METI
Ministry of Economy, Trade and Industry

The Cyber/Physical Security Framework（CPSF）

Version 1.0

Cybersecurity Division

Commerce and Information Policy Bureau

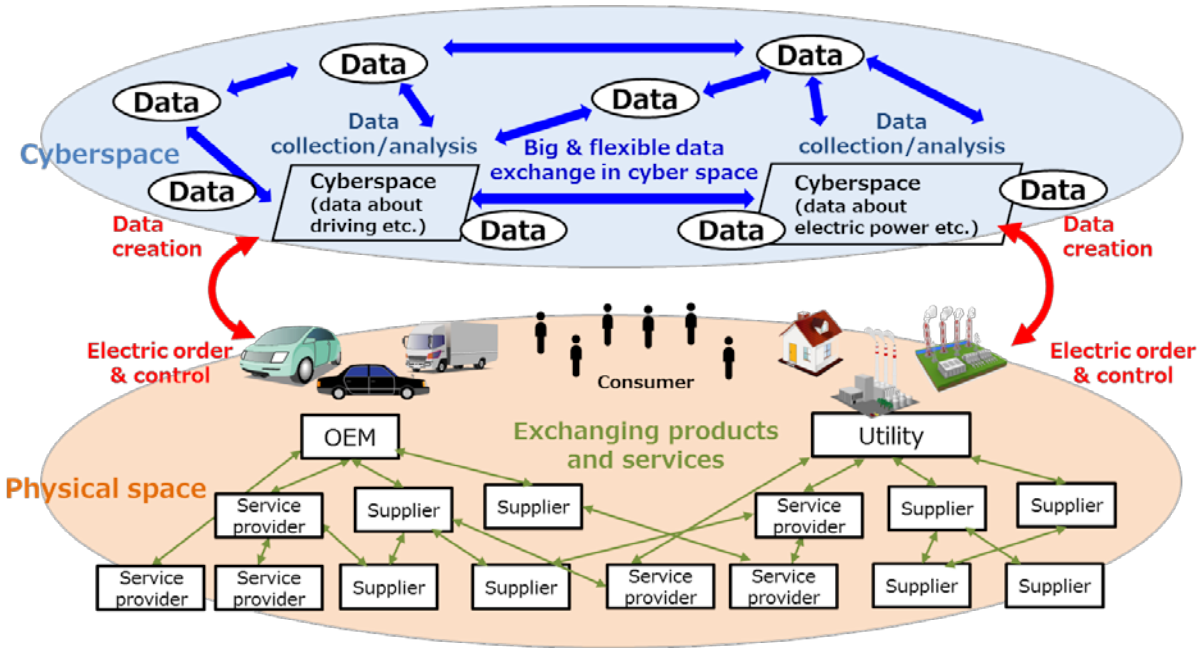
Ministry of Economy, Trade and Industry

Apr. 18 2019

Risks in Cyber/Physical Integrated Society (Society 5.0)

[Conventional Supply Chain]

[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)

⇒ **Cyberattack 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)

- ***METI has published CPSF (Ver. 1.0) on Apr. 18, 2019***
- ***Proposing “Three-Layer Approach” to articulate risks and appropriate measures in whole supply chain***
- ***With correspondence tables to ISO/IEC 27001, NIST CSF and SP800-171***

The Third Layer
(Connections in Cyberspace)

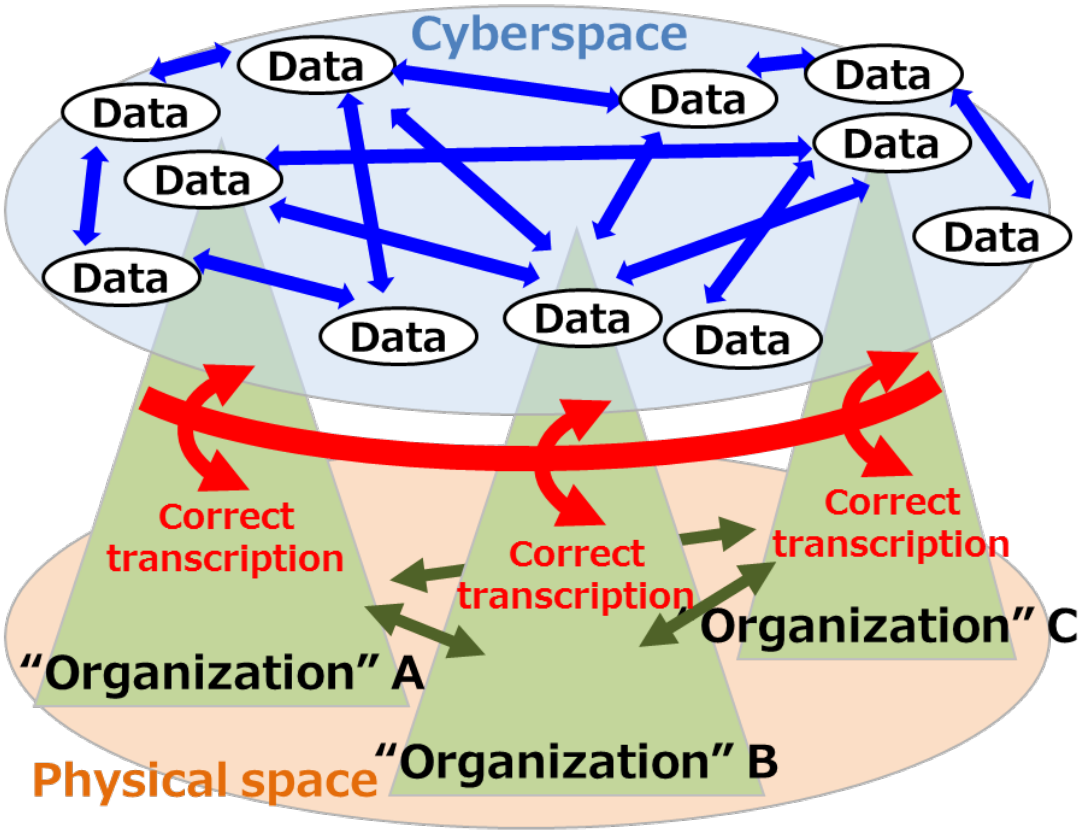
•**Trustworthiness of data** is a key for secured products and services

The Second Layer
(Connections between Cyber & Physical space)

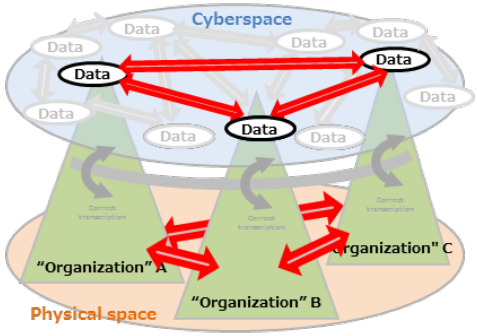
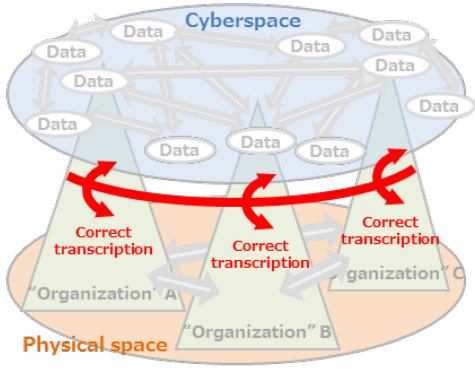
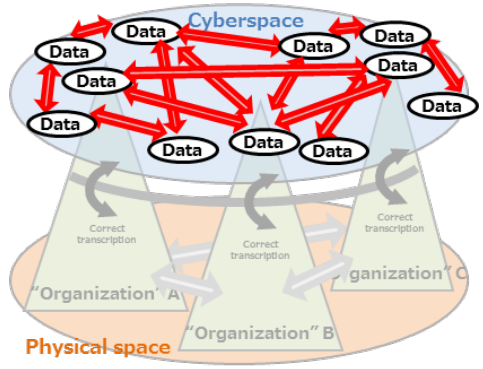
•**Trustworthiness of “transcription function” between cyber & physical space**, which is IoT system’s essential function

The First Layer
(Connection between Organizations)

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

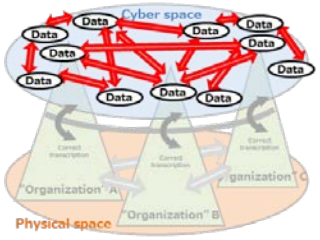


Brief image of CPSF

	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			
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

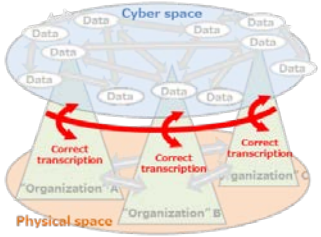
Further discussions based on CPSF

【3rd layer】



Connections in Cyberspace

【2nd layer】



Connections between Cyber & Physical space

【1st layer】

Connections between Organizations

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.

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

- 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 (⇒ Security requirements for IoT systems, etc.)