Innovation Platform Agency, Japan
Beyond Digital

ICSCoE REPORT
Industrial Cyber Security Center of Excellence
8.31.2026
vol. 27

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

9th Core Human Resource Development Program Introducing Activities of Our Final Projects Part1

Cultivating Cybersecurity Talent from an Early Age

Backgrounds and Issues

In recent years, technological innovation, particularly in the field of AI, has accelerated significantly. To maintain a competitive edge, it is essential for companies to continuously adapt to these new technologies. At the same time, cyberattacks are becoming increasingly sophisticated and complex, requiring organizations to balance the adoption of new technologies with strengthening their security posture. However, there is a critical shortage of professionals capable of driving both technology adoption and cyber defense, and securing such talent from the external market remains challenging.

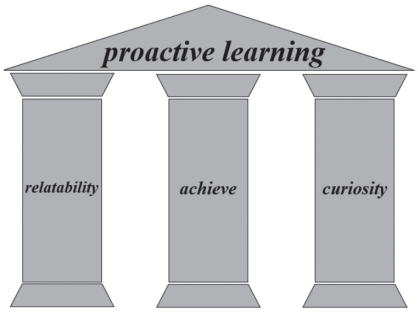
Consequently, internal workforce development has become paramount. Yet, conventional security training often stops at mere knowledge transfer; it frequently fails to help participants internalize cyber risks their own concern and ultimately change their behavior. As a result, preventing human error and deterring insider threats remain ongoing challenges. Furthermore, it is practically impossible to completely prevent incidents rooted in human judgment and behavior relying solely on technical controls. The approach of continuously layering on new technical countermeasures also has clear financial and operational limits.

A common underlying factor across these challenges is that the security literacy required to make appropriate judgments and take correct actions in response to new technologies and threats is not yet deeply rooted within the organization. Therefore, this project explored a new approach by focusing on human awareness and behavior, alongside the ever-evolving landscape of technology and cyber threats.

Issue-Solving and Outcomes

For this project, we set our primary target as high school students, who are growing up at the forefront of our digital society. Having grown up using smartphones and other devices since childhood, they are highly susceptible to cyber threats. We believe that providing early education to this next generation will help raise security standards across society as a whole.

In implementing this educational initiative, our greatest focus was on creating content that encourages "proactive learning" among students. To motivate them to voluntarily study cybersecurity—a field often avoided for being perceived as overly rigid and unapproachable—we incorporated three approaches designed to stimulate "relatability," "a sense of achievement," and "curiosity."



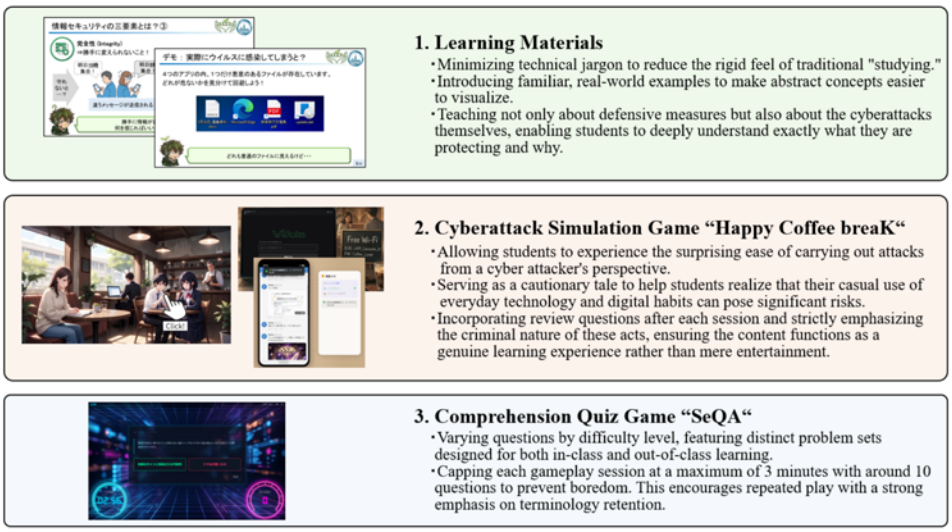
✓ Relatability
- Minimizing technical jargon
- Connecting real-world examples and cyber threats to students' everyday lives.

✓ Achievement
- Integrating quizzes throughout the session to allow students to self-assess their comprehension.
- Recognizing and praising students who complete tasks or answer correctly during class.

✓ Curiosity
- Incorporating more hands-on activities, such as games and quizzes.
- Conveying the intrinsic appeal and fascination of the cybersecurity field.

Three approaches supporting proactive learning

To embodying these approaches, we developed "learning materials" for foundational knowledge, alongside a "cyber attack simulation game" and a "comprehension quiz game" for practical, hands-on learning. Utilizing these tools, we conducted on-site guest lectures at schools. By combining traditional classroom learning with hands-on activities, we aimed to foster a strong sense of personal ownership and awareness among the students.



Created Content

Following the lectures, we conducted an effectiveness analysis using data such as student survey results and game progression data. The results of this analysis serve not merely as the deliverables of this project, but are also shared with the participating schools to aid in their future educational endeavors.

We believe that the learning approaches and empirical data developed through this initiative will not only provide valuable insights for educational institutions but will also be broadly applicable to improving corporate employee training and elevating security literacy at a national level.

Graduate Interview

What is your utmost benefit from this project?

The greatest takeaway from this project was demonstrating how "hands-on" (experiential) learning can maximize educational effectiveness. Typical corporate cybersecurity education relies heavily on e-learning squeezed into the spare moments of a workday; even courses labeled "practical" are often merely extensions of classroom lectures with brief reflection times. However, by incorporating mechanisms that encourage proactive learning through interactive experiences like games, I realized we could draw out genuine interest in a field that often fails to attract learners' interest, thereby promoting deeper and efficient learning. This realization regarding the "impact of active learning" is a valuable insight that can be directly applied to strengthening security and cultivating talent within our own organization, extending far beyond its use in educational institutions.

Methods for utilizing project outcomes

By incorporating these tools into new employee training or on internal educational portals, employees can voluntarily engage with (play) them. These tools serve as a powerful resource to deepen their understanding of cybersecurity. Furthermore, the content is designed so that even family members without specialized knowledge can enjoy learning together. We strongly recommend actively utilizing these materials not only to protect organizations, but also as a form of "security learning to safeguard personal lives" against everyday cyber threats. As this approach takes hold, our hope is that a security mindset will become ingrained in the next generation—not just as a rule, but as everyday common sense and a core part of our culture.

Mr. NARUSHIMA Toshiya (front row center) and project members

This is unique to the ICSCoE!

This past year has been an exceptionally valuable period, allowing me to comprehensively study the vast domain of cybersecurity. I was able to receive direct guidance from frontline specialists in areas where my understanding was not yet fully developed. Additionally, by deepening my learning alongside peers from diverse backgrounds, I gained practical insights truly unique to ICSCoE.

Above all, the most significant achievement of all is the "connection with my colleagues" - a network of peers with whom I can discuss security across professional boundaries. Meeting colleagues who share the common goal of "protecting companies, society, and people's lives," with whom I can cooperate and occasionally engage in friendly competition, has become an irreplaceable asset that I could never have obtained elsewhere.

From Defensive Compliance to Growing Stronger Through Compliance

— Guidelines for Responding to Japan's Cyber Response Capability Enhancement Act —

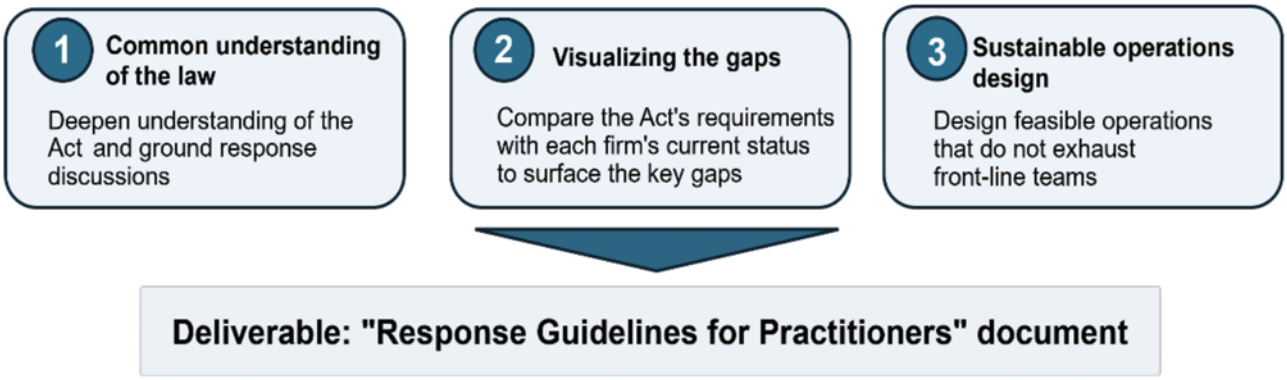
Backgrounds and Issues

Sophisticated cyberattacks, primarily originating from outside Japan, have become a national security risk to critical infrastructure. To address this challenge, the Cyber Response Capability Enhancement Act, officially known as the Act on Prevention of Damage to Critical Computers by Unauthorized Acts, along with related legislation, was enacted and is scheduled to take effect on October 1, 2026. The Act primarily covers essential infrastructure providers (designated social infrastructure providers) that use specific critical information systems among the 15 sectors defined under the Economic Security Promotion Act. Vendors supplying products and services to these providers (suppliers of electronic computing systems and related equipment) are also positioned as key stakeholders under the Act.

However, the providers and vendors subject to the Act faced uncertainty due to the lack of finalized guidelines defining specific compliance requirements. As a result, many organizations found it difficult to determine what actions to take and fell into a "wait-and-see" mode. In addition, operating environments, organizational capacity, and regulatory obligations vary by the industry in which each provider belongs. While the statutory text makes clear what the law requires, it does not clarify what affected providers and vendors should do, by when, and how they should respond. This lack of clarity has been a challenge among all covered providers and vendors. Rather than waiting for additional guidance, this project took a proactive approach by identifying practical and effective actions for providers and vendors.

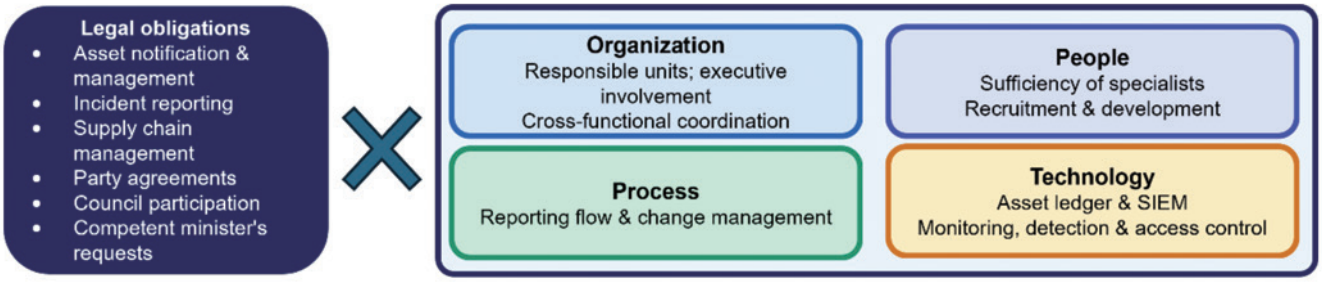
Issue-Solving and Outcomes

Rather than treating compliance as a mere obligation, this project adopted the concept of "strengthening security through legal compliance," positioning responses to the Act not simply as a requirement to fulfill, but as an opportunity to enhance each company's security without exhausting frontline teams. We pursued our project based on three pillars: ❶**building a common understanding of the legal framework**, ❷**visualizing gaps**, and ❸**designing sustainable operations**.

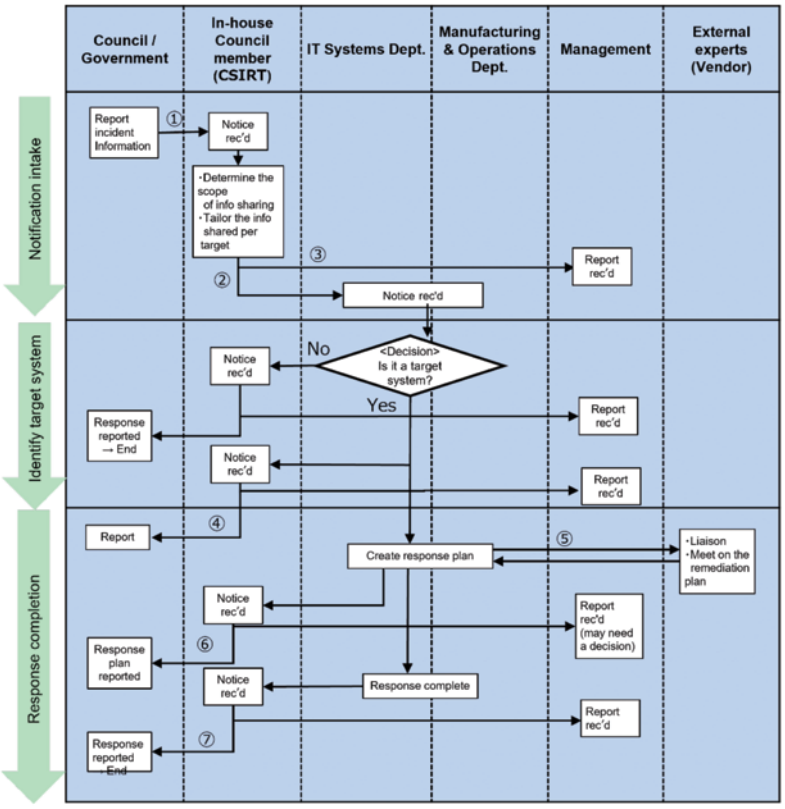


The project's three pillars and the resulting deliverable: a practical guidance document for practitioners

We conducted a cross-industry gap analysis of affected providers and vendors by evaluating each legal obligation across four dimensions — organization, people, process, and technology — and visualized the gaps between the Act's requirements and each company's current state. The analysis revealed that the biggest challenge lies not in a lack of technical capabilities or resources but in the difficulty of translating the Act's requirements into internal procedures and operations, particularly because some requirements have yet to be fully clarified. Conversely, the findings suggest that most companies can achieve compliance not by starting from scratch, but by restructuring their existing governance, processes, and capabilities.



Gap analysis framework: legal obligations mapped against four assessment axes (organization, people, process, and technology)



An example information-sharing workflow via the council established under the Act (example operating workflow)

Our study went beyond desk research by engaging in discussions with overseas CSIRTs and industry associations, interviewing the National Cybersecurity Office (NCO), and gathering feedback from visitors through exhibition at Interop Tokyo. These activities allowed the project to incorporate both domestic and international insights as well as voices from the field.

These findings were consolidated into a practical guidance document for practitioners. The document is designed to help practitioners understand the overall picture of the Act, compare it against their company's current state, and determine what to prioritize now. It provides an overview of the Act and timelines toward its enforcement, summarizes the challenges identified through the gap analysis, highlights key considerations from the vendor perspective, and presents sustainable operating models with representative response workflows. The document concludes with recommendations structured around three key areas: self-help (preparations each provider should undertake independently), mutual assistance (industry-wide knowledge sharing and alignment), and public assistance (early publication of standards and other forms of support sought from the government).

Graduate Interview

What is your utmost benefit from this project?

At the outset, my understanding was still vague — I only recognized that "new obligations would be introduced and we would need to respond." My greatest takeaway from this project was gaining a deeper understanding of what the Act clearly defines and what remains unclear. By identifying the areas that remained unclear, I was able to distinguish between matters that require further clarification and those we can begin preparing for in advance.

Methods for utilizing project outcomes

The document we developed compiles the common challenges identified through a survey of providers regarding compliance with the Act, along with proposed solutions to those challenges. It also includes operating models and example workflows for key obligations. After returning to my company, I plan to use it as a reference for checking whether we face similar challenges and to support the development of our own operational workflows.

This is unique to the ICSCoE!

One thing I found unique to the Industrial Cyber Security Center of Excellence (ICSCoE) at IPA was the environment, where trainees from diverse backgrounds could engage in meaningful discussion on a shared topic. Thanks to introductions from ICSCoE instructors, I had the opportunity to exchange views directly with experts in Europe and the United States, as well as with international communities such as E-ISAC. This gave me perspectives

Mr. Yuma Takahashi (third from the right in the front row)

that could not have been gained from domestic sources alone and was invaluable experience that would have been difficult to gain elsewhere. The breadth of the ICSCoE curriculum, which covers topics from technical expertise to strategic recommendations for executives, was another important factor behind the success of this project. In addition, the opportunity to gain external insights that would not normally have been available to us broadened our perspectives and contributed to the project outcomes. It is this combination of diverse learning opportunities and professional networking that represents the unique value of ICSCoE. I plan to continue leveraging the connections I have built here and apply what I have learned to my future work.

Innovation Platform Agency, Japan
Bunkyo Green Court Center Office,
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591
TEL 03-5978-7554 FAX 03-5978-7513

ICSCoE HP

卒業プロジェクト