The 4th Core Human Resource Development Program

Releasing Our Final Projects on the website

We are releasing the outcomes of our final projects available for general use to raise security awareness on the IPA Website.

◆ Drone Security

The project team developed the "Drone Security Handbook" to safely employ drones been rapidly spreading. This handbook introduces the history of drones, basic functions/ specifications, related laws and regulations, usage cases, accidents/ cyber attacks, and protections. The team also examined cyber attacks against drones (vulnerabilities) and countermeasures and summarized some grasping points to utilize and apply safely to drones on the handbook. The team expects this handbook will be instrumental in recognizing the importance of the Safety and Security of drones.

ドローンセキュリティハンドブック
～安全なドローン利活用の勘どころ～

◆ The Cool Security Action Committee

The project team created a manga-style handbook titled "Everyday ZeroDay", hoping children understand cybersecurity to raise the security awareness of the entire society in the future. This handbook explains technical terms in a comprehensible manga style and would be a good opener for children to develop interests in cybersecurity while enjoying the manga.

▶ Check the link below
https://tapas.io/series/EVERYDAY-ZERODAY/info

◆ Use of Zero Trust Strategy
– Introducing Zero Trust into IT and OT Systems –

The team developed the "Introductory Handbook for Zero Trust", helping enterprises implement Zero Trust. The team built an environment utilizing the functions for Zero Trust and summarized the know-how obtained by verifying the functions implemented into systems.

Zero Trust is generally designed on the assumption of implementing into information systems. Thus, implementing zero trust into control systems is difficult (or no benefits). However, the team verified and reviewed the implementation of zero trust into control systems because they assumed that the connectivity requirements with information systems: IoT devices and cloud computing, would be beneficial to control systems implementing zero trust.

ゼロトラスト導入指南書
～情報系・制御系システムへのゼロトラスト導入～

◆ Security Dojo

Despite the growing importance of security for industrial control systems due to implementing IoT devices and promoting digital transformation (DX), we lack plant-wide security awareness.

In response to this situation, the team created a quiz-format board game used as an introductory security material for newly hired employees assigned to a plant recently. The employees can learn security through it while they enjoy playing the game repeatedly; thus, enterprises can utilize it for new employee training and security education.

セキュリティ道場

◆ 10 Cases of Threats to Safe and Stable Operations

The project team created "10 Cases Threatening Safety and Stable Operations" to be the first step toward considering the security of control systems. It introduces ten actual cases of cyber attacks targeted control systems in Japan and overseas and describes potential damages caused by those attacks. It also provides "Cybersecurity Countermeasures Applied to Operation Sites". Please use it for security education on control systems.
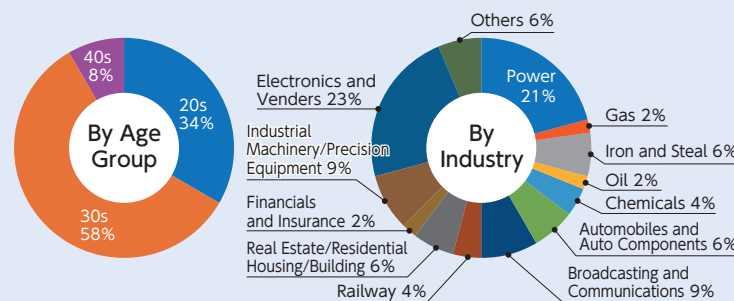
安全・安定操業を脅かした
サイバー攻撃事例
10選

▶ Industrial Cyber Security Center of Excellence Core Human Resource Development Program Final Projects (only in Japanese)

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

---

The 5th Core Human Resource Development Program Began

The Core Human Resource Development Program for the fifth cohort began in July 2021. Forty-eight trainees from various industries have participated in this program, aiming to be a core resource leading Japan's future in the cybersecurity field.

By Age Group
- 40s 8%
- 20s 34%
- 30s 58%

By Industry
- Others 6%
- Power 21%
- Gas 2%
- Iron and Steal 6%
- Oil 2%
- Chemicals 4%
- Automobiles and Auto Components 6%
- Broadcasting and Communications 9%
- Railway 4%
- Real Estate/Residential Housing/Building 6%
- Financials and Insurance 2%
- Industrial Machinery/Precision Equipment 9%
- Electronics and Venders 23%

IPA Better Life with IT

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

1.11.2021

vol. 11

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

Final Projects

46 trainees undertook 15 projects. We will introduce the remaining projects continued from Volume 10.

Develop Evaluation Items and Procedures for ICS Penetration Testing

◆ Backgrounds and Issues

Cyber attacks targeting critical and industrial infrastructures have frequently occurred overseas and caused fatal damages. In Japan, companies utilizing industrial control systems, such as plants, strongly urge to develop in-house penetration testing within the group companies in order to protect their sensitive information. However, Japan currently has no standardized testing methodologies; buyers and suppliers do not know test items to be specified and concrete tests to perform, respectively. Therefore, our challenge is to clarify penetration testing methods for industrial control systems.

◆ Issue-Solving and Outcomes

The project team defined the specific testing procedures and developed a "Test Item List" and "Individual Test Procedures", which enable buyers and suppliers to share common knowledge of their test contents.

Test Item List

Test Items	Details	Procedure IDs	Implemen-tation
Unauthorized command messages	Send an unauthorized command message···	Aa-01	
		Aa-02	○
...	...		

Test Procedures

The list and procedures are linked with ID

Aa-01

1. Test Item List

The team looked into the guidelines and knowledge bases that its members could refer to penetration testing for industrial control systems to develop a "Test Item List". The team referred to the ATT&CK having organized systematic strategies and methodologies of attackers established by the MITRE Corporation, a US Not-for-Profit, and then created a list of test items crucial to penetration testing for industrial control systems.

Since this list describes the purposes of each test item and technical overviews of penetration testing in an easy-to-understand manner, buyers and suppliers can confirm the items both sides must test in setting those test items.

2. Individual Test Procedures

The team devised versatile procedures for performing individual tests not swayed by equipment or environment.

They also detailed some examples of penetration tests (proceedings and results) conducted on the simulated plants at the ICSCoE.

Since both buyers and suppliers refer to the same materials: "Test Item List" and "Individual Test Procedures", they can proceed to "Define/Examine" their test scope while obtaining consensus on that test scope and to "Perform" the tests. Thus, we can expect to realize penetration testing suitable for the actual conditions of systems and businesses.
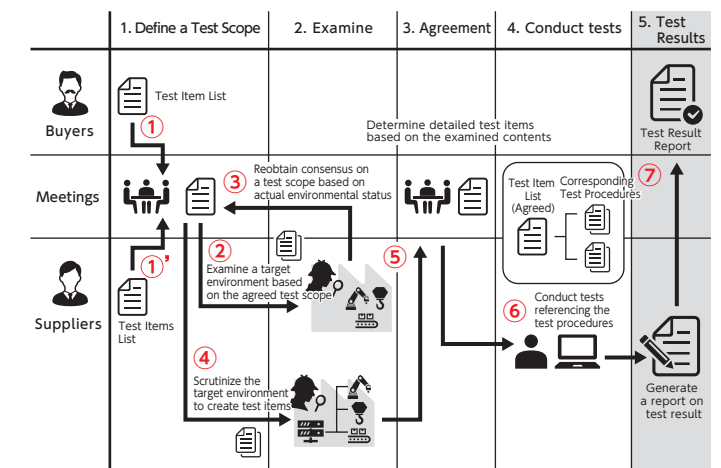
Buyers and suppliers can refer to the List and Procedures for their meetings

---

◆ Interview with Graduates
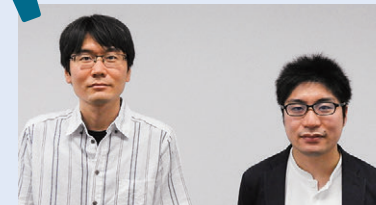
From Left:
Mr. SAKAI Kazuhito (Team Leader)
Tsuken Electric Ind Co., Ltd.
Mr. SAKAI Shogo
Chuden CTI Co.,Ltd.

◆ What is Your Utmost Benefit from the Project?

Mr. SAKAI (K): I had no knowledge of penetration testing, but I could understand and clarify the actions to be taken during penetration tests while operating the simulated plants.

◆ Methods for Utilizing Project Outcomes

Mr. SAKAI (S): I believe that I will be able to apply the skills and ideas, along with the outcomes, absorbed through this project to my company to expand its business operations.

◆ This is Unique to the ICSCoE!

Mr. SAKAI (K): For me, the ICSCoE is a place where we can learn penetration testing from lecturers skilled in this field; thus, we could immediately ask any questions when facing difficulties and proceed with our tasks proactively.

Mr. SAKAI (S): That is the simulated plants. There is nowhere else where you can perform penetration tests without any restraints.

How to Become a Beloved Security Department

◈ Backgrounds and Issues

In order to promote in-house security, it is essential to form cooperation among the security department and field personnel (other departments). In many cases, the operational departments tend to have negative images and opinions toward the security department, such as,

"They use too many jargon, hard to understand."

"I don't understand why we need to implement security measures."

"They always prevent us whatever we try to do something."

Therefore, our challenge is to build interactive communication and share common perceptions among departments in order to propel security measures in cooperation with field personnel. The team launched this project to solve this challenge since the security department needs to become a more reliable and beloved division.

◈ Issue-Solving and Outcomes

First, the team interviewed all ICSCoE trainees regarding their images of the security department in order to clarify the issues to address. Since the trainees had extensive backgrounds transcending corporate and industrial borders, the team could hear a wide range of frank opinions (specific episodes) through the eyes of field personnel.

Second, the team classified the frequently appeared words during the interviews into four levels and developed an indicator called the "SecuLove Model" to measure how much the security department is beloved by field personnel.

Level	Security Department	Why-Why-Analyze per keyword	Measures
Level 4 Love	Easy to ask (consult), high-skilled, flexible, easy to understand, thankful, clever, helpful, supportive, affable, prompt, entirely, broad perspective, consultation, alternatives, excellent	→	• Measure A • Measure B • Measure C
Level 3 Love a bit	practical, take care of, alert detection, incident response, educate, latest technology, protect, information sharing, information dissemination, expertise, incident prevention	→	• Measure A • Measure B • Measure C
Level 2 Dislike a bit	insistent, play by the book, wreck, heading in different directions between the security department and field personnel, a lack of understanding of field conditions, self-protection, individualistic, secrecy, complicated, unattainable policy, inflexible, hard-headed	→	• Measure A • Measure B • Measure C
Level 1 Dislike	incomprehensible, unilateral, imposition, sudden, oppressive, uncaring, condescending, know-it-all, slow, troublesome, unnecessary, no explanation, apathetic	→	• Measure A • Measure B • Measure C

Secu Love Model

The team also analyzed causing factors "why interviewees perceived in such way" per keyword.

Moreover, in parallel with their analysis, they interviewed security experts engaging in operating security organizations and establishing CSIRT and examined some real-world approach cases.

Based on these analytical findings, the team discussed how to project a positive image of the security department and complied their conclusions into a booklet titled "A Path to a Reliable Security Department".

頼られる
セキュリティ部門への
道すじ

START

～もっと頼られるはじめの一歩～

This booklet explains necessary actions to be taken by the security department as "the Eight Articles for Reliable". In this booklet, the team categorizes the Eight Articles" into four levels: from beginner to super-advanced, based on the "SecuLove Model" developed earlier. The team envi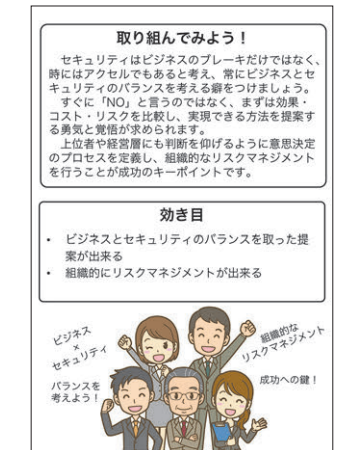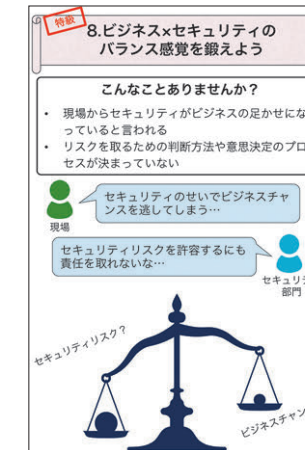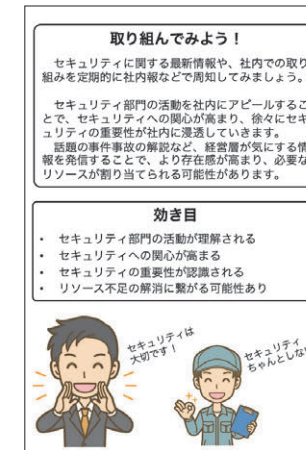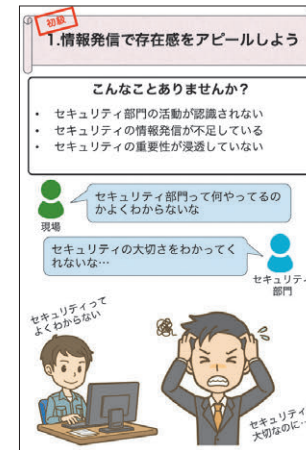sions this "the Eight Articles for Reliable Security" will be a "path" to shorten the distance between the security department and field personnel by undertaking the security measures beginning with the least complex one.

On the pages explaining each content of the Eight Articles, the team first portrays the problems facing the security department revealed through the interviews as a question, "Don't you have these problems?" Second, the team exemplifies "Let's tackle your problems (response procedures)!" that examined in the project and describes

The Eight Articles for Reliable Security

Beginner
Let's get to know each other
1. Let's appeal to your presence by disseminating.
2. Let's explain intelligibly and suavely.
3. Let's get to know field personnel.

Intermediate
Put yourself in the field personnel's shoes
4. Let's put ourselves in the field personnel's position.

Advanced
Let's grow with field personnel
5. Let's get field personnel involved in our activities.
6. Let's optimize rules and policies.
7. Let's build a professional organization.

Super-Advanced
Let's promote our business together
8. Let's train a sense of balance between business and security.

expected effects (efficacy).

The consistent theme throughout this booklet is "to value communication between the security department and field personnel". The team expects that the security department and field personnel will build an easy-to-communicate channel and improve their security systems hand in hand.

For more details, please visit the IPA website, "The Ways to Become a Reliable Security Department".
We will introduce the outcomes of our final projects on the following page.

🎤 Interview with Graduates

From Left
Mr. TERAMOTO Tsubasa (Team Leader)
The Kansai Electric Power Company, Incorporated

Mr. SHIMIZU Keita (Sub-leader)
ANA Systems Co., Ltd.

◈ What is Your Utmost Benefit from the Project?

Mr. TERAMOTO: Before starting this project, I had a vague awareness of the issues regarding the relationship between the security department and field personnel and could not verbalize the actual situation. However, I feel fortunate that we could compile them as a mutual agenda enabling us to share with many people by verbalizing them as a booklet-form through this project.

◈ Methods for Utilizing Project Outcomes

Mr. TERAMOTO: First, I would like to share the contents of this booklet within my company and affirm what my department has been capable of doing incapable of doing. Second, I would like to develop a mutual awareness of the issues within my department and pound out the details of specific approaches to improve our communication channels with other departments.

Mr. SHIMIZU: I believe that the outcomes of this project cover not only security matters but also a major theme, "how to build a desirable relationship with other departments. I am willing to utilize this booklet to promote company-wide initiatives in the future if I have an opportunity.

◈ This is Unique to the ICSCoE!

Mr. TERAMOTO: We tend to consider matter based on the stereotypes and commonsense set by the enterprise or industry we belong to, but it may be hard to realize we are doing so. The remarkable thing about the ICSCoE is that we can hear the diverse opinions of its trainees, lecturers, and experts who have different mindsets from mine.

Mr. SHIMIZU: One of the valued characteristics of the ICSCoE is the diversity of its trainees having various backgrounds: security department, field personnel, IT, and OT. We could build relationships of trust among the trainees and share honest opinions about one common theme by learning together. As a result, we could generate the project efforts reflecting our diversity.