METI
Ministry of Economy, Trade and Industry

Cybersecurity Policy in Japan

- METI's effort against cyber threat -

METI

Cybersecurity Division

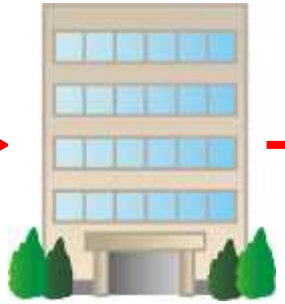
(Case) Ransomware "WannaCry" running rampant

- In May 2017, Worldwide cyber attacks have infected more than 230,000 computers in over 150 countries.
- **Japanese companies are also infected through the infected foreign companies in supply chains.**

Screen lock and payment demand in Bitcoin

Company abroad

Spread



Company in Japan

Spread

ICS PC is also locked and production stops

Spread infection out of the company

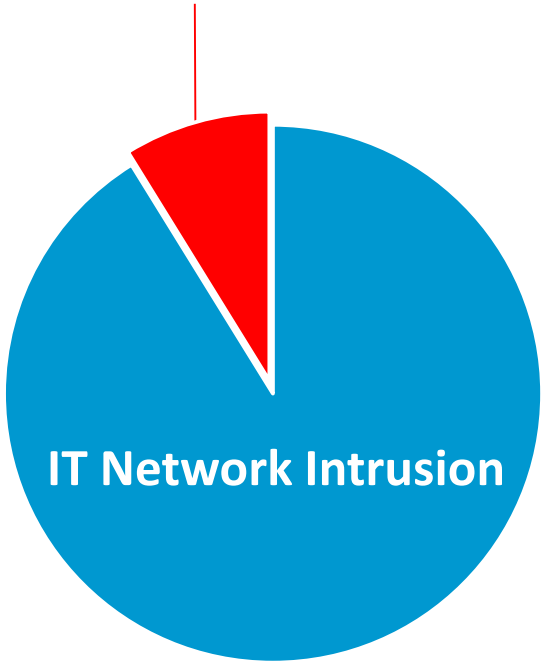
Once the malware intrudes into an office, the infection is exponentially spread via the vulnerability of Windows

Intrusion through Internet or WAN

(Case) Cyber Attacks to ICSs (Industrial Control Systems)

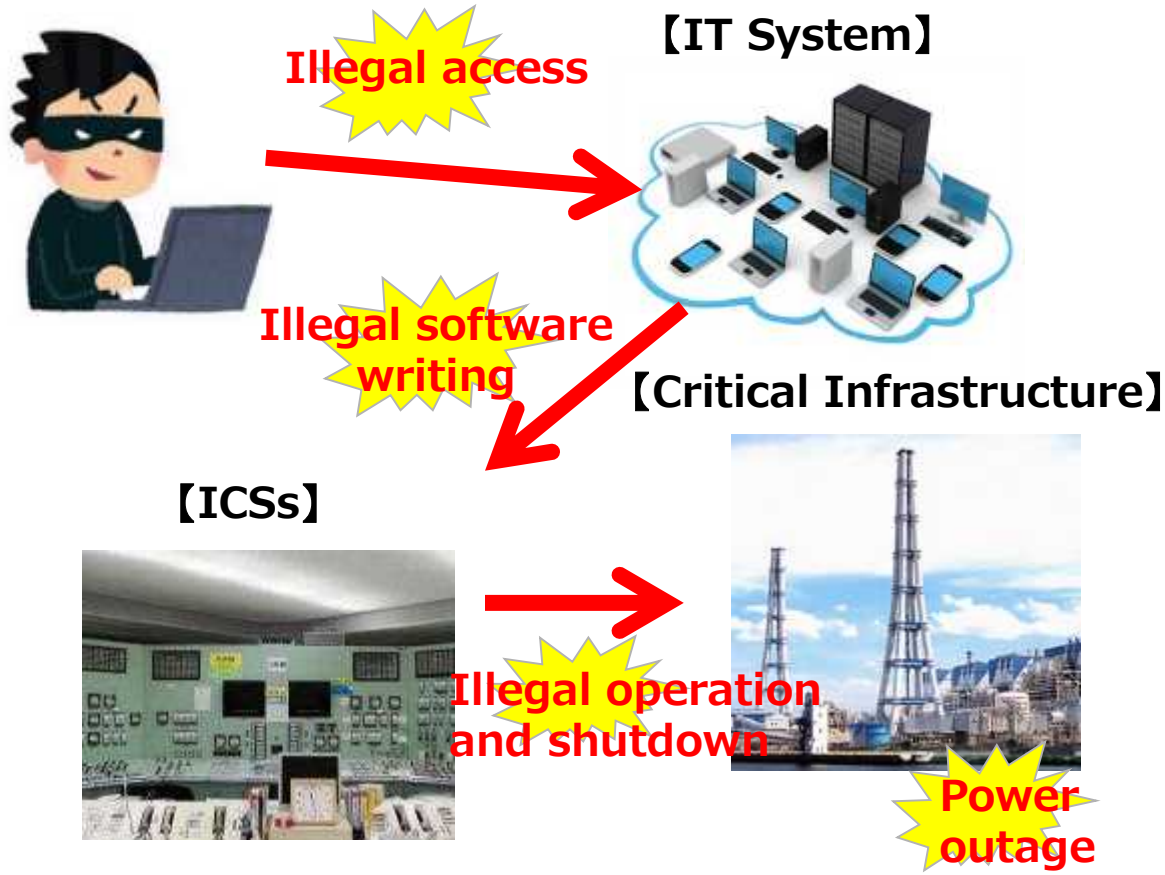
Cyber attacks to critical infrastructures in the US

10 % attacks reached to ICSs



(Source) NCCIC/ICS-CERT Year in Review FY2015
Homeland Security

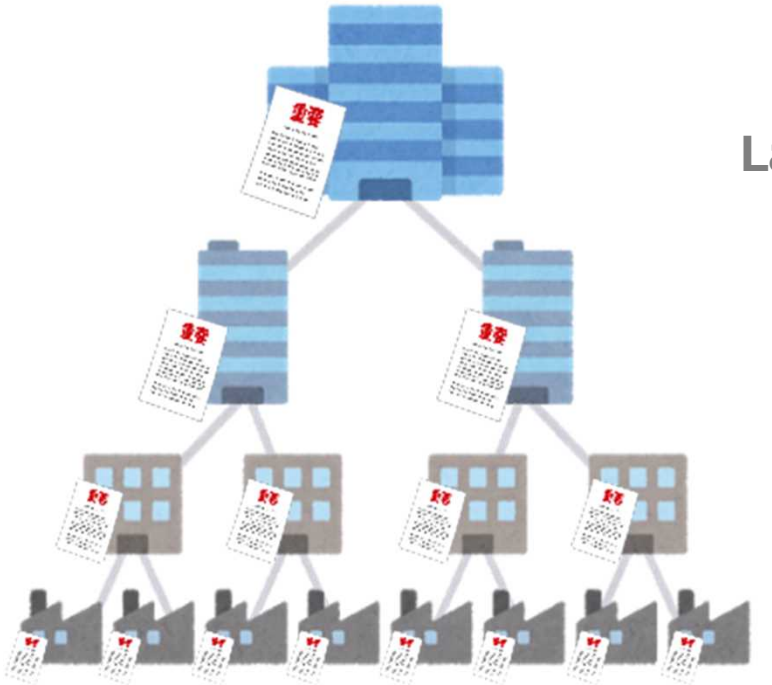
Ukrainian blackout in 2016 (CrashOverRide(Industryoyer))



Importance of supply chain cybersecurity

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

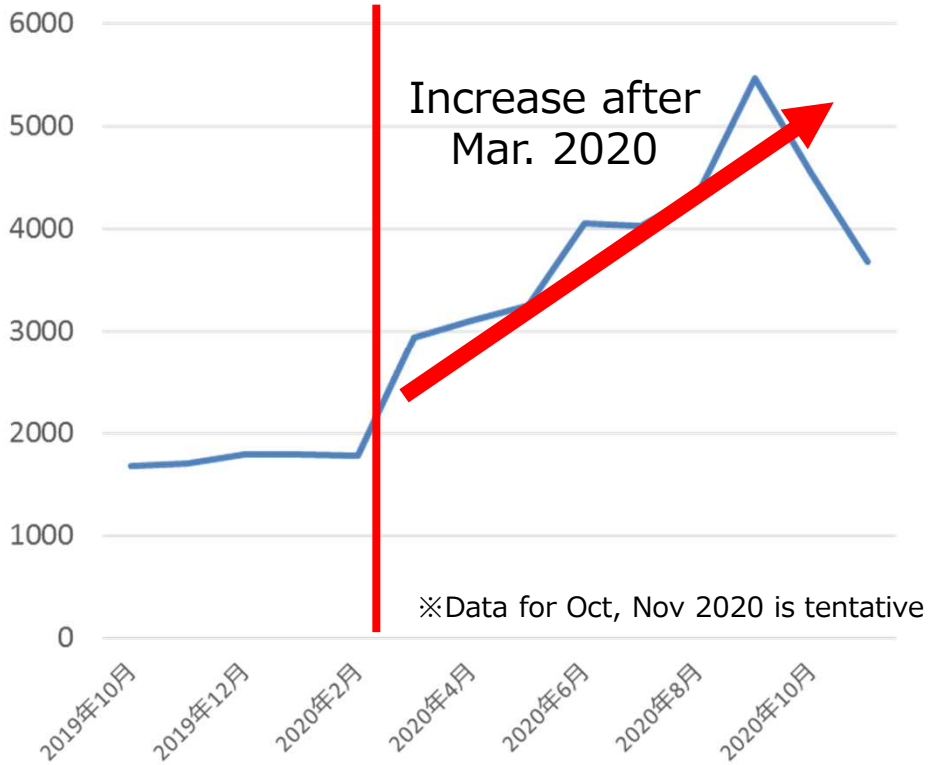
- One of the features of recent cyberattack is increasing number of attacks with intrusion from relatively weak security organizations in the supply-chain, such as overseas branches and business partners.



Recent situation of inquiries related to cyber attacks

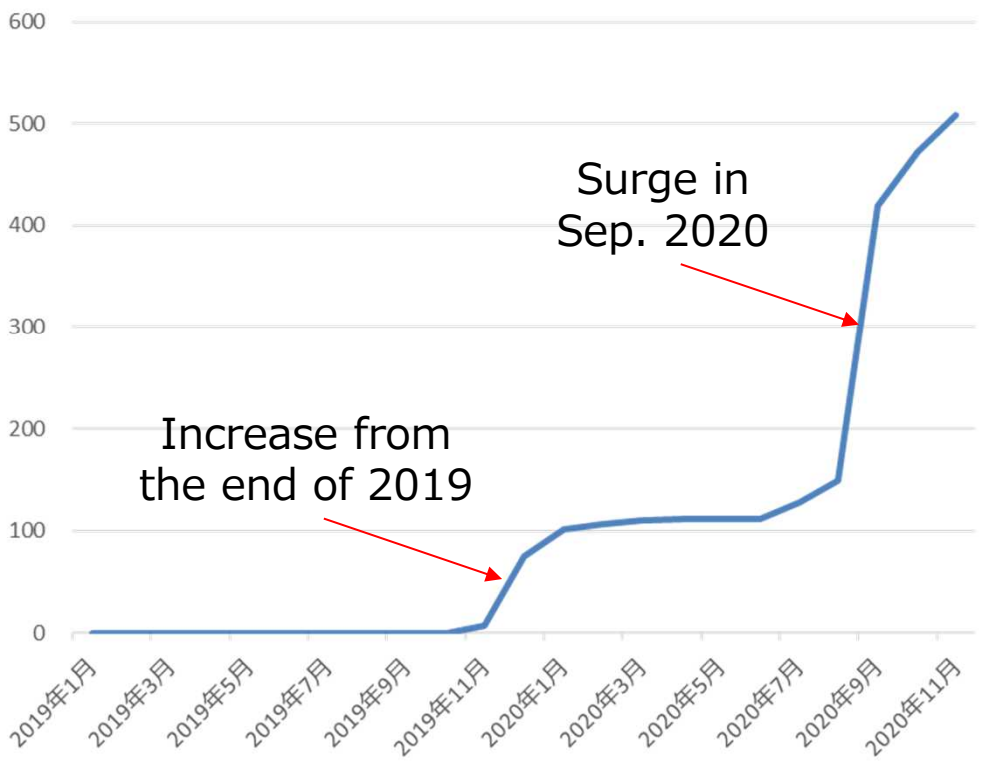
- Since March 2020 under the Covid-19 pandemic, the number of inquiries related to cyber incidents increased.
- Especially, inquiries related to “Emotet” surgered.

Number of inquiries related to cyber incidents to JPCERT/CC (monthly)



<JPCERT/CC>

Number of inquiries related to Emotet to IPA (accumulated)



<IPA>

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

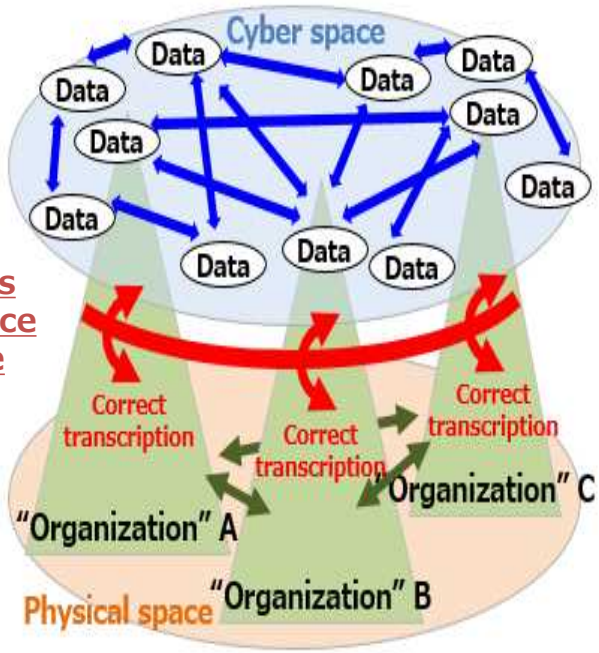
- "**Society 5.0**", where cyber and physical spaces are highly integrated, **enables rather dynamic and flexible creation of supply chain**, while facing with **new risks such as spreading attack points and increasing impact to physical space**.
- **Published "Cyber-Physical Security Framework (CPSF) 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

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.

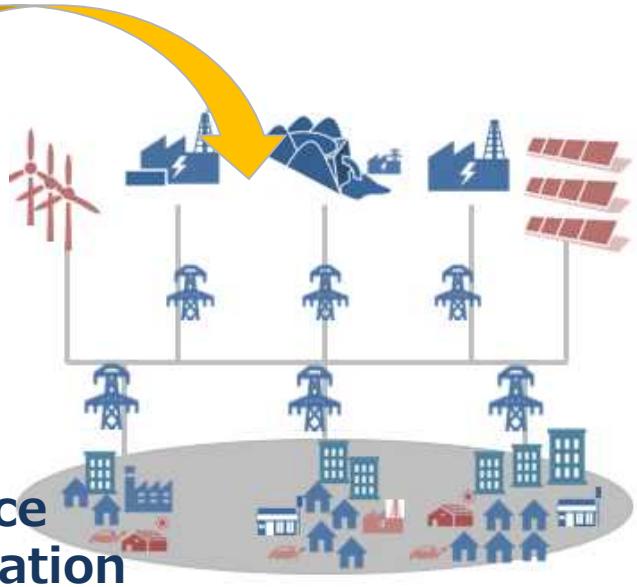
『2nd layer』TF : TF for ensuring the trustworthiness of『Connection between cyber and physical』
- Developed "IoT Security Safety Framework" for ensuring the trustworthiness between cyber space and physical space

Adoption of CPSF in sectoral security guidelines

- CPSF is incorporated in some security guidelines, such as cross-sector or specific sectors where the cybersecurity is a key to maintain the operations.
  - Smart City Security Guidelines (Ver. 2.0) -- published by Ministry of Internal Affairs and Communications (MIC), in June 2021
  - ERAB(Energy Resource Aggregation Business) Cybersecurity Guideline (ver. 2.0) --- published by Agency for Natural Resources and Energy (ANRE), in December 2019

Smart City

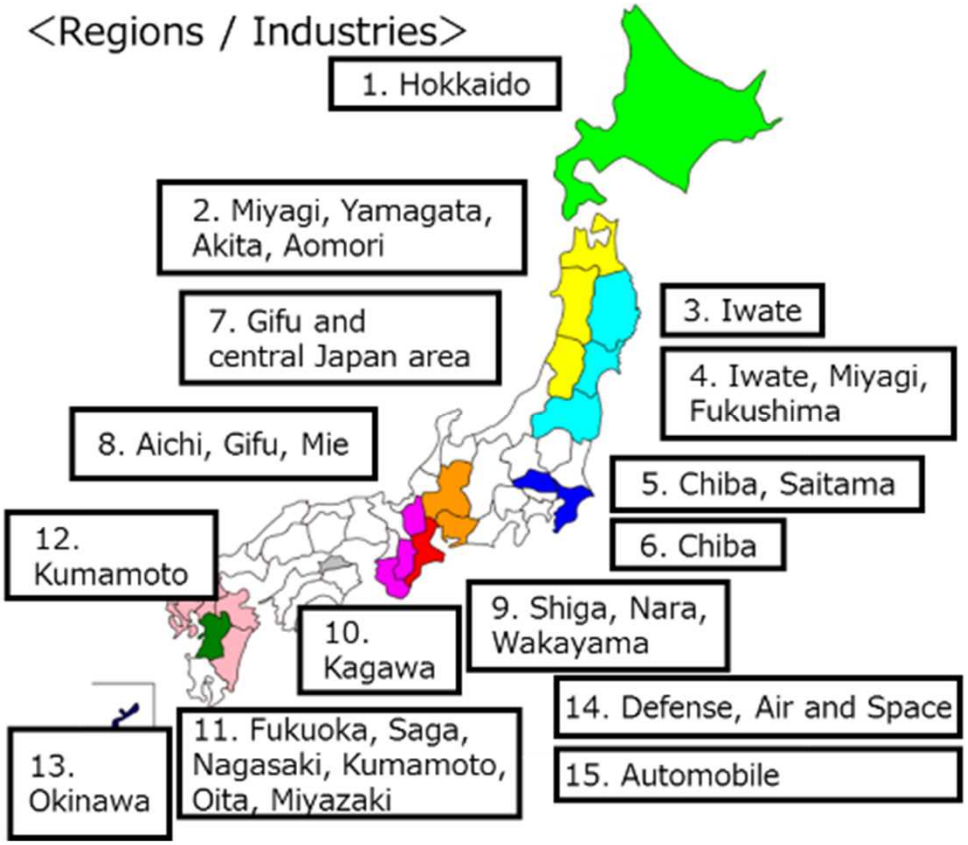
CPSF

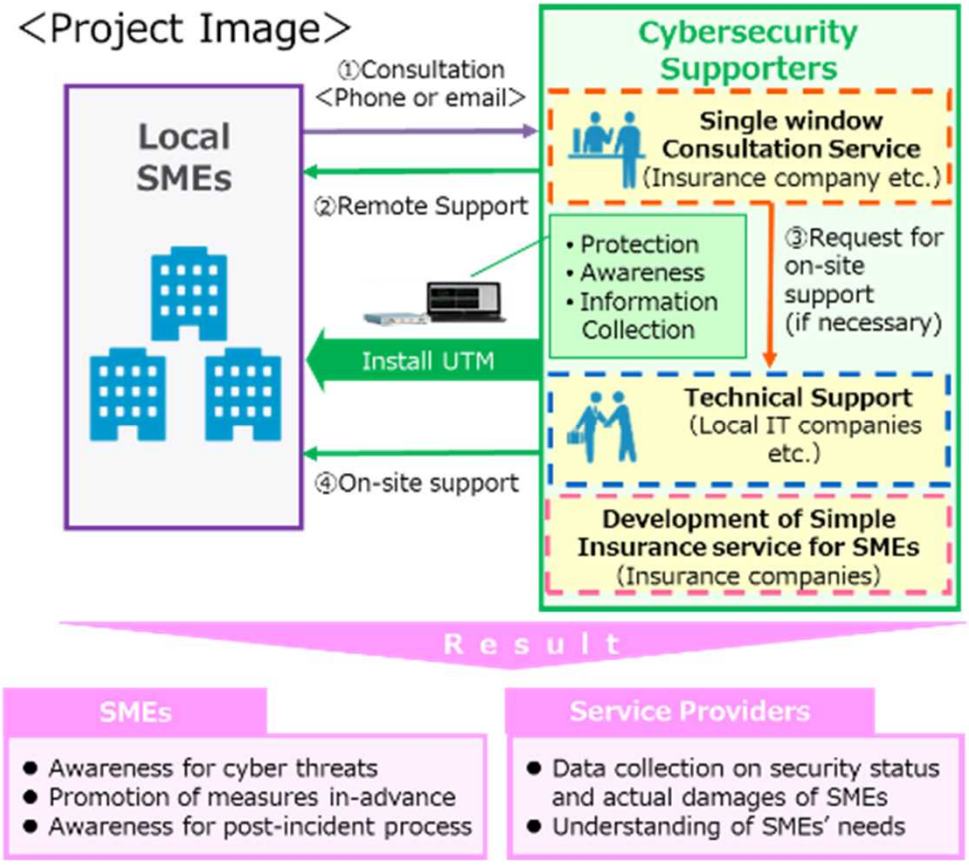


Energy Resource Aggregation

“Cybersecurity Supporters” for SMEs in FY2019-2020

- Local organizations, security companies, and insurance companies formed a consortium to implement POCs structuring security measure support system for SMEs (FY2019: 8 projects, FY 2020:15 projects).
- Aimed to generate a simple security insurance service for SMEs by the private sector through promotion of proactive measures by SMEs, awareness raising for SMEs, understanding actual situation of attacks and needs.





*Project Regions in FY2019（8 Regions in total, 1064 SMEs joined）:
1. Miyagi, Iwate, Fukushima, 2.Niigata, 3.Nagano, Gunma, Tochigi, Ibaraki, Saitama, 4. Kanagawa, 5. Ishikawa, Toyama, Fukui, 6. Aichi, 7. Osaka, Kyoto, Hyogo, 8. Hiroshima, Yamaguchi

Industrial Cyber Security Center of Excellence (ICSCoE)

- Established in Apr. 2017. Provides one-year program for comprehensive study on technology, management, and business.
- 48 trainees in 5th year of "Core HR Development Program" from Jul. 2021.

☐ **Intensive training throughout year.**

☐ **From companies such as Electric power, Oil, Gas, Chemicals, Automobiles, Railways.**
(Number of Trainees: 1st Year : 76、2nd Year : 83、3rd Year : 69、4th Year : 46、5th year: 48)

Annual Schedule

July	Aug.	Sep.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	April	May	June
Primary (Basic Knowledge Review)			Basic (Basic Exercise)				Advance (Advanced Exercise)			Final Project	
Opening			Business/Management/Ethics								Closing
			Professional Networking (including overseas)								

- Foster specialists for IT and OT
- Plan measures by utilizing mock-up plants
- Assess the security and reliability of ICS
- Investigate and analyze cyber attacks

Cultivate leaders of industrial cybersecurity

☐ **Programs in cooperation with overseas partners.**

➢ Extensive hands-on training 301 conducted by DHS

➢ Lectures, exchange opinions with government, industry and start-up companies

➢ Exchange opinions with security experts from government and industry, visit to research institutions

ICSCoE (Akihabara Campus)

Entrance

Simulated Plants

Active Learning Room

ICSCoE (Bunkyo Campus)

Entrance

Active Learning Room B

Active Learning Room A

Lecture Room

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

- METI and ICSCoE, in collaboration with the government of the United States (DHS/CISA, DOS and DOE) and the European Commission (DG CONNECT), hosted JP-US-EU Industrial Control Systems (ICS) Cybersecurity Week.

- **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>