



The ICSCoE Report is a public relations newsletter on ICSCoE's activities.



Minister for State of Cybersecurity (Then), Mr. TAIRA, Visited ICSCoE's Akihabara Training Facility

The Industrial Cyber Security Center of Excellence, ICSCoE, conducts the Core Human Resource Development Program designed to strengthen cybersecurity measures for social and industrial infrastructures. This program offers practical training using actual control systems employed in industrial environments, aiming to nurture personnel who can immediately contribute to enterprises upon returning to dispatching ones.

In September 2025, Minister for State of Cybersecurity (then, hereafter the same), Mr. TAIRA, visited the Akihabara training facility of the ICSCoE, which was utilized for exercises by the trainees.

Tour of the Simulated Real Plants

During the tour, the instructor of the Core Human Resource Development Program delivered two demonstrations of possible cyber attacks to former Minister TAIRA using the simulated real plants that replicate control systems, such as building management systems and in-vehicle

cle control systems.

The instructor also explained the potential impacts and damages to our society caused by cyber attacks and provided an overview of the ICSCoE's initiatives to cultivate cybersecurity professionals.



Minister TAIRA being briefed on simulated real plants (left)



Receiving an explanation about the in-vehicle control systems

Exchanging views with former Minister TAIRA

During the observation, Minister TAIRA posed insightful questions on various topics, including risks Japan's social infrastructures face, security measures, cyber attack cases, and the Core Human Resource Development Program offered by the ICSCoE, leading to a lively exchange of opinions.



Exchanging views on future
cybersecurity initiatives



JP-US-EU Industrial Control Systems Cybersecurity Week 2025 for the Indo-Pacific Region



Participants from the Indo-Pacific region and organizers

From November 18th to 21st, the JP-US-EU Industrial Control Systems Cybersecurity Week was held in Tokyo, bringing together experts from Japan, the United States, and the EU to share knowledge and experience.

This annual event, launched in 2018, invites participants from across the Indo-Pacific region, including cybersecurity professionals responsible for IT and OT in critical infrastructure operators, experts from national Computer Security Incident Response Teams (CSIRTs), and policy specialists from relevant ministries and authorities. It is organized in collaboration with the U.S. Government (Department of Homeland Security/Cybersecurity and Infrastructure Security Agency [DHS/CISA] and Department of State [DOS]) and the European Commission (Directorate-General for Communications Networks, Content and Technology [DG CONNECT], ENISA, and EEAS).

This year, in order to maximize efforts to strengthen supply chain resilience among Japan, the United States, and the EU, as well as to enhance capacity building in the Indo-Pacific region, the scale of the exercise was significantly expanded—resulting in approximately five times more participants compared to last year when including remote attendees. We conducted industry-specific workshops using virtual scenarios that incorporate industry-specific risks and case studies, as well as hands-on exercises on cyberattacks utilizing AI in the industrial control sector. Additionally, as a new program, the European Union Agency for Cybersecurity (ENISA) hosted workshops.

In addition, as part of a program to share security measures implemented by Japanese critical infrastructure companies, Mr. Daisuke Tatsumi, a graduate of the Core Human Resource Development Program (7th cohort), delivered a seminar titled “Supply Chain Security Management in OT Systems.” This provided participants with a valuable opportunity to gain insights and enhance their capabilities.



Supply Chain Security Management Seminar by ICSCoE Alumni