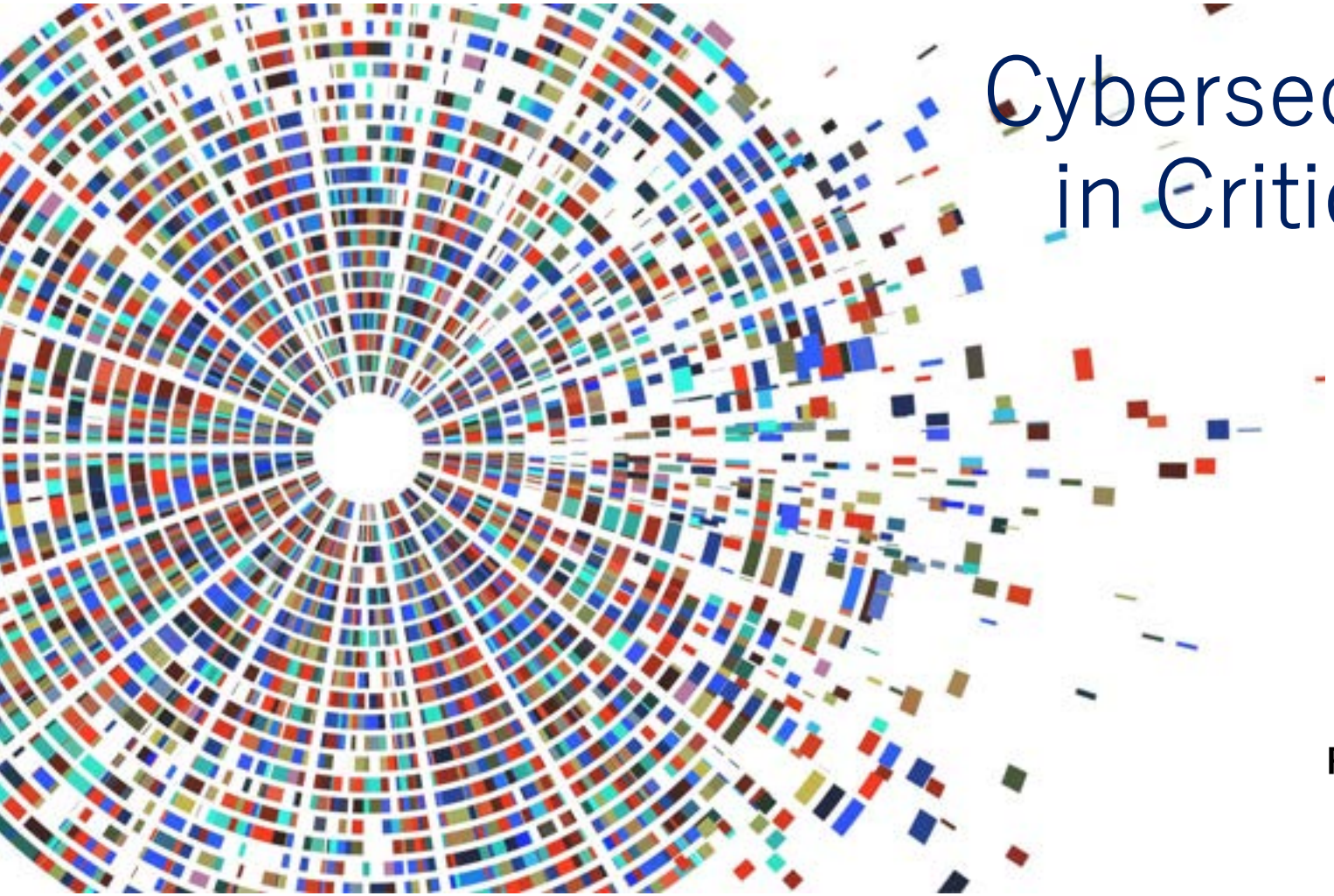


Cybersecurity Preparedr in Critical Infrastructures (CIs)

IC-AJCC 2023

Kenji Watanabe

Professor of Graduate School of Social Engineering
Head of Disaster and Safety Management

Nagoya Institute of Technology (Japan)

AGENDA

1. Scope of Critical Infrastructures(CIs) and important factors to be discussed

2. Case Study: Cyber-Physical Security for Seaport Operations

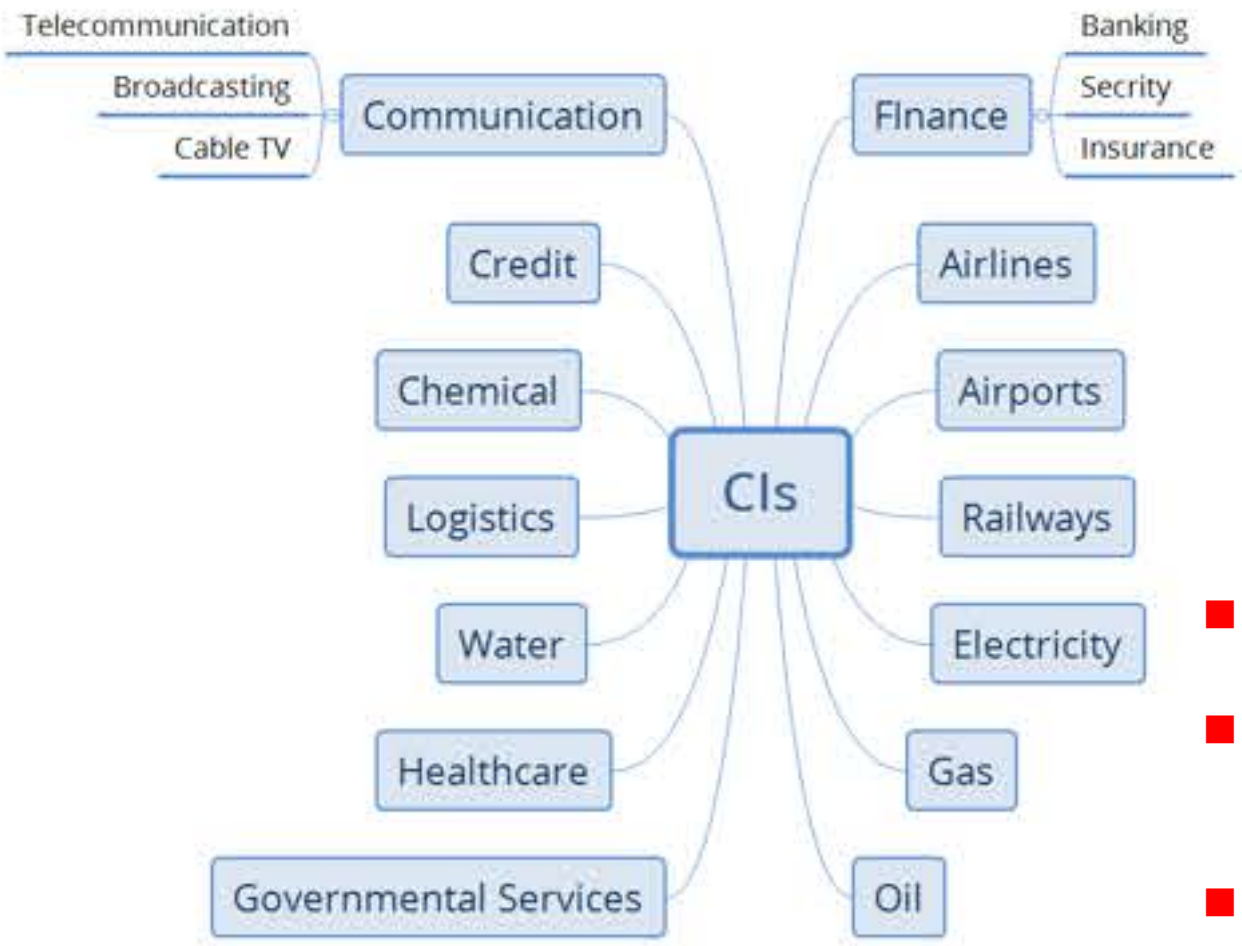
3. Important aspects to be discussed for Cyber-Physical Security for CIs

Next Steps and Challenges

1. Scope of Critical Infrastructures（CIs） and important factors to be discussed

Scope of Critical Infrastructures (CIs) in Japan [1/2]

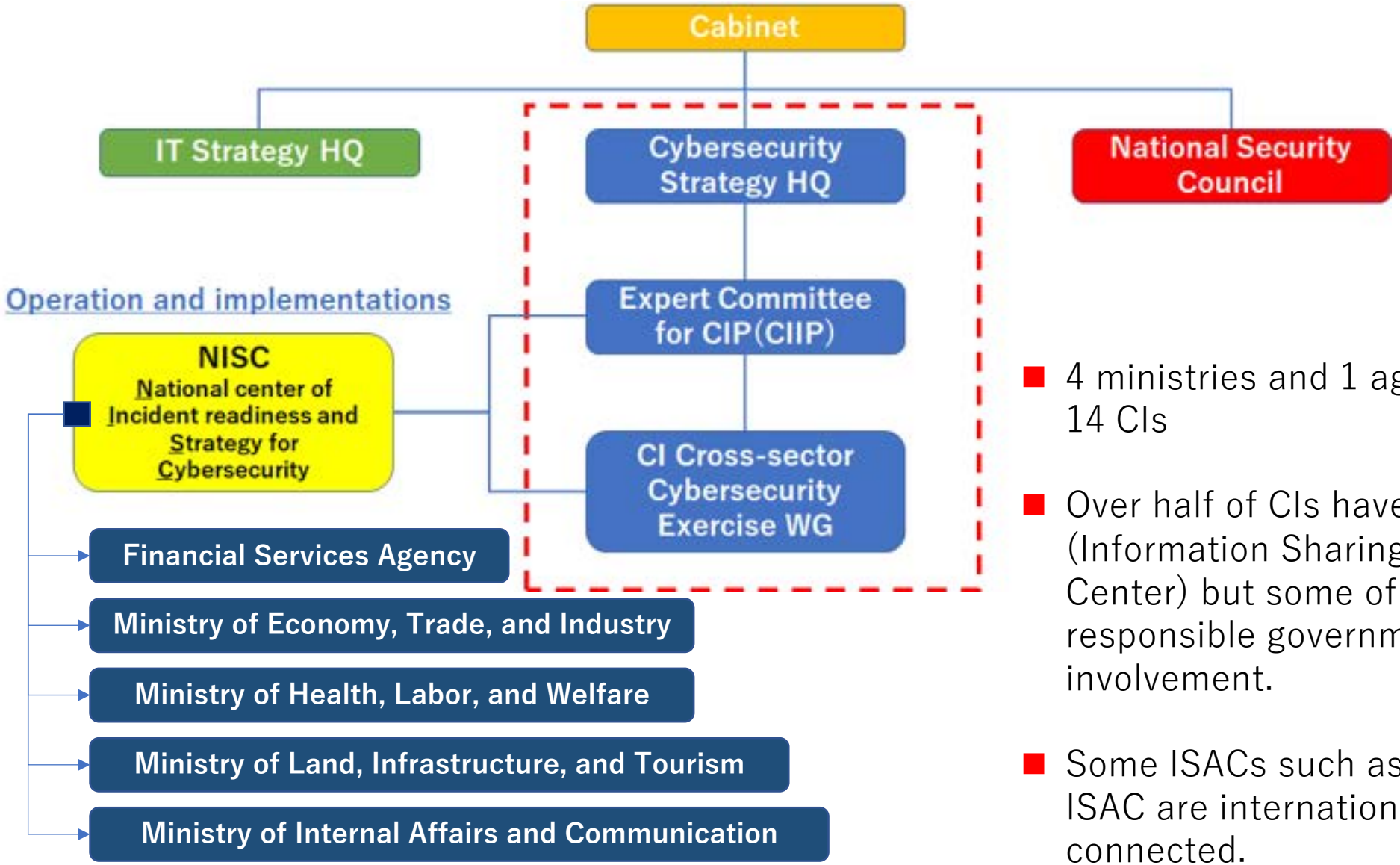
Definition of critical infrastructure varies slightly from country to country: “Autonomic” approach



- 14 CIs are defined by the Cybersecurity Basic Act
- NISC is monitoring CI operations to define safety standards and to coordinate cross-sector exercises.
- Actual coordination with CIs is governed by each responsible ministry or agency.

Scope of Critical Infrastructures (CIs) in Japan [2/2]

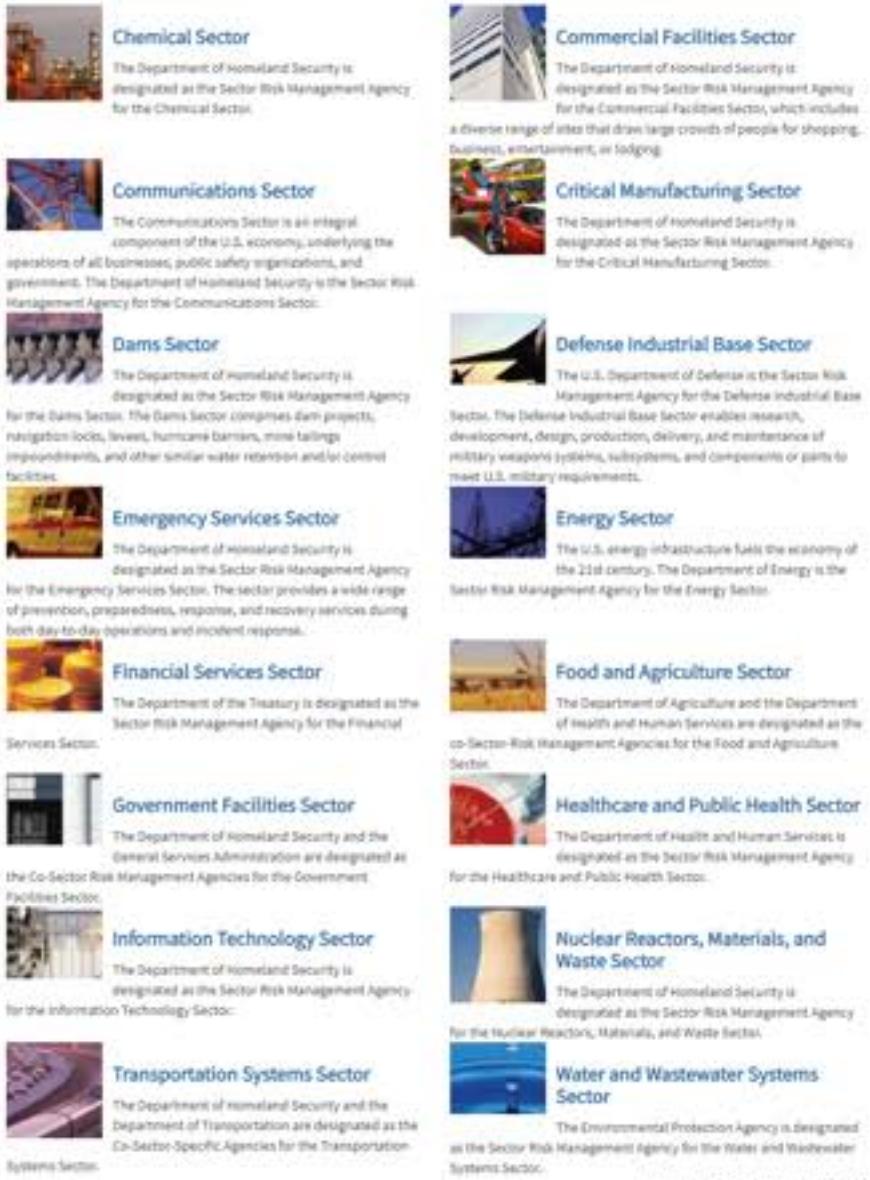
Definition of critical infrastructure varies slightly from country to country: "Autonomic" approach



- 4 ministries and 1 agency govern 14 CIs
- Over half of CIs have ISAC (Information Sharing and Analysis Center) but some of them have responsible government's involvement.
- Some ISACs such as Financial ISAC are internationally connected.

Scope of Critical Infrastructures (CIs) in US [1/2]

Definition of critical infrastructure varies slightly from country to country: Cross-sector approach



Chemical Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Chemical Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector Risk Management Agency for the Communications Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Financial Services Sector
The Department of the Treasury is designated as the Sector Risk Management Agency for the Financial Services Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector Risk Management Agencies for the Government Facilities Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Information Technology Sector.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Critical Manufacturing Sector.

Defense Industrial Base Sector
The U.S. Department of Defense is the Sector Risk Management Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector Risk Management Agency for the Energy Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the co-Sector-Risk Management Agencies for the Food and Agriculture Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector Risk Management Agency for the Healthcare and Public Health Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Nuclear Reactors, Materials, and Waste Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector Risk Management Agency for the Water and Wastewater Systems Sector.

*DHS: Department of Homeland Security, **CISA: Cybersecurity and Infrastructure Security Agency

- Systems or assets, whether physical or virtual, that are critically important to the United States
- An impact that, if unavailable or destroyed, would undermine security, national economic security, or national public health or safety.
- First defined in PDD***-63 during the Clinton administration in 1998 and subsequently revised.
- Cross-departmental related organizations include CISA (Cybersecurity & Infrastructure Security Agency) and DHS (Department of Homeland Security).
- Differences from Japan: Dams, emergency services, government facilities, IT, commercial facilities, core manufacturing, military industry, food and agriculture, sanitation, sewage

***PDD: Presidential Decision Directive

Scope of Critical Infrastructures (CIs) in US [2/2]

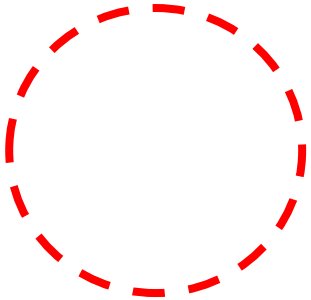
CISA is working with the corresponding sector-specific agencies in cybersecurity

CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & CISA
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Scope of Critical Infrastructures (CIs) in UK

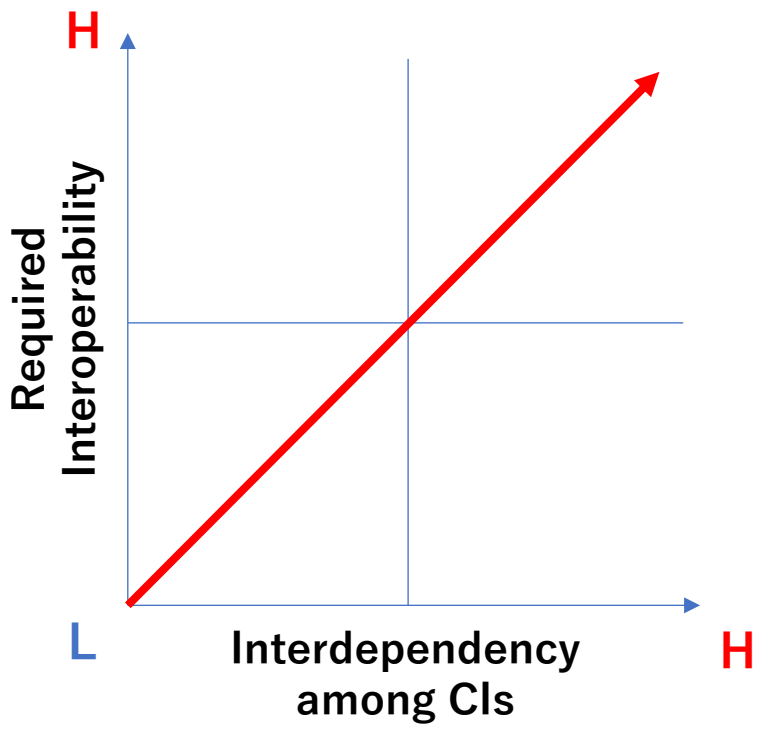
Definition of critical infrastructure varies slightly from country to country: UK(CPNI*)

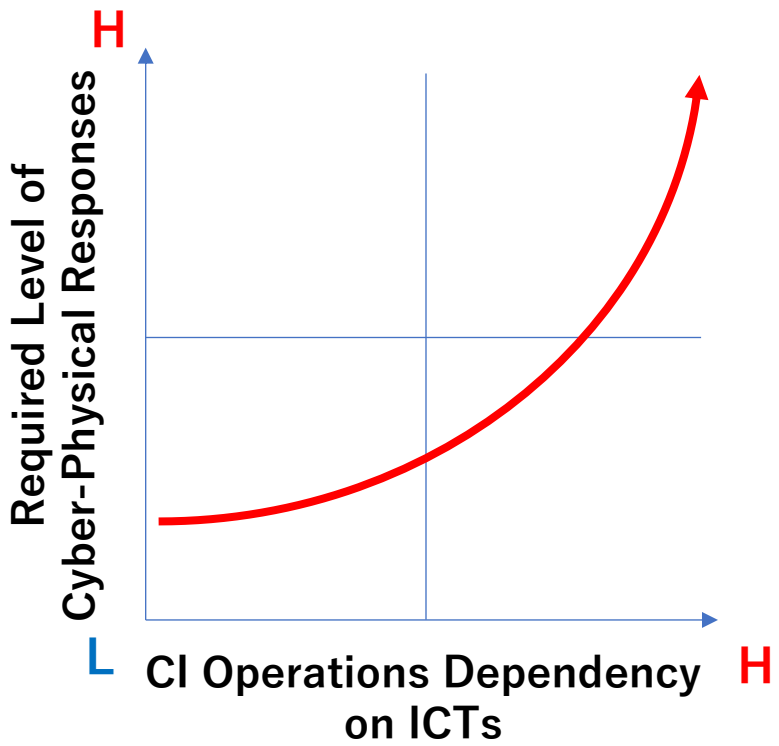
*CPNI: Centre for the Protection of National Infrastructure



Important factors to be discussed: It's obvious but things to be reminded [1/3]

Interdependencies, Interoperability, and Cyber-Physical Integrated Responses





- Rapidly **increasing interdependencies** among CIs require **well-coordinated interoperability** among CI operators and responsible governmental agencies in the **incident responses** (cyber and physical incidents)
- Emerging **dependencies on ICTs** of CI operations caused **more physical failure consequences** triggered by cyber incidents which requires **Cyber-Physical integrated responses**.

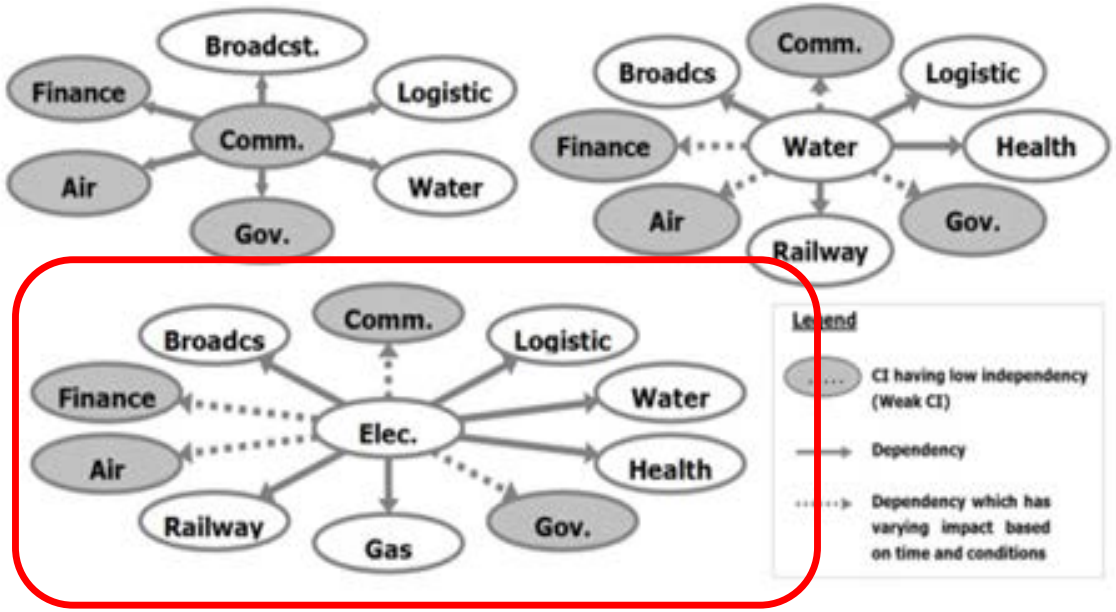
Important factors to be discussed: It's obvious but things to be reminded [2/3]

There are some "hub" of interdependencies among CIs and highly possibility cause failure consequences

- **The electricity sector** is in a position to demand a more resilient cybersecurity system because the **social and business impacts of service outages and functional degradation in the sector would be significant**. (Many of other CIs have heavy dependency on the electricity sector)

- Any disruptions in the sector will **cause chain failures** in the sector of **Telecom, Finance, Railways, Healthcare, Broadcast, and Governmental Services**.

- This makes it **an ideal target for cyberattacks** that could **cause social disorder** and all related CIs have to **build interoperability in the incident responses** with responsible governmental agencies.



Important factors to be discussed: It's obvious but things to be reminded [3/3]

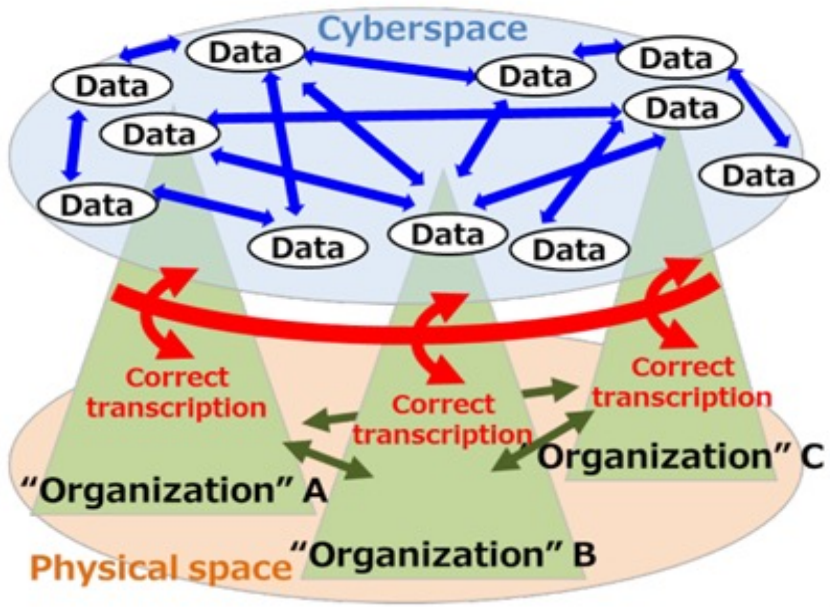
Emerging dependencies on ICTs of CI operations cause more physical failure consequences

- **Emerging dependencies on ICTs** of CI operations caused **more physical failure consequences** triggered by cyber incidents which requires **Cyber-Physical integrated responses**.
- This **accelerates failure spreads** among CIs through **interdependencies**.
- METI (Ministry of Economy, Trade, and Industry of Japan) has **developed a framework** to mange the situation. (**CPSF: Cyber Physical Security Framework**)
- CPSF is currently **being standardized internationally** based on a Japanese proposal, and addressing supply chain risks, among others.

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



CPSF Framework developed by the Japanese Government (METI)

2. Case Study: Cyber-Physical Security for Seaport Operations

Cyber-Physical Incident in Seaport Operation (July 4,2023: Nagoya, Japan)

Cyber-triggered physical incident and the importance of establishing communication lines with local police

- The Nagoya Port**, one of the largest container handling port**, had been **closed for two and half days by cyberattack** with ransomware.
- Approximately **20 thousands containers** could not be handled.
- The operator recovered the system **from the back-up data**.
- Aichi **Prefectural Police contributed** to the early recovery.

July 4, 2023

0630: Container handling system shutdown
0730: A large number of threatening texts were printed from printers
0900: Notify the Cyber Attack Response Team at the Aichi Prefectural Police
1400: Verify all encryption of physical and virtual servers
1800: Discussed response with Aichi Prefectural Police
（Virus removal of backup data, network failure response, etc.）

July 6, 2023

1415: System recovered and backup data and yard inventory consistency checked.
1500: Operation resumed sequentially from Tobishima Pier South Terminal

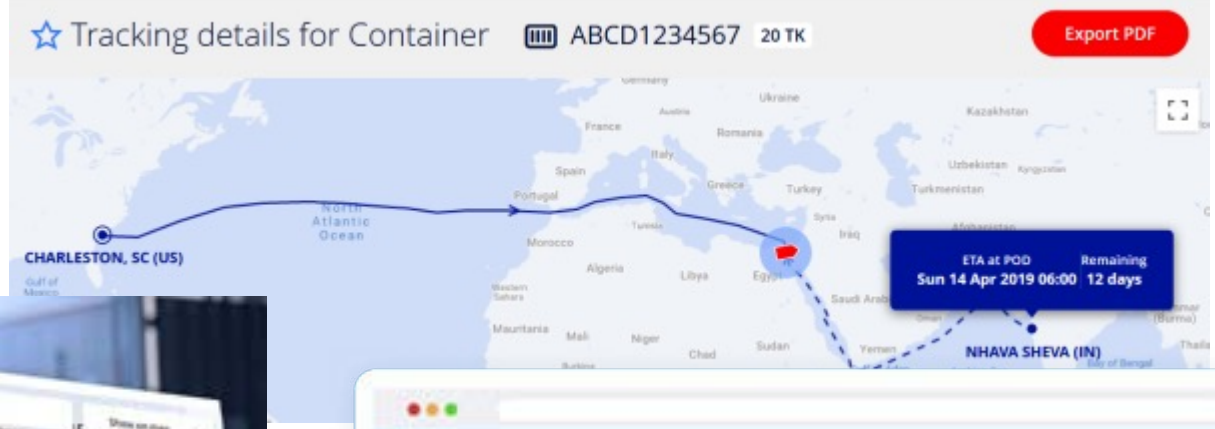
Consideration for more severe cyber-triggered physical incidents

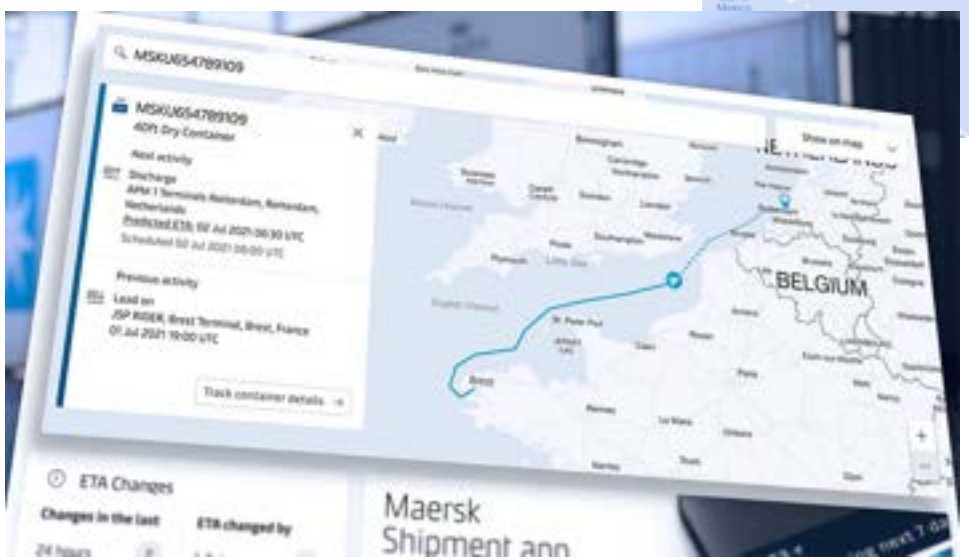
Many stakeholders in private/public sectors make the situation difficult in response to the severe incidents

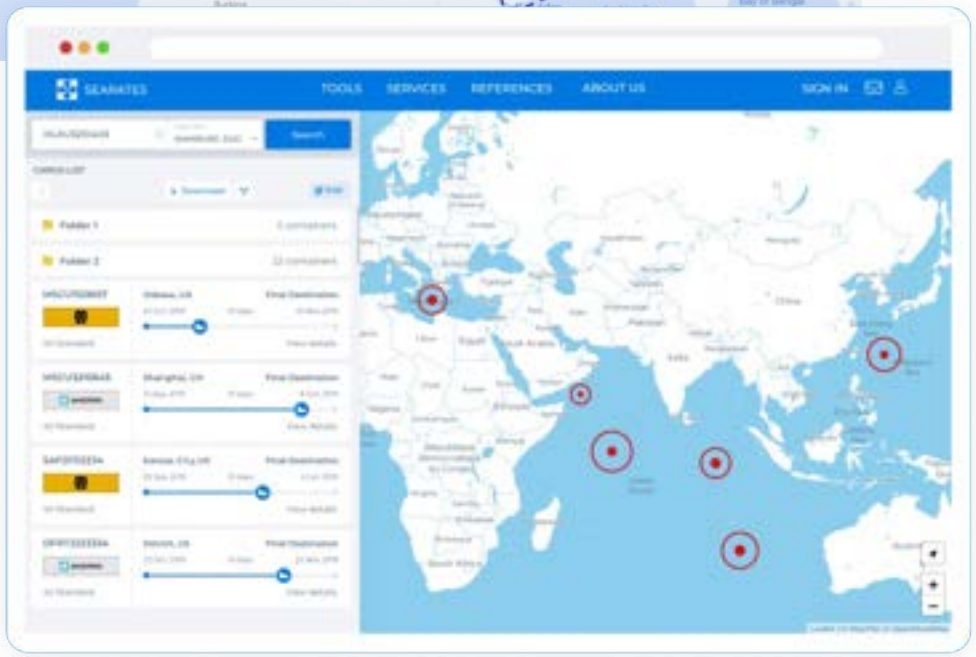
- **Largest manufacturing and import/export operations** of TOYOTA locate in the Nagoya area.
- Critical **suppliers for global supply chains** also locate.
- **Too many large stakeholders** are factors of challenges for coordination
- **4 cities and 1 village** are responsible for the Port of Nagoya and it also makes the situation difficult.
- **2 ministries** (for transportation and industry supply chains) should be involves **addition to the local governments**
- Companies for port handling, warehousing, container transportation, and other related companies are **additional stakeholders to be coordinated**.

Another Cyber-Physical Incident in Marine Transportation (2017)

Cyber-triggered physical consequences at the global level: MARSK Container & Freight Tracking System







- Individual container status can be monitored in addition to ship navigation status.
- In the event of an incident, it is used to coordinate and negotiate with shipping companies and business partners.

Another Cyber-Physical Incident in Marine Transportation (2017)

Cyber-triggered physical consequences: global confusions and many servers, PCs, and software replaced

World Maritime University
The Maritime Commons: Digital Repository of the World Maritime University

World Maritime University Dissertations | Dissertations

11-4-2018

Cyber-attacks: a digital threat reality affecting the maritime industry

David Miranda Silgado

Follow this and additional works at: https://commons.wmu.se/all_dissertations
Part of the Transportation Commons

Recommended Citation
Miranda Silgado, David, "Cyber-attacks: a digital threat reality affecting the maritime industry" (2018). *World Maritime University Dissertations*. 663.
https://commons.wmu.se/all_dissertations/663

This Dissertation is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.

Cyber-attacks_ a digital threat reality affecting the maritime in.pdf

Lessons learnt from the case and further discussion points

Importance of preparedness phase and leveraging knowledges & experiences in natural disaster responses

Lessons learnt

- Importance to establish **communication line with the local police before any incidents**. It made them able **to recover with in a short term** and to keep the incident **within a single CI sector**.
- **Independent data backup** is effective but need periodical virus check.
- **Public communication at appropriate timings and intervals** are important to avoid unnecessary confusions

Further Discussions

- Some industry players in the automotive industry **absorbed the impacts** of the 2 and half days' disruption **by normal production adjustment** for **natural disasters**(typhoon, flood, snow) and **suppliers' operational troubles**.
- However, the difficult part for them in taking response actions was **the situation that they could not know when it would be ended**.
- If the expected recovery time would take longer, they were going to **activate the wide-area BCP (Business Continuity Plan)** with the alternative options **prepared for the severe earthquake** expected in the region.

3. Important aspects to be discussed for Cyber-Physical Security for CIs

Important aspects to be discussed for Cyber-Physical Security in CIs

Consideration focusing on consequential(resulting) events rather than on cause (trigger) events

- The number of the incidents in CI operations **triggered by a cyber cause and resulted in physical consequences** in the people's life and socioeconomic activities **are still limited**.

- However, if we **leverage our knowledges and experiences** in the consequences after the disruption of CI operations **cause by the natural disasters**, **simulations and evaluations of consequences after a cyber incident can be done**.

- **Combined approach of ETA (Event Tree Analysis) and FTA(Fault Tree Analysis)** will be an effective way to **enrich incident scenarios** that can be used for **preparedness(e.g. drill & exercises) & response(e.g. proactive defense) phases.**

- In order to **ensure economic rationality** of **the investment of management resources** (HR/Tools/Money/Information) in cybersecurity, **BIA(Business Impact Analysis)** and **SIA(Social Impact Analysis) are necessary**.

- In the actual incident response by CI providers, it is important to **establish a regional cross-CI community** including the **local police or investigation agency** through **periodical information meetings and cross-sectoral exercises** before actual cyber-physical incidents.

Local professional community for Cyber-Physical CIP (Nagoya-Japan)

CCSC: A private sector-driven security community for CIP

- As cyber incidents that occur in critical infrastructure are **likely to have physical consequences**, it is necessary to **ensure coordination and interoperability among CI** providers that actually operate in a particular region, especially in greater metropolitan areas.
- The **Chubu Cyber Security Community (CCSC)** in the Chubu region (Nagoya) is actually implementing such efforts, promotes **information sharing** and the **implementation of exercises** under a region-specific structure.
- Local **electric power grid company** takes a role of a secretariat, and critical infrastructure providers such as **gas**, **telecommunications**, **railroads**, **airport**, **automotive**, and **highways**, along with **prefectural polices**, **experts**, and **specialists.**

CIs defined by NISC

Electricity

中部電力

Gas

東邦ガス株式会社

MEITETSU

Railroad

NTT 西日本

Telecom

centrair

Airport

CIs defined by the Region

NEXCO 中日本

Highway

TOYOTA

Automotive

Supporting Agency

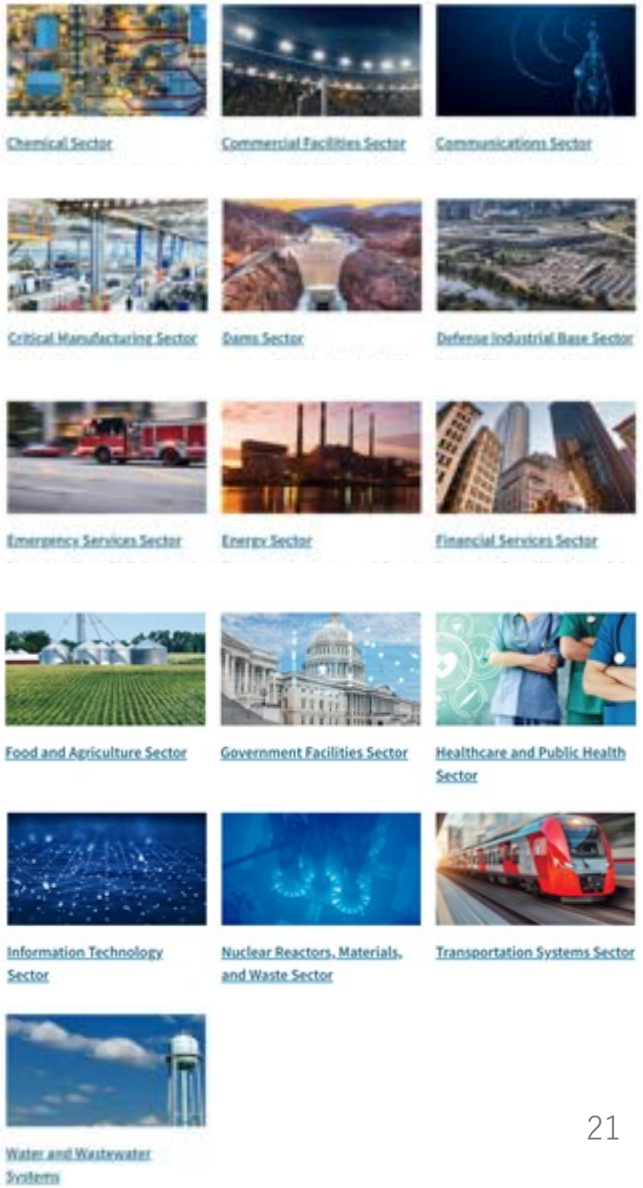
Prefectural Polices

Local professional community for Cyber-Physical CIP (US)

InfraGard: A partnership between FBI and CI operators for CIP

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes: business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security.

- Region-focused CIP
- FBI provide a platform for education, information sharing, networking, and etc.
- Also responses to the needs for intelligence supports
- FBI is supporting the efforts in Japan



Source: https://www.infragard.org/

Next Steps and Challenges

Next Steps and Challenges

- **Operational integration** of cyber and physical security by **PPP (Public-Private, Private-Private, Public-Public)**-based joint efforts.
- **Organically merge the professionals** in the both area (Cyber/Physical) into **practical CIP operations**
- Enhance each **region-focused approach**(including trial & error) and connect **nationwide and internationally** to build resilient CIP network.
- Apply knowledges and experiences of **consequential incident responses** of CIs in large scale **natural disasters** into the Cyber-Physical security for CIs. (Especially **in metropolitan areas**)

"To start from Cyber, or to start from Physical, that is NOT the question !"

Thank you

For further discussions:

watanabe.kenji@nitech.ac.jp