

Towards the construction of reliable 5G infrastructure

Hiroaki Kamoda
Director for Policy Planning,
Cybersecurity Division

5 G infrastructure

Cyber/Physical Security Framework (CPSF)

Risks from Cybersecurity Viewpoints in 5G Infrastructure

(1) Hardware

- Because general purpose hardware will be mainly used in 5G infrastructure, **the scope of damage from a malfunction of an equipment would be larger compared to the case of 4G.** (In 4G infrastructure, specific purpose hardware is mainly used. So, the impact of a malfunction of an equipment is limited within a specific function)

(2) Software

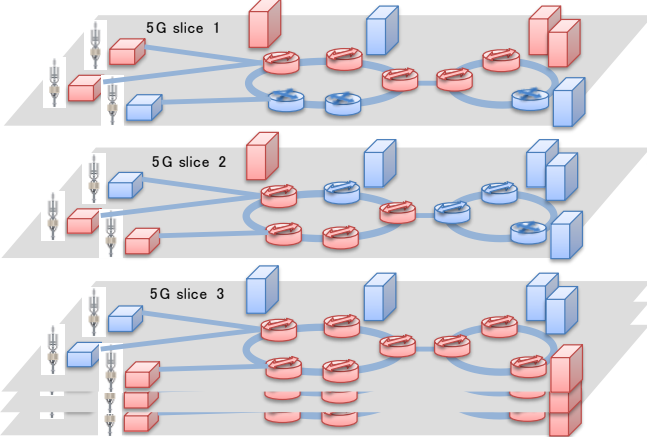
- **Fundamentally, verification on software is not perfect.** In addition, there will be huge, combined and complicated software in 5G, which will operate various functions. It's difficult to avoid vulnerability of software perfectly.

(3) Software update

- Because of (2), there will be frequent software updates in 5G, since the software is updated in 5G infrastructure. **There is no perfect real-time verification technology for software.** It means that **trustworthiness of entities involved into 5G infrastructure is much more important compared to the case of 4G.**

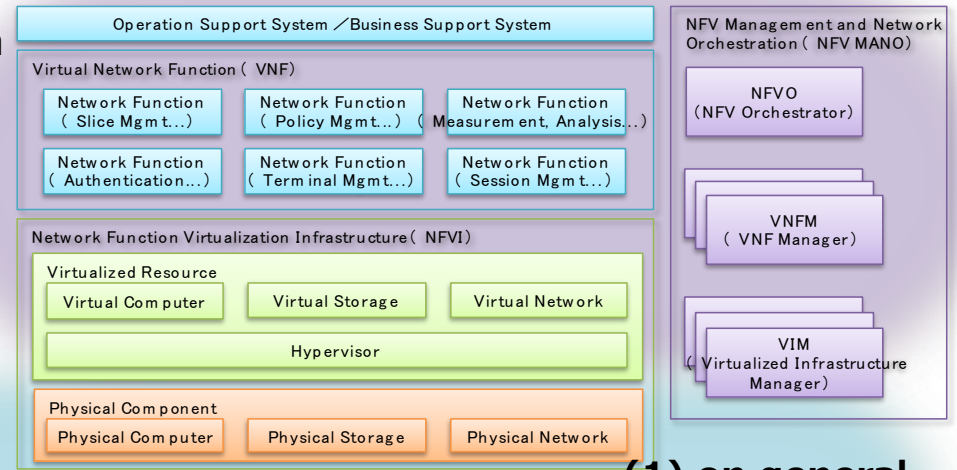
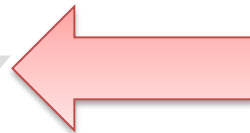
【 5 G infrastructure】

Logical network for each purpose
(Specific functions and performance can be selectable for its' purpose)

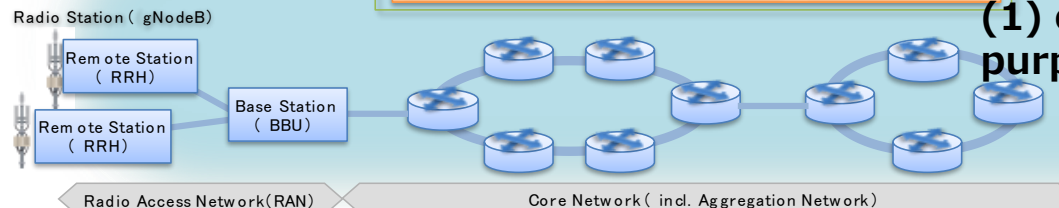


(3) supplying network slices as separated logical networks

(2) building a network with software



(1) on general purpose hardware



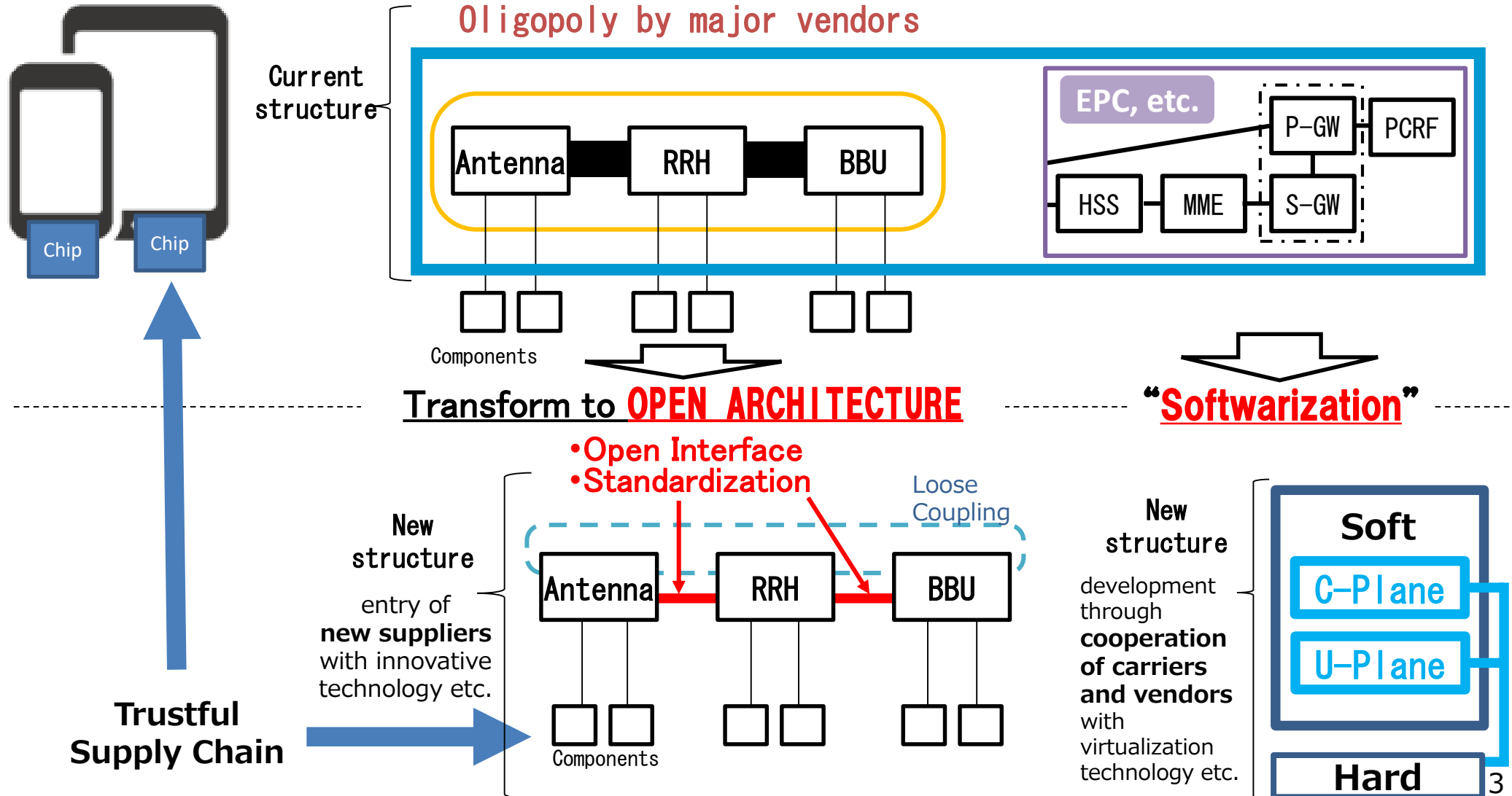
Transformation of Industrial Structure for 5G Construction

- To introduce robust & innovative infrastructure with innovative & reliable suppliers, "Open Architecture", requiring open interfaces among functions, should be realized.

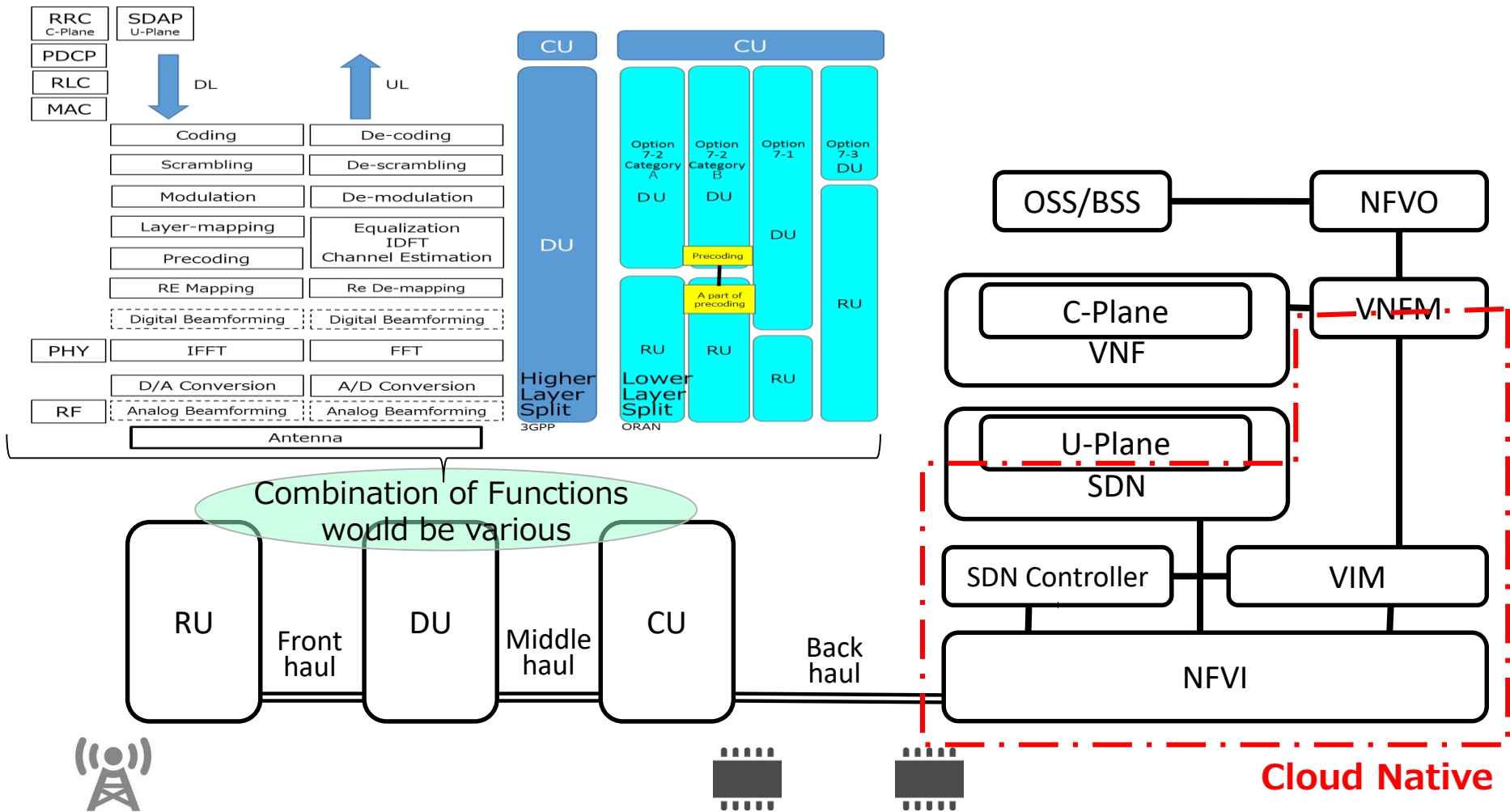
1. User Equipment

2. RAN (Radio Access Network)

3. Core Network

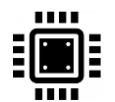


Assumed Basic Structure of 5G Infrastructure



Combination of Functions would be various

Cloud Native



- RU : Radio Unit
- DU : Distributed Unit
- CU : Centralized Unit
- VNF : Virtualized Network Function
- VIM : Radio Resource Control
- SDN : Software Defined Network
- NFVI : Network Function Virtualized Infrastructure
- VNFM : Virtualized Network Function Management
- NFVO : NFV Orchestrator
- OSS/BSS : Operation Support System/Business Support System

5G infrastructure

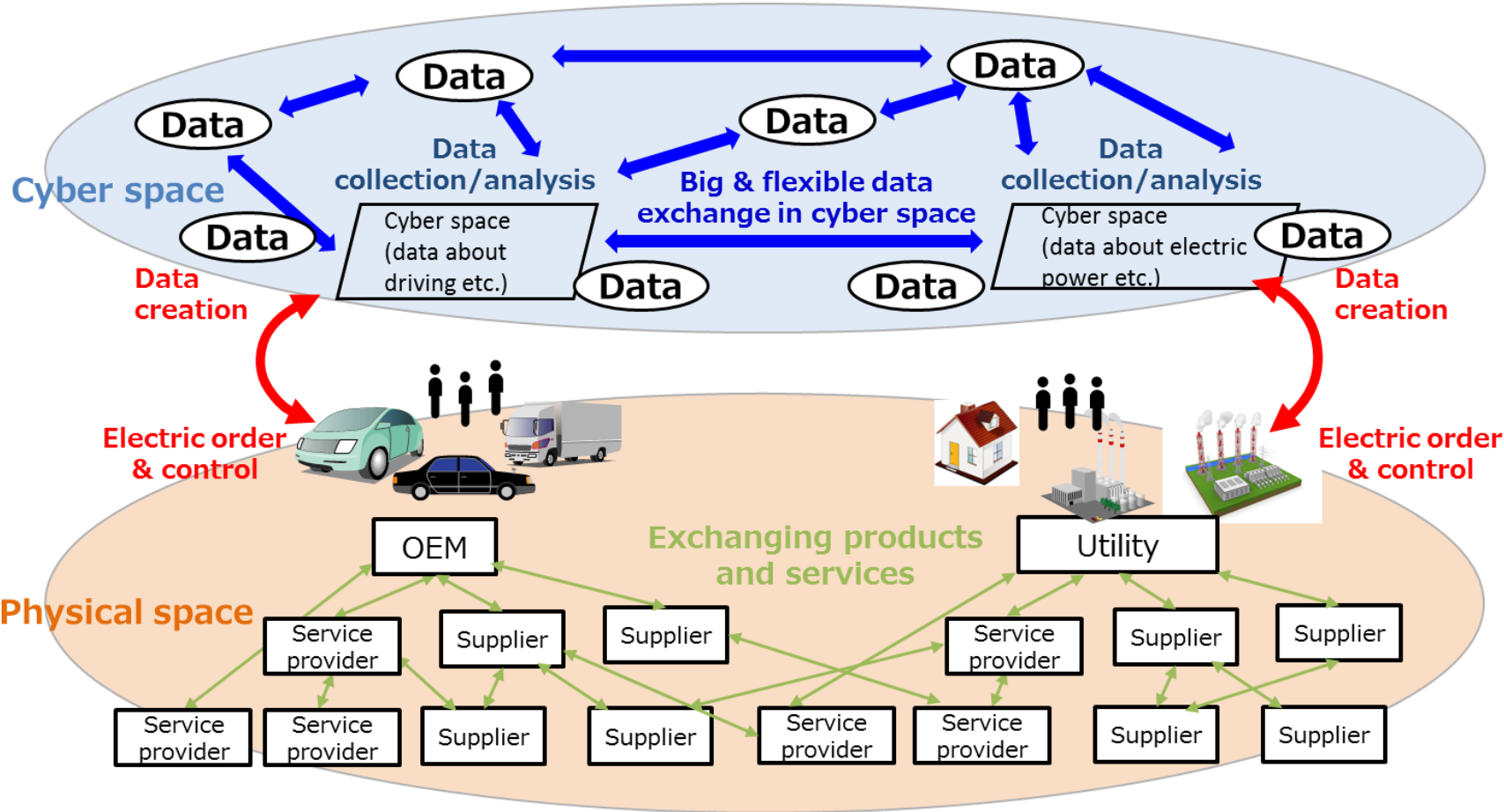
**Cyber/Physical Security Framework
(CPSF)**

Supply Chain in Society 5.0 (Cyber-Physical Integrated Society)

<Conventional Supply Chain>



<Society 5.0's Supply Chain (Value Creation Process)>



Purpose of Three Layers' Approach

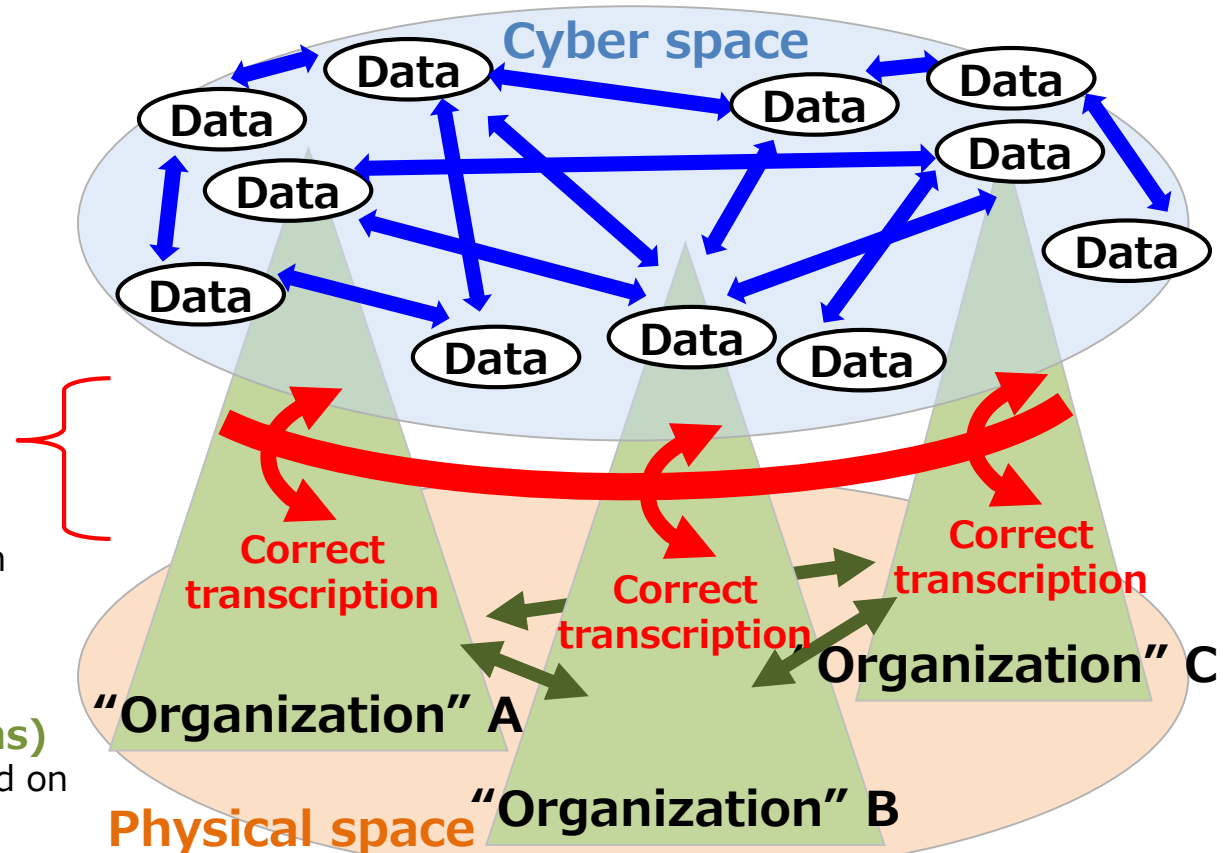
- Three layers' approach would be useful to articulate and control complicated risks of the new supply chain, "value creation process".
- Each layer has a unique role to protect trustworthiness of organization, transcription, and data.

- 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



The Cyber/Physical Security Framework (CPSF)

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

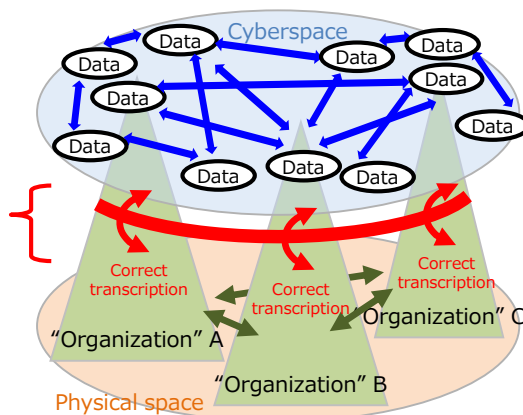
- While "**Society 5.0**", where cyber and physical spaces are highly integrated, makes it possible to **construct non-linear and flexible supply chain**, this new supply chain, which is defined as "value creation process," faces **new risks such as an expansion of cyber attacking points and an increasing 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)

The Second Layer
(Mutual connections between cyberspace and physical space)

The First Layer
(Connections between organizations)



"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

Data

People

Procedure

Components

System

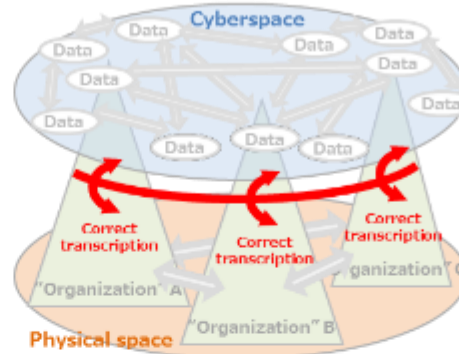
Brief image of CPSF

Connections between Organizations [The First Layer]

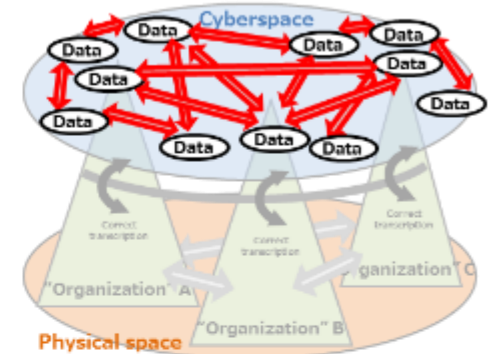


Sort of new supply chain structure

Mutual connections between cyberspace and physical space [The Second Layer]



Connections in cyber space [The Third Layer]



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

20 categories of security measures

Category Name	acronym	Related category of NIST Cybersecurity Framework v1.1
Asset Management	CPS.AM	ID.AM (Asset Management)
Business Environment	CPS.BE	ID.BE (Business Environment)
Governance	CPS.GV	ID.GV (Governance)
Risk Assessment	CPS.RA	ID.RA (Risk Assessment)
Risk Management Strategy	CPS.RM	ID.RM (Risk Management Strategy)
Supply Chain Risk Management	CPS.SC	ID.SC (Supply Chain Risk Management)
Identity Management, Authentication, and Access Control	CPS.AC	PR.AC (Identity Management and Access Control)
Awareness Improvement and Training	CPS.AT	PR.AT (Awareness and Training)
Data Security	CPS.DS	PR.DS (Data Security)
Processes and Procedures to Protect Information	CPS.IP	PR.IP (Information Protection Processes and Procedures)
Maintenance	CPS.MA	PR.MA (Maintenance)
Protection Technology	CPS.PT	PR.PT (Protective Technology)
Abnormal Activities and Events	CPS.AE	DE.AE (Anomalies and Events)
Continuous Monitoring of Security	CPS.CM	DE.CM (Security Continuous Monitoring)
Detection Process	CPS.DP	DE.DP (Detection Processes)
Response Plan	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
Communication	CPS.CO	RS.CO (Communications) RC.CO (Communications)
Analysis	CPS.AN	RS.AN (Analysis)
Mitigation	CPS.MI	RS.MI (Mitigation)
Improvement	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

Development of sector-specific measures and guidelines

METI's Study Group on Industrial Cybersecurity

WG 1 Rules, Technology, Standards

[Held 5 times since Feb. 2018~]

→ **Developed The CPS Framework in Apr. 2019**

Standard Model

Examine sector-specific security measures in Sub WGs

- Building (EV, EMS, etc)
- Electric Utility
- Defense
- Auto Vehicle
- Smart Home
- And so on

[Held 8 times since Feb. 2018~]

→ **Developed the 1st Draft of Guideline**

[Held 4 times since Jun. 2018~]

[Held 8 times since Mar. 2018~]

[Held once since Apr. 2019~]

[Held 8 times since Mar. 2018~]

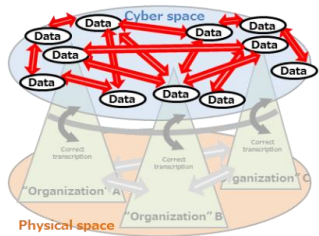
Cross-sectoral SWG

Collaboration Platform

Proposal of International Standards & Mutual Recognitions

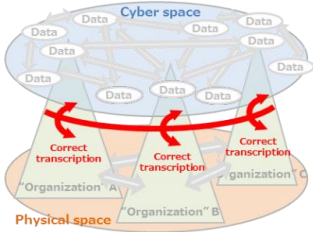
Further discussions based on CPSF

[3rd layer]



Connections in Cyber space

[2nd layer]



Connections between Cyber & Physical space

Industrial activities

Cross sectoral cooperation with data

By Sector

- Building
- Electric Utility
- Defense
- Auto Vehicle
- Smart Home, etc.

By Scale

- Large companies
- SMEs, and etc.

[1st layer]
Connections between Organizations

Rules and methodologies for verification of trustworthiness

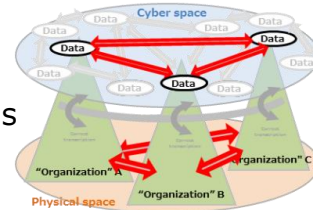
Trustworthiness of Data
(integrity & authenticity of data, etc.)

Trustworthiness of Transcription Function of IoT

- IoT devices
- IoT systems, etc.

Trustworthiness of Software

- Software component transparency, etc.



METI's WG to Develop CPSF

CPSF as a Standard Model

Cross-sectoral SWG

Building (EV, EMS, etc) SWG

Electric Utility SWG

Defense SWG

Smart Home SWG

Auto Vehicle SWG

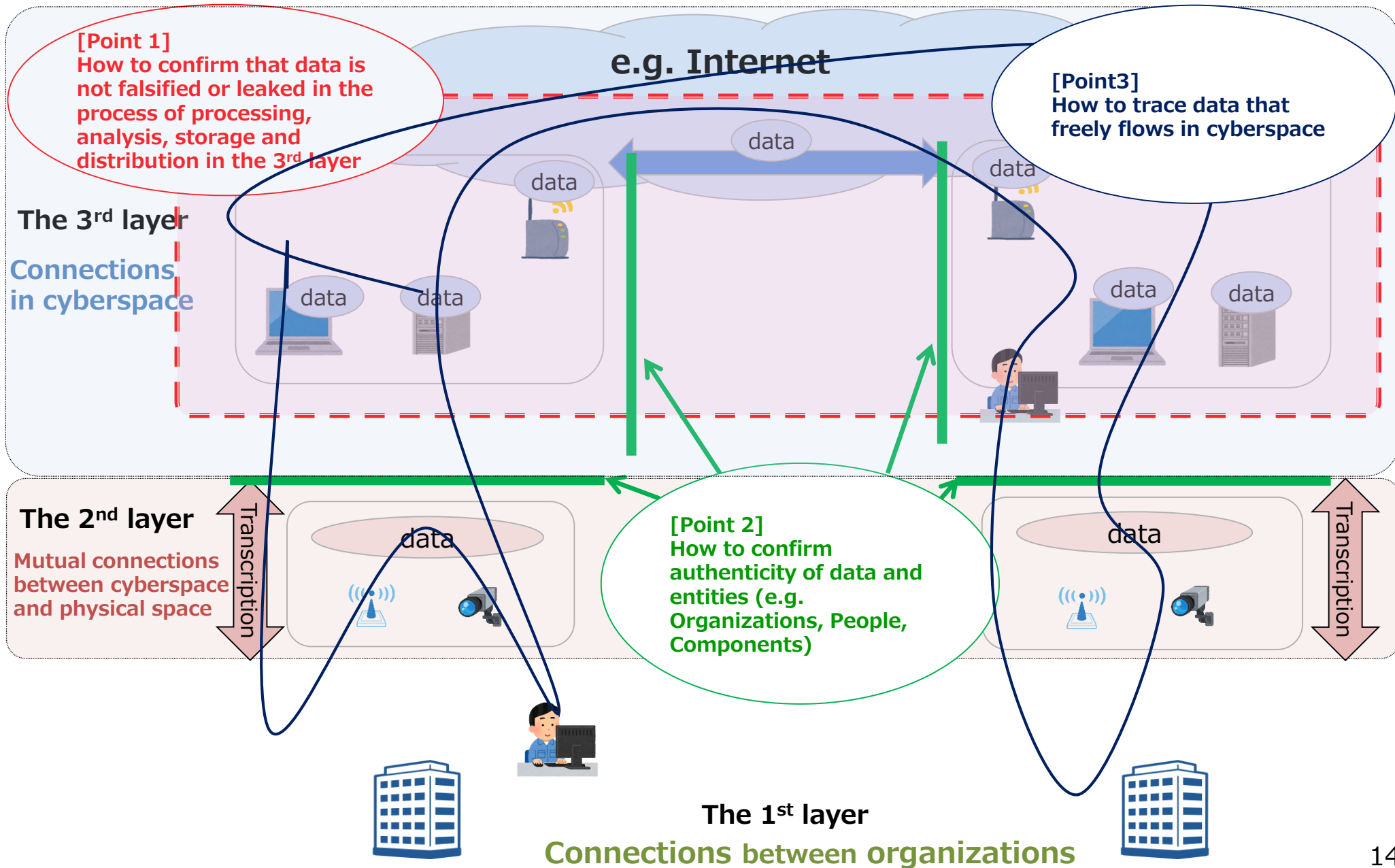
And so on

『3rd layer』 TF (⇒ Security requirement for each data category)

Software TF (⇒ Software management including OSS)

『2nd layer』 TF (⇒ Security requirements for IoT systems, etc.)

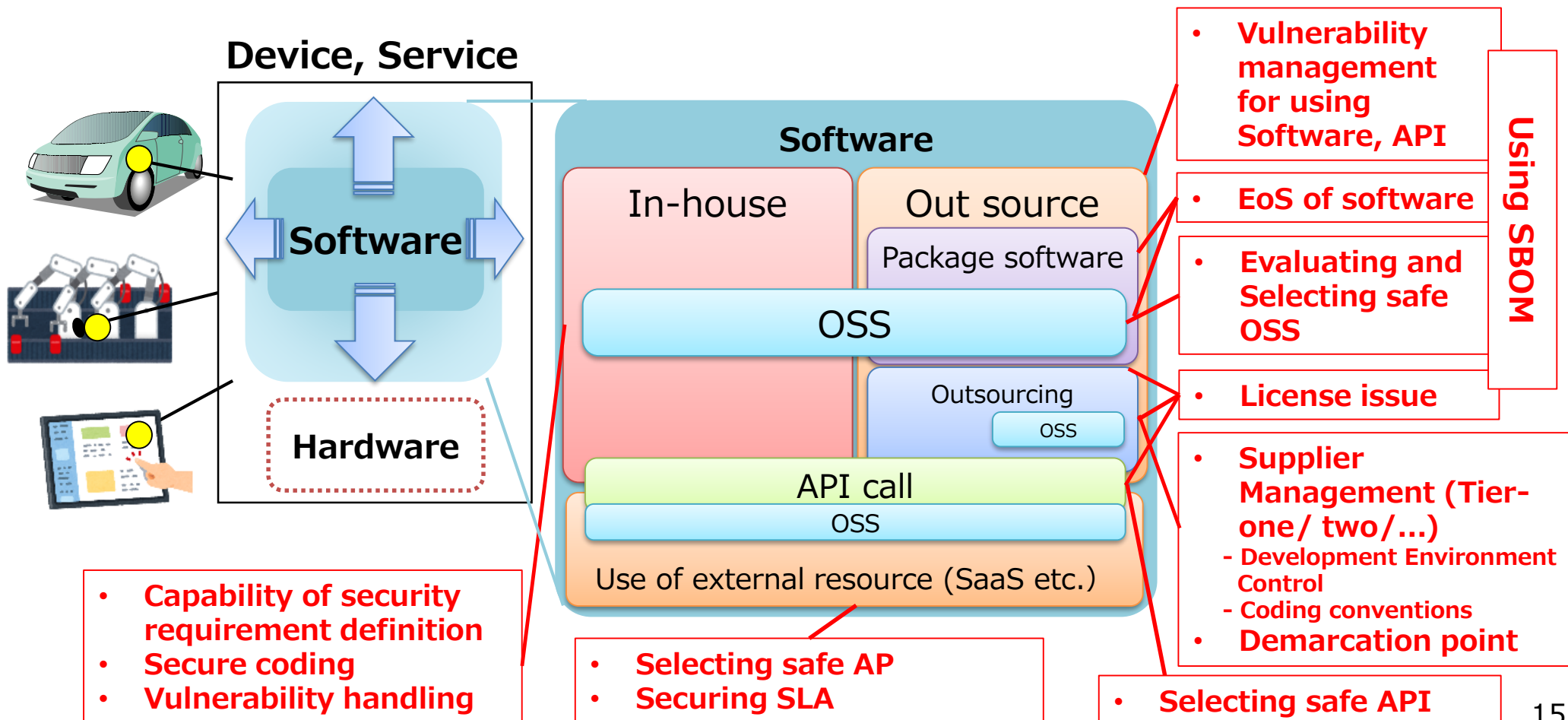
[3rd Layer TF] Discussion Points for Ensuring Trustworthiness of **Data**



[Software TF] Effective Methods for **Software** management

- Software TF aims to discuss cross-sectoral methods for effective software management, taking into account related int'l discussions including NTIA's Software component Transparency initiative.

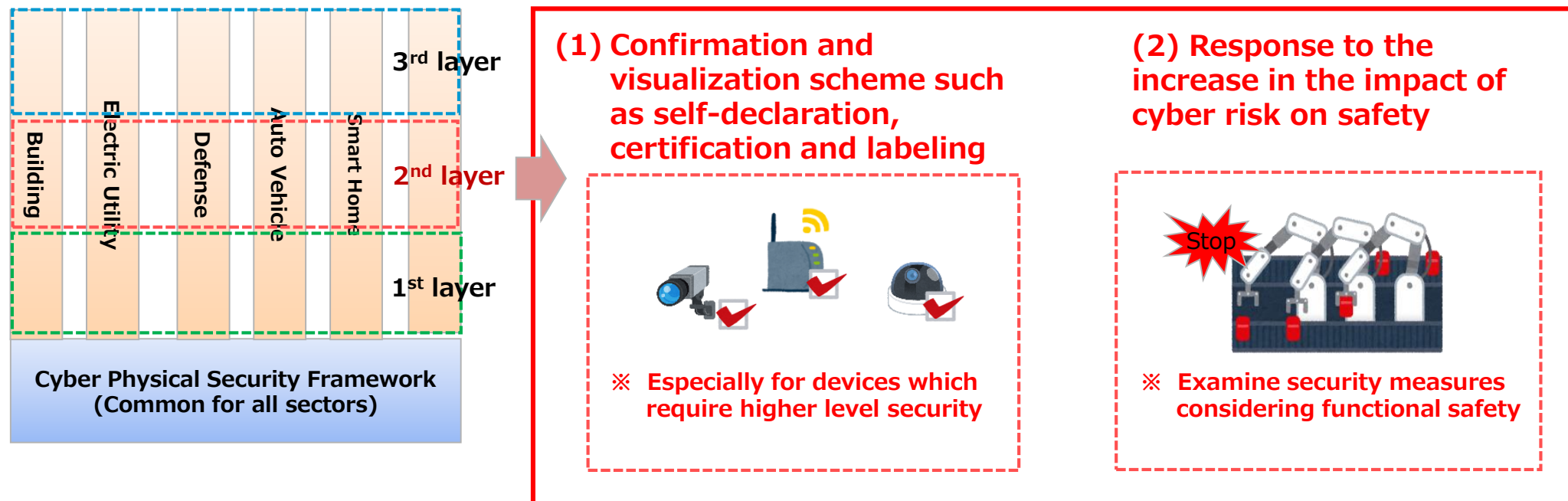
Illustration of issues concerning software



[2nd Layer TF] Discussions on Cross-sectoral Issues of **IoT** Security

- 2nd Layer TF aims to discuss ways to confirm and visualize IoT security like certification, labeling, and ways to treat fusion of security and functional safety from the cross-sectoral viewpoint.
- This TF refers to sector-specific issues covered by existing sector-specific SWGs when necessary.

An idea of discussion points for 2nd Layer TF





METI

Ministry of Economy, Trade and Industry

Interagency Agreement for Government Procurement of IT system, Equipment, and Services and Procurement Procedure (Excerpt)

1. Purpose

[issued on Dec 10, 2018]

In order to further improve cybersecurity measures in government agencies responding to increasingly complicated cyber attacks, government's new efforts are needed to reduce the serious adverse effects of cybersecurity in the procurement of information systems, devices, services, etc. related to important operations. Regarding the basic policies and procedures of procurement concerning information systems, equipment, services that should be specially protected in each ministry and agency, ministries agree and clarify necessary measures to be taken as follows.

3. Criteria to be referenced

In the procurement of information systems, devices, services, each ministry or agency especially consider points set forth in "Part 4: Outsourcing" and "Part 5: Information system life cycle" of the "Uniform Standard for information security measures of government agencies" (FY2018 version) (Decision of Cyber Security Strategy Headquarters on July 25, 2020) .

Guidelines for developing measures standards for Government Agencies (Excerpt)

5.1.2 (1) Regulations on procurement of equipment

[issued on Jul 25, 2018]

(a) The Chief Information Security Officer should establish the selection criteria for equipment, etc. If necessary, add criteria on management without unauthorized change in the life cycle of development of devices etc., and the appropriate management could be confirmed.

(Commentary) On 5.1.2(1)(a) "without unauthorized change"

It is required not to procure devices that can not be dispelled by the possibility of incorporating malicious functions in the development/manufacturing process, and devices of companies that can not be dispelled from concerns regarding supply chain risk by means of taking supply chain risk as one of the requirements on the procurement, based on information on domestic and foreign information security.

Guidelines for establishing specific base stations for introduction of the 5th Generation Mobile Communication System(Excerpt)

[issued on Dec 14, 2018]

6. Matters on promotion of smooth establishment of specific base stations and other necessary matters

3 Person/Entity that applies for authorization of establishment plan pertaining to this establishment guideline must submit the development plan, described according to Article 27-13 Paragraph 2 of the law, Article 25-4 Paragraph 2 and Schedule 1 of the license rule, to the Minister of Internal Affairs and Communications.

Schedule 1: Matters to be described in the development plan

1 (Omitted)

2 Matters concerning ability to smoothly develop a specific base station according to the development plan

1 (Omitted)

2 Plan for procurement of radio equipment of specific base station (attention should be paid to the "Uniform Standard for information security measures of government agencies" (FY2018 version) , "Interagency Agreement for government procurement of IT system, equipment, and services and procurement procedure (issued on Jul 25, 2018).) and its basis

3 (Omitted)

3 Matters concerning technical ability to install and operate telecommunications facilities

1 (Omitted)

2 Plan for procurement of radio equipment of specific base station (attention should be paid to the "Uniform Standard for information security measures of government agencies" (FY2018 version) , "Interagency Agreement for government procurement of IT system, equipment, and services and procurement procedure (issued on Jul 25, 2018).) and its basis

3-5 (Omitted)

[3rd Layer TF] Discussion Points for Ensuring Trustworthiness of **Data**

Considering appropriate security measure requirements according to data category

Managing data securely

⇒ Clarification of security requirements of, for example, management, process, security policy and system requirement.

confidentiality

integrity

availability

Considering confirmation methods for trustworthiness of data

Confirming data itself and data producers themselves
⇒ Confirming authenticity of data and Components, etc.

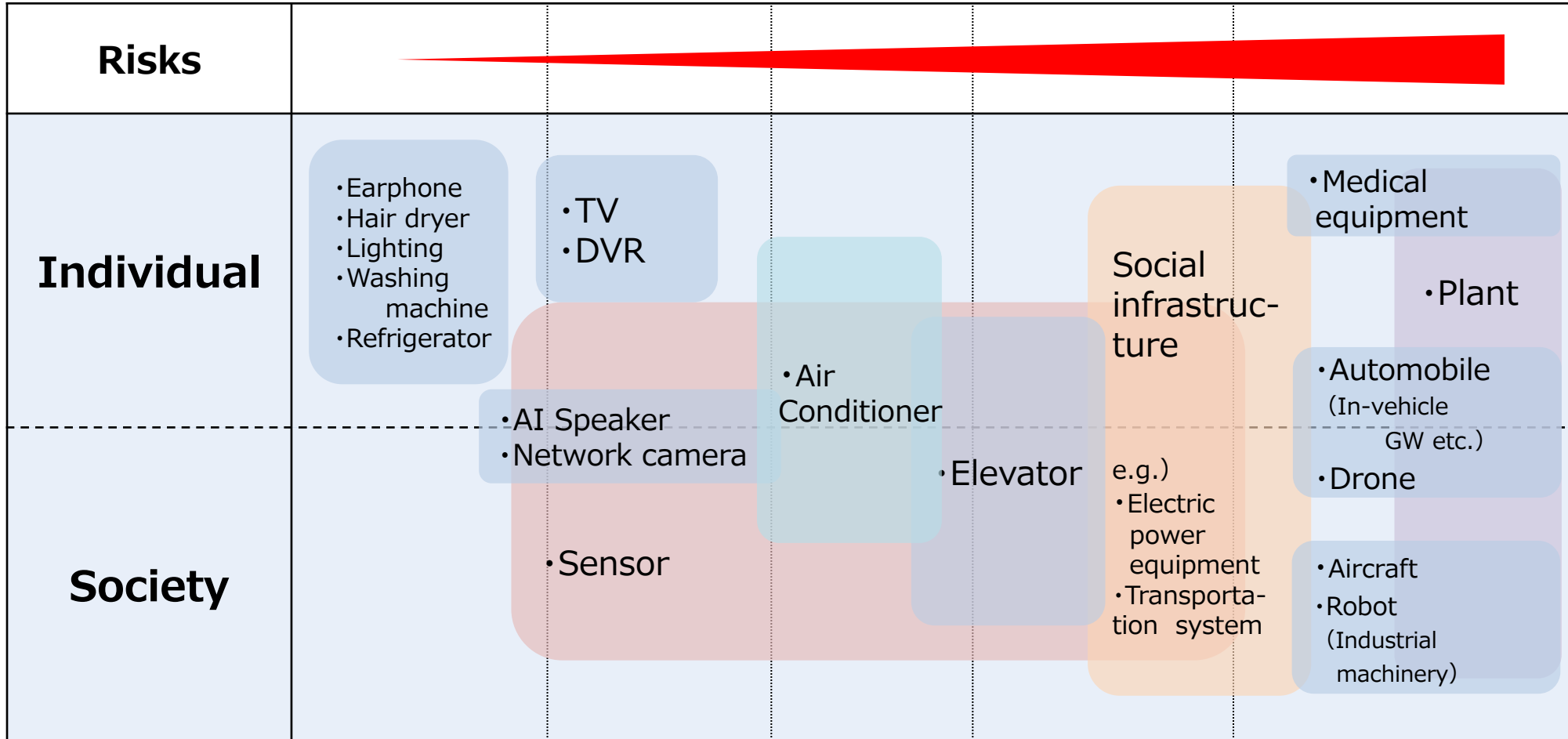
authenticity

Confirming data flow
⇒ Confirming traceability, etc.


accountability

non-repudiation

[2nd Layer TF] An idea of hidden risks in devices that connect cyber and physical spaces



[2nd Layer TF] An idea of Categorization from the point of view of Depth and Range of Damage

Risks			
Individual	<ul style="list-style-type: none"> • Earphone • Hair dryer • Lighting • Washing machine • Refrigerator <p>Trouble to daily life</p>	<ul style="list-style-type: none"> • TV • DVR <p>Serious trouble to daily life</p>	<ul style="list-style-type: none"> • Medical equipment • Plant <p>Damage to life and property</p>
Society	<ul style="list-style-type: none"> • AI Speaker • Network camera <p>Adverse impact on business activity</p>	<ul style="list-style-type: none"> • Elevator (e.g.) • Electric power equipment • Transportation system <p>Suspension of business activity</p>	<ul style="list-style-type: none"> • Drone • Aircraft • Robot (Industrial machinery)

[Software TF] Effective Methods for **Software** management

	In Development	In Operation (Gathering vulnerability information)	In Operation (Vulnerability response)
HeartBleed		<ul style="list-style-type: none"> ✓ Understanding the version information of the OSS in use 	<ul style="list-style-type: none"> ✓ Update of OSS ✓ Interim protection using WAF, etc. ✓ Service suspension
Apache Struts - ClassLoader Security Bypass Vulnerability		<ul style="list-style-type: none"> ✓ Assessment of vulnerability information ✓ Confirmation of EoS 	
Copay - Modified to load malicious code	<ul style="list-style-type: none"> ✓ Assessment of development process 	<ul style="list-style-type: none"> ✓ Understanding the version information of the OSS in use ✓ Assessment of vulnerability information ✓ Verifying code signing certificate 	
Triada - pre-installed by Third-party vendor			<ul style="list-style-type: none"> ✓ Update of software ✓ Interim protection using FW, etc. ✓ Suspension of the use of software
ASUS - update server hacked	<ul style="list-style-type: none"> ✓ Security assessment of update server 	<ul style="list-style-type: none"> ✓ Assessment for vulnerability information 	<ul style="list-style-type: none"> ✓ Anti-Malware
OSS license violation	<ul style="list-style-type: none"> ✓ Confirmation of License 		<ul style="list-style-type: none"> ✓ Correction of license violation

Optimization by JVN, etc. (Japan Vulnerability Notes)
 Optimization by SBoM, etc.

Optimization/Automation by STIX/TAXII