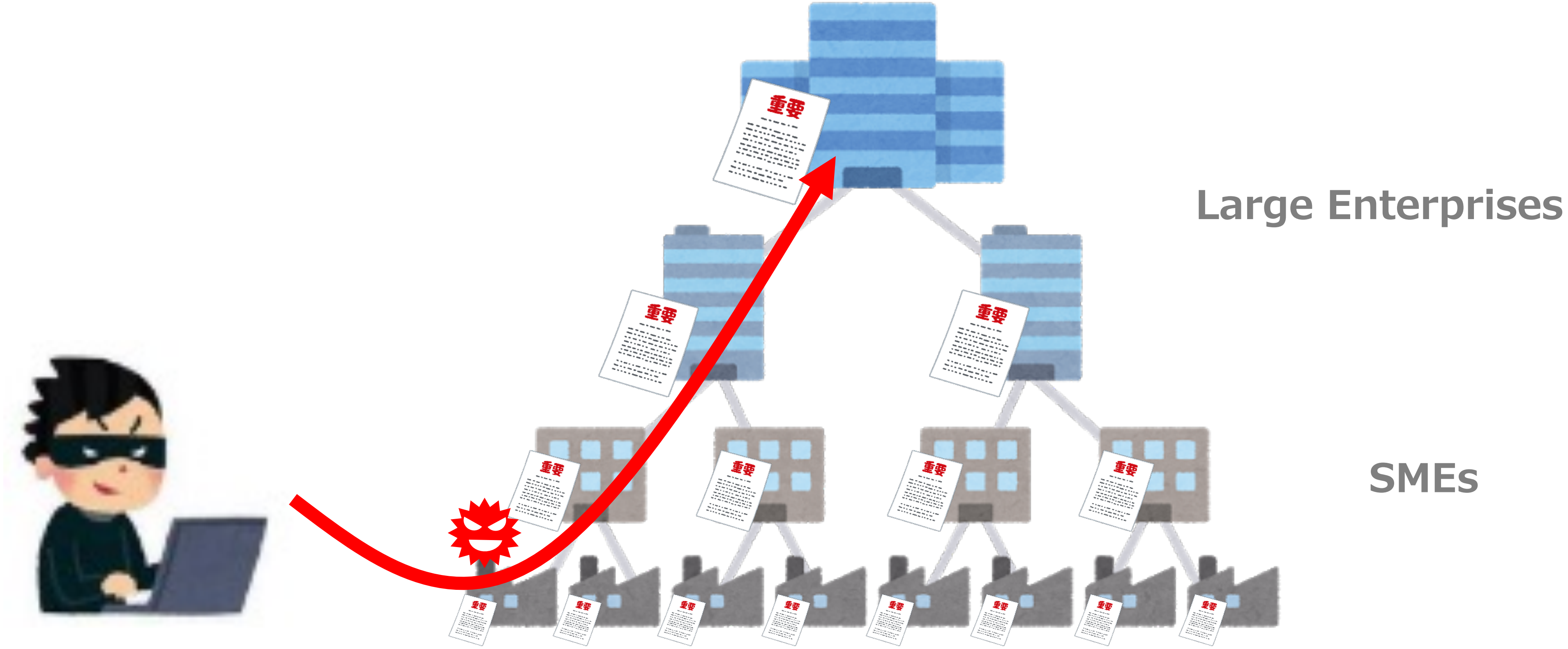
To promote collaborative activities for cybersecurity among stakeholders

Toshikazu　Okuya

Importance of Supply Chain Cybersecurity

- **Attacks targeting weak points in supply-chain have seriously increased and been getting sophisticated.**

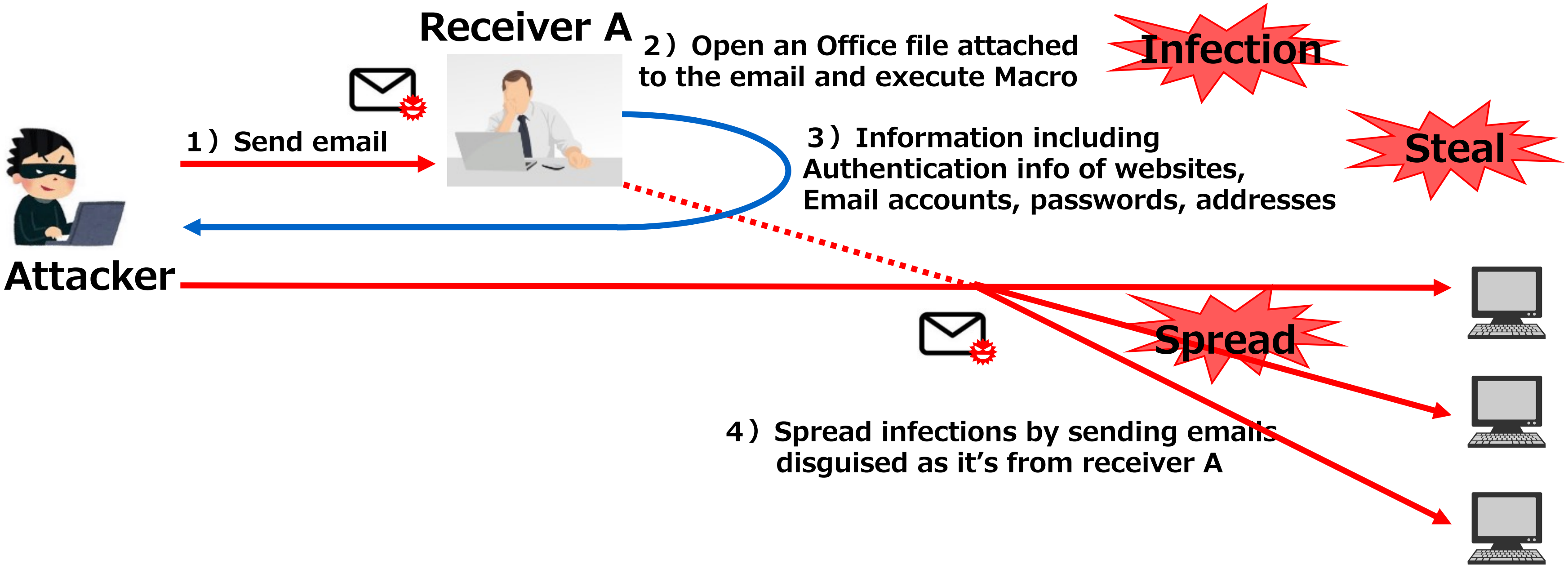
- One of the features of recent cyberattack is increasing number of attacks with intrusion from relatively weak security organizations in the supply-chain, such as overseas branches and business partners.



(Ref.) Emotet Rampant

- **Emotet is a computer malware program which is used to spy on data and spreads like worm.**
- **In 2019 and 2020, many cases of Emotet infection were reported in Japan.**

The image of attacks and infections


Receiver A
2） Open an Office file attached to the email and execute Macro
Infection
1） Send email
3） Information including Authentication info of websites, Email accounts, passwords, addresses
Steal
Attacker
Spread
4） Spread infections by sending emails disguised as it's from receiver A

https://www.ipa.go.jp/security/announce/20191202.html
https://www.jpcert.or.jp/newsflash/2020072001.html

Surveys about cyber attack situation on SMEs

- **Even regional SMEs are under cyber attacks, while many of them have insufficient awareness.**
- **Many Large companies received damages from hacked SMEs.**

Results of network traffic analysis of actual SMEs systems

- Sept. 2018 - Nov. 2019
- Network traffic analysis of 30 SMEs

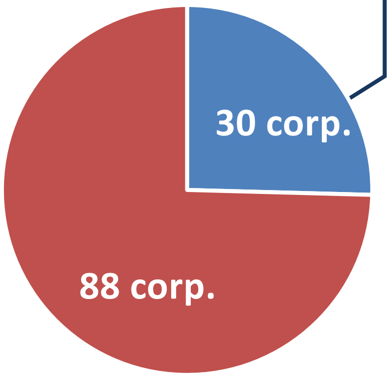
- **All companies received cyber attacks**:
  - Suspicious **remote control** of PC
  - Communication with **external malicious server**
  - Communication with servers located in **suspicious countries**

- 5 companies (or possibly more) had information leakage:
  - Sophisticated attacks on **vulnerabilities** such as HeartBleed
  - Backdoor-type **malware** detected

Results of questionnaire to Large companies about their partners' cyber security

- Feb. – March, 2018
- 118 companies with over 100 employees

- **30 of the 118 companies (25%) received damages through hacked business partners.**



Reference: The Osaka Chamber of Commerce "Survey on cyber security measures of suppliers in the supply chain" (May, 2019)

The Cyber/Physical Security Framework (CPSF)

～for value creation process in Society5.0's supply-chain ～

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

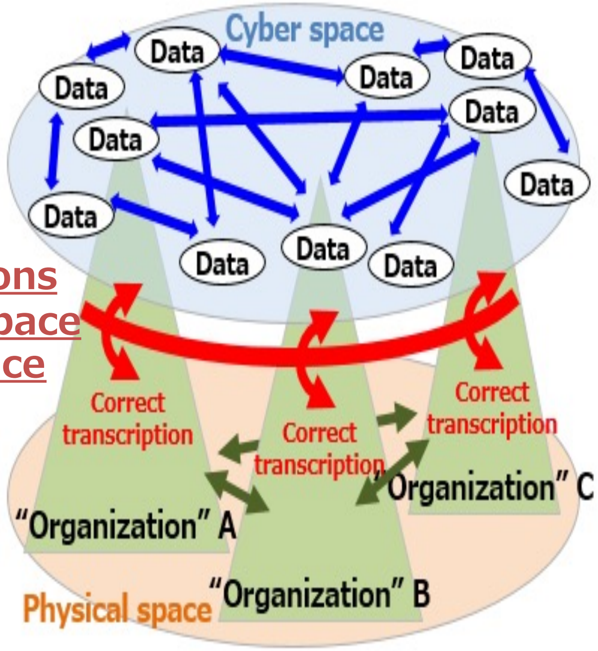
- "**Society 5.0**", where cyber and physical spaces are highly integrated, **enables rather dynamic and flexible creation of supply chain**, while facing with **new risks such as spreading attack points and increasing impact to physical space**.
- **Published "Cyber-Physical Security Framework (CPSF) Ver1.0" on April 18, 2019,** which outlines security measures against new risks in Society 5.0.

Three Layers Approach by CPSF

【Third Layer】
Connections in Cyberspace

【Second Layer】
Mutual connections between Cyberspace and Physical space

【First Layer】
Connections between organizations



Six Elements Approach by CPSF

Organization	Components	Procedure
People	Data	System

Concept of risk management in CPSF

1. Function of each Layer
2. Security Incident
3. Risk Source (Sorted by 6 elements)
4. Measure requirement
5. Countermeasure Example

International harmonization

Correspondence Tables with:

- NIST Cybersecurity Framework
- NIST SP800-171
- ISO/IEC 27001 Annex A

(Ref.) International Harmonization

- In the Framework, there are correspondence tables between the Framework and other standards.
- An enterprise which uses the Framework as security measures, can make sure that it satisfies security requirements of the other standards. A foreign enterprise can show its sufficient security treatment based on the other standards through the tables.

<Appendix C> CPSF ⇒ Other standards

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Example of Security Measures	Subject that implements measures	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 Annex A	IEC 62443
CPS.AM-1	・・・	L1_1_a_COM, L1_1_b_COM, ・・・	<H.Advanced> ・・・	O/S	○	○	–	

<Appendix D> Other standards ⇒ CPSF

NIST Cyberseucurity Framework v1.1			Cyber/Physical Security Framework	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Identify (ID)	AM-1	Physical devices and systems within the organization are inventoried	CPS.AM-1	Document and save the list of hardware and software, and management information of those composing the system.
	AM-2	・・・		

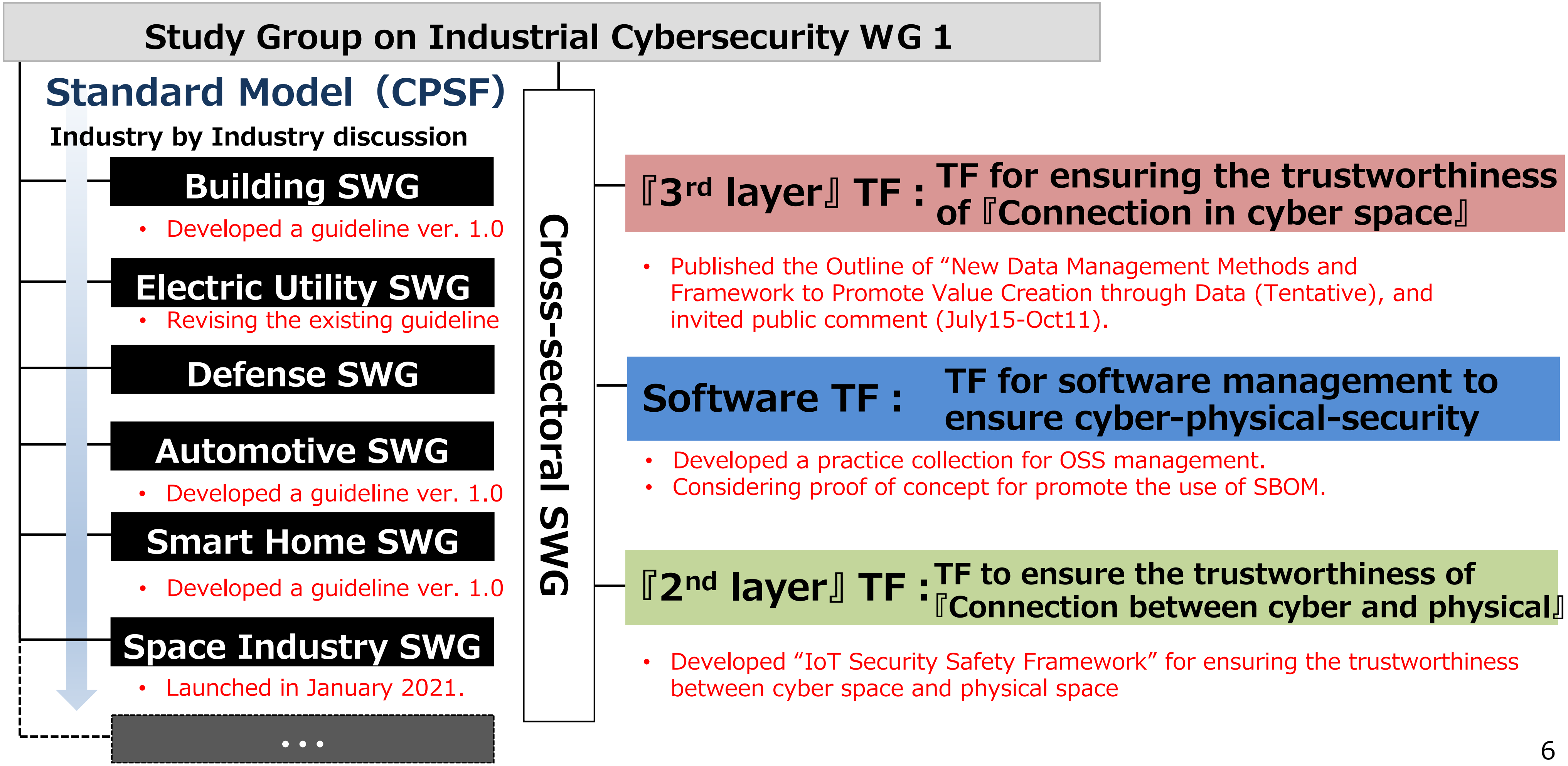
NIST SP 800-171	NIST SP 800-53 Relevant Security Controls referred from NIST SP 800-17	Cyber/Physical Security Framework

ISO/IEC 27001:2013 Annex A	Cyber/Physical Security Framework

Further discussions based on CPSF

- Established **six industry-specific sub working groups (SWG)**, and developing CPSF based security guidelines.

- Established **three cross-sectoral task-forces (TF)** for common challenges.



Study Group on Industrial Cybersecurity WG 1

Standard Model（CPSF)

Industry by Industry discussion

Building SWG

- Developed a guideline ver. 1.0

Electric Utility SWG

- Revising the existing guideline

Defense SWG

Automotive SWG

- Developed a guideline ver. 1.0

Smart Home SWG

- Developed a guideline ver. 1.0

Space Industry SWG

- Launched in January 2021.

・・・

Cross-sectoral SWG

『3rd layer』TF : TF for ensuring the trustworthiness of『Connection in cyber space』

- Published the Outline of "New Data Management Methods and Framework to Promote Value Creation through Data (Tentative), and invited public comment (July15-Oct11).

Software TF : TF for software management to ensure cyber-physical-security

- Developed a practice collection for OSS management.
- Considering proof of concept for promote the use of SBOM.

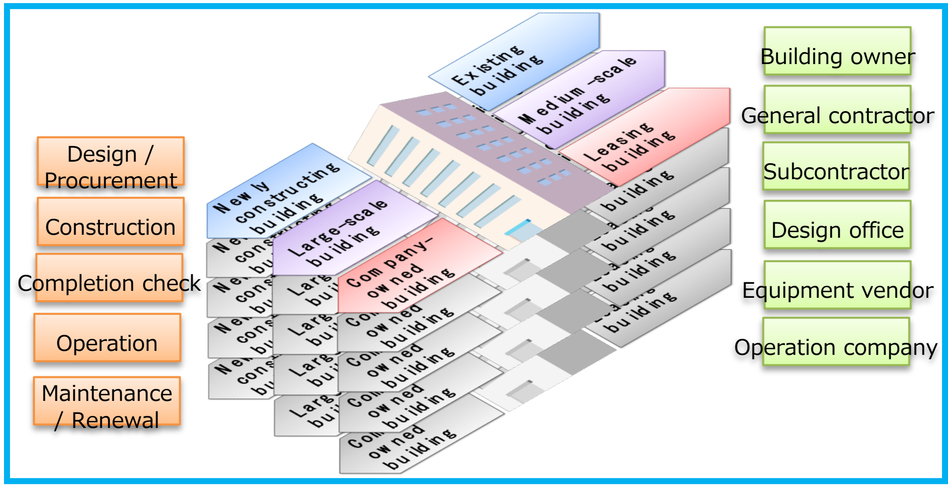
『2nd layer』TF : TF to ensure the trustworthiness of『Connection between cyber and physical』

- Developed "IoT Security Safety Framework" for ensuring the trustworthiness between cyber space and physical space

(Ref.) Building SWG

https://www.meti.go.jp/english/press/2019/0617_005.html

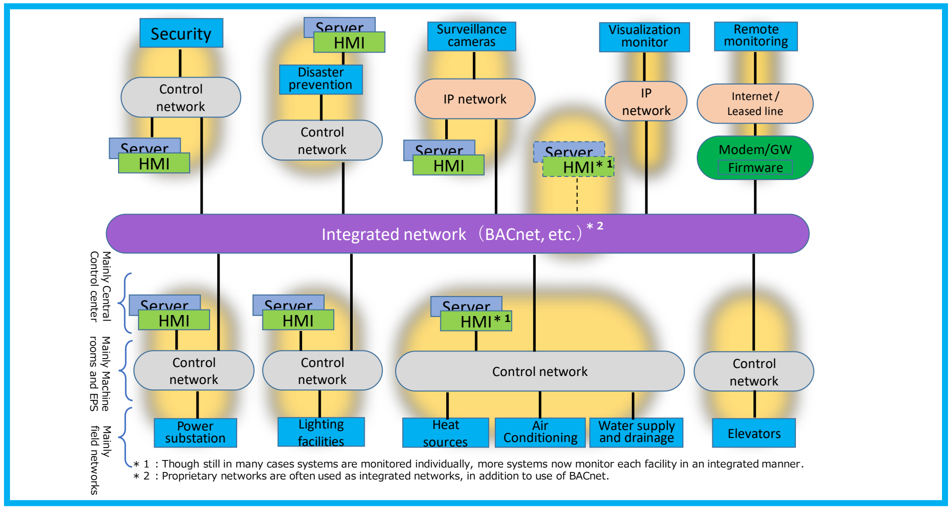
- "The Guidelines for Cyber-Physical Security Measures for Building Systems (1st ver.)" was published on June 17, 2019.
- Currently, developing further description enhancement and individual equipment edition (ex. air-conditioning edition) are underway. Also, we are considering a information sharing mechanizm among the related parties.



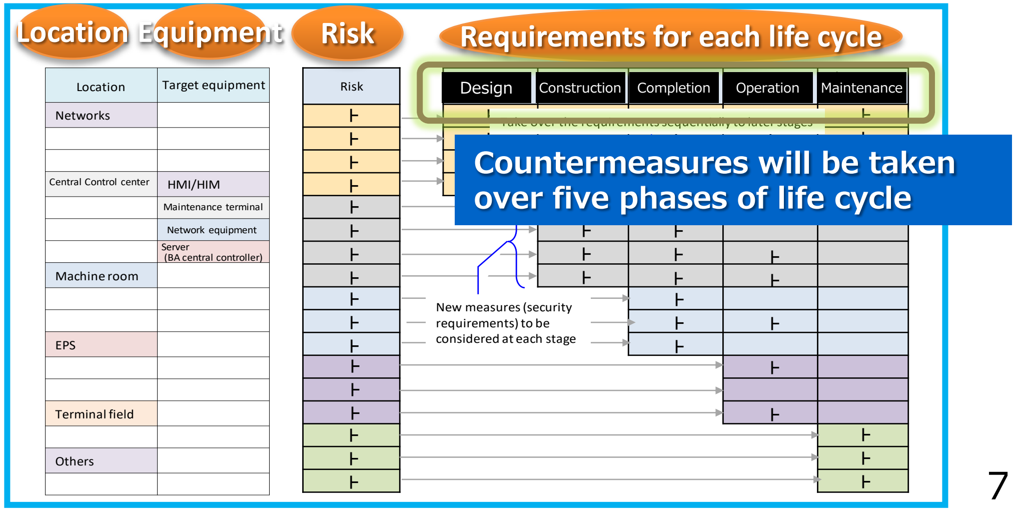
Building systems are characterized by that there are various types of buildings, various stakeholders are involved, various types of equipment are operated, and they have a long life cycle consisting of multiple stages.

Assuming a standard model of building systems.

Organize life cycle-conscious measures against risks that depend on the installation location of building systems and individual devices.



＊1 : Though still in many cases systems are monitored individually, more systems now monitor each facility in an integrated manner.
＊2 : Proprietary networks are often used as integrated networks, in addition to use of BACnet.



Countermeasures will be taken over five phases of life cycle

(Ref.) Electric Utility Sub WG

- Discuss about short-term and long-term challenges and directions for both the government and private companies

<Members>

Experts (professors, lawyers, etc.), Electric utility companies, Business organizations

<Example of Topics>

- Security measures for **major electric power companies**
  - → **Conducted an assessment** of cybersecurity measures of major electric power companies with common framework based on related- domestic/international frameworks
  - → Discuss about short-term and long-term challenges and directions considering the timeframe towards **the Tokyo Olympic and Paralympic Games**

- Security measures for **new entrants**
  - → Developed a guideline of security measures for **electric power retailers**
  - → Conducted surveys about **small power generation companies**' security measures
  - → **Introduction of cybersecurity requirements to the grid code** for all power generation facilities including solar power generation facilities connected to the grid

- **Supply chain risk management**
  - → Consideration of measures against supply chain risks in accordance with international trends

(Ref.)
CPSF based Guidelines in Smart home and Automotive Industries

- Development of Industry-Specific Guidelines based on CPSF is in progress, in addition to already published Building Guidelines.
- Guidelines for Smart home and Automotive industries were published.

Smart home SWG

Published on 1st Apr. 2021

Purpose

- Provides guidance on security measures required for variety of stakeholders

Objective

- **Various stakeholders for Smart home**
  - **IoT Devices Providers**
  - **Service Providers**
  - **Management company, Resident e.g.**

Points

- Knowledge level and background of each stakeholder are diverse
- Based on incidents concerned from use cases, describes **from simple message to specific requirements & Comparison with other standards**

Further Direction

- Public awareness
- Enrich measures

Automotive SWG

Published on 1st Dec. 2020

Purpose

- **Raising security level of entire industry**
- Efficient inspection of measurement level

Objective

- **Enterprise domain** of all companies in Automotive Industry
- Minimum requirements for SMEs and OEM (Voluntary)

Points

- Supply-Chain measurements for **Parts, Services, Software**
- **Described by industry-specific practices and terminology based on CPSF**
- **Self check list**

Further Direction

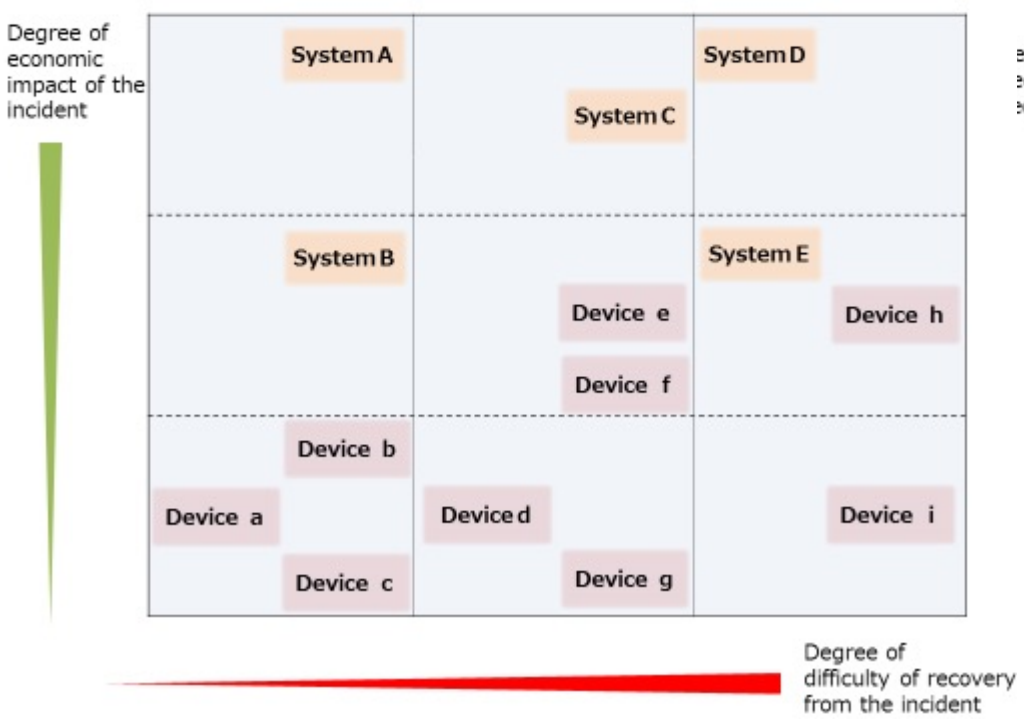
- **Consider requirements for further raising security level**
- **Expand to factories, connected cars**

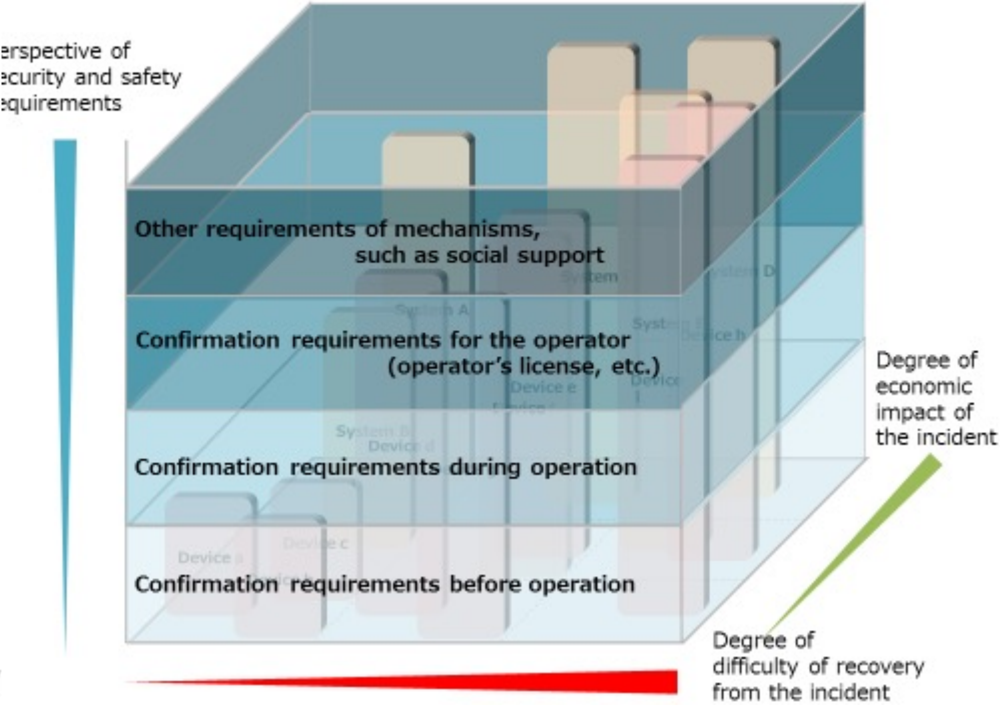
http://www.jama.or.jp/it/cyb_sec/cyb_sec_guideline.html

[2nd Layer TF] IoT Security and Safety Framework (IoT SSF)

https://www.meti.go.jp/english/press/2020/1105_002.html

- **METI published IoT Security and Safety Framework (IoT SSF) on November 5, 2020.**
- In this framework, METI aims to categorize devices and systems connecting physical space and cyberspace, or IoT devices and systems, on a map based on the impact of the incident that these devices and systems may cause.

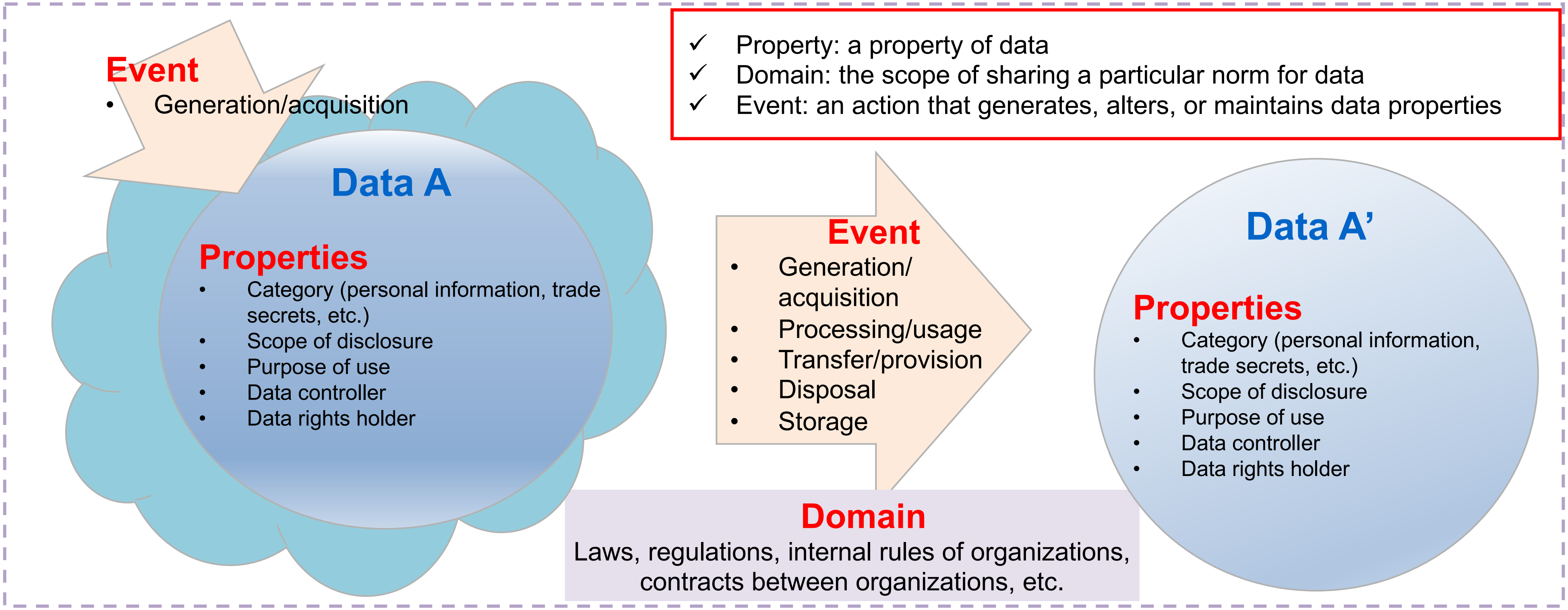




erspective of ecurity and safety equirements
Other requirements of mechanisms, such as social support
Confirmation requirements for the operator (operator's license, etc.)
Confirmation requirements during operation
Confirmation requirements before operation
Degree of economic impact of the incident
Degree of difficulty of recovery from the incident

[3rd Layer] Outline of ”New Data Management Methods and Framework to Promote Value Creation through Data (Tentative)” (Draft)

- Data management is defined as “**managing the processes during which data properties change due to events in the domains based on the life cycle**”.
- **It makes it easier to ensure a certain degree of predictability on data changes** due to data transitions and **to share awareness among stakeholders**.



- ✓ Property: a property of data
- ✓ Domain: the scope of sharing a particular norm for data
- ✓ Event: an action that generates, alters, or maintains data properties

[Public Comment was Invited (July15-Oct11)] https://www.meti.go.jp/english/press/2021/0715_002.html

[3rd Layer] Outline of ”New Data Management Methods and Framework to Promote Value Creation through Data (Tentative)” (Draft)

- **Visualize the data status in the value creation process using the four steps below.**
- In each step of the data lifecycle, stakeholders of the value creation process are **expected to ensure data trustworthiness by visualizing the risks and then working on the measures that each entity should take while forming consensus with other entities.**

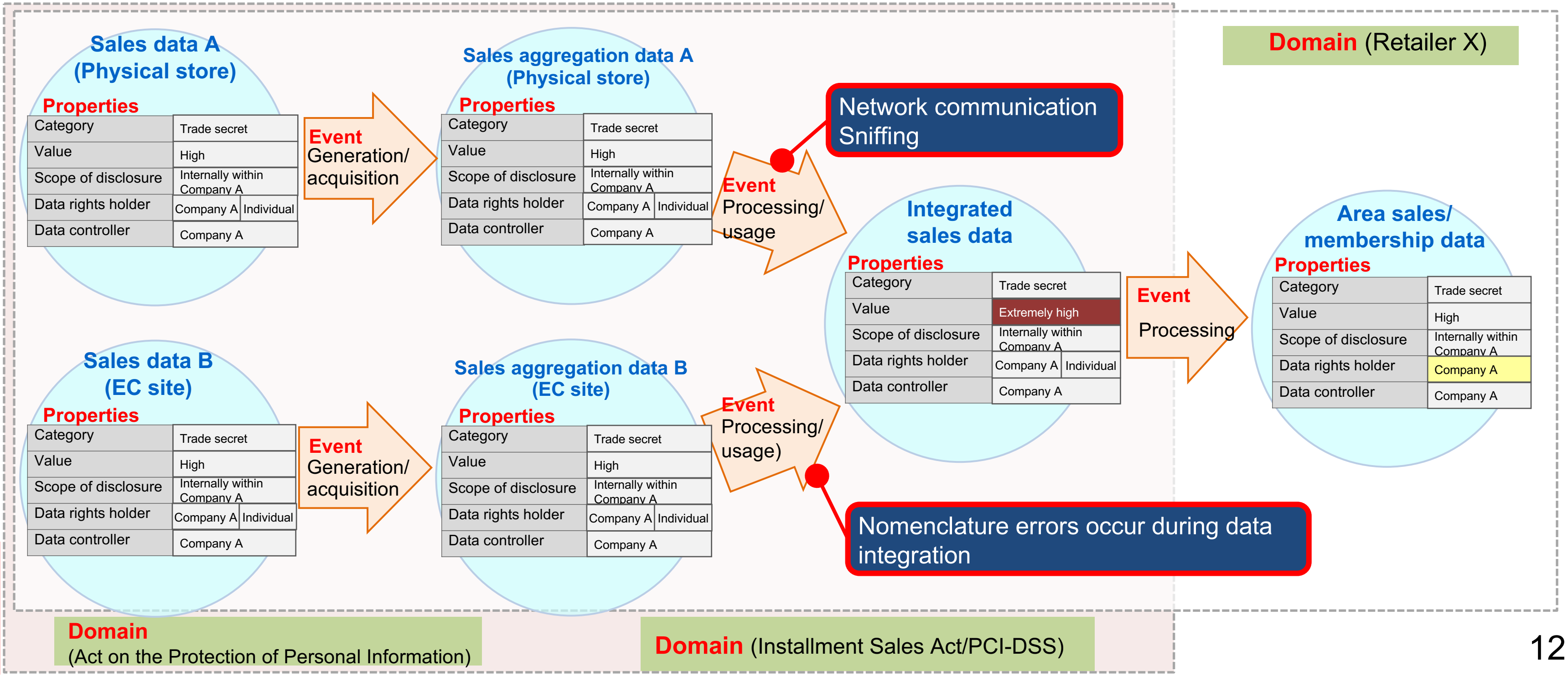
Examples of POS data utilization by retailer

STEP 1
Visualize the data processing workflow (“events”)

STEP 2
Organize the necessary institutional safeguards (“domains”)

STEP 3
Specify the “properties”

STEP 4
Identify the risks of each “events”



Sales data A (Physical store)

Properties

Category	Trade secret	
Value	High	
Scope of disclosure	Internally within Company A	
Data rights holder	Company A	Individual
Data controller	Company A	

Event Generation/ acquisition

Sales aggregation data A (Physical store)

Properties

Category	Trade secret	
Value	High	
Scope of disclosure	Internally within Company A	
Data rights holder	Company A	Individual
Data controller	Company A	

Event Processing/ usage

Network communication Sniffing

Sales data B (EC site)

Properties

Category	Trade secret	
Value	High	
Scope of disclosure	Internally within Company A	
Data rights holder	Company A	Individual
Data controller	Company A	

Event Generation/ acquisition

Sales aggregation data B (EC site)

Properties

Category	Trade secret	
Value	High	
Scope of disclosure	Internally within Company A	
Data rights holder	Company A	Individual
Data controller	Company A	

Event Processing/ usage

Nomenclature errors occur during data integration

Integrated sales data

Properties

Category	Trade secret	
Value	Extremely high	
Scope of disclosure	Internally within Company A	
Data rights holder	Company A	Individual
Data controller	Company A	

Event Processing

Area sales/ membership data

Properties

Category	Trade secret
Value	High
Scope of disclosure	Internally within Company A
Data rights holder	Company A
Data controller	Company A

Domain (Retailer X)

Domain (Act on the Protection of Personal Information)

Domain (Installment Sales Act/PCI-DSS)

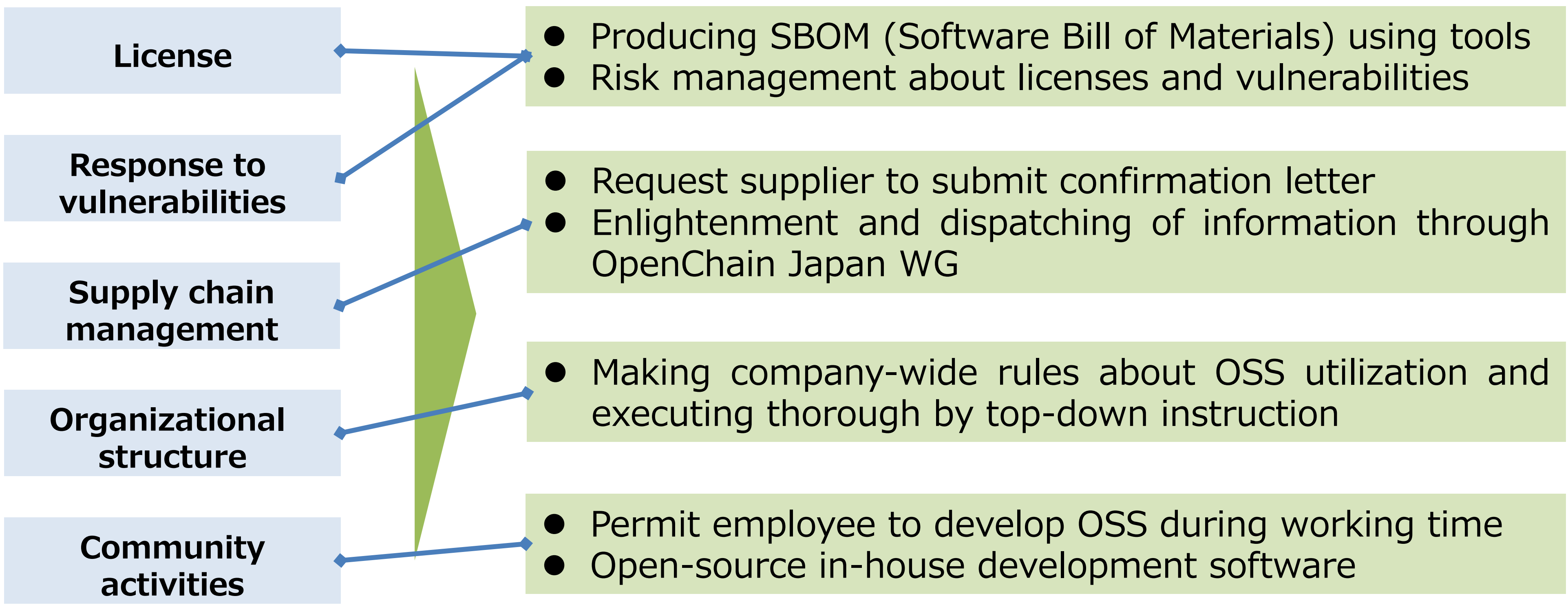
[Software TF] The Practices Collection for OSS management

(2021/4/21)

- While the growing use of OSS, there is a demand to share the best practices about OSS because burden is much heavy to verify OSS by only own company.
- **The collection helps industries to promote appropriate OSS utilization**, by organizing practices for OSS management.

OSS issues（ex.）

Sample of good practices in Practices collection



License

Response to vulnerabilities

Supply chain management

Organizational structure

Community activities

- Producing SBOM (Software Bill of Materials) using tools
- Risk management about licenses and vulnerabilities

- Request supplier to submit confirmation letter
- Enlightenment and dispatching of information through OpenChain Japan WG

- Making company-wide rules about OSS utilization and executing thorough by top-down instruction

- Permit employee to develop OSS during working time
- Open-source in-house development software

https://www.meti.go.jp/english/press/2021/0421_003.html

Development of Technical Report in ISO & IEC

- **Technical Report (TR) referring to the concept of CPSF** as one of the security reference architectures for cyber-physical systems (CPS) is under development in JTC1 SC27/WG4 based on the proposal from Japanese experts.

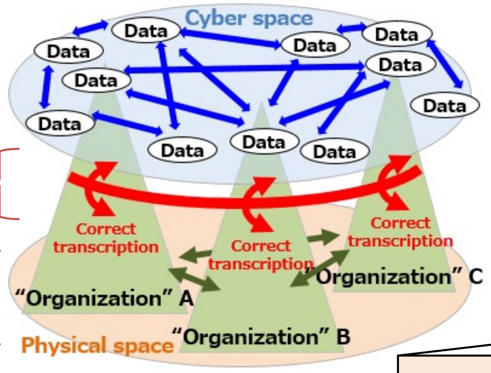
CPSF

Three Layers

【Third Layer】
Connections in Cyberspace

【Second Layer】
Mutual connections between Cyberspace and Physical space

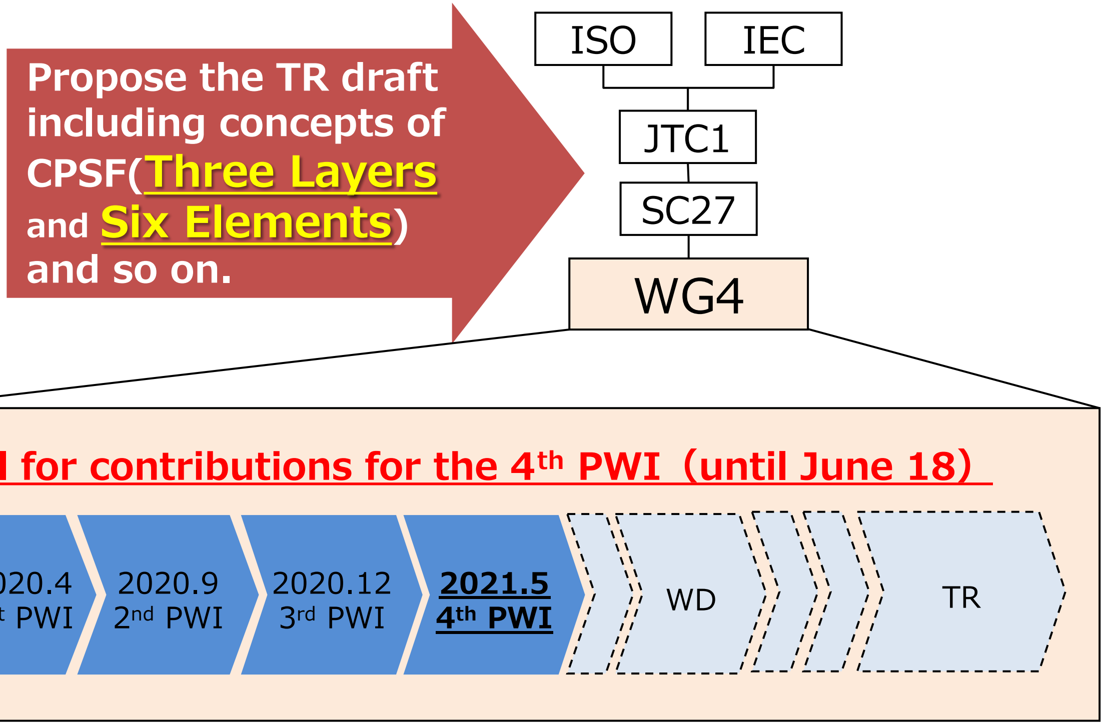
【First Layer】
Connections between organizations



Six Elements

Organization	Components	Procedure
People	Data	System

International standardizing body

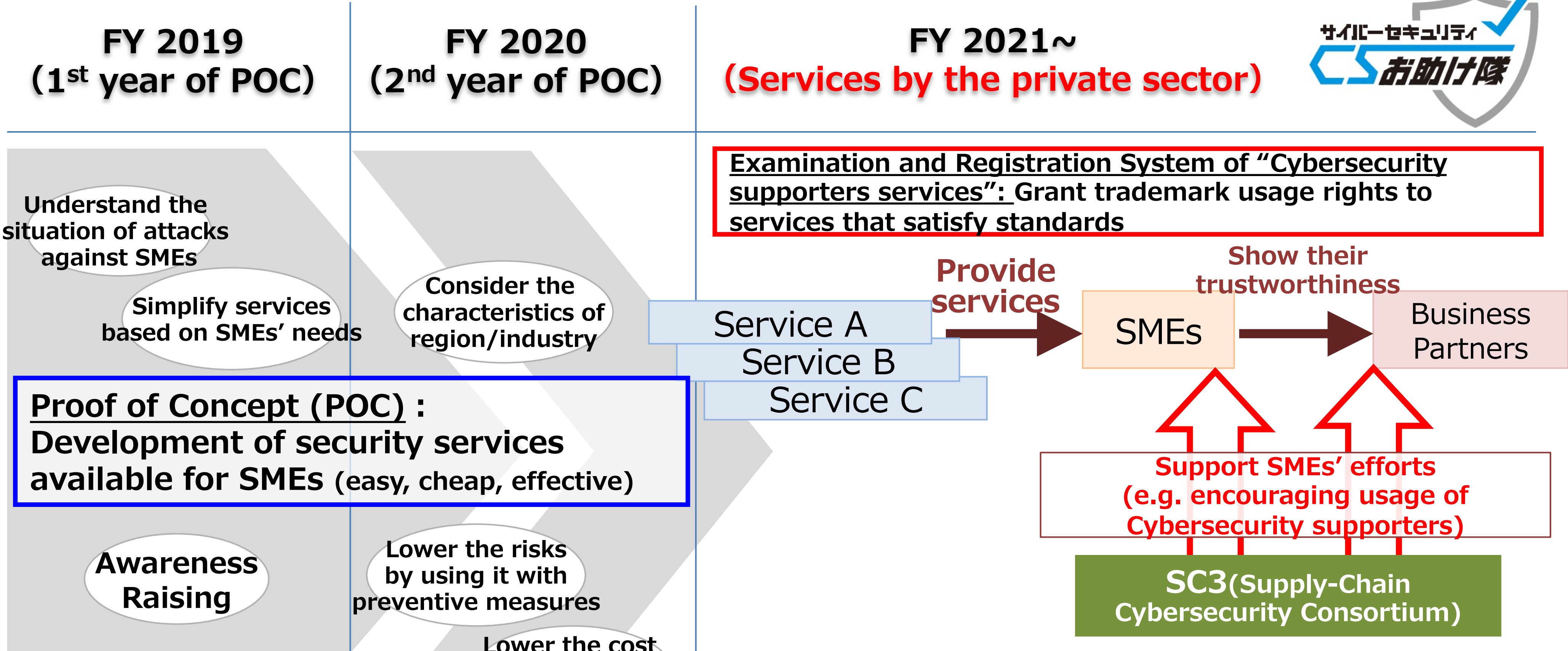

Propose the TR draft including concepts of CPSF(**Three Layers** and **Six Elements**) and so on.

Call for contributions for the 4th PWI (until June 18)

Establishment of “Cybersecurity Supporters Service” Brand

- Based on the results of government’s program, the standards for cybersecurity services for SMEs (named “Cybersecurity Supporters Service”) was established.
- It conducted the first examination in March 2021, and from April 15, private services registered as “cybersecurity supporters service”* were in the market with the brand logo.

* Private companies’ services which satisfy “cybersecurity supporters service” standards consisting of essential cybersecurity services for SMEs including inquiry counter, monitoring of systems, emergency support, and simple cyber insurance



FY 2019 (1st year of POC)

FY 2020 (2nd year of POC)

FY 2021~ (Services by the private sector)

サイバーセキュリティ CSお助け隊

Understand the situation of attacks against SMEs

Simplify services based on SMEs’ needs

Consider the characteristics of region/industry

Proof of Concept (POC) : Development of security services available for SMEs (easy, cheap, effective)

Awareness Raising

Lower the risks by using it with preventive measures

Lower the cost Of Installation and operation

Examination and Registration System of “Cybersecurity supporters services”: Grant trademark usage rights to services that satisfy standards

Service A

Service B

Service C

Provide services

SMEs

Show their trustworthiness

Business Partners

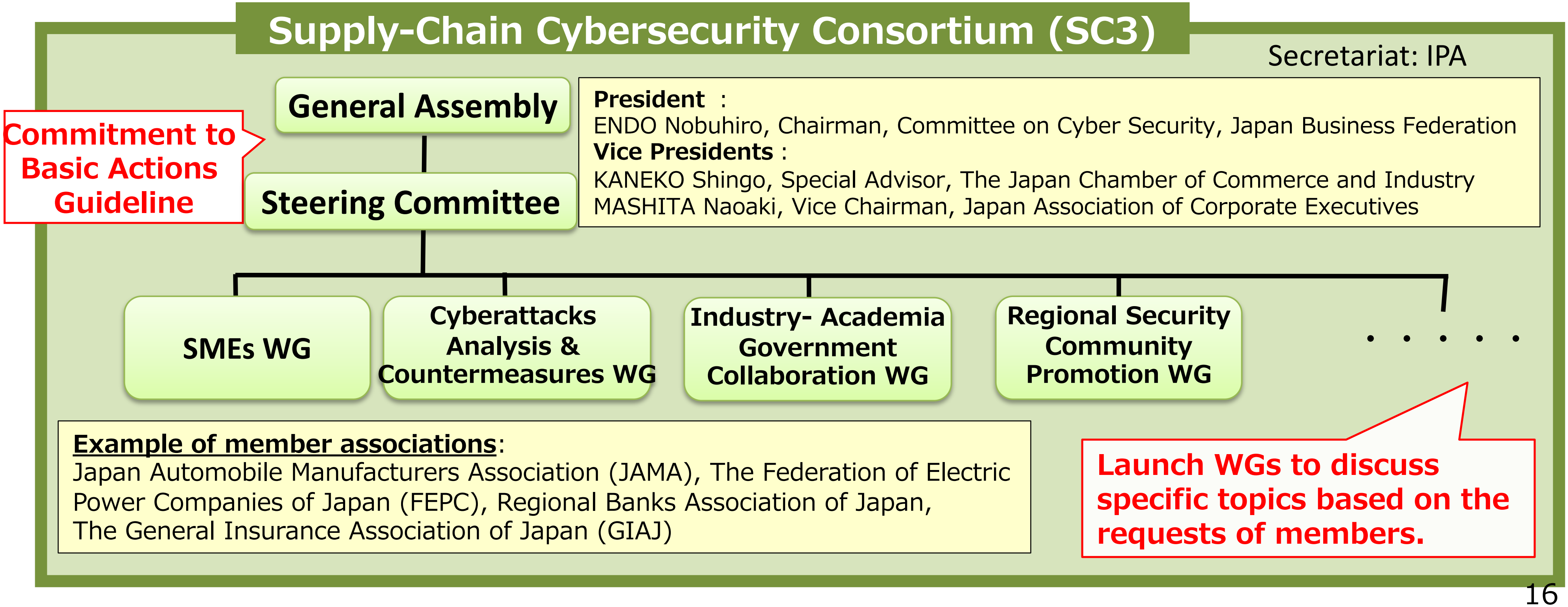
Support SMEs’ efforts (e.g. encouraging usage of Cybersecurity supporters)

SC3(Supply-Chain Cybersecurity Consortium)

→ By promoting the use of Cybersecurity supporters services in SC3, which consists of various industrial associations, encourage more SMEs to use the service and make sure that SMEs can take proper measures even if they are attacked by hackers.

Overview of Supply-Chain Cybersecurity Consortium (SC3)

- **Concept:** Industry-wide movement to promote **the Basic Actions Guideline** (Sharing, Reporting and Announcement) and **strengthen cybersecurity of whole supply-chains** by both large enterprises and SMEs.
- **Participants:** Major Business Associations (Japan business Federation, The Japan Chamber of Commerce and Industry, Japan Association of Corporate Executives), Major Sectoral Industrial Associations and so on.(175 members as of the end of Oct. 2021)
- **Date of the Start**: November 1, 2020
- **Example of activities:** In SME Working Group, members will discuss how to encourage SMEs to strengthen cybersecurity by branding Cybersecurity Supporters services, etc.



Supply-Chain Cybersecurity Consortium (SC3)

Secretariat: IPA

Commitment to Basic Actions Guideline
General Assembly
Steering Committee
SMEs WG
Cyberattacks Analysis & Countermeasures WG
Industry- Academia Government Collaboration WG
Regional Security Community Promotion WG
. . . . .

President :
ENDO Nobuhiro, Chairman, Committee on Cyber Security, Japan Business Federation
Vice Presidents :
KANEKO Shingo, Special Advisor, The Japan Chamber of Commerce and Industry
MASHITA Naoaki, Vice Chairman, Japan Association of Corporate Executives

Example of member associations:
Japan Automobile Manufacturers Association (JAMA), The Federation of Electric Power Companies of Japan (FEPC), Regional Banks Association of Japan, The General Insurance Association of Japan (GIAJ)

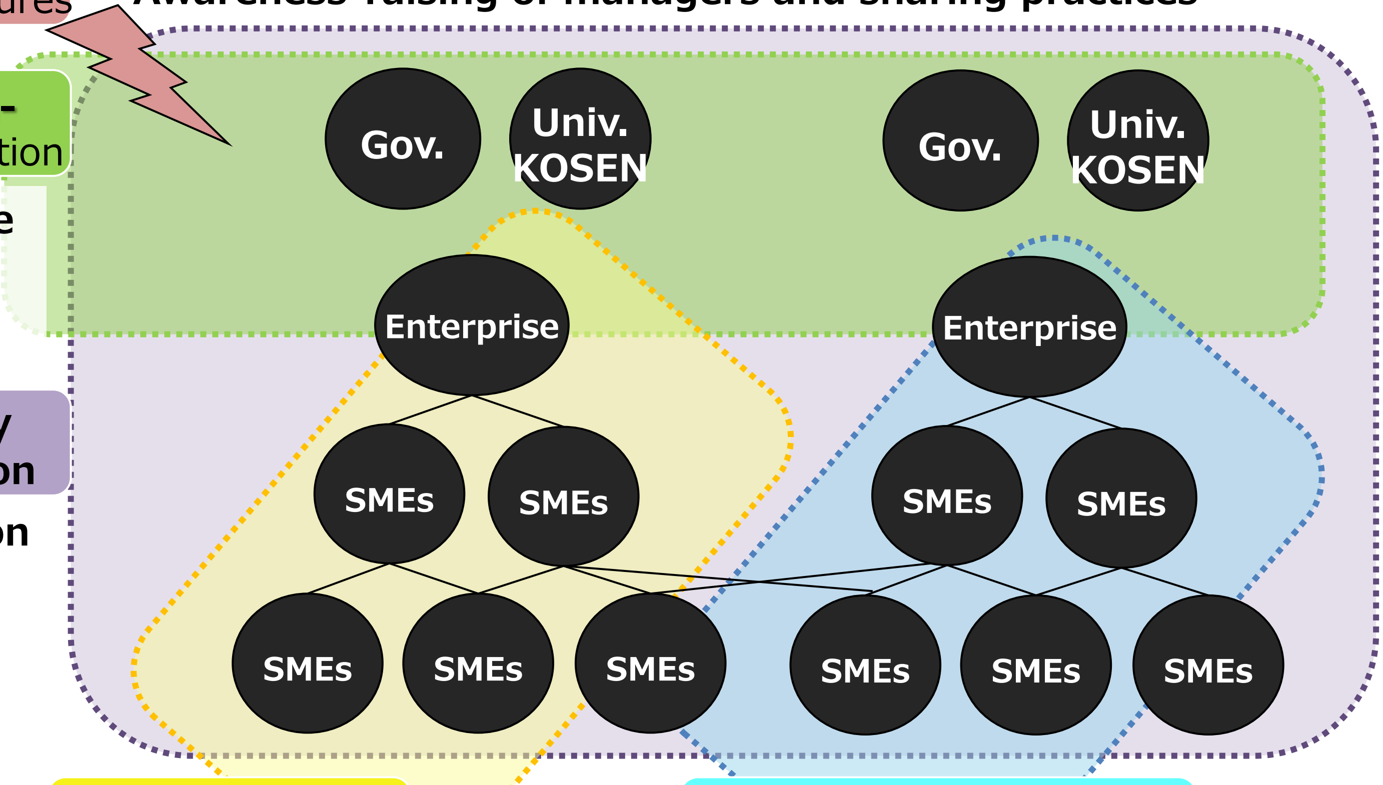
Launch WGs to discuss specific topics based on the requests of members.

Activity Plan of Supply-Chain Cybersecurity Consortium (SC3)

- SC3 is expected to function as a platform for accelerating industry-academia-government collaboration, awareness-raising of managers, and efforts by region and industry to let supply-chain cybersecurity measures permeate throughout the industry.

Cyberattacks
Analysis & Countermeasures

- **Trend of cyberattacks and countermeasures**
- **Awareness-raising of managers and sharing practices**



Industry- academia-government Collaboration

- **Human resource development**
- **Joint research**

Regional **Security Community Promotion**

- **Accelerate formation of regional security community**
- **Share issues, solutions and practices**

SMEs
WG

- **Strengthen cybersecurity of SMEs**
- **Promote "cybersecurity supporters services"**
- **Share issues, solutions, and practices**

Supply-chain security initiatives by industry

- **Share initiatives by industry (building, automotive, electric utility, defense, smart-home, space)**
- **Roll out initiatives to other industry**

JP-US-EU ICS Cybersecurity Week for the Indo-Pacific Region

- METI : Japan, in collaboration with DHS/CISA, DOS and DOE: the U.S. and DG CONNECT : the EC, hosted JP-US-EU Industrial Control Systems (ICS) Cybersecurity Week for Indo-Pacific region.

- **Date :** October 25-29, 2021, Online
- **Participants :** 40 Participants from power/oil/gas companies, National CSIRTs, relevant ministries in the Indo-Pacific Region (ASEAN member states, India, Bangladesh, Sri Lanka, Mongolia and Taiwan) + Audience were invited to the seminar part. Trainees and graduates from the Core Human Resource Development Program provided by ICSCoE joined some sessions as well.
- **Contents :** Remote hands-on training by ICSCoE, ICS cybersecurity seminars by experts from Japan, the U.S., and the EU, Workshops regarding risk assessment/ workforce development by INL and ICSCoE.

<Opening Remarks>

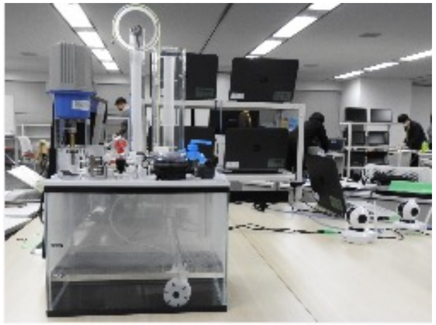
Mr. HOSODA Kenichi
State Minister of Economy, Trade and Industry

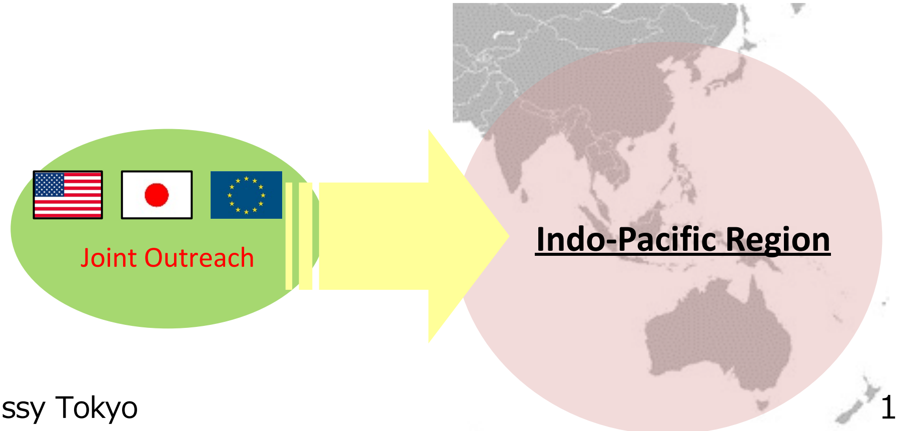
Mr. Eric GOLDSTEIN
Executive Assistant Director for Cybersecurity, CISA

Ms. Lorena BOIX ALONSO
Director, DG CONNECT

Mr. Raymond F. GREENE
Chargé d'Affaires ad interim, U.S. Embassy Tokyo

<Remote Hands-on Training>




Joint Outreach
Indo-Pacific Region