researchers and entrepreneurs in the future, NICT provides an 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



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

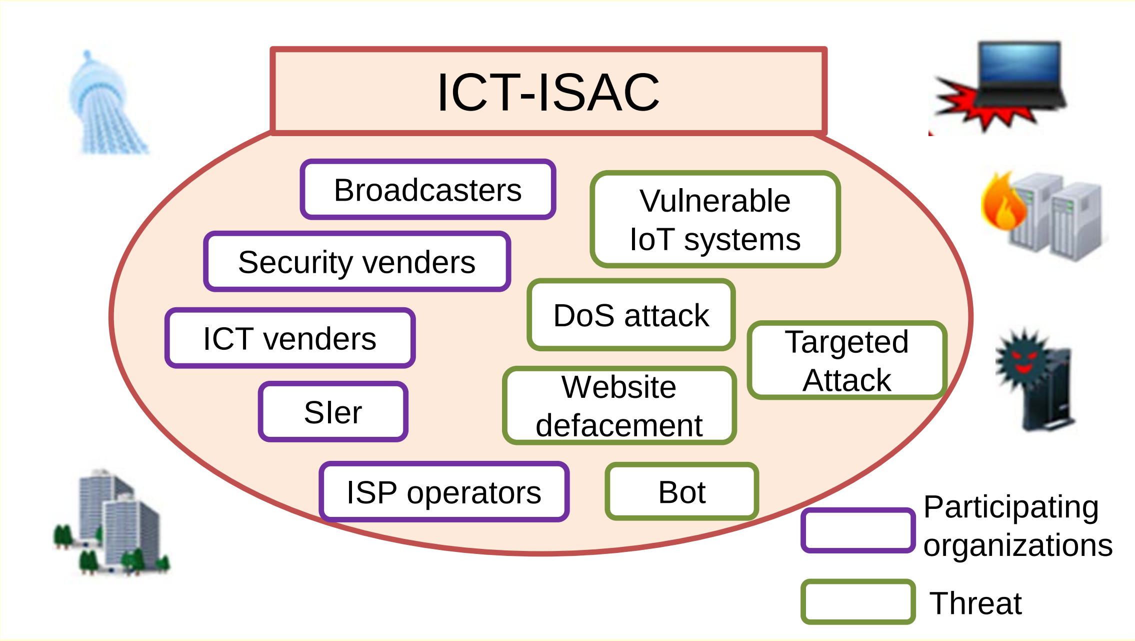
Lecture

Hackathon

Cooperation through ISAC

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

Overview of ICT-ISAC Japan



ICT-ISAC JAPAN
ICT Information Sharing and Analysis Center Japan

President:
Tadao Saito

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