HUMAN RESOURCE DEVELOPMENT TO IMPROVE ORGANIZATIONAL RESILIENCE TO CYBER INCIDENTS

サイバーインシデントに対する組織的レジリエンス向上のための人材開発

YUITAKA OTA

Doctor of Engineering (Dr.-Eng.)
Department of Architecture, Civil Engineering and
Industrial Management Engineering
Nagoya Institute of Technology

January 2022

ABSTRACT

This thesis aims to propose the model for cyber security exercise design proportional to the maturity of the organization. This thesis is composed of seven chapters, each of them dealing with the different aspects of cyber security design and execution.

CHAPTER 1 In this chapter, based on the cyber incidents that have targeted ICS so far, we will explain the reality that cyber-attacks threaten the safety of ICS.

CHAPTER 2 In chapter 2, based on the research background described in Chapter1, I will propose that organizational structure and ICS- BCP required to respond to cyber incidents be developed.

I will also present the elements required for companies to respond to cyber incidents and describe the issues involved in achieving them.

CHAPTER 3 In this chapter, I categorize exercises for experiencing cyber incidents in ICS and explain why I developed two types of exercises.

CHAPTER 4 In this chapter, I will explain the method of human resource development using the exercises described in Chapter 3, and the human resources needed to manage and develop the exercises. It also explains the mechanism for improving the exercises.

CHAPTER 5 This chapter describes the exercises we conducted based on the exercises and exercise implementation methods presented in Chapters 3 and 4. It also shows the new findings obtained by analyzing the exercise results and the feedback from exercise participants.

CHAPTER 6 This chapter will summarize what has been discussed in this paper to solve the problem set in chapter 2..

CHAPTER 7 In the final chapter, I will conclude this study and discuss the remaining works to be studied in the future..

PUBLICATIONS

Some ideas and figures have appeared previously in the following publications:

[1] D. N. Yuitaka Ota Tomomi Aoyama and I. Koshijima. "Cyber incident exercise for safety protection in critical infrastructure". In: *International Journal of Safety and Security Engineering* 8.2 (2018), pp. 246–257. DOI: 10.2495/SAFE-V8-N2-246-257.

[2] A. Tsuchiya, Y. Ota, Y. Takayama, T. Aoyama, T. Hamaguchi, Y. Hashimoto, and I. Koshijima. "Cyber Incident Exercise Admitting Inter-Organization for Critical Infrastructure Companies". In: *13th International Symposium on Process Systems Engineering (PSE 2018)*. Ed. by M. R. Eden, M. G. Ierapetritou, and G. P. Towler. Vol. 44. Computer Aided Chemical Engineering. Elsevier, 2018, pp. 1645–1650. DOI: 10.1016/B978-0-444-64241-7.50269-X.

[3] I. Kato, Y. Ota, and I. Koshijima. "Fundamental Consideration on Lean and Agile Program Management - Reconsideration of Innovation Processes for Nurturing Innovators - (in Japanese)". In: *Journal of International Association of P2M* 13.2 (2019), pp. 60–80. DOI: 10.20702/iappmjour.13.2_60.

[4] Y. Ota, I. Kata, R. Kato, I. Koshijima, and Y. Hashimoto. "Fundamental Consideration on Incident Response Program - Framework for proactive response - (in Japanese)". In: vol. 2019.Spring. 2019, pp. 458–475. DOI: 10.20702/iappmproc.2019.Spring.0_458.

[5] Y. Ota, R. Kato, Y. Hamada, I. Koshijima, and Y. Hashimoto. "Fundamental Consideration on improve organizational incident response (in Japanese)". In: vol. 2019.Autumn. 2019, pp. 482–495. DOI: 10.20702/iappmproc.2019.Autumn.0_482.

[6] H. Asai, T. Aoyama, Y. Ota, Y. Hashimoto, and I. Koshijima. "Design and Operation Framework for Industrial Control System Security Exercise". In: *Security of Cyber-Physical Systems: Vulnerability and Impact*. Ed. by H. Karimipour, P. Srikantha, H. Farag, and J. Wei-Kocsis. Springer International Publishing, 2020, pp. 25–51. ISBN: 978-3-030-45541-5. DOI: 10.1007/978-3-030-45541-5_3.

[7] Y. Ota, T. Aoyama, H. Asai, Y. Hashimoto, and I. Koshijima. "Research on Human Resource Development Exercises for Resilience to Cyber Incidents in Critical Infrastructure". In: vol. 2021.04. 2021.

[8] Y. Ota, E. Mizuno, K. Watarai, T. Aoyama, T. Hamaguchi, Y. Hashimoto, and I. Koshijima. "Development of a Hybrid Exercise for Organizational Cyber Resilience". In: *WIT Transactions on the Built Environment* 206 (2022), pp. 55–65.

ACKNOWLEDGMENTS

I would like to thank Prof. Hashimoto and Prof. Hamaguchi for their support of my work. I am also grateful to the members of my committee for their patience and support in overcoming numerous obstacles I have been facing through my research.

Also, I would like to thank Prof. Watanabe, Prof. Arakawa and Prof. Yamashita for reviewing my thesis and giving me advice.

I would like to thank the students whom collaborated with for their diligence and cooperation. In addition I would like to express my gratitude to the staff of the department for their kind support.

Last but not the least, I would like to thank my family for supporting me spiritually throughout writing this thesis and my life in general.

Finally, I have to mention that this research was partially supported by the Ministry of Education Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No. 16H01837.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1

INTRODUCTION

Chapter 1 is describes how cyber security risk becomes more and more threat to industrial systems and critical infrastructure and its potential impact.

1.1 IMPACT OF CYBER RISKS ON INDUSTRIAL SYSTEMS

According to the "Guide to Industrial Control Systems (ICS) Security [1]" published by NIST (National Institute of Standards and Technology), ICS is a control system that includes SCADA (Supervisory Control and Data Acquisition system), DCS (Distributed Control Systems), and PLC (other control system configurations such as skid-mounted Programmable Logic Controllers). ICS are used in various fields, from regular air conditioners and elevators to critical infrastructures (electricity, water, gas, transportation, etc.) that support our daily lives. The control systems [2] that support large-scale control objects such as plants operate in consideration of natural disasters (earthquakes, typhoons, etc.), equipment failure, operator error, human error, etc., even though they are controlling something that is not even safe.

It has been said that these control systems are resistant to cyber risks. This is because control systems have traditionally been designed and operated on the premise that they are not connected to the Internet or internal information technology (IT) systems but are operated as independent systems in isolated networks. The control system is not a general-purpose OS (e.g., windows), and each plant has its hardware, software, and protocols. For this reason, it has been said that control systems are safe from cyber-attacks.

However, in recent ICS, COTS (Commercial Off The Shelf, such as Windows OS, Intel PC, and open source applications) [3] devices have been adopted to reduce the budget for OT system implementation.

There are also DX (Digital Transformation) efforts to shift from physical to virtual operations by using IoT (Internet of Things), AI (Artificial Intelligence), and cloud computing together with virtualization. Due to these trends, OT systems, which have been resistant to cyber-attacks, are at an increased risk of being cyber-attacked.

It has been thought that a cyber-attack on ICS was a theory and could not happen. However, due to the above reasons, cyber-attacks have become a real threat to the safety of ICS as the environment has changed from one that was said to be resistant to cyber-attacks to one that may be subject to cyber-attacks.

After discovering a worm called Stuxnet in July 2010 [4], companies using ICS began to recognize cyber attacks as a threat to the safety of their plants. Stuxnet is a virus that targeted uranium enrichment centrifuges in Iran's nuclear fuel facilities. What made this Stuxnet one of the first cyber-attacks to be identified as a risk was that it successfully attacked a control device that was not connected to the Internet. Many research institutes have studied Stuxnet, and there have been many investigations into how it was transmitted. Once Stuxnet had infected a PC, it hijacked it and used the vulnerability of that PC to expand the attack to the next target. It found the final target, a Siemens PLC, and succeeded in destroying the centrifuge by hijacking the control equipment and sending an unusual control program. With the control equipment hijacked, the operators' HMI (Human Machine Interface) made it appear as if everything was normal. They were operating under cover of an attack. This Stuxnet made a strong impression that even OT systems, which are not connected to the Internet and have been said to be resistant to cyber-attacks, are capable of cyber-attacks and threaten plant safety.

In 2015 and 2016 [5], a cyber-attack on electricity facilities in Ukraine caused power outages and affected the Ukrainian people. Ransomware called WannaCry was introduced in 2017. This ransomware is a virus that uses a vulnerability in Windows to encrypt data on infected computers, demands a ransom to unencrypt the data, and spreads from the infected PC through the network. Before WannaCry hit the scene, Microsoft had issued a warning and update for this vulnerability. In other words, this is ransomware that could have been prevented if only the

vulnerability used had been fixed. At Hitachi, Ltd.[6], the ransomware infected the inspection equipment in which Window was embedded and spread to all the equipment that had not been protected against the vulnerability in just over three hours. A PC used at Honda Corporation's Sayama plant was infected with WannaCry but did not develop the disease. The company decided to shut down its operations to quarantine the virus and prevent recurrence from preventing the infection spreading, resulting in the production of about 1,000 cars being halted.

Most recently, in May 2021, the Colonial Pipeline, an oil pipeline company in the U.S., lost its fuel supply for about a week due to a hacker attack that shut down its IT system, which is the production system, not the ICS [7]. This company supplied as much as 45% of the East Coast's fuel and was a cyber incident case affecting multiple states and citizens.□

Since Stuxnet, the number of reported cases of cyber-attacks targeting ICS has been increasing year by year, and cyber-attacks targeting ICS have become a serious threat not only to the business of companies but also to our daily lives [8].

1.2 CYBER-ATTACKS TARGETING INDUSTRIAL CONTROL SYSTEM

Fig. 1.1 shows a cybersecurity testbed and a virtual ICS network. The testbed heats water with a heater in the lower tank and circulates the heated water through a simple pipeline to the upper tank (using a pump). The testbed is also equipped with actual industrial control devices and automatically controls [9]. In this ICS network, OLE for Process Control (OPC) Servers collect and exchange process data and monitor them by using Supervisory Control And Data Acquisition (SCADA) function included in the OPC Servers. OPC Servers receive various parameters from the testbed's sensor, and SCADA gives instructions to the control equipment using the parameters' data.

1) Attack Step 1: Reconnoitering and enumeration The attacker executes the Armitage to launch the Metasploit framework [10]. Then, the attacker executes the Nmap, which scans a target network (ICS-2

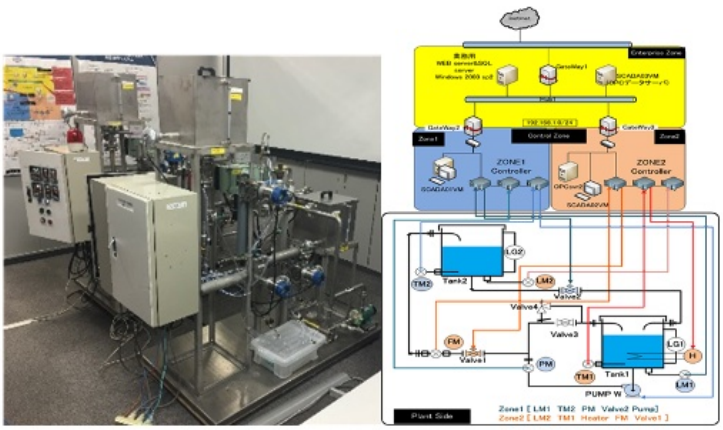

Figure 1.1: Cyber Security Testbed and ICS Network

Network 192.168.12.0/24). After completing the scan, the attacker gets target information.

2) Attack Step 2: Intrusion and advanced attacks According to the functions of the Armitage, the attacker ascertains an attack method and vulnerability in the Metasploit framework. The attacker exploits payloads, which execute inappropriate code in the use of the vulnerability. After sending the payloads, the attacker obtains the administrator's permission for the OPC2 illegally.

3) Attack Step 3: Malware insertion The attacker uploads a malware execution file to an OPC2 background process to execute a malware file. The configuration file of OPC2 was rewritten, and then the OPC2 was restarted. It resulted from the attack, the valve controlled by the OPC2 shutdown.

4) Attack Step 4: Clean-up The attacker deletes the malware file and the configuration file from OPC2 storage to avoid leaving the cyber-attack evidence and finish the cyber-attack. As the valve is opened, the stage of the testbed changes. Usually, the testbed's state transition appears on the monitor of the operator (Fig. 1.2). The changing graph shows the liquid level of the upper tank. The liquid level is changing due to the malfunction of the valve. The operator can notice the testbed abnormality due to the unusual process deviations from the steady-state condition through the monitor. However, the attacker conceals the cyber-attack information not to let anyone notice the cyber-attack.

Figure 1.2: HMI Screen Shot in Operation(Safety Incident)

The testbed monitoring screen is hidden, as shown in Fig. 1.3, while the cyber-attack causes severe accidents at the testbed.

This demonstration shows a possibility of safety incidents caused by cyber-attacks to ICS.

Figure 1.3: HMI Screen Shot in Operation (concealed by the attacker)

1.3 INITIATIVES IN JAPAN

In Japan, the Cabinet Secretariat announced the "Special Action Plan for Cyber Terrorism of Critical Infrastructures" in 2000, and started to look into countermeasures against cyber attacks on critical infrastructures. The "Critical Infrastructure Specialist Committee" was established under the "Information Security Policy Council" of the Cabinet Secretariat, and started to look into the defense of critical infrastructures, and required to formulate and implement sector-specific security guidelines in the targeted areas. In addition to the approach from such guidelines, the following approaches are also taken to enhance individuals' skills against cyber attacks.

1.3.1 *SIP (Cross-ministerial Strategic Innovation Promotion Program)*

SIP was established in the Comprehensive Strategy for Science and Technology Innovation and the Japan Supreme Strategy in order for the Council for Science and Technology Policy to exercise its command function and realize science and technology innovation. As the Tokyo Olympics and Paralympics be held in 2021, the threat of cyber-attacks is a serious issue for Japan, and the research title was "Ensuring Cyber

Security in Critical Infrastructures" to conduct research and development to protect critical infrastructures[11]. This research included not only the development of tools, which is one of the defensive measures against cyber attacks, but also focused on the development of security human resources, focusing on those who would respond in the event of a cyber-attack.

1.3.2 *NISC*

With the rapid development and spread of IT, IT has penetrated into every part of the society and has become an indispensable part of the social infrastructure. On the other hand, the Cyber Security Basic Law was enacted in November 2014 under the situation that any failure in IT could have a great impact on the people's lives and economic activities. In accordance with the law, National center of Incident readiness and Strategy For Cybersecurity (NISC)[12] established in the Cabinet Secretariat in January 2015 has taken the lead in conducting this exercise. This exercise has been conducted since 2006, and since the Third Action Plan in FY 2014, it has been conducted for critical infrastructure providers to verify the effectiveness of the failure response system, including information sharing, with a focus on matters related to response to IT failures.

1.3.3 *ICSCoE*

Under these circumstances, the IPA Industrial Cyber Security Center of Excellence (ICSCoE) was established on April 1, 2017, to fundamentally strengthen the defense against cyber attacks on critical infrastructure and industrial bases that support society. (ICSCoE: Industrial Cyber Security Center of Excellence) was established on April 1, 2017. Among its various projects, it has been implementing the "Core Human Resources Program" targeting human resources (core human resources) who connect the management of companies and other organizations with front-line personnel from the perspective of security[13].

2

RESPONSE TO CYBER-INCIDENT

Chapter 2 describes the efforts the real-world companies are making to protect themselves from cyber-risks and discusses the step that can be taken to secure ICS and minimize the impact of cyber-risks on a company's business.

2.1 APPROACHES TO CORPORATE CYBER-ATTACKS

As mentioned in Chapter 1, cyber-attacks must be recognized as a risk that threatens the security of ICS and the business of the company. Of course, many companies have taken measures to deal with cyber-attacks.

Many companies are taking measures to create an environment that is not susceptible to cyber-attacks, such as introducing mail checker to prevent cyber-attacks called targeted attacks, training new employees, employees on information system security regularly, and introducing VPN (Virtual Private Network) to ensure the secure communications as more and more employees work from home due to the COVID-19. However, I believe that it is impossible to prevent all cyber-attacks, no matter what measures are taken. Because attackers can be anywhere in the world, and new vulnerabilities in not only IT system and also OT system are reported almost every day, as well as vulnerabilities in Control Devices (like PLC). These reported vulnerabilities do not include all the vulnerabilities that have been discovered. They are only disclosures of vulnerabilities in products handled by the company, or information is found and reported by people with good intentions. If the person who found the vulnerability had a malicious purpose, they would not say it, and these vulnerabilities are used for cyber-attacks. In other words, it is impossible to find all the vulnerabilities, and it is impossible to eliminate all the vulnerabilities. This doesn't mean that

companies are immune to cyber-attacks because they have addressed all the vulnerabilities that have been disclosed.

Even if it were possible to eliminate all vulnerabilities, there would always be vulnerabilities associated with the people who use the system. Whether human errors such as unauthorized downloading of apps that should not be installed, or unauthorized connection to a wireless LAN that should not be connected, occur depending on the person using the system. Even if we could manage the employees and install the perfect tools and systems, there is still a possibility that something will go wrong with the business.

We believe it is impossible to prevent all attacks for the above reason. However, this doesn't mean that companies' measures to deal with cyber-attacks so far are useless. Some cyber-attacks, such as WannaCry, can be prevented by applying patches to publicly available vulnerabilities. Hence, it is necessary to deal with the cyber risk by segregating the risks that can be prevented by the companies' measures so far and the cyber risk cannot be prevented.

2.2 RESPONSE TO CYBER INCIDENT

It is necessary to understand the impact and visible effects of cyber-attacks on plants to respond to cyber-attacks. Cyber-attacks on IT systems, such as personal information leakage and credit card information exploitation, are carried out in the invisible Internet space, making it difficult to grasp the impact of cyber-attacks. Cyber-attacks against ICS are also conducted via the Internet, just like cyber-attacks against IT systems. However, unlike cyber-attacks on IT systems, the impact of a cyber-attack on an ICS is easier to understand. Because, unlike cyber-attacks on IT systems, the effect of a cyber-attack on an ICS is easier to understand because the goal of a cyber-attack on an ICS is to damage the company by shutting down the plant and not being able to produce the required quality of products. Of course, whether the attacker's goal is to target IT systems or ICS, a cyber-attack is just a means to achieve the attacker's intent.

We are focusing on cyber-attacks targeting ICS; the consequences of a cyber-attack depend on the characteristics of the plant. For example, an attacker hijacks a data server (DCS, OLE for Process Control server, etc.) that gives parameters and commands to control devices such as a PLC (Programmable Logic Controller) and gives the control devices malicious instructions. Such an attack can lead to abnormal operation and an incident, similar to a data server or control equipment failure or operator error with traditional equipment.

That is, incidents caused by cyber-attacks in ICS systems are incidents that have already been considered in HAZOP scenarios with Engineering phase. Operating companies have taken countermeasures to ensure the safety of the plant for many years. Companies are preparing countermeasures to ensure safety (Safety Response) under an incident at their plant. Human resource development is also carried out based on the countermeasures to respond when an incident occurs. In other words, even if an abnormality occurs due to a cyber-attack, it is possible to ensure the safety of the plant if the operation staff takes a proper Safety Response. However, problems peculiar to cyber-attacks, such as rewriting server configuration files and rewriting control device programs, may hinder the implemented safety-based Safety Response.

In the case of the cyber-attack described in Section 1.2, the plant abnormality that would normally appear on the HMI that operator is checking in hidden, and the plant abnormality cannot be noticed and safety response cannot be performed, which is a situation unique to cyber-attacks. Figure 2.1 shows the response the structure proposed by the author for cyber-incidents [14].□If the plant is operating abnormally caused by the cause considered so far, it is possible to restore plant safety by performing a safety response, as shown on the left side of the Figure 2.1. However, there is a possibility that cyber-attacks will interfere with safety response (e.g., concealment of a plant's information on the monitor). Companies must consider where cyber-attacks interfere with safety response. Moreover, it is necessary to take the responsibility to eliminate the effect of cyber-attacks (security response) to take safety response as shown on the right side of figure 2.1.

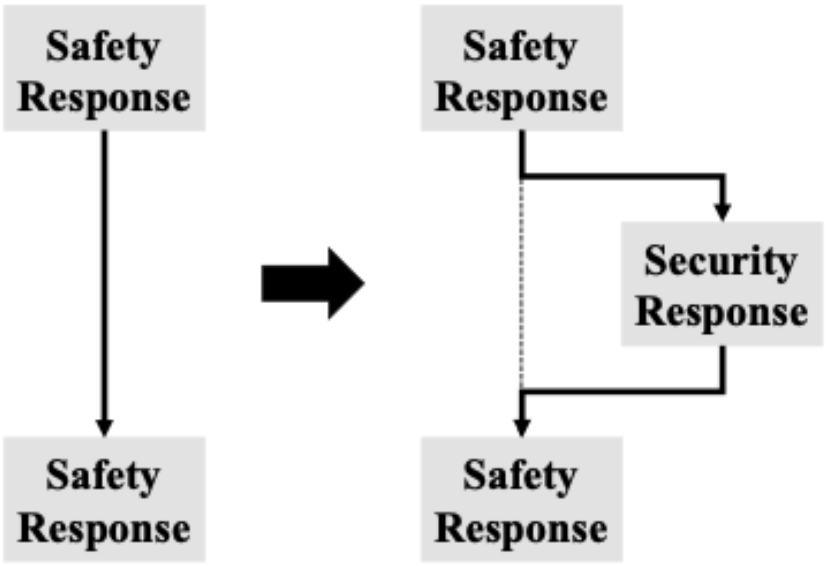

Figure 2.1: Cyber Incident Response Structure

Therefore, if a cyber-attack causes a plant's abnormal operation, a response to rectify the situation is required in combination with a structure to add a security response to the safety response.

Therefore, if a cyber-attack causes abnormal operations, a response to rectify the situation is required in combination with a structure to add a security response to the safety response. The requirements for such a process are as follows:

- A cyber-attack manifests itself in an ICS as an abnormal operation. Therefore, the safety of the plant must be immediately secured.
- The possibility of a cyber-attack must be verified to implement a security response. Therefore, measures must be taken to investigate the cause of the abnormal operation.
- The safety response and the security response must be made simultaneously.

A process that satisfies these requirements appears in Table 2.1 and involves six steps to cope with a cyber-attack. The six basic steps come from the cyber response for IT systems [15]. The authors developed an ICS process that ensures the ICS controls the attacked plant's safety by building on these steps.

Table 2.1: The process to Simultaneously Achieve Safety and Security in ICSs.

Step	Security Response	Safety Response
Detection of Events	Detection of activity on network different from usual	Detection of plant behavior different from normal operation
Preliminary Analysis and Identification	Determine whether to treat it as cyber incident	Determine whether to treat it as normal abnormality or equipment failure
Preliminary Response Action	Data collection for initial movement for defense, prevention of damage expansion and further cause analysis	Data collection for initial response for ensuring safety, propagation prevention of insecure state and further cause analysis
Incident Analysis	Understand technical details, rot cause and the potential impact of cyber incident	Understand technical details, root cause and the potential impact of plant unsafe conditions
Response and Recovery	Recover the current situation of the affected par (soft, hard), prevent further damage, restore normal operation and prevent recurrence	Restore the current state of the affected equipment, prevent further damage and return to normal operation
Post-Incident Analysis	Confirm the effectiveness and efficiency of incident handling	Confirm effectiveness and efficiency of safety response

In other words, by understanding the impact of cyber-attacks on the plant, it is necessary to consider what part of the Safety Response that has been studied and trained should be updated.

2.2.1 *ICS-BCP*

Companies formulate a Business Continuity Plan (BCP) in advance to continue their business in an emergency. BCP is a plan that sets out the activities to be carried out during normal times, as well as the methods and means for business continuity during emergencies, to enable the continuation or early recovery of core business operations while

minimizing damage to business assets in the event of an emergency such as a natural disaster or terrorist attack. It is a plan that sets out the activities to be carried out during normal times and the methods and means for business continuity in an emergency.

Guidelines are often used as a reference as a general method of preparing BCPs. In addition, some companies formulate their BCPs by referring to the guidelines of industry associations or advice from constituents, experts, etc., rather than the guidelines issued by the government. Many BCP guidelines recommend that the assumed risk at the start of BCP formulation should be natural disasters, especially earthquakes, due to the geographical environment of Japan, where natural disasters such as earthquakes and typhoons are frequent.

BCPs for natural disasters such as earthquakes can be formulated according to the guidelines. By experiencing a natural disaster, it is possible to identify areas for improvement in the BCP and take countermeasures to make it even better.

However, it is difficult to formulate a business continuity plan for unknown threats such as cyber-attacks because, unlike natural disasters, companies have not experienced how they will affect them. It is essential to create a BCP that recognizes cyber-attacks as a risk in advance so that people can act quickly to minimize the impact on business continuity in the event of a cyber-incident. However, even if we develop a plan for cyber incidents, they can occur in ways that are beyond our imagination. In addition, it is nearly impossible to create a plan that includes all cyber risks.

2.2.2 *Organization Structure Required for Incident Response*

In Japanese companies, when an incident happens at a plant, departments and divisions related to where the abnormality is caused have investigated the cause and responded.

Whatever the cause, if the plant operation goes haywire, the operators working at the plant will take care of it.□While it is essential to keep the plant running, safety is the most critical priority. However, in the case of a cyber-attack (cyber incident), there is a possibility that

damage other than the part where the abnormality is happening (infecting other equipment, etc.). In other words, various departments and divisions need to deal with cyber incidents. And if these departments and divisions deal with cyber incidents in their own hands, the proper response would be delayed, and the damage caused by cyber incidents could be expanded. To respond proper response, it is necessary for companies to prepare an organizational structure according to the purpose to be achieved beforehand and to dynamically change the organizational structure in accordance with the trend of the situation (change in purpose).

The authors visualized the state in which the work volume changes over time. As described above, when an abnormality occurs in a plant, the work volume of actions to ensure the plant's safety to prevent accidents is large.

Then, once the initial response has ensured the plant's safety, the cause of the abnormal plant operation will be investigated. This time, the work volume of Security is shown as it increases because it considers the response to cyber incidents.

Whatever the cause of the anomaly in the plant, a decision needs to be made that will affect the company's business, such as whether to keep the plant running or shut down the plan until the cause is identified and eliminated. Therefore, after the incident situation is resolved, the workload of the business increases.

These work volume transitions will have different corresponding organizations depending on the purpose of the action. Therefore, I have developed an organizational structure necessary for the transition of work volume, as shown in Figure.2.2.

(a) Operation Staff

The purpose of this organization is to operate the plant normally and provide the company's services. The operation Staff is familiar with the plant's normal operation to detect the plant's behavior differently from normal operation.

(b) ICS-ERT (Emergency Response Team)

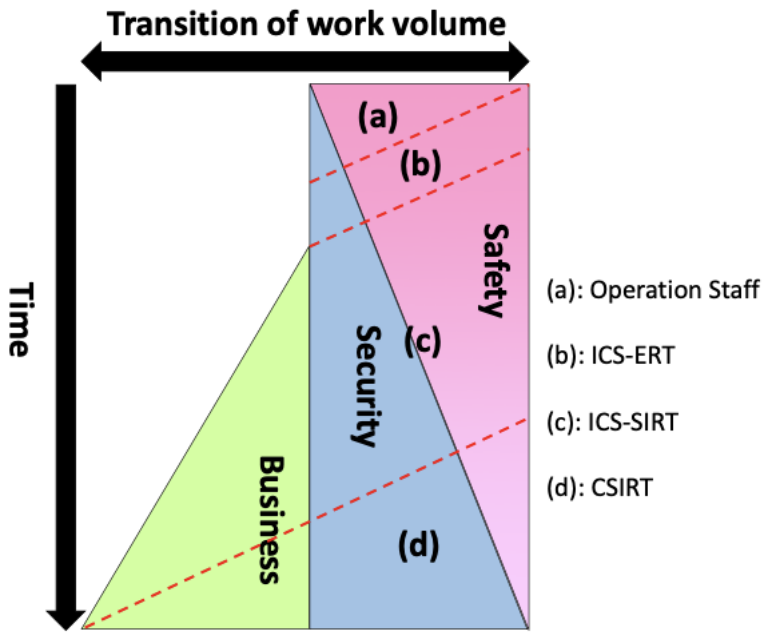

Figure 2.2: Organization Image for Cyber Incident Response

The purpose of this organization is to ensure the plant is safe, whatever the cause is. Instead of focusing on the grounds of plant malfunction, ICS-ERT will focus on the state of the plant and take responsibility. Moreover, ICS-ERT manages the Operation Staff (including the IT Staff in the field) and ensures the plant's safety.

(c) ICS-SIRT (Security Incident Response Team)

The purpose of this organization is to respond to incidents and return to the state of normal plant for continuity Company's business. In the case of a plant abnormality caused by a cyber incident, it is necessary to respond to IT to ensure the safety of ICS, not only for ICS.

(d) CSIRT (Computer Security Incident Response Team)

The purpose of this organization is to respond to parts (IT system) other than the ICS-SIRT service (ICS system) and return it to the state of an ordinary enterprise IT system

2.2.3 *Resilience*

As mentioned above, responding to a cyber incident requires a response plan that considers the impact of the cyber-attack in advance and establishes an organization accordingly. Ideally, the plan should identify all the cyber risks to the company and include actions to address all of them. However, there are as many cyber-attacks as attackers, and they can fatten our expectations. This means that the plans we have prepared may not be directly applicable to incident response. However, the company must respond even to incidents that we have never experienced or expected before to protect the company. I believe that resilience, or the ability to respond to situations never experienced, is essential.

Resilience (or resiliency) [16] is defined as the ability of a system to adjust its functions and maintain required essential behavior in the face of risks that threaten the system's actual conduct, whether expected or unexpected, before, during, or after a change or disturbance. Resilience is often described and explained as elasticity, resilience, excellent recovery, and so on.

According to Dr. Kitamura, one of the primary reasons the concept of resilience has started to spread is that we witnessed the enormous damage caused by the Great East Japan Earthquake in 2011 and the resulting accident at TEPCO's Fukushima nuclear power plant. Japan is prone to natural disasters such as typhoons and earthquakes and has been dealing with them for many years, preparing to minimize the damage and recover quickly even if such risks occur. The Fukushima nuclear power plant is no different, as it deals with nuclear power, a hazardous and unstable substance, and safety has been discussed and addressed continuously.

However, these are discussions of risks within the scope of our assumptions, and when events beyond the scope of our beliefs occur, our response is delayed, and the damage spreads. Although we can do what we are supposed to do, we are often unable to make decisions on the spur of the moment when we go beyond the scope of what we have

learned or been taught. Through such experiences, the importance of resilience has been advocated.

2.2.3.1 *Safety-I & Safety-II*

When discussing safety, the concept of safety-I and safety-II is often used. Safety-I has traditionally been defined as" the state in which nothing can go wrong" when describing safety. More strictly speaking, since it is impossible to guarantee that nothing will go wrong, it has been posited that such a situation is safe when the number of things going wrong is acceptably small. In other words, it eliminates all elements that might cause bad things to happen, and that state is defined as a safe state.

Rather than forcing the continued use of the Safety-I concept, Safety-II focuses on developing the ability to succeed in ever-changing situations by changing the definition of safety from" avoiding something going wrong" to "ensuring that everything goes right. This idea leads to the concept shown in Figure 2.4, where safety management aims to provide as many things as possible to go in the right direction. Daily operations achieve their objectives rather than eliminate causal factors to avoid unacceptable results like in Safety-I. Instead, the goal of safety management is to ensure that as many things as possible are going in the right direction and that every day's work achieves its objectives. To ensure that the required level of performance is maintained at the highest possible level under changing conditions, safety is ensured by anticipating possible events.

In plants where control systems are used, risks that threaten the plant's safety have been discussed and implemented. However, cyber-attacks are not included in this risk. There are as many ways of cyber-attacks as there are attackers, and there is no way to prevent all cyber-attacks. Cyber-attacks may cause events outside the scope of what has been expected. Therefore, resiliency is needed to cope with unforeseen circumstances such as cyber-attacks.

2.3 RESPONSE REQUIRED BY COMPANY

As mentioned above, cyber-attacks are not limited to natural disasters (earthquakes, typhoons, etc.), equipment failures, erroneous operations, human errors, etc., which have been considered threats to plants' safety using control systems and, Cyber-attacks are now required to be recognized as a" clear and real threat" to plant operation. Companies that own plants have spent a long time working on and responding to natural disasters and equipment failures/malfunctions.

Based on this experience, training programs have been developed, and plant operators are trained to deal with plant abnormalities that they have experienced or can assume. However, to respond to a plant abnormality caused by a cyber-attack, it is necessary to understand the impact of the cyber-attack on the plant, understand what kind of abnormality is caused by the cyber-attack, and consider and implement the measures required to make the unsafe condition safe. In addition, by increasing the level of experience, it is necessary to establish rules such as manuals and train operators to improve their response capabilities.

Hence, companies using ICS are required the follow:

- Formulation of ICS-BCP

  Many companies have created a BCP in advance to continue even during natural disasters such as earthquakes and typhoons. It is essential to develop a similar program for cyber incidents. It is necessary to analyze the risks in a cyber incident and formulate an ICS-BCP that includes countermeasures for reducing, holding, avoiding, and mitigating the effects of the risks.

- Human Resource Development

  Even in unprecedented situations such as cyber incidents, companies must respond to continue their business. And it is the employees who respond to the incident. If the personnel's ability to respond to the incident is not sufficient, the company's damage will increase. In other words, as a company, it must develop human resources who will respond.

However, they may have experience dealing with information cyber-attacks such as information leakage. Still, they do not have experience dealing with cyber-attacks even if they try to improve their ability to deal with cyber-attacks on plants (even if they have been cyber-attacked, they may not have the detection capability to identify it as a cyber-attack). Using the above problem background, this research will solve the following problems to ensure the safety of plants and business continuity of companies threatened by cyber risks.

2.4 PROBLEM SETTING

As for the first issue," lack of experience in cyber-attacks in plants," a mechanism is needed to accumulate knowledge. Experience can be gained through experience of an event happening to oneself or through virtual experience gained by watching and listening to information from people, news, and books. To enhance the experience of cyber-attacks, it is desirable actually to experience cyber-attacks.

However, companies have few environments where cyber-attacks can be experienced, so the experience is impossible. In other words, there is a need for a mechanism to experience a cyber-attack on a plant virtually. As for the threats posed by cyber-attacks to plants, there are countermeasures in introducing tools, such as the introduction of network monitoring tools used in IT systems because of cyber-attacks and the introduction of authentication control for controllers that should be protected. There are also countermeasures in introducing devices, such as the introduction of network monitoring tools and the introduction of authentication controls on the controllers to be protected. Of course, the introduction of tools is a tangible measure and one that is likely to produce results.

However, even with the introduction of practical tools, it is essential to maintain the environment and develop human resources, including training the people who will use the tools and how they will use them. This leads to the second point," There is no way to train human resources to respond to cyber incidents.

To solve these problems, this research takes an ”exercise” approach. The following two problems are set to improve re- resiliency to cyber incidents in enterprises in this research.

- Development of Organizational Behavior Exercises
- Human Resource Training Methods Using Exercises

3

EXERCISES FOR IMPROVING ORGANIZATIONAL RESILIENCE TO CYBER-INCIDENTS

This chapter will explain the solution to the problem set in Chapter 2, "Development of Organizational Behavior Exercises. First, I describe the purpose of developing the exercises and then explain the preconditions for the exercises we designed. Then, I will explain the exercises developed based on the preconditions.

3.1 IMPORTANCE OF VIRTUAL EXPERIENCE

The term "training" is also used as a synonym for "exercise," but it is essentially different. Training is conducted to improve proficiency. In other words, training is conducted to enable a person to perform a given task or procedure correctly and more reliably (or more quickly), and various efforts are made to maximize its effectiveness.

One of the purposes of exercises is to improve skills, but the primary purpose is to verify them. In other words, the purpose of exercises is to confirm and verify whether the incident preparedness, including the content of plans and manuals, is adequate. In other words, the purpose of "exercises" is to confirm and verify the adequacy of the incident preparedness, including the content of the plan and the manual. The individual capabilities required before implementing a strategy are maximized through training to implement the plan. However, the exercise examines whether the plan can be implemented alone. Exercises can bring problems and contradictions that were not discovered in the planning phase. In this way, while training focuses on the skill level of responding predictably, exercises focus on whether or not the plan will work.

If you want to increase your proficiency in dealing with obvious and unchanging things, training is the best way. However, to respond to

something like a cyber incident, which has never been experienced before or is unimaginable, decisions on how to respond must be made on the spot. To make quick decisions, the body must react instead of thinking with the head. To do this, it is necessary first to give them an image of what could be caused and what they need to think about in a cyber incident. Therefore, it is essential to make people aware of what will happen in the plant when a cyber incident occurs and what they need to respond to. A response plan should be developed based on this awareness considering the cyber incident. Then, we will examine whether the developed plan works. After implementing this flow, it is essential to identify the parts that can be handled without thinking, in other words, manualization, and to conduct training to improve the accuracy and speed of the response. Companies must prepare a BCP in advance for cyber incidents and develop human resources to carry it out. However, many companies have no cyber-attack experience with ICS, and it is not easy to imagine how cyber-attacks may affect companies. A mechanism is needed to experience cyber incidents and discuss necessary countermeasures.

As an approach to that mechanism, the authors chose an exercise. Figure3shows the flow for developing a training exercise. By analyzing incidents in the real world, we can extract the causes of incidents and the commonality of cyber-attacks targeting ICS. The exercise participants will learn systematically by giving the extracted information rules and game characteristics. Thus, participants experience cyber-attacks on ICS through exercises. Even staff who have never experienced a cyber incident can increase their experience with cyber incidents through exercises. By expanding this experience value, the team will more likely think and act even if people have a similar incident or an incident that people have never experienced before.

3.2 PURPOSE OF EXERCISE

The purpose of the exercise is not to teach the participants the answers. Especially when considering cyber incidents, there are as many ways of cyber attacks as there are attackers. It is nearly impossible to think of

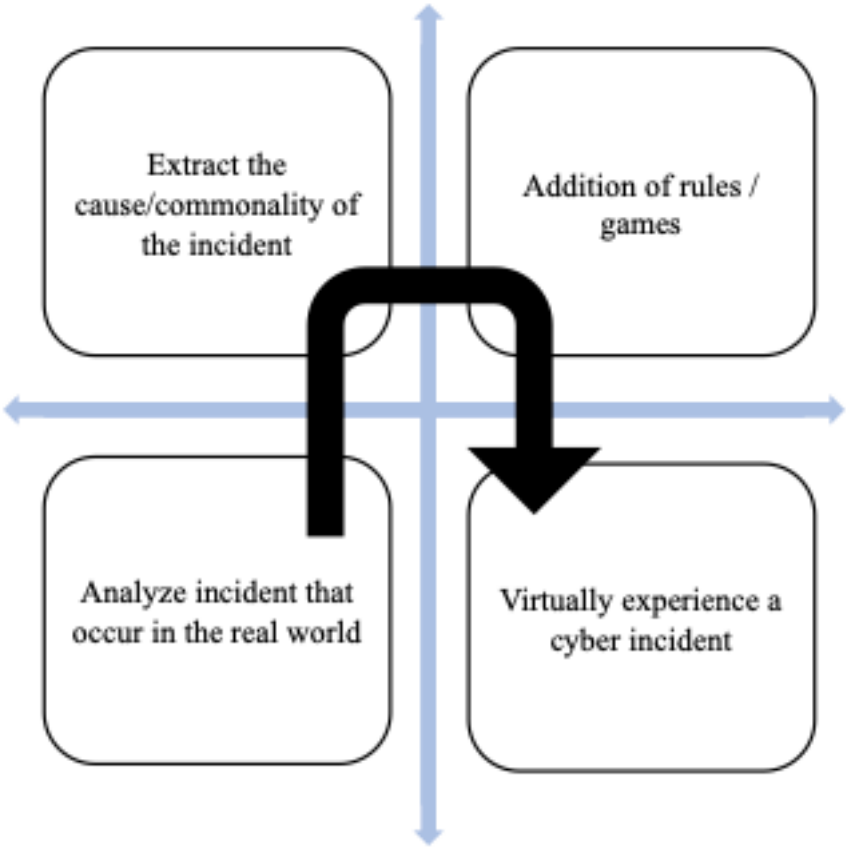

Figure 3.1: Exercise Development Process

and implement countermeasures for all of them. An exercise is not an answer, but a place to confirm a certain level of response, such as hiding behind a desk to hide your head in case of an earthquake, or a place to discuss how to respond to different situations, just like an evacuation drill. In the sense of providing a place, it may be preferable to conduct exercises that can reflect the background of the participants. However, if an exercise is undertaken with specific content, the participants may become fixated on the content and find it challenging to develop various ideas. In a situation such as a cyber-attack, where something beyond one's imagination can happen, it is not enough to conduct one exercise to deal with everything. Still, one should go through several exercises, look back, and discuss.

The core idea of the exercise is to "provide a forum to discuss the organizational response to cyber-attacks on control systems. If a cyber-attack on the control system causes a plant failure, it is necessary to restore the plant from an unsafe state to a safe one. The department in

charge of plant operation will be the one to take this action. If the plant falls into a dangerous condition, the company's service level is likely to be affected. The department in charge of the business should take the lead in this response. Finally, cyber-attacks are the potential to be conducted through information networks. The department in charge of IT in the company will be the primary responders. Therefore, the target organizations and responses for the exercise are as follows.

- Organization

  Organizations involved in the management of ICS (primary response organizations)

  Organizations involved in the operation of the project (secondary response organizations)

- Response

  Respond to cyber-attacks (cyber-incident response) while taking safety measures into account (safety response)

Given the combination of organization and response described above, the exercise needs to meet the following requirements.

- Even if I provide a place for discussion, it does not mean that people are willing to discuss. When people express their opinions, they feel that it is relevant to them and that they need to think about them seriously.

  Therefore, it is necessary that the exercise can make the target audience feel that it is relevant to them and that they need to take the initiative.

- A response is only effective if done at the right time by the right person. There is no point in responding too late or too early if you cannot respond at the right time. It is necessary to understand the situation to select which response is appropriate to make a decision. In other words, to take an appropriate response, it is essential to consolidate the proper information in the proper time for those who will decide to respond. At this point, if all the information were to be aggregated, the amount of information would be too large, and it would take time to make a decision.

Therefore, the participants must understand the importance of communication to implement an appropriate response at a proper time.

- Many companies that own plants have been considering and implementing countermeasures against natural disasters that could make the plants unsafe and control system failures caused by equipment failure, malfunction, or misoperation. The situation that a cyber-attack on a plant can trigger is not much different from the plant failures I have experienced so far. The plant's safety can be ensured by implementing the measures that have been taken so far. However, considering the restoration of the plant, the actions taken so far may be inappropriate. In the past, all that was needed was to remove the cause of the plant failure, such as the equipment that caused the failure. In the case of cyber-attacks, the effects may spread to various places via networks, not just the directly affected part. If we do not check the effects and eliminate all cyber-attacks, the same situation will likely occur even if the plant is restarted.

  Therefore, the exercise needs to consider how to apply the safety measures taken so far to the response to cyber-attacks and which of the actions that have been taken so far may become a hindrance.

- Many companies are required to establish a CSIRT (Computer Security Incident Response Team) to respond to cyber incidents. This CSIRT is often an organization specializing in IT systems cyber incidents. Considering the personnel mentioned above in charge of the exercise, it is necessary to involve the IT and OT departments and the management when a cyber incident occurs in a plant.

  Therefore, the exercise should examine the organizational structure necessary to respond to a cyber incident at a plant and the organization that will be the main body of the response. However, it does not have to be the CSIRT currently in place or about to be established.

3.3 EXERCISE PHASE

When considering a company's response to cyber incidents, the company's behavioral indicators, such as response goals and priorities, vary with safety, security, and business work volume. When an incident occurs in a plant, whether it is a cyber incident or not, it is necessary to ensure the plant's safety. Then, it is essential to investigate the cause after ensuring the plant's safety. If the reason is a cyber-attack, it is necessary to investigate the extent to which the impact of the cyber-attack has spread. Initially, the safety workload is significant, but the security workload gradually increases. Then, there will be a response to confirm the extent of the impact of cyber-attacks on plant safety and business continuity. Hence, I visualized the state that this working volume changes with the progress of time(Fig 3.2). To visualize these working volume changes with the progress of time, It is easy for participants to recognize changes in the purpose of the response.

The work volume is divided into safety, security, and business. The participant understands a change of this working volume through exercise.

1. Predictive Phase

   This phase aims to ensure the safety of plants threatened by cyber-attacks. In this phase, the participants examine the safety response obstructed by a cyber-attack. After detecting suspicious communication in a section that monitors the network, the exercise begins with an alert for the status of the liquid in the plant. In this phase, the participants must ensure the safety of the plant. Once safety is ensured, participants must investigate the abnormal operation. In this phase, participants can recognize how different causes can influence the safety response.

2. Emergency Phase

   The purpose of this phase is to continue the business. The participants consider the plant's security and how the exercise implicates a real cyber-attack. They must also consider how their business will be affected by the cyber-attack. In this phase, the participants consider practical measures taken to ensure business continuity

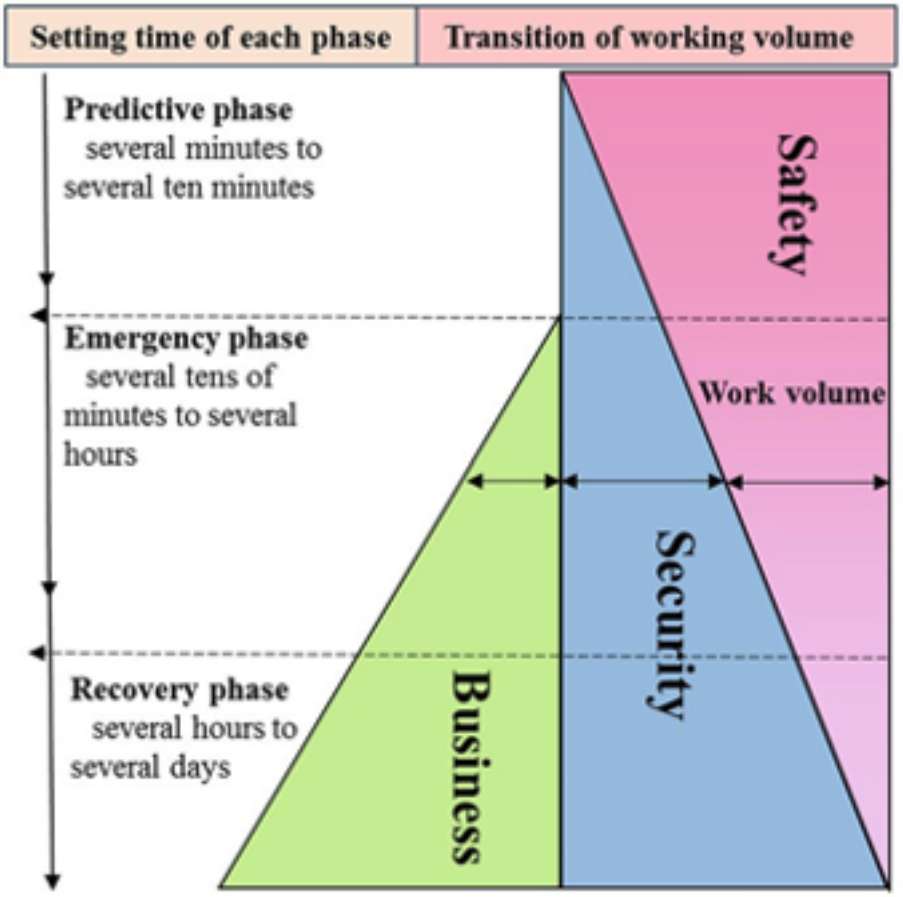

Figure 3.2: Structure of exercise with workload image for safety, security, and business continuity activities

throughout the company. This phase begins after the abnormal operation of the plant reveals a cyber-attack. In this phase, participants can recognize that the entire company must be mobilized to treat a situation caused by a cyber-attack.

3. Recovery phase

   The purpose of this phase is to restore own business to regular operation rapidly. The participants must find a way to nullify the influence of the cyber-attack so that the plant can return to regular operation. In addition, they must consider how business is affected by the temporary plant shut down. In this phase, the participants examine the start-up procedure crippled by a cyber-attack. In addition, the participants examine methods to prevent the recurrence of similar cyber-attacks. This phase begins after

a cyber-attack stops the plant. In this phase, participants think about how to restart the plant. In this phase, participants can see how different causes affect the restoration of normal plant operations.

3.4 CORE SCENARIOS FOR EXERCISE

The developed exercises are based on the same scenario with different methods. The base scenario is required to consider the ideal organizational cooperation and necessary soft/hard skills for the organization to respond quickly in the event of a cyber-attack through exercises. The created scenario was composed of three scenarios to think about safety, security, and business.

The company profile specifies the participant's roles and limitations while playing their roles. In setting up the company image, the following conditions are determined.

- Business contents
- Organizational structure
- Communication role
- Plant Structure
- Network structure

Virtual Company:

Participants from various companies, departments have different backgrounds. A typical scenario is indispensable for the participants to share the exercise. In addition, using a realistic and straightforward virtual company makes it easier to apply the awareness of the exercise to the business.

Figure 3.4 is an organizational chart of the created virtual company. Practical prerequisites, such as the company's business profile and its organization's intercommunication rule, have been set to achieve the exercise's objectives. Participants can discuss how information should be shared and how an organization should respond to cyber-attacks.

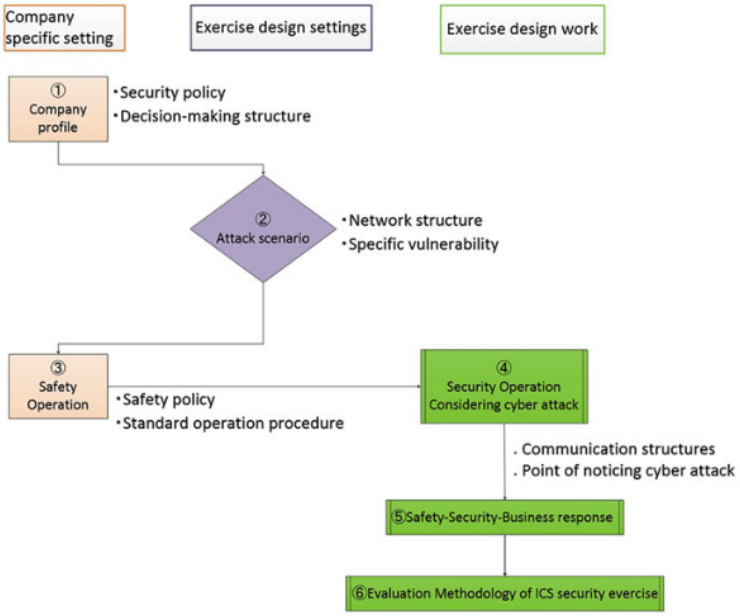

Figure 3.3: The Exercise Design Procedure and Points of Company Uniqueness

Figure 3.5 is the network structure of a virtual enterprise. The attacker will attack using the computer that was hijacked by the cyber-attack as a steppingstone. The attacker steps on the hijacked computer and moves to the computer he wants to attack. In other words, the effects of cyber-attacks are spreading to the attack target and the attack process. For mitigating the impacts of cyber-attacks, it is necessary to consider countermeasures within the range of the effects of cyber-attacks. By conducting exercises based on this network structure, participants can discuss the Security Response required to respond to cyber incidents.

Plant Operation Status Scenario:

A real-world plant consists of many devices, pipes, valves, etc. If the plant is used as the subject of the exercise, the discussion may be complicated, and the purpose of the exercise may not be achieved. The plant used as the subject of the exercise should have a simple structure. It uses a plant with a simple design as the issue makes it possible to facilitate discussions focusing on the cyber incident that is the purpose of the exercise. In addition, it becomes easier to obtain meta-knowledge about cyber incidents, and it becomes easier to apply the knowledge gained through exercises to actual plants. This scenario is based on our cybersecurity testbed(fig1.1). And we have introduced the

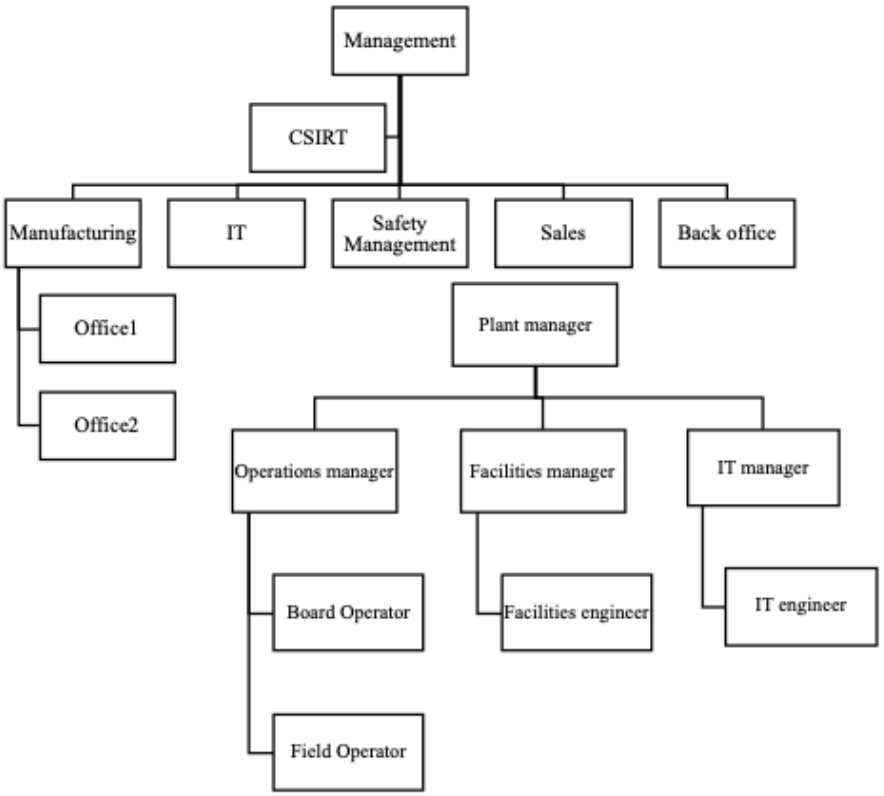

Figure 3.4: The organization chart of a virtual company

control equipment used in the actual plant. This testbed aims to test and develop ICS security solutions. Based on the cyber-attack demonstration conducted as part of the research, the plant operation information caused by the cyber-attack is used for the exercise.

The abnormality, which can occur at the site, does not change even in the case of a cyber-attack or equipment failure/malfunction, although the causes thereof are not identical. In other words, the on-site operators can put out regular safety measures for the abnormalities. Safety procedures are divided into several branches according to the situation. However, the defense scenario is designed based on one safety measure focused on incorporating the result (situation) into the defense scenario based on the attack scenario.

Trying an attack similar to the attack in the attack scenario to the simulated plant makes it possible to create the defense scenario into which more accurate information is incorporated. Moreover, it is preferable to select a person involved in a security field or on-site work as a designer

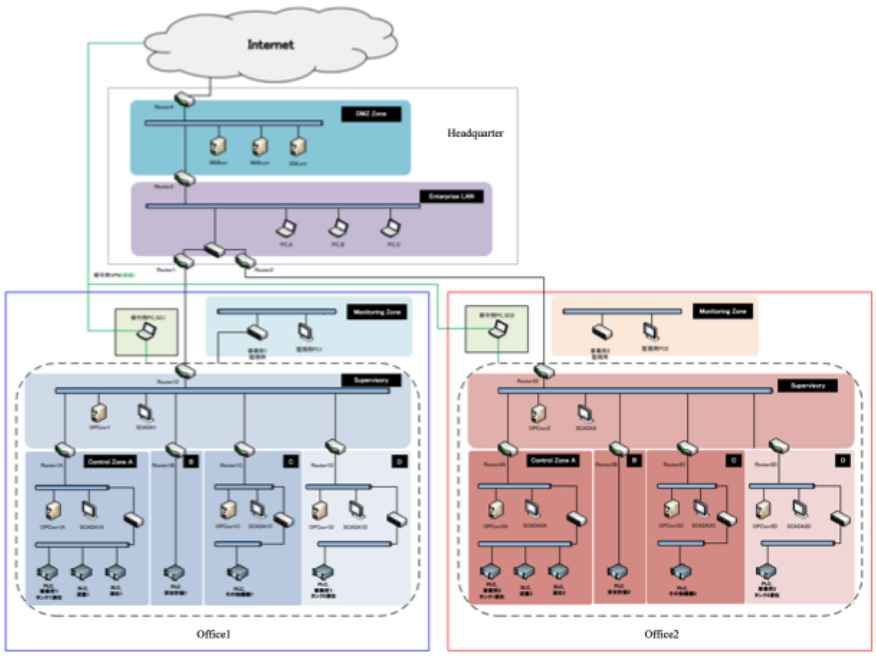

Figure 3.5: The network structure of the virtual company

of the defense scenario. It is also desirable to prepare a company outline, an organization structure, a plant outline, and a network diagram in advance to make it easier to reflect normal business activities to the defense scenario.

Once the safety measures are taken, the safety measures that take into consideration the cyber-attacks and the safety measures that take into consideration business impact are added. Regarding the following matters, as many measures as possible should be added.

1. What is a new measure formed in considering the effect of the cyber-attack?
2. In what way is information shared (in the communication network)?
3. Who will decide the measures in the presence of the information?

An existing safety measure is required to cope with actual abnormalities. Also, under the influence of the cyber-attacks, since concealment and simultaneous occurrence of abnormalities may be performed, the irregularities that may be caused at a place where the abnormality is not confirmed and abnormalities caused on purpose should be watched out

for. Specifically, it should be considered to include whether abnormal signals detected on SCADA monitors reflect the actual plant process data. When an abnormal state is set in a control device, it is recognized that maintenance activities are necessary to confirm the device's status by using the vendor's provided engineering stations.

Besides, the degree of impact from the cyber-attack changes communication among corporate departments. When an abnormality occurs, opportunities to cope with other departments (usually irrelevant departments) will increase. Also, the information sharing method should be considered not to become a bottleneck in the overall operation. In cooperation with departments in different technical fields, it is necessary to consider the information sharing protocol to reduce traffic volume and errors.

Attack Scenario:

After setting up the company image, the attack scenario is created. Currently, there is little recognition that cyber-attacks occur at control systems leading to many serious accidents. Therefore, the participants must recognize the cyber-attack as a real problem with the importance of the security measures in the exercise [17] [18]. An exercise developer should create a scenario that enables the participants to notice the attacks through the security measures designed in the scenario. Likewise, if an intruder (external factor) intrudes from a place without security measures and causes a cyber-attack in the scenario, the importance of security measures can be further recognized. The method for creating the cyber-attack scenario is shown below.

Typically, an attacker attacks based on Cyber Kill Chain. However, in the exercise, it is desirable to assume the worst possible scenario from risk management and education viewpoints. In our created scenario, I have considered the flow of the Cyber Kill Chain in a reverse direction (Table 3.1) so that the maximum risk (maximum abnormality) is expected and the attack targets are determined. It also provides an attack route through which intruders pass after intruding from areas with weak security measures.

First, the participants of the exercise are decided. In the exercise, considering the safety measures, a discussion is made mainly about

Table 3.1: The process to Simultaneously Achieve Safety and Security in ICSs.

cyber kill chain	Design cyber-attack scenario
1st-Reconnaissance	1. Maximum risk (objectives)
2nd-Delivery	2. Malicious operation (lateral movement)
3rd-Compromise/exploit	3. ICS hacking (C&C)
4th-infection/installation	4. Installation of ICS hacking (infection)
5th-Command and control	5. Prerequisite for attack (compromise)
6th-Lateral movement/pivoting	6. Recent situation scenario2 (delivery)
7th-Objectives/exfiltration	7. Recent situation scenario1 (reconnaissance)

changing the safety measures in a plant site. At the same time, a discussion is also made to develop information. When the exercise is carried out to educate on-site operators, the scenario is created where measurements in the plant site will change drastically.

On the other hand, when the exercise is carried out to consider the security measurements for the company as a whole, the scenario is created. In the created scenario, not only the security countermeasure on the plant site but also the information network can be experienced by the participants. Also, in the scenario, attack target sites should have a linked business structure (such as a supply-chain, a common market) so that business conflicts to be considered by the attacks being built into the exercise.

Second, abnormalities (risks) such as accidents and breakdowns not wanting to happen are identified. Regarding safety and security, abnormalities in the simulated plants are identified. In terms of businesses, possible management risks are identified. First of all, the top goal in the safety security business is raised as a company. Next, threats that may hinder that goal are conceived. Finally, outliers that cause that risks are identified. In this way, specific plans can be listed to reveal various opinions quickly. Then, the more plans are listed, the more the scenario options are obtained. It can be selected as an efficient method to brainstorm ideas asking for "Quantity over quality." For a similar

purpose, in creating the scenario, it is desirable that persons from various departments, such as site operators, IT engineers, and managers, be involved in creating the scenario.

Third thus, identified abnormalities are summarized, and a trigger in the attack scenario is determined. The opinions are also set in the scenario to have branches based on the abnormalities incorporated. The possible abnormalities are roughly divided into those in safety, security, and business. After splitting the abnormalities, the determined abnormalities are classified regarding the relationship between the result and the cause. By doing so, the abnormalities are further organized, and new ideas come out. In repeating this work, critical risks can be seen as the causes so that a choice of abnormalities to be considered in the scenario can be obtained.

After that, to experience conflict, which is a significant object of the exercise, common abnormalities related to two or three of the safety, security, and business are selected from the determined abnormalities. Further, in the abnormalities in safety, critical (in importance) and trouble-some (on frequency) abnormalities are chosen. Thus, the participants have increased some opportunities to consider their experiences, referring to the abnormalities in the exercise. In other words, safety measures considered in the exercise are likely to be reflected their business activities resulting in a more practical exercise.

In the exercise, linking points between safety-security operation processes and business continuity operation processes are also implicated in recognizing the safety-security-business constraint of each linking energy with the market impact. Therefore, it is necessary to select common safety, security, and business anomalies. The attack scenario can have more opportunities for participants to compare with their experiences.

Fourth, to cause the abnormalities, the attack route is selected from the attacker's viewpoint. Depending on the network structure of the simulated plant, network elements on the attack route that have security holes and weak countermeasures are specified by the attacker's view. Along with the attack route, concealment of traces of intrusion should be considered to understand a delay in recognizing the cyber-attack.

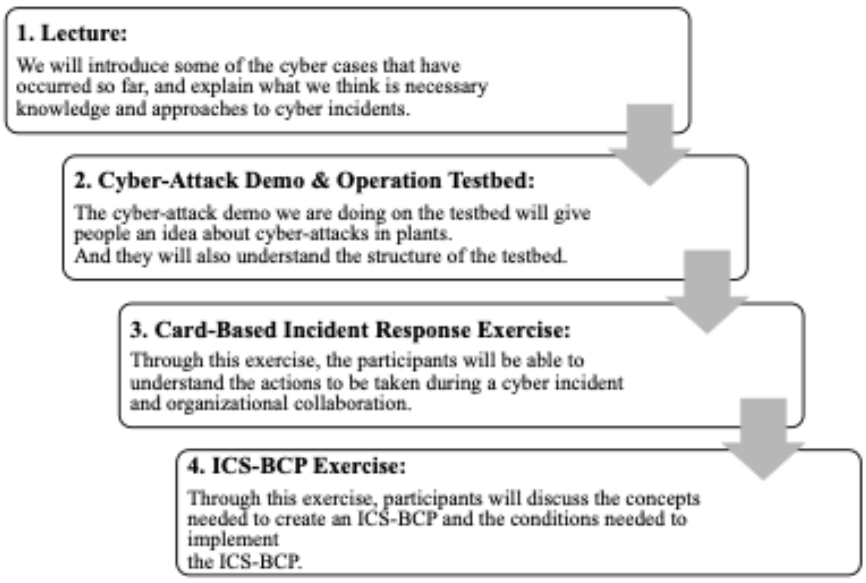

Figure 3.6: Relationship between the exercises

3.5 STRUCTURE OF THE EXERCISE

This exercise combines simulation exercises (Cyber-attack Demo and Operation Testbed) based on our testbed and table-top exercises (Card-Based Incident Response Exercise and ICS-BCP Exercise). In this combination, I examine how a company would respond to a cyber-attack as a member of a virtual company (Card-Based Incident Response Exercise and ICS-BCP Exercise).

Figure3.6 shows the objectives of each exercise and the flow for conducting the exercises. The exercise participants have different backgrounds in terms of work experience and knowledge. Before the exercise, classroom lectures are taught to prepare the learning base of the exercise participants. Then, the participants operate the testbed to perform start-up, steady-state operations, and emergency operations. Participants deepen their understanding of plants and OT systems using these simulation exercises. Next, they engage in organizational collaboration during cyber-incidents via table-top-style exercises. By experiencing this sequence of events, the exercise participants deepen their knowledge of cyber-attacks on OT systems and understand the safety responses required to make a plant safe.

3.5.1 *Cyber-Attack Demo and Operation Testbed*

This exercise aims to help participants understand the steps involved in a cyber-attack on an OT system and how it can affect the plant via the network. The exercise participants observe a cyber-attack demonstration on the testbed (Figure 1.1) in our laboratory. Figure 3.7 shows the flow of the cyber-attack demo that we implemented. This attack demonstration is carried out following the flow of the cyber kill chain. The cyber kill chain consists of seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives". Since this cyber-attack demo is intended to make people aware of the risks to the plant, it does not cover all the steps but is built by this concept. This cyber-attack demonstration is the same as Section 1.2.

The cyber kill chain consists of seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. The cyber kill chain consists of seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. Since this cyber-attack demonstration is intended to make people aware of the risks to the plant, it does not cover all the steps, but it is built according to this concept. The final goal of the cyber-attack is to attack the OPCSvr1 that controls the plant, rewrite the server's configuration file, and hide the attack from the operators so that they do not notice the attack, causing a failure in the plant control. The details of the cyber-attack demonstration are described below.

1. Step1:Reconnaissance and weaponization

   As you can see from Figure3.7, the ultimate goal, OPCSvr1, exists in the lowest layer of the network. Although it would be desirable to establish communication with OPCSvr1 and attack it directly, the OPC server functions as a data historian and is rarely touched by people. However, to make people understand that an intrusion from the IT net can attack the ICS net, attacker will hijack the PC of an employee working at the head office and attack OPCSvr1. Therefore, attacker will create the terminal information of the

employee's PC that will be used as a stepping stone for the attack and the attack program to be launched on OPCSvr1. This step will be prepared in advance during the cyber-attack demonstration.

2. Step2: Attacking a Stepping Stone PC

   To hijack an employee's PC and perform the actions intended by the attacker, it is necessary to establish a connection between the employee's PC and the attacker's PC. There are various ways to do this, but attacker will use a targeted attack. Based on the information obtained in Step 1, the attacker sends a fake email to the email address of the employee who is using the employee's PC, which is the target of the attack, to lead the employee to a malicious URL (phishing site) and establish a connection with the employee's PC. The email is designed to be a normal business email, so it is assumed to be pressed by mistake. This allows the attacker to launch various attacks against the employee's PC.

3. Step3: Internal travel

   Next, the attacker needs to expand the attack area to the network where the target OPCSvr1 is located. Therefore, attacker will use an employee PC that can be freely used as a stepping stone and gradually take over the PCs that communicate with this PC to expand the attack range and reach OPCSvr1.

4. Step4: Controller tampering

   After establishing communication with OPCSvr1, the target of the attack, the attack program created in Step 1, is sent to OPCSvr1 and executed. When this program is executed, it modifies the OPCSvr1's currently unrigged file, causing a problem with the plant's control and making the plant behave strangely. The program then hides the SCAD screen from the operator's view, delaying the detection of the plant malfunction and causing a serious accident. And by hiding the SCAD screen from the operator's perspective, they are delaying the detection of plant malfunctions, leading to serious accidents.

   When the cyber-attack demonstration is implemented with this step, the trend graphs that the operators see are hidden, as in the

case of Stuxnet, so that they cannot notice the problems in the plant. This allows the operator to be aware of the threat of not taking action when he would have been able to notice and take action and the threat that cyber-attacks pose to the plant's safety.

In this cyber-attack demonstration, the OT system operating the plant is attacked via the Internet through the IT system, and the control equipment of the plant is damaged. Then, the exercise participants experience the start-up, shutdown, and emergency operations of the testbed by themselves. In this experience, participants deepen their understanding of the relationship between the plant and the controller and the communication flow between the OT systems (e.g., the data management server, human-machine interface, and data-historian server) built to operate the plant. This simulation gives the exercise participants an idea of the actions that need to be taken to keep the plant safe and operational during a cyber-incident and the locations from which the effects of the cyber-incident need to be removed.

After Cyber-Attack Demo, the Participant will take an operation simulation exercise.

This exercise is designed to be conducted by a group of three people (or two people), each of whom plays a given role (see Figure3.8). By experiencing the flow from start-up to the plant's shutdown, the students will deepen their understanding of "safety in plant operation" by confirming accidents during plant operation and thinking about things that would be troublesome during operation.

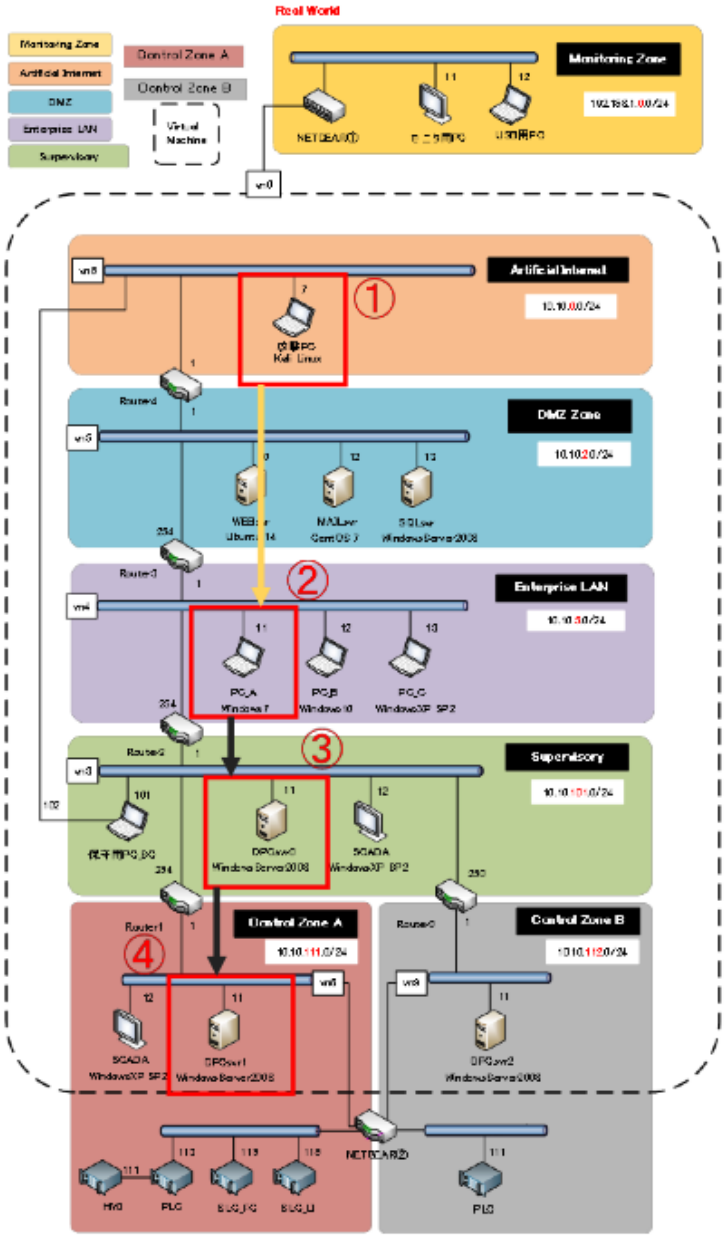

Figure 3.7: Cyber-Attack Demo Flow

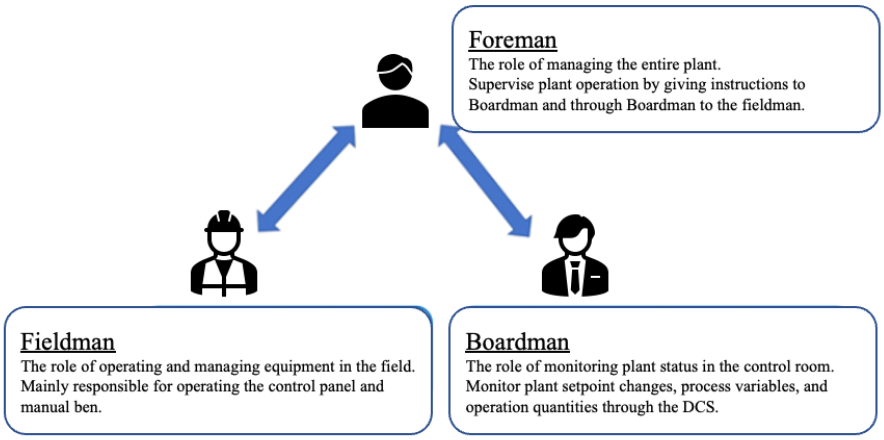

Figure 3.8: Operation Simulation Exercise

3.5.2 *Kaspersky Exercise*

The Kaspersky Interactive Protection Simulation (KIPS) was developed by Kaspersky Lab [19]. KIPS is a hybrid game with action cards and a game simulator intended to deepen the common understanding of the timeline of cyber incidents. Through KIPS exercises, players practically simulate an incident response while experiencing the effects of a cyber-attack on a virtual CI company. Players acting as security administrators for a virtual company determine countermeasures against cyber-attacks within time and cost constraints. The game's goal is to maximize revenue when responding to cyber incidents.

The KIPS exercise for multiple players comprises a game board, action cards, and a game console. The game board represents the plant and network configuration of the virtual company. Players use the game board to understand how the plant works and the devices related to the plant's operations. The game board also includes space for enabled action cards. Once a player enables an action card, it is placed in usable space. Thus, players can observe which action cards have been used. An action card represents a set of cybersecurity countermeasures. There are thirty types of action cards, e.g., a network disconnection card. Each action card represents a countermeasure and shows the required time and costs. Some action cards are added in some cases. A player can combine action cards according to the situation, such as plant status

and the available budget and time. The game console is used to simulate the game, and it provides players with information about the virtual company. In addition, players send their selected action cards to a game moderator.

3.5.2.1 *Scenario for CI Company*

The KIPS provides two CI-related scenarios, i.e., a water purification plant , and a combined cycle power plant. The water purification plant has two production lines, each comprising a precipitation tank, sand filter, disinfection tank, and drinking water tank. The power plant has two turbines, i.e., a gas turbine-powered by burning fuel and a steam turbine powered by boiling water. Exhaust gases heat the water. Then, the exhaust gas is emitted through a gas filter. In addition, the steam is changed to liquid water by cooling water.

Here, PLCs control both plant operations, and the PLCs are connected to a server in the control network. In the control network, there are various devices, such as a Human Machine Interface, a Data Historian, and an Engineering Workstation. Process data are sent to the headquarters over the Internet. The goal is to protect the devices using action cards.

3.5.2.2 *Game Simulation*

The game consists of a message phase, an action phase, a revenue phase, and a report phase. These four phases are cycled five times to complete the game. Before starting the four phases, the moderator explains the rules of KIPS and shows the participant's threats of the same industry as news. The moderator operates a dedicated game console to advance each phase. In the message phase, players receive various information, such as the news from the same industry and the status of the plant. Next, in the action phase, players use the game console to evaluate the current situation and use action cards as countermeasures. The action phase is finished after the moderator has received action cards from all teams. The administrator console calculates each team's revenue according to their actions. The results of a team's actions and revenue are sent to the applicable team in the report phase. Then, a card assistant distributes additional action cards to some groups that chose an action

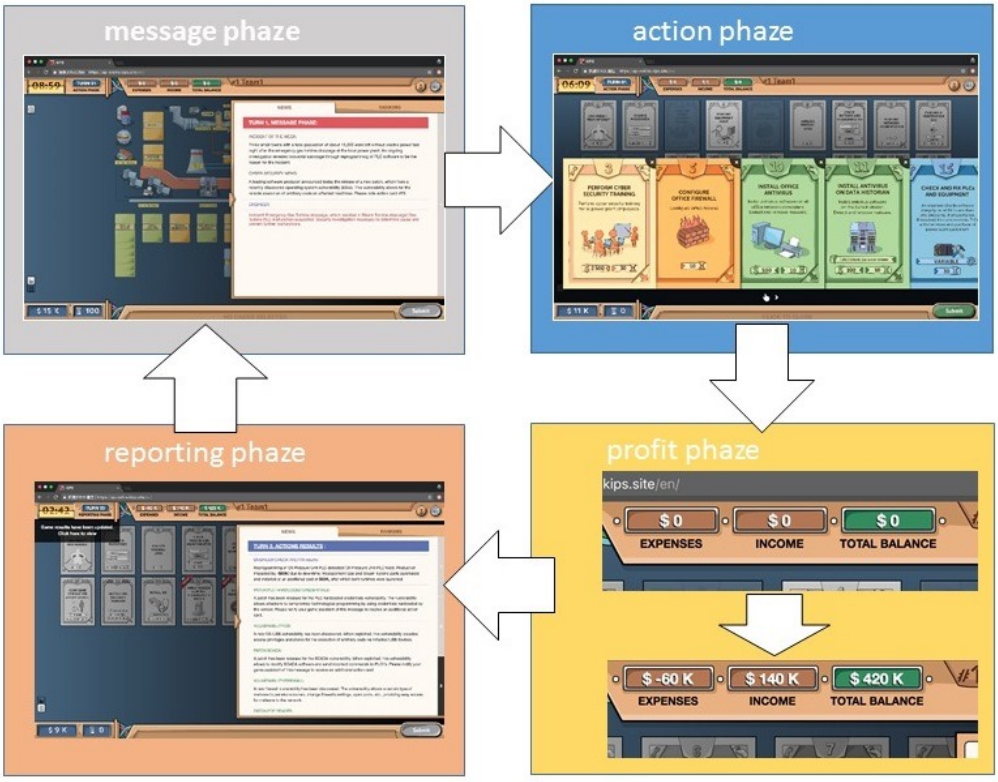

Figure 3.9: Game console of KIPS

card that leads a new event. In the report phase, all players review their team's result. Figure 3.9 shows game console of KIPS by four phases.

At the end of the game, the moderator shows the total revenue and budget left after the five game cycles. In addition, bonuses are added to the revenue depending on the actions taken. The total revenue and remaining budget can be used to evaluate how security countermeasures contribute to the company's performance. Figure 3.10 shows the relationships among the KIPS stakeholders.

1. *Structure of Proposed Cyber Incident Exercise*
2. *Inter-organization cooperation*

KIPS was designed to make aware the importance of inter-organizational incident response through game simulation. KIPS participants play the role of a security administrator. However, compared to actual CI companies, incident response is performed by several departments because both business and safety objectives should be considered simultaneously relative to a cyber incident. However, these objectives sometimes

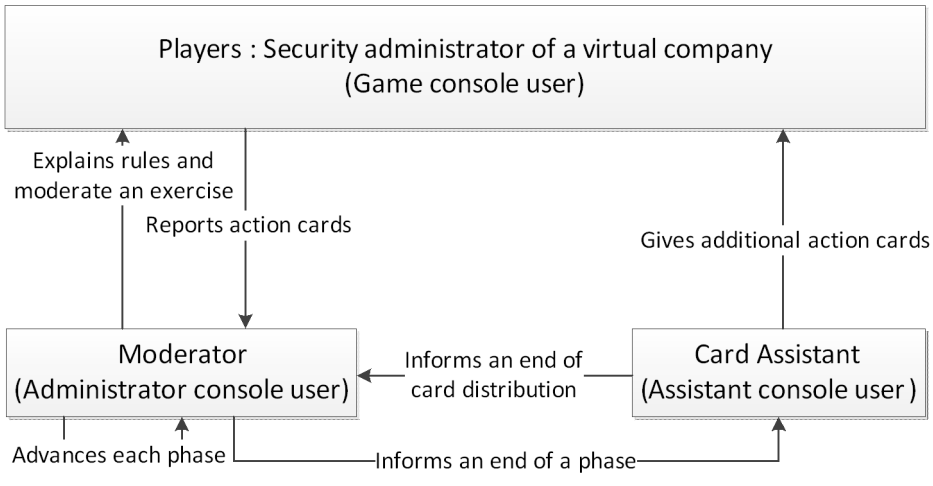

Figure 3.10: Relationships among KIPS stakeholders

have a low affinity of a response due to differences among the policies of different departments. Therefore, I incorporate a cooperative inter-organization perspective into KIPS.

Therefore, I consider the following mechanisms to design KIPS from the perspective of inter-organization cooperation.

- Separate one team into several groups

An information gap is created by dividing a team into several groups. This information gap results in more complex decision-making scenarios. A group may communicate with other groups to acquire unique information. Then, players should consider the nature of the current situation and what information is required for the given situation.

- Observe player decision making

A mechanism to evaluate non-technical skills is required, and the decision-making process should be observable.

3.5.2.3 *Proposed Exercise*

Players form two groups to create the information gap within a team, i.e., a plant administrator group and a headquarters administrator group. The former is responsible for maintaining the safety and security of the plants. The objective of the plant administrator group is to maintain stable plant operations through five turns regardless of the nature of

the cyber incident. On the other hand, the headquarters administrator group is responsible for the overall network security, the company's budget, and its profit. The objective of the headquarters administrator group is to maximize revenue. Here action cards are distributed to the groups based on their role. One group does not initially know the other group's action cards. Then, both groups discuss their actions through a chat system. The chat system enables us to observe the decision-making process because it records the communication.

In the proposed exercise, the chat system is used by both the players and the facilitator. The facilitator provides information about the message phase with the plant and headquarters administrator groups at the start of the action phase. Each group receives only the information related to their responsibility: however, the players can obtain information from each other using the chat system. When players determine the action cards they will play, the headquarters administrator group notifies the facilitator of the cards' IDs. After the facilitator enters the selected action cards into the game console, the moderator uses the administrator console to proceed to the revenue phase. The administrator console shows the temporary revenue and budget available after the revenue phase.

Then, the facilitator checks the result of each team on the game console and sends the results to each group. The card assistant then gives an additional action card to an applicable group that chose an action card which leads new event in the report phase. The moderator then oversees the next message phase and cycles the above five times. Figure 3.11 shows the relationships among the stakeholders in the proposed exercise.

The water plant scenario was used for a prototype implementation. Here, 12 action cards were assigned as headquarters administrator cards, and 18 action cards were assigned to the plant administrators.

Slack [20] was used as the chat system for the proposed exercise. Slack records user messages and can create channels for individual communication. Here, channel 1 was between the headquarters administrators and the facilitator, channel 2 was between the plant administrators and the facilitator, and channel 3 was between the headquarters administra-

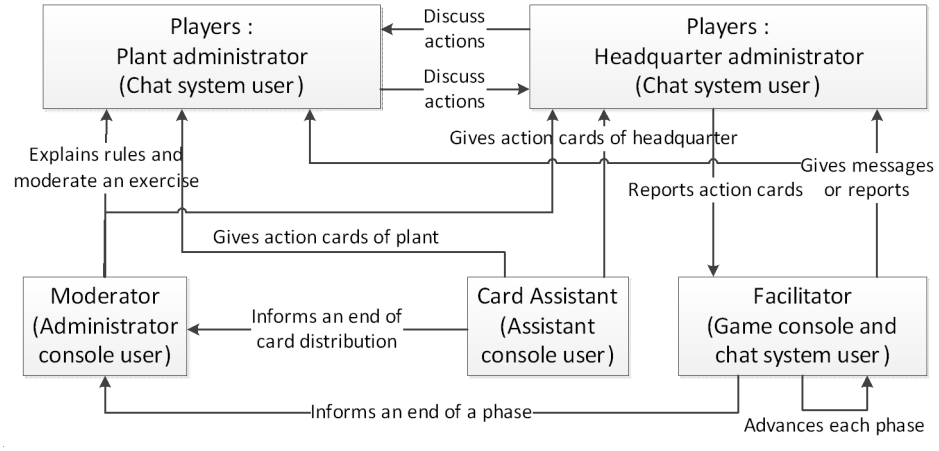

Figure 3.11: Relationships among stakeholders in proposed exercise

tors and the plant administrators. Note that the facilitator could observe channel 3 to understand the teams' situations.

3.5.3 *Field Response Confirmation Exercise*

When an incident occurs in a plant, the safety instrumentation of the plant may be activated, and the plant operation may be stopped. However, it is essential from the viewpoint of business continuity if the unsafe condition can be made safe before the safety instrumentation is activated. Even if the plant has to be shut down, it is also essential to determine how quickly it can be restored after shutdown. At the heart of these responses is the need for human intervention. This is no exception, even in the case of cyber incidents. Therefore, the on-site response confirmation exercise is an exercise in which participants understand the outline of the target plant and the risks that may occur in the plant and then consider how to respond to the incident as if it were happening. Through this exercise, the participants will discuss how to respond to an incident at the plant and the organizational coordination required to carry out such a response. The exercise consists of five steps. The exercise consists of five steps: 1) introduction, 2) explanation of prerequisites, 3) group work, and 4) presentation. (See Figure3.12)

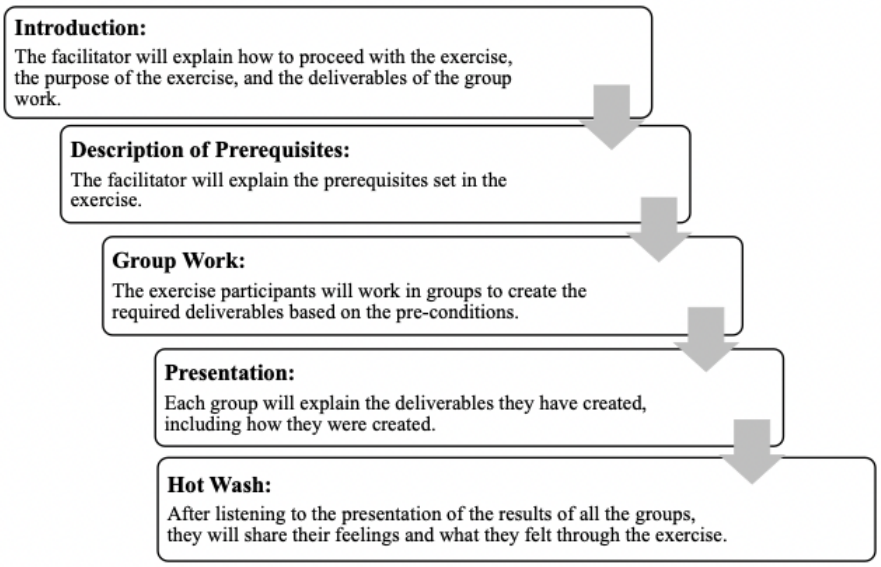

Figure 3.12: Human resource development training flow

- Introduction:

  The facilitator explains the purpose of the exercise and how to proceed. The general scenarios of the exercise are introduced to the participants. At this step, participants understand the importance of the exercise and, therefore, be motivated to apply themselves fully. By doing so, participants can increase the benefit of the exercise.

- Description of Prerequisites:

  Participants perform group work as a virtual company that owns a plant and provides products. The facilitator explains the preconditions about the virtual company at the beginning of the exercise. Prerequisites include the plant's status, the state of the IT network, and the company situation. Participants watch a video to understand the preconditions (In this phase, I use the videos was created to help participants understand the prerequisites.).

  The participants envision the outcome based on the prerequisites.

- Group-Work:

  This exercise mainly aims to increase the participants' understanding of the impact of cyber-attacks on a plant and discuss what actions are needed to protect the plant from cyber-attacks. In this

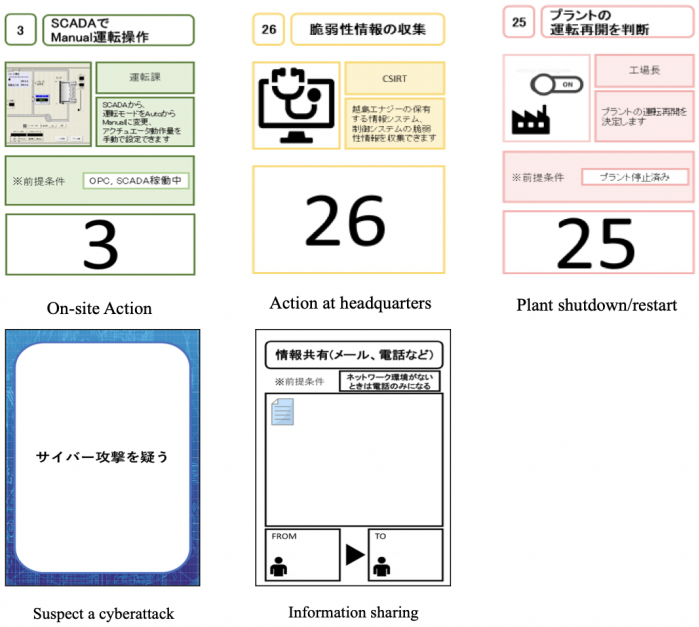

Figure 3.13: Cards using Exercise

exercise, the participants need to understand the situation of the virtual company from the conditions provided by the facilitator and examine and create a workflow to minimize the damage that a cyber-attack can inflict on the plant. The group is given a total of 38 normal cards of three types, i.e., “Field-side action,” “Head office action,” and “Shut down/restart plant,” and two special cards, “Suspect/confirm cyber-attack” and “Information sharing.” On the normal card, the result after taking action is written on the backside, and the participant thinks about the following action based on that information. There are two types of special cards: ”suspect/validation of cyber-attack” and ”information sharing.” The information-sharing card is used to share the information obtained by each department with other departments. In this exercise, participants discuss and strategies countermeasures from a bird’s-eye-view, that is, without playing a specific role. However, in reality, information cannot be shared with others unless it is shared by the person who has the information. Participants use the information-sharing card to share the information held by each department. This makes it possible to express the flow of information sharing on the workflow. An important action in this exercise is to suspect/validate a cyber-attack. No security

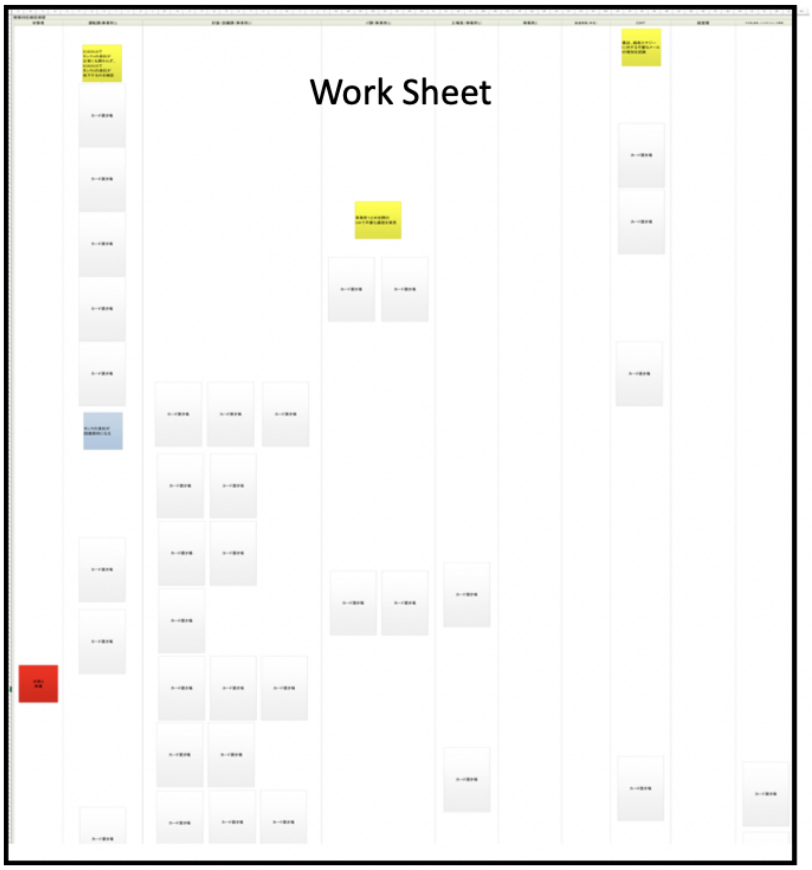

Figure 3.14: Group worksheet (Excel Screen)

response will be given unless the cause of the plant malfunction is suspected to be a cyber incident. There is information that can trigger a suspect that it is a cyber incident, and someone must judge that it is a cyber incident based on that information. By describing it on the workflow, In the group work, the participants need to create a workflow (Fig.3.15) using these given cards.

- Presentation:

  The content of the discussions and deliberations in the group during the creation of the response workflow is significant, and that is the product of this exercise. It would be best to record everything said during the group work. Still, even if we recorded all the conversations, we would not be able to analyze them unless we knew at what point and time the conversations were taking place while considering how to respond to the situation. Even if we filmed

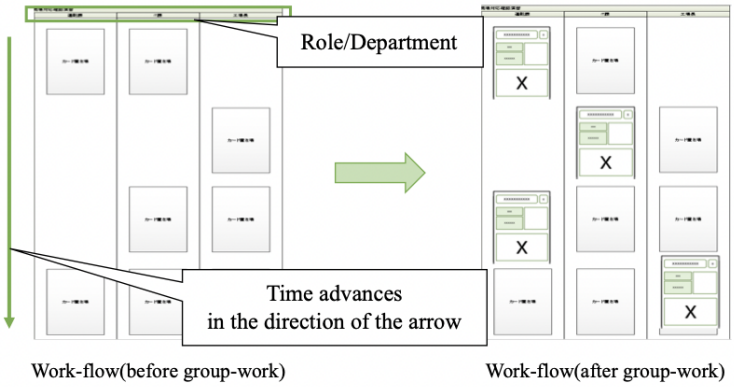

Figure 3.15: Workflow development (image)

the group work as a video, it would take much time to watch all the videos when looking back, and it would be unrealistic.

Therefore, in this exercise, each group will share how they made the corresponding workflows based on their ideas and policies based on the workflows created in the group work. In this exercise, each group will share the concept and approach of the response workflow based on the workflow created in the group work. After that, each team will make a presentation using the corresponding workflow, explaining the team's thinking and the parts of the workflow where the discussion got heated.

Groups with a lot of work experience in plants create workflows that focus on plant safety. Groups with a lot of work experience in the IT department develop workflows that mainly support IT systems. Workflow, the product of group work, depends on group members' background and experience. By sharing the workflow and the workflow creation process, the exercise participants confirm the similarities and differences between the ideas of other groups and their own group's ideas. This step can enhance the effectiveness of the exercise. When each group makes a presentation, ask them to focus on the following three points.

- How did you think about "who (which department), when, why" and placed the action card?
- What did you imagine when you created the workflow from the information given?

  - How did you feel through the exercises what kind of human resources, information sharing, and organization-related systems should respond to cyber incidents?

  Participants can understand other groups' ideas and gain new knowledge by listening to other groups' presentations and asking and answering questions.

- Hot-Wash:

  After presenting the group's plans, the facilitator will show an example of the exerciser's workflow. This workflow presented is the optimal solution that the exercise developer thinks. The facilitator will give the same presentation as the participants in the exercise. After the facilitator's presentation is over, the ideal inter-organizational collaboration for cyber incidents, information sharing, and necessary human resources will be discussed.

  Through the exercises, exercise participants will experience the response to cyber incidents and understand the impact of cyber-attacks on ICS. And it is possible to gain insights on ideal organizational cooperation and necessary soft skills and hard skills so that the organization can respond quickly in a cyber-attack.

3.5.4 *Safety Response Confirmation Exercise*

This exercise is a BCP creation exercise. Participants create an incident response exercise based on a given scenario (such as a virtual business scenario). Participants will consider how to attack the plant from the attacker's point of view, consider actions to protect the company from cyber-attacks, and create an ICS-BCP. The exercise aims to understand the perspective of things needed to develop an ICS-BCP.

The safety response confirmation exercise is almost the same as the on-site response confirmation exercise. This exercise aims to have the exercise participants discuss the response to the incident at the plant and the organizational coordination required to implement the response. The exercise is also designed to allow the participants to consider the impact of existing safety responses to a cyber incident. The difference

Figure 3.16: An example of Team Discussion in Group Work

between this exercise and the on-site response confirmation exercise is that the participants are asked to consider the response from scratch and create a response workflow rather than using cards.

Figure3.16 shows the actual implementation of the safety response confirmation exercise. As shown in this figure, the participants create a workflow for responding to a cyber incident based on the preconditions set in the same way as the on-site response confirmation exercise. Each participant is provided with an A0-size worksheet, different colored sticky notes, and markers. The worksheet is printed with the preconditions and the safety responses to the preconditions. After understanding the preconditions and safety responses on the worksheet, participants add their responses if they find the safety responses inadequate to deal with the cyber incident or write alternative solutions in the form of sticky notes on the worksheet if they feel the safety responses are not helpful to the cyber incident. If they think that the safety response is not beneficial to the cyber incident, they can list alternatives in sticky notes on the worksheet.

This exercise consists of five steps: scenario explanation, group work, demonstration, exercise review, and open discussion. Participants in the exercise identify the company's risks from the given prerequisites. Next, consider an example of a cyber-attack that may cause that risk. Then, think about how to respond to the incident caused by the cyber-attack and create an ideal ICS-BCP.

- Description of the Scenario:

  Virtual enterprise scenarios, plant scenarios, and cyber-attack scenarios are required to create incident response exercises. In this exercise, I want participants to discuss how to create an ICS-BCP rather than create a scenario. Therefore, the scenario is provided by the facilitator in advance. In addition, since there are infinite attack scenarios, some scenarios are presented, and participants select from those scenarios. In this step, those scenarios will be explained.

- Group-work:

  This exercise also creates deliverables through group work. The worksheets and action cards required for the card-type incident response exercise are the deliverable to be created.

  - First, participants analyze the risks of a virtual company from a given virtual company and plant scenario
  - Next, participants create a cyber-attack scenario that causes the analyzed risk. Participants create a scenario of the impact on the company and the plant's operating status due to the created cyber-attack scenario
  - Finally, participants create an ideal workflow for the company to perform incident response exercises and create actions that use that workflow as action cards

- Demonstration:

  In this step, participants perform their exercises on other groups. Exercises will be conducted for different groups using workflows and action cards created in group work. This step confirmed that they could convey the message through the exercise (ideal response / inter-organizational collaboration) to other groups. Par-

ticipants can also gain more cyber-incident experience by taking exercises in various scenarios.

- Group-work (Review of the exercise):

  Many things can be gained by doing exercises. Participants review the exercises they have created based on the results of the exercises conducted by other groups. The group once again discusses whether the ideal workflow they have considered is the optimal solution, what factors hinder the ideal workflow they have created, and so on.

- Hot-Wash:

  Each group will share what they have reviewed their exercises and learned through the exercises in this step. By listening to various people's opinions through this step, it is possible to discuss how to view the things necessary for creating an ICS-BCP.

3.5.5 *Exercise to Identify Necessary Conditions*

IDEF is a business reform tool and BPR (Business Process Re-engineering) method that not only summarizes the various contradictions and trade-offs that occur in the process of practicing to achieve objectives (process), and organizes and analyzes the current actual situation, but also enables the construction of a new business reform system. It is a business reform tool and a BPR (Business Process Re-engineering) method. IDEF0 [21] is one of the IDEF methods that model the process of decisions, actions, and activities in a system in a top-down hierarchical and detailed manner. IDEF0 is organized around actions or verbs. IDEF0 is composed of "Activity," which represents behavior, "Input," which is processed by the activity, "Output," which is the result of the activity's execution of the input "thing," "Control," which is used to control the activity, and "Mechanism," which is necessary to perform the activity.

In this exercise, the format of IDEF0 is used. The ideal scenario, which is a scenario that avoids the worst possible outcome under certain assumptions, can be created by ignoring the constraints during the ICS-BCP exercise. If the planned ideal response can be implemented,

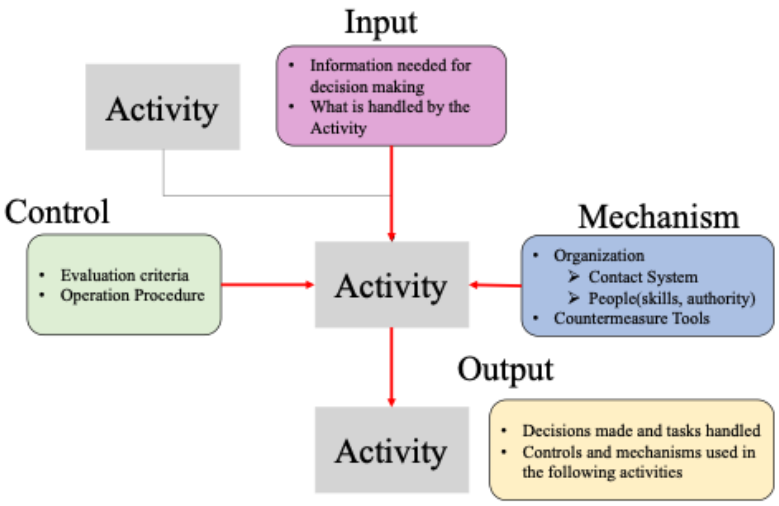

Figure 3.17: Exercise Image

the worst-case scenario will not occur, and the outcome will be good. However, in reality, the ideal scenario cannot be executed as planned due to various constraints and disturbances, such as missing tools that were supposed to be there or the absence of people who can respond to the situation.

Therefore, the resources required to execute the ideal scenario are identified according to the IDEF0 format. (Figure3.17) Then, check the differences between the existing resources and the ideal resources. You can find the ideal responses that cannot be implemented with the current resources. By eliminating them, the ideal scenario can be implemented. By discussing how to fill the gap between reality and ideal, it is possible to consider security investments and alternatives, such as whether to invest in something that does not exist now or whether it is necessary to recreate the ideal scenario to deal with its resources exist now.

3.5.6 *Simulation Exercise Called IMANE*

This exercise [22] aims to confirm the effectiveness of the created ICS-BCP by simulating the incident response. This exercise is a simulation exercise that uses a personal computer to create a game based on a scenario, input chat, and respond to an incident by selecting a response.

3.5.6.1 *Exercise Steps*

This exercise consists of five steps: identifying stress factors such as no one to deal with or no tools to deal with, adding storylines, simulating incident response, reviewing the exercise, and open discussion. Participants will play the role given and aim for business continuity while responding to incidents as virtual company members.

- Identifying Stress Factors:

  The ICS-BCP created by ICS-BCP creation exercise is an ideal workflow. In other words, the plan is based on the premise that all the assumed actions can be performed. However, in reality, it may not be possible to perform actions that should be possible due to various factors, such as lack of resources such as people and tools required to perform actions. Participants will identify stress factors that can hinder their operating the ICS-BCP they have created. Stress factors are the risks involved in conducting ICS-BCP, and it is essential to have advanced preparations and alternatives to eliminate the stress factors.

- Adding Storylines:

  The created ICS-BCP only identifies the actions and the shared information, instruction contents, and information on the operation transition of the plant due to the actions are hidden between the actions. Participants identify the hidden information and necessary information communication paths. Then, create a game scenario by incorporating the stress factors created in the previous step.

- Simulating Incident Response:

  This step simulates an incident response. Figure3.18 shows the structure of this exercise. In previous exercises, exercise participants were required to create a group workflow without being assigned to a specific role. In this exercise, roles are assigned to each exercise participant, and incident response is performed by taking actions for each role. It is an exercise that is closer to the actual incident response.

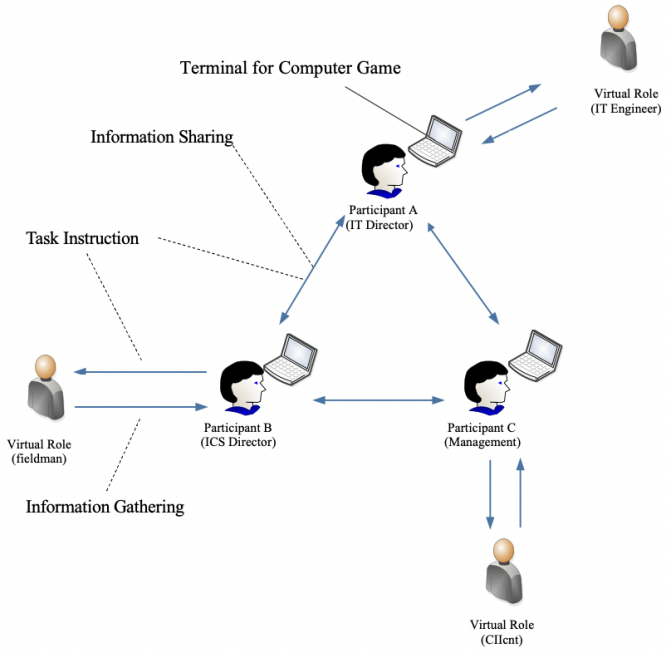

Figure 3.18: IMANE Structure

Figure3.19 is a console screen operated by the participants. Participants share information with other players and take action based on the information flowing in the tray. Each participant must understand the situation and take action based on the information displayed on their console screen. In addition, since the actions that can be performed for each role and the information is given are different, sharing the information necessary to converge the situation with other players is also required. Participants use the interface in Figure 3.19 to share information and select actions. The information displayed in the tray in Figure 3.20 is linked to the story created in the previous step, and the information displayed differs depending on the action performed so that the incident response can be made more realistic.

Figure 3.19: The User Interface of IMANE Exercise

Figure 3.20: the Action User Interface of IMANE Exercise

- Review of the Exercise: After the end of this exercise, it can be output as a product of the exercise, as shown in Figure 3.21. This workflow includes the information given to each role, the actions taken, and the flow of information-sharing, and participants can use this workflow to review the incident response after the exercise.

  Using this deliverable, exercise participants can objectively review ICS-BCP by looking back on their responses. It is possible to improve the accuracy of ICS-BCP by checking for missing or defective ICS-BCP.

- Hot-Wash: In this step, each participant shares the impressions gained through the exercise. Participants will discuss the ideas needed to create an ICS-BCP and human resource development using this exercise.

By performing these exercises in various scenarios, the participants can increase their imagination and resilience to cyber incidents.

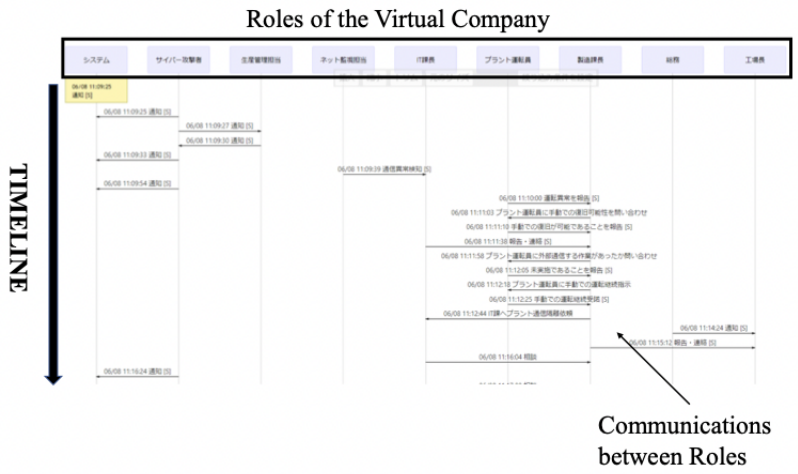

Figure 3.21: Example Deliverable of IMANE

3.5.7 *Exercise to Understand Incident Mitigation and Response*

3.5.7.1 *Purpose of This Exercise*

The focus of the exercises developed so far has been on the aftermath of a cyber-attack on a plant that results in its operational failure. However, to mitigate the effects of cyber-attacks, it is necessary to develop an exercise that allows the user to understand proactive measures that should be taken before any abnormalities occur in the plant. The purpose of this new hybrid exercise is to understand the flow of cyber-attacks on plants, the proactive measures that can be taken to protect plants from any cyber-attack, and the responses that can be taken to eliminate the effects of cyber-attacks when they occur.

Accordingly, a new exercise was conducted by adopting a game called "Red vs. Blue Gamification [23]" developed and provided by Threat-GEN for simulations (Fig.3.22) using a simulated system.

3.5.7.2 *About the Red vs. Blue Gamification portal*

ThreatGEN Red vs. Blue is the industry's first online multiplayer strategy computer game designed to teach real-world cybersecurity. The game consists of a turn-based system (3 min/turn) for a total of 75 turns, where the player chooses a given action (3.23) under the constraints

Figure 3.22: Red vs. Blue Gamification portal

of time, money, and human resources. Players can play as either the attacker (Red) or the defender (Blue).

The Red side chooses actions to shut down the plant using various attack methods, whereas the Blue side chooses actions to protect the plant from attackers and continue their business. The method of play can be player vs. computer or player vs. player. Using ThreatGEN Red vs. Blue, players can enjoy learning about the actions and mindset of an attacker (Red side) during a cyber-attack and the actions and mindset of a defender acting to protect (Blue side) the plant from that attack.

3.5.7.3 *Exercise Method Using ThreatGEN Red vs. Blue*

In this game, exercise participants only have to select an action to proceed through the scenario. In other words, if they play the game without thinking about it, the benefits they obtain from the game are reduced. Thus, to increase the effect of the game, I combined ThreatGEN (the simulation exercise) with the following additional actions.

Figure 3.23: Sample Screen of the Blue Side for Select Action

3.5.7.4 *Lecture prior the Game*

As in the previous exercises, a classroom lecture is conducted before playing the game. This classroom lecture focuses on the NIST framework [24] and cyber kill chain [25]. The NIST framework can prioritize actions to reduce cybersecurity risks by classifying them into five categories, that is, identity, protect, detect, respond, and recover. Cyber kill chain, as proposed by the Lockheed Corporation, models the sequence of actions in a targeted attack and divides the attack into seven phases. The NIST framework is explained for reference when thinking about Blue side behavior, while the cyber kill chain is explained for reference when thinking about Red side behavior.

3.5.7.5 *Play the Game*

After the classroom lecture, the exercise participants then play the game. The objective of this phase is to understand the primary usage of the game. After the game, exercise participants understand how to play the game, and the game play helps them understand their abilities. Then, they record their scores.

3.5.7.6 *Analyze the taken Action*

In this phase, the exercise participants analyze the actions that can be selected in the game. At the same time, they analyze the actions selected in the game, the type of content they have, and their impact. Table 2 shows the phases of the cyber kill chain in which the Red side can choose actions.

RED ACTION	RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOTATION	INSTALLATION	COMMAND & CONTROL	ACTION ON OBJECTIVES
HOST SCAN	✓						
PORT SCAN	✓						
SERVICE ENUMERATION	✓						
FIND PUBLIC VULNERABILITIES	✓						
ATTACK				✓			
MANIPULATION				✓			
DENIAL				✓			
FUZZING	✓						

Figure 3.24: Categorized Attacker's Actions (RED-side)

Next, exercise participants examine which categories of the NIST framework the Blue side can be chosen from for its actions. Table 3 is used to organize which phase of the cyber kill chain the selected actions are effective against.

BLUE ACTION	Category (NIST FRAMEWORK)	RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOTATION	INSTALLATION	COMMAND & CONTROL	ACTION ON OBJECTIVES
POLICIES AND PROCEDURES	Respond & Recover	✓		✓	✓			
2-FACTORS AUTHENTICATION	Protect	✓			✓	✓	✓	
CREATE IR PROCEDURES	Respond				✓			
ENCRYPT NETWORK TRAFFIC	Protect	✓						
ENFORCE STRONG PASSWORDS	Protect	✓			✓	✓	✓	
IMPLEMENT SDLC		✓			✓		✓	
IMPLEMENT STRONG Wi-Fi		✓		✓	✓			
SECURITY AWARENESS		✓	✓	✓	✓	✓	✓	✓
SECURITY SKILLS TRAINING		✓	✓	✓	✓	✓	✓	✓

Figure 3.25: Categorized Defender's Actions (BLUE-side)

By organizing the actions in this way, the attacker can have better a grasp on the phases required to accomplish the attack and selects the actions to be taken for each phase. On the other hand, the defenders select actions to prevent cyber-attacks by understanding the attacker's attack flow and organizing the actions to be taken to stop this flow.

3.5.7.7 *Play the Game Strategically*

The participants then play the game again based on the actions and strategies they analyzed and discussed during group-work. They compare their new scores with their previous scores to see if the strategy they considered is appropriate or needs to be revised.

3.5.7.8 *Hot Wash*

Participants in the exercise share their insights and impressions throughout the game-based exercise. They also share the strategies they developed and the results of the exercise. They then discuss what constraints exist in applying the actions in the game and the strategies they formulated to a real-world company to use what they learned in the game.

3.6 CONCLUSION

In this chapter, I have presented the exercises we have developed to provide a service to help people understand the risks and impacts of cyber incidents in their plants and get a sense of how they might need to respond.

These exercises have been developed based on the idea that hard skills such as plant operation techniques, IT log monitoring and analysis methods, and forensics, and soft skills such as information communication and decision-making are essential for incident response.

These exercises will help participants understand cyber incidents through hands-on experience, from cyber-attack demonstrations to testbed simulations.□In addition, for the participants to be aware that the entire organization, not just one department, is responsible for responding to cyber incidents, the exercise is based on discussions so that they can participate in the exercise from a bird's eye view rather than as a member of one department.

Through these exercises, the participants will be able to discuss not only cyber incident response in plants but also the perspectives required for inter-organizational cooperation necessary for a response from the standpoint of other departments, which will help them grow into human resources who understand the perspective of others.

4

HUMAN RESOURCE TRAINING METHODS USING EXERCISES

This chapter describes how to create an environment and develop human resources to respond to cyber incidents, using exercises developed to solve the set problems described in Chapter 3.

4.1 TRAINING METHODS USING VIRTUAL EXPERIENCES

To improve a company's ability to respond to incidents, it is necessary to enhance the ability of individuals, groups, and organizations to respond to incidents. To respond appropriately when an incident occurs, the initial response is crucial. Each person has a different background. Even if the same incident is discovered whether it is considered an incident depends on the person who found it. The first person who responds to an incident should judge it as an incident. In other words, the first person who responds to an incident needs to be capable of judging it as an incident. The company needs to establish proper reporting rules to consider the correct information at the right time.

And in ICS cyber incidents, the damage and the cause are scattered in different places: on the plant side, where the deterioration of the incident appears, and on the IT side, the root cause of the incident. To minimize the damage caused by these cyber incidents, the Safety Response, which is necessary to ensure the safety of the plant directly affected, and the Security Response, which is required to eliminate security incidents and causes that hinder the Safety Response, must be coordinated. Each response should be implemented separately. Each response should not be implemented individually but should be optimized by considering the impact of the Safety Response on the Security Response and the impact of the Security Response on the Safety Response. In other words, it is necessary to move from individual-level

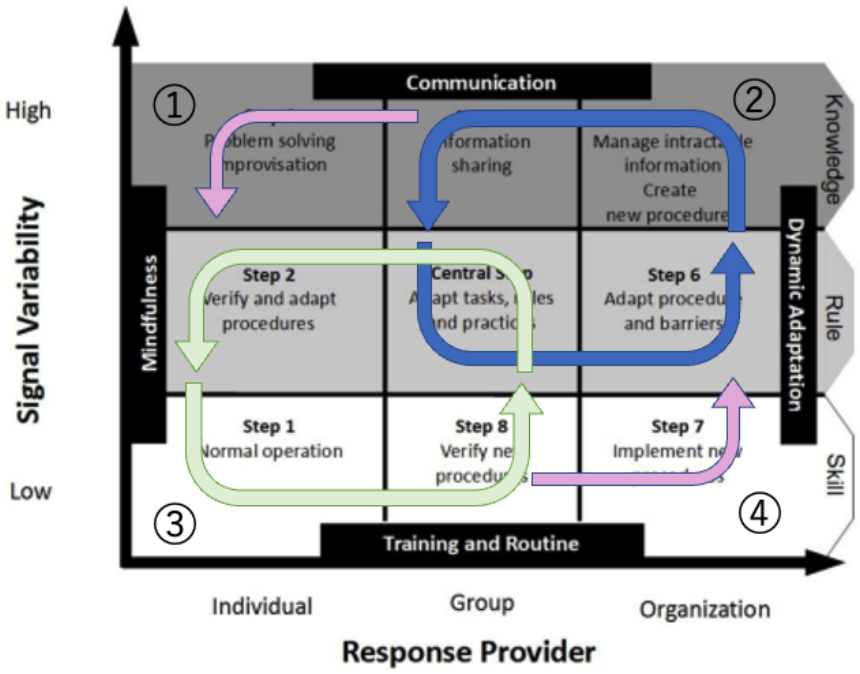

Figure 4.1: Human Resource Development Model for Security Personnel

responses to group responses in which the OT and IT sides cooperate. It is also necessary to consider how to respond to the situation as a company, from the individual to the group and from the group to the organization.

The factors that are necessary for companies to improve their incident response capabilities(Figure 4.1) are based on the resilience matrix by Bracco's Resilience Matrix [26].

1. Information Input of actual Cyber-attacks

   There are almost no reported cases of incidents in which plant abnormalities occurred due to cyber-attacks in Japan. In addition, the companies that own the plants are engaged in stable operations working at the plant sites belonging to the companies that own the plants. Their interest in cyber incidents is uneven. And they have a strong perception that cyber incidents are the responsibility of IT. Therefore, it is necessary to input information to understand and recognize that cyber incidents at plants are relevant to them.

2. Creating a BCP at the management level

   Companies are required to generate a steady stream of profits. When an incident occurs, they need to prioritize what to do to keep the business going, when to recover the business, and what alternative measures to take if they cannot recover. The ICS-BCP that companies are required to create also needs to reflect the ideas of the management. Hence, When creating a BCP, these need to be included, and even in the case of a cyber incident, the company needs to think in advance about how it should respond and inform its employees.

3. Creating a BCP with an additional on-site perspective

   It is necessary to respond to incidents based on the BCP as a company created in 2). However, the management's priority is business continuity, and it is the people working in the plant, i.e., the people in the field, who respond to incidents.

   To incorporate the policies created in the BCP into the field level, it is necessary to check the BCP from the field perspective, identify the responses required by the management. Still, the field cannot take it and modify the BCP to add the field perspective.

4. Share the ideas of all layers

   Through (2) and (3), companies created a BCP that includes both management and field levels. Based on this BCP, it is necessary to disseminate it to the people who belong to the company to act in case of an actual incident.

   Therefore, it is necessary to improve the accuracy of the ICS-BCP by conducting drills based on the ICS-BCP that has been formulated and by checking the omissions and inadequacies of the formulated ICS-BCP through actual actions and by continuing to modify the ICS-BCP to respond to them.

The activities mentioned above do not end with just doing them once. Still, by making various assumptions and running the PDCA cycle, companies can improve our incident response capability as a company.

4.2 HOW TO TRAIN HUMAN RESOURCES USING ORGANIZATIONAL BEHAVIOR EXERCISES

To spiral upward for the individual through the exercises, it is necessary to tailor the exercises developed to the recipient, i.e., the person who will become a security manager. The most important thing is to make the cyber-attack on the plant a matter of concern to you.

The first step is to input information about the plant that will be the subject of the exercise and recognize the risks, including cyber-attacks, that may occur at the plant (plant operation simulation exercise).

Then, cyber-attacks are conducted at the target plant to give an image of cyber-attacks at the plant (cyber-attack demonstration). Then, a cyber incident response exercise is undertaken in a scenario based on the cyber-attack (Safety Response Confirmation / Security Response Confirmation exercises). This will give you an idea of the incident response

The next step is to identify the resources needed for incident response as a hypothetical company (IDEF exercise) and recognize the necessary information for incident response. Finally, the participants will conduct and examine (IMANE) whether they can respond as per their perception.

Through these exercises, the participants will understand how to respond to incidents by coordinating the responses implemented by the OT and IT sides. Afterward, they will look back on the exercise results and conduct the exercise again, using the PDCA cycle to improve their resilience by connecting and understanding each other's perceptions gained through the exercise in the space of awareness. Figure 4.2 shows the flow of conducting the exercises.

However, even if the exercise is conducted by the flow of the exercise described above, there may be a gap between the intention of the exercise provider and that of the participants, depending on the background of the participants and the learning content required, and the effect of the exercise may not be realized.

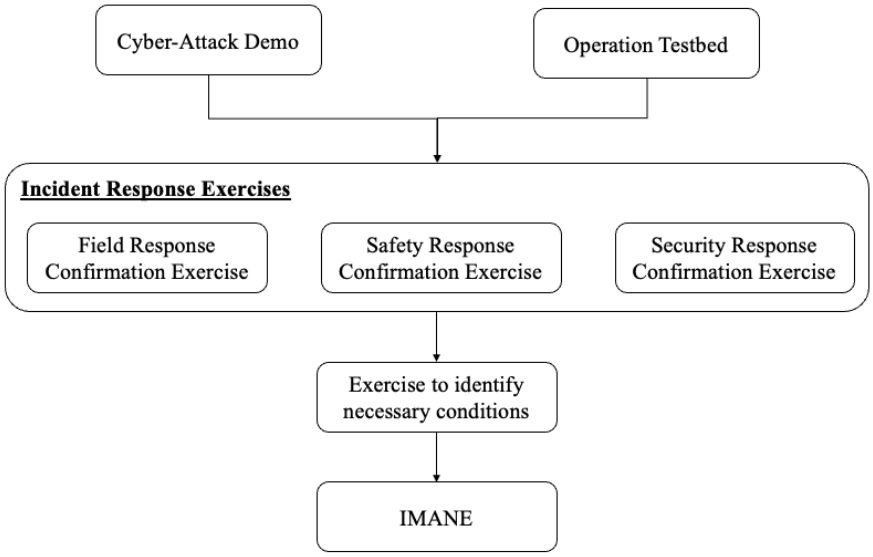

Figure 4.2: Exercise Implementation Flow

4.3 ORGANIZATION FOR CONDUCTING EXERCISE

To conduct an exercise, people must develop the exercise and people to run the exercise.

4.3.1 *Human Resources Needed to Run Exercise*

The exercise we have developed is designed for multiple groups of participants. It is difficult for a single person to pay attention to all the participants and exercise. In addition, if the exercise does not proceed smoothly, it may cause stress to the participants, and the purpose of the exercise may not be achieved. Therefore, it is necessary to use many people instead of one person to facilitate the exercise. However, if there are too many people, the exercise may not be successful. However, many people do not necessarily mean that the exercise will proceed smoothly.

For this purpose, the roles required for the exercise are defined as follows. The exercise will be managed according to these roles to ensure smooth implementation and achieve the exercise's objectives.

- Facilitator

  The facilitator is the organizer of the exercise. In the introduction, the facilitator explains to the participants the general outline of the exercise and the general scenario of the conditions that need to be set for the exercise to take place. If this explanation is poor and the participants are not engaged in the exercise, they will not engage. This will ruin the exercise. Facilitators need to explain in a way that is easy to understand and engages participants in the exercise. In the prerequisite explanation, the facilitator explains the prerequisites prepared to keep the participants on their toes. During group work, check each group's progress and adjust the time for group work. During the presentation, moderate and ask questions about the workflow that is the product of each group work to stimulate discussion.

- Advisor

  The advisor is the participant's helper. The advisor's primary role is to assist the participants during the group work. For this reason, one advisor is assigned to each group. The advisor conducts group work with the members of the given group. Currently, the advisor does not actively participate in the group work but participates from taking a step back. The advisor answers questions during the group work explains the assumptions in detail and advises creating the workflow.

- Supporter

  Supporters are the people behind the scenes of the exercise. Before the exercise begins, they set up the exercise site. The exercise will be conducted in groups, and each group will have people in it. Therefore, it is necessary to set up the desks so that they can accommodate the number of participants and allow for group work. We will also distribute sticky notes, markers, and worksheets for group work. These worksheets will be new for each phase. Since there are many groups, many people will be needed. However, since it is difficult to secure enough people, facilitators and advisors often serve concurrently.

4.3.2 *Human Resources Needed to Develop Exercise*

The purpose of the exercise service we provide is to make the participants aware of the cyber risks in the plant and the need to respond to them. Of course, there is a lot to discuss and gain from the exercises we provide. Still, we believe it is necessary to tailor the activities to the characteristics of each company.

The exercise introduced in Section 3 is just one example. Essentially, the effectiveness of the exercise cannot be enhanced without changing the scenario, the method of the exercise, and the target audience of the exercise according to the characteristics of each company for human resource development.

I hope that companies will develop their exercises based on the exercises we have designed and adapt them to their characteristics to build resilient organizations to cyber incidents.

Exercises are not completed once they are created. This is because various factors such as the organization, social conditions, and business orientation of the company will be the exercise change over time. Therefore, exercises must be constantly updated. Exercises have a creator and a receiver, and exercises need to be developed to meet the receiver's needs and incorporate the objectives of the creator. If the exercise is not aligned with the recipients' needs, then the exercise's effect will be reduced. It is also essential to repeatedly conduct the exercise to update it and get feedback from the artifacts and the participants in the exercise.

Therefore, I propose a system to design the exercise more effectively based on the concept of "Framework for Fostering and Supporting Innovators [27]", which is based on the super-program structure proposed by the authors.

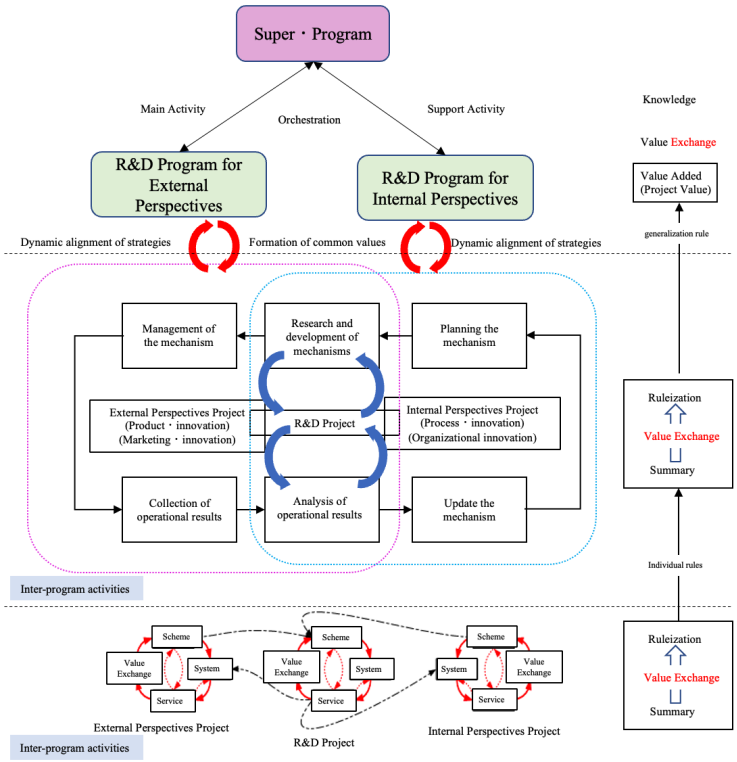

Figure 4.3: Framework for Developing and Supporting Innovators

The structure of the super program, which is the top part of Figure 4.3, the R&D program for the external perspective, and the R&D program for the internal view, in terms of running the exercise, is as follows.

The left side of Figure 4.4 shows the relationship between the management side and the student side. The exercise operator needs to conduct the exercise and implement the PDCA cycle to train human resources. To do this, it is necessary to understand the background of the partici-

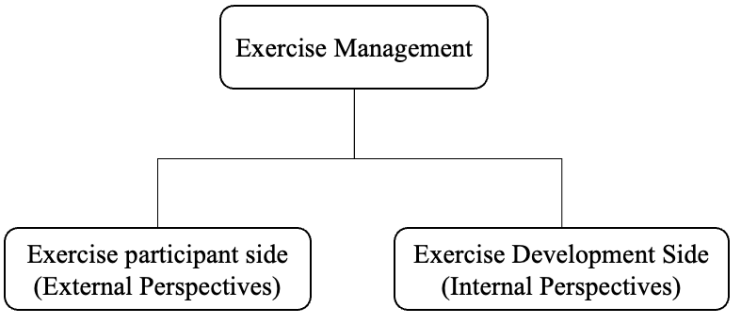

Figure 4.4: Program Structure in Exercise Implementation

pants, what kind of security manager they need to become, and what type of security manager they are aiming to become.

The right side of Figure 4.4 shows the management side and the exercise development side. After obtaining the information from the students as described above and considering how to combine the exercises, sometimes it may be necessary to adapt the prerequisites and methods of the activities to the students. By feeding back the communication between the management and the students to the exercise development side, it will be possible to provide the exercise contents necessary to develop human resources to respond to cyber incidents.□

In this way, exercises are developed, human resource development is conducted using them, and the results of the exercises are analyzed to improve them. Then, based on the results of the exercises, organizational and operational reforms and a database of human resources can be created to make the organization more resistant to incidents.

4.4 CONCLUSION

In this chapter, the human resource development method used the exercise developed to build a strong organization against cyber incidents was introduced in Chapter 3. And the human resources and mechanisms required to implement and improve the exercise were explained.

Using this mechanism, we have developed many exercises up to now. I believe that by applying this system to each company, each company can create exercises that incorporate the company's characteristics and develop the human resources that the company needs.

Through this exercise, I believe that companies can educate employees about cyber incidents and identify departments and personnel who can be critical players in an incident.

5

DEVELOPMENT OF PRACTICAL EXERCISES

This chapter describes the actual implementation and results based on the exercises for improving resilience to cyber incidents described in Chapters 3 and 4.

5.1 PILOT EXERCISE

The exercise is established for a simulated plant of our study room through the methodology mentioned in Chapter 3 in this paper.

5.1.1 *Target Plant*

The target company in the exercise prepared in this paper is a plant having the structure shown in the figure and a company holding the internal network. This company's service is a service that generates energy to move air conditioning and supplies energy to the area. Tank 1 is a tank possessed by a supplier, and tank 2 holds a supply destination. The plant has the following functions:

1. The heater warms the water in the lower tank
2. Hot water is supplied to the upper tank using a pump

Zoning and firewalls are also introduced as network security measures. Control of Valve 2 and heater by Single Loop Controller (SLC) in the different zone makes it possible to detect open firing events caused by lowering the liquid level of Tank 1 and continuation of heater operation.

Also, by looking at the level of each tank on the SCADA screen in each Zone, you can notice abnormality even if a cyber-attack conceals one screen. Moreover, installing a firewall makes it possible to detect and block suspicious communication from outside. Participants understand

the impact of concurrency and concealment of abnormalities by cyber-attacks on correspondence through exercise. It is used to learn the skills and elements necessary to prepare the organization and communication system required to deal with cyber-attacks.

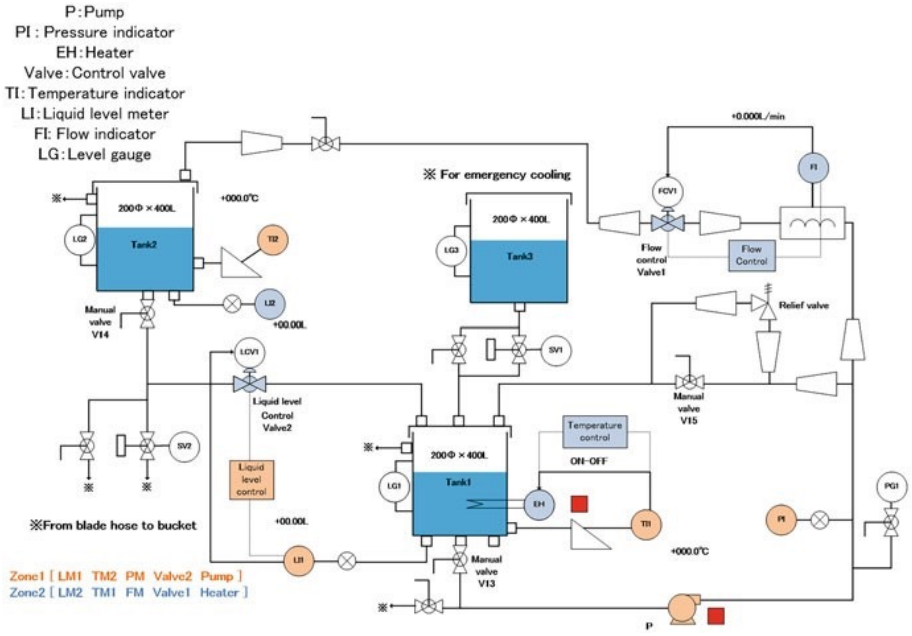

Figure 5.1: A simulated plant heats water with a heater in the lower tank and circulates the heated water through a simple pipeline to the upper tank (using a pump)

5.1.2 *Profile of Virtual Company*

The virtual company's profile is as follows:

1. Project outline: District heating and cooling service business
2. Organizational structure: Outline of the simulated plant (Figure 5.1), network structure (Figure. 5.2)
3. Roles with a communication network (Figure. 5.3)

5.1.3 *Attack Scenario*

The object of the exercise to be created this time is a virtual company. Therefore, education for improving the company's security is the exercise purpose. Specifically, the purpose is to allow the participants to

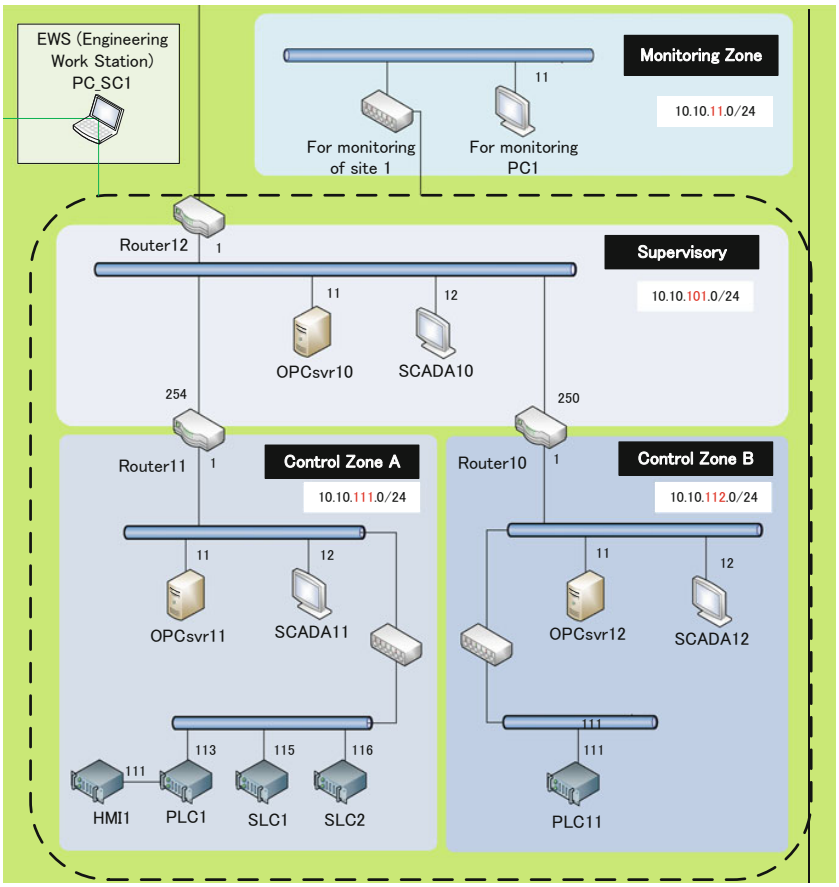

Figure 5.2: In this ICS network, OPC servers collect and exchange process data, and monitor them by using SCADA function included in the OPC Servers

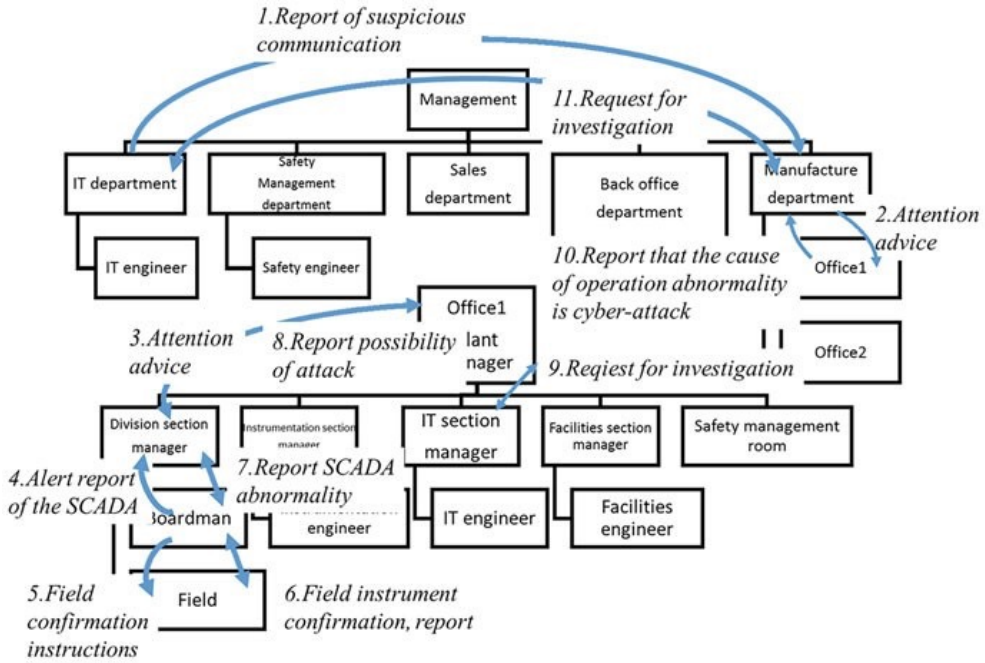

Figure 5.3: Communication Management under Emergency

consider the difficulty of early warning of the cyber-attacks and the measures in the company as a whole. Therefore, the participants of the exercise are all members belonging to the virtual company. The designer creates exercises con-figured to think about three aspects of safety, security, and business.

Next, the designer identifies possible abnormalities as many as possible. The participants should be aware that the abnormalities due to the cyber-attacks may lead to severe accidents. Also, the participants should realize in the exercise that such abnormalities are events related to the life of persons at the supply destination and employees. For that reason, we will aim for safe operation at safety and maximum continuous operation for business as the top targets.

Likewise, companies that do not take security measures and education are more likely to deal with cyber-attacks late. Therefore, the maximum targets are pre-venting the damage and the spread of infection by cyber-attacks. By determining the top goal, it becomes possible to discover the risks of impeding the achievement of the goal.

Therefore, the following risks are listed:

1. Safety: An abnormality occurs in the plant
2. Security: Damage caused by the cyber-attacks, infection of terminals
3. Business: Shut down of the plant

The participant uses the brainstorming method to clarify the events that cause these risks. Table 5.1 shows the revealed events. In Table 5.1, in the safety viewpoint, the first line indicates the results generated by the risk, and the second and subsequent lines show the causes thereof.

From the revealed events, the participant selects an event to be generated by the scenario of the cyber-attack. The abnormality chosen must be a common abnormality related to multiple safety, security, and business risks. The business risks are associated with the safety and security risks if the cause of the business risk as "the event where conveyance to the customers is failed" in Table 5.1 is abnormal at the plant. The risk is a common abnormality in all aspects of safety, security, and busi-

ness. Therefore, the risk is selected as the event generated by the attack scenario.

Table 5.1: The Maximum Goal and Risk of the Company for Cyber-attack

	Goal	Risk
Safety	Safe operation of the plant	An abnormality occurs in the plant
Security	Prevention of damage and spread of infection	Damage and infection of devices
Business	Continuing plant operation	Shut down plant

Next, the participant selects another event where the services cannot be supplied to the customer in the safety/security viewpoint abnormality. From the viewpoint of safety risk where an exception occurs in the plant site, if one of the events appears when Valve 2 is not fully closed, or Pump is stopped, the water does not circulate to Tank 2 as the supply destination. As a result, the liquid level of Tank 2 drops, and the hot water supply service becomes impossible.

Even if the manual valve of Tank 2 is closed to prevent the liquid level of Tank 2 from lowering, the hot water does not circulate, and the service quality gradually deteriorates, as shown in Figure 5.4. An arrow indicates the water flow, and the part where the flow is stopped (Valve 2 and Heater) is designated by x. Also, the valves and pumps are likely to be failed. Therefore, the on-site operator firstly suspects equipment failure and responds accordingly.

Also, since the same SLC controls the Valve 2 and Pump in the network diagram, the network is easily attacked. From the above, it is difficult to conclude that the event where the Valve 2 does not close, or the pump stops is recognized as a cyber-attack. Therefore, this event is considered optimal for an attack scenario, as it causes an influential incident and causes an attacker to create a structure that is easy to attack.

Concealment of cyber-attack is also essential. The attacker simultaneously causes a plurality of malicious abnormalities. In doing so, the attacker operates (concealment) that delays the detection of abnormality to prolong the time the attacker freely attacks. Precisely, in this

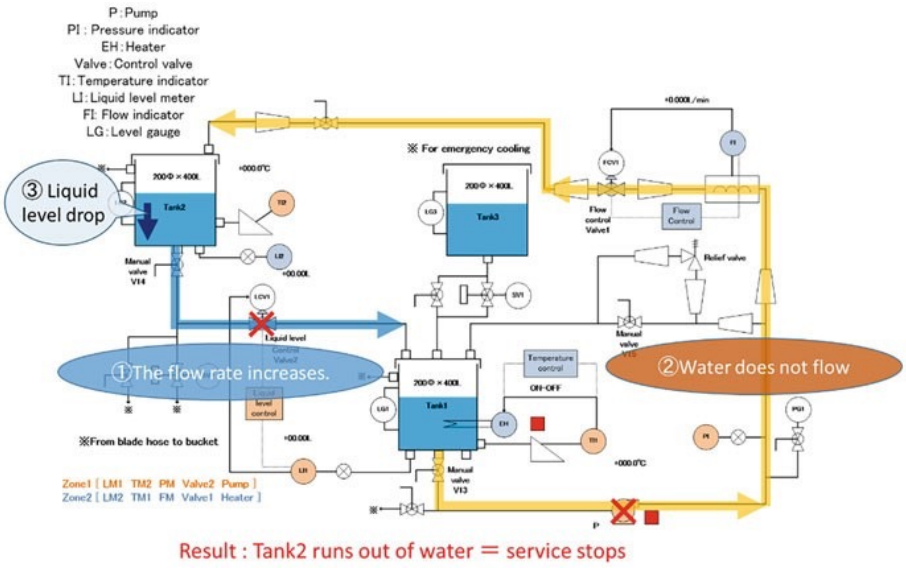

Figure 5.4: Abnormal Events caused in the Plant for Exercise

scenario, the attacker conceals the monitoring screen (SCADA screen) to delay the detection of the abnormality. Therefore, in the at- tack scenario, the event "the instruction is not reflected on the SCADA screen" in Table 2 is selected. Based on the above, the events, which will be incorporated in the attack scenario, are colored in Table 5.2.

In the attack scenario, the participant must recognize the necessity of security measures. The firewall installed between the headquarters and business sites in a company network system can block cyber-attacks. Therefore, in the attack scenario, the intrusion is performed at the place (within the plant site) where the firewall is not installed. Although a severe accident cannot be caused only by Zone splitting, a scenario is created where the attacks are repeated within the same zone, and the events selected from figure 5.5 are generated. The attack scenario corresponding to the procedure of the Cyber Kill Chain is organized, as shown in Table 5.2.

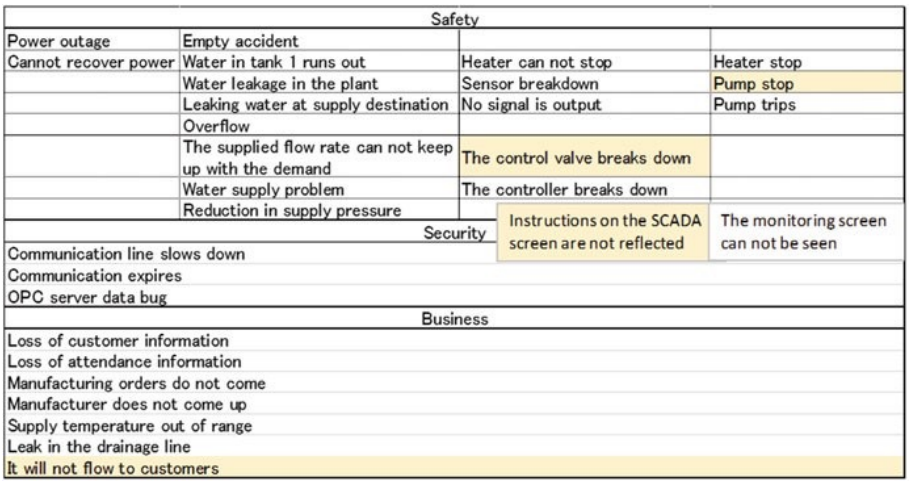

Figure 5.5: Selected events—in safety, the first line caused the risk, and as a result, the second and subsequent lines indicate the cause

Table 5.2: Design procedure of the cyber-attack scenario (NIT exercise)

Cyber-attack scenario template	NIT exercise—cyber-attack Scenario
1. Maximum risk (objectives)	1. Stopping the plant
2. Malicious operation (lateral movement)	2. Instructions for stopping the pump full indication of valve 2
3. ICS hacking (C&C)	3. Program change of SLC
4. Installation of ICS hacking (infection)	4. Malware infection due to execution of the attached file
5. Prerequisite for attack (compromise)	5. Open the attached file on user (supervisory zone employee PC)
6. Recent situation scenario2 (delivery)	6. Send mail with malware (enterprise/supervisory zone employee PC)
7. Recent situation scenario (reconnaissance)	7. External vulnerability scanning send phishing email (to the company)

In this scenario, the information system department belonging to the headquarters warns that "Recognizing that suspicious e-mails are increasing in the company recently." The attacker's attack with the above procedure. They send e-mails containing the virus inside the headquarters and office. Since companies do not have security education, they both open e-mails.

A firewall that can't intrude by the attacker is set up at the headquarters. On the other side, the office does not have a firewall so that

the attackers can intrude. After that, they take over the SLC through OPC Server 1 of Plant 1. They rewrite the program so that operation on the SCADA screen and the on-site panel is not reflected, and open Valve 2 and stop Pump. The operators can be turned on them manually. However, an incorrect command is continuously sent from the rewritten program; the command immediately turns off the pump and does not start it. As a result, unknown abnormalities occur frequently and simultaneously, and the plant is forced to shut down.

The designed attack procedure can be indicated by FTA (Fault Tree Analysis) [28]. By issuing an event corresponding to the attack procedure given by FTA, situations on the site that can occur in the exercise scenario can be seen. They can be reflected as a premise (Figure 5.6). It is also good to illustrate the network that added what kind of route to attack, like Figure 5.7. It helps designers consider the correspondence and assume the influence range of cyber-attack at the same time.

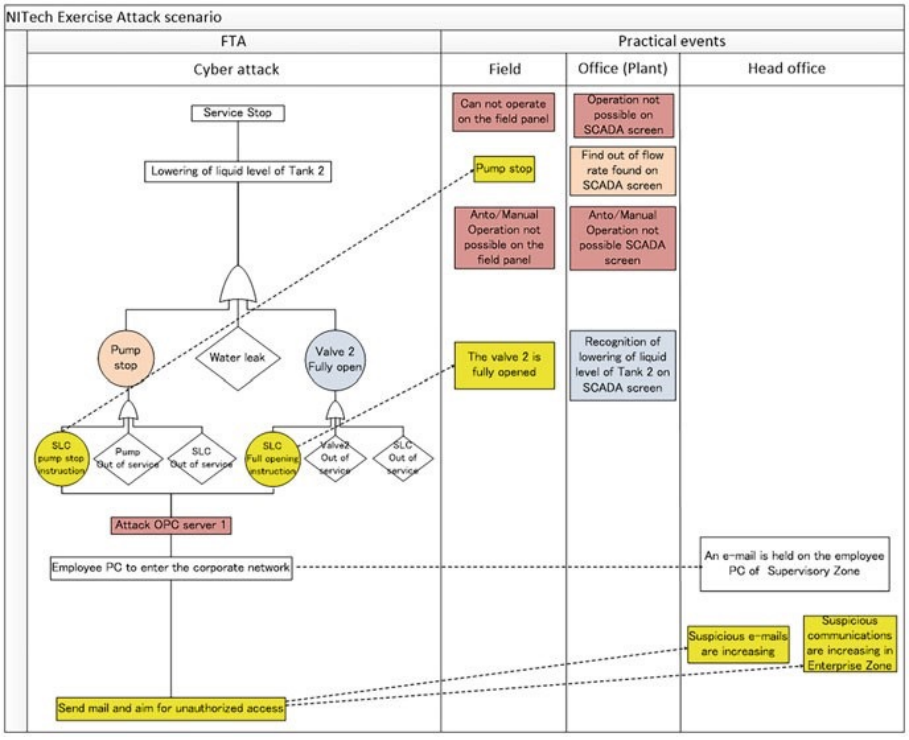

Figure 5.6: Selection of Prerequisites for Exercises using FTA

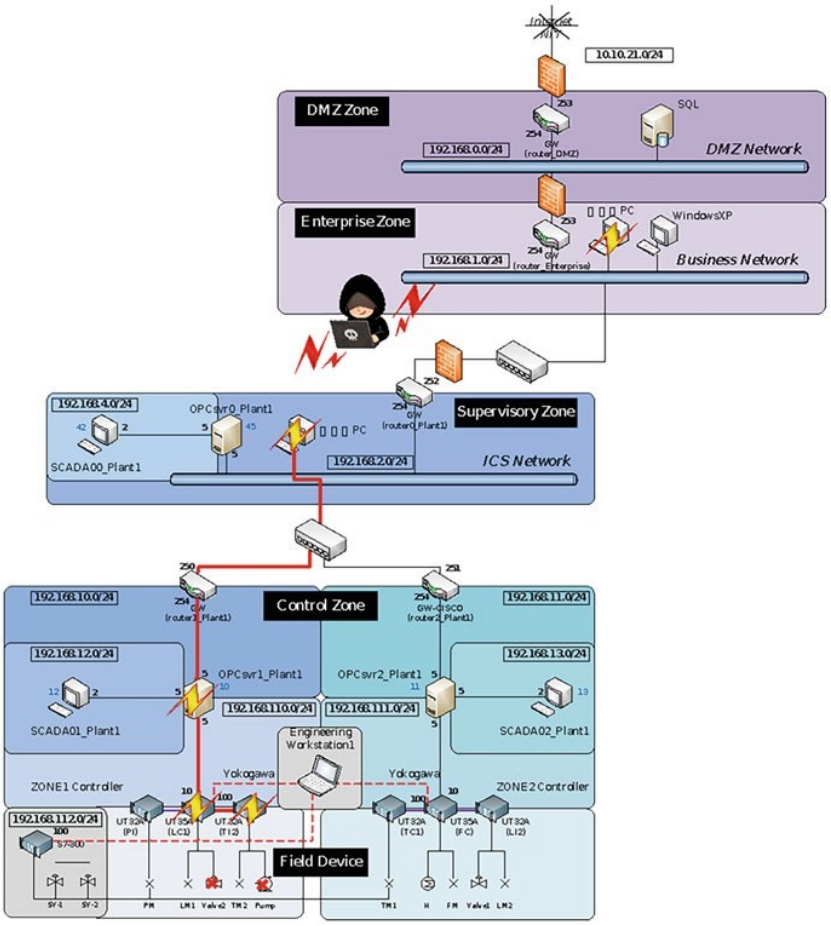

Figure 5.7: Cyber-attack Scenario on the Company's Network

5.1.4 *Defense Scenario*

A safety response is created in the attack scenario. The designer creates an attack scenario based on the abnormality occurring at the site according to the ordinary work procedure. After that, the designer adds security counteractions and business counteractions considering the cyber-attack. Specifically, the response from the site, such as on-site confirmation and inspection spots, is increased due to multiple simultaneous abnormalities. Moreover, when considering the business impact, new information developed from the worksite to the head office and reflection of decisions based thereon are deemed. The measures are changed when creating the defense scenario, as shown in Figure 5.8 and Figure 5.9.

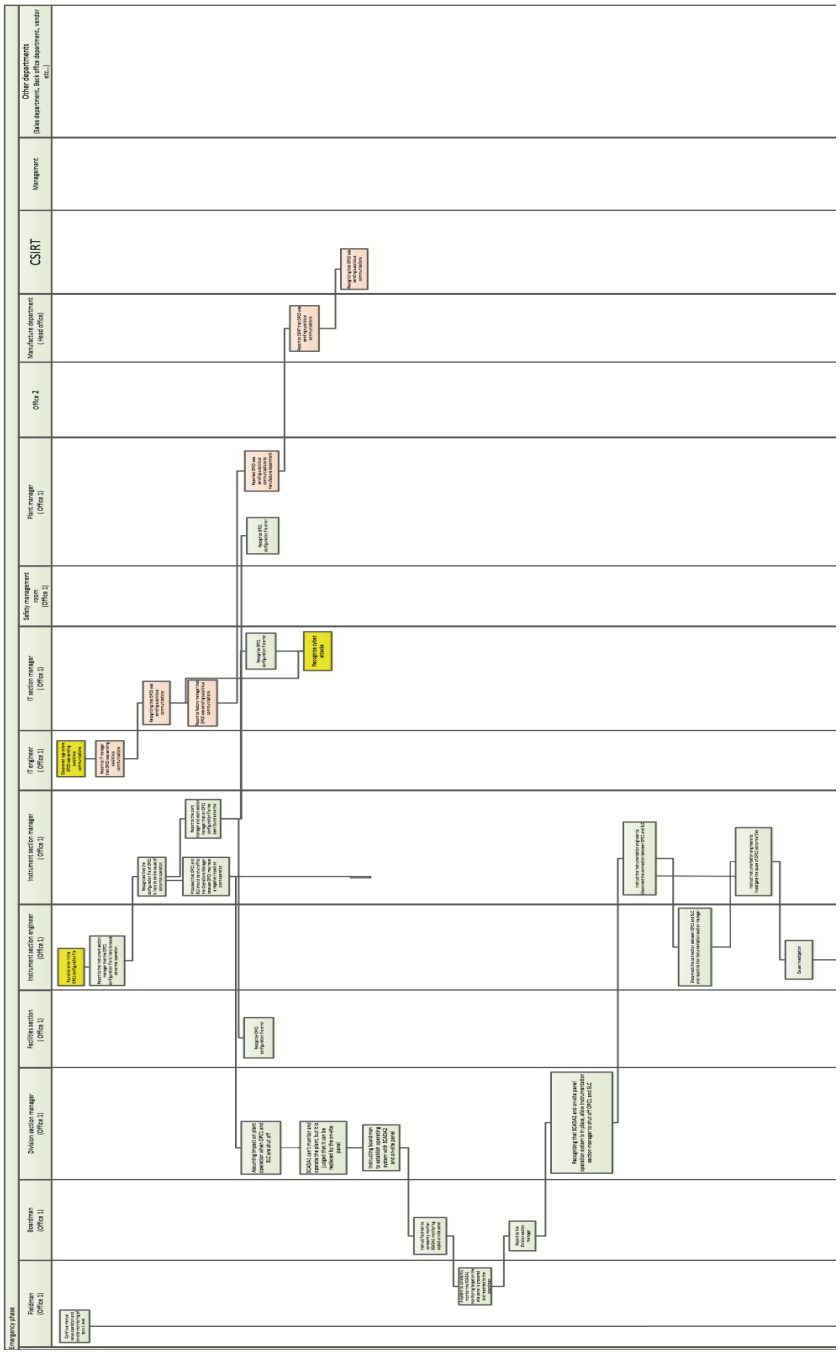

Figure 5.8: Workflow—Safety Response

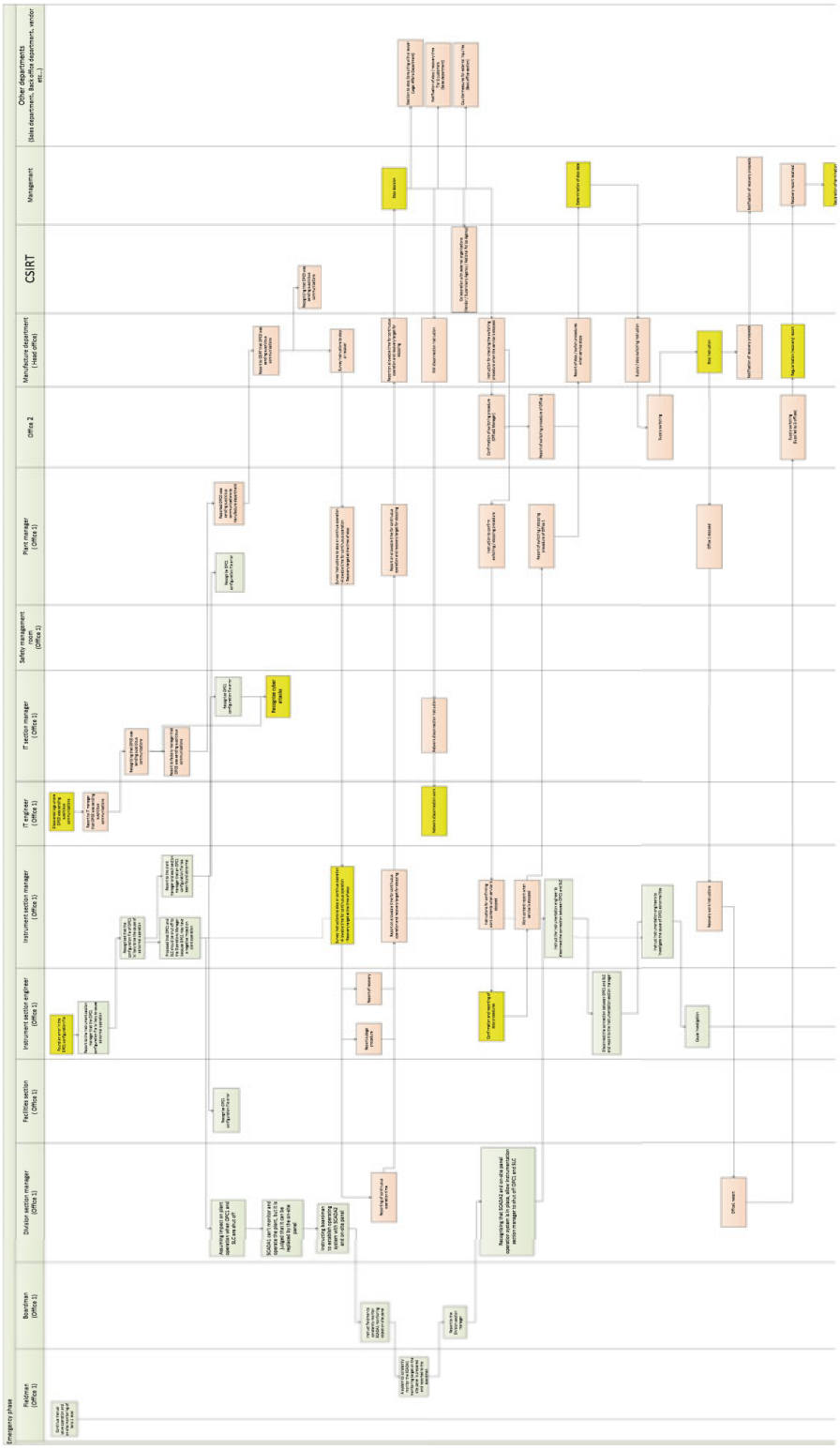

Figure 5.9: Workflow—Safety Response considering Cyber-attack

5.2 FEEDBACK OF PILOT EXERCISES

5.2.1 *Field Response Confirmation Exercise & Safety Response Confirmation Exercise*

While improving the developed exercises step by step, many security and operation experts participated in the Nagoya Institute of Technology security workshops from 2015. To get an opinion to improve the exercises, we asked the participants to complete the questionnaire. The questionnaire was answered with a maximum of 5 points. We have been conducting this exercise in workshops since 2015. We have received excellent evaluations from the participants indicating that the table-top exercise was easy to understand and that they were able to understand the safety measures necessary to make a plant safe, which was the primary purpose of the exercise, by experiencing the cyber-attack demonstration and plant operation simulation using the actual equipment (testbed). At the same time, the results of the exercises revealed the following issues:

- Lack of discussion on how to respond to cyber-attacks before signs appear in a plant

  These exercises focus on responses to ensure the safety of a plant after a cyber-attack when the plant shows signs of abnormalities. Many of the exercise participants confirmed that they were able to gain an understanding of this stage. However, to minimize the impact of cyber-attacks, proactive measures should be taken prior to a cyber-attack, and it is necessary to develop exercises that can discuss these security responses.

- Space for setting up a simulated plant is required to conduct the exercise

  One of the features of this exercise is that it was developed using a simulated plant that can be operated manually. The exercise participants can easily understand the impact of cyber-attacks on the plant by touching the simulated plant and watching the demonstration of a cyber-attack on it. Then, participating in the table-top exercises with an understanding of the subject of the exercise, the

educational effect of this hybrid exercise is enhanced. However, it is essential to have a physical space for the simulated plant to conduct the exercises. As a result, the place where the exercise is provided is limited to the physical location of the simulated plant.

- Structure makes it challenging to check the effects of the exercises

  This exercise was developed to acquire the meta-knowledge necessary to respond to cyber-attacks targeting OT systems. Feedback from the exercise participants has indicated that they feel that they have gained such meta-knowledge. However, we have failed to confirm whether the capabilities of the participants improved. Even if the exercise is conducted under a different scenario to measure the effect of the exercise, if the subject of the exercise (e.g., a simulated plant or a scenario of a disguised company) is the same, it may not be an exercise but rather a drill to confirm the procedures.

- Structure makes it challenging to understand the point of view of the cyber-attacker

  To protect a plant from cyber-attacks, it is essential to understand how cyber-attackers think and conduct their attacks. These exercises focus on the perspective of the defender. A cyber-attack scenario, including the point of view of the cyber-attackers, was created during the scenario development phase of these exercises, and these exercises were developed based on this cyber-attack scenario. However, these exercises were not designed to make the exercise participants intensely aware of the cyber-attacker's perspective.

In addition, the following was found by analyzing the deliverable of the exercise.

- Plant safety first

  Since the plant is the most affected by cyber-attacks, the manufacturing department is taking the lead in instructing various departments to respond and sharing information to deal with cyber-incidents. One characteristic of this pattern is that the plant-

first response may result in the deletion of information necessary for investigating the cause. As a result, the time required for recovery may be prolonged due to the inability to identify the areas to be recovered.

Therefore, for the manufacturing department to take the lead in responding to a cyber incident, they need to have knowledge of the plant and knowledge of the plant itself, and a good understanding of the impact of the incident on the business.

- Security first

  Since this is an abnormal situation caused by a cyber-attack, the department takes the lead in responding to the cyber incident by giving instructions and sharing information with various departments. The characteristic of this pattern is that the investigation of the cause of the cyber-attack is given priority. To ensure the plant's safety, the cause of the cyber-attack should be thoroughly investigated. However, investigating the cause may interfere with the plant's safety measures and put the plant in a dangerous situation. In addition, there is a possibility that the plant cannot be restored due to the investigation of the cause, resulting in damage to the business.

  Therefore, for the department to respond to a cyber incident, it is necessary to have knowledge of the plant and knowledge of the plant, and a good understanding of the impact of the incident on the business.

- Business first

  To respond to cyber-attacks that have a significant impact on the company's business, the company's top management plays a central role in instructing various departments to respond and share information to deal with cyber-incidents. The characteristics of this pattern are as follows. This pattern is characterized by the fact that the company's top management gives the instructions. This pattern is characterized by the fact that the instructions come from the company's top, which allows for a smooth response. However, if the plant is put in a dangerous state because the company's profit is the only consideration, or if the plant is unsafe

because the company's profit is the only consideration, then the plant may be damaged. However, in the interest of the company's profit, the plant may be dangerous, or information necessary for investigating the cause of abnormal plant operation may be deleted. Therefore, the management department should play a central role.

Hence, for management to take the lead in responding to cyber incidents, they must understand the business impact of the incident and have a thorough understanding of the plant.

Safety Response Confirmation Exercise is be held on December 11, 2020, 28 people participated, and the following questionnaire results were obtained (Max point is 140). From the results of this questionnaire, the people who participated in the exercise understood the purpose of the exercise that we set and received high praise for the exercise.

Questionnaire content for Card-Type Incident Response Exercise and ICS-BCP Creation Exercise:

1. Was the goal set for the exercise, and was it possible to attain it?
2. Do you think you learned about organizational collaboration in the event of a cyber incident?
3. Do you think you learned about the organizations needed to respond to cyber incidents?
4. Was the information necessary to proceed with the exercise given?

Questionnaire content for IMANE:

1. Was the goal set for the exercise, and was it possible to get it?
2. Do you think you learned about organizational collaboration in the event of a cyber incident?
3. Do you think you learned about the organizations needed to respond to cyber incidents?
4. Is it designed so that necessary information is communicated and given to each role?
5. Do you feel that you were able to experience information gathering and decision-making in an emergency?

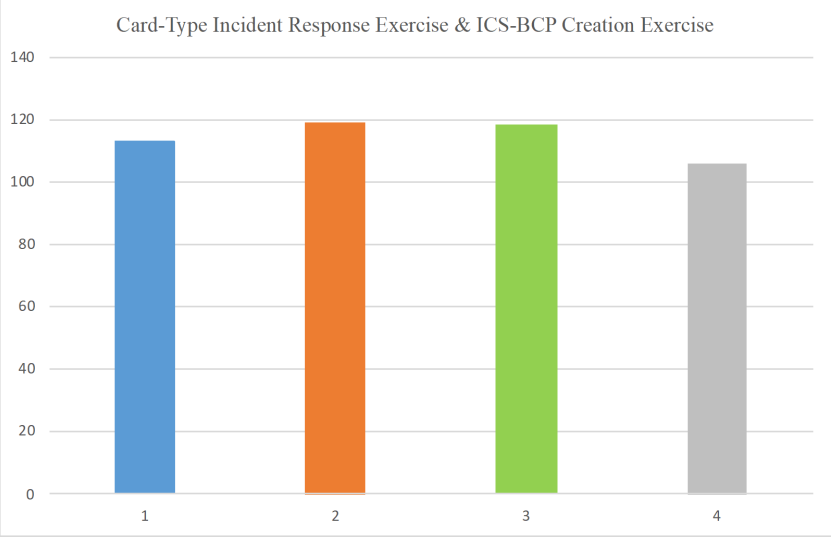

Figure 5.10: Questionnaire results of Card-Type Incident Response Exercise & ICS-BCP Creation Exercise

In addition, the following was found by analyzing the deliverable of the exercise.

- Plant safety first
  Many workflows can keep the plant safe, even if the backgrounds of the participants in the exercises vary. Even if the cause of the plant abnormality is a cyber-attack, it is easy to imagine the visible situation, and appropriate measures can be taken. .
- No action has been taken to identify a cyber-attack
  Analyzing the workflow, selecting situation sharing and actions for performing Safety Response is possible. However, information sharing for performing Security Response, such as identifying the range of influence of cyber-attacks, is often not successful. This is thought to be because they have never experienced cyber-attacks and lack the knowledge to consider actions. In addition, Safety Response is easy to imagine because it corresponds to the visible physical impact on the plant. Still, Security Response is difficult to imagine because it compares to the invisible network.
- Organization that is the center of the response
  To respond to cyber incidents to ICS, it is necessary to fluidly change the organization that is the core of the response.
  It must respond to plant operation abnormalities caused by cyber

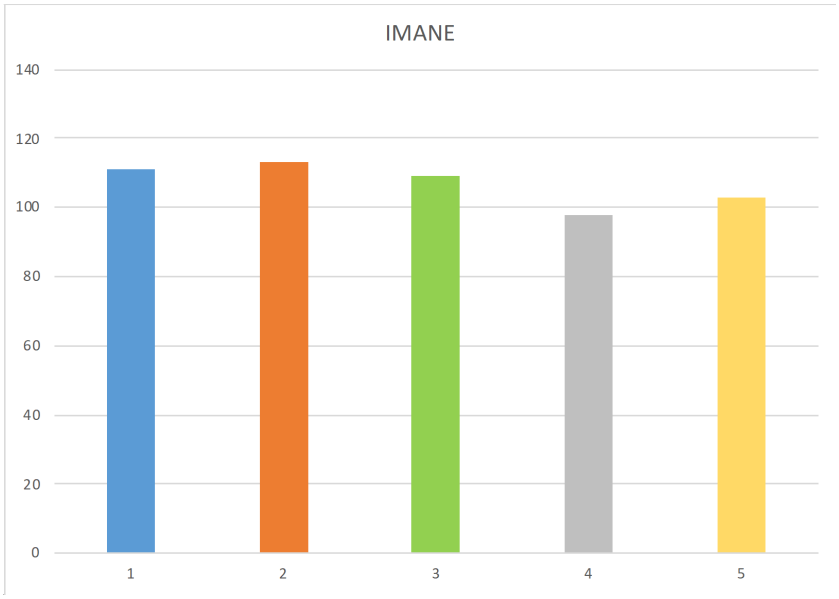

Figure 5.11: Questionnaire results of IMANE

incidents in the initial response. The person working at the plant takes action. After ensuring the plant's safety, it is necessary to eliminate the effects of cyber incidents. IT department takes this action. Finally, it is essential to continue the business considering the impact of the cyber incident on the business. Management considers actions for the business gains.

In this way, the work to be done changes over time, and it is necessary to respond while changing the organizational response that is the core of the response accordingly.

5.2.2 *Security Response Confirmation Exercise*

The scores of the exercise participants generally improved. We believe that the fact that they played the game a couple of times has an effect; however, we also think that, now that they understand the perspective of the attacker/defender, they can strategically choose their actions. The exercise participants gave positive feedback, saying that they were able to gain various things through the game; simultaneously, they were able to measure their growth by being evaluated by a score. However, the following areas for improvement were identified.

- Participants need to be made very aware of the intent of the exercise

  The game can be carried out even if choices are made without thinking. When playing on the Red side, it is essential to understand the attack methods. It is also necessary to understand that, as the attack phase progresses, the target of the attack changes. When playing on the Blue side, participants can choose actions under the managing constraints, such as budget and human resources. Participants, however, may not be aware of the inter-organizational cooperation required to perform counter-actions. Therefore, I believe that a mechanism to make participants aware of the purpose and intent of the exercise (e.g., adding content to the classroom lecture) is necessary.

5.3 CONCLUSION

In this chapter, I have created a scenario for the ICS security-aware exercise proposed in Chapter 3, using our testbed as an example, and presented the results of the pilot test as well.

After testing the presented exercise several times with participants with various experiences and backgrounds, we found that participants aware of the risks of cyber incidents were more focused on the exercise.□

In addition, even those who have little interest in ICS security in plants seem to have learned about the importance of cyber security and the necessity of responding to it through the exercise.

Although the exercise was developed based on the same scenario, the exercise methodology developed for the exercise seems to have allowed us to understand the purpose of the exercise we intended, recognize the differences between our company and the hypothetical company, and then discuss whether and how to apply it to the actual company.

6

DISCUSSION

The two solutions to the problems mentioned in Chapter 2 will be discussed throughout this study.

6.1 BUILDING ORGANIZATIONAL BEHAVIOR EXERCISES

To achieve the objective of the exercise, which is "to provide a forum for discussing organizational responses to cyber-attacks on control systems," I identified the scenarios necessary for the exercise and constructed the "plant operation simulation," "cyber-attack demonstration," "on-site response confirmation exercise," "safety response confirmation exercise," "IDEF exercise," and "IMANE" Based on the scenarios, we developed the "Plant Operation Simulation," "Cyber Attack Demonstration," "On-Site Response Confirmation Exercise," "Safety Response Confirmation Exercise," "IDEF Exercise," and "IMANE." Each exercise has a specific objective, and we have developed a method to achieve the goal. However, we have not developed a way to evaluate the validity of the structure of these exercises, and it is not possible to assess them objectively.

6.2 EDUCATIONAL METHODS USING ORGANIZATIONAL BEHAVIOR EXERCISES

Based on the organizational behavior exercise we developed, I proposed an educational method to improve resiliency. This method was implemented at the Industrial Cyber Security Center and received a certain level of evaluation. However, since there is no index to evaluate how the people who received this education have grown, it is necessary to

establish this index in the future to confirm the validity of the education method.

6.3 DISCUSSION OF THIS THESIS AS A WHOLE

In this study, we developed an organizational behavior exercise to improve resiliency and a teaching method using the exercise. Through this training, participants can experience the impact of cyber-attacks on control systems and learn the concept of organizational response, essential in incident response to cyber-attacks. In addition, it is possible to enhance the effectiveness of the exercise by providing the most appropriate exercise according to the objectives of the participants, rather than just taking the exercise. Finally, I believe that the participants will be able to examine the validity of the security measures considered through the exercises.

7

CONCLUSION

7.1 CONCLUSION OF THIS THESIS

This thesis aims to increase resilience to the risk of cyber incidents in OT systems. This thesis is composed of six chapters, each of the dealing with the different aspects of cyber security resilience.

- CHAPTER 1

  In chapter1, I explained that cyber-attacks are a risk that threatens the safety of ICS and the business continuity of companies, based on actual cases and cyber-attack demonstrations conducted in our laboratory.

  I then explained the efforts Japan is making to protect businesses from cyber-attacks.

- CHAPTER 2

  In chapter 2, I explained what Japanese companies are doing to protect their companies from cyber-attacks and the importance of business continuity planning and human resource development, assuming a cyber-incident occurs, in addition to creating a cyber-attack-resistant environment.

  To protect your business from cyber incidents, companies need to understand the differences between the incidents you have experienced and the actions companies need to take. I also explained that it is necessary to understand the organizations required to respond to cyber incidents and develop ICS-BCP in advance to react quickly. However, since it is impossible to develop a plan to respond to all cyber incidents□Hence the concept of resilience is used to protect companies from cyber incidents.

- CHAPTER 3

  In chapter3, I described the need to apply exercises to increase resilience capabilities to cyber incidents. In developing the exercises, we described the objectives and settings of the exercises we set up and told the activities we have created so far.

  The exercise we developed can be categorized into two types.

  The first is an exercise focusing on simulated experience. We use testbed owned by our laboratory to deepen exercise participants' understanding of the impact of cyber-attacks on ICS and the actual possible field-side action of the operators in the field.

  In this type of exercise, the participants can move their hands to deepen their understanding.

  The second is a simulation-type exercise in which participants simulate a response to a cyber incident as a member of a virtual company and discuss how to look at things to respond to a cyber incident.

  This type of exercise uses a straightforward scenario, making it easy for participants to apply the insights gained through the exercise to their own companies.

  The purpose and implementation of each exercise and the framework developed to design the exercise is explained.

- CHAPTER 4

  In Chapter4, I explained how to use the exercises described in Chapter 3 for human resource development who respond to cyber-incidents.

  Companies cannot maximize their resilience capacity simply by undergoing exercises. It is essential to provide the developed exercises according to the level and learning objectives of the exercise participants, and I explained the concept required to do so.

- CHAPTER 5

  In Chapter 5, I presented the exercises proposed in Chapters 3 and 4 and an example of how to conduct a human resource

development exercise using these exercises. I explained that the exercise can be based on our testbed and that the exercise can be tailored to the objectives.

□ In the proposed exercise, the participants were able first to understand what a cyber incident is in ICS through the simulation exercise and better understand the plant. In the tabletop exercise, the participants were able to discuss to strengthen their communication skills and share their thoughts and awareness of the issues among those with various backgrounds. This exercise was found to enhance resilience to cyber incidents and have aspects such as problem-solving and sharing of ideas with related departments that would cooperate during a cyber incident.

Many participants highly evaluated this exercise, and some of them said they would like to retake this course.

7.2 FUTURE WORK

Cyber-attacks have been discussed as a risk to plant safety in recent years, and many responses to cyber-attacks have been published. However, most research has focused on advanced measures, i.e., network structures, to create an environment less susceptible to cyber-attacks. In this study, I focus on the response after a cyber incident occurs, but the answer is also strongly influenced by the tools and environment prepared in advance. and, this research is not structured to observe and bridge before and after a cyber-attack. In addition, although we often receive high evaluations from the exercise participants, we have no way of confirming whether or not the participants of this exercise have increased their capability to deal with cyber incidents. Therefore, I believe that the following is the future work of this study.

- How to check for capacity building through exercises

  In addition to conducting the exercise, the purpose of the exercise is to build an organization that is resilient to cyber incidents. It is necessary to make an organization strong to make its human resources strong. Currently, it is not possible to measure whether

the exercises have improved the ability to deal with incidents. Therefore, it is necessary to establish a system to measure how the human resources have grown through the exercises.

- Methods of organizational and operational reform using exercises

  In this paper, I have been researching the subject of exercises to build a company that is resilient to cyber incidents.

  If it is possible to measure the improvement of skills through exercises quantitatively, it is highly likely to visualize the capabilities of human resources. This may provide many benefits, such as identifying key persons for organizational development and using them for career paths in companies. Therefore, it is necessary to continue research on quantitatively measuring the improvement of abilities and applying the exercises to business reform.

7.3 IMPLICATIONS

This research has been done on a trial-and-error basis. I made assumptions about what we thought would happen and created exercises as a mechanism to check whether our assumptions were correct or not. We found out that the assumptions we made were correct by doing the exercises, and we created exercises to prove our assumptions. As a result, we developed a training program to improve resilience capabilities to cyber incidents using exercises.

Initially, it would take a lot of time and resources to design and develop an exercise with specific information inputs to be rolled out to each company. However, this exercise is intended to be generalized using a simple exercise scenario, structure, and implementation method. It is also essential to focus on discussion and hot wash for exercises that have no answers, such as cyber incident response.

The exercises we have developed have their objectives, enabling us to deliver exercises according to the purposes of the exercise participants and allowing the exercise operators to focus on learning and reviewing the performance during the exercise.

This study concludes with the hope that more companies and organizations will adopt this exercise and start the cycle to be resilient to cyber incidents.

BIBLIOGRAPHY

[1] K. Stouffer, J. Falco, and K. Scarfone. *Guide to Industrial Control Systems (ICS) Security*. 2015. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[2] J. Frohm, V. Lindstrom, M. Windroth, and J. Stahre. "The industry's view on automation in manufacturing." In: *In: IFAC Proceedings Volumes 39.4* (2006), pp. 453–458.

[3] R. Shell. "Handbook of industrial automation". In: *CRC Press* (2000).

[4] Institute for Science and International Security. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* 2010. URL: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-Natanz-enrichment-plant/8.

[5] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. *Cyber-Attack Against Ukrainian Critical Infrastructure*. URL: https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[6] HITACHI,Ltd. *Hitachi Review, 2018 vol.100, No.3*. URL: https://www.hitachihyoron.com/jp/archive/2010s/2018/03/05b02/index.html.

[7] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. *PIPELINE CYBERSECURITY INITIATIVE*. URL: https://www.cisa.gov/pipeline-cybersecurity-initiative.

[8] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. *Alerts*. URL: https://www.cisa.gov/uscert/ncas/alerts.

[9] T. Aoyama, M. Koike, I. Koshijima, and Y. Hashimoto. "A unified framework for safety and security assessment in critical infrastructures". In: *In: Safety and Security Engineering V. WITPRESS LTD* (2013).

[10] *Metasploit Framework*. URL: https://www.metasploit.com/.

[11] New Energy and Industrial Technology Development Organization. *Cross-ministerial Strategic Innovation Promotion Program (SIP) Second Phase: Cyber-Physical Security for IoT Society*. URL: https://www.nedo.go.jp/english/activities/ZZpage_100140.html.

[12] National center of Incident readiness and Strategy For Cybersecurity. *About NISC*. URL: https://www.nisc.go.jp/eng/index.html#sec1.

[13] Information-technology Promotion Agency(IPA). *Industrial Cyber Security Center of Excellence (ICSCoE)*. URL: https://www.ipa.go.jp/icscoe/english/index.html.

[14] Y. Ota, T. Aoyama, N. Davaadorj, and I. Koshijima. "Cyber Incident Exercise for Safety Protection in Critical Infrastructure". In: *Int J. Saf. Secur. Eng. 8* (2018), pp. 246–257.

[15] Progressive Management. *21st Century U.S. Military Documents: Cyber Incident Handling Program (Chairman of the Joint Chiefs of Staff Manual) - Computer Forensics, Malware and Network Analysis, CYBERCON*. Progressive Management, 2015.

[16] M. Kitamura. "New Concept of Safety Pursued and Implemented by Resilience Engineering". In: *IEICE ESS Fundamentals Review* 8 (2014), pp. 84–95. ISSN: 1882-0875. DOI: 10.1038/nature24010. URL: https://doi.org/10.1587/essfr.8.84.

[17] A. Jahromi, S. Hashemi, A. Dehghantanha, K.-K. R. Choo, H. Karimipour, D. Newton, and R. M. Parizi. "An improved two-hidden-layer extreme learning machine for malware hunting". In: (2019). URL: https://doi.org/10.1016/j.cose.2019.101655.

[18] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour. "A survey on internet of things security: requirements, challenges, and solutions. Internet Things". In: (2019). URL: https://doi.org/10.1016/j.iot.2019.100129.

[19] Kaspersky Lab. *Kaspersky Security Awareness*. URL: https://www.kaspersky.com/enterprise-security/security-awareness.

[20] slack. URL: https://slack.com/.

[21] Integrated DEFinition Methods (IDEF). *IDEFo Function Modeling Method*. URL: https://www.idef.com/idefo-function_modeling_method/.

[22] H. Hirai, T. Aoyama, N. Davaadorj, and I. Koshijima. "FRAMEWORK FOR CYBER INCIDENT RESPONSE TRAINING". In: *WIT Transactions on The Built Environment* 174 (2018), pp. 273–283. URL: https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/174/36521.

[23] ThretGen. *Red vs. Blue Gamification*. URL: https://threatgen.com/red-vs-blue/.

[24] NIST. *CYBERSECURITY FRAMEWORK*. URL: https://www.nist.gov/cyberframework/framework.

[25] LOCKHEED MARTIN. *THE CYBER KILL CHAIN*. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[26] F. Bracco, T. Francesco, and G. Dorigatti. "TURNING VARIABILITY INTO EMERGENT SAFETY: THE RESILIENCE MATrIX FOR PROVIDING STRONG RESPONSES TO WEAK SIGNALS". In: *PROCEEDINGS 5th REA SYMPOSIUM MANAGING TRADE OFFS* (2014), pp. 23–28. URL: https://www.resilience-engineering-association.org/wp-content/uploads/2016/09/Frontpage-REA5SYM-proceedings-030916.pdf.

[27] I. Kato, Y. Ota, and I. Koshijima. "Fundamental Consideration on Lean and Agile Program Management -Reconsideration of Innovation Processes for Nurturing Innovators-". In: *Journal of International Association of P2M* 13 (2019), pp. 60–80. DOI: 10.1038/iappmjour.12.2_60. URL: https://doi.org/10.20702/iappmjour.13.2_60.

[28] The Nikkan Kogyo Shimbun, Mech. Des. 62, 41-44(2018).