Securing IoT and their supply chains
- SIP/CPS, a government program in Japan -

SIP: Cross-ministerial **S**trategic **I**nnovation Promotion **P**rogram

CSTI: Council for Science, Technology and Innovation

Atsuhiro Goto

Program Director for SIP/CPS, Cabinet Office, Government of Japan

President and Professor, Institute of Information Security, Japan

What we should protect from cyber attacks

One of 12 projects in SIP 2nd Stage(2018—2022) **"Cyber Physical Security for IoT Society (SIP/CPS)"** to develop technologies for securing IoT and their supply chains

SIP/CIS in SIP 1st Stage 2015-2019

SIP: Cross-ministerial Strategic Innovation Promotion Program

CSTI: Council for Science, Technology and Innovation

New value created by IoT System in **Society 5.0**

Critical Infrastructure Evolution	New Value for Industry	New Value for Individual Consumer
5G and beyond	Smart Factory	Smart Building
	Smart Logistics	Autonomous Cars
		Smart Home Appliances

Critical Infrastructures in Japan for Tokyo 2020 and beyond

ALERT! Bump Ahead: Supply chain risk

What was presented at Black Hat 2015?

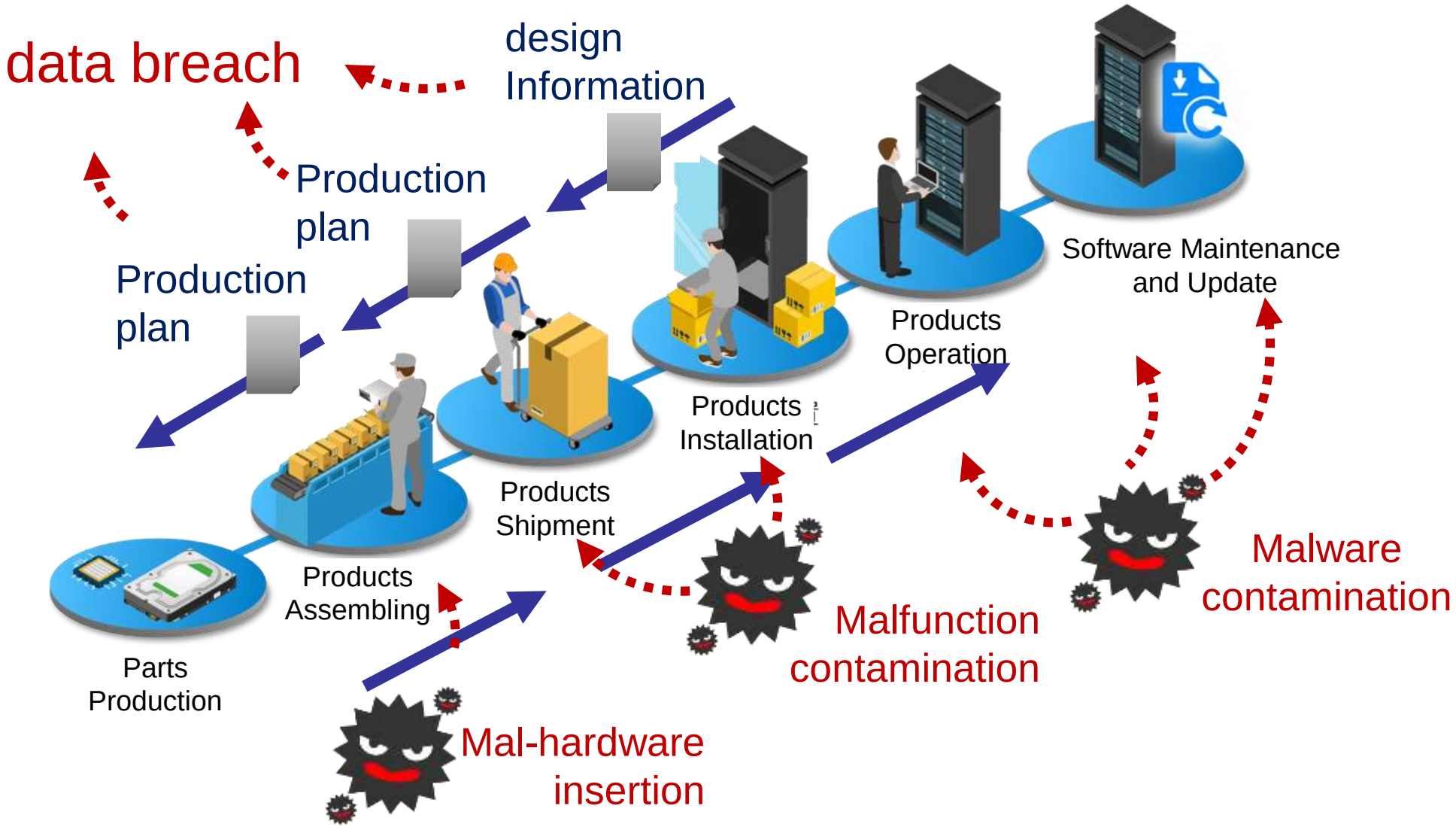
Vulnerable communication + vulnerable hardware

= 1.4M recalls

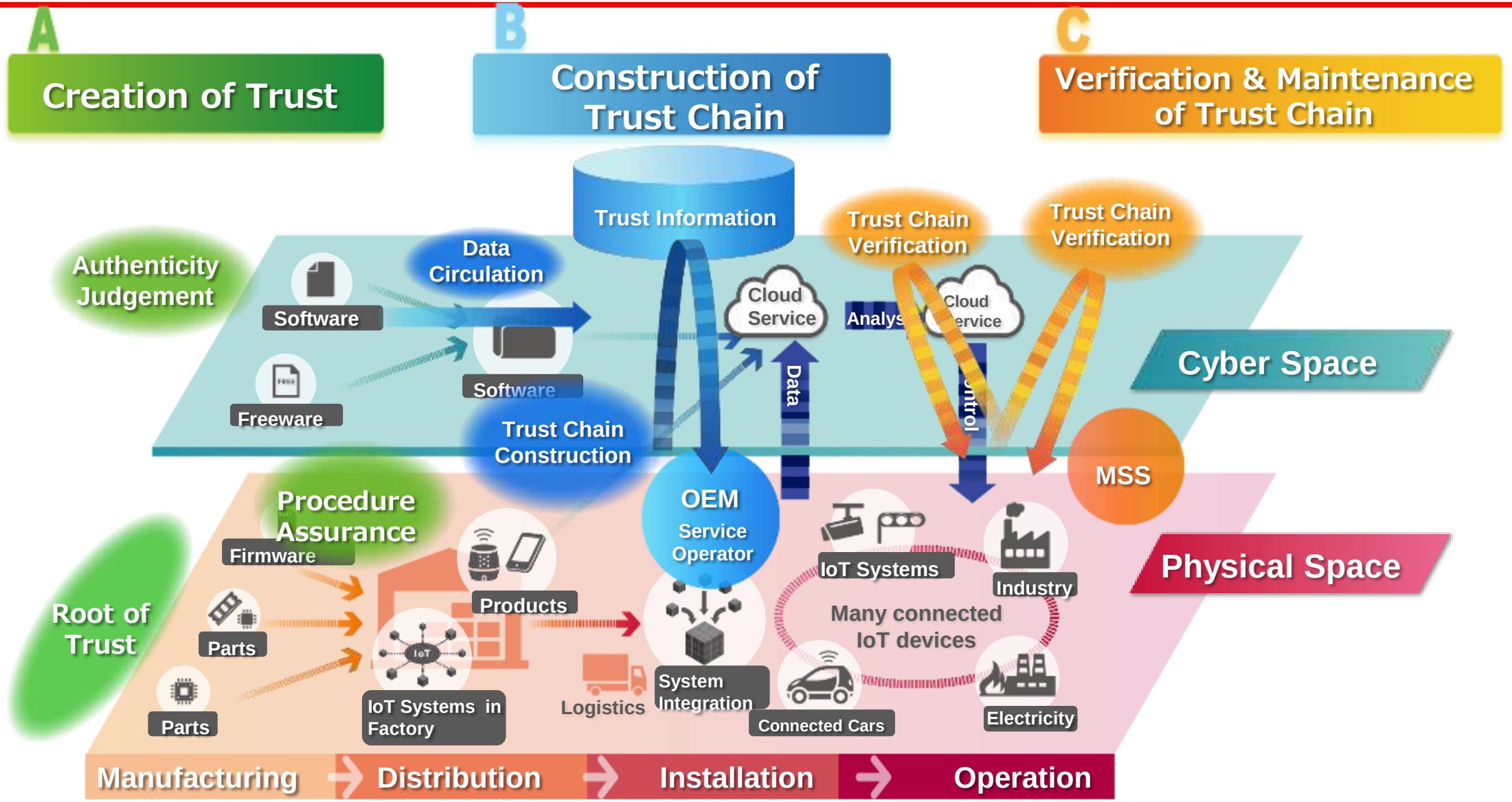
= €€€€€€€€€

Source: Wired on July 21, 2015 <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Supply chain risk: contamination, falsification, data breach



Cyber-Physical Security Eco-System for IoT Society



Three R&D Technology Goals in SIP/CPS (2018—2022)

R&D Budget: around €15M to € 20M annually for 5 years

A. Creation of Trust

1. Creating trust by tamper-resist cryptographic module embedded in IoT devices.
2. Confirming trust through monitoring of authenticity and integrity of IoT devices
3. Confirming trust through certification of the eligibility of procedures

B. Construction of Trust Chain

1. Constructing trust chain based on industry-specific profiles.
2. Safe distribution of information related to the trust chain using block chain technology

C. Verification & Maintenance of Trust Chain

1. Verifying trust chains between business operators.
2. Maintaining trust chains by detecting, analyzing, and mitigating anomalies in cyber-physical system.

SIP/CPS R&D team and Supporting Ministries

R&D Team by Industry-Academia Collaboration

Cabinet Office
(Management Staff)

PD Atsuhiro Goto

NEDO

Promotion Committee
Gov: NISC, METI, MIC, MOD, ・・・.
Academia, Industry

A. Creation of Trust
- NTT, Hitachi, NEC, KDDI, etc.
- ECSEC, AIST, YNU, UT, others

B. Construction of Trust Chain
- Fujitsu, Hitachi, NEC,KDDI, etc
- AIST, NII, others

C. Verification & Maintenance of Trust Chain
- Hitachi, NTT, NEC, KDDI, Mitsubishi etc.
- AIST, ATR, U-Osaka, others

Supporting Ministries in Japanese Government

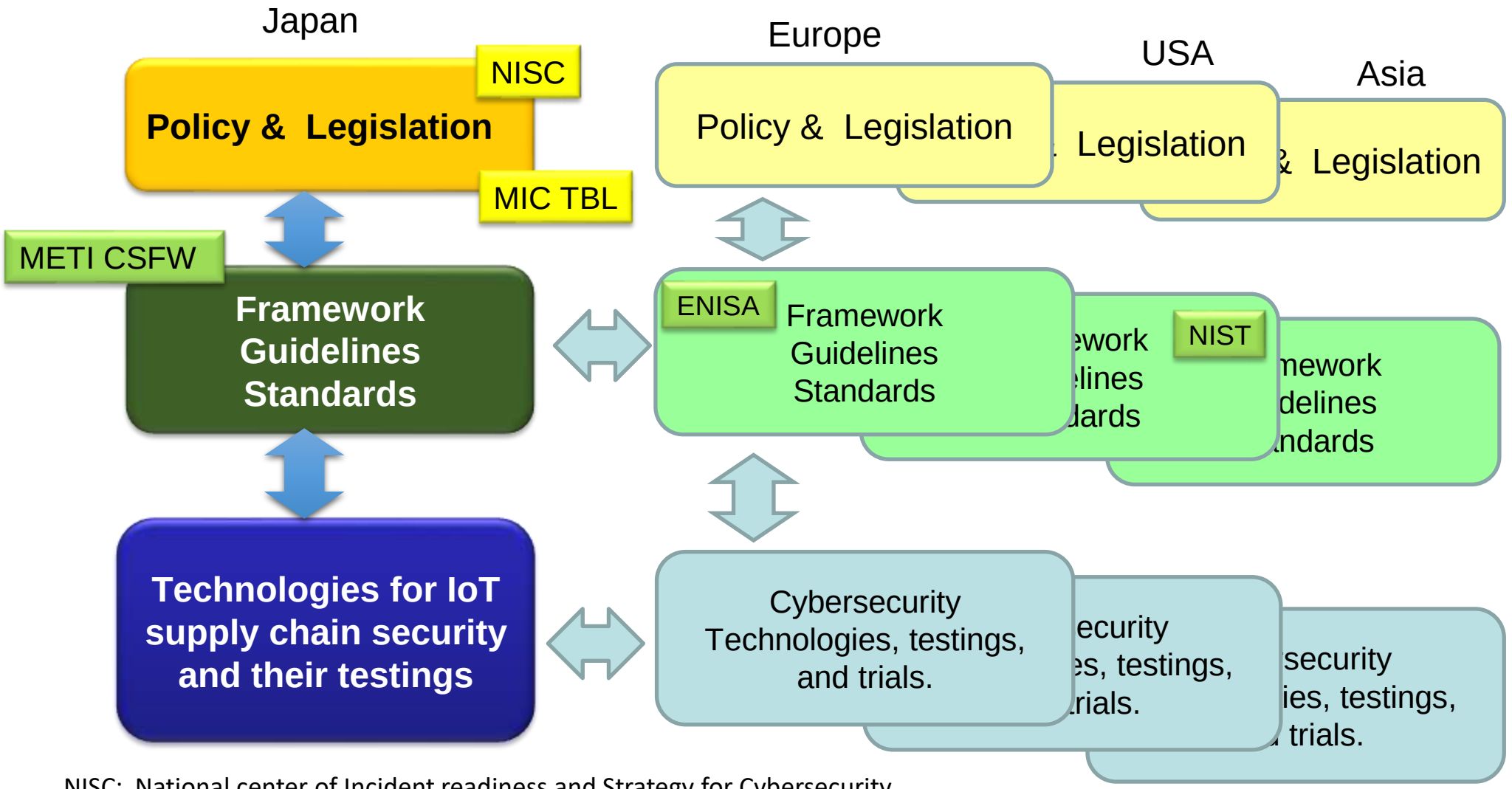
NISC
- SIP/CPS as a main R&D program in ***Cybersecurity Strategy***

METI
- SIP/CPS as an enabler of ***Cyber/Physical Security Framework***

MIC
- SIP/CPS as a possible contributor to 5G network security
- SIP/CPS collaborates with ***NOTICE*** Project

NISC: National center of Incident readiness and Strategy for Cybersecurity MIC: Ministry of Internal Affairs and Communications
METI : Ministry of Economy, Trade and Industry, NOTICE: (National Operation Towards IoT Clean Environment)

Vertical and Horizontal Harmonization



NISC: National center of Incident readiness and Strategy for Cybersecurity
MIC TBL: Ministry of Internal Affairs and Communications, Telecommunications Business Law
METI CSFW: Ministry of Economy, Trade and Industry, Cyber/Physical Security Framework

What are we doing and looking for?

To accomplish these three research goals,

- Practical experiments and trials in the “working” environment with support from industries (in smart manufacturing, logistics, buildings)
- Make research outputs compliant and consistent with relevant Regulations, Standards, Guidelines and Frameworks in Europe and U.S. as well as in Japan
- Share our ongoing status, challenges, and accomplishments with those who are concerned!

Suggestions?, interested?, or curious?

Please let us know any suggestions for opportunities:

- to learn and contribute to the latest regulations, standards, guidelines, and frameworks relevant to IoT and supply chain,

and

- to share our latest status, challenges, findings, and accomplishments with you!

Contact: goto@iisec.ac.jp

atsuhiro.goto.n9b@cao.go.jp

For more details & Related Information

LATEST SIP/CPS Plan above:

Source: Cross-Ministerial Strategic Innovation Promotion Program (SIP) Research and Development Plan for Cyber Physical Security for IoT Society <https://www.nedo.go.jp/content/100896109.pdf>

SIP overview

- https://www8.cao.go.jp/cstp/panhu/sip_english/sip_en.html

NISC Cybersecurity Strategy

- https://www.nisc.go.jp/eng/index.html

METI Cyber/Physical Security Framework [Appendix A]

- https://www.meti.go.jp/english/press/2019/0418_001.html

MIC NOTICE Project (National Operation Towards IoT Clean Environment) [Appendix B]

- https://notice.go.jp/en/

Questions?

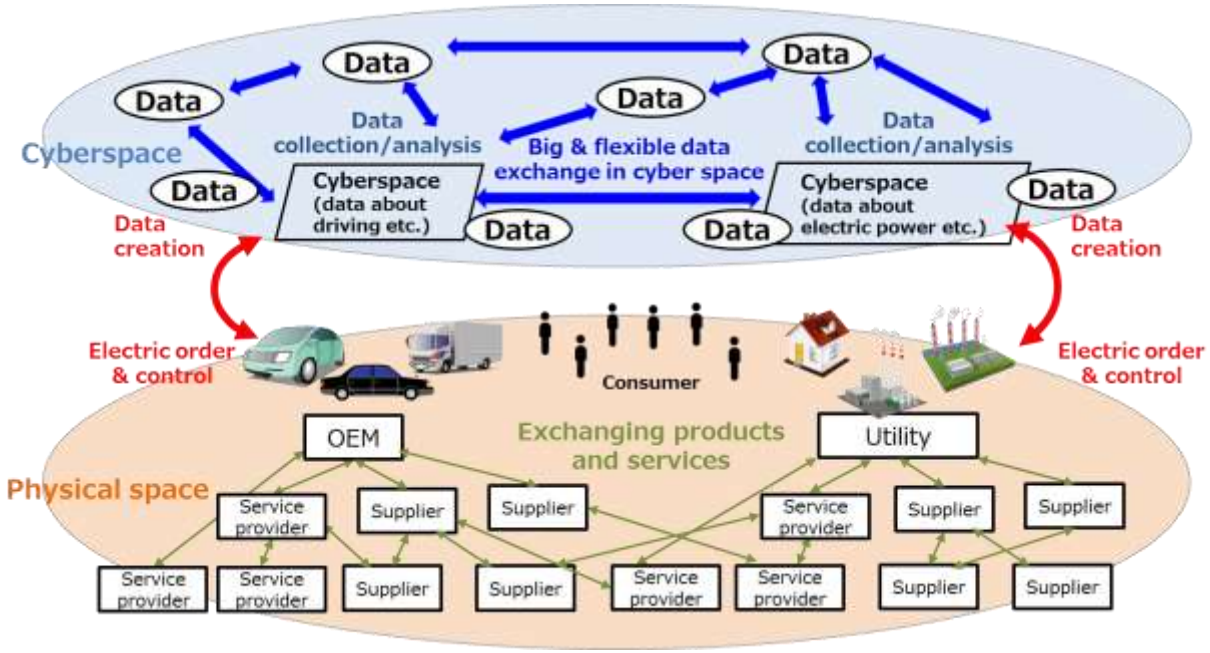
Appendix A

The Cyber/Physical Security Framework (CPSF)

Transforming society through cyber/physical integration

- Japanese government has proposed a new society, "**Society 5.0**", where **cyber and physical spaces are highly integrated** is coming.
- Supply chain is transforming from linear and fixed style to non-linear and flexible style. Ministry of Economy, Trade and Industry (METI) defined this **Society 5.0's new supply chain** as "**value creation process**".

[Society 5.0's Supply Chain (Value Creation Process)]



Big data circulation
⇒ **Importance of data control**

Integration of cyber / physical spaces
(expansion of border between cyber & physical through IoT)
⇒ **Cyber attack reaches physical space**

Complex Supply Chain
⇒ **Expansion of attacking points**

Cyber threats which give serious damages are expanding in whole supply chain

The Cyber/Physical Security Framework (CPSF)
～for value creation process in Society5.0's supply chain ～

- On April 18th 2019, METI released "**Cyber/Physical Security Framework (CPSF) ver 1.0**", which is a comprehensive framework for securing the "value creation process".

- The basic structure of CPSF is to **identify the risk source of the value creation process** in **Three Layers**, **present measure requirements for each risk source** for the **Six Elements**, and present specific examples of the measures.

◆Three Layers

The first layer
- Connections between organizations

The second layer
- Mutual connections between cyberspace and physical space

The third layer
- Connections in cyberspace

◆Six Elements

Organization, People, Components, Data, Procedure, System

Purpose of Three Layers' Approach

- Three layers' approach would be **useful to articulate and control complicated risks of "value creation process"**.

The Third Layer
(Connections in Cyber space)

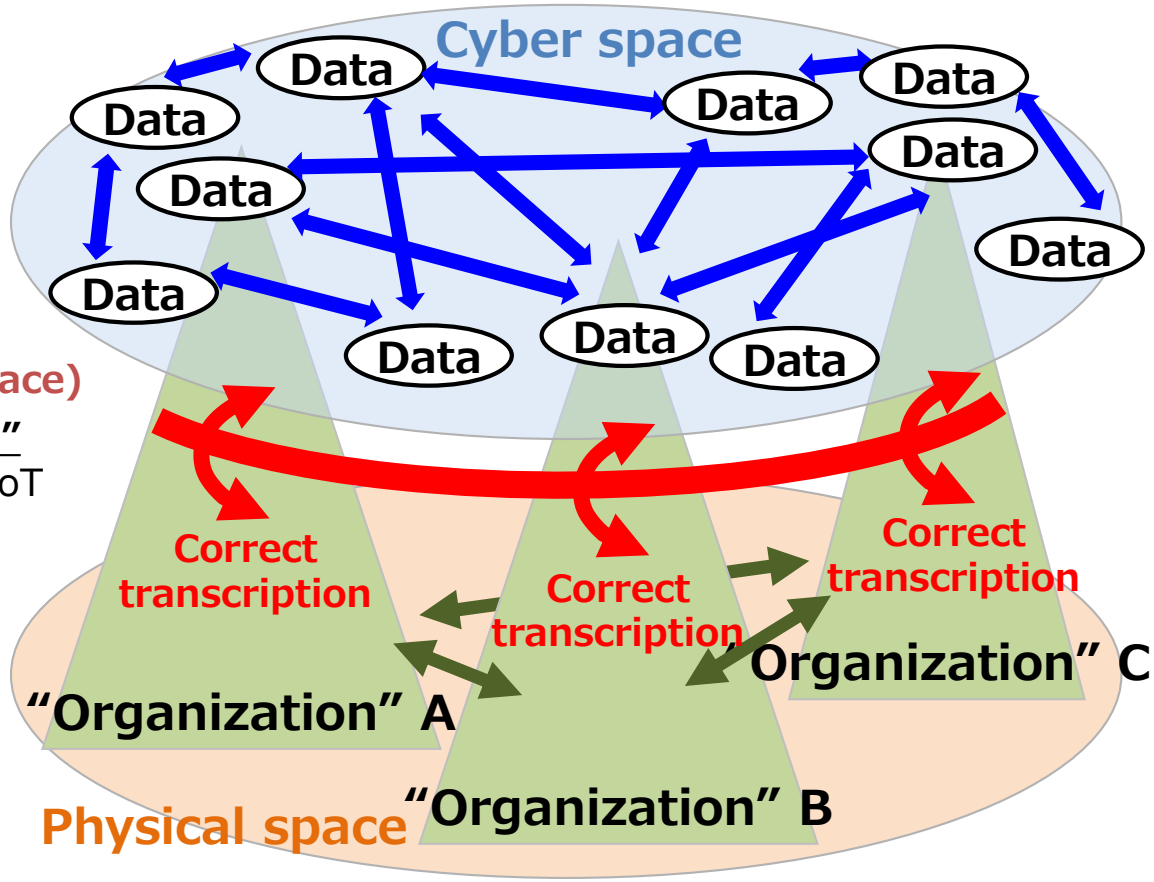
•**Trustworthiness of data** is a key for secured products and services

The Second Layer
(Connections between Cyber & Physical space)

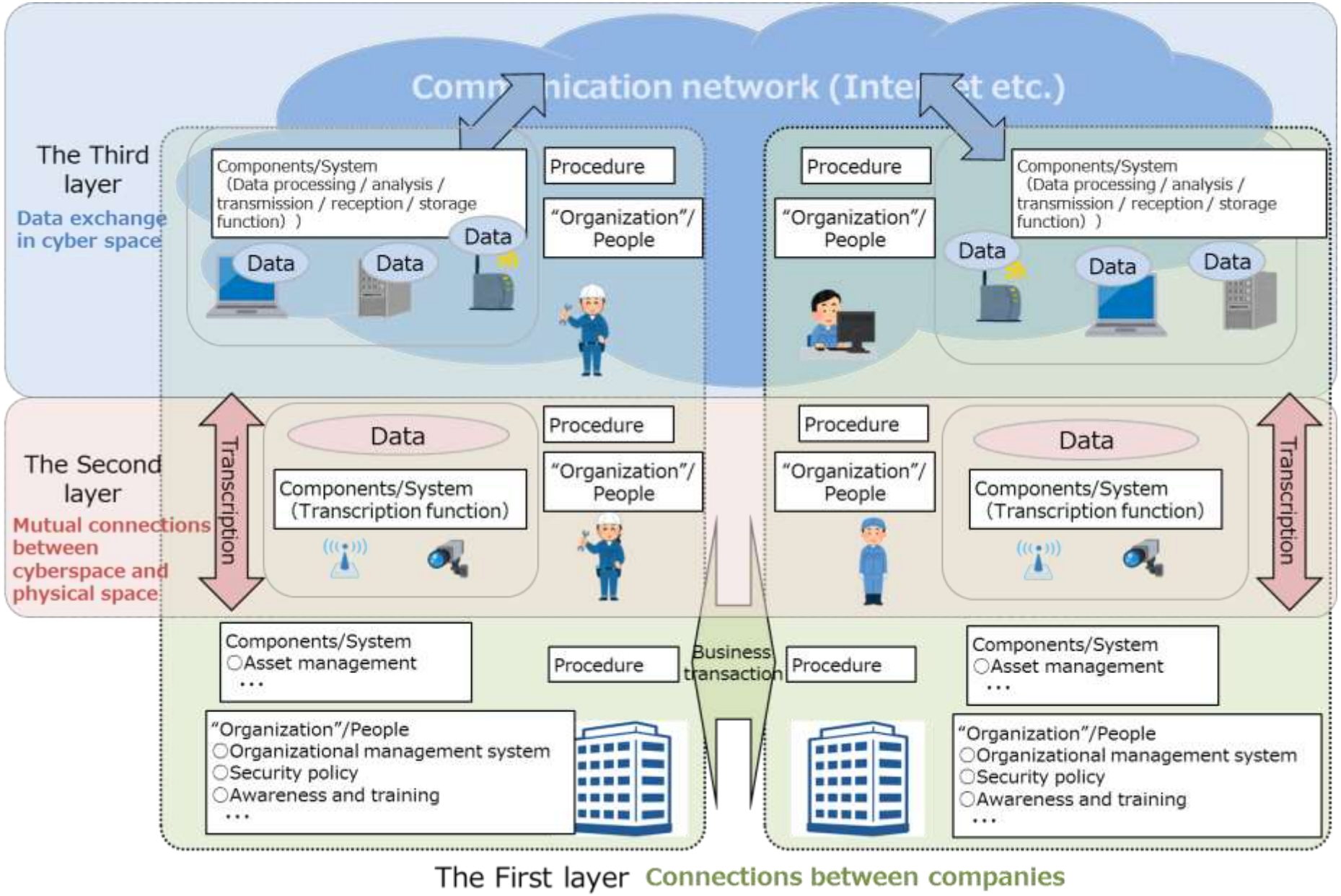
•**Trustworthiness of "transcription function" between cyber & physical space**, which is IoT system's essential function

The First Layer
(Connection between Organizations)

•**Trustworthiness of organization's management** is a key for secured products and services



Relationship of Six Elements in Three Layers



【Ref.】 The Cyber/Physical Security Framework (CPSF)

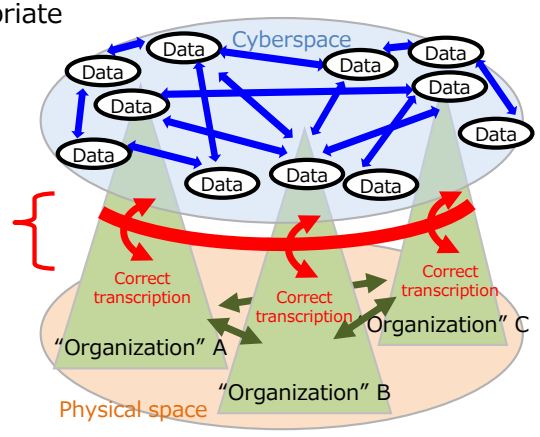
~ To ensure trustworthiness of a new type of supply chain in "Society5.0", so-called "Value Creation Process"

- While **"Society 5.0"**, where cyber and physical spaces are highly integrated, makes it possible to **construct non-linear and flexible supply chain**, this new supply chain, which is defined as "value creation process," faces **new risks such as an expansion of cyber attacking points and an increasing impact on physical infrastructure.**
- For this reason, **on April 18th 2019, METI released "Cyber/Physical Security Framework (CPSF) ver 1.0"**, which is a comprehensive framework for securing the new supply chain in society 5.0.
- **A wide variety of individuals and organizations from all over the world submitted various comments** (800 from 51 domestic and 22 foreign individuals and organizations) on CPSF through two times of public comments METI held. Through this process, CPSF earned an international attention.

"Three-Layer Model" proposed in CPSF

The Third Layer
(Connections in cyberspace)
Trustworthiness of data for service through appropriate management

The Second Layer
(Mutual connections between cyberspace and physical space)
Trustworthiness of function "correct transcription" from cyber to physical / from physical to cyber



The First Layer
(Connections between organizations)
Trustworthiness of each organization based on appropriate management

https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf

"Six Elements" proposed in CPSF

- In order to promote **a risk based security measures**, **six elements that make up the value creation process** are defined.

Organization	People	Components	Data	Procedure	System

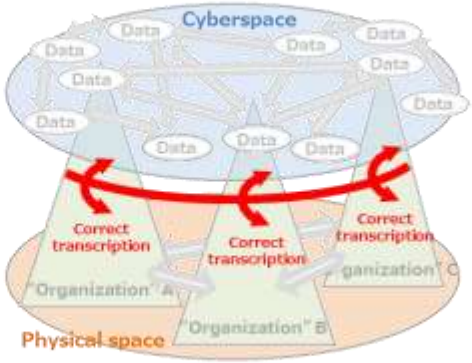
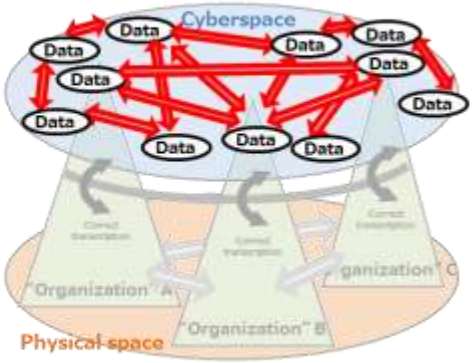
Risk Management Method in CPSF

Functions (of each layer) → **Security incidents** → **Risk sources (organized by the Six Elements)** → **Measure requirements** → **Examples of Security measures (classified into three levels)**
- High-Advanced
- Advanced
- Basic

Ensuring consistency between international standards and CPSF

- **Comparing CPSF with major international standards** (Part III, Appendix C and D)
- **Comparing each major international standard with CPSF** (Appendix D)
  - NIST Cybersecurity Framework
  - NIST SP800-171
  - ISO/IEC 27001 Annex A

【Ref.】 Brief image of CPSF

	Connections between Organizations [The First Layer]	Mutual connections between cyberspace and physical space [The Second Layer]	Connections in cyber space [The Third Layer]
Sort of new supply chain structure			
Function (Object to be protected)	• Establishing, operating and maintaining risk management system effective in both normal time and emergency/within and between organizations	• Correct transcription of data between physical space and cyber space	• Processing and analyzing data • Storing data • Sending and receiving data
Security incident	• Compromise of assets to be protected • Business stop due to the occurrence of security incident in other organization	• Sending incorrect data • Operation with safety problems	• Data leakage • Receiving data from an unauthorized organization due to spoofing
Risk source (Sorted by six elements)	• Lack of governance on security risks • Unknown status of cooperation with other organizations	• Connection with unauthorized IoT devices • Input data outside the permissible range	• Network is not protected • The connection destination is not identified
Measure requirement	■ Compliance with management rules ■ Clarification of role sharing with stakeholders	■ Authenticating the connection destination ■ Introduction of IoT device considering safety	■ Data protection by encryption ■ Confirming the trustworthiness of data providers

Appendix B

“NOTICE” Project

(1) Outline of the “NOTICE” Project

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

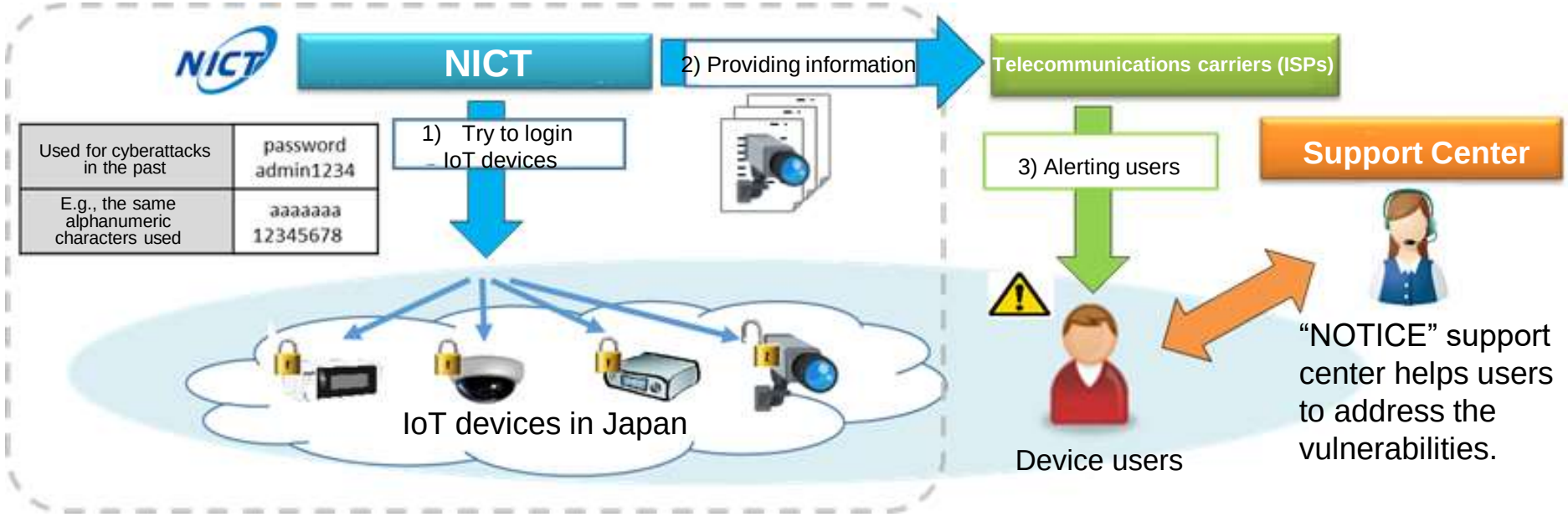
*National Operation Towards IoT Clean Environment

<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**.



(2) Project to Alert Users of IoT Devices Infected with Malware

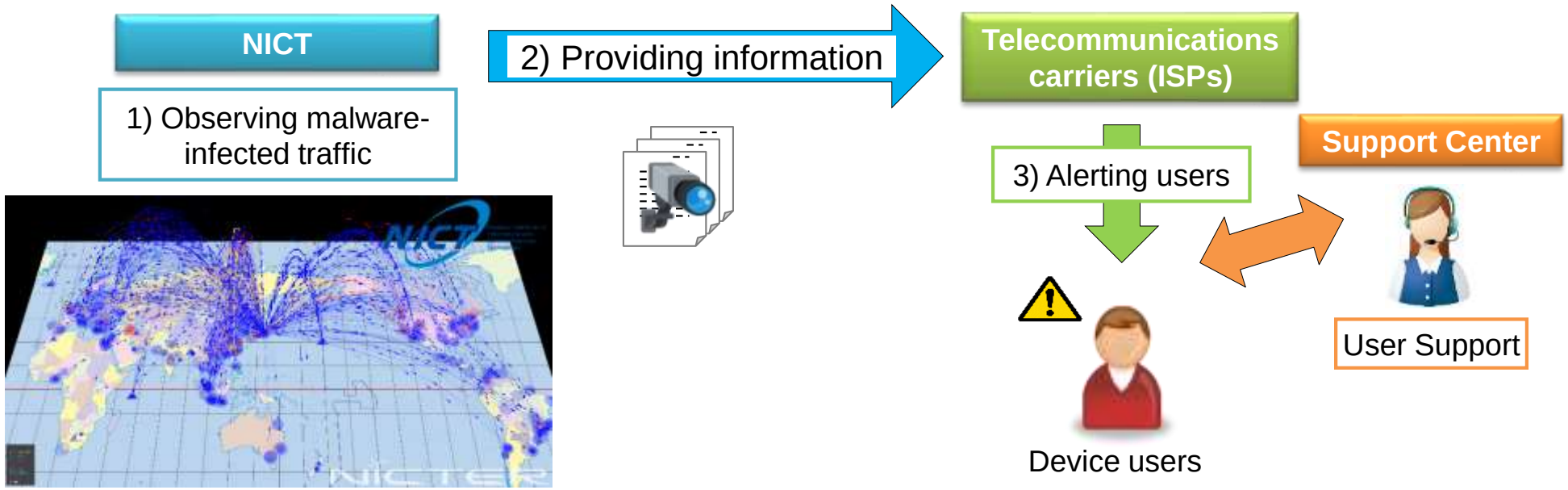
Along with NOTICE, MIC and the NICT, in cooperation with ISPs, conduct the project to identify devices infected with malware by using NICTER system and notify the ISPs so that they can alert users of the infected devices from mid June 2019.

<Overview of the project>

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

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

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



Progress on the Projects

Among 200 million IP addresses in Japan, approximately **90 million IP addresses** managed by **33 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. 31,000-42,000

In the above, the number of those which were **successfully logged-in** to with **weak password settings** and were **subject to user alert** → Total 147

(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** → 112-155 per day

The number of Internet Service Providers participating in the project is 33.
In addition to these measures, a proactive measure is required.

(⇒next page)

(3) Proactive measure for IoT security

Amendment of the Technical Condition of Terminal Equipment for IoT Security

- **Terminal equipment** that is directly connected to telecommunication network through internet protocol **is required to have**:
  1) access control on the remote control function,
  2) feature to **encourage its user to change the default IDs/passwords**
  3) firmware update feature for the future security fixes,
  or any equivalent/better security measures to/than 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 the guideline for the security requirements of the Technical Condition, which describes the scope of device types, details of the requirements, etc.

Schedule

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