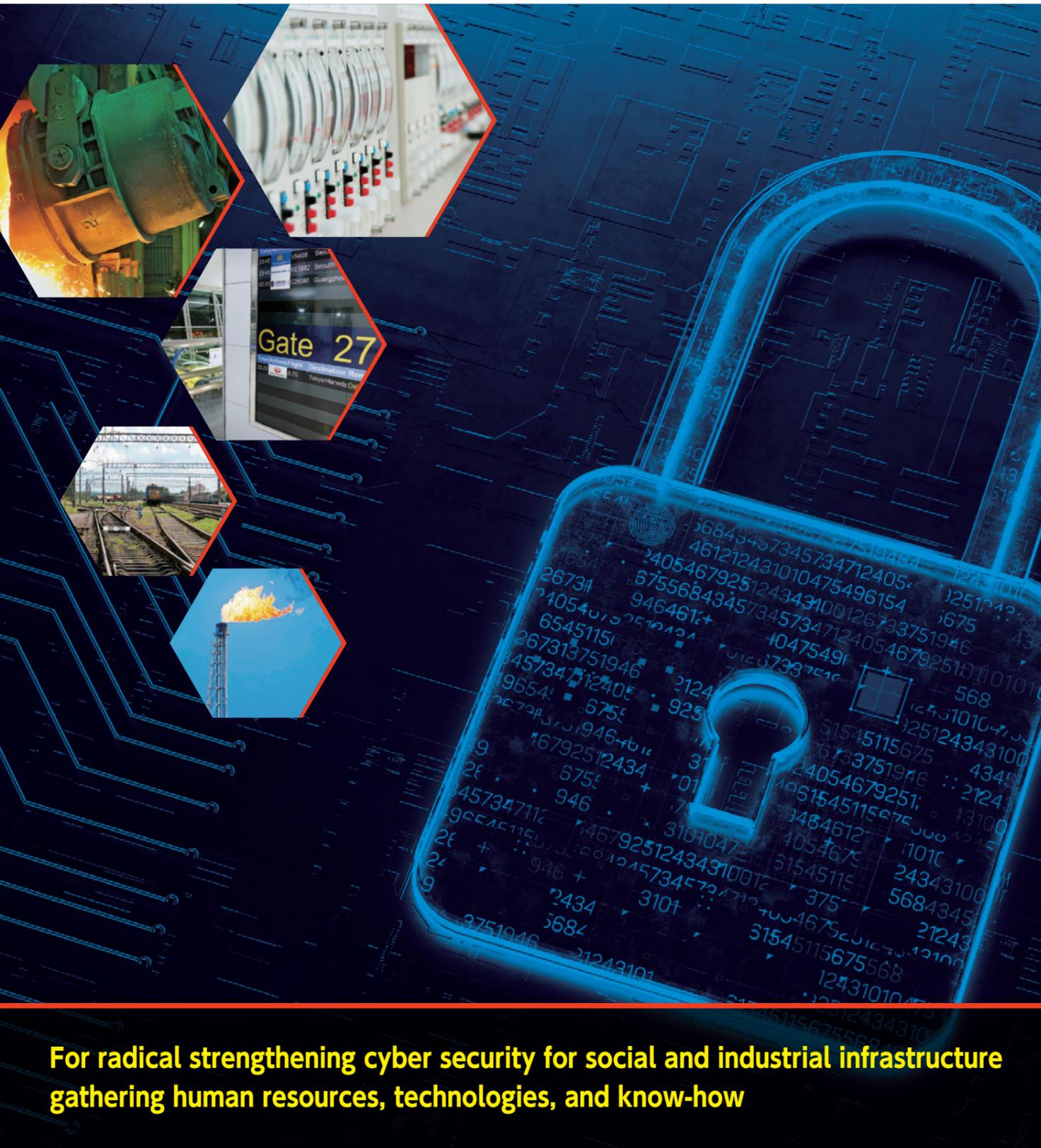


In recent years, the risks of cyber attacks that inflict physical damage on the social and industrial infrastructures have been increasing. Due to the cyber attacks launched by foreign countries, the incidents endangering the safety of such infrastructures have already occurred overseas. Strengthening protections against cyber attacks in social and industrial infrastructures is an urgent national issue.



For radical strengthening cyber security for social and industrial infrastructure gathering human resources, technologies, and know-how

A core hub achieving world-class cyber security measures assembling OT and IT

産業サイバーセキュリティセンター (ICSCoE)
Industrial Cyber Security Center of Excellence

Human resource development program

- Provide programs for the operators engraining in social and industrial infrastructures to develop human resources capable of determining necessary security measures while identifying risks of in-house systems
- Install the simulated plants, where preparing everything from information systems to operational systems; Conduct exercises for safety and reliability verification and prompt system recovery together with experts
- Learn state-of-art technologies and know-how and create communities to promote collaborations with security officers and experts from other industries and overseas
- Accumulate global knowledge and create opportunities to exchange knowledge with overseas experts through active collaborations with foreign countries
- Disseminate information and provide training to corporate executives on the actual situation of cyber attacks and the necessity for industrial cybersecurity

Ideal of industrial cybersecurity experts

Develop the capabilities to understand the necessity of cybersecurity measures and promote projects enthusiastically, based on both OT (operational technology) and IT (information technology) skills

Understanding of ethics, norms, and laws

- Learn the fundamental principles of contributing knowledge and skills back to societies

Management & leadership

- Promote projects enthusiastically
- Prioritize measures and incorporate them into business plans
- Create a roadmap of reform concepts

Technology skills (OT/IT)

- Identify threats to critical infrastructures and examine their defensive measures
- Respond to incidents and secure business continuity

Business skills

- Understand business models and competitive advantages of companies
- Grasp the impacts of cyber damage quantitatively
- Calculate cost-efficiency
- Prioritize measures

Professional network formation

Risk assessment activities on the safety and reliability of actual control systems

- Conduct risk assessments on the safety and reliability of control systems for social and industrial infrastructures in Japan
- Investigate all possibilities of cyber attacks and plan the necessary measures

Investigation and analysis of cyber attacks

- Collect information on the latest cyber attacks (e.g., observe decoy systems, amass information on cyber attacks from professional organizations in the private sector, etc.)
- Investigate and analyze new attack methods to utilize for human resources development and system verification activities

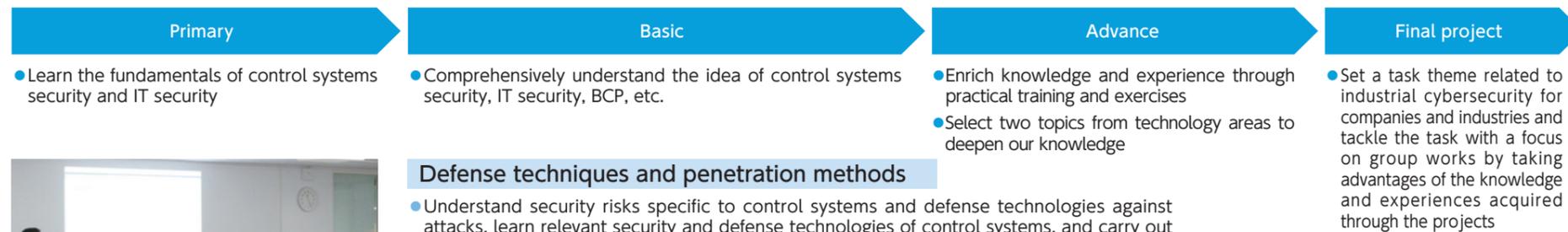
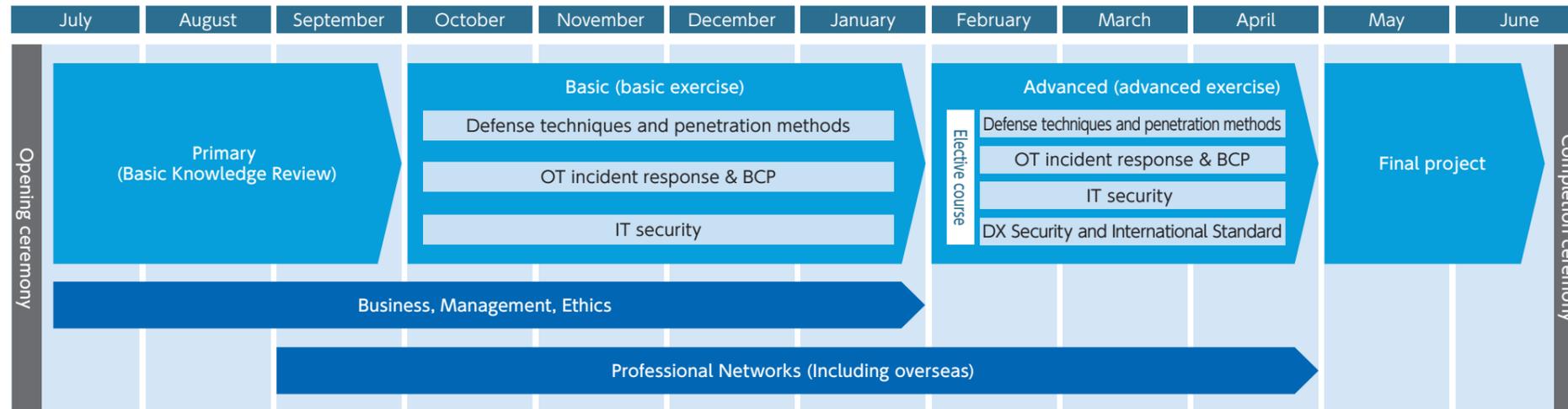


Core Human Resources Development Program

Provide a one-year-full-time program targeting “core human resources” who will connect field personnel and corporate executives in the future

- Develop human resources who have well-balanced abilities to understand the necessity of cybersecurity measures and promote projects enthusiastically with a focus on both control systems (Operational Technology: OT) and information systems (Information Technology: IT)
- Develop human resources who resolutely express his or her opinions regarding cybersecurity measures to the executive officers and steadily get into a tough negotiation, without losing the philosophy of minimizing risks of the entire organization even if the business department calls him or her to account for the burdens on and losses of business due to security measures

Program Calendar



Our classroom training learning security fundamentals



Our simulated plant used for the exercise

Defense techniques and penetration methods

- Understand security risks specific to control systems and defense technologies against attacks, learn relevant security and defense technologies of control systems, and carry out planning of measures using our simulated plants

OT incident response & BCP

- Conduct the exercises for OT incident responses, balancing safety with business continuity, and ones for BCP response to control systems
- Manage the safety and security of plants and control systems, utilize BCM under stressful conditions, and conduct BCM response exercises
※BCM(Business Continuity Management)

IT security

- Learn IT design, IT incident response, and system improvement to achieve the security of control systems
- Understand and experience attack detection methods for control systems, utilize state-of-art technologies, and conduct exercises for incident responses to attacks

DX Security and International Standard

- Undergo training on AI, IIoT^{※1}, commercial Cloud, and DLT^{※2} (blockchain technology)
- Study and utilize the laws and regulations, international standards, and guidelines relevant to the mentioned fields
※1 IIoT(Industrial Internet of Things) ※2 DLT(Distributed Ledger Technology)



Our simulated plant used within the group works



Our progress report session inviting the supervisors from trainees' dispatching companies

Business, Management, Ethics

- Learn "business skills making investment decisions on security" and "management skills influencing field personnel," necessary to plan cybersecurity strategies and explain issues to corporate executives, such as risks of business administration and financial affairs
- Develop abilities to understand cybersecurity-related laws correctly, cultivate high ethical standards, and contribute to both companies and societies

Professional Networks

- Introduce domestic and foreign advanced cases and hold special lectures given by invited experts
- Hold deployment exercises through which physically visit France and the UK and gain experiences



Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region



Overseas deployment exercise (France)



Overseas deployment exercise (UK)

Efforts after completing the Core Human Resource Development Program

The trainees who completed the Core Human Resource Development Program are entitled to:

- Receive a full waiver of a Registered Information Security Specialist Examination under the provisions of the Act on Facilitation of Information Processing
- Use our logo mark (Trademark Registration Number: 6023942)
- Use the following titles:
産業サイバーセキュリティエキスパート (Trademark Registration Number: 6158314)
Industrial Cyber Security Expert (Trademark Registration Number: 6158313)



Alumni Community (Kanae-kai)

- Update knowledge even after completion
- Build personal network beyond the different completing years
- Contribute graduates' knowledge back to societies

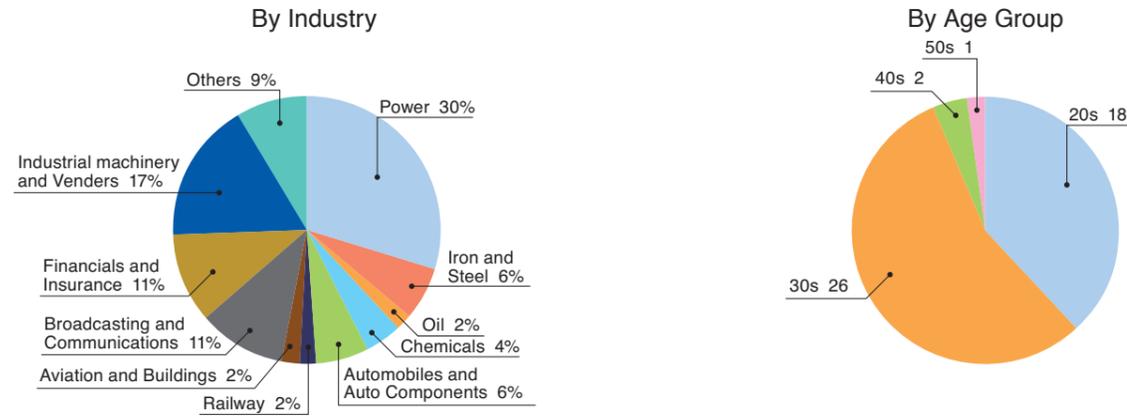


Build collaboration networks on control systems security across various sectors



Achievement of Core Human Resource Development Program

<Composition of the FY2020 (4th- cohort) trainees>



<FY2019 (3rd- cohort) Efforts>

■FY2019 (3rd- cohort) Events

Month	Event	Dates
July	External facility visit (Chiba)	7/12, 7/26, 8/2
	External facility visit (Kanagawa)	7/11, 7/26, 8/2
	External facility visit (Miyagi)	7/12, 7/26, 8/2
September	Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region (Tokyo)	9/9-12
	Overseas deployment exercise (Paris)	9/23-24
October	External facility exercise (Tokyo)	10/18, 11/15, 12/18
	CSS2019 (Nagasaki)	10/21-24
	External facility visit (Miyazaki)	10/28
	CODE BLUE2019 (Tokyo)	10/29-30
December	External facility visit (Kobe)	12/2
	Overseas deployment exercise (London)	12/2-3
	Black Hat Europe 2019 (London)	12/2-5
January	External facility visit (Ibaraki)	1/20
	Hardening 2020 (Okinawa)	1/24-25
March	Kyushu Cyber Security Symposium (Oita)	3/18-19

● For all trainees (participate any one of days) ● Applicants only ● Selected applicants only ● Lecturer-recommended events (applicants only)

■Final Project Efforts (Total 25 Projects)



Project examples

Optimization of Asset Management in Control Systems

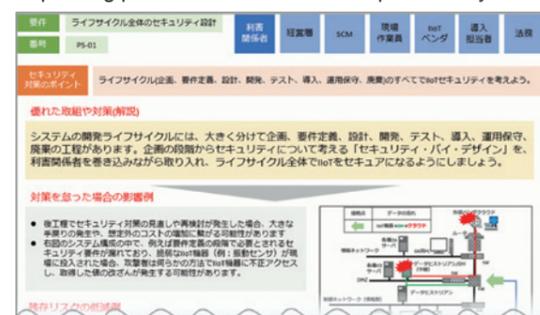
The team developed asset management guidelines, automation tools, and product verification outcomes for control systems.

Security for IIoT Implementation

The team developed a workflow and security measure guideline manual for new system implementation, which focuses on the necessary security measures when implementing IIoT (Industrial Internet of Things) into plants. The manual clearly and concisely explains the security measures mentioned in "Good Practices for Security of Internet of Things in the Context of Smart Manufacturing" published by ENISA. Furthermore, the team added the exemplifications of stakeholders and the possible impacts in the case of failing to implement countermeasures to the manual in order to examine risks concretely and induce to proceed with the security measures.

※1 European Network and Information Security Agency
 ※2 Good Practices for Security of Internet of Things in the context of Smart Manufacturing, <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iiot>
 Japanese Translation by IPA <https://www.ipa.go.jp/files/000073490.pdf>

Explaining professional materials comprehensively



Produced CSIRT Card Games

The team produced three types of card games useful for the initial stage of education at CSIRT.

※ CSIRT (Computer Security Incident Response Team)

Cloud Security Guidelines

Under "Information Security Management Guidelines for the use of Cloud Computing Services" established by the Ministry of Economy, Trade and Industry, the team mapped other guidelines and auditing rules for commercial cloud services and developed a "Guideline Summary Sheet" which standardized those guiding principles. In addition, the team created "Website Deployment Template", which would enable us to automatically build a secure website for each cloud service, and an "Auditing Rules Template" would automatically set the rules following the guidelines using the auditing functions provided by each cloud service. These templates can be used to improve the security level for the cloud environment.

※Information Security Management Guidelines for the use of Cloud Computing Services https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html

How to use guidelines and templates for cloud services



Programs for managers and practitioners

Programs for Managers

Cyber Resilience Enhancement eXercise by industry (CyberREX) ... 2 days

October 23 to 24, 2020 (Tokyo) November 27 to 28, 2020 (Osaka)

This exercise aims to enhance readiness and resilience on cybersecurity within divisions and departments and to strengthen the entire business organization with an awareness of industry characteristics.

This exercise is distinctive by hands-on-activity-based training using scenarios, which assume a virtual company by industry. Also, we will hold intensive lectures where explain cybersecurity regulations and guidelines, which business partners, such as foreign subsidiaries, affiliates, and supply chains, may encounter.

Target segments: "infrastructure-related" segments including power, railway, building, and logistics and "industry-related" segments including automobiles (manufacturing) and factory automation



Cyber Crisis Response Tabletop Exercise (CyberCREST) ... 3 days

January 27 to 29, 2021

In this exercise, participants will learn the advanced cybersecurity strategy established by the United States, called "Collective Defense", in order to protect companies who have been implementing control systems. This strategy is based on the idea of protecting companies against cyber threats while sharing information with governments and competitors in the same field.

Also, the former US cyber command experts, CISOs, and security architecture experts will share their experiences with the participants and introduce how to apply this strategy to companies while conducting some role-playing exercises.



Strategic Management Seminar

Under the wave of business digitalization (digital transformation), companies have an increased need for correctly acknowledging cybersecurity as a management issue.

This seminar targeting the personnel responsible for security measures, including policy planning and risk management, will give them lectures on the organizations and functions essential to security measures in terms of business continuity.



Program for Practitioners

Cybersecurity Exercise for Control Systems ... 2 days

December 15 to 16, 2020

In this exercise, participants will utilize our simulated process control networks and experience the cyber attacks used to maliciously control equipment and the defenses applying countermeasures against those attacks. The contents of this program are practical that the participants will deeply understand the security control systems. The participants will learn the security of industrial control systems, such as the architectures of IT and control systems, security vulnerabilities, and measures specific to control systems.

