METI
Ministry of Economy, Trade and Industry

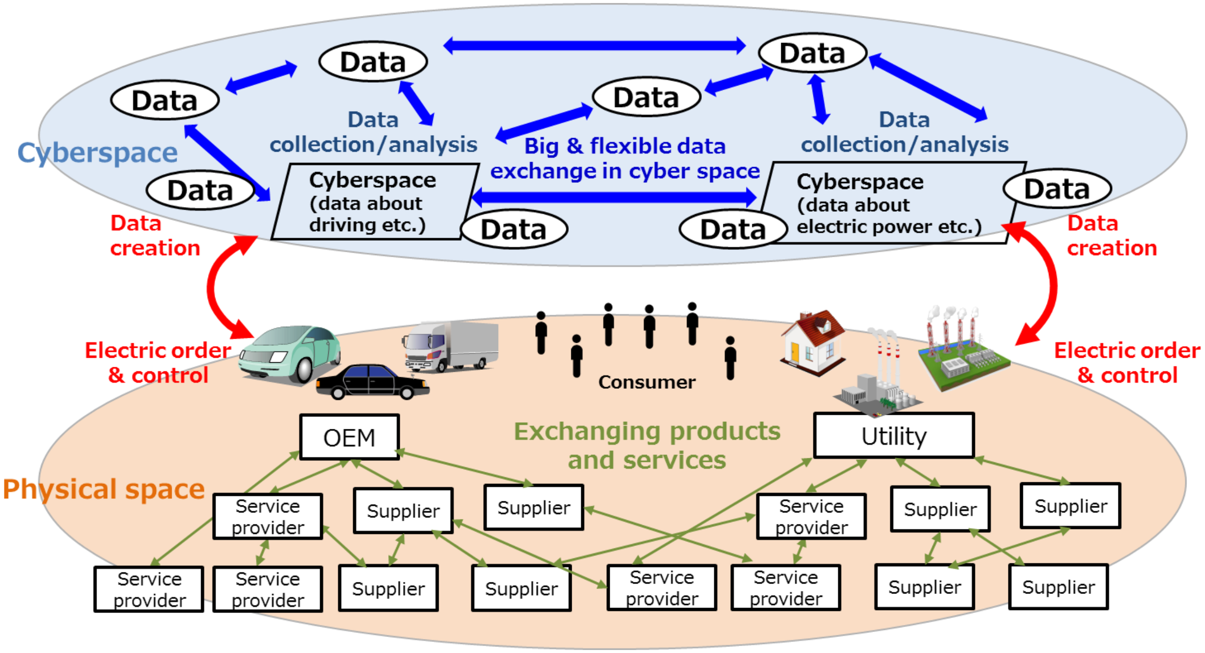
Cyber/Physical Security Framework
&
Basic Frame for IoT Security Management

Toshikazu Okuya
Director, the Cybersecurity Division
Ministry of Economy, Trade and Industry

Transforming society through cyber/physical integration

- 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. METI defined this Society 5.0’s new supply chain as “**value creation process**”.
- Cyber threats are also expanding according to this structural change.

[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

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 Cyber space)

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

The Second Layer

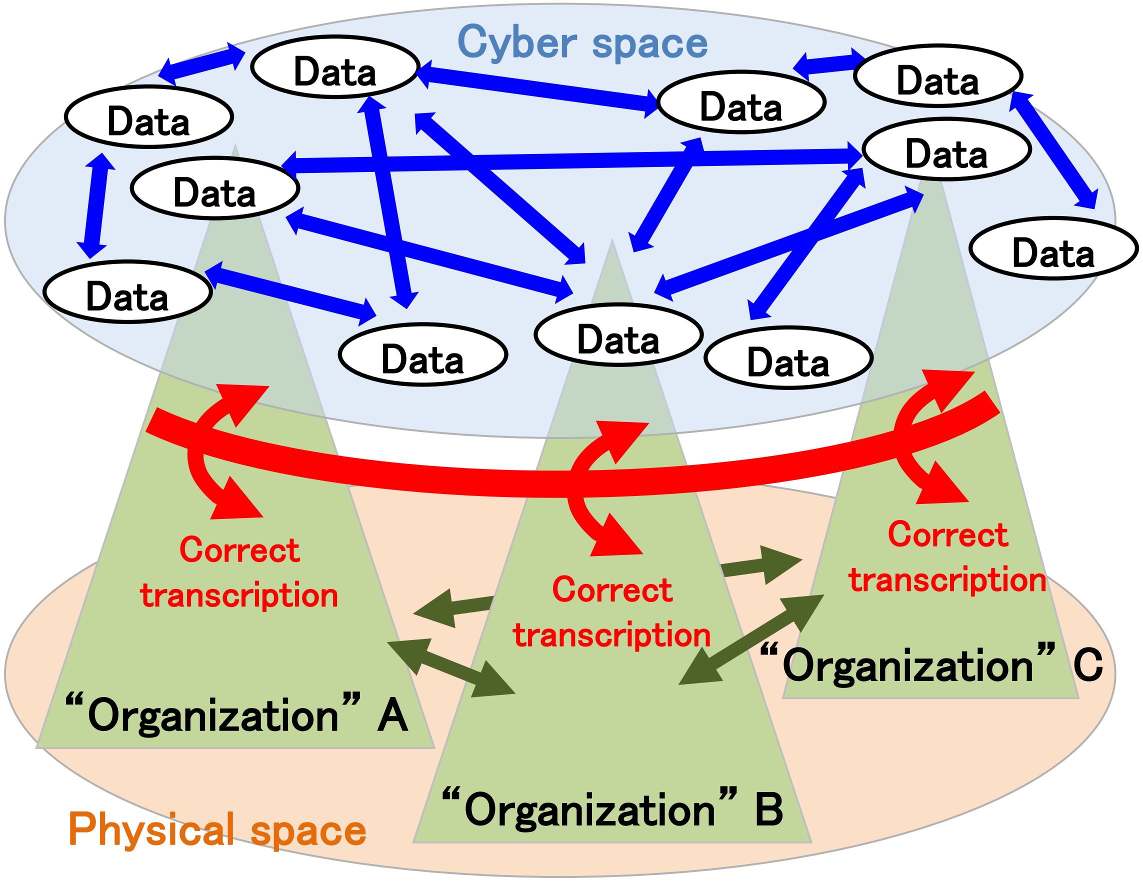
(Connections between Cyber & Physical space)

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

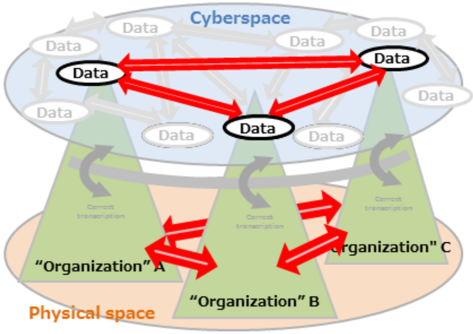
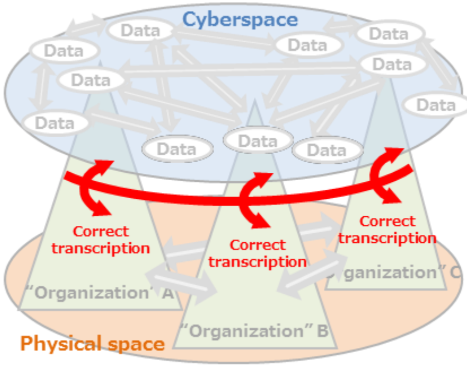
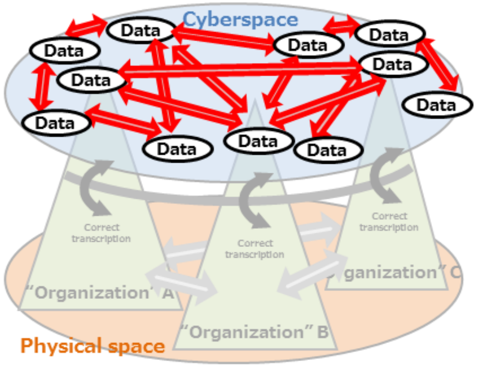
The First Layer

(Connection between Organizations)

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



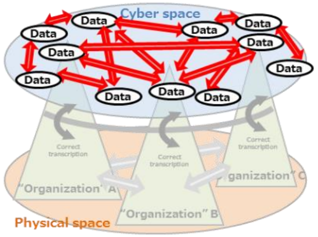
Brief Structure of CPSF

	Connections between Organizations [The First Layer]	Mutual connections between cyberspace and physical space [The Second Layer]	Connections in cyberspace [The Third Layer]
Sort of new supply chain structure	 Cyberspace Data Data Data Data Data Data Data Data Data Data Correct transcription Correct transcription Correct transcription “Organization” A “Organization” B rganization" C Physical space	 Cyberspace Data Data Data Data Data Data Data Data Data Data Data Data Correct transcription Correct transcription Correct transcription “Organization” A “Organization” B ganization” C Physical space	 Cyberspace Data Data Data Data Data Data Data Data Data Data Data Data Correct transcription Correct transcription Correct transcription “Organization” A “Organization” B ganization” C Physical space
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

CPSF Ver. 1.0 ⇒ https://www.meti.go.jp/english/press/2019/0418_001.html

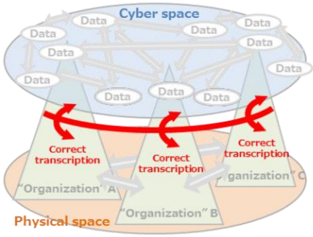
Further discussions based on CPSF

【3rd layer】



Connections in Cyber space

【2nd layer】



Connections between Cyber & Physical space

Industrial activities

Rules and methodologies for verification of trustworthiness

Cross sectoral cooperation with data

By Sector

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

By Scale

- Large companies
- SMEs, and etc.

Trustworthiness of Data

(integrity & authenticity of data, etc.)

Trustworthiness of Transcription Function of IoT

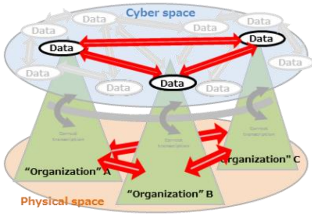
- IoT devices
- IoT systems, etc.

Trustworthiness of Software

- Software component transparency, etc.

【1st layer】

Connections between Organizations



METI's WG to Develop CPSF

CPSF as a Standard Model

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

Cross-sectoral SWG

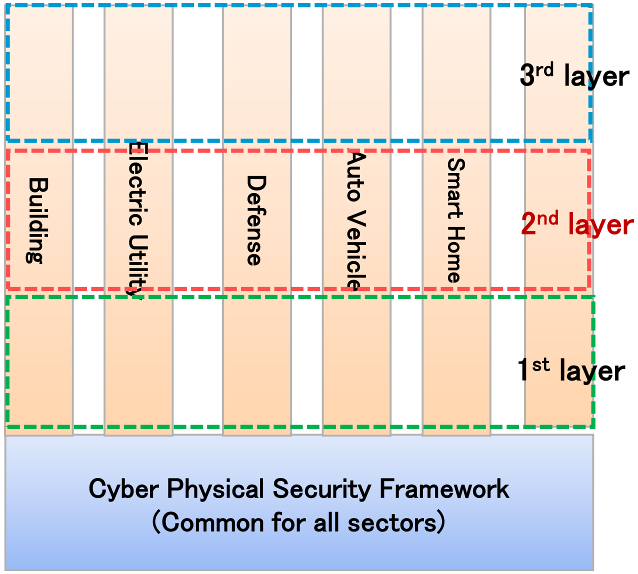
『3rd layer』TF (⇒ Security requirement for each data category)

Software TF (⇒ Software management including OSS)

『2nd layer』TF (⇒ Appropriate labeling and certification for each device, integration of security and safety, etc.)

[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.

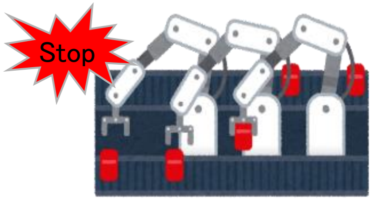


An idea of discussion points for 2nd Layer TF

(1) Confirmation and visualization scheme such as self-declaration, certification and labeling

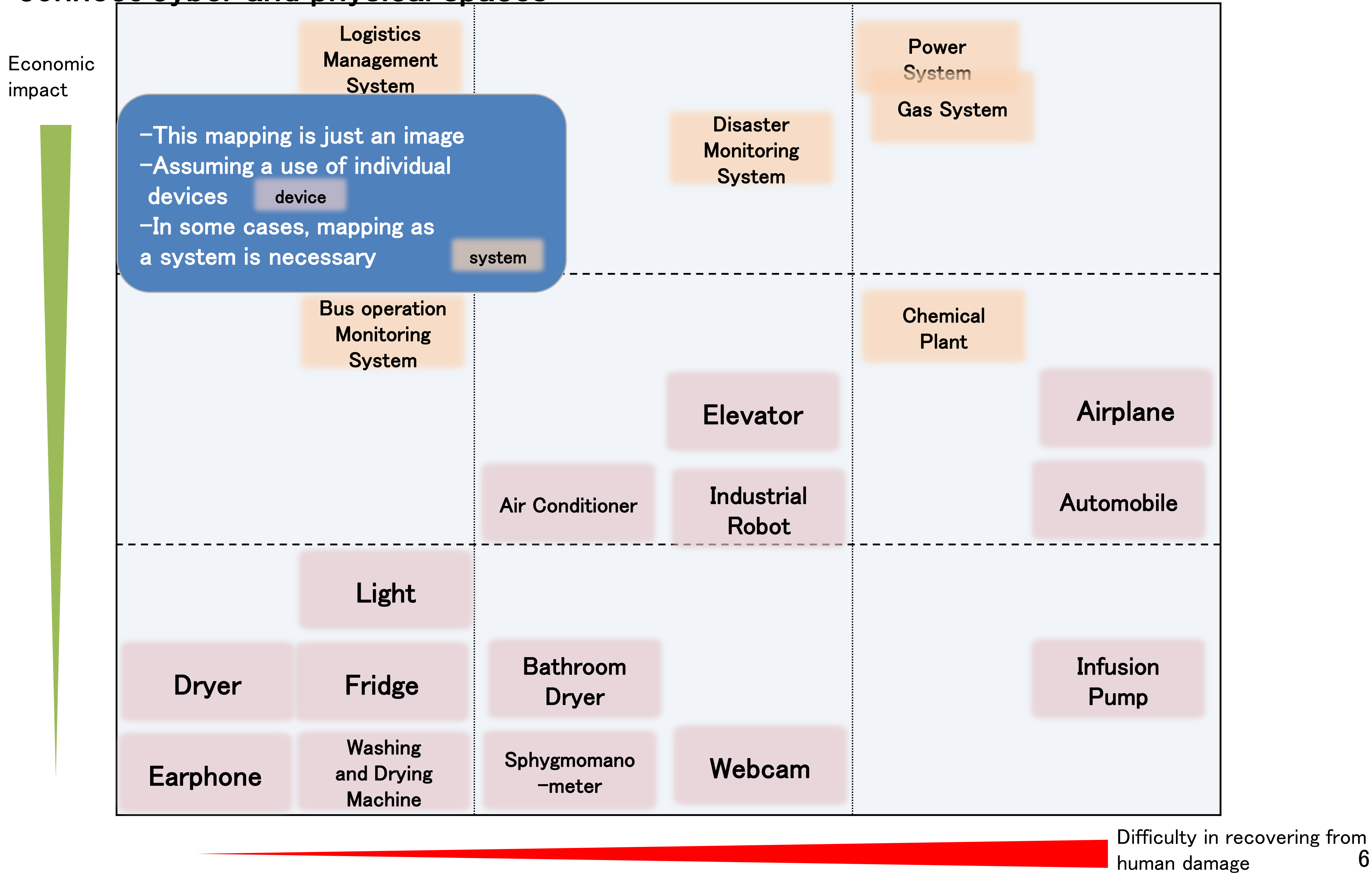
※ Especially for devices which require higher level security

(2) Response to the increase in the impact of cyber risk on safety

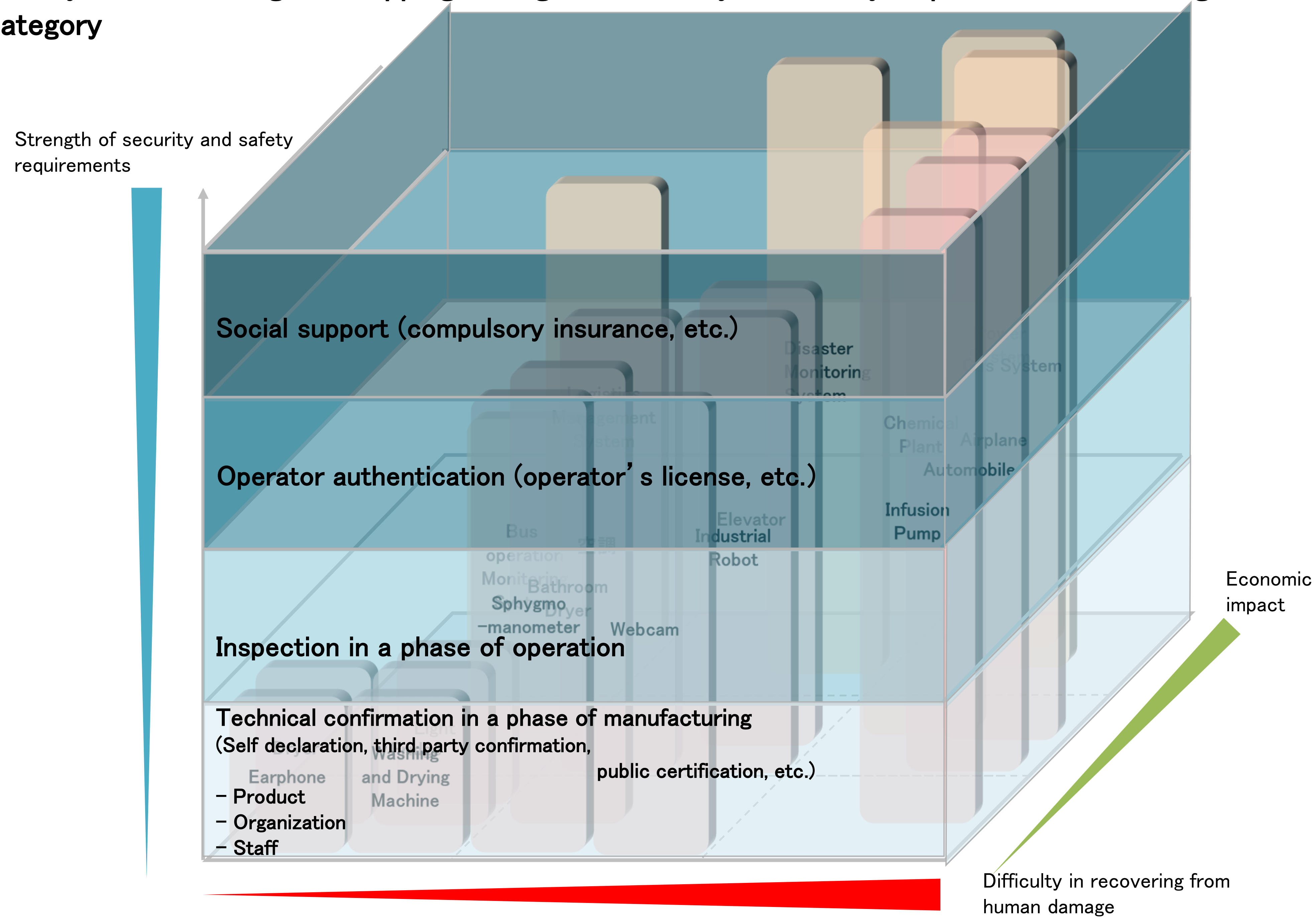


※ Examine security measures considering functional safety

[2nd layer TF] An image of mapping for hidden risks in products and systems that connect cyber and physical spaces


Economic impact
Logistics Management System
Power System
Gas System
Disaster Monitoring System
−This mapping is just an image
−Assuming a use of individual devices
device
−In some cases, mapping as a system is necessary
system
Bus operation Monitoring System
Chemical Plant
Elevator
Airplane
Air Conditioner
Industrial Robot
Automobile
Light
Dryer
Fridge
Bathroom Dryer
Infusion Pump
Earphone
Washing and Drying Machine
Sphygmomano−meter
Webcam
Difficulty in recovering from human damage

[2nd layer TF] An image of mapping strength of security and safety requirements according to category



Social support (compulsory insurance, etc.)

Operator authentication (operator' s license, etc.)

Inspection in a phase of operation

Technical confirmation in a phase of manufacturing
(Self declaration, third party confirmation, public certification, etc.)

- Product
- Organization
- Staff

Strength of security and safety requirements
Economic impact
Difficulty in recovering from human damage
Disaster Monitoring System
Logistics Management System
System
Chemical Plant
Airplane
Automobile
Infusion Pump
Elevator
Industrial Robot
Bus operation Monitoring System
空調
Bathroom Dryer
Sphygmo -manometer
Webcam
Light
Washing and Drying Machine
Earphone