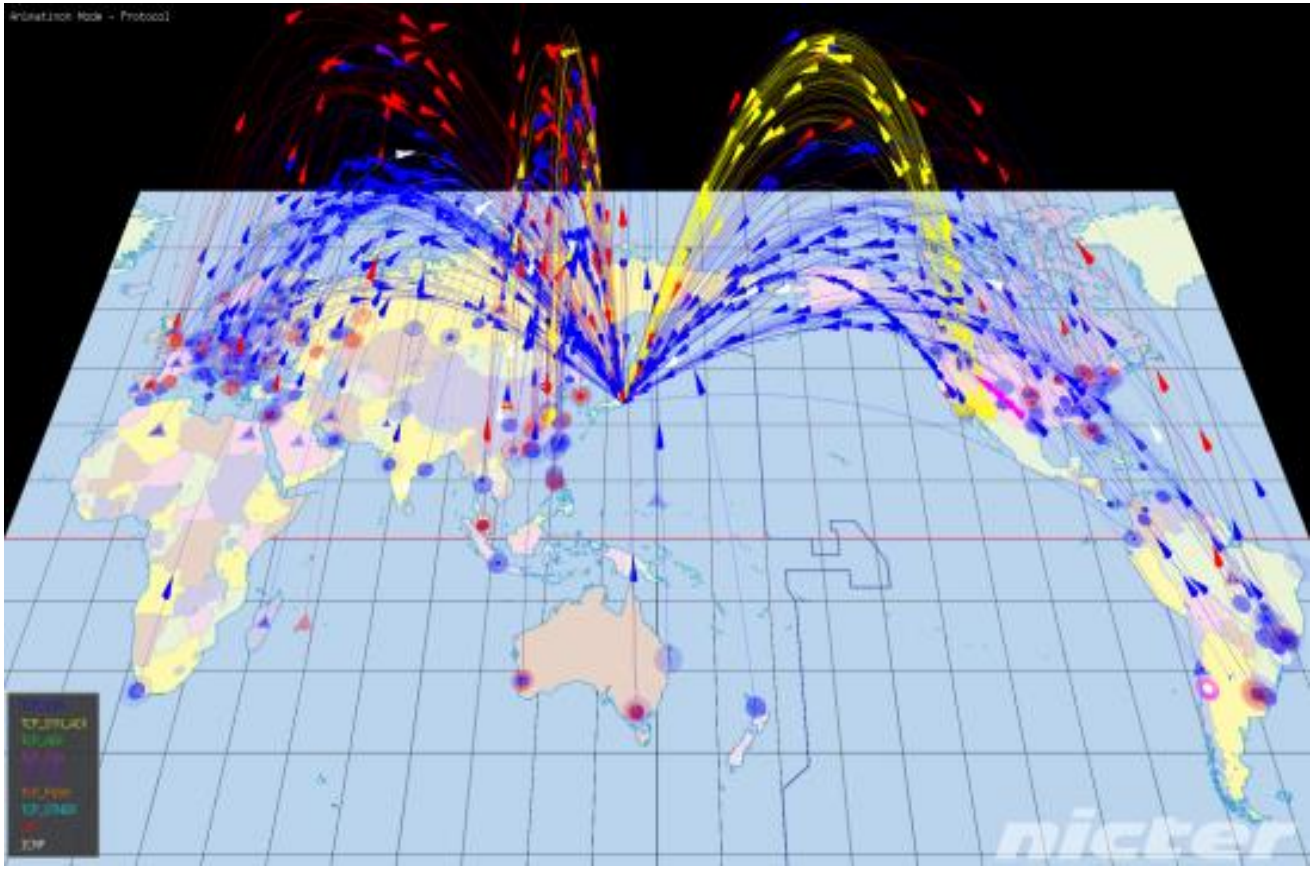
Security Measures in IoT/5G Era

November 11th, 2019

TAKEUCHI Yoshiaki
Director-General for Cybersecurity
Ministry of Internal Affairs and Communications (MIC)
JAPAN

Cyberattacks Observed by NICTER

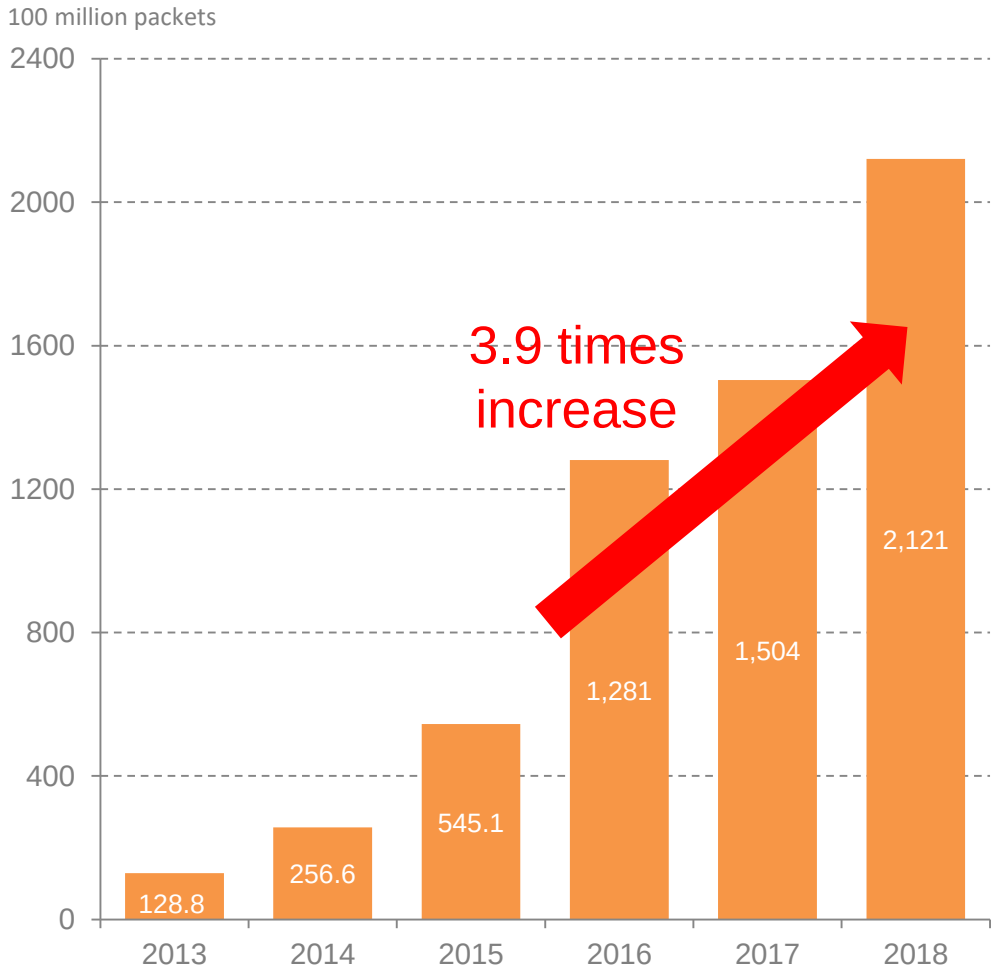
The National Institute of Information and Communications Technology (NICT) is observing cyber attacks globally by monitoring 300,000+ unused IP addresses (NICTER).



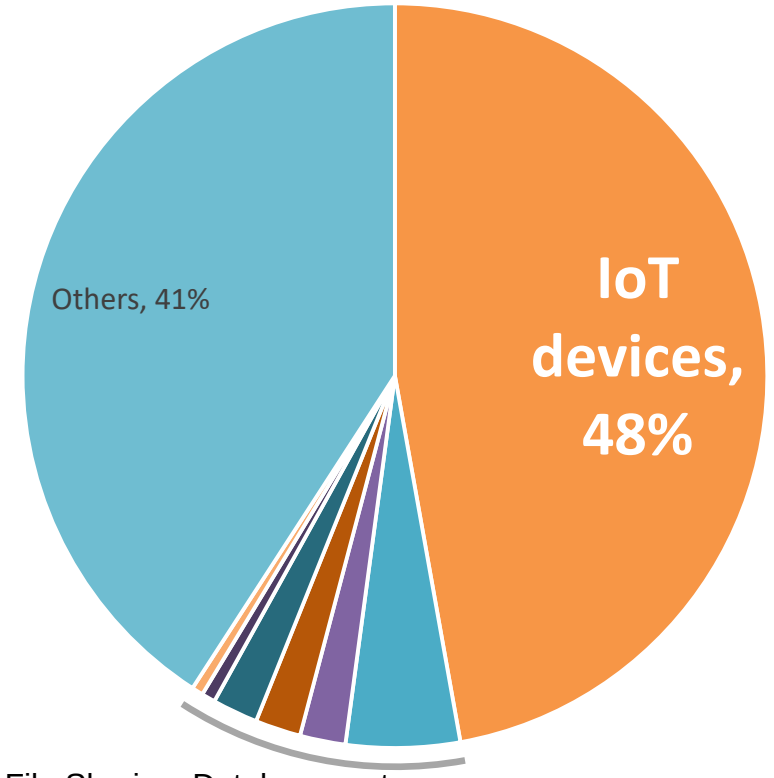
TCP SYN TCP SYN/ACK TCP ACK TCP FIN
TCP RESET TCP PUSH TCP Other UDP ICMP

Attacks on IoT Devices (Observed by NICTER)

IoT Devices: Router, Web Camera, Sensor, etc.



Number of cyberattacks observed by NICTER in one year

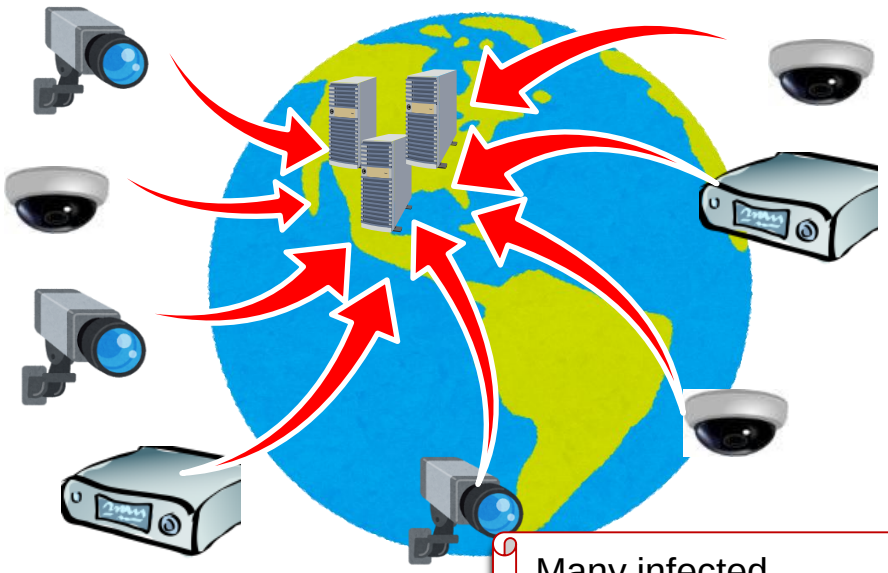


Targets of cyber attacks observed by NICTER

About half of attacks are targeted at IoT devices!

Large-scale DDoS Attacks due to IoT devices

- On October 21, 2016, the Dyn's DNS server in the United States experienced two large-scale DDoS attacks
- A number of companies that use Dyn's DNS service were also affected due to a communications failure
- The attacks originated from a large number of IoT devices infected with malware called "Mirai"

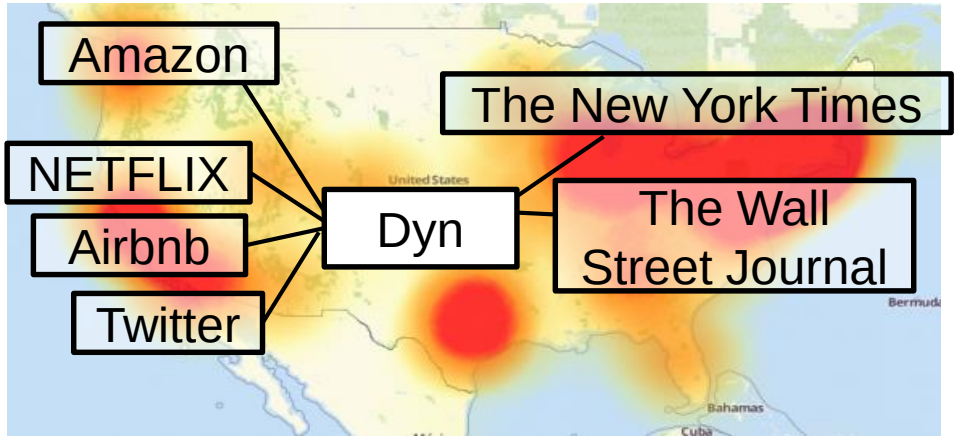


Many infected devices with simple and weak ID and PW

ID: root
password: 1234

- ✓ A large volume of communication targeting Dyn's system was generated from over 100,000 IoT devices infected with malware
- ✓ It reportedly reached 1.2 Tbps.
- ✓ Many leading Internet services and news sites using Dyn's DNS service were affected

Status of System Failure



Why are IoT Devices Targeted ?

(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 never expected.

IoT Security Measures by the Government

Effective Measures

- Identify vulnerable IoT devices, such as ones with default ID/password settings, and alert the users of these devices to change the settings.

Challenges

- It is prohibited to access IoT devices on the Internet without the permission of users.

Government Action

- Amended the law in May 2018 to implement the above measure without violating any laws, and started the “NOTICE” project, in February 2019.

Outline of the “NOTICE” Project [A]

Starting on February 20, 2019, the Ministry of Internal Affairs and Communications (MIC) and NICT, in cooperation with Internet Service Providers (ISPs), have been carrying out the “NOTICE”* project to survey vulnerable IoT devices, and to alert users to any problems found. This project is implemented in compliance with the amendment of the NICT Act.

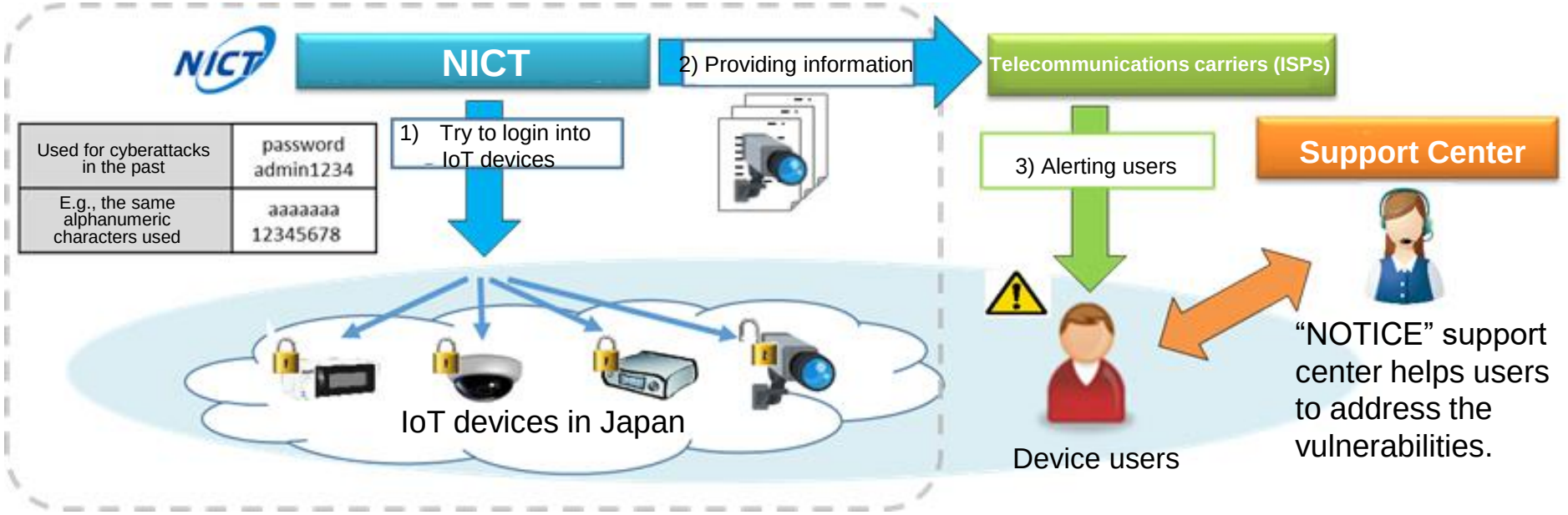
*National Operation Towards IoT Clean Environment

<Overview of the “NOTICE” Project>

(1) NICT surveys IoT devices on the Internet and **identifies vulnerable devices**, which are those with weak ID/password settings.

(2) NICT **provides the information** of the identified vulnerable devices **to ISPs**.

(3) The ISPs identify the users of the devices and **alert users**.



Project to Alert Users of IoT Devices Infected with Malware [B]

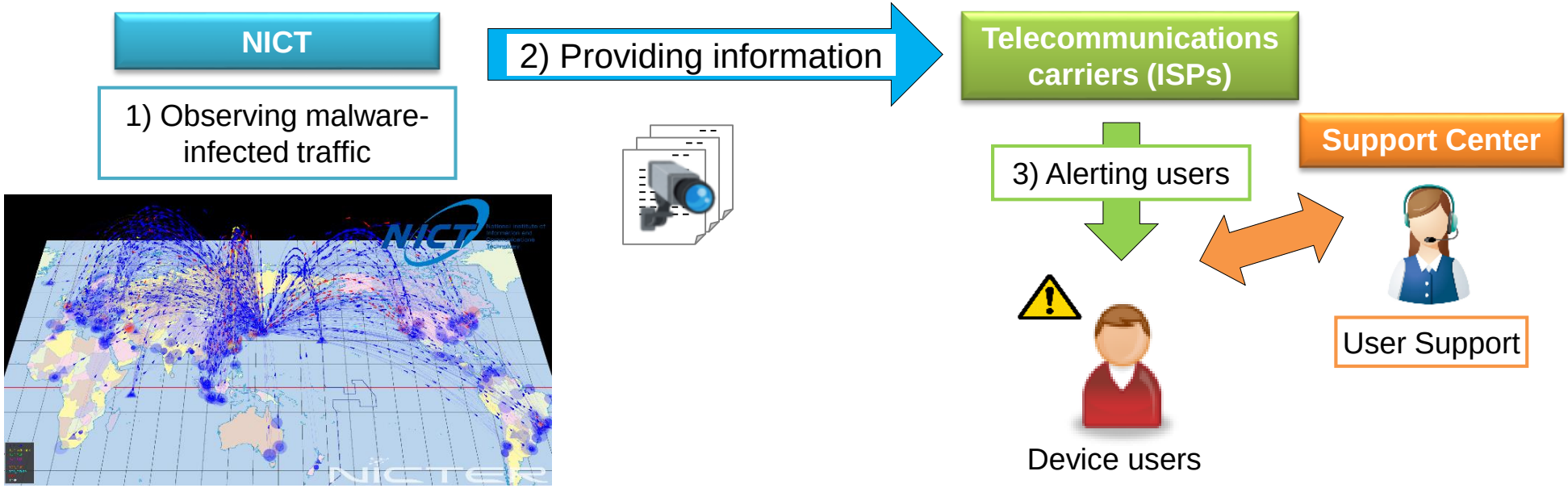
Along with NOTICE, MIC and the NICT, in cooperation with ISPs, are carrying out the project to identify devices infected with malware by using the NICTER and to notify the ISPs so that they can alert users of the infected devices from mid June 2019.

<Overview of the project>

(1) NICT identifies the devices generating the malware-infected traffic by using the NICTER.

(2) NICT provides information about malware infected devices **to ISPs**.

(3) The ISPs identify the users of the devices **and alert them**.



Progress on the Projects (As of the end of September 2019)

Among 200 million IP addresses in Japan, approximately 100 million IP addresses managed by 34 ISPs that are participating in the projects have been investigated.

(1) Results of NOTICE

Number of IP addresses in which **ID and password could be entered** → Approx. 98,000

In the above, the number of those which were **successfully logged-in** to with **weak password settings** and were **subject to user alert** → Total 505

(2) Results of the project to alert users of malware-infected IoT devices

Number of IP addresses which seem to be **infected with malware** and were **subject to user alert** → 80-559 per day

34 Internet Service Providers are participating in the project.
In addition to these measures, a proactive measure is required.
(⇒next page)

Proactive measures for IoT security [C]

Amendment of Technical Conditions of Terminal Equipment for IoT Security

- **Terminal equipment** that is directly connected to telecommunication networks through internet protocols **are required to have**:
  1) access control via a remote control function,
  2) features to **encourage users to change default IDs/passwords**
  3) firmware update features for future security fixes,
  or any equivalent/better security measures to the above.
- The requirement does not apply to personal computers or smartphones that are generally protected by other security measures such as anti-virus software.
- MIC published guidelines for the security requirements for the Technical Conditions, which describe the scope of device types, details of the requirements, etc.

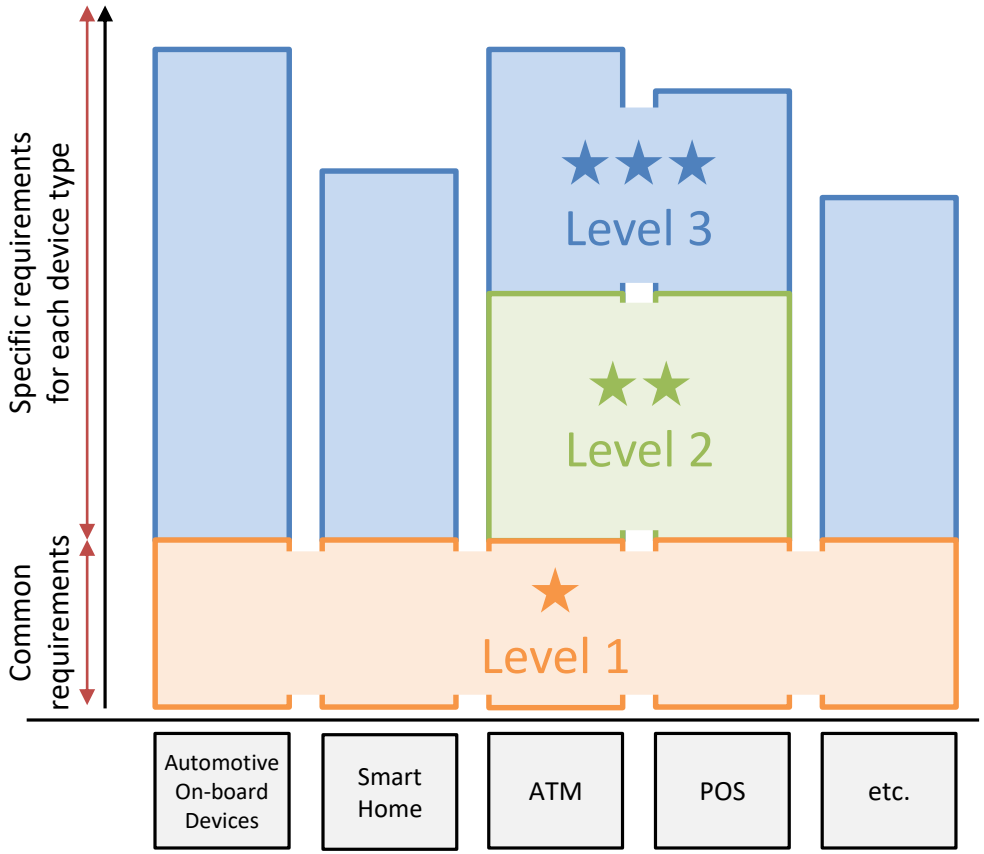
Schedule

- The amended Technical Conditions will be enforced on April 1, 2020.
  After this, approval will only be given to terminal equipment that conform to the Technical Conditions.

Certification Program by CCDS

Connected Consumer Device Security council (CCDS) has started non-mandatory certification program for IoT devises in October 2019.

Three-layered model for the certification program



CCDS is a general incorporated association formed by related businesses / organizations which aims to improve the security of consumer devices including IoT devices. (200 members as of November, 2019)

CCDS 2019 ★ Security Certification

Level 1:
- Common and baseline requirements for IoT devices
- Started in October 2019

CCDS 2019 ★★ Security Certification

Level 2:
- Specific requirements introduced by industry groups
- Will be started in April 2020

CCDS 2019 ★★★ Security Certification

Level 3:
- Specific requirements for the protection of users' lives and property
- Will be started in April 2020

Resources : CCDS's public documents (https://www.ccds.or.jp/public_document)

International Cooperation is Required

- Since botnets are formed globally and cyber attacks are conducted across borders, security measures should be undertaken in all countries.
- To realize a safe and secure cyberspace, **it is important that all countries share best practices with each other, and implement IoT security measures.**
- In Japan, we are implementing three security measures for IoT devices [A],[B] and [C]. In addition, CCDS initiatives are also expected to be effective measures.

[Proposal]

- We would be happy to cooperate with other countries, for example by sharing Japanese IoT security measures and providing relevant information about malware-infected devices observed by our system (NICTER).
- We would also appreciate it if you could share information about IoT security measures taking place in your country.

ISAC Collaboration

ISACs in Japan

ICT-ISAC JAPAN
Information Sharing And Analysis Center Japan

F-ISAC

Financials ISAC Japan Information Sharing and Analysis Center

JE-ISAC

JE-ISAC Japan Electricity Information Sharing and Analysis Center

J-AUTO-ISAC

Software ISAC

etc.

MoU between ICT-ISAC Japan and IT ISAC

ISACs in US

IT ISAC

MS-ISAC

NCC

H-ISAC HEALTH · ISAC

HEALTHCARE READY

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

DNG-ISAC

AVIATION ISAC

MARITIME ISAC

DIB ISAC Defense Industrial Base Information Sharing and Analysis Center

WATER ISAC

ONG-ISAC

AUTO-ISAC Automotive Information Sharing and Analysis Center

RETAIL & HOSPITALITY ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

National Defense ISAC

Elections Infrastructure ISAC

FINANCIAL SERVICES ISAC

REN-ISAC

etc.