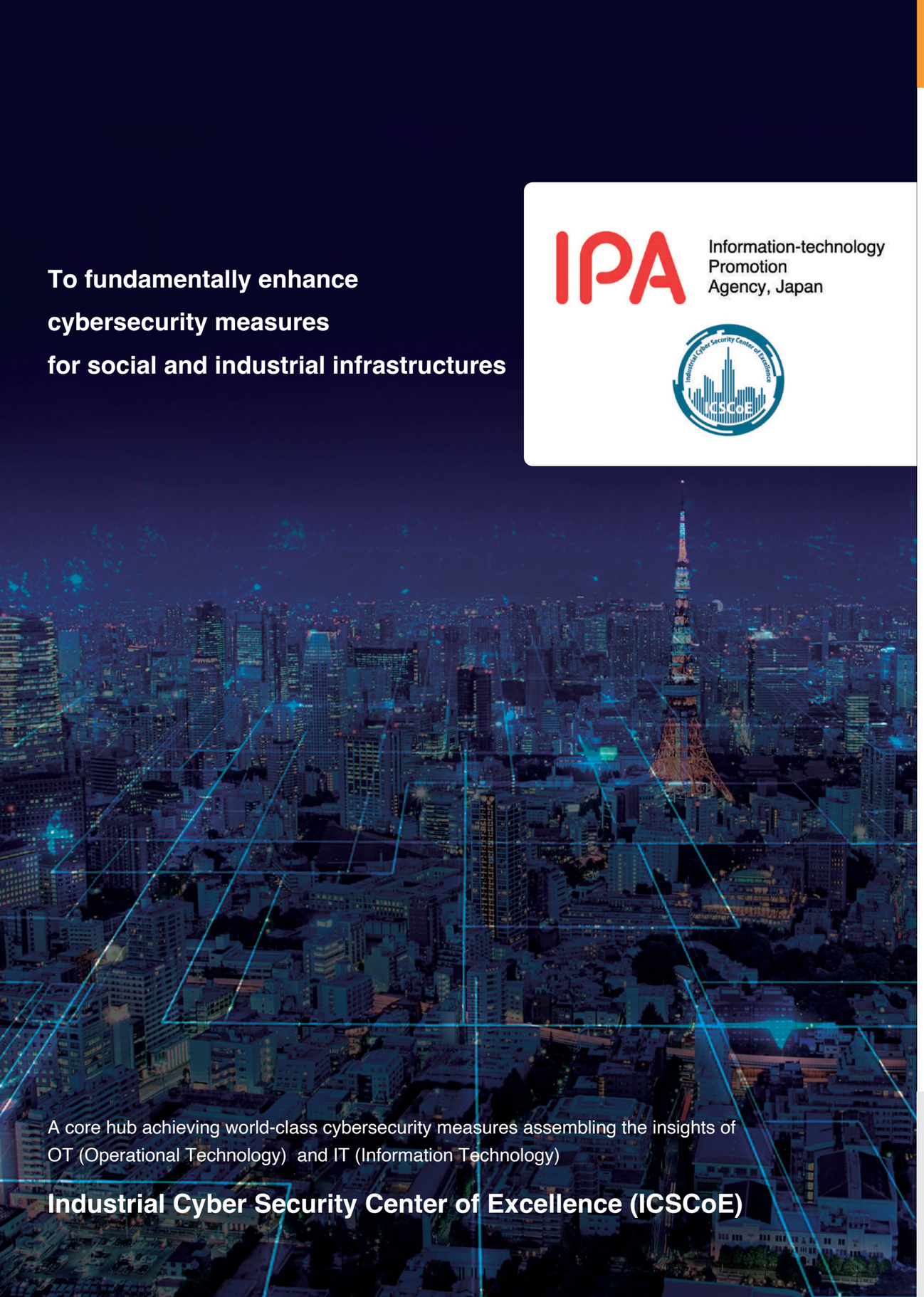
To fundamentally enhance cybersecurity measures for social and industrial infrastructures

IPA Information-technology Promotion Agency, Japan

Industrial Cyber Security Center of Excellence



A core hub achieving world-class cybersecurity measures assembling the insights of OT (Operational Technology) and IT (Information Technology)

Industrial Cyber Security Center of Excellence (ICSCoE)

The largest industrial cybersecurity human resource community in Japan

Kanae-kai

Will Come True 叶会

Purposes

- Update knowledge and skills
- Build networks beyond program years
- Give knowledge and skills back to the societies

Establish collaborative systems for cybersecurity across industries

The aim of “Kanae-kai” is to strengthen cybersecurity measures for whole societies through the active participation of our graduates, who absorbed numerous knowledge and skills from the Core Human Resource Development Program. Thus, we have proceeded with activities performed by the graduate community, “Kanae-kai”, as a support system for them while forming network with the graduates and their enterprises.

Our Activities

Kanae-kai General Assembly

- Annual gathering across program years
- Conduct exercises and seminars
- Present the latest trends and share knowledge and skills
- Provide opportunities for Information gathering and networking

Subcommittees

- The graduates established and have operated the subcommittees based on themes and objectives:
  Know-How Sharing Committee, Regional Activity Committee, etc.
- Develop Activities Independently

Information Sharing Activities

- The ICSCoE provides its graduates with information on cybersecurity, such as vulnerabilities, threats, incidents and their countermeasures, technical and practical knowledge and skills, and trends in cyberspace.
- The ICSCoE uses its unique information -sharing tools to provide above information.

Origin of the name of our graduate community, “Kanae-kai”

- “Kanae（叶）” is derived from one-character calligraphy performed by the chief priest of the Kumano Hongu Taisha Grand Shrine, the world’s cultural heritage, in 2008.
- “Yatagarasu (three-legged crow)”, the protectorate god of Kumano Sanzan (the three Grand Shrines of Kumano), is the god of navigation and guidance. Thus, we named with the hope that God “fulfills” and “conduces” each graduate’s wishes.

IPA Information-technology Promotion Agency, Japan

Bunkyo Green Court Center Office, 17th Floor 2-28-8 Honkomagome Bunkyo-ku, Tokyo, Japan, 113-6591
Tel: 03-5978-7554 Fax: 03-5978-7513 Email: coe-promotion-info@ipa.go.jp

WEB page of the Industrial Cyber Security Center of Excellence

Our public relations magazine “ICSCoE REPORT”

To become an expert in industrial cybersecurity who protects societies and organizations

Core Human Resource Development Program

A one-year full-time program to nurture “Core Human Resource” possessing both OT (Operational Technology) and IT (Information Technology) skills to connect management and field personnel

After completion of our program, our graduates will

- Be granted the title of “Industrial Cyber Security Expert”
- Receive full waiver of Registered Information Security Specialist Examinations

Program Features

Comprehensively learn technologies (OT/IT), business and management fields

Trainees will understand security and business by overviewing entire organizations, supply chains, and whole industries with a broad perspective from field personnel to management.

Practical exercises with simulated real plants

Simulated real plants for various industry systems.
Trainees will experience exercises in similar environments to their enterprises and gain a deeper understanding of risks in the fields.

Network building with relevant domestic and international agencies

Networking with top-level contacts beyond nations and industries.


Group lectures at the Bunkyo location


Learning from our group works


Our training base in Akihabara

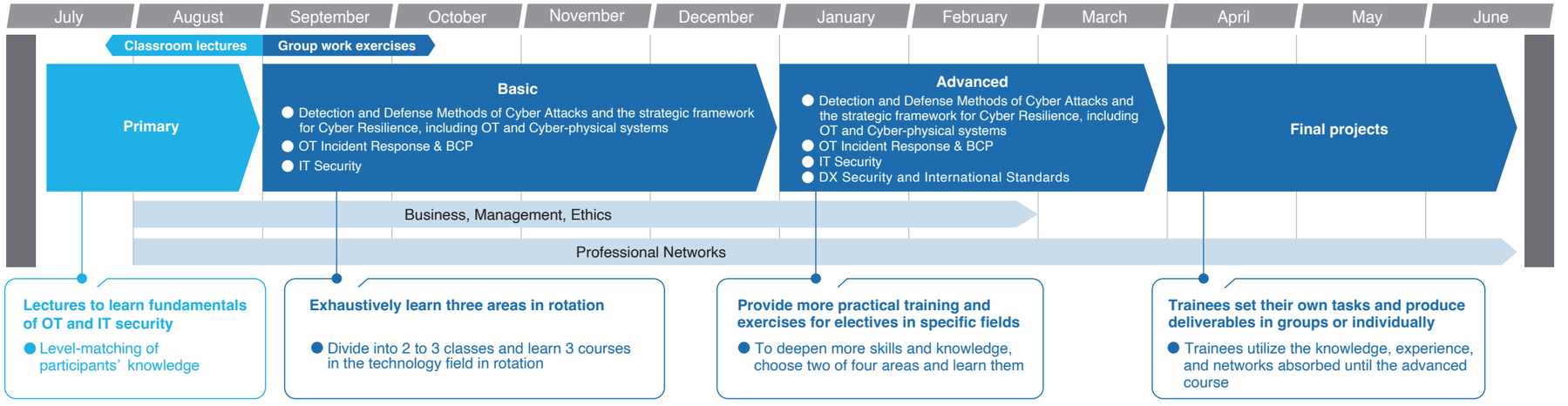

Practical learning in our simulated real plant


Overseas deployment exercise (France)


Observing a scene of the control systems (Kumejima, Japan)

Annual Schedule

From introductory level-matching to high-level and practical exercises and final projects



Fields of Study

Detection and Defense Methods of Cyber Attacks and the strategic framework for Cyber Resilience, including OT and Cyber-physical systems

- Purple team exercise with simulated real plants
- Realistic Security risk assessment including OT and Cyber-physical systems
- Understanding defense technologies of cyber attacks specific to control systems that are different from IT systems
- Penetration testing methods
- Cyber Forensic technologies
- Understanding the strategic framework for Cyber Resilience Plans

OT Incident Response & BCP

- Safety & Security Management of Industrial Control Systems
- OT Incident Response for Safety and Business Continuity Management
- Cyber BCP Exercise under Stress Environment

IT Security

- Incident response for IT and control systems
- Comprehending detection methods for attacks against control systems
- Risk assessment and countermeasures for smart control systems

DX Security and International Standards

- Security issues and countermeasures for AI, IIoT, commercial Cloud, and DLT
- Exercises for utilizing foreign laws and regulations, standards, and guidelines

Business Management and Ethics

- Business skills to motivate management
  −Strategization, management risks, financial risks
- Management skills to motivate on-site personnel
  −Organizational Behaviors and Leadership, Human Resource Management

Professional Networks

- Special lectures and exercises by experts
- Collaborative Training in collaboration with relevant overseas institutions

IPA Better Life with IT

Industrial Cyber Security Center of Excellence

About ICSCoE

Business Overviews

The Industrial Cyber Security Center of Excellence (ICSCoE) gathers human resources, technologies, and know-how and proceeds those as three core business pillars to enhance protections against cyber attacks physically damaging our social and industrial infrastructures.

Human Resource Development

Nurture human resources who can recognize the risks of their enterprise systems and determine necessary security measures

- Foster skills appliable in the fields through practical exercises utilizing our simulated real plants
- Facilitate collaboration with experts and specialist from inside and outside of Japan
- Enlighten enterprise management about the need for cybersecurity measures and personnel utilization

Core Businesses

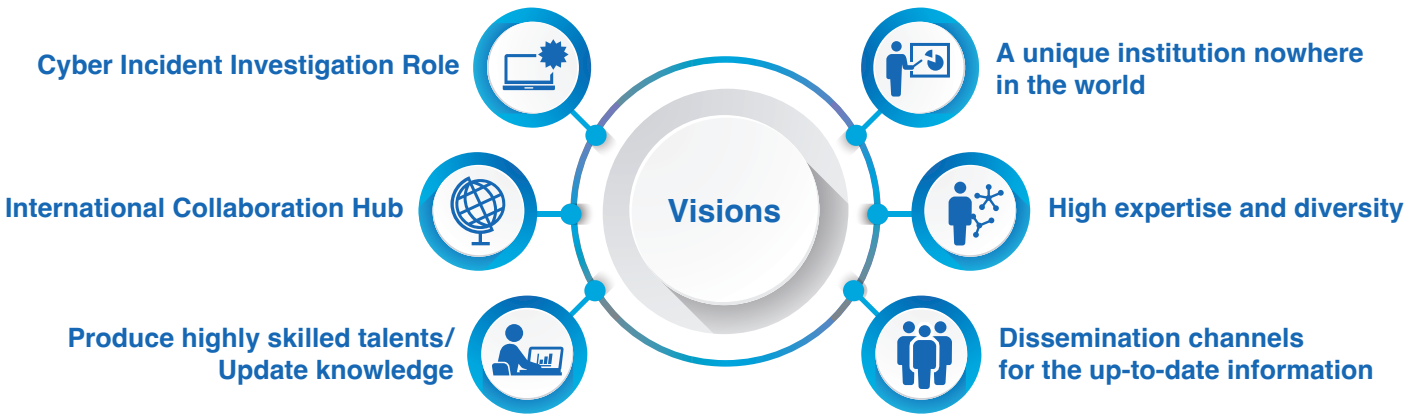
- Core Human Resource Development Program
- Short-term Programs

Validation of safety and reliability of actual control systems

- Assess risks for the safety and reliability of control systems
- Verify possibilities of cyber attacks and formulate necessary measures

Examine and analyze information on cyber attacks

- Collect Information on cyber threats and examine and analyze new attack methods
- Examine and explore advanced cyber techniques while obtaining the cooperation of external white hackers



WEB page of the Industrial Cyber Security Center of Excellence

Our public relations magazine "ICSCoE REPORT"