

CONTROL SYSTEMS SECURITY AND COMMUNICATION

Achieving Organizational Resilience through Exercise

制御システムセキュリティとコミュニケーション
- 演習で実現する組織レジリエンス

TOMOMI AOYAMA



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

September 2019

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 six chapters, each of them dealing with the different aspects of cyber security design and execution.

CHAPTER 1 Chapter 1 is introductory and describes how cybersecurity risk becomes more and more relevant to industrial systems and critical infrastructures and its potential impacts.

CHAPTER 2 In this chapter, we examine the available resources to understand the trends and definition of the field. The chapter consists of 3 sections. Section 1 reviews the literature in the related field to define exercises. Section 2 investigates current Industrial Control System security exercises available in the field. We discuss the limitation of the conventional approach. Section 3 illustrates the trends specific to the Japanese market and what makes it peculiar.

CHAPTER 3 The interaction between two parties makes cyber incident response unique in comparison with natural hazards. We discuss the uniqueness of the field from three perspectives; 1) the time-lag of the adversarial interaction, 2) the shift of focused activities, and 3) the management challenges. In this chapter, we investigate the nature of incident management by observation studies at a large scale adversarial exercise.

CHAPTER 4 ICS security exercise should be designed and applied proportional to the organization's preparedness. This chapter introduces the model to be applied to design the exercise from three axes: exercise participant, exercise style, and the goal of the exercise. The chapter illustrates how exercises can play the role of a driving power

to improve an organization and community's cyber security preparedness. We discuss the details for how the model should be applied to understand the existing exercises. It highlights the limitation of current cyber security exercise landscape.

CHAPTER 5 Achievement of a secure and resilient society requires a shared protocol among stakeholders. Even within the organization, cyber incident communication is a challenge because of the conflicting value of safety and security. We designed the training program specifically to address this problem in align with the maturity-based exercise model presented in chapter 4. Exercises designed for this program are introduced in this chapter.

CHAPTER 6 Conclusion. This interdisciplinary study was based on an investigation of both organizational behavior and exercise management. Discussion-based exercise tailored to the organizations' maturity cultivates a shared mental model among participants. We conclude that exercises can play the role of a driving power to improve an organization and community's cyber security preparedness. In this chapter, we conclude the study by discussing the exercise management implications, the research implications, and the implications for the organization behavior.

PUBLICATIONS

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

- [1] T. Aoyama, M. Koike, I. Koshijima, and Y. Hashimoto. "A unified framework for safety and security." In: *Safety and security engineering V* 134 (2013), p. 67.
- [2] M. Matta, M. Koike, W. Machii, T. Aoyama, H. Naruoka, I. Koshijima, and Y. Hashimoto. "Industrial control system monitoring based on communication profile." In: *Journal of Chemical Engineering of Japan* 48.8 (2015), pp. 619–625.
- [3] T. Aoyama, H. Naruoka, I. Koshijima, and K. Watanabe. "How management goes wrong?—The human factor lessons learned from a cyber incident handling exercise." In: *Procedia Manufacturing* 3 (2015), pp. 1082–1087.
- [4] H. Naruoka, M. Matsuta, W. Machii, T. Aoyama, M. Koike, I. Koshijima, and Y. Hashimoto. "ICS HoneyPot System (CamouflageNet) based on attacker's human factors." In: *Procedia Manufacturing* 3 (2015), pp. 1074–1081.
- [5] H. Eguchi, T. Aoyama, K. Seki, D. O'Donovan, and I. Koshijima. "Organizational structure on the resilience of production processes based on artificial factors in the chemical industry." In: *Journal of the Institute of Industrial Applications Engineers* 3.3 (2015), pp. 141–147.
- [6] H. Eguchi, T. Aoyama, K. Seki, and I. Koshijima. "Optimal Personnel Reallocation based on the Skills and Knowledge in The Chemical Industry." In: *Journal of the Institute of Industrial Applications Engineers* 3.3 (2015), pp. 126–133.
- [7] H. Eguchi, T. Aoyama, K. Seki, D. O'Donovan, and I. Koshijima. "A Metric for Quantitative Estimation of Production Process Resilience Based on the Skills and Knowledge of Production Plant Personnel in the Chemical Industry." In: *Journal of Chemical Engineering of Japan* 49.1 (2016), pp. 35–41.
- [8] T. Aoyama, H. Naruoka, I. Koshijima, W. Machii, and K. Seki. "Studying resilient cyber incident management from large-scale cyber security training." In: *Control Conference (ASCC), 2015 10th Asian*. IEEE. 2015, pp. 1–4.

- [9] W. Machii, I. Kato, M. Koike, M. Matta, T. Aoyama, H. Naruoka, I. Koshijima, and Y. Hashimoto. "Dynamic zoning based on situational activities for ICS security." In: *Control Conference (ASCC), 2015 10th Asian*. IEEE. 2015, pp. 1–5.
- [10] H. Eguchi, K. Seki, T. Aoyama, and I. Koshijima. "Optimal job routine assignment for the improvement of operational resilience based on skills and knowledge of production staff in the chemical industry." In: *Soft Computing and Intelligent Systems (SCIS), 2014 Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium on*. IEEE. 2014, pp. 861–866.
- [11] M. O. Diallo, S. Aoki, T. Aoyama, and K. Watanabe. "Evaluation of the Effectiveness of Modern Communication Channels During Emergency Situations." In: *WIT Transactions on The Built Environment* 173 (2017), pp. 131–142.
- [12] H. Shintani, T. Aoyama, and I. Koshijima. "Study on High Resilient Structures for IoT Systems to Detect Accidents." In: *Journal of Disaster Research Vol* 12.5 (2017), p. 1073.
- [13] T. Aoyama, T. Nakano, I. Koshijima, Y. Hashimoto, and K. Watanabe. "On the Complexity of Cybersecurity Exercises Proportional to Preparedness." In: *Journal of Disaster Research Vol* 12.5 (2017), p. 1081.
- [14] T. Aoyama, k. Watanabe, I. Koshijima, and Y. Hashimoto. "Developing ICS Security Training for Resilient Cyber Incident Management." In: *Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes (PSE Asia 2016)* (July 2016).
- [15] Y. Ota, T. Aoyama, D. Nyambayar, 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.
- [16] H. Hirai, T. Aoyama, D. Nyambayar, and I. Koshijima. "Framework for Cyber Incident Response Training." In: *WIT Transactions on The Built Environment* 174 (2018), pp. 273–283.

ACKNOWLEDGMENTS

I would like to thank Prof. Watanabe, Prof. Hashimoto, and Prof. Koshijima 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.

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.

CONTENTS

1	INTRODUCTION	1
1.1	Increasing Cyber Threat in Critical Infrastructure . . .	1
1.1.1	Effect of Cyber Attack on Industrial Control System	1
1.1.2	Industrial Control System Structure	2
1.1.3	Benefit of Automation	2
1.1.4	Impact of Cyber Attack targeting Industrial Control System	4
1.1.5	Shattered Myth of Control Systems Security . .	4
1.1.6	Business Continuity	5
1.2	Cyber Incident Response Training	6
1.3	Measuring the Cyber Security Maturity of Organization	7
1.3.1	Cybersecurity Capability Maturity Model	8
1.3.2	IEC 62443	9
1.3.3	World Economic Forum	9
1.3.4	NIST Cyber Security Framework	10
2	ICS SECURITY EXERCISE LANDSCAPE	17
2.1	Literature Review	17
2.1.1	What is Exercise?	17
2.1.2	Establishing the Terminology	20
2.2	Available Exercises	21
2.2.1	Capture The Flag	21
2.2.2	Game: Kaspersky Industrial Protection Simulation	22
2.2.3	Drill: ICS Cyber Security Exercise by CSSC . . .	24
2.2.4	Table-top Exercise: Critical Infrastructure Incident Response Exercise by NISC	24
2.3	Conclusion	25
3	UNDERSTANDING THE NATURE OF THE CYBER INCIDENT MANAGEMENT	27
3.1	Field of Study	27
3.1.1	Red Team - Blue Team Exercise Overview . . .	28
3.1.2	Typical Scenario of Red-Blue Exercise	29
3.1.3	Simulation Gaming	30

3.1.4	Designed Challenges in the Exercise	31
3.2	Asymmetrical Timeline	32
3.2.1	Attacker Free Time	32
3.2.2	Observation Conducted	33
3.2.3	Exercise Scenario under Microscope	35
3.2.4	Observed Behavior	37
3.2.5	Results	39
3.3	Adaptive Resource Allocation	40
3.3.1	Observation Conducted	40
3.3.2	Red Team Activities	40
3.3.3	Shift of Defence Activities in Blue Team through the Game	40
3.3.4	Cyber Defence as a Crisis Management in Esca- lating Situation	42
3.3.5	Discussion: the Cause of Defeat	43
3.4	Management Challenges	44
3.4.1	Time Critical Decision Making with High Un- certainty	44
3.4.2	Management Challenges and Decision Making Trade-offs	44
3.4.3	Transition of Control Mode	45
3.4.4	Challenges and Control Modes	47
3.5	Conclusion	48
4	EXERCISE DESIGN FRAMEWORK	51
4.1	Maturity and Exercises	51
4.2	Exercise Classification for Scope Tailoring	52
4.2.1	Range of Participants	52
4.2.2	Exercise Styles	54
4.2.3	Exercise Aim	57
4.3	Exercise Program Design Framework	58
4.4	Conclusion	60
5	EXERCISE DEVELOPMENT UNDER UNIFIED STRUCTURE	63
5.1	Exercise Program Design	63
5.1.1	Designing a Curriculum	63
5.1.2	Goals of the Program	65
5.1.3	Method: Discussion-Based Exercise	66
5.2	Exercise Environment	66

5.2.1	NI Tech Testbed	66
5.2.2	Testbed Structure	67
5.3	Core Scenario Development	69
5.3.1	Company Profile	70
5.3.2	Attack Scenario	71
5.3.3	Defense Scenario for Plant Operation	73
5.3.4	Roles Defined	75
5.3.5	Scenario Phases	75
5.4	Gaming: Communication Training with KIPS+	78
5.4.1	Gaming Simulation Structure of KIPS	78
5.4.2	Inter-organization Cooperation	78
5.4.3	Proposed Exercise Method	80
5.4.4	Implementation and Trial	81
5.5	Functional Exercise: TsurumaiGO	82
5.5.1	Incident Commanding Structure	82
5.5.2	Proposed Exercise Structure	83
5.5.3	Prototyping	86
5.5.4	Implementation of TsurumaiGo	87
5.6	TTX: Workflow Exercise Design	89
5.6.1	Exercise Steps	89
5.6.2	White Teaming	91
5.6.3	Detailed Attack Scenario	92
5.6.4	Exercise Feedback Cycle	97
5.7	Practical Appraisal of Developed Exercises	98
5.7.1	Pilot Exercises with Experts	98
5.7.2	Survey Result of Pilot Exercises	98
5.7.3	Variation of Incident Management Structure	99
5.7.4	Discussions	101
5.8	Conclusion	101
6	CONCLUSION	103
6.1	Conclusion of This Thesis	103
6.2	Implications	106
A	APPENDIX: RELATED PUBLICATIONS TO UNDERSTAND THIS THESIS	109
A.1	Unified Framework to Describe Cyber Incident	111
A.2	Cyber Incident Crisis Communication	123
A.3	Cyber Incident Exercise Facilitation	131

B	APPENDIX: CASE STUDY FOR APPLYING PROPOSED FRAME- WORK	143
B.1	Case Study: Critical Infrastructure Incident Response Exercise by NISC	143
C	APPENDIX: EXERCISE MATERIALS	149
C.1	Example of TTX Deliverable	151
C.2	KIPS+ Operation Manual	177
C.3	TsurumaiGo Operation Manual	189
C.4	Card-based TTX Operation Manual	245
	BIBLIOGRAPHY	253

LIST OF FIGURES

Figure 1.1	Basic control structure [3]	3
Figure 1.2	Shattered Myths of secure Industrial Control System environment.	5
Figure 1.3	Cybersecurity Capability Maturity Model architecture[31].	8
Figure 1.4	Mesh use of maturity level with Security Level in IEC 62443[34].	10
Figure 1.5	Cyber resilience maturity model by World Economic Forum[35].	11
Figure 2.1	Types of exercise proposed in NIST Special Publication 800-84 -Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities- [38] and Homeland Security Exercise and Evaluation Program (HSEEP) [37]	18
Figure 2.2	Rasmussen’s model of three level behavior [40].	19
Figure 2.3	Game phases of Kaspersky Industrial Protection Simulation	22
Figure 2.4	Outline of Kaspersky Industrial Protection Simulation. Pictures from the website[44].	23
Figure 2.5	Exercise process of Control Systems Security Center training[46]	24
Figure 2.6	Outline of Control Systems Security Center training.	25
Figure 2.7	Mapping exercises available in Japan.	26
Figure 3.1	Red team participants engaging the exercise.	28
Figure 3.2	Role of the participants during the exercise.	29
Figure 3.3	Activity timeline of the exercise.	30
Figure 3.4	Room arrangement for the blue team.	32
Figure 3.5	Blue team’s network structure provided to the red team.	32
Figure 3.6	Network map provided to the blue team.	33
Figure 3.7	Cyber Kill Chain®[51]	34

Figure 3.8	Attack life cycle presented in NERC HILF report[52].	35
Figure 3.9	Cause analysis of attacker free time	35
Figure 3.10	The route of power switch hack scenario.	36
Figure 3.11	Event log of the activities related to the power switch hack.	38
Figure 3.12	The red team’s activity timeline.	40
Figure 3.13	Shift of blue team activities throughout the day.	41
Figure 3.14	Blue team activities divided in four phases.	41
Figure 3.15	Observed shift of control mode.	47
Figure 4.1	The guideline for exercise configuration with respect to each tier	53
Figure 4.2	Mapping of exercise styles into the category of targeted achievement	55
Figure 4.3	Difference of expected effects from exercise and drill.	57
Figure 4.4	Achieving resilience requires awareness and preparedness as its foundation.	59
Figure 4.5	Relation between the maturity and exercise goals.	60
Figure 5.1	Proposed cyber resilience exercise program.	64
Figure 5.2	The plant side (left) and the operator side (right) of the testbed. Testbed visitors can operate the system during the demonstration.	67
Figure 5.3	Network architecture of the testbed.	68
Figure 5.4	Piping and Instrumentation Diagram of the testbed.	68
Figure 5.5	Exercise design procedure and points of company uniqueness.	70
Figure 5.6	Roles and communication paths defined in the exercise.	76
Figure 5.7	Stages of disruption proposed by Y.Sheffi [64], recreated by the authors.	76
Figure 5.8	Kaspersky Industrial Protection Simulation structure.	79
Figure 5.9	Kaspersky Industrial Protection Simulation+ structure.	81
Figure 5.10	TsurumaiGo exercise structure.	85

Figure 5.11	User Interface of TsurumaiGo.	87
Figure 5.12	Action User Interface of TsurumaiGo.	87
Figure 5.13	Example deliverable of the exercise.	88
Figure 5.14	Exercise plan overview.	89
Figure 5.15	The example of the worksheet (left) and pictures from the exercise (right) where participants engage in group work (top right) and present their group work at discussion time (bottom right). Participants' faces are blurred out for their privacy.	90
Figure 5.16	Facilitation Structure.	92
Figure 5.17	Abnormally caused in the testbed plant system.	94
Figure 5.18	Selected events - In the safety, the first line caused the risk, and as a result, the second and subsequent lines indicate the cause.	95
Figure 5.19	Organizing Scenario using FTA	96
Figure 5.20	Cyber attack scenario shown on the network map.	97
Figure 5.21	PDCA feedback cycle of the exercise.	98
Figure 5.22	Participant's profile distribution.	99
Figure 5.23	Observed communication structure design in the exercise.	99
Figure B.1	Exercise structure of CIIREX.	143
Figure B.2	Observed participation styles.	145

LIST OF TABLES

Table 1.1	Potential impact of successful cyber attack on Industrial Control System [4].	13
Table 1.2	Maturity Indicator Level Characteristics proposed in Cybersecurity Capability Maturity Model	14
Table 1.3	Example use of MIL in Cybersecurity Capability Maturity Model.	15
Table 3.1	Organizational resilience indicator and corresponding activities observed in the field	42
Table 3.2	Characteristics for the four control modes in terms of number of goals, available time, evaluation and how actions are selected [58]. . . .	46
Table 3.3	The four control modes and its relation to observed challenges.	49
Table 5.1	Procedure for the cyber-attack scenario	72
Table 5.2	The maximum goal and risk of the company for cyber-attack	93
Table 5.3	Design procedure of the cyber-attack scenario for the testbed	96

ACRONYMS

BCM	Business Continuity Management	61
BCP	Business Continuity Planning	65
CCTV	Closed-Circuit Television	2
CI	Critical Infrastructure	1
CIIREX	Critical Infrastructure Incident Response Exercise	58
CIP	Critical Infrastructure Protection	66
COCOM	Context Control Model	45
CSSC	Control Systems Security Center	24
CTF	Capture The Flag	21
C2M2	Cybersecurity Capability Maturity Model	8
DDoS	Distributed Denial of Service	144
ENCS	European Network for Cyber Security	28
GUI	Graphical User Interface	4
HMI	Human Machine Interface	2
HSEEP	Homeland Security Exercise and Evaluation Program	18
HVAC	Heating, Ventilation, and Air Conditioning	2
IACS	Industrial Automation and Control Systems	9
ICS	Industrial Control System	1
IDS	Intrusion Detection System	34
IEC	International Electrotechnical Commission	8
ISA	International Society of Automation	9
ISO	International Organization for Standardization	19
IT	Information Technology	27
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center	144
KIPS	Kaspersky Industrial Protection Simulation	22
MIL	Maturity Indicator Level	8
NISC	National Information Security Center of Japan	24
NIST	National Institute of Standards and Technology	8
NITECH	Nagoya Institute of Technology	64
OPC	Open Platform Communication	96
PDCA	Plan Do Check Act	97

PID	Piping and Instrumentation Diagram	68
PLC	Programmable Logic Controller	2
RTBT	Red Team - Blue Team	28
RTU	Remote Terminal Unit	
SAL	Security Assurance Level	9
SCADA	Supervisory Control And Data Acquisition	69
SLC	Single Loop Controller	68
TTX	Table-top Exercise	64
UI	User Interface	86
WEF	World Economic Forum	9
WEP	Wired Equivalent Privacy	36

INTRODUCTION

Chapter 1 is introductory and describes how cyber security risk becomes more and more relevant to industrial systems and critical infrastructures and its potential impacts.

1.1 INCREASING CYBER THREAT IN CRITICAL INFRASTRUCTURE

1.1.1 *Effect of Cyber Attack on Industrial Control System*

Cyber attacks on CI¹ are no longer a theoretical, but a real problem since the discovery of the Stuxnet worm in July 2010. Stuxnet is a threat that was primarily designed to target an ICS² or a set of similar systems. Industrial control systems are used in gas pipelines, power plants, chemical and petrochemical plants. The ultimate goal of Stuxnet is to sabotage these facilities by reprogramming Programmable Logic Controllers to operate as the attackers intend them to, most likely out of their specified boundaries[1]. Well-designed ICS worms have been deployed after Stuxnet.

Security researchers believe that the goal of the next generation of malware is not to harm people, but to quietly stop production at a utility, or impact the production of a rival, or short sell the shares of a company or extort money under the threat of a disruption[2]. There-

¹ Critical Infrastructure

² Industrial Control System

fore, a cyber security hazard is not only about computer malfunction but is also affecting safety and business continuity of CI.

1.1.2 *Industrial Control System Structure*

ICS are used in many industrial sectors. There are two processes categories. Continuous manufacturing processes are typically used in a power plant, a refinery, and a chemical plant. In the process with distinct processing steps, batch manufacturing processes are used. ICS can be used to control systems in remote locations, such as pipelines, electrical power grids, and railway transportation systems[3].

CONTROL LOOP. ICS contains many control loops, human interfaces, and remote diagnostics tools. A control loop utilizes sensors, actuators, and controllers (such as PLC³) to manipulate controlled processes.

INTERFACE. Human operators use HMI⁴ to monitor, configure, and adjust the parameters. Diagnostics and Maintenance utilities are used to prevent and recover from failures.

DATA HISTORIAN. The process data is often stored in one or more data historian systems. Then the information can be analyzed for quality control purposes. Other assets in the network may be valuable for analysis too, such as HVAC⁵ systems, CCTV⁶, and access control systems. The functionality of data historians led the process-specific data historization to operation-wide business intelligence [4].

1.1.3 *Benefit of Automation*

When control systems get connected to the network and increased the automation of the process, industries started to grow rapidly. Current

³ Programmable Logic Controller

⁴ Human Machine Interface

⁵ Heating, Ventilation, and Air Conditioning

⁶ Closed-Circuit Television

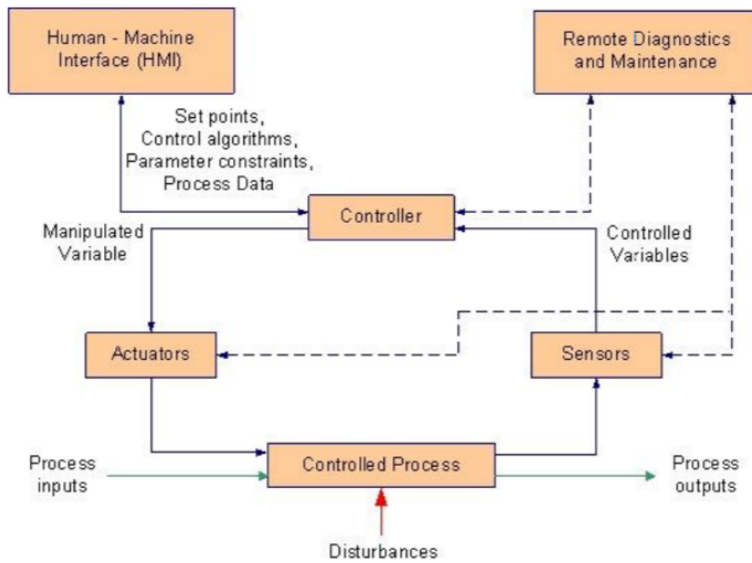


Figure 1.1: Basic control structure [3]

economical growth is the result of the rapid technological progress with the development of information technologies in 1970s[5].

The benefit of automation varies[6]; increase of productivity, decrease of costs[7], improvement of production efficiency, and enhancement of operational safety[8]. Affordable tools no longer require huge capital investments, and digital tools connected designing and manufacturing process[9].

Specifically to ICS, following advantages changed the way we interact with the production system.

LARGE AREA DISTRIBUTION. Electric power grid, traffic control systems, pipelines, and offshore oil platforms - many critical services are enabled thanks to the wide connectivity of network.

REMOTE CONTROL. Remote control allowed us to manage otherwise dangerous systems - such as nuclear reactor and chemical processing. Operators can monitor and control the process from the safe distance. Operation status can be monitored from offsite, including the offsite office space and maintenance site.

INCREASED VISIBILITY. Operators can supervise the system from GUI⁷. Comprehensive understanding of the process is no longer necessary to operate ICS. The system is well connected to the production scheduling systems, enabling the flexible manufacturing without the interference of the human operator. The operator's job is reduced to supervise the system to work as planned.

1.1.4 *Impact of Cyber Attack targeting Industrial Control System*

Control system is responsible for manufacturing process, and disturbance to the operation of ICS can cause the physical damage. Knapp et al. categorized the consequences of successful cyber incident as table 1.1.

- Delay, block, or alter the intended process, that is, alter the amount of energy produced at an electric generation facility.
- Delay, block, or alter information related to a process, thereby preventing a bulk energy provider from obtaining production metrics that are used in energy trading or other business operations.
- Unauthorized changes to instructions or alarm thresholds that could damage, disable or shutdown mechanical equipment, such as generators or substations.
- Inaccurate information sent to operators could either be used to disguise unauthorized changes (see Stuxnet later in this chapter), or cause the operator to initiate inappropriate actions.

1.1.5 *Shattered Myth of Control Systems Security*

Since the appearance of the Stuxnet malware in 2012 [10], targeted malicious cyber attack has become a realistic thread to critical infrastructure. The Stuxnet malware was designed to infect a commonly used industrial control systems device in the energy, nuclear, and other critical sectors. Initially delivered via an infected flash drive, Stuxnet

⁷ Graphical User Interface

was crafted to exploit multiple zero-day vulnerabilities to gain access to its target device and inject code to change process.

Nowadays, plant instrumentation systems are composed of versatile operating systems, software and hardware, which are vulnerable to targeted cyber attack. In addition, security patches are difficult to be applied in real time systems because they requires system shutdown. Thus systems remain unprotected. In critical infrastructures it is important to keep operating services even under a cyber attack, which requires organizations high resilience; the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions [11].

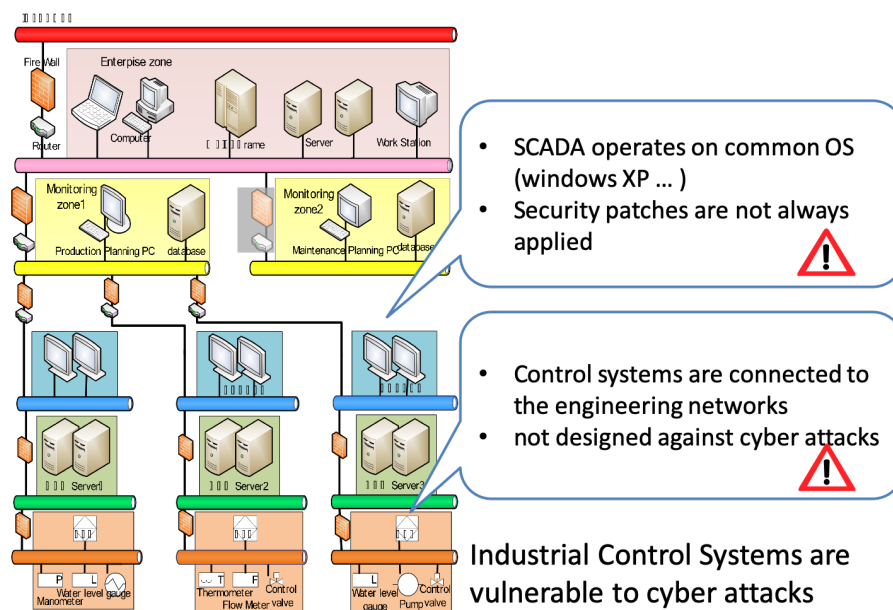


Figure 1.2: Shattered Myths of secure Industrial Control System environment.

1.1.6 Business Continuity

A sophisticated and targeted cyber attack can endanger safety and business continuity. In December 2015, an Ukrainian power grid underwent a cyber attack which caused approximately one hour of service outage[12].

For CI owners, cyber attacks are no longer a theoretical problem. The interdependence of CI is increasing the complexity of the entire system. In the highly connected society as nowadays, infrastructures

are connected physically, geographically, logically, and in cyberspace [13]. A disruption on a CI may cause impact across other CI sectors. More complex the system, the harder to mitigate its vulnerability. Planning contingency plan for every possible scenario of CI breakdown is not feasible. Rather, preparation for such a crisis needs to focus on increasing resiliency in response [14].

1.2 CYBER INCIDENT RESPONSE TRAINING

Emergency response training plays a major role to prepare the personnel for incident management [15]. The personnel faces many problems that are not encountered in training for routine operations [16]. Specifically, business continuity management exercises often adopt the "worst-case scenario" to train the response capability beyond the plan [17].

One of the leading cyber security incident response training in the field of ICS security is the ICS-CERT's 5 days training which includes a Red-team/Blue-team exercise. In this exercise, participants play the role of either the attacking (Red) or the defending (Blue) teams [18]. Similar adversarial exercises are provided by other key centres in the world, such as Queensland Institute of Technology in Australia [19, 20], and European Network for Cyber Security (ENCS) in the Netherlands.

The entire exercise is set up in a secure environment [21] for participants to experience how an organization can be compromised by a cyber attack. It should be noted that the exercise focuses on the impact of a cyber attack on a single organization, rather than on the whole CI stakeholder community. However, we believe that it represents one of the most recognized exercises in the field of ICS security. Therefore, we devote this subsection to the description of its characteristics.

Branlat et al. [22, 23] studied the exercise operated by ICS-CERT, and pointed out that the realistic timeline of the exercise allows participants to simulate the complexity of incident handling. Encouraged by their work, we have been studying the dynamic adaptation of organizations' decision-making structures, by monitoring the training of ENCS [24, 25].

Our on-site observation confirmed that the environment of the exercise provides valuable lessons regarding cyber incident management. Indeed, the reproducibility and the realistic timeline of the exercise allow participants to have an authentic experience. Moreover, it is a rare opportunity to establish technical skill-sets required in cyber defense, and to see how certain skills can impact the target system within the dynamics of a cyber attack.

Arguably, one of the most noticeable strengths of the exercise is the heterogeneous background and expertise of the participants and facilitators. In fact, team-working among these professionals provides a new perspective to their mental model and enhances the impact of the training.

However, considering the technicality and the intensive nature of the exercise - even though it portrays the realistic speed of a cyber attack —, participants focus on their immediate task leaving little time for communication with each other, let alone for sharing ideas towards better incident management. As a result, the exercise does not explicitly provide a structured framework to learn about the importance of communication and cooperation among the different departments of an organization or across organization boundaries.

Participants are not guided in understanding how an effective communication of their technical knowledge could influence the decision-making. Moreover, they are not taught to see the bigger picture, making it difficult for them to comprehend how dynamically the organization's communication structure should adapt to the timeline of a cyber attack.

1.3 MEASURING THE CYBER SECURITY MATURITY OF ORGANIZATION

The level of cyber security preparedness varies significantly among organizations. This implies that training and exercises must be tailored with respect to preparedness. In this paper we review a framework that formalizes a method to measure the degree of preparedness. Maturity model can be used to review an organization's security capa-

bilities[26]. A maturity model can provide a benchmarks to evaluate the achieved security practices, processes, and methods to set priorities for investment[27]. There are limited numbers of ICS security guidelines with maturity model. Here, we review the maturity models designed specifically to ICS security (C2M2⁹, IEC¹⁰ 62443), and non-ICS specific security (NIST¹¹ Cybersecurity Framework, World Economic Forum’s hyperconnection readiness curve).

1.3.1 Cybersecurity Capability Maturity Model

C2M2 Program was established to improve electricity sub-sector cyber security capabilities[28] as a public-private partnership effort. Other than the energy sector[29], C2M2 is applied to oil and gas sector[30] and IT services[31]. The model is focused on the implementation and management of cyber security controls. C2M2 uses Maturity Indicator Levels to measure the progression. All sub-sector guidelines include MIL¹² based measurement as the core framework.

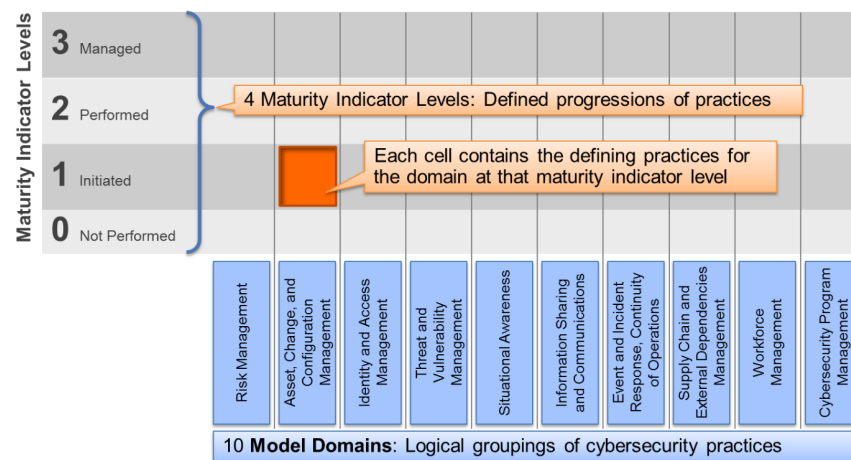


Figure 1.3: Cybersecurity Capability Maturity Model architecture[31]

A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline[27]. C2M2 uses four levels; MILs 0-3. Overview of each level’s characteristics is shown in table 1.2. MILs are used in combination

⁹ Cybersecurity Capability Maturity Model

¹⁰ International Electrotechnical Commission

¹¹ National Institute of Standards and Technology

¹² Maturity Indicator Level

with the security control domains(Figure 1.3), and domain specific MIL is specified. Table 1.3 shows the example use of MIL and domains.

1.3.2 IEC 62443

IEC 62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure IACS¹³[32] based on ISA¹⁴99. The standard introduced the basic ICS environment structure with the concept of zones and conduits, and SAL¹⁵.

According to Exida[33], the axis of maturity is as follows;

- Maturity Level 1 – Ad-hoc process
- Maturity Level 2 – Documented process, but not necessarily repeatable
- Maturity Level 3 – Documented process that is repeatable and consistently followed
- Maturity Level 4 – Documented process that is repeatable, consistently followed, measured, and steadily improved

The maturity level introduced in IEC 62443 is similar to MIL's four levels. In 62443, maturity level is designed to use as the secondary axis to SAL(Figure 1.4).

1.3.3 World Economic Forum

WEF¹⁶ introduced five staged cyber resilience maturity model as the tool to review the organizations cyber resilience capability towards hyper connected world[35]. In the hyperconnection readiness curve, the maturity is defined in five levels; unaware, fragmented, top-down, pervasive, and networked(Figure 1.5).

¹³ Industrial Automation and Control Systems

¹⁴ International Society of Automation

¹⁵ Security Assurance Level

¹⁶ World Economic Forum

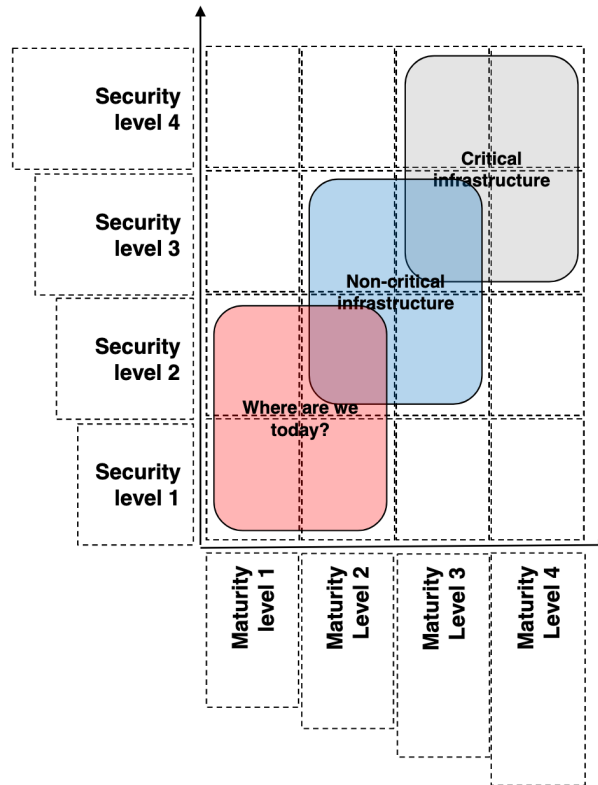


Figure 1.4: Mesh use of maturity level with Security Level in IEC 62443[34].

1.3.4 NIST Cyber Security Framework

The National Institute of Standards and Technology of the United States published a framework for improving critical infrastructure cyber security in 2014. The framework allows organizations to assess their current cyber security risk management capabilities, define the target state, establish an improvement process, evaluate the progress towards the target, and communicate among internal and external stakeholders with the common rationale [36].

The framework consists of three key features; the framework *core*, implementation *tiers*, and a *profile*. These three components of the framework enable risk - based approach to managing cyber security.

The *core* is a set of cyber security activities, desired outcomes, and relevant references that are common across critical infrastructure sectors [36]. *Tiers* describe the degree to which an organization's cyber security risk management practices exhibit the characteristics defined

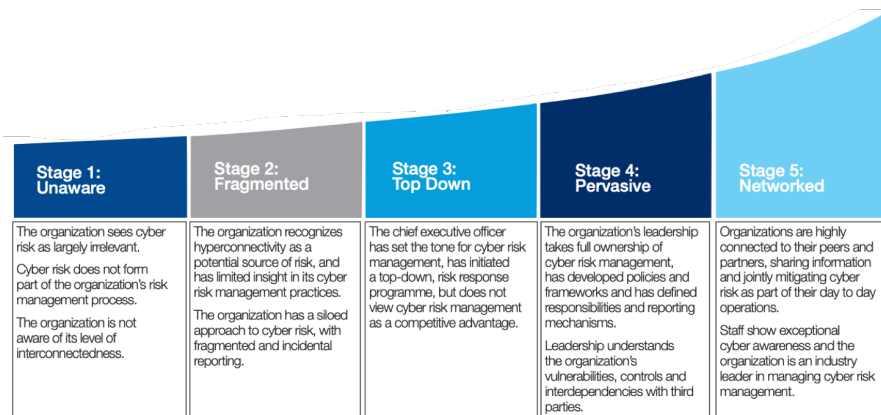


Figure 1.5: Cyber resilience maturity model by World Economic Forum[35].

in the Framework. The *profile* is a selection of items from the *core*, based on an organization's needs, that helps identify opportunities for improving cyber security by moving from *current state* to *target state*. In this paper, *tiers* are used as a measure of cyber security management skills; therefore, they are briefly described in the next subsection.

One of the key features of the NIST Cyber Security framework[36] are implementation tiers. They can be used by organizations to assess the current cyber security risk management capabilities and how they are aligned with the principle of the framework. Tiers range from Partial(Tier 1) to Adaptive(Tier 4);

- Tier 1 : Partial – The approach to cyber security risk management is ad hoc and reactive, based on informal practices. At the organizational level, awareness of cyber security risk is limited and an organization-wide approach is missing. Moreover, collaborations with other entities are not established.
- Tier 2 : Risk Informed – Risk management processes are approved by management. There is awareness of risk at organization level, but lack of an organization-wide approach. The organization knows its position with respect to other entities, but collaborations are not formalized.
- Tier 3 : Repeatable – Risk management practices are expressed as policy, and an organization-wide approach is established. Risk-informed policies, processes, and procedures are defined. The

organization receives from its partners information that helps the decision making in response to events.

- Tier 4 : Adaptive – The organization adapts its practices based on previous and current cyber security activities. Technology and practices are continuously improved to keep up with evolving and sophisticated threats. The organization shares information with partners before and after cyber security events.

Table 1.1: Potential impact of successful cyber attack on Industrial Control System [4].

Incident Type	Potential Impact
Change in a system, operating system, or application configuration	<ul style="list-style-type: none"> - Command and control channels introduced into otherwise secure systems - Suppression of alarms and reports to hide malicious activity - Alteration of expected behavior to produce unwanted and unpredictable results
Change in programmable logic in PLCs, RTU ^s , or other controllers	<ul style="list-style-type: none"> - Damage to equipment and/or facilities - Malfunction of the process (shutdown) - Disabling control over a process
Misinformation reported to operators	<ul style="list-style-type: none"> - Inappropriate actions taken in response to misinformation that could result in a change to operational parameters - Hiding or obfuscating malicious activity, including the incident itself or injected code
Tampering with safety systems or other controls	<ul style="list-style-type: none"> - Preventing expected operations, fail safes, and other safeguards with potentially damaging consequences
Malicious software (malware) infection	<ul style="list-style-type: none"> - Initiation of additional incident scenarios - Production impact resulting from assets taken offline for forensic analysis, cleaning, and/or replacement - Assets susceptible to further attacks, information theft, alteration, or infection
Information theft	<ul style="list-style-type: none"> - Leakage of sensitive information such as a recipe or chemical formula
Information alteration	<ul style="list-style-type: none"> - Alteration of sensitive information such as a recipe or chemical formula in order to sabotage or otherwise adversely affect the manufactured product

Table 1.2: Maturity Indicator Level Characteristics proposed in Cybersecurity Capability Maturity Model

MIL ₀	Practices are not performed
MIL ₁	Initial practices are performed but may be ad hoc
MIL ₂	<p>Institutionalization characteristics:</p> <ul style="list-style-type: none"> - Practices are documented - Stakeholders are identified and involved - Adequate resources are provided to support the process - Standards or guidelines are used to guide practice implementation <p>Approach characteristic:</p> <ul style="list-style-type: none"> - Practices are more complete or advanced than at MIL₁
MIL ₃	<p>Institutionalization characteristics:</p> <ul style="list-style-type: none"> - Activities are guided by policy (or other directives) and governance - Policies include compliance requirements for specified standards or guidelines - Activities are periodically reviewed for conformance to policy - Responsibility and authority for practices are assigned to personnel - Personnel performing the practice have adequate skills and knowledge <p>Approach characteristic:</p> <ul style="list-style-type: none"> - Practices are more complete or advanced than at MIL₂

Table 1.3: Example use of MIL in Cybersecurity Capability Maturity Model.

MIL ₀	
MIL ₁	a. The organization has a cybersecurity program strategy
MIL ₂	<p>b. The cybersecurity program strategy defines objectives for the organization's cybersecurity activities</p> <p>c. The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure</p> <p>d. The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities</p> <p>e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program</p> <p>f. The cybersecurity program strategy is approved by senior management</p>
MIL ₃	g. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile

In this chapter, we examine the available resources to understand the trends and definition of the field. The chapter consists of 3 sections. Section 1 reviews the literature in the related field to define exercises. Section 2 investigates current Industrial Control System security exercises available in the field. We discuss the limitation of the conventional approach. Section 3 illustrates the trends specific to the Japanese market and what makes it peculiar.

2.1 LITERATURE REVIEW

2.1.1 *What is Exercise?*

The term "Exercise" is often used as a synonym of other personnel education programs such as training, drill, and testing. In this section, we review its definition from various relevant documents to understand its characteristics.

FROM A NATIONAL PREPAREDNESS PERSPECTIVE. The Homeland Security Exercise and Evaluation Program is a guideline for managing the exercise program from the perspective of national preparedness [37]. It states that an exercise is a tool to achieve a high capability for managing risk. Exercise can be used to test the system, to train people, to improve communication and to identify opportunity

for improvement. In the document, the word is used as a generic term for drill, training, and testing.

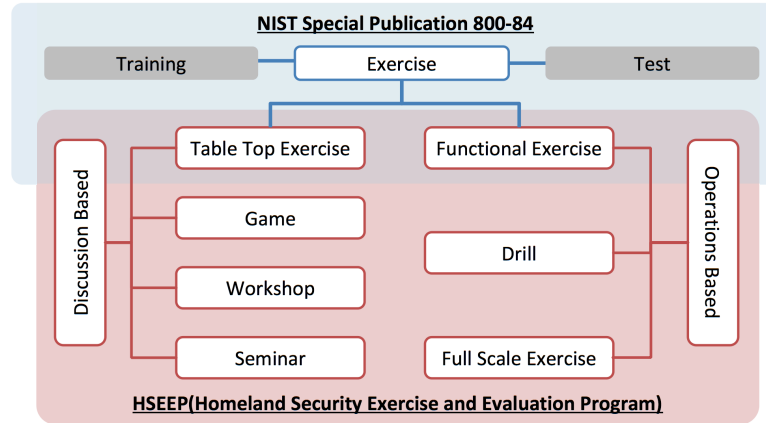


Figure 2.1: Types of exercise proposed in NIST Special Publication 800-84 -Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities- [38] and Homeland Security Exercise and Evaluation Program (HSEEP) [37]

FROM A CYBER SECURITY PERSPECTIVE. NIST has published the special publication series of cyber security so called SP 800 series. NIST Special Publication 800-84 -Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities- [38] clearly separate the use of terms exercise, test and training for the purpose of the publication. It defines exercise as a scenario-driven simulation of an emergency situation, which is designed to validate the effectiveness of one or more aspects of an IT plan.

Meanwhile, the term "test" is only used for validation of the operability of systems or system components. Training refers only to educating personnel of their responsibilities and skills, as the preparation for engaging in exercises, tests, and actual emergency situations. Comparison of the NIST and HSEEP¹ taxonomies are shown in the figure 2.1

¹ Homeland Security Exercise and Evaluation Program

FROM A BUSINESS CONTINUITY MANAGEMENT PERSPECTIVE. ISO² 22398:2013 Societal security – Guidelines for exercises [39] is a standardized guideline to control exercise program in the context of business continuity management. It describes exercise as an event to assess personnel, process and the achievement of the competencies. It defines testing as a verification process of a capability and training as an activity to facilitate learning. Training and testing can be included in an exercise. The document clearly separates the meaning of drill from others by defining it as a repetitive practice of skills.

FROM A HUMAN FACTOR PERSPECTIVE. Rasmussen has introduced a model of human performance in a routine task by dividing it into three typical levels; skill-based, rule-based, and knowledge-based [40]. Figure 2.2 shows the relation of three behavior levels.

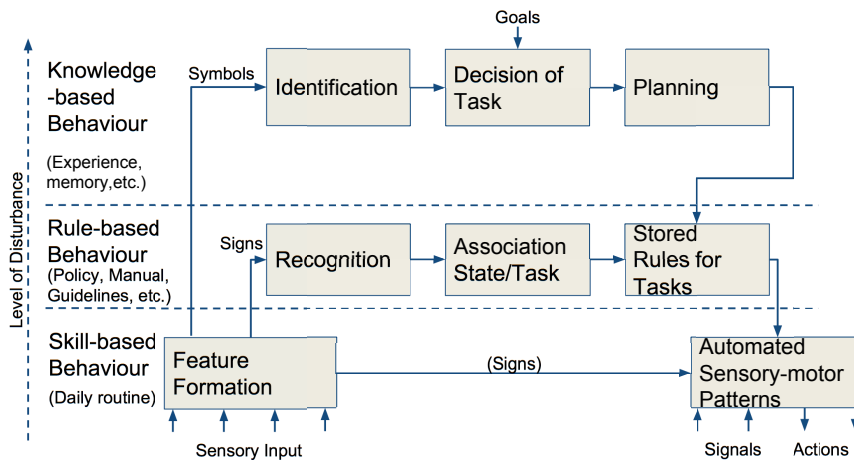


Figure 2.2: Rasmussen's model of three level behavior [40].

The skill-based behavior represents an action that takes place without thinking, such as stimulus-response behavior [41]. In the rule-based behavior, the sequence of actions is controlled by rules and procedures that the operator has learned and experienced in past similar occasions.

² International Organization for Standardization

The boundary between skill and rule-based behavior is unclear, and it depends on the level of training and attention of the operator. When an operator faces unfamiliar situations for which no rules of the past are relevant, the decision of the consequent action is made at a higher conceptual level. At this level, knowledge drives performance, according to the analysis of the environment and the aim of the individual.

Rasmussen's model can be applied to the context of operator education program. The skills required in the daily routine work is regularly trained on the job. Guidelines for the operations in unique situations with little disruption such as system maintenance, start-up, and emergency cases are documented in the operation manuals. These documented actions are trained by recreating the situation. This type of education program can be referred as a drill. The evaluation of the performance is based in accordance with the operation manuals.

Occasionally, the ability to adapt to the situations with significant disturbances to the day-to-day operation is tested in a safe environment. The performance is assessed based on adaptability and resilience. This type of program to test the ability to use the knowledge in practice may be referred as an exercise.

2.1.2 *Establishing the Terminology*

Considering the variety of the word definitions in the documents mentioned above, it seems natural to see the vague understanding of the role of exercise in the reality. In this paper, we define terms as follows.

- exercise: the instrument to measure and improve the capability of elements or process (such as personnel, system, communication, and organization) that is essential for performing a fast recovery and mitigating the impact from a disruption. The exercise is conducted based on a scenario which requires a knowledge based decision action and decision making, such as a situation that is not scripted in the incident handling manual, or with high disturbance to the core business process.

- test: the validation process of a system operability and capability.
- drill: the repetitive practice of skills within a recreated situation.
- training: theoretical education of the personnel about their responsibilities and skills, that prepares them for exercises, tests and actual emergencies.

2.2 AVAILABLE EXERCISES

Cyber security exercises are organized in many ways, with different goals. Some are open to the public, and some are privately conducted. An organization who is looking for opportunity to develop or strengthen their cyber security capability may look for publicly held exercises.

Most of these exercises do not require any preparation process; therefore it is relatively easy to participate. However, the simulated environment may be theoretical or unrealistic for certain organizations. On the other hand, a privately organized exercise is usually designed and developed internally, or by hiring specialists. While it has the benefit of emulating a realistic situation specific to that company, the long term development process might require a commitment and dedicated resource. In this section, we review the variety of styles and objectives of cyber security exercises with few public example cases.

2.2.1 *Capture The Flag*

The computer security community has adapted the concept of a traditional children's outdoor game to a technical competition. Since the well-known hacking convention defcon introduced the competition in 1996, various styles of CTF³ has been organized in the community. Eagle pointed out that the competition became a platform to attract more people to work in the field of cyber security[42].

³ Capture The Flag

2.2.2 Game: Kaspersky Industrial Protection Simulation

A cyber security company Kaspersky Lab developed a role-playing game to establish an understanding of the IT, business, and CxOs[43]. In KIPS⁴, teams of participants run a simulated company. The team adopt financial, IT or security strategies by placing activity cards on the game board which illustrates the companies network structure. The consequences of the decision are provided as the financial gain by the successful production(Figure 2.3). Because the undergoing cyber attack scenario is concealed to the participants, and they can experience the decision making in uncertainty with the limited resources(Figure 2.4).

KIPS is a hybrid game with action cards and a game simulator that is 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 cyberattack on a virtual CI company. Players acting as a security administrator for a virtual company determine countermeasures against cyberattacks within time and cost constraints. The goal of the game is to maximize revenue when responding to cyber incidents.

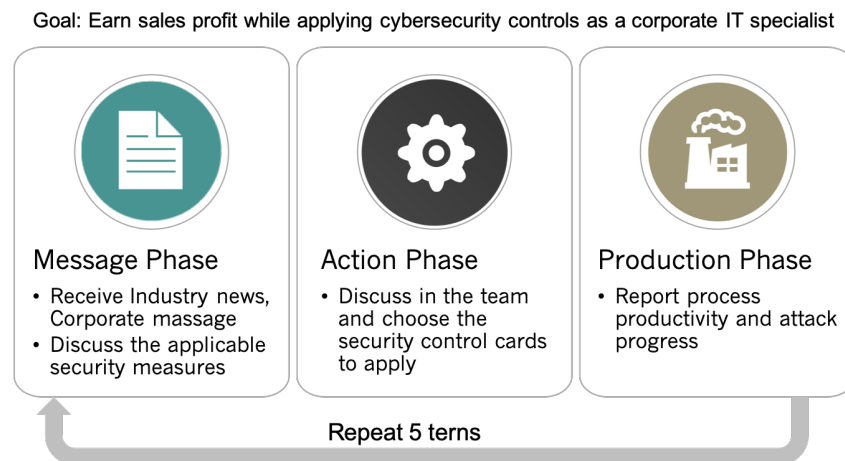


Figure 2.3: Game phases of Kaspersky Industrial Protection Simulation

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

⁴ Kaspersky Industrial Protection Simulation

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 an applicable space. Thus, players can observe which action cards have been used. An action card represents a set of cyber security countermeasures.


Hours	2 hours	
Exercise Type	Game	
Participants	12 ppl (4 groups)	
Target Audience	All	
Focus	Defense Strategy	
Exercise Environment	Board/Card game	
Scenario	Fictitious company	
Activity	Restricted by cards	
Pros	Numerical score feedback (\$) Easy introduction to industrial cybersecurity	
Cons	Actions are restricted by cards IT security heavy	

Figure 2.4: Outline of Kaspersky Industrial Protection Simulation. Pictures from the website[44].

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. 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.

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 of which comprises 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. The water is heated by exhaust gases. 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.

2.2.3 Drill: ICS Cyber Security Exercise by CSSC

CSSC⁵[45] has been organizing cyber security exercises specific for gas, electricity, chemical, and building management operations. The exercise is tailored for the engineers and operators of these fields. The program employs the control system testbed for the exercise. The exercise facilitator guides several exercise participants to operate the control system while the exercise controller runs the exploitation scenario(Figure 2.5). By using the testbed system dedicated to the specific fields, the participants can observe and experience the realistic effect of cyber attack to their daily job, and learn practical methods to prevent and detect the cyber attack(Figure 2.6).

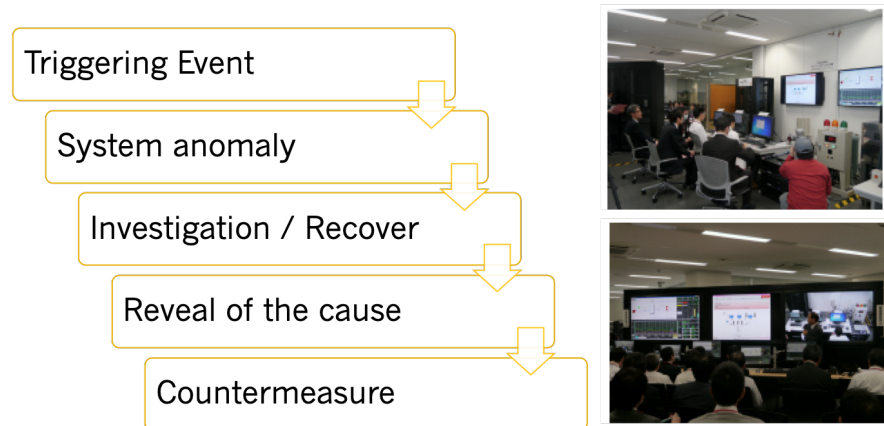


Figure 2.5: Exercise process of Control Systems Security Center training[46]

2.2.4 Table-top Exercise: Critical Infrastructure Incident Response Exercise by NISC

the cross-sectoral exercise organized by NISC⁶ has become an annual event for all 13 CI domains in Japan[47]. The purpose of this exercise

⁵ Control Systems Security Center

⁶ National Information Security Center of Japan


Hours	2 days	
Exercise Type	Lecture + Functional Exercise	
Participants	20 – 30 ppl.	
Target Audience	Gas, chemical, building management, energy sectors	
Focus	5 defense scenario	
Exercise Environment	Operational Hands-on	
Scenario	Fictitious company	
Activity	Follow the directions	
Pros	Focus on the operator role	
Cons	Limitation in the participants	

Figure 2.6: Outline of Control Systems Security Center training.

is to enhance the incident response capability of CI operators and to train the information sharing efficiency among CI operators, the related authorities, and other stakeholders. Over 2000 participants from 500 organizations joined the exercise in 2016. During the exercise, the participating organizations receive the scenario injections which describes the current event. Triggered by the information provided, the participants plan the action to take, and contact the stakeholders based on their rules. We use this exercise as an example of multi leveled exercise and discuss how it can be managed based on the proposed framework at the later section.

2.3 CONCLUSION

The examples above show the variety of exercise styles. Each exercise has a unique structure and objectives. In order to incorporate these exercises into the company's cyber security capability development plan, organizations have to select the exercises that suitable for their current scope of their training plan. However, there is no specific guidance on how to select exercises. Moreover, the scope of the exercise is not described in standardized method, which makes it harder to understand how effective the exercise can be.

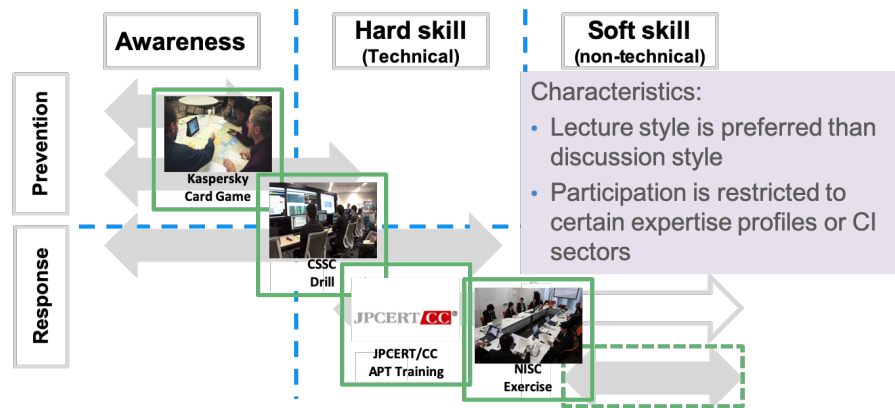


Figure 2.7: Mapping exercises available in Japan.

In Japan, there have been discussions about whether the Red-Blue teams exercise is necessary, and so far this format has not been adopted for domestic CI stakeholders. Conversely, there are several ICS security training programs that consist of class-room lectures and drills, which do not include active discussion among participants. More importantly, participation to these training programs is restricted to certain expertise profiles or CI sectors (e.g. banking, chemical). However, large-scale cyber incident can cause an impact beyond boundaries of CI sectors in a highly inter-connected society. In case of such an event, the cooperation of CI sectors and other stakeholders (e.g. government agencies) is essential [48]. Nevertheless, the current training system is isolated by sectors, and does not include stakeholders outside the organization. The results of such limited diversification of expertise are that the participants' perspective on cyber security issues is narrowed down, and that knowledge transfer across sectors is not facilitated.

3

UNDERSTANDING THE NATURE OF THE CYBER INCIDENT MANAGEMENT

The interaction between two parties makes cyber incident response unique in comparison with natural hazards. We discuss the uniqueness of the field from three perspectives; 1) the time-lag of the adversarial interaction, 2) the shift of focused activities, and 3) the management challenges.

In this chapter, we investigate the nature of incident management by observation studies at a large scale adversarial exercise.

3.1 FIELD OF STUDY

The study on human contribution to cyber resilience is unexplored terrain in the field of critical infrastructure security. So far cyber resilience has been discussed as an extension of the IT¹ security research. The current discussion is focusing on technical measures and policy preparation to mitigate cyber security risks. Although cyber security training is a common measure to implement security experts because of its low cost, most of the training courses aim at improving security awareness of employees, in order to mitigate human-error. This approach does not address resilience in handling a cyber incident. However, we believe that security training should provide more than just awareness.

¹ Information Technology

The need for cyber security training beyond awareness is growing in the industry, and several authorities are providing training for cyber incident handling. The difference between awareness and incident handling training is that the latter has learning objectives, while the former just tends to aim at gathering attention by showing shocking virtual images. We studied full-scale adversarial cyber security training from the perspective of human factor and management skills.

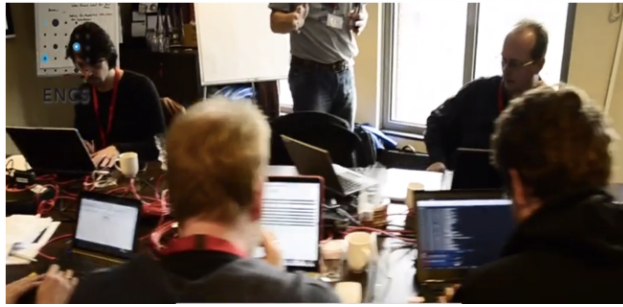


Figure 3.1: Red team participants engaging the exercise.

However the training was not designed to evaluate team's non-technical skill, it was obvious that the team's capability of the non-technical skill affects the overall performance. In addition, most of the team experienced similar management challenges. In this paper we summarize the management challenges that are observed in the incident handling training as possible challenges that can emerge in real-world cyber incident management.

3.1.1 *Red Team - Blue Team Exercise Overview*

The observation was conducted several times in the Red Team – Blue Team RTBT² exercise held by ENCS³ (The Hague NL). In this exercise a realistic scenario will be enacted with a "chemical" factory, which has to be operated and protected by the Blue team, while the Red team tries to hack the company's network resources and aims to disturb the production process. Participants are allocated to either red (offensive) / blue (defensive) team (Figure 3.2).

² Red Team - Blue Team

³ European Network for Cyber Security

The red team consists of 10 participants in average, while the blue team consists of 20. Each team sits in physically separated rooms and plays the exercise for 8 hours. Several authorities organize Blue team style exercise, such as by Idaho National Laboratory in United States [49], and by Queensland University of Technology in Australia[50].

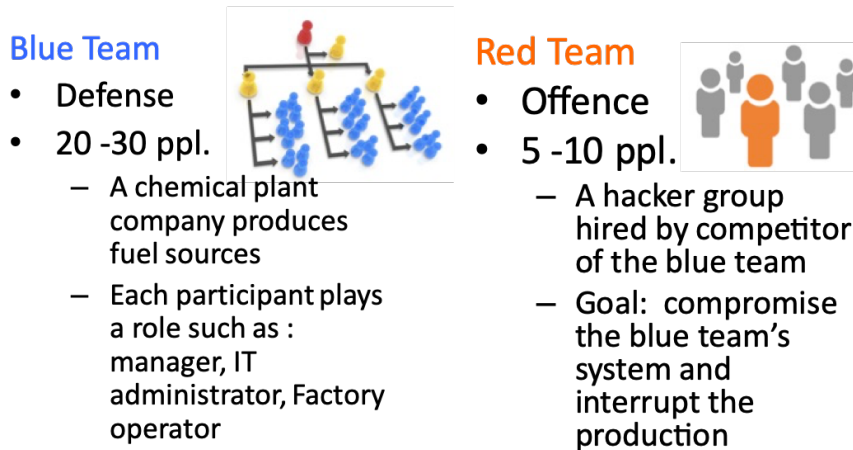


Figure 3.2: Role of the participants during the exercise.

Figure 3.3 shows the overview of offence/defence timeline and its relation to the blue team's network. In the beginning, the red team starts from outside of the blue team's network, and this team exploits the blue team organization's network to the depth till they gain the control of the physical plant system. Facilitator controls the timeline of the red team activity by giving a hint and new incentives. Meanwhile the blue team's timeline is dependent to the red team. The events are driven both internally and externally, and the main challenge for the blue team is flexible responses to the escalating cyber attack.

3.1.2 Typical Scenario of Red-Blue Exercise

The blue team in the setting of a chemical plant that was just the start of the operation, and to act as a company as a whole team, given the role of managers, IT engineer and operator. While producing specified products, the blue team has to act on security tasks, such as 1) Identify the problem on security (detection activities), 2) Change the system in order to improve the security, reporting (prevention activities), and 3) Reporting Incidents (and corresponding activities).

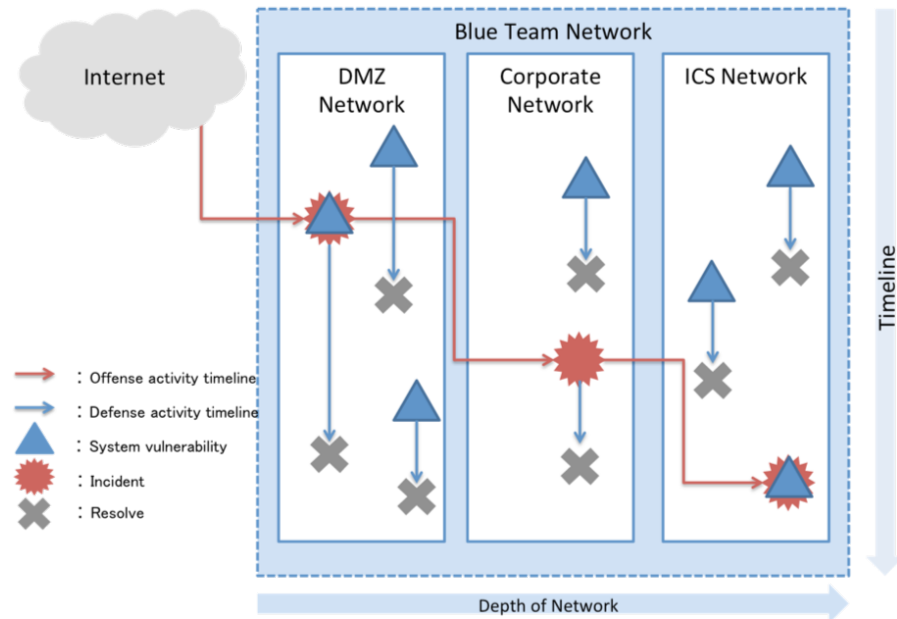


Figure 3.3: Activity timeline of the exercise.

On the other hand, the red team plays a role as a hacker group that was hired by a competitive organization of the blue team's organization. The goals of the red team are: 1) To gather information about the production system and configuration of Blue team companies to be targeted, 2) Interfere the production activity, and 3) Conceal the attack.

3.1.3 Simulation Gaming

As a game, incentives to motivate each team to act on hacking/defending activities are provided. The teams can gain points by reporting particular hacking/defending activities to the White team, which is played by the exercise facilitator. White team is in an intermediate position to control the game as facilitator so that the game will be almost carried as designed. The white team supervises activities of both team and provides technical and strategic advise.

3.1.4 *Designed Challenges in the Exercise*

The exercise environment is intentionally designed to create challenges. Some of them simulate the obstacles that defenders will face while implementing security, and others enhance the stress in the game.

REPORTING DUTY. Blue team managers have to inform every incident and can not implement the change request without the approval of the c-level played by the white team. This additional procedure not only creates a delay, but the c-level often rejects their claims due to the insufficient reasoning. This bottleneck effect in communication is common in the real-world, and participants learn how to explain the significance of the incident to non-technical personnel and convince them.

ROOM CONFIGURATION. Communication is a lot harder when walls physically separate your teammates. The red team sits in a meeting room surrounding a table, which promotes the interaction and cooperation among the teammates. Meantime, the blue team's rooms are separated physically by partitions (Figure 3.4).

Each role has a designated area to work. IT security engineers are sitting away from the factory operators, and the managers are sitting away from the shop floor. It embodies the wall between the IT, OT, and management personnel, and also creates difficulty in communication flow among teammates.

BIASED INFORMATION. Both teams receive a network map of the blue team at the beginning of the exercise. The red team obtains a plain map that shows a layered network structure (Figure 3.5). The red team starts with a public network to intrude into the depth of the system. On the other hand, the blue team receives a detailed network map (Figure 3.6). However, the blue team's network diagram is outdated, and there are some undescribed changes - including rogue devices. Frequently, the blue team trust the map too much and neglect to do inventory.

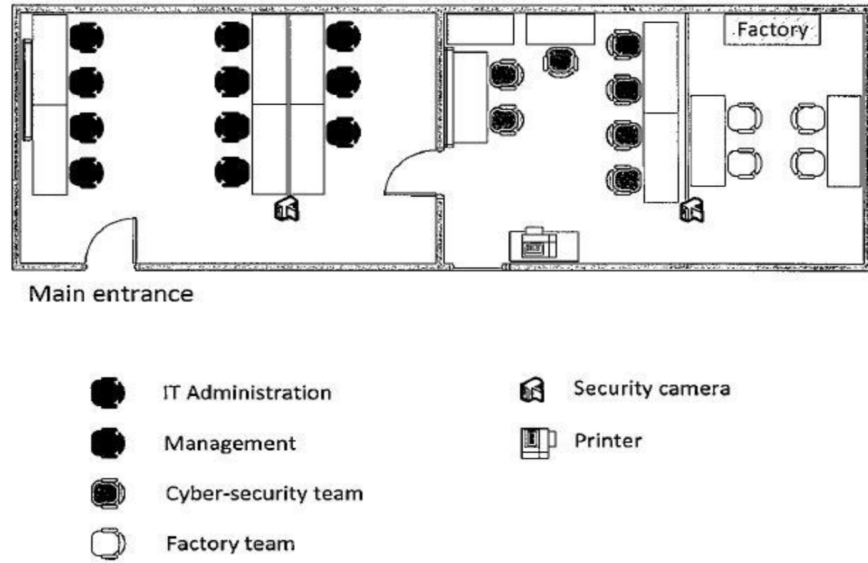


Figure 3.4: Room arrangement for the blue team.

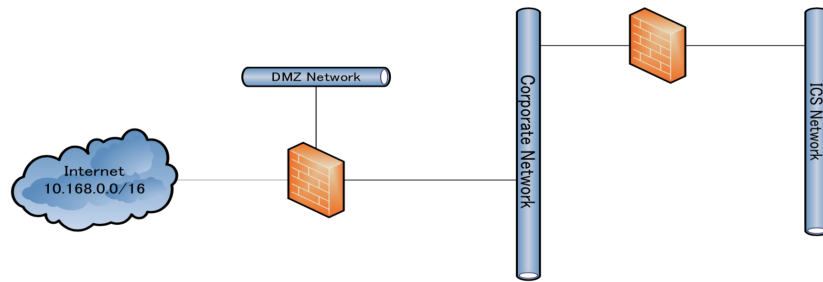


Figure 3.5: Blue team’s network structure provided to the red team.

3.2 ASYMMETRICAL TIMELINE

Cyber security is a cat and mouse game. Based on the current defense capability, attackers look for the new attack vector. The defender will soon get to learn the indicator of this attack, and create a solution. Attackers have an advantage over Defenders in this endless game.

3.2.1 Attacker Free Time

Cyber Kill Chain enhances visibility to an attack process[51]. The attacker does reconnaissance, weaponization, delivery, exploitation, installation, command& control, then actions on objectives (Figure 3.7). From the defenders perspective, it is hard to catch the attack in the

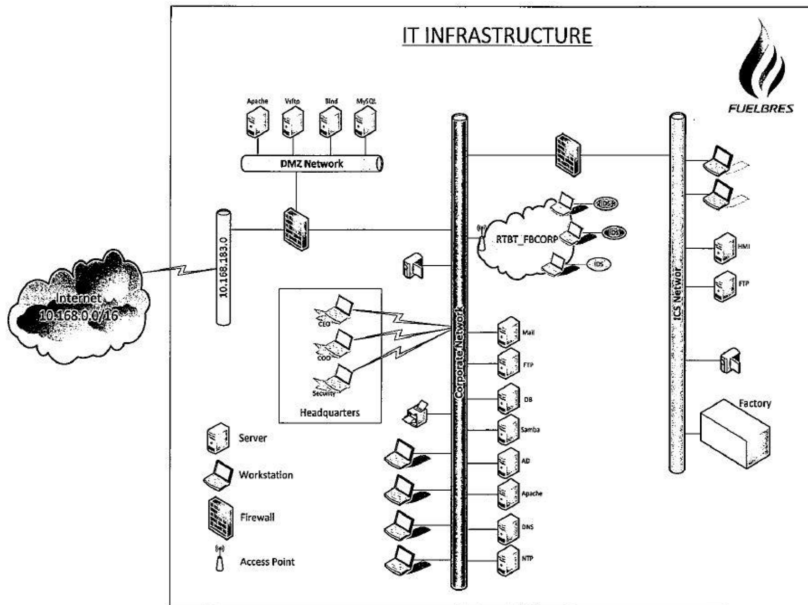


Figure 3.6: Network map provided to the blue team.

early stage of the kill chain. Often they realize the attack only after the attacker reached the goal.

The time gap between the attacker's intrusion to the system and the defender's identification is called "attacker free time"(Figure 3.8)[52]. The defender's challenge is to reduce this free time by detecting the intrusion fast, diagnosis the symptoms, apply the treatment and recover.

3.2.2 Observation Conducted

Defending the system is not necessarily a technical issue. People, process, and technology issues are affecting the longer attacker free time(Figure 3.9).

- People - Lack of awareness and knowledge can delay the response. Education and training are necessary for site operator, OT engineer, IT security engineer, and c-levels. It is often affected by the organizational culture.
- Process - Inadequate documentation and procedure can delay the response. Solutions include change management, Incident

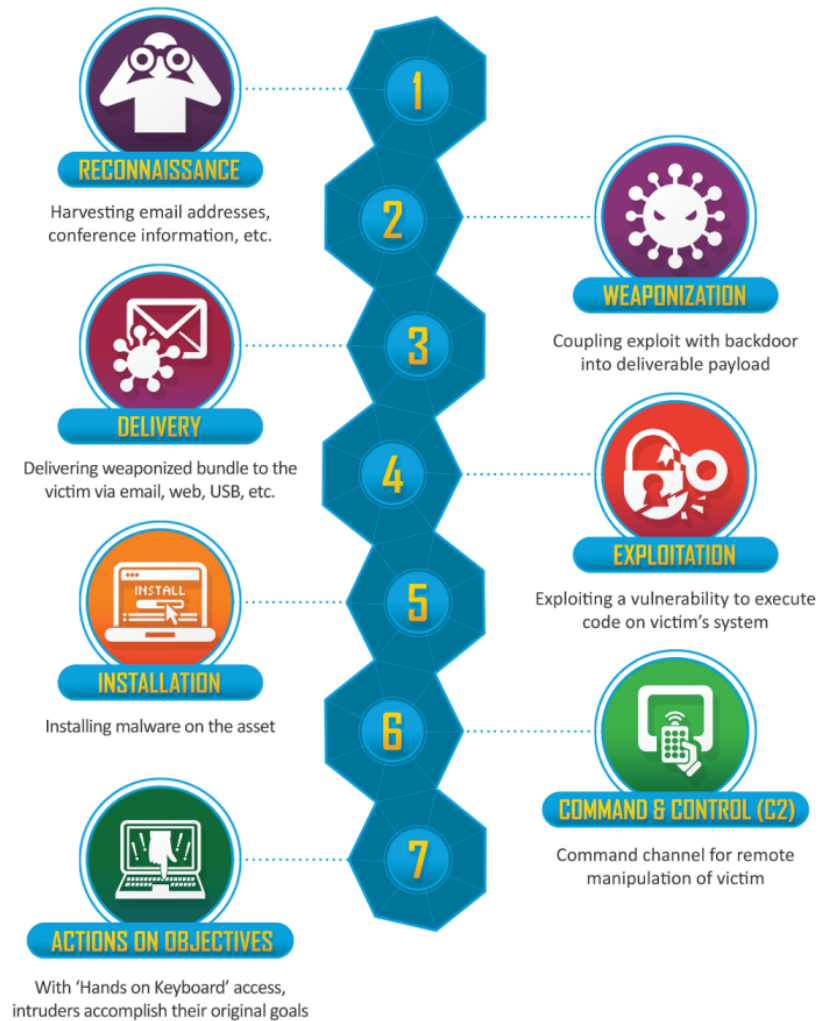


Figure 3.7: Cyber Kill Chain®[51]

response plan, error reporting process, standardized reporting format, and cross-sectoral communication plan.

- **Technology** - Absence or ill-configuration of technical solutions can elongate the attacker free time. Solutions include IDS⁴, fire-wall configuration, logging, and network segmentation.

In this study, we focus on people and process issues - especially what factor would elongate the attacker free time, and why it occurs. For this reason, we focused on one specific event, and observed the blue teams behavior.

⁴ Intrusion Detection System

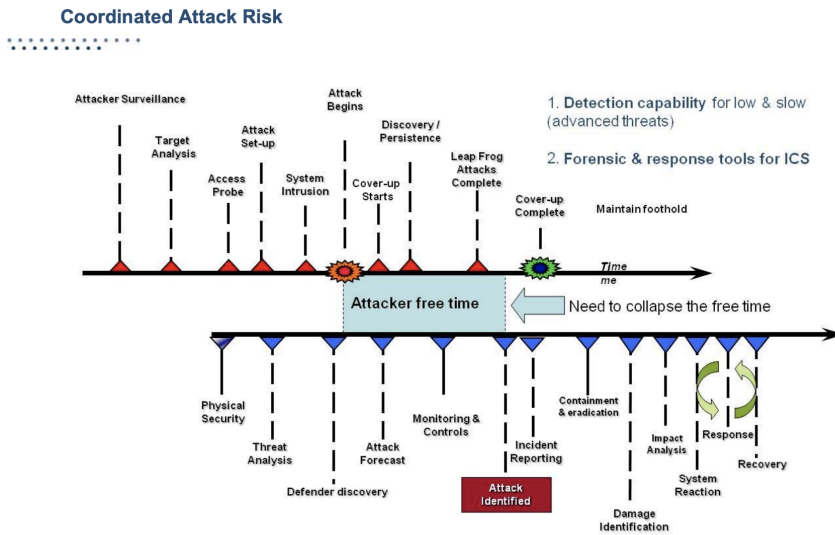


Figure 3.8: Attack life cycle presented in NERC HILF report[52].

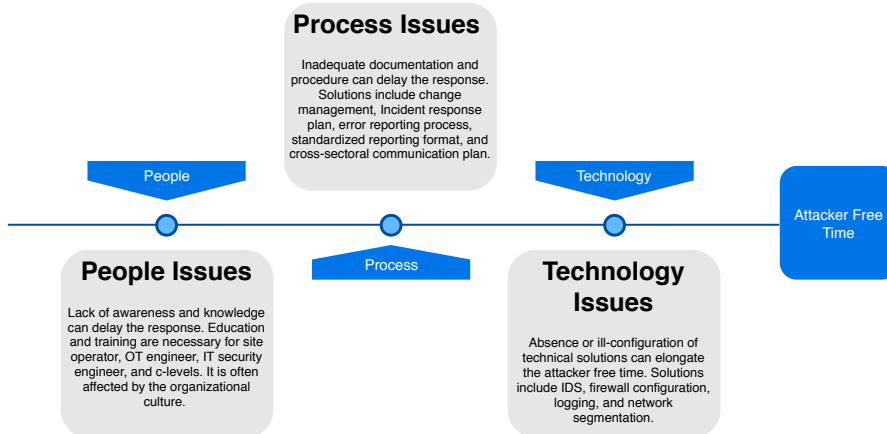


Figure 3.9: Cause analysis of attacker free time

3.2.3 Exercise Scenario under Microscope

The exercise scenario consists of several events. Events were the crafted scenario around the implanted vulnerabilities in the blue team network. The event triggers when the attackers discover vulnerability. One of the events is the power down in the blue team office. Here we will call this sequence of the event as "Power switch hack."

POWER SWITCH HACK SCENARIO. Usually, the attacker needs to go through layers of networks to reach the ICS network. This defense in depth strategy[53] is a common practice in security. This practice

is ineffective when there is an uncontrolled point of entry directly to the ICS network - such as an unauthorized backdoor, USB devices, or a wireless access point. This common blind spot is designed into the exercise scenario.

The exercise has an undocumented wireless router hidden in the blue team ICS network. Since it is unexpected, the blue team tends to forget to scan the wireless network. This wireless network uses a weak security protocol (WEP⁵), which the attacker can easily eavesdrop[54], and invites the attacker to the ICS network as the backdoor.

There is another hidden device in the ICS network - power switch. This networked power switch provides electricity to the PC monitors and printers in the blue team room. The power switch is controllable via a browser, which is protected by a default password.

Again, the blue team often neglects to verify the network structure and unmarked power switch stay unnoticed for most of the time.

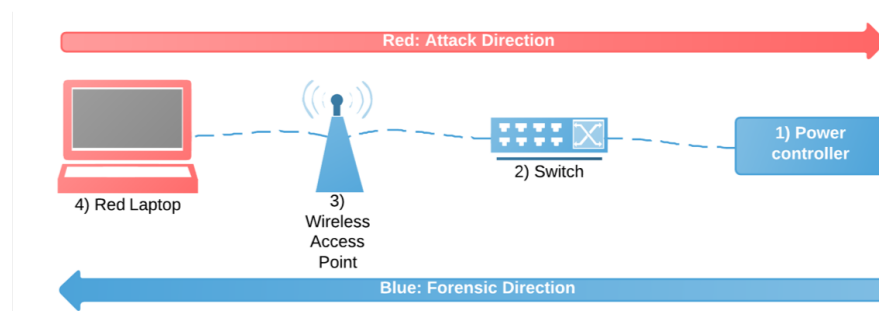


Figure 3.10: The route of power switch hack scenario.

RED TEAM ACTIVITIES. In this part of the event sequence, it starts with the red team scanning the wireless network to find the hidden access point. Then crack the WEP to intrude to the ICS network. The red team finds connected devices by scanning the network, including the power switch, as mentioned above. While attacking the other (and more critical) devices in the network such as PLC, the red team looks for the password to log in the power controlling console. The once they acquire the password, the red team can disturb the blue team's operation by turning off the electric power of devices such as HMI monitor and printers.

⁵ Wired Equivalent Privacy

3.2.4 *Observed Behavior*

The blue team realizes the anomaly from the sudden blackout of the computer screens. They have to determine the cause of the outage (power controller), then how the attacker entered the network.

Figure 3.11 shows the timeline of the reported events during the exercise.

We followed the reporting time of the related event by both red and blue team. In this game, red team successfully turned off the power switch at 12:00, and it took 50 minutes for blue team to regain the control of the power switch. The blue team reset the power switch at 12:50.

RED TEAM'S REPORT.

- Red Report A: Red team reports that they found the hidden Wifi (around 10:00).
- Red Report B: Red team reports that they gained the entry to the power switch (around 11:45).
- Red Report C: (After getting permission to exploit the power switch around 12:00,) Red team reports the power is switched off (around 12:30).

BLUE TEAM'S REPORT.

- Blue Report 1: Blue team reports that they identified the cause of the power outage as the overtaken IP-connected power adapter (around 12:45).
- Blue Report 2: Blue team updates the report that the power adapter was overtaken due to the default password (around 12:55).
- Blue Report 3: Blue team discovers the WiFi access point, and request to change its security setting (around 16:30).

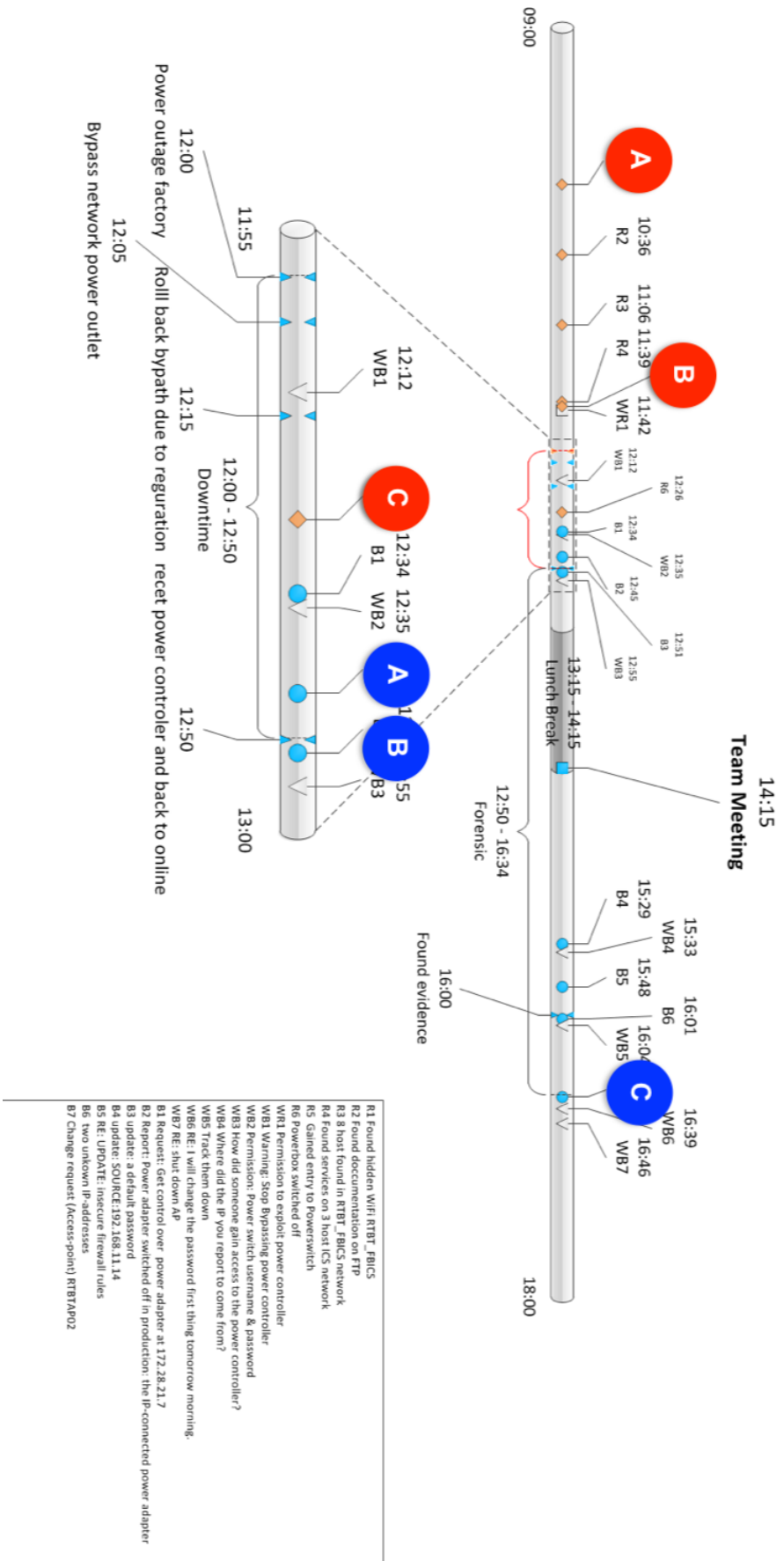


Figure 3.11: Event log of the activities related to the power switch hack.

3.2.5 Results

CALCULATING THE ATTACKER FREE TIME. Once the red team gains access to the wireless network, they start exploring the ICS network for valuable targets. In this case, the attacker discovered and cracked the WiFi access point at 10:30 - thus the beginning of the attacker free time. Meanwhile, the blue team did not realize the presence of the attacker in the network until the red team starts acting visibly.

Until the power outage at 12:00 occurs the blue team had no knowledge of intrusion. It took another 45 minutes for the blue to identify the cause of the outage. Distracted by other incidents, the blue could not identify the wifi access point until 16:30 - which allowed the red team to freely roam in the ICS network for 6 hours. By then the red already other assets on the ICS network was attacked and installed the backdoor.

CAUSE OF THE DELAY. It was difficult for the blue team to doubt the network map and investigate the cause. Even after identifying the IP connected power switch on the ICS network, they believed that the attacker intruded via the corporate network. They falsely reported that insufficient firewall rules between the networks allowed the attacker to reach the ICS network. The blue team knew that it is necessary to track down the cause. However, the task was not assigned to any team member and left unresolved for a long time.

One issue was that participants did not have technical skills to identify the cause. The other issue was coordination - even though some of the blue team knew that they need to investigate how the power switch was taken over, there was a communication issue that the task remained unassigned.

For this reason, we conclude that communication and coordination is necessary to shorten the attacker free time.

3.3 ADAPTIVE RESOURCE ALLOCATION

3.3.1 *Observation Conducted*

The observation of the blue teams behavior in the exercise was conducted in the March 2014 training course held by ENCS. The focus of the observation was to see the BLUE team's incident management activities and its relevance to the team's resilience. 18 training participant formed the BLUE team. The team consists of four divisions; plant operation group, system administration group, cyber security group and management group.

3.3.2 *Red Team Activities*

Red team's behavior is controlled by the white team. Their activity creates a dynamic event flow in the game. The red team moves from outer network to DMZ, DMZ to Cooperate network, then to ICS network. The transition makes four escalating stages in the game.

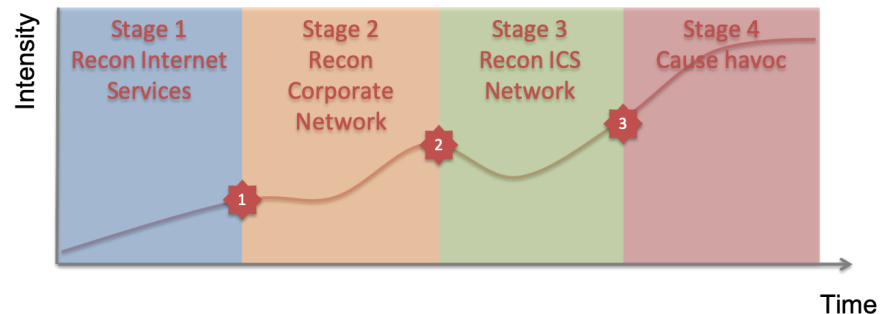


Figure 3.12: The red team's activity timeline.

3.3.3 *Shift of Defence Activities in Blue Team through the Game*

During the game from 8:30am to 6pm, we conducted hourly questionnaire to all 12 training participants who played roles in system administration and cyber security group to specify the task they are engaged at the moment. The responses are categorized in prevention,

detection or response activity. As the summary, Figure 3.13 shows the hourly shift or defense activity trends.

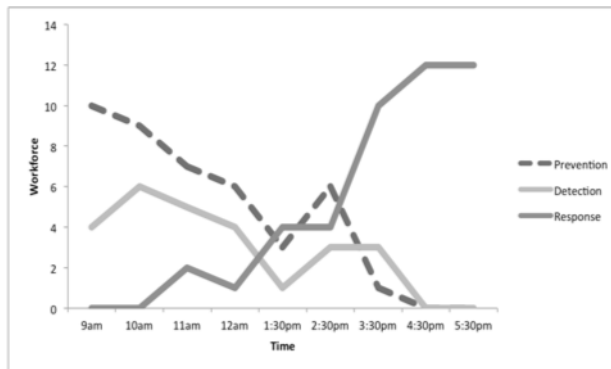


Figure 3.13: Shift of blue team activities throughout the day.

When the exercises start in the morning, the team focused on prevention activities strategically. The team discovers the first incident before 11am and from then the number of people who is assigned to response activity starts to increase. The resource allocation changes dynamically to follow the progress of attack activities by the red team.

Around 1pm the plant operation was no longer possible due to the red teams successful attack. In order to recover quickly from the damage, the management group held an all-in meeting to request all team members to focus on response activities. While the forensic revealed security holes in the network, few people temporary moved back to prevention tasks (at 2:30pm) in order to control the future damage by the security hole. The management group gathered the team member again around 4pm, to give up the chance for recovery and focus on scoring more points by submitting incident reports to the white team.

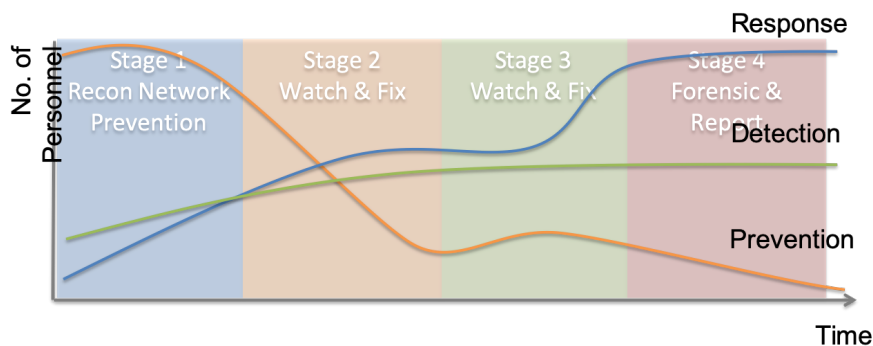


Figure 3.14: Blue team activities divided in four phases.

3.3.4 *Cyber Defence as a Crisis Management in Escalating Situation*

Bergstörn presented a theoretical framework of generic competencies for proactive crisis management [55]. The framework contains the following four categories: 1. Information Management, 2. Communication and Coordination, 3. Decision and Implementation, and 4. Effect control. However the framework was developed in the field of Safety Engineering, it is also applicable to cyber incident handling. In this observation we adapted the four indexes from the framework for observing key activities of the Blue teams incident management. The observed activities are summarized in Table 3.1.

Table 3.1: Organizational resilience indicator and corresponding activities observed in the field

Organizational Resilience Indicator	Activities Observed
Information Management	Incident Reporting Re-prioritizing tasks
Communication and coordination	All-in Meetings
Decision and Implementation	Centered to managers Top-down
Effect Control	Progress control by managers

In order to manage the information in the organization, management group gathers team member for meetings. This management activity corresponds to 1. information management and 2. communication and coordination. With the lapse of time, the strategy of management team changes the center of their attention to potential crisis (, i.e. prevention work centered), then actual and factual crisis (, i.e. monitoring and response work centered), and then in the end a opportunity centered driven by game incentives. Their focus became shorter and shorter as the situation escalates.

For 3. Decision and Implementation, the team had a strong top-down decision making culture. The management group was the decision maker through the day, and strategy was driven by managers decision. This structure allowed other team member to concentrate on the assigned task, but at the same time the team lost the opportunity to consider opinions from other team member. One-directed communication brought misunderstanding and friction between management group and other team member.

As 4. Effect control, management team tried to keep track of each members progress in their task, although the management did not control the team member's skill and capability. For this reason the management did not consider the one's aptitude for task execution, and as result the management failed in effect control of their decision. After the decision to concentrate only on incident reporting, the management assigned a new role to a security group member as an incident manager. Since he worked on tasks whole day with other team member, the new incident manager had a good overview of the group's capability and could control the task progress effectively. He also posted incidents that is currently in progress, and tracked the changes that have been made.

3.3.5 *Discussion: the Cause of Defeat*

At the end of the game this BLUE team could not gain the higher score than the red team and loses the game. From the perspective of resilience engineering, this team had a good flexibility in changing organization structure and prioritizing works, but the team kept the top-down decision making process, and hold closed strategy meeting within the management group separately from other team members, which ended up excluding opinions from non-management role players.

By the end of the exercise, the team member even had repulsive feelings for managers. Also there was no culture for information sharing over groups, and it led to overlap and delay of task. One of causes of failure includes the lack of experience and knowledge of management of the participants; however, on the other hand, the incident manager could handle the resource allocation of the team well, even though he had no background in management.

The difference between him and the management group were that he knew the team's capability well and could assign the task that fits to one's aptitude and by sitting in with the cyber security group he could have two-way communication with other team member easily.

3.4 MANAGEMENT CHALLENGES

3.4.1 *Time Critical Decision Making with High Uncertainty*

Unlike natural hazards, cyber incidents have two event timelines, in the offensive and defensive sides. The offence side tries to penetrate into the targeted network by exploiting system vulnerabilities.

Meanwhile, the defense side tries to 1) prevent any incident or accident to happen, 2) detect anomaly, and 3) response to cyber incidents [56]. The tasks in defensive side are often illustrated as a linear three-step cycle, but they also can be parallel. Events in defensive side are driven by both internal and external disturbances; therefore the event timeline is hardly linear.

Cyber defense under an ongoing attack is always a race against time. The defense team always needs to act faster than the offence team on prevention and response against propagating malfunctions, while keeping high mindfulness in detection. Moreover, the overview of an attack is often unrevealed until a detailed digital forensics ends. No one knows what's going on and everybody wants to know [57]. The uncertainty of the situation creates high frustration inside the organization, which affects the performance of the incident management.

3.4.2 *Management Challenges and Decision Making Trade-offs*

During the interplay, the following management challenges and decision making trade-offs were observed in every training course. The team should prepare for the future confusion in the team caused by these challenges.

- Complete assigned tasks vs. overtake new events: The execution of original task is often interrupted by other event.
- Mis-communication: Communication between task groups and managers increases the frustration, and leads misunderstandings. The communication path prepared for the normal operation is not enough in the crisis. Stuck in communication path can

affect the critical decision making too. Predesigned protocol for communication is a key to control the situation. Also, over communication should be avoided.

- Prevention vs. detection vs. response task priority: Resource of the team should be allocated to prevention, detection and response tasks in a good balance. It is notable that the allocation should not be static.
- Fix big security hole vs. protect the critical production path: The defense team have a tendency to focus on quick fix of easily noticeable security holes. The management must conduct risk/impact analysis to determine the significance to production line. In addition, with limited resource in the team, sometimes there is not enough resource available to address on two critical security breach.
- Ambiguous responsibility of role (assumption): This challenge is highly related to the game's nature. Even though the roles are given to each participant in the beginning of the exercise, its responsibility is up to the team. Ambiguity of the role definition leads to gap or overlap between task groups. This challenge is linked to miscommunication.
- Priority of entire game vs. priority of the moment: When the situation become intense, the management often loses their ability to foresee long-term goal.

3.4.3 *Transition of Control Mode*

In the COCOM⁶[58], Hollnagel and Woods operationalized the concept of control. The orderliness of performance is characterized by the following four control modes: strategic, tactical, opportunistic and scrambled (Table 3.2). Level of control is seen as context specific and transitions between control modes are important aspects of the adaptations that guarantee resilience in complex environments [59].

⁶ Context Control Model

Table 3.2: Characteristics for the four control modes in terms of number of goals, available time, evaluation and how actions are selected [58].

Control mode	Number of goals	Subjectively available time	Evaluation of outcome	Selection of action
Strategic	Several	Abundant	Elaborate	Based on models/predictions
Tactical	Several (limited)	Adequate	Detailed	Based on plans/experience
Opportunistic	One or two competing goals	Just adequate	Concrete	Based on habits/association
Scrambled	One – not necessarily task relevant	Inadequate	Rudimentary	Random

3.4.4 Challenges and Control Modes

The four control modes can be adapted to explain the management of the defense team. The management style changes (sometimes unintentionally) to adapt to the escalating incident situation. The more unexpected event occurs, the more flexible control mode the team tends to shift. Table 3.3 shows the relation between the four control modes and the above-mentioned challenges and trade-offs.



Figure 3.15: Observed shift of control mode.

In strategic control mode, most of the challenges do not come to surface yet. Some irregularity can be seen as a sign of external disturbance, and the number of unexpected events starts to grow. When the prepared strategy is no longer align with the situation, the control mode shifts to tactical mode.

In tactical control mode, the decision-making authority is distributed to each division. Challenges become tangible, and uncertainty of the situation increases. It requires the team to adjust their system dynamically to the events.

As the difficulty to handle challenges increase, the control mode shifts to opportunistic. The team’s goal is narrowed down, and individuals are assigned to task in order to achieve the goal as fastest.

When frustration in the team increases and the number of event overflows the team’s capability of task administration, finally the mode shifts to scrambled control mode. Transition to this mode should be

avoided, as the mode is hardly manageable. Manager should carefully supervise the level of management obstacles, and maintain the most suitable control mode.

3.5 CONCLUSION

In observations, when a management system does not handle the situation, elevation of decision-making privilege has been observed together with the shift of the control mode. The core decision maker shifts from the top management to each division, then to individuals. From the perspective of management engineering, scramble mode should be avoided and being strategic mode is the most efficient and ideal.

Manager in charge of incident handling should be able to capture the change of their control status, and adopt the best management system to each control mode. For this reason, factors in organizations behavior that trigger the shift of control mode needs to be clarified. With more extended study, the challenges and control modes we explored in this paper can be the indicator to evaluate management performance in the training, and that will broaden the scope of the exercise to train cyber incident management methodology.

This study highlighted the fact that training the crisis communication and incident management structure can reinforce resilience of the organization. However, the optimal training method in this purpose still needs to be examined.

Table 3.3: The four control modes and its relation to observed challenges.

Control modes (Number of unexpected events)	Strategic (o-small)	Tactical (Medium)	Opportunistic (Large)	Scrambled (Large)
A) Complete the original tasks vs. overtake new events	Several, controlled by strategy	Frequent, controlled by division	Random, based on personal skills	Random
B) Miscommunications	Seldom	Several, Near miss	Frequent, triggers scrambled mode	Confusion
C) Prevention vs. detection vs. response task priority	Several, triggers tactical mode	Frequent changes, triggers opportunistic mode	Random, based on personal skills	Random
D) Fix a big security hole vs. protect the critical production path	Seldom	Several	Frequent	Frequent
E) Ambiguous responsibility of roles (assumption)	Several, near miss	Frequent, triggered by miscommunication	Frequent, triggered by miscommunication	Frequent
F) Priority in the entire game vs. priority of the moment	Follows strategy	Follows divisional goal	Follow incentives	Random

ICS security exercise should be designed and applied proportional to the organization's preparedness. This chapter introduces the model to be applied to design the exercise from three axes: exercise participant, exercise style, and the goal of the exercise. The chapter illustrates how exercises can play the role of a driving power to improve an organization and community's cyber security preparedness.

We discuss the details for how the model should be applied to understand the existing exercises. It highlights the limitation of current cyber security exercise landscape.

4.1 MATURITY AND EXERCISES

We have discussed cyber security maturity models in chapter 1. Although the NIST Cybersecurity Framework is useful to implement cyber security comprehensively, it underestimates the importance of exercising. In the framework *core* list, the closest concept to *exercise* is Awareness and Training (unique identifier: PR.AT), which is categorized under the possible outcome of the Protect function, together with access control and data security. The role of training is described as follows: *The organization's personnel and partners are provided cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements* [36].

The purpose of the training is strictly limited to the reinforcement of cyber security awareness, as opposed to *exercises* that represent a personnel education program beyond awareness. In the past cyber security exercise related studies, we discussed the importance of exercise debriefing. It has the effect of creating the shared lessons learned from experience gained during the exercise, and it can trigger the organization to improve their security preparedness [60].

4.2 EXERCISE CLASSIFICATION FOR SCOPE TAILORING

Organizations in different framework tier have a different appetite for exercise complexity. Implementing an exercise which is appropriate for the capability will maximize the learning. Usually, overscaled exercise is unsuccessful, because the participant cannot focus on the core learning point, or unmotivated by not achieving the exercise goal, or simply get disorganized. Likewise, exercise with a smaller scope than the capability is ineffective. It does not stimulate the learning of participants, and completing exercise goals too easily may give a wrong idea of satisfaction to the current ability.

Figure 4.1 shows the recommendation of the exercise configuration for each tier. The column corresponds to the NIST cybersecurity framework tiers 1 to 4. The rows represent the aspects of exercise to be considered, which are the participant range, style of exercise, and aim. An organization with a certain tier profile can arrange an exercise according to the arrows in the column of each tier. Also, in order to plan an exercise to motivate a transition to the higher tier, the organization may adapt the exercise configuration that overlaying two columns.

4.2.1 *Range of Participants*

According to the NIST Cybersecurity Implementation Framework [36], the degree of preparedness (i.e. tiers) is also related to the extent of cyber security awareness within an organization hierarchy. Here we

	Tier 1 (Partial)	Tier 2 (Risk Informed)	Tier 3 (Repeatable)	Tier 4 (Adaptive)
Participant	Individual	Group (Department, Functional group)	Organizational	Stakeholder
Style	Game, Seminar	Workshop, Drill	Table-top Exercise	Functional Exercise, Full Scale Exercise
Aim	Awareness	Technical Skill	Non-technical Skill	Resilience

Figure 4.1: The guideline for exercise configuration with respect to each tier

describe the hierarchical levels within an organization and how their specific education can impact the organization's preparedness:

- Individual – within the *Tier 1* they are in charge of finding *ad hoc* solutions to a problem, even if awareness at the organizational level is limited. Therefore, *individuals* should be the target of specific personal exercises from *Tier 1*.
- Group – in *Tier 2* the administration approves risk management practices, but does not formalize them as organization-wide policy. Moreover, cyber security information is shared within the organization on an informal basis. In this context, groups of individuals may be the target of collaborative exercises to strengthen practices at a group level. For organizations ranked as *Tier 1*, new exercises programs should target groups for a smooth transition from *Tier 1* to *Tier 2*.
- Organization – in *Tier 3* an organization-wide approach to risk management is established. Organizational practices are regularly updated based on the changing threat and technology landscape. Therefore the organization should also be involved in exercises that reinforce practices as soon as they are updated. An organization that seeks to upgrade its tier rank from 2 to 3 should create new exercise programs at an organization-wide level.

- Stakeholder – in *Tier 3* multiple organizations should reinforce their ability to share information *after* a cyber security event occurs. While in *Tier 4*, exercises should also strengthen information sharing among stakeholders *before* a cyber security event. Upgrading from tier 3 to 4 requires an organization to setup new exercises that target information sharing for prevention.

4.2.2 Exercise Styles

The use of exercises is one of the most effective measures to improve awareness and preparedness, both in the fields of physical [37] and cyber security [38] (Chapter 4). The former domain has been reviewed by the Homeland Security Exercise and Evaluation Program [37], which defined exercises according to two broad categories: *discussion based* and *operations based*. As opposed to the *operations based* category, the *discussion based* one do not involve deploying equipment or other resources. The *discussion based* category includes *table-top exercise, game, workshop, seminar*. On the other hand, the *operations based* category comprises *functional exercise, drill* and *full scale exercise*.

In the field of cyber security, the NIST Special Publication 800-84, covered *exercise, training* and *test* as available tools to improve the ability to prepare for, respond to, manage, and recover from adverse events that may affect the organization's missions [38]. Specifically, two styles of *exercise* are highlighted as the most widely used: *table-top* and *functional exercise*.

Here we review all the available styles of exercises in the order of complexity. Simple exercises such as seminar and gaming are appropriate for *Tier 1*, while more complex exercises, such as the full-scale exercise, are suitable for *Tier 4*.

- Seminar – informal discussion that provides an overview of –new or updated– plans, policies, procedures, protocols, resources, authorities, concepts, and ideas. This type of exercise is useful for *Tier 1* organizations to form organizational cyber security risk management practice. This would reinforce current capabilities and lead to a smooth transition to *Tier 2*.

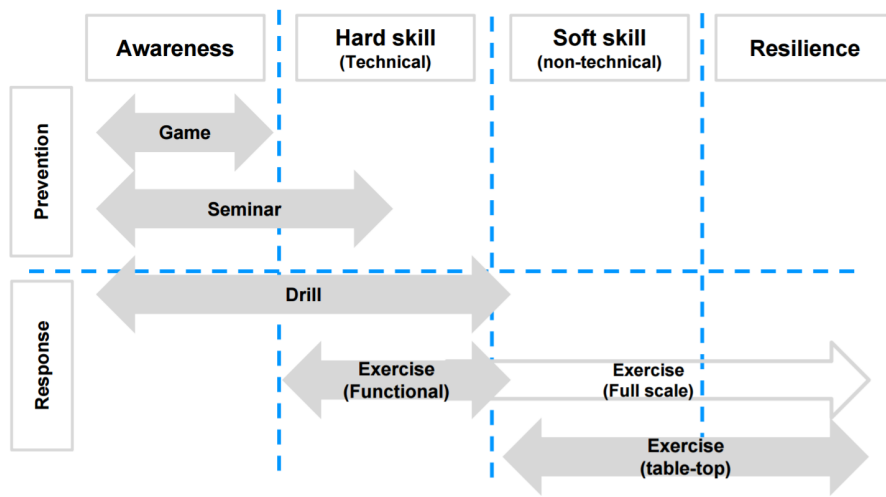


Figure 4.2: Mapping of exercise styles into the category of targeted achievement

- **Game** – games are often played by two or more teams that make decisions and actions in a hypothetical situation. The consequences of player actions can be predetermined or dynamically decided. This style is useful to validate procedures or evaluate resource requirements. As with seminars, games can be used to gain awareness about the cyber security risk within an organization to reinforce capabilities and reach *Tier 2*.
- **Workshop** – they are similar to seminars; however, they are characterized by an increased interaction among participants and they focus on building a product. To be effective, they should have clearly defined objectives, products, or goals, focus on a specific issue, and be attended by relevant stakeholders. This type of exercise can be used to reinforce risk management practices (*Tier 2*), or to review the organizational policy towards transition to *Tier 3*.
- **Drill** – it is a coordinated, supervised activity that aims at validating a specific function within a single organization. Typically it is employed to learn new equipment, validate procedures or practice skills. It is also useful to understand if plans can be ef-

fectively executed, if more training is needed, or to reinforce best practices. Personnel need to be familiar with the procedures to be drilled. Since drills are used for the reinforcement of practices, it is most effective when repeated on a regular basis. The practices being reinforced should be already validated and approved by management, which means that awareness at the organizational level is already established (*Tier 2*).

- Functional exercise – it is covered both by the HSEEP and NIST documents. It is designed to validate and evaluate coordination, command and control functions of personnel. An exercise scenario typically drives events at the management level, in a realistic real-time environment, where movement of personnel and equipment is simulated. The exercise controllers typically use an event list to ensure that activity remains within predefined boundaries and that objectives are accomplished. Simulators can inject scenario elements to simulate real events. Functional exercises can be used to strengthen the current capabilities, and to achieve high *adaptability* (*Tier 3-4*).
- Table-top exercise – it is covered both by the HSEEP and NIST documents. The personnel participates as individuals or groups and discusses about roles and responses options during a hypothetical, simulated emergency. This style of exercise can be used to enhance general awareness, conceptual understanding, validate procedures, rehearse concepts and assess the systems needs with respect to prevention, protection, mitigation, response and recovery. Table-top exercise is especially effective to review management procedures and to validate management skills. Given its complexity, it is suitable for *Tiers 3-4*.
- Full scale exercise – it is the most complex type of exercise. A multi-agency, multi-jurisdictional, multi-discipline exercise that aims at validating multiple aspects of preparedness. Activity in the exercise scenario are driven with real-time event updates at the operational level, that try to reconstruct the stressful environment of a real incident. Personnel and resources may be actually mobilized. Problems are realistic and require critical thinking, rapid and effective responses; activities may occur simultane-

ously. Given the complexity of the exercise, it is appropriate for *Tier 4*.

It should be noted that as defined in chapter 2, the expected outcome from drills and exercises are different in its nature. Drills are effective in preparation for certain scenario, and achieve faster first response coordination. However, it rarely test the organization's flexibility and stimulate participant's knowledge based problem solving skill. On the other hand, since exercises often conducted in different scenario every time, it may lack the repetitive practice of coordination in the same situation.

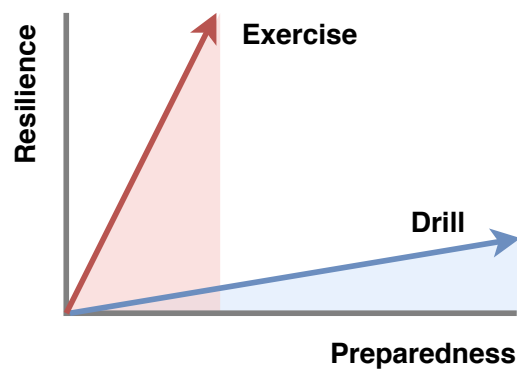


Figure 4.3: Difference of expected effects from exercise and drill.

4.2.3 *Exercise Aim*

The style of an exercise affects the possible range of aims to be designed. Figure 4.2 is a mapping of exercise styles into the category of targeted achievement. The expected outcome is the acquisition of awareness, technical-skill, non-technical skill, or resilience. The acquisition of these skills will improve the protection or response capability. In this context, the broader meaning of response is adopted, which includes detect, respond, recover functions identified in the NIST framework.

- Awareness - Awareness exercise is useful to introduce the personnel to cyber security. This type of exercise is beneficial for organizations in tier 1 and tier 2. It reinforces the concept of cyber security to beginners in tier 1, and for the organizations

in tier 2. It can also be used to reinforce roles and responsibility that personnel has within the organization. Achieving the organization-wide security awareness will lead tier 1 organizations to reach a higher tier.

- Technical skill - Exercises designed to aim for the acquisition of technical skills are mainly targeted to certain personnel who has to operate a particular procedure regarding cyber incident management. This type of exercise often takes the style of drills and functional exercises. It strengthens the cyber security duty assigned to staff members in tier 2. Periodic exercise should be organized in tier 3 and 4.
- Non technical skills - besides the technical skillsets, the so-called non technical skills, such as coordination, communication, and decision making, are also an important factor in establishing high incident management capability. It can be trained in discussion-based exercises, such as the table top exercise. The reinforcement of non technical skills will allow a better coordination of individual or divisional functions. It is also useful to review the command and control structure of organizations in tier 3.
- Resilience - Complex exercises such as full-scale and table-top ones can evaluate the adaptiveness of an organization to the unexpected situation. These exercises aim to achieve a higher resiliency in the organization and they appropriate for tier 4 organizations.

Appendix B.1 shows the example of how one form of exercise can be adapted to several tier levels, by examining observed cases from CIIREX¹.

4.3 EXERCISE PROGRAM DESIGN FRAMEWORK

Basic security measures are essential in the same way as basic hygiene is important to maintain health and prevent disease. Cyber Hygiene is the concept developed based on the personal hygiene. Although

¹ Critical Infrastructure Incident Response Exercise

washing hands may not prevent the complicated disease, but you will have less chance catching a cold. Cyber hygiene may not be effective for the highly targeted attack, however, there will be less chance of the low profiled cyber attack damaging the system. Same fundamental strength is necessary in terms of cyber resilience.

Literature and field studies in chapter 2 and 3 suggest that high cyber resilience in the organization can be achieved when the organization is trained and has a basic knowledge and skill (Figure 4.4).



Figure 4.4: Achieving resilience requires awareness and preparedness as its foundation.

In order to achieve resilience by exercise, awareness and fundamental preparedness (both technical and non-technical) are necessary. In the chapter 2 we reviewed a variety of trading available for control system security. So far we have discussed the effect of training as a single, discontinuous event. However, from asset owners perspective, managing cyber incident handling capability is a continuous improvement. Organizations develop the contingency plan and policy, create procedures, invest in technologies to automate process, and exercise and review the capability.

For this reason, repeating the exercise matching to current capability is not sufficient. Exercise should challenge the organizations preparedness, therefore planned to achieve the targeted maturity level. The process will be a multi year program with continuous improvement.

Figure 4.5 shows the road-map for exercise program design. The model is based on the build-up model shown in the figure 4.4, tar-

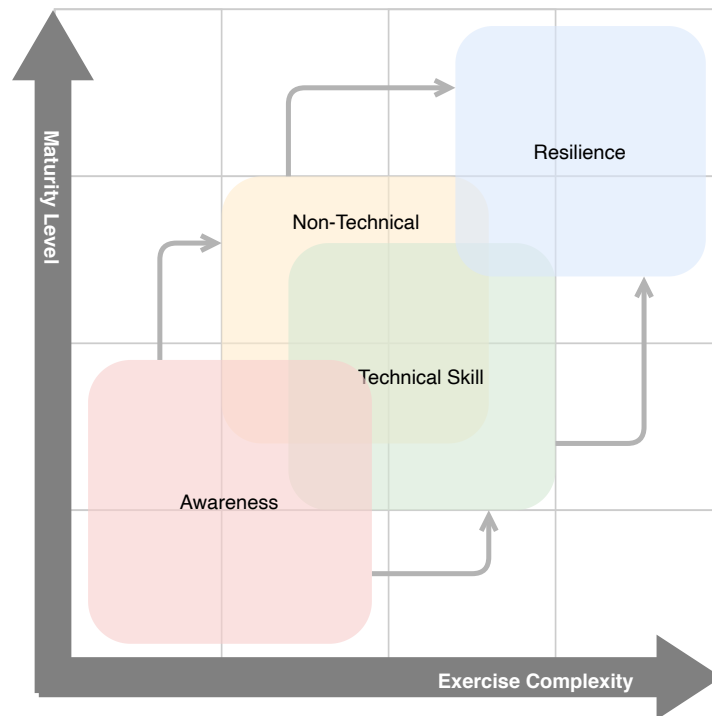


Figure 4.5: Relation between the maturity and exercise goals.

getting from awareness, preparedness then to resilience. It is recommended to start to implement training aiming to gain awareness in the organization especially while the organization is not matured. This type of training can be conducted to stakeholders throughout the organization, and recommended to perform repeatedly. The technical and non-technical training such as table-top exercises and drills are recommended as the next step. Especially drills will help the organization to understand and establish the first response coordination. Once organization achieved certain maturity, more complex exercise including functional and table-top exercises, and full-scale exercises to test organization's crisis plan for unexpected or extreme situation.

4.4 CONCLUSION

In this chapter, we proposed a guideline to select the best exercise style, aim and participants according to the current level of preparedness of an organization, and according to the possible need to improve such capabilities. For this purpose, we adopted the ranking of preparedness (i.e. tiers) formalized by the NIST Cybersecurity Implementation

Framework. Subsequently, we reviewed the styles of exercises that are used both in the cyber (NIST) and physical (HSEEP) security domains. Based on this review we hypothesised that games and seminars are suitable for low degrees of preparedness; workshops are useful at an intermediate degree; while functional, table-top, drill and full-scale exercises range from intermediate to high degrees.

Furthermore, according to the characteristics of the NIST implementation tiers, we recommend to include participants according to a proportional rule between the *tiers* (from 1 to 4) and the hierarchical level of an organization (from individual to stakeholders). Similarly, the aim of the exercise (from awareness to resilience) should be proportional to the tiers (from 1 to 4). The adoption of these guidelines would guarantee that lessons learned from exercises are well absorbed by the personnel, resources are not wasted, and improvement of capabilities is smooth between tiers.

The concepts expressed in this paper are inspired by observation at private BCM² exercises and at available domestic cyber security training programs, such as the CIIREX Critical Infrastructure Incident Response Exercise organized by NISC. The proposed guideline should be validated empirically and experimentally. Therefore, future studies should evaluate the application of the proposed guideline to the available exercises, and examine how it impacts the organizations in reality.

² Business Continuity Management

EXERCISE DEVELOPMENT UNDER UNIFIED STRUCTURE

Achievement of a secure and resilient society requires a shared protocol among stakeholders. Even within the organization, cyber incident communication is a challenge because of the conflicting value of safety and security. We designed the training program specifically to address this problem in align with the maturity-based exercise model presented in chapter 4.

5.1 EXERCISE PROGRAM DESIGN

5.1.1 *Designing a Curriculum*

Based on the framework proposed in chapter 4, we designed ICS security training curriculum for professionals (Figure 5.1). Using our water circulation ICS testbed as the main scenario source, we create several exercises.

- **Live Demonstration** - Cyber attack demonstration on ICS testbed system.
- **KIPS+ Communication Card Game** - Communication exercise between IT - ICS engineer.

- **Card Exercise** - TTX¹ for developing incident management procedure.
- **Hands-on Training** - Offence and Defence skill training for ICS security to complement exercise programs.
- **Tsurumai-Go** - Computer based functional exercise for understanding the communication procedure.
- **Workflow Exercise** - TTX for creating incident management structure with safety, security and business continuity harmonization.



Figure 5.1: Proposed cyber resilience exercise program.

We have introduced and been offering this program to the following cases;

- NITech² ICS security workshop, since 2015, 1-2 day(s), 1-2 times per year, 30-40 participants per time.
- Fujitsu Learning Media cyber security training course, 2016-2017, 4 days, annual, 20-30 participants per time.

¹ Table-top Exercise

² Nagoya Institute of Technology

- City of Nagoya IoT security series, since 2018, 4 days, 1-2 times per year, 30 - 40 participants per time.
- ICSCoE Industrial Cybersecurity Center of Excellence core expert development program since 2017, 1 year, 60-80 participants per year.

5.1.2 *Goals of the Program*

Communication Management

We studied management issues in the incident response in chapter 3. Observations suggested the cross-department communication is a key issue to achieve high resilience in the organization. In fact, in some cases, good communication can not only streamline the operation, but can add value to the organization by positive reinforcement (Appendix A.2).

As previously mentioned, the lack of communication skills is a major issue in cyber incident management. Therefore, the exercise has the major objective of highlighting the importance of communication and cooperation among CI stakeholders. Specifically, the scenario represents a cyber incident within a simplified organization structure, where participants discuss and strategize countermeasures with a bird's-eye-view, that is without playing a specific role. This helps them understand the importance of effective communication among stakeholders, rather than focus excessively on technical aspects.

Security, Safety, and Business Continuity

In ICS environment, safety is always the first priority. We have studied the relationship of safety and security risks in ICS, aiming to unify safety and security measurement in one perspective (Appendix A.1). Usually, in critical infrastructure companies, a production division prepares safety-BCP³s against physical troubles, such as fires, toxic spills, and natural disasters. An information system division also has prepared IT-BCPs to respond to cyber incidents on the business

³ Business Continuity Planning

network, such as information leaks and so on. Some cyber attacks on the ICS cause hazardous situations in the plant, and as a result, it should invoke a particular BCP of the company. There are, however, difficulties in integrating safety-BCPs and IT-BCPs because of a lack of experience of cyber incidents that covers the both BCPs.

For preparing the above situation, each company has to plan required corporate resources and educate their staffs and operators using an SSBC (Safety-Security-Business Continuity) exercise.

5.1.3 *Method: Discussion-Based Exercise*

Considering the sectorized nature of the existing Japanese CIP⁴ training programs, our aim is to develop an exercise that is open for any CI stakeholder, and that enables knowledge transfer among participants. This motivated the adoption of a discussion-based table-top exercise style, since it stimulates the discussion among participants with a large variety of backgrounds, allowing them to compare their views on an issue [61]. In addition, it is often used to develop new plans and procedures, focusing on strategic issues [62]. For all these reasons, it provides new perspectives to each participant's conceptual knowledge structure, and helps to build a shared mental model among them.

5.2 EXERCISE ENVIRONMENT

5.2.1 *NITech Testbed*

We developed multiple training scenario around NITech ICS testbed settings (Figure 5.2). In 2012, a testbed for ICS security was developed in NITech. The design of the specifications of the testbed is based on the requirements of those who are concerned with control systems security (e.g. vendors, researchers, users etc.). From the requirement analysis, the purpose of the testbed was decided as follows:

⁴ Critical Infrastructure Protection



Figure 5.2: The plant side (left) and the operator side (right) of the testbed. Testbed visitors can operate the system during the demonstration.

- Training for gaining public awareness: the testbed will be used as an educational training tool, in order to show the importance of cyber security and the threat of cyber attacks.
- Intrusion detection: the testbed is used to test the intrusion detection tool under development.
- Improvement of plant resiliency: data obtained from the testbed by simulating plant operation will be analysed, for the research on the effectiveness of security and safety measures.

5.2.2 Testbed Structure

The testbed consists of two plant systems, a controlling network for each plant, and a corporate network connecting the two control networks. Each plant is a closed hot water circulation system consisting of two tanks: water in the lower tank is heated by a heater, then circulated to the upper tank by a pump. With respect to the exercise, the testbed models a community heating/cooling facility of a fictitious company that provides services to two different areas [63]. Safety violations, such as spilling water or heating an empty tank, could not only damage the equipment and harm the personnel, but may cause the discontinuation of the plant.

The network structure and PID⁵ of the target organization is shown in the figure 5.3, 5.4. The service that this company does is a service that generates energy to move air conditioning and supplies energy to the area. The tank 1 is a tank possessed by a supplier, and the tank 2 is a tank holding 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

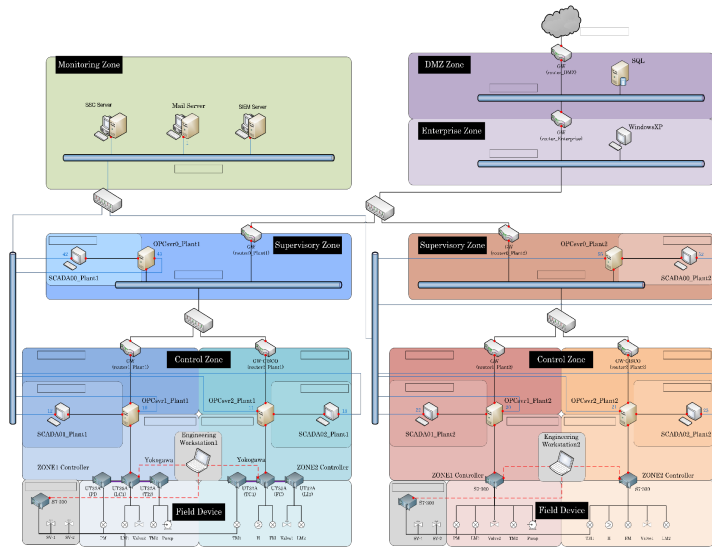


Figure 5.3: Network architecture of the testbed.

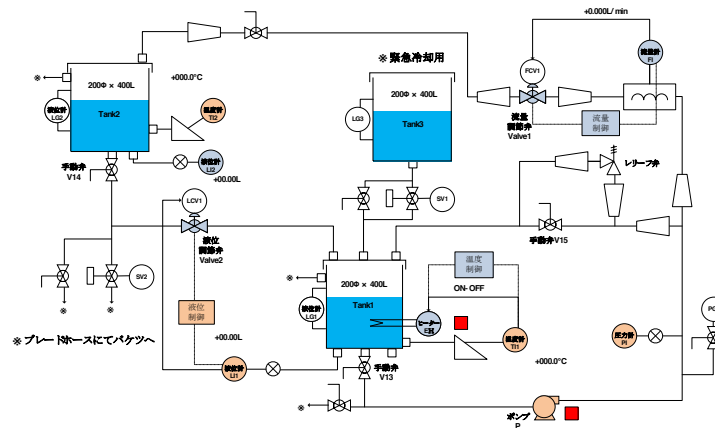


Figure 5.4: Piping and Instrumentation Diagram of the testbed.

Zoning and firewalls are also introduced as network security measures. Control of Valve 2 and heater by SLC⁶ in the different zone

⁵ Piping and Instrumentation Diagram
⁶ Single Loop Controller

makes it possible to detect empty firing events caused by lowering of the liquid level of Tank 1 and continuation of heater operation. Also, by looking at the level of each tank on the SCADA⁷ screen in each Zone, you can notice abnormality even if one screen is concealed by cyber attack. Moreover, by installing a firewall, it is possible to detect and block suspicious communication from outside.

5.3 CORE SCENARIO DEVELOPMENT

Participants of the SSBC (Safety-Security-Business Continuity) exercise need to learn not only safety methods but also security methods against cyber attacks on a simulated plant with field control devices, ICS networks, and information networks that mimic corporate operation structure.

Critical infrastructure companies, therefore, need to prepare training facilities that include simulated plants with control systems. Using this facility, not only field operators but also IT staffs and managers learn the knowledge of process safety and practical procedures under cyber attacks.

The SSBC exercise is conducted on a scenario that reflects company's profile. Through this exercise, participants have to learn the knowledge of security measures and security-related operation processes on the simulated plant. The proposed design procedure of the SSBC exercise is shown in Figure 5.5.

In the procedure, in the first step, a virtual company for the exercise is specified based on the actual company's profile, and possible attack scenarios to the company are selected. In the second step, process operations based on the company's standardized safety procedure are assigned to meet the simulated plant. In the third step, safety counteractions are taken into consideration selected process signals affected by the result of the cyber attack. In this step, additional conditions, resources to the existing safety-BCP will be clarified.

Then, security counteractions are specified to arrange the existing IT-BCPs where business impacts are considered based on the virtual

⁷ Supervisory Control And Data Acquisition

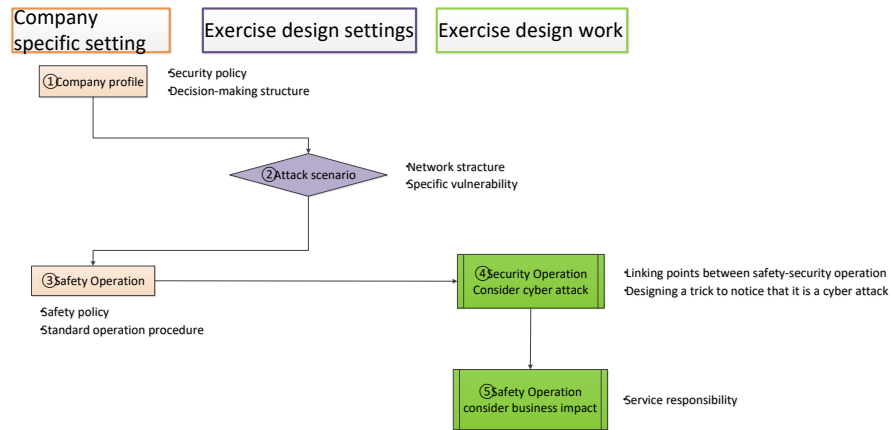


Figure 5.5: Exercise design procedure and points of company uniqueness.

company's profile. In this step, factors such as company's security policies, and network and communication structures will be testified their readiness and resilience to bottom-up actions from the field operation to the company's business operations.

5.3.1 Company Profile

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

- Business contents
- Organizational structure
- Organization's role (Routine work, Skills)
- Communication role
- Plant structure
- Network structure

It is difficult to evaluate the impacts of the cyber attacks on the company if the network structure does not match the actual structure characteristics. Accordingly, for example, it is also desirable to take into account the structure connecting between the local production sites and the headquarters. However, if the actual conditions are used for exercise, the exercise becomes complicated, so the selected conditions

should be simplified. These selected conditions are temporary and evolutionary improved through the exercise-evaluation process (a kind of PDCA cycle).

5.3.2 *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 many serious accidents. Therefore, it is necessary for the cyber attack to be recognized by the participants as a real problem with the importance of the security measures in the exercise. An exercise developer should create the scenario that enables the participants to notice the attacks through the security measures designed in the scenario. Likewise, if in the scenario, an intruder (external factor) intrudes from a place without security measures and causes the cyber attack, 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[51]. However, in the exercise, it is desirable to assume the worst possible scenario from the viewpoints of risk management and education thereof. In our created scenario, we have considered the flow of the Cyber Kill Chain in a reverse direction (Table 5.1) 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, in consideration of the safety measures, a discussion is made for mainly about changing the safety measures in a plant site. At the same time, a discussion is also made for the development of 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

Table 5.1: Procedure for the cyber-attack scenario

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 & Control	5. Prerequisite for attack (Compromise)
6th-Lateral Movement / Pivoting	6. Recent situation scenario ₂ (Delivery)
7th- Objectives / Exfiltration	7. Recent situation scenario ₁ (Reconnaissance)

by the participants. Also, in the scenario, it is preferable that target sites to be attacked should have a linked business structure (such as a supply-chain, a common market) so that business conflicts to be considered by the attacks is built into the exercise.

Second, abnormalities (risks) such as accidents and breakdowns not wanted to happen are identified. Regarding safety and security, abnormalities that can occur in the simulated plants are identified. In term of businesses, possible management risks are identified. First of all, as a company, the maximum goal in safety security business is raised. Next, risks that may hinder that goal are conceived. Finally, outliers that cause that risks are identified. In this way, specific plans can be listed in order so that various opinions are revealed easily. 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 belonging to various departments, such as site operators, IT engineers, and managers involve 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, those in security and those in business. After roughly dividing 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, key events in the 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, that is a major 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 troublesome (on frequency) abnormalities are selected. Thus, the participants have increased some opportunities to consider his or her experiences referring to the abnormalities in the exercise. In other words, safety measures considered in the exercise are likely to be reflected his or her business activities resulting in the more practical exercise.

In the exercise, linking points between safety-security operation processes and business continuity operation processes are also implicated in recognizing safety-security-business constraint of each linking point with the market impact. Therefore, it is necessary to select common anomalies related to safety, security, and business. 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 viewpoint of the attacker. 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 to recognize the cyber attack.

5.3.3 *Defense Scenario for Plant Operation*

The abnormality, which can occur at the site, does not change even in the case of cyber attack nor 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 by incorporating the result of the safety measure (situation) into the defense scenario based on the attack scenario.

By trying an attack similar to the attack in the attack scenario to the simulated plant, it is possible to create the defense scenario into which more accurate information is incorporated. Moreover, then, it is preferable to select a person who is involved in a security field or in on-site work as a designer 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. In consideration of 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?

In an existing safety measure, it is required to cope with actually occurred abnormalities. Also, under the influence of the cyber attacks, since concealment and simultaneous occurrence of abnormalities may be performed, not only the abnormalities which may be caused at a place where the abnormality is at present not confirmed but also abnormalities caused on purpose should be watched out. 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 status of the device by using the vendors provided engineering stations.

Besides, the degree of impacts from the cyber attack changes communication among corporate departments. When an abnormality occurs, opportunities to cope with other departments (normally irrelevant departments) will increase. Also, the information sharing method should

be considered so as not to become a bottleneck in the overall operation. In cooperation with departments in different technical fields, it is necessary to consider information sharing protocol to reduce traffic volume and errors.

ORGANIZATIONAL SCENARIO. It is desirable to design the exercise so that the participants can focus on the safety measures newly added in consideration of the cyber attacks. Therefore, only the place where the required safety measures are made is left separately from the existing safety measures to create the attack scenario and the defense scenario. However, when only the place to be added is left as an exercise, it does not add up. To cope with this, necessary information in the front and back of the place is left.

Also, it is necessary to incorporate the conflicts that may occur in the actual measure into the exercise. Specifically, there is the conflict where the priority of measures cannot be determined easily in forming a work flow, the conflict where the measures cannot be concurrently performed but overlapped, and the conflict where it seems that a communication pass cannot be connected smoothly. Also, the aforementioned necessary information in the front and the back of the place should be left. Each conflict installed may occur in the actual situation, and the participants should experience conflicts through the exercise.

5.3.4 *Roles Defined*

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.

5.3.5 *Scenario Phases*

The phases of the scenario follow the time line of incident handling proposed by Sheffi et al. [64]. They suggested that any significant

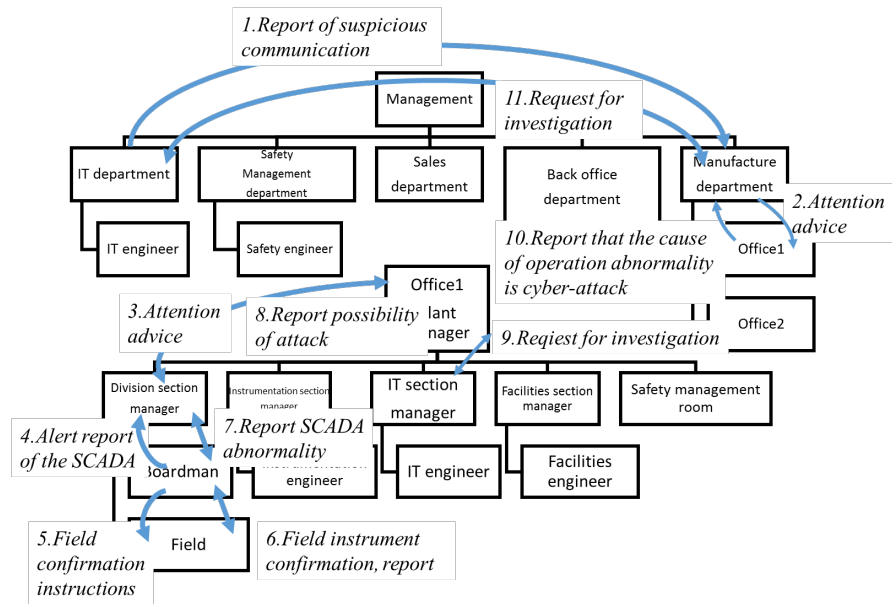


Figure 5.6: Roles and communication paths defined in the exercise.

disruption has a typical profile in terms of its effect on company performance. Moreover, the nature of the disruption and the dynamics of the company’s response can be characterized by eight phases (Figure 5.7). From the originally proposed, three phases were adopted in the exercise: first response to an disruptive event, preparation for recovery, and recovery. In the following paragraphs, the phases are described in detail, under the convention that *italicized* text represents the actual scenario descriptions provided to the participants.

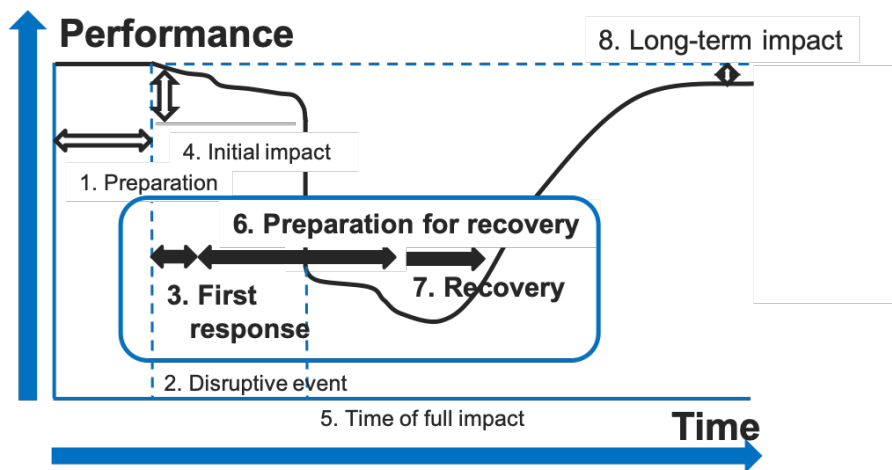


Figure 5.7: Stages of disruption proposed by Y.Sheffi [64], recreated by the authors.

DISRUPTIVE EVENT / FIRST RESPONSE. The exercise starts when *an anomaly in network traffic is detected by the monitoring room and control room operators in Plant No. 2 notice unexpected value declaration in a level sensor*. The goal of this phase is to determine that the incident is caused by a cyber attack, and that is not the result of either equipment or sensor failure. The participants discuss how to implement a cyber incident response for a transition to safe manual operation of the plant, and how IT and other departments can support the plant system to achieve safety.

PREPARATION FOR RECOVERY. The preconditions of this phase are that proofs of a cyber attack are confirmed (i.e. *no equipment/sensor malfunction detected, the configuration file of an OPC server in Plant No. 2 has been changed in an unauthorized manner*) and that *Plant No. 2 is operated manually*. The key decision-making in this phase is whether operation in Plant No. 2 should be shut down. Moreover, in case the plant is kept in manual operation, what measure should be taken to ensure safety. The participants discuss what kind of information is required to make a decision, if such information is available, and who has the authority to make a decision in this circumstance. They will conceive how to conduct business continuity management, in order to mitigate the further impact on business performance by the disruption. For example, what action should be taken at Plant No. 1 which is connected to Plant No. 2 through the corporate network, and what roles do the sales and public relations (PR) departments play.

RECOVERY. This phase assumes that the following conditions are met: *Plant No. 2 has been shut down and Plant No. 1 is operating without network connection (limited productivity)*. The task in this phase is to plan the efficient and safe plant reactivation based on the start up procedure manual. Additionally, participants review the past phases and discuss the measures to prevent a recurring failure.

As for the third and final phase of the exercise, the goal is to reexamine the balance of technical, management, and external cooperation capability to achieve high resiliency in the organization.

5.4 GAMING: COMMUNICATION TRAINING WITH KIPS+

5.4.1 *Gaming Simulation Structure of KIPS*

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. Prior to starting the four phases, the moderator explains the rules of KIPS and shows the participants 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 news from the same industry and the status of the plant. Next, in the action phase, players evaluate the current situation and use action cards as countermeasures using the game console. 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 their 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 card which leads new event. In the report phase, all players review their team's result.

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 5.8 shows the relationships among the KIPS stakeholders.

5.4.2 *Inter-organization Cooperation*

KIPS was designed to show importance of inter-organizational incident response through game simulation. KIPS participants play the role of a security administrator. However, compared to real CI companies, an incident response is performed by several departments

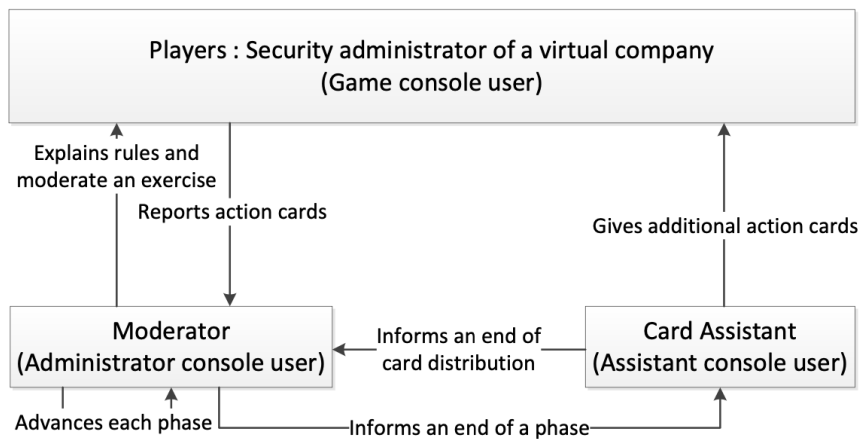


Figure 5.8: Kaspersky Industrial Protection Simulation structure.

because both business and safety objectives should be considered simultaneously relative to a cyber incident.

However, these objectives sometimes have a low affinity of a response due to differences among the policies of different departments. Therefore, we incorporate a cooperative inter-organization perspective into KIPS. Therefore, we consider following mechanisms to design KIPS from the perspective of inter-organization cooperation.

SEPARATE A 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 a group's 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.

5.4.3 *Proposed Exercise Method*

To create the information gap within a team, players form two groups, i.e., a plant administrator group and a headquarters administrator group (Figure 5.9).

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 information about 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 facilitator. The facilitator provides information about the message phase with the plant and headquarter 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 process five times. Figure

3 shows the relationships among the stakeholders in the proposed exercise.

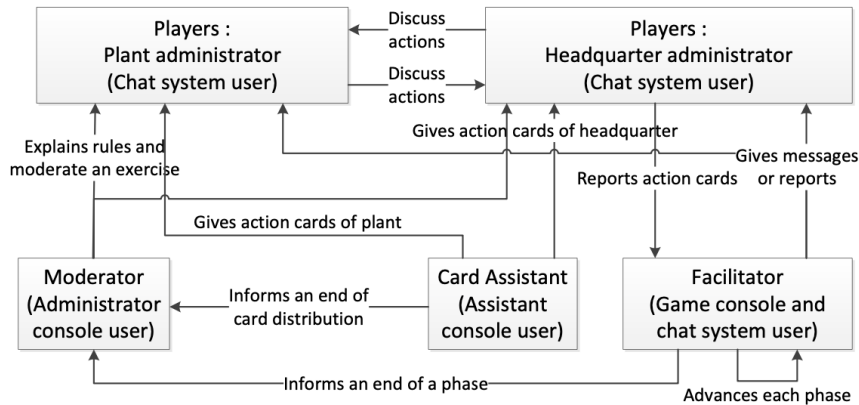


Figure 5.9: Kaspersky Industrial Protection Simulation+ structure.

5.4.4 Implementation and Trial

Prototype Implementation

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 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 administrators and the plant administrators. Note that the facilitator could observe channel 3 to understand the teams' situations. In appendix C.2, we provide the operation manual developed for this trial.

Trial of KIPS+

In September 2017, the proposed exercise was performed with 42 participants involved in CI companies. Seven teams were organized in this trial. Facilitator provide information with head quarter group and site group. Participants try a prototype game and evaluate if the game is good to make aware an importance of communication skill

of incident response by a survey. As a result, 97% of the participants desired implementation of the proposed exercise at their company, which shows that this exercise is an effective evaluation tool.

we have proposed a new cyber incident exercise method that considers the complexity of decision making and communication skills. KIPS is an effective training tool for security awareness at CI companies; thus, we redesigned KIPS as an inter- organization exercise by implementing a chat system. An initial trial of the proposed exercise satisfied many participants who work at CI companies. In future, we plan to analyze the chat log of players that earned high revenue to determine effective communication processes.

5.5 FUNCTIONAL EXERCISE: TSURUMAIGO

5.5.1 *Incident Commanding Structure*

Even if CIs prepare the cyber incident response plan, it is not easy for companies to implement cyber incident response plan that does not have experience. Cyber incidents in ICS cause not only problems with cyber security but also problems with plant's safety and company's business. Therefore, against cyber incidents in ICS, multiple departments such as IT department and ICS department must proceed response in parallel. However, when multiple departments proceed response in parallel, there may be errors in decision-making due to lack of information sharing among departments and conflicts due to differences in response objectives between departments. Therefore, under cyber incidents in ICS, Incident Commanders (from now on referred to as the "commanders") to coordinate and make decisions between departments are especially important.

Many companies have Computer Security Incident Response Team (CSIRT) as commanders against cyber incidents in IT. However, few companies have specialized response teams against cyber incidents in ICS. Therefore, if cyber incidents occur in ICS, the leaders of divisions or departments in the existing organization may have to become commanders. However, it is challenging for anyone who has never ex-

perienced cyber incidents in ICS to properly perform the commander role. For this reason, companies holding CIs need to educate position who have to become commander under cyber incidents in ICS. Therefore, in this research, the authors will develop training for Incident Commander's educational support for companies holding CIs. However, in cyber incidents in ICS, abnormal situations in each company is unique to each company occurs. The role that commanders should be in cyber incidents varies widely from company to company, and therefore, the content of their training needs to be customized for each company. However, it is inefficient for us to develop customized training for each company. For this reason, the training is developed in this research must include the mechanism that each company can customize on its own. Thus, cyber exercise is developed in this research is training for commanders, including the mechanism that each company can customize in-house.

5.5.2 *Proposed Exercise Structure*

Form of Training

To customize the training for each company, the training components need to be divided into parts that are common to all critical infrastructure companies and parts that must depend on the individual characteristics of each company. Customizing the training is to change the part of the training that depends on the individual nature of each company, which is a component of the training, into one that is unique to each company. To do this, training in the form of computer games is useful. Computer games consist of programs and data embedded in programs. For this reason, in computer games, the programs are a common part that can be used by all critical infrastructure companies, and the data can be viewed as a part that depends on the individuality of each company. Therefore, incorporating company-specific information into the data creates a customized computer game for each company. Therefore, the fact that the training is in the form of computer games is effective from the viewpoint that the training can be customized for each company, and therefore, the training be developed in this research is in the form of computer games.

Requirements for the Gaming elements

The purpose of the computer game is to enable participants to learn about the role of commanders and to perform that role properly. For this purpose, simulated training methods that allow participants to experience the role of commanders are useful. For this reason, it is essential to have mechanisms that allow participants to simulate the role of commanders in the computer game. To clarify what commanders should do cyber incidents to clarify the mechanism required for the computer game. Cyber incidents in ICS cause not only cyber security issues but also safety and business issues simultaneously. For this reason, not only IT departments, but also ICS departments, management, and others need to take action at the same time. To facilitate this company-wide response, it is necessary for the leaders of each department to act as commanders, to coordinate among departments, and to direct the company-wide response. To do this, each commander must perform the following:

- Collection of information on cyber incidents (information on damage status of ICS, network logs, operation status, etc.)
- Sharing information with other commanders and external organizations (customers and affiliates)
- Decision making based on information obtained and task instructions to workers and other commanders based on contents of decision making.

Thus, for the participants to simulate the role of commanders, the following mechanisms need to be established in the computer game.

- Mechanism by which more than one participant can participate in the computer game as another commander (ICS Director, IT Director, Management, etc.)
- Mechanism by which participants can collect information, share information, and issue task instructions as commanders

To illustrate these mechanisms, the computer game with the configuration shown in Figure 5.10 is proposed.

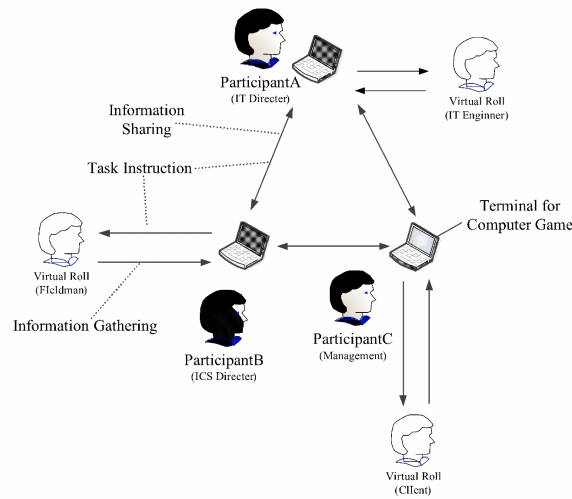


Figure 5.10: TsurumaiGo exercise structure.

Each participant has the terminal for the computer game and participates in the computer game as the separate commander. Each participant uses the terminal to collect information, share information, and issue task instructions among the participants. However, the commander needs to collaborate not only with other commanders but also with workers who are subordinates of the commander and external organizations (customers, affiliates, etc.). For this reason, it is necessary to prepare workers and external organizations as virtual roles on the computer game, which have the function of returning responses to collecting information, sharing information, and task instructions from participants. This allows each participant to interact not only with other participants but also with his subordinates and external organizations within the computer game.

Also, to play the computer game, scenarios for proceeding the computer game is required. The game scenarios consist of cyber attacks scenario and an ICS state transition scenario affected by cyber attacks. Based on the game scenarios, Virtual roles must respond to the participant. Participants understand the situation by using information from the Virtual roles. The computer game also requires the mechanism whereby the instruction is reflected in the game scenarios when participants issue the task instructions to the Virtual roles. For example, if the ICS Director instructs the Fieldman to operate the ICS, then the status of the ICS in the gaming scenarios must change to the state

in which the instruction is reflected. This mechanism is essential in the computer game, and with this mechanism, participants can aim for convergence of cyber incidents in ICS, which is the goal of the computer game.

Thus, the requirements to be met by the computer game are as follows.

- Some participants can participate in the computer game as separate commanders
- Each participant can collect information, share information, and perform task instructions to other participants and virtual roles.
- Based on the game scenarios, the Virtual roles interact with the participants.
- Task instructions to the participants' workers are reflected in the game scenario

Additionally, what is indispensable in training is the feedback after training. In feedback, participants should assess whether they were able to adequately perform their commander roles, identify problems, and discuss remedial measures. However, to provide feedback, a workflow is required to record what the participants did in the computer game. Therefore, the computer game also requires the ability to output workflows.

5.5.3 *Prototyping*

We developed the prototype computer game that satisfies the requirements described in the previous section. The programs of the computer game were described in Java. Figure 5.11 is the UI⁸ of terminals used by participants in the computer game. Participants can use this UI to collect information, share information, and issue task instructions. In UI, the communication sent and received is arranged in chronological order. Therefore, it is displayed on this UI when itself communicates with other participants or virtual roles, or when itself receives communication from other participants or virtual roles. Pressing the buttons

⁸ User Interface

above the tray in which the communication in Figure 5.11 is arranged opens the box shown in Figure 5.12. When communication contents, address, etc. are set in this box and transmitted, the information is sent to the specified address. The operation manual and materials are presented in appendix C.3.



Figure 5.11: User Interface of TsurumaiGo.



Figure 5.12: Action User Interface of TsurumaiGo.

5.5.4 Implementation of TsurumaiGo

In September 2017, the authors held the trial event of the prototype for 38 people from companies holding CIs. The data of prototype was developed based on the virtual company used in the current cyber exercise. As commanders of the virtual company, participants experienced the prototype with the goal of convergence of cyber incidents. Figure 5.13 is the deliverable by participants. In the workflow, rolls of the virtual company are aligned on the horizontal axis, and the vertical axis represents the time axis.

In the workflow, communication by participants at all timings is recorded. And workflows were evaluated by the following items.

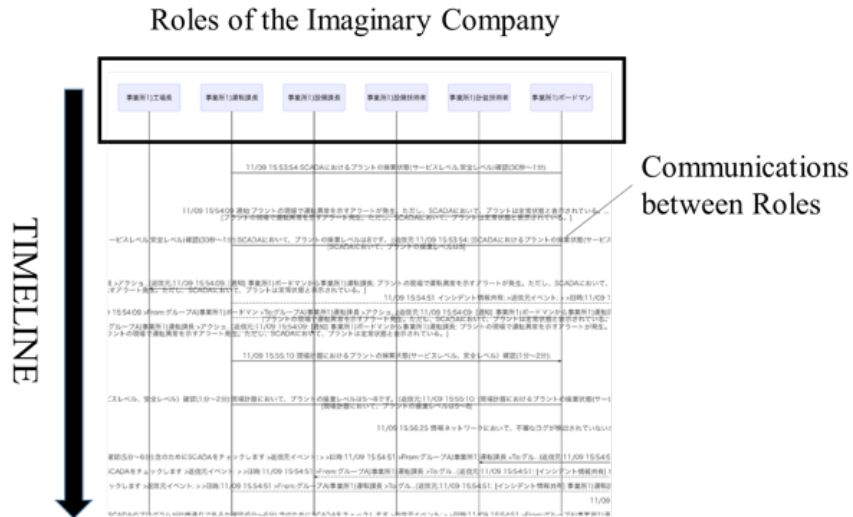


Figure 5.13: Example deliverable of the exercise.

- Whether it was possible to converge cyber incidents in the computer game
- Whether it was possible to implement appropriate information sharing and task instruction by appropriate timing

As a result of the evaluation, many teams failed to converge the cyber incidents. In the post-implementation questionnaire, 17 out of 38 respondents answered that they would be trained on the question, "Can this game be used to train the Incident Commanders?" Therefore, it can be said that this game was evaluated as effective to a certain extent.

In this research, the authors developed the cyber exercise in the form of a computer game for educating incident commanders in CI owner companies. Through workshops with OT and cyber security experts, the developed prototype was successfully evaluated by using the participants' questionnaire. To apply this prototype to each company, it is necessary to customize the data to reflect the situation (such as the organization structure, the jurisdiction scope, the corporate culture and so on) of each company. At present, however, the complexity of the data integrity makes it difficult to prepare unified template to simplify the customization. Accordingly, we will continue to develop the utility tools to promote our exercise.

5.6 TTX: WORKFLOW EXERCISE DESIGN

5.6.1 Exercise Steps

The exercise is composed of five steps: briefing, scene description, group work, discussion and debriefing (Figure 5.14). As mentioned in the previous section, the scenario is divided into three scenes (i.e. disruptive event / first response, preparation for recovery, and recovery). Therefore, scene description, group work and discussion are repeated as one cycle for each scene.

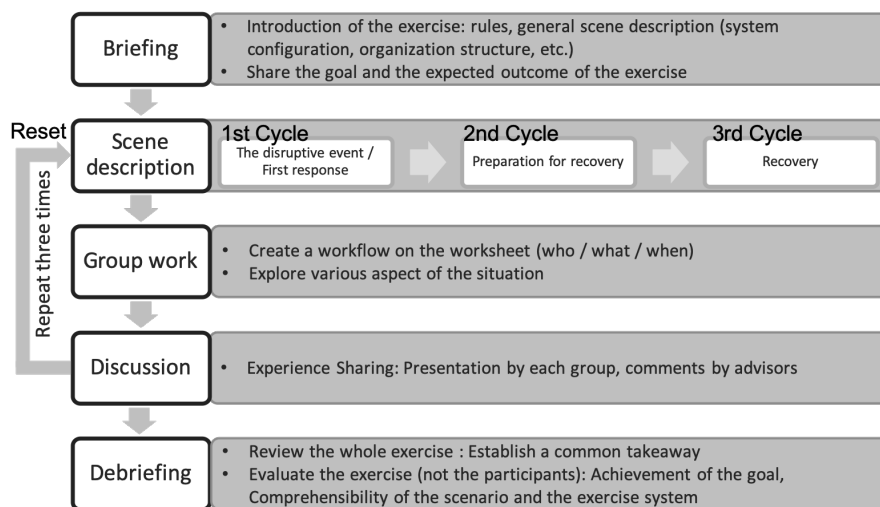


Figure 5.14: Exercise plan overview.

BRIEFING

At the beginning of the exercise, participants are divided into groups consisting of four to six members with different backgrounds. A facilitator introduces the group task and the general scenario. If needed, some ice breaker activities may be carried out to motivate all participants to become actively involved in the group work. Most importantly, the purpose of the exercise is shared with participants, so that they can all understand the significance of the activity.

SCENE DESCRIPTION

As for the opening of each scene, the status of the plant and IT network system are revealed along with the (fictitious) organiza-

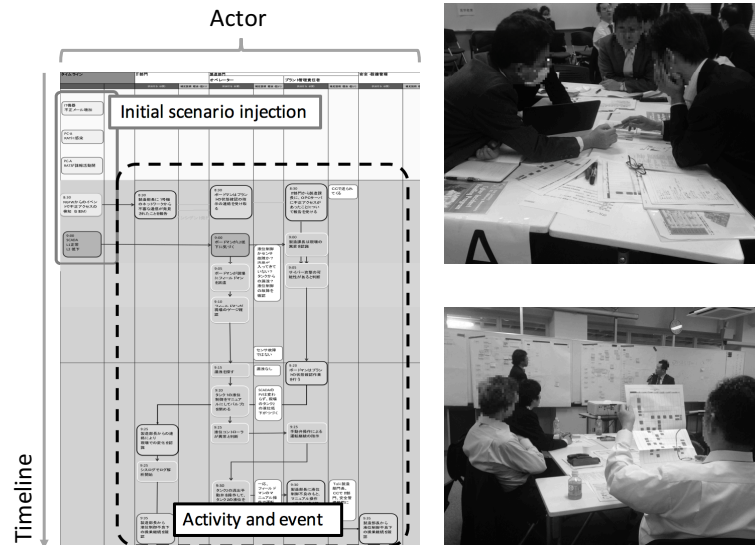


Figure 5.15: The example of the worksheet (left) and pictures from the exercise (right) where participants engage in group work (top right) and present their group work at discussion time (bottom right). Participants' faces are blurred out for their privacy.

tion's understanding of the situation. The scene is reenacted in a short video, which is used as visual aid.

GROUP WORK

The group task is to create a work flow of actions that would solve the given situation. Each group is provided with a printed A0-sized worksheet, colored sticky-notes, and markers. On the worksheet, the columns of actors (e.g. IT dept., manufacturing dept., maintenance dept.) and the initial scenario injections are printed (Figure 5.15). The list of actor names provided in the worksheet is not comprehensive, therefore participants are recommended to add/remove actor columns. At the beginning of each cycle, new worksheets including the scenario injections matching the current scene are distributed. The types of activity such as actor-system interaction (action) and actor-actor interaction (command) are color coded. In order to add an activity to the worksheet, a sticky-note of the matching color is used. In this way, the worksheet visualizes the flow of actors' actions and the organization's communication structure.

DISCUSSION

The former process helps participants to create shared mental models within their group. On the other hand, discussion and debriefing are activities that create a shared mental model among all participants. Discussion is the final step of one cycle. Each group gives a short presentation of their work flow while displaying the worksheet to everyone. The members of other groups may raise some questions. In this way, participants compare their worksheets to discover similarities and differences among their subjective perspectives regarding the many degrees-of-freedom of the scenario (e.g. likelihood of an event, consequence of an action).

DEBRIEFING

To conclude, the goals of the exercise are revisited, and participants share results and lessons learned. This activity helps the organizers to evaluate if the exercise method was appropriate, and more importantly, if the intended learning outcomes are achieved.

5.6.2 *White Teaming*

The size and complexity of the exercise required a large number of personnel for assisting the exercise facilitation. For a smooth administration, the role were divided as follows: facilitator, adviser, and replier(Figure 5.16).

FACILITATOR

The facilitator guides participants through the exercise. He/she explains the exercise at briefing, and describes the scene at each cycle. During the group work, the facilitator pays attention to each group's progress, while keeping track of time. He/she also supervises the discussion and debriefing. In debriefing, he/she helps participants to summarize results and lessons learned.

ADVISER

During group work, the adviser walks among tables and gives suggestions to each group based on his/her expertise. He/she

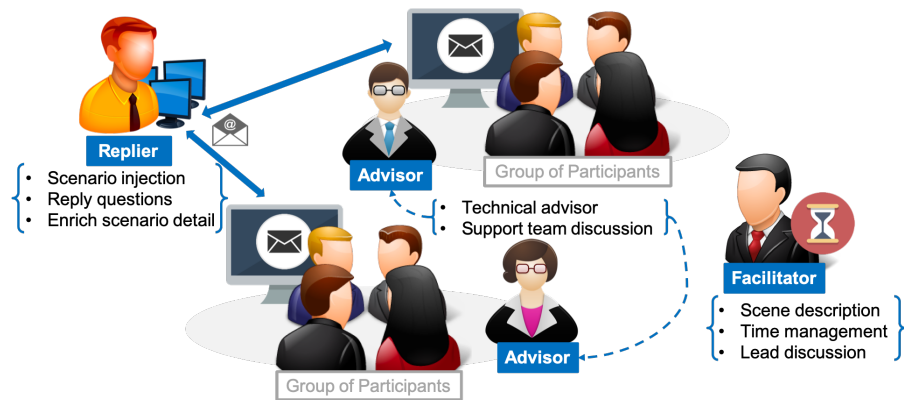


Figure 5.16: Facilitation Structure.

also asks questions that trigger more actions and discussion. Therefore, the role requires knowledge and experience in the field. During discussion, the adviser provides positive feedback and comments for each group. We invited IT security specialists, ICS security researchers, and experts from ICS security agencies as advisers. These experts also helped during the process of scenario development.

REPLIER

The role of the replier is to reply the emails from each group as a (fictitious) “company employee” and to supplement the scenario. Participants cannot touch the system by themselves, given the nature of the table-top exercise. Therefore, some of the participants’ emails are requests for additional information, while others are requests for taking action.

It must be noted that training of the facilitator is necessary to provide consistent quality of support. In doing so, understanding the error model in the facilitation is needed (Appendix A.3).

5.6.3 Detailed Attack Scenario

The object of the exercise to be created this time is a virtual company. Therefore, education for improving the security of the company is the exercise purpose. Specifically, the purpose is to allow the participants to 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 the members belonging to the virtual company. The designer creates exercises configured so that the participants think about 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 serious 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 maximum 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 preventing the damage and the spread of infection by cyber attacks. By determining the maximum goal, it becomes possible to discover the risks of impeding the achievement of the goal. Therefore, the followings are listed as the risks.

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 5.2 shows the revealed events. In Table 5.2, in the safety viewpoint, the first line indicates the results caused by the risk, and the second and subsequent lines indicate the causes thereof.

Table 5.2: The maximum goal and risk of the company for cyber-attack

	GOAL	RISK
Safety	Safe operation of 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

The participant selects, from the revealed events, an event to be generated by the scenario of the cyber attack. The selected abnormality must be a common abnormality related to multiple risks to the safety,

security, and business. The business risks are associated with the safety risks and the security risks if the cause of the business risk as "the event where conveyance to the customers is failed" in Table 5.2 is abnormal at the plant. That is, the risk is a common abnormality in all aspects of the safety, security, and business. Therefore, the risk is selected as the event generated by the attack scenario.

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

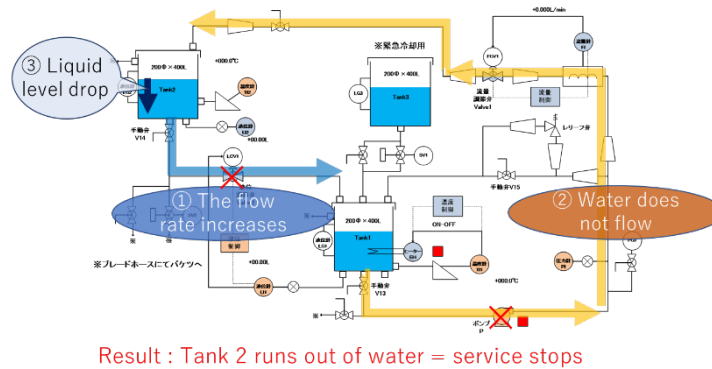


Figure 5.17: Abnormally caused in the testbed plant system.

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 5.17. The flow of water is indicated by an arrow, 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 to be optimal for an attack scenario, as it not only causes an influential

incident but also causes an attacker to create a structure that is easy to attack.

Concealment of cyber attack is also important. 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 where the attacker freely attacks. Specifically, in this scenario, the attacker conceals the monitoring screen (SCADA screen) to delay the detection of the abnormality. Therefore, in the attack scenario, the event "the instruction is not reflected on the SCADA screen" is selected. Based on the above, the events, which will be incorporated in the attack scenario, are colored in Figure 5.18.

Safety			Security	Business
Power outage	Empty accident		Communication line slows down	Loss of customer information
Cannot recover power	Water in tank 1 runs out	Heater can not stop	Heater stop	Loss of attendance information
	Water leakage in the plant	Sensor breakdown	Pump stop	Manufacturing orders do not come
	Leaking water at supply destination	No signal is output	Pump trips	Manufacturer does not come up
Overflow				Supply temperature out of range
	The supplied flow rate can not keep up with the demand	The control valve breaks down	Instructions on the SCADA screen are not reflected	
	Water supply problem	The controller breaks down		Leak in the drainage line
	Reduction in supply pressure		The monitoring screen can not be seen	It will not flow to customers

Figure 5.18: Selected events - In the safety, the first line caused the risk, and as a result, the second and subsequent lines indicate the cause.

In the attack scenario, it is important that the participant recognizes the necessity of the security measures. In a company network system, the firewall installed between the headquarters and business sites can block the 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 serious 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 Table 5.3 are generated. The attack scenario corresponding to the procedure of the Cyber Kill Chain is organized as shown.

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 attackers 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 the

is also good to create an illustration of the network that added what kind of route to attack like Figure 5.20. It helps designers to consider the correspondence and assume the influence range of cyber attack at the same time.

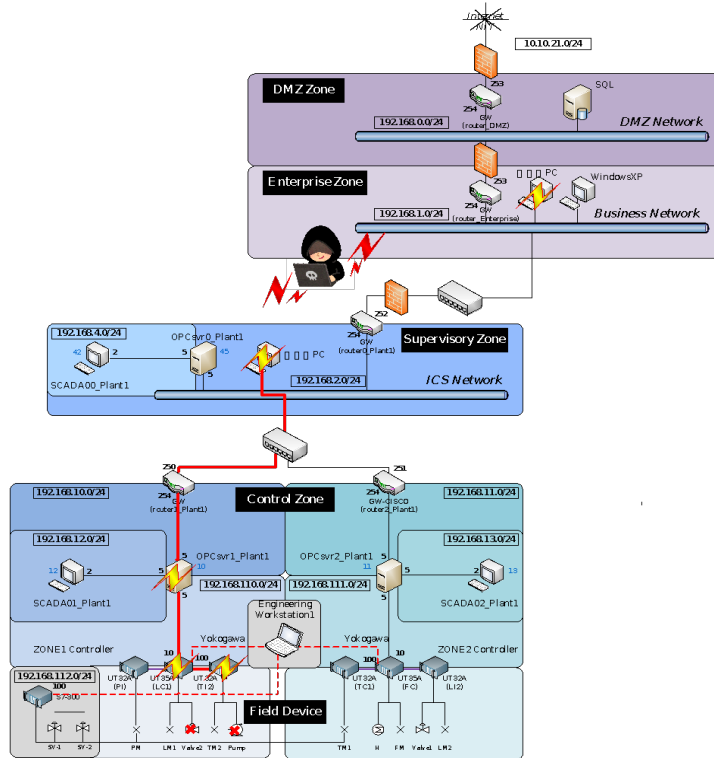


Figure 5.20: Cyber attack scenario shown on the network map.

5.6.4 Exercise Feedback Cycle

The exercise designed by the methodology is immediately provided to the participants. The participants disclose important safety-security-business constraints, but will voluntarily reveal unknown and uncertain conditions, rules, and activities. These published entities have been evaluated, some of which have been implemented. When the next exercise is designed, this design evaluation loop provides a PDCA¹⁰ cycle for less experienced cyber incidents concerning ICS (Figure 5.21)

¹⁰ Plan Do Check Act

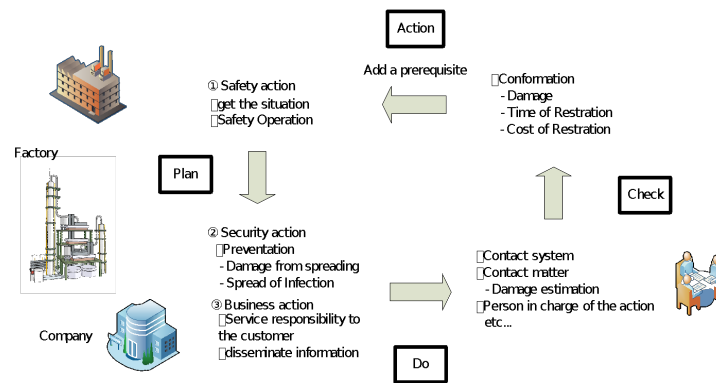


Figure 5.21: PDCA feedback cycle of the exercise.

5.7 PRACTICAL APPRAISAL OF DEVELOPED EXERCISES

5.7.1 Pilot Exercises with Experts

Pilot exercises were conducted at the campus of Nagoya Institute of Technology as a part of two days ICS security workshop in August 2015 and March 2016. The number of participants was 45 and 46 respectively, and their expertise was heterogeneous. The distribution of participants' profiles at each workshop is shown in Figure 5.22, where participants are classified by their organization types and occupational category.

The sectors of CI owners included chemical, energy, gas, and telecommunication. In both exercises, participants were divided into six groups—totalling twelve groups—in order to facilitate the discussion. Since the exercise aims at stimulating the discussion and expand the participants' perspective, groups were carefully composed in order to maximise intra-group heterogeneity of expertise, background and position.

5.7.2 Survey Result of Pilot Exercises

A survey was conducted after each pilot exercise. The results show that 94.7% (in August) and 90.9% (in March) of the participants were satisfied with the exercise, and that 83.0% (in August) and 90.6% (in March) would recommend the exercise to other CI stakeholders. In

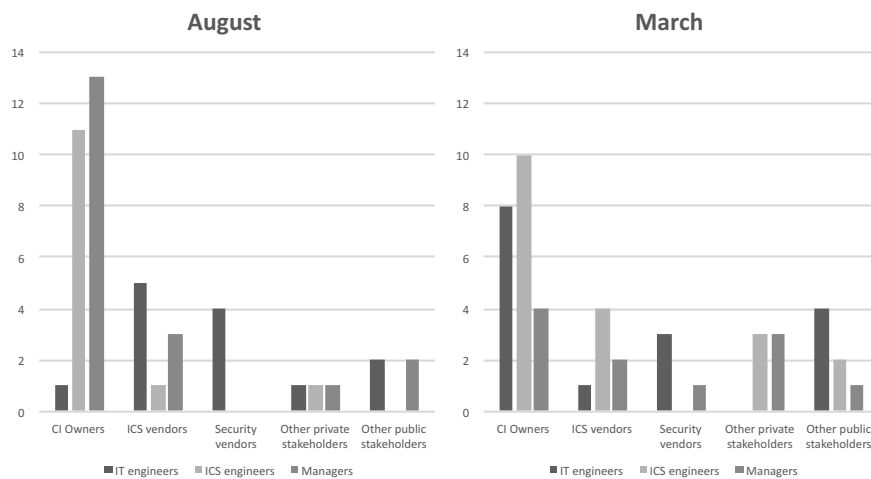


Figure 5.22: Participant's profile distribution.

fact, some of the August workshop participants participated in the March workshop as well, and some extended the invitation to their colleagues.

5.7.3 Variation of Incident Management Structure

The groups' worksheets were analyzed at discussion and debriefing time, by comparing the structure of their actions and commands. Example outcome of exercises (8 groups, 3 phases) are provided in appendix C.1. As a result, the following three types of incident management structures were found (Figure 5.23): IT department centered, production department centered, and management centered.

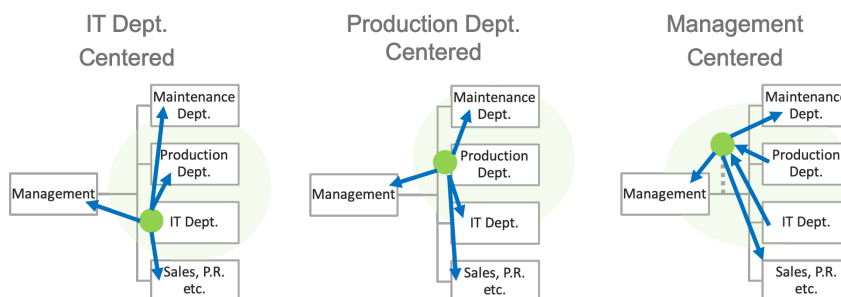


Figure 5.23: Observed communication structure design in the exercise.

IT DEPARTMENT CENTERED

The IT department plays the leading role during the incident management. Specifically, it investigates the incident, and gives directions to the production department. Additionally, it provides updates about the situation to the management and to other departments who may be affected by the incident (e.g. sales, PR). In a real life situation, this structure may be applicable to an organization with a strong IT capability. Moreover, for the IT department to successfully lead the cyber incident response, it should have knowledge of the plant systems and a full understanding of the incident's impact on the business.

PRODUCTION DEPARTMENT CENTERED

The production department leads the response, cooperates with the IT and other departments in charge of maintaining the production (e.g. the maintenance department), and gathers information related to the investigation and to the situation of the damage. This structure may be suitable for a large plant system where the production department has a strong leadership and authority. However, if the production department is unprepared to handle a cyber incident, the investigation may take longer than necessary, and potentially cause a bigger impact. Therefore, a thorough cyber security training of the production department personnel is necessary for this structure.

MANAGEMENT CENTERED

The management department leads the operation, by keeping an exclusive communication with the IT and the production departments, which don't directly exchange information with each other. One group even suggested to set up a crisis management headquarter, where all department and management heads would cooperate. This structure is similar to the incident command system adopted for natural disasters [65], where plans and objectives are decided at the top of the hierarchy, while activities at the lower levels are a consequence of those decisions. In reality, this structure may be applicable to an organization with a highly centralized management system, or to a situation

that requires the involvement of top management (e.g. large scale disaster, the critical service is not substitutable).

5.7.4 *Discussions*

The proposed table-top exercise aimed at training communication management skills of CI stakeholders and strengthen the cooperation capability of the CIP community, by engaging participants in discussion. We could observe that participants were stimulated by the exercise to express their point of view, acknowledge variety, and achieve a mutual understanding of an issue, regardless of their background. It can be said that the exercise encourages CI stakeholders to cultivate a shared mental model, which may positively influence performance [66]. Moreover, the exercise was general enough to stimulate the participants who did not belong strictly to the ICS security community (i.e telecommunication sector), who in turn were satisfied by the acquisition of new knowledge. In conclusion, the unique experience of the exercise was appreciated by the CIP community.

5.8 CONCLUSION

In this chapter, we proposed ICS security training program developed by following the proposed maturity based training framework. In doing so, we described scenario development procedure using our testbed as the example. Subsequently, we introduced various exercises based on the testbed scenario, accompanied by pilot testing results.

Numerous testing of the presented exercises to the participants with various skill level, it came to our attention that the more skilled they are, participants feel more comfort with conceptual exercise scenario. Although we used same attack scenario for several exercises, the granularity was not always the same. For the attack demonstration, we used step-by-step guide to the attack process, its effect, potential impact and real-life cases. Participants seemed to have difficulty in finding a commonality between their own system and the testbed. Meanwhile, in the pilot TTX conducted with highly - matured organi-

zations, participants were comfortable reflecting their experiences to the fictitious organization in the exercise.

We developed this training program to provide exercise as a service. Drills and exercises developed within the organization requires a time and resource in the design and development phase, often overlooking the importance of exercise hot-wash and feedback. By providing the accessible exercise programs ready to be tailored to each organizations, asset owners can focus more on the learning and reviewing of the performance during the exercise. We hope our effort to encourage more organizations to incorporate the exercise based cyber response capability management cycle.

CONCLUSION

6.1 CONCLUSION OF THIS THESIS

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 chapter 1, we introduced how ICS can be vulnerable to cyber threats, and what consequences can occur due to the cyber attack targeting ICS. High level of cyber security can be achieved by combining technical security controls, engineering works, and organizational efforts on policy and education. Cyber security training is known to be an essential controls, however, we pointed out that training programs are not managed in accordance to the level of capability.

CHAPTER 2

Chapter 2 studied deep into the cyber security training literature to seek for the definition and terminologies for training, exercise, and drilling. We conducted a filed study of the available exercise programs over years., and from the comparison we discovered that Japanese training market is leaning towards drills and guided training methodologies rather than exercising the flexibility and resilience.

There are many ICS security training programs that consist of class-room lectures and drills, which do not include active discussion among participants. Also, participation to these training programs is restricted to certain expertise profiles or CI sectors (e.g. banking, chemical). However, large scale cyber incident can cause an impact beyond boundaries of CI sectors in a highly

inter-connected society. In case of such an event, the cooperation of CI sectors and other stakeholders (e.g. government agencies) is essential [48]. Nevertheless, the current training system is isolated by sectors, and does not include stakeholders outside the organization. The results of such limited diversification of expertise are that the participants' perspective on cyber security issues is narrowed down, and that knowledge transfer across sectors is not facilitated.

CHAPTER 3

In order to study the need of resilience in cyber incident operation, chapter 3 was dedicated to organizational behavior study in the adversarial exercise filed. The observation results highlighted how cyber resilience is resonated with the preparedness to the change and decision making dilemmas.

We discovered that elevation of decision-making privilege has been observed together with the shift of the control mode. The core decision maker shifts from the top management to each division, then to individuals. From the perspective of management engineering, scramble mode should be avoided and being strategic mode is the most efficient and ideal.

Manager in charge of incident handling should be able to capture the change of their control status, and adopt the best management system to each control mode. For this reason, factors in organizations behavior that trigger the shift of control mode needs to be clarified. With more extended study, the challenges and control modes we explored in this paper can be the indicator to evaluate management performance in the training, and that will broaden the scope of the exercise to train cyber incident management methodology.

CHAPTER 4

The training needs to be planned in phases in order to achieve higher resilience. Chapter 4 introduced the framework of exercise planning in accordance to the preparedness or the organization. The phases were designed in align to NIST Cybersecurity Framework Tiers.

We proposed a guideline to select the best exercise style, aim and participants according to the current level of preparedness of an organization, and according to the possible need to improve such capabilities. For this purpose, we reviewed the styles of exercises that are used both in the cyber (NIST) and physical (HSEEP) security domains. Based on this review we hypothesised that games and seminars are suitable for low degrees of preparedness; workshops are useful at an intermediate degree; while functional, table-top, drill and full-scale exercises range from intermediate to high degrees.

Furthermore, matching to the characteristics of the NIST implementation tiers, we recommend to include participants according to a proportional rule between the *tiers* (from 1 to 4) and the hierarchical level of an organization (from individual to stakeholders). Similarly, the aim of the exercise (from awareness to resilience) should be proportional to the tiers (from 1 to 4). The adoption of these guidelines would guarantee that lessons learned from exercises are well absorbed by the personnel, resources are not wasted, and improvement of capabilities is smooth between tiers.

The concepts expressed in this chapter are inspired by observation at private BCM exercises and at available domestic cyber security training programs. The proposed guideline should be validated empirically and experimentally. Therefore, future studies should evaluate the application of the proposed guideline to the available exercises, and examine how it impacts the organizations in reality.

CHAPTER 5

Chapter 5 showed the illustrative example of the exercise design and implementation using the proposed framework in chapter 4. With one set of the testbed, we illustrated that exercises can be tailored to specific preparedness. The details of conducted training program elements were provided.

The proposed exercise aimed at training communication management skills of CI stakeholders and strengthen the cooperation capability of the CIP community, by engaging participants in

discussion. We could observe that participants were stimulated by the exercise to express their point of view, acknowledge variety, and achieve a mutual understanding of an issue, regardless of their background. It can be said that the exercise encourages CI stakeholders to cultivate a shared mental model, which may positively influence performance [66].

Moreover, the exercise was general enough to stimulate the participants who did not belong strictly to the ICS security community (i.e telecommunication sector), who in turn were satisfied by the acquisition of new knowledge. In conclusion, the unique experience of the exercise was appreciated by the CIP community.

6.2 IMPLICATIONS

We conclude that exercises can play the role of a driving power to improve an organization and community's cyber security preparedness. In this chapter, we conclude the study by the discussing the implications for the organization behavior, the exercise management implications, and the research implications.

ORGANIZATIONAL BEHAVIORAL STUDY IMPLICATIONS

The field study in chapter 3 was following the research conducted by Branlat[23][22]. In stead of examine the verbal cues of the participants, we studied the relation of the participants behavior to the incident timeline and its change as one dynamic organization. The study also expanded Holnagel's COCOM[58] to the organizational decision making. The study tested the new application domain of resilience engineering research.

EXERCISE MANAGEMENT IMPLICATIONS

In this study we emphasized the importance of using an exercise as the milestone to review the security management practices, and achieve better resilience. For this reason, we adopted commonly used NIST Cybersecurity framework tier as the guiding

axis to measure the maturity. We hope this study provides a new perspective to operate exercise programs.

RESEARCH IMPLICATIONS

In recent years, variety of exercise case studies can be found in resources, such as academic and classroom cyber security trainings[67][68], national exercises[69][70], functional exercises[71][72], and table-top exercises[73][74]. However, few literature suggests the exercise management plan in the recurrent scheme aiming to achieve higher preparedness. The proposed guideline should be validated empirically and experimentally. Therefore, future studies should evaluate the application of the proposed guideline to the available exercises, and examine how it impacts the organizations in reality.

This interdisciplinary study was based on an investigation of both organizational behavior and exercise management. Discussion-based exercise tailored to the organizations' maturity cultivates a shared mental model among participants. We developed a training program to provide exercise as a service. Drills and exercises developed within the organization requires a time and resource in the design and development phase, often overlooking the importance of exercise hot-wash and feedback. By providing the accessible exercise programs ready to be tailored to each organizations, asset owners can focus more on the learning and reviewing of the performance during the exercise. We conclude this study in the hope of more organizations to incorporate the exercise based cyber response capability management cycle to mature an organization and community's cyber security capability.

A

APPENDIX: RELATED PUBLICATIONS TO UNDERSTAND THIS THESIS

A.1 A UNIFIED FRAMEWORK FOR SAFETY AND SECURITY ASSESS-
MENT IN CRITICAL INFRASTRUCTURES

A unified framework for safety and security assessment in critical infrastructures

T. Aoyama, M. Koike, I. Koshijima & Y. Hashimoto
Nagoya Institute of Technology, Japan

Abstract

The appearance of Stuxnet malware changed the idea of security on critical infrastructures greatly. However, in previous studies, cyber security issues have been addressed only from an IT security perspective, with a focus on the detection of malicious activities and the elimination of IT threats. However, these studies missed out the discussion relating to the robustness of the designed plant system. In this research, the relation between information system security and physical plant safety is defined on the basis of a novel framework. This study introduces a preliminary approach which tackles plant safety and security from a more comprehensive point of view. In this context, not only computer security is considered, but also plant availability and robustness. In particular, the presented methodology allows us to understand how unsafe activities and cyber-attacks may propagate throughout the plant system and affect the physical side of the plant.

Keywords: control systems security, plant safety, cyber-terror.

1 Introduction

1.1 Definition of security and safety

The term ‘security and safety’ are common words which are frequently used in the same context. Their difference, however, is often unclearly stated. Burns *et al.* [1] proposed the following informal definition of the terms safety and security: “A system is not safe if it can harm us; it is not secure if it gives others the means of harming us”. Moreover, inside IEC 61508 safety is defined as “Freedom from unacceptable risk ... as a result of damage to property or to the environment [2–4]. In this research, we follow the interpretation given by Furuta *et al.* [5], in



which safety and security are simultaneously defined on the basis of the intentionality of acts. More precisely, an unsafe status in the plant system could be triggered by two types of acts: unintentional or intentional. The former acts are mainly caused by human errors, such as slips and lapses of the plant operators and are addressed as a safety issue. On the contrary, intentional acts deliberately create violation or sabotage of targeted systems and are considered as a security issue that directly or indirectly links to a certain safety issue.

1.2 Cyber security and safety for critical infrastructures

A violation or sabotage to critical infrastructures can be driven by a physical attack (e.g. disconnection of a cable) or by an indirect attack from the cyberspace and in this paper we focus on the latter. According to the terminology in IEC62443-1-1 [6], cyber security is defined as “actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets”. It is important to underline that Information System security and Critical Infrastructures security have different profiles. In Information Systems, the most valuable property is Information, therefore Confidentiality has the highest priority, followed by Integrity and Availability (CIA). On the other hand, failures in Critical Infrastructure threaten public safety and environmental health. Moreover, the failure of services and products can directly cause a loss of profits. Therefore, in the context of Critical Infrastructure, the order of priority changes to AIC, which means that Availability must come first.

2 Problem statement

The reason why IT security approaches are not enough to guarantee Availability, our highest priority, is represented by the fact that a system without vulnerabilities is hard to achieve and new exploit techniques are always available to hackers. Therefore, in order to protect the Availability, we first need to study in detail about Availability robustness. The robustness can be evaluated by assessing the safety and security in the physical side. Accordingly, the connectivity between information systems security and physical infrastructures safety must be clarified in an effective way. To this end, this study proposes a methodology that allows understanding how unsafe activities and cyber-attacks may propagate throughout a critical infrastructure from the IT side to the physical side of the system. In this paper, we focused on modelling of a plant system, which is one of the basic architecture of critical infrastructure.

3 The unified framework

3.1 Plant system decomposition

Devices in a plant system can be decomposed into four categories according to their functionality: plant equipment, field device, control device and office IT



device. Plant equipment is directly involved in the production activity and its usage is mostly limited to its particular function (e.g. tanks, pipes). Field devices are involved in the physical actuation and sensing of the plant equipment (e.g. pump, valve). Control devices are responsible for the control and supervision of the field devices during the production activity (e.g. PLC). The data related to the operation of the plant are gathered and stored in IT servers, which are accessible through the Office IT system, which also supports the intra-office communication. In order to model the interaction between the different components of a plant system, we designed a new framework, inspired by the Open Systems Interconnection (OSI) Reference Model.

3.2 OSI reference model and the unified framework

The original OSI model defines IT network communication protocols by dividing them into seven layers: physical, data-link, network, transport, session, presentation and application layer. These layers were reinterpreted comprehensively, based on the original definition provided by Zimmermann in 1980 [7], in order to include the field equipment, field devices and control devices. This unified framework is necessary to describe the data flow in the plant system. It is important to underline that the concepts of the original OSI model are still used to represent the IT communication protocols of the office IT system.

Detailed explanations of each layer in the unified framework are provided below:

Application layer The application layer provides service applications for the operation of the plant. Some of the entities of this layer allow human operators to manage and supervise the production process (e.g. Operator interface), while other entities communicate with each other in order to control and maintain autonomously the operation of the plant (e.g. loop control program).

Presentation layer The services provided by this layer are supporting the upper layer activities. In particular, it translates information coming from lower layers so that they become meaningful to the application services. For example, supposing that a lower layer entity provides information about temperature in Fahrenheit degrees and an application layer entity requires the same information in form of Celsius degree, the presentation layer handles the translation.

Session layer The session layer models the interaction between presentation entities which are highly interdependent. For example, in the case that those presentation entities such as “Temperature” and “Pressure” are related to a fluid, they must satisfy the law of nature described by the session entity “perfect gas equation of state”.

Transport layer The transport layer entities represent the properties of the information media used in the network layer and they are used to describe and support the equilibrium laws described in the upper layer. In this way, the same transport entity can be used to represent two different materials



of the network layer. For example, the Transport entity “delta-temperature” can be used to characterize both water and gas flow. The prefix delta is used to highlight that these entities are used in the upper layer to define equations representing the natural laws.

Network layer The entities in this layer are the media that support the information flow (e.g. gas stream, water flow).

Data-link layer If a physical connection between devices exists, this doesn't necessarily mean that there is an information flow. In order to model the active flow of a media between devices, we use the Data-link layer. For example, the flow of water from Device 1 to Device 2 and from Device 2 to Device 1 is represented by two different variables. Moreover, if Device 1 and Device 2 are physically connected but there is no flow, then this connection is considered void in the Data-link layer.

Physical layer The physical layer represents the physical connection between devices. Both active and non-active connections must be included in the model. For example if a pipe and a tank are physically connected, but no flow of material exists, their connection is still modelled in the physical layer.

Figure 1 shows the communication flow between Plant equipment and Field devices. This unified framework explains the communication between devices in detail, which is useful for detecting the cause of a failure in a system.

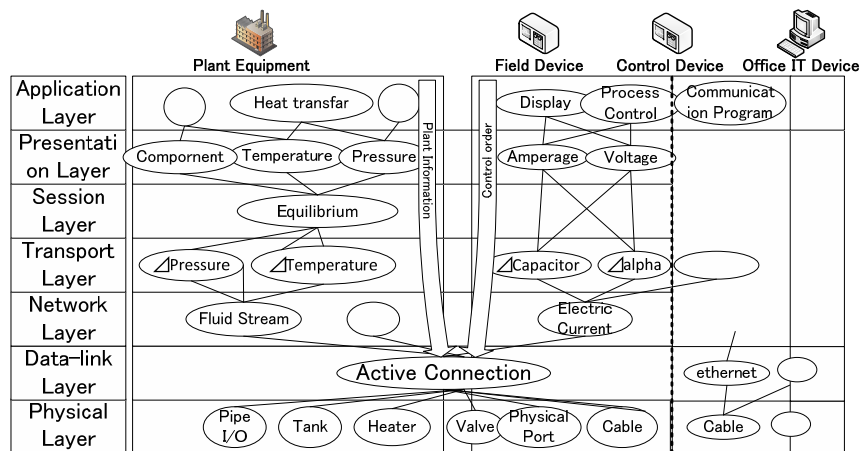


Figure 1: The entire structure in the framework.

4 System implementation based on the framework

One of the goals of this study is to design a unified framework for the modeling of the plant network so that safety and security could be assessed in a unique domain. Still, connectivity scheme obtained from the proposed unified model requires a suitable visualization.

4.1 Model implementation into DSM

The DSM (Design Structure Matrix) [8] can be used as a networking model to embody the idea of the unified framework. By applying the DSM paradigm, it is possible to visualize all the available paths in the overall system. In particular, the focus is on possible horizontal inter-device connections at each layer of the unified framework. On the other hand there is no need to analyze the vertical communication between layers because it is mainly caused in an intra-device activity. As a result, connectivity matrices for each layer are designed in seven matrices. Also, as one of the extended usage of DSM, the reachability from one node to the other can be calculated. According to the unified framework, physical connectivity is considered as the universal protocol in the physical layer. Therefore, the physical static structure of the entire plant system is represented by the static DSM of the first layer. On the other hand, unlike the first layer, for each of the layers from the second to the seventh (upper layers), the DSM represents the information flow. For this reason, it is possible to describe the vectors of the protocol flow by the input-output relationship of the dynamic DSM. By using this approach, each upper layer contains fragments of the entire information flow. These upper layers matrices are used for finding information linkages.

4.2 Safety and security assessment methodology

At this point, the plant risk analysis based on the DSM obtained from the unified framework is presented. The achieved model was used to perform two types of risk analysis: FTA (Fault Tree Analysis) and HAZOP (hazard and operability study). The FTA is used for assessing system vulnerabilities based on a priori knowledge, while the HAZOP is used for potential danger which is not known in advance, nor predictable. By combining both methodologies, event probability of both external fault and internal fault could be achieved.

4.2.1 Adapting HAZOP to the unified framework

In corresponding context of the presented unified framework, a HAZOP parameter is equivalent to unique media (e.g. water flow) supporting each entity in the layers of the framework. Therefore, since the DSM represents the input-output relationship between two devices at a given layer, HAZOP analysis can be applied to each cell of each DSM matrix of the model. The process of eliciting HAZOP deviations from the DSM is shown in Figure 2 and explained below.

1. **To generate the fundamental DSM:** As previously mentioned, the DSM which is plotted by the first layers linkage shows the physical structure of the entire network. From this DSM the fundamental information for generating HAZOP deviations is obtained.
2. **To select the parameters:** Devices of a system have HAZOP parameters representing their features. These parameters can be found according to the profile of the devices in the perspective of the framework, so that the found parameters are added to columns. For example, the heater has the



parameters “temperature” in Presentation Layer and “electric flow” in Network Layer. The combination of devices and parameters are plotted so as to form multi domain matrix (MDM) beneath the DSM.

3. **To connect the parameters and guide words:** Guide words are defined as “word or phrase which expresses and defines a specific type of deviation from an element’s design intent” [9]. Their role is to stimulate imaginative thinking, to focus the study and to elicit ideas and discussion, thereby maximizing the chances of study completeness. Here, all possible combinations of the guide words and parameters is plotted so as to form a matrix next to the generated MDM. Since the relation between HAZOP parameters and the guide words does not change, this matrix is a universal matrix, and is independent from the DSM generated from the objective network.
4. **To elicit the deviation:** By combining the parameters and the guide words, causes of deviation from the design intent can be found [10] (e.g. Higher-Temperature, Lower-Temperature). At this point also, the device element should also be combined (e.g. Heater – High – Temperature, Tank – Higher – Temperature). In this way, all the possible deviations in a given network are elicited.

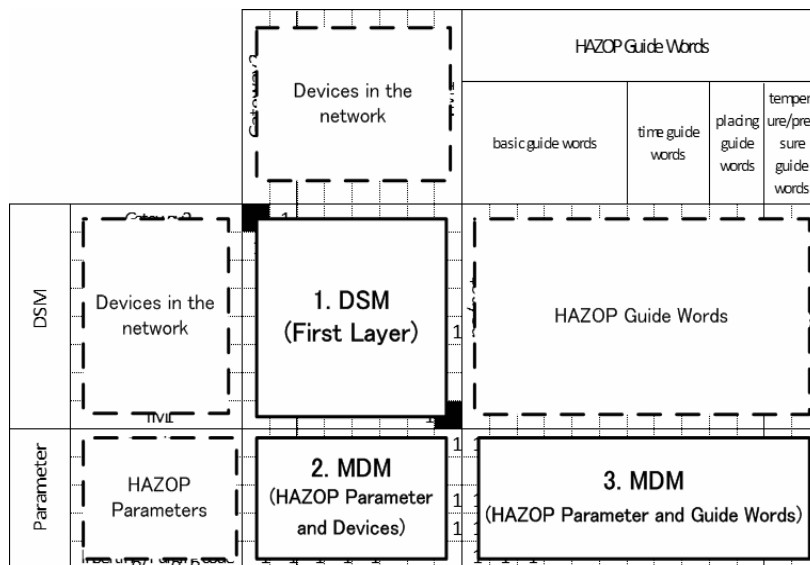


Figure 2: The process for eliciting HAZOP deviations from the DSM.

For instance, from the point of view of security, packets, which are media of IT protocols, can be treated as HAZOP parameters. In this case, by applying the guide words (e.g. “More – Quantitative increase” [11]), security issues might be highlighted (e.g. buffer overflow). It should be noted that according to the basic idea of layering, each layer adds value to services provided by the set of lower

layers in such a way that from the highest layer set of services is offered as to run distributed applications. Thus, the layering divides the total problem into small pieces [7]. Therefore, the HAZOP analysis should be applied in detail to each layer, in order to specifically locate a cause of an anomaly.

4.2.2 To apply FTA to the unified framework

The FTA analysis is adopted to perform a risk analysis on the basis of a provided framework. In particular, the determination of a device contributing to an event is derived easily by tracing back reachable paths from the DSM of the unified framework. This is because, in this context, the contribution to an event is considered as a reachability matter. The reachable paths enable systematic and logical determination of all contributors to a particular event.

As the contributors to the critical event are found from the reachable paths, the lower-level event related to the contributors should be analyzed to identify realistic causes. At this point the HAZOP analysis can be performed easily. The parameter of a selected contributor is derived from the framework, and then, by combining HAZOP guide words with the parameter, potential deviations are specified. Their causes are categorized in human errors, equipment failure, and external events, from the perspective of cyber security.

5 Illustrative example

In this section, a part of our cyber security testbed is analysed as an example (pictures of the testbed in Figure 3). In 2012, a testbed for ICS security was developed in the Nagoya Institute of Technology (NIT). The design of the specifications of the testbed is based on the requirements of those who are concerned with control systems security (e.g. vendors, researchers, users etc.).

From the requirement analysis, the purpose of the testbed was decided as follows:

- a. **Training for gaining public awareness:** the testbed will be used as an educational training tool, in order to show the importance of cyber security and the threat of cyber attacks.
- b. **Intrusion detection:** the testbed is used to test the intrusion detection tool under development.
- c. **Improvement of plant resiliency:** data obtained from the testbed by simulating plant operation will be analysed, for the research on the effectiveness of security and safety measures.

From this testbed, the example work only focuses on a simple control process which is illustrated in Figure 4. In detail, the temperature information of Tank 1 is sensed by TM1, and the data is gathered to a controller (“UT35A (TC1)”). At this point, the controller uses the temperature information in order to send a command to a heater. The controller communicates with an OPC data server and the information of the operation is stored in the server. Meanwhile, a human operator will observe and handle the operation using SCADA. The gateway is not directly connected to the Internet; however it is connected to the office area, which is in turn connected.



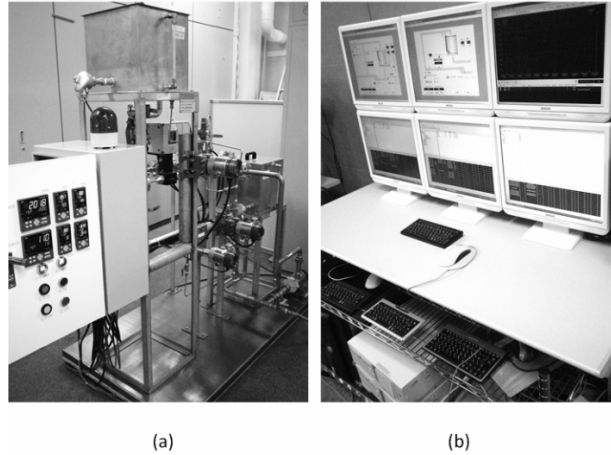


Figure 3: The plant side (a) and the operator side (b) of the testbed.

Devices and applications used in this control process are listed below;

- M-SYSTEM SCADALINXpro OPC DA2.0 on WindowsXP Professional SP2 as OPC data server (OPC1)
- M-SYSTEM SCADALINXpro on WindowsXP Professional SP2 as SCADA system (SCADA1)
- Yokogawa UT35A/UT32A Digital Indicating Controllers as controller (UT35A (TC1)).

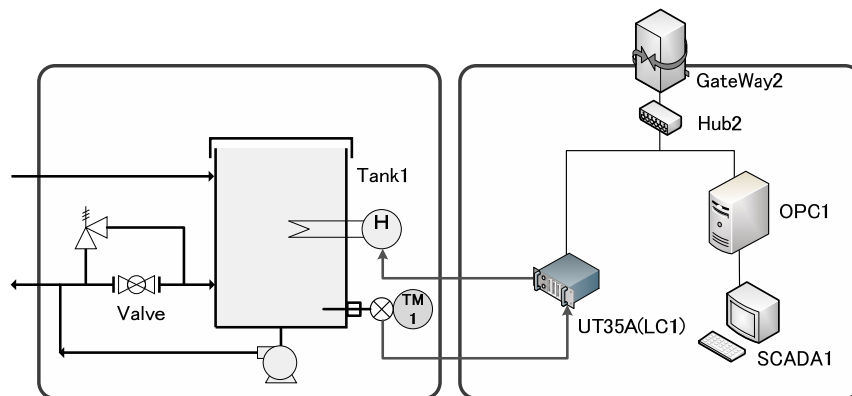


Figure 4: Part of the control process through the testbed.

A given network is translated into a DSM of the first layer (Figure 5). The matrix is sequenced to form two sequences; an information system area and a plant system area. It is noted that the controller (“UT35A (TC1)”) is functioning as a connector between the two areas.

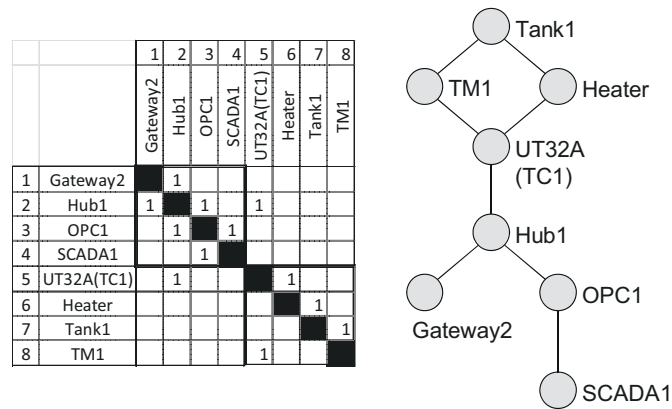


Figure 5: DSM of the first layer, and its translation into the digraph to identify the flow of contributors.

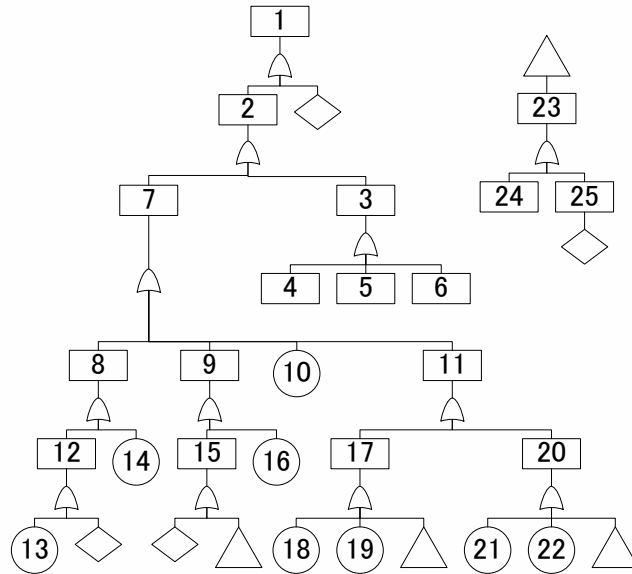
As previously mentioned, the reachability path is found in the DSM by applying the FTA. In this way, elements to be analysed due to a potential effect can be detected easily. For instance, the DSM can be visualized as a simple digraph as shown in Figure 5, which explains reachability to the Tank 1. In this way, the contributors to the event are defined.

	DSM	Gateway2	Hub2	OPC1	SCADA	UT32A(TC1)	H	Tank1	TM1	HAZOP Guide Words													
										basic guide words				time guide words		placing guide words	temperature pressure guide						
										no/not	more	less	part of	reverse	other than	sooner	later	other than	where else	other than	higher	lower	
	Gateway2	1																					
	Hub2	1	1																				
	OPC1		1	1																			
	SCADA			1	1																		
	UT32A(TC1)		1			1				1													
	H						1																
	Tank1							1															
	TM1								1														
Parameter	Sampling					1		1	1	1							1		1				
	temperature						1	1								1	1				1	1	
	electric flow	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	protocol flow	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Inserting code	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 6: Determine HAZOP deviations by applying HAZOP Guide Words on DSM.

As the next step, a cause of a top event (failure) should be defined. To this end, the MDM introduced in the previous chapter is generated (Figure 6).

Possible HAZOP deviations of the contributor are added beneath the contributing events, as lower level contributing events. As a result a fault tree is generated in the way explaining the intrusion path of a cyber attack to the system (Figure 7).



No.	Fault Event Name	9	18
1	Overheating in Tank1	Failure in Program	Operator Human Error
2	Failure/ Deviation in Heater	UT32A Mechanical Failure	Protocol Failure
3	Heater Mechanical Failure	Deviation in Program parameter	Failure/ Deviation in SCADA
4	Higher Temperature	Failure/ Deviation in Sampling	Protocol Failure
5	Longer Heating	Sensor Mechanical Failure	Operator Human Error
6	Stronger Heating	TM1 Mechanical Failure	Malicious code executed
7	Failure/ Deviation in UT32A	Program Overwritten	Physically Incerted
8	Failure/ Deviation in TM1	Missprogramming	Infected via network
		Failure/ Deviation in OPC1	

Figure 7: HAZOP based FTA generated from the control process path.

6 Concluding remarks

The authors just take the very first step of a research towards the combination of safety and cyber security in plant systems. Through this research, we proposed a framework for applying a uniform analysis method for safety and security simultaneously. The research was, although, limited to theoretical study due to insufficient amount of real-world data to practically assess SIL (Safety Integrity Level) and SAL (Security Assurance Level) using the FTA. This is caused by the difficulty in collecting data of incidents in cyber crimes, since disclosure of a

certain data tends to be avoided. Therefore, future works will be devoted at filling the gap between our present theoretical study and its possible applications in real infrastructures. The presented framework is an attempt to provide a comprehensive and general methodology for retrieving risk information related to a critical infrastructure. This could be beneficial for organizations and companies in their decision making process, which must include risk control.

Acknowledgement

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (B), No. 24310119 (2012) and (B), No. 25282101 (2013).

References

- [1] A. Burns, J. McDermid, and J. Dobson. On the meaning of safety and security. *The Computer Journal*, 35(1):3–15, 1992.
- [2] IEC 61511-1-1: 2003: Functional safety – safety instrumented systems for the process industry sector – part 1-1: Framework, definitions, system, hardware and software requirements, Jan 2003.
- [3] IEC 61508 – functional safety of electrical / electronic / programmable electronic safety-related systems (7 parts). Available as BS IEC 61508 from BSI, Milton Keynes, UK, or from the IEC, Geneva (www.iec.ch).
- [4] DHS. National cyber incident response plan. Draft, September 2010.
- [5] K. Furuta, S. Nagasaki, Introduction to Safety, Nikkagiren, 2007 (in Japanese).
- [6] IEC/TS 62443-1-1: 2009: Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models, July 2009.
- [7] H. Zimmermann. OSI reference model – the ISO model of architecture for open systems interconnection. *Communications, IEEE Transactions on*, 28(4):425–432, 1980.
- [8] S.D. Eppinger and T.R. Browning. *Design Structure Matrix Methods and Applications*. Engineering Systems. MIT Press, 2012.
- [9] International Electrotechnical Commission *et al.* IEC 61882. Hazard and Operability Studies, (HAZOP Studies) Application Guide, 2001.
- [10] International Electrotechnical Commission *et al.* IEC 60050-191 International Electrotechnical vocabulary. International Electrotechnical Commission, Geneva, 1990.
- [11] G. Baradits and J. Abonyi. A new software-based HAZOP study development methodology. In 8th International Symposium of Hungarian Researchers, November, pages 15–17, 2007.



A.2 ON THE IMPORTANCE OF AGILITY, TRANSPARENCY, AND
POSITIVE REINFORCEMENT IN CYBER INCIDENT CRISIS COM-
MUNICATION

On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication

Tomomi Aoyama, Atsushi Sato, Giuseppe Lisi, and Kenji Watanabe

Nagoya Institute of Technology, Gokiso-cho 4668555, Aichi, Japan
aoyama.tomomi@nitech.ac.jp

Abstract. Cyber incident crisis management protocols often overlook the importance of crisis communication. This paper reviews the crisis communication literature to define explicit communication strategies for each stage of a cyber incident. We applied the proposed model to analyze the Norsk Hydro case: a Norwegian aluminum and renewable energy company halted operations due to a ransomware attack. By combining traditional communication outlets and social media, the company kept high transparency of their recovery operation, with frequent (i.e., agile) updates about the cyber incident. The positive presence of Norsk Hydro on social media allowed them to manage reputation throughout the process. Employees' creativity and loyalty were crucial in the recovery process, and it was promptly publicized globally. This empowered other employees at other branches to act creatively and inspired the community. We conclude the study by suggesting the agility, transparency, and positive reinforcement were the success factor of this crisis communication operation.

Keywords: Cyber incident response · Crisis communication · Information sharing · Communication agility · Transparency · Positive Reinforcement.

1 Introduction

Cyber-attacks continue to pose risks to critical infrastructure. Due to the increasing connectivity, digital and non-digital assets are both vulnerable to threats via Information Communication Technologies [16]. Unlike natural hazards, a cyber incident is caused by the malicious intent of an attacker. Attackers can take advantage of the responding organization's visibility and counteract to the defense.

An example is the Protonmail DDoS (Distributed denial-of-service) attack in 2018 [11]. The initial DDoS attack for the End-to-end encrypted email service provider ProtonMail caused service outage of several minutes. The small hacker group Apophis Squad targeted ProtonMail at random while testing a beta version of a DDoS booter service. Although it was not their intention to persistently attack ProtonMail, but decided to conduct a more massive attack after ProtonMail's CTO, Bart Butler, responded to one of their tweets addressing the group

provocatively[3]. Especially during the cyber incident, the communicator should be aware of the risk of provocation, which leads them to be cautious and be hesitant to communicate to the public.

This study aims at understanding the advantage of active crisis communication operation to the public during a cyber incident. Although the theoretical work on modern crisis communication is extensive, it lacks in reflecting the challenges and benefit from the empirical case studies, particularly in the field of cyber crisis management. We addressed this problem by developing the cyber crisis communication strategy model from the literature review highlighting the shortcomings. Then, we conducted an empirical study of a Norwegian aluminum company's case to analyze the benefit of employing a coordinated communication operation.

2 Cyber Incident Crisis Communication Strategy Model

Crisis communication during the cyber incident should be concurrent with incident response activities. Fig. 1 shows the crisis communication strategy model based on the literature review. In the field of crisis management study, Coombs grouped the crisis communication stages to pre-crisis, crisis-event, and post-crisis [4] as the macro-level framework. Kulikova et al. studied the challenges organization face in cyber incident information disclosure [10]. Steelman [12], Coombs [4], Weiner [17] worked on the best practices of crisis communication.

The research work of Veil [15] is dedicated to determining the advantage and disadvantage of social media use during the crisis. Their findings are incorporated into the Fig. 1, as the cyber incident crisis management activities.

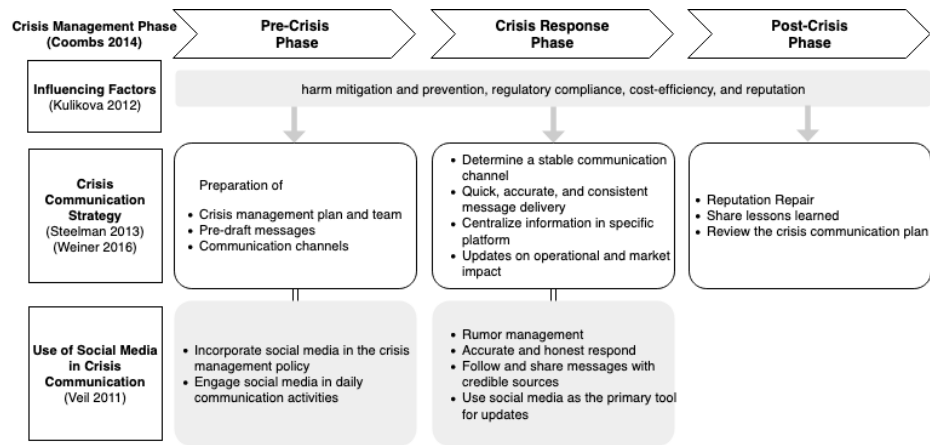


Fig. 1. Cyber incident crisis communication strategy and best practices of social media use in three phases.

From the literature review, we found that previous literature is missing case studies specifically to understand the benefit of utilizing social media in the cyber incident crisis communication. Here, we review a recent cyber incident case and the victim organization's use of social media from the crisis communication perspective.

3 Case Study: Norsk Hydro

The company underwent the production stoppage due to a ransomware attack on the 19th of March 2019. In the following paragraphs, we reconstruct the incident timeline as described on media outlets and the official update by Norsk Hydro (top panel of Fig. 2). As of April 30th 2019, the overall impact on the first quarter of 2019 is NOK 400-450 million (Euro: 45 million; US Dollars: 51 million)[2].

In this section, we describe the crisis communication timeline reconstructed from the social media channels of Norsk Hydro (bottom panel of Fig. 2). On March 19th, the official website of the Norsk Hydro becomes inaccessible. Immediately, the company reports the incident through Twitter and Facebook and establishes the latter as the main channel of communication (i.e., 'Updates regarding the situation will be posted on Facebook'). In the following 24 hours, the Twitter and Facebook accounts of Norsk Hydro posted 7 and 6 updates about the incident, respectively. On March 20th, the company organizes the first press release and Q&A, open to the public via the webcast service webtv.hegнар.no, to provide updates about the cyber incident, and publicizes the event via Twitter and Facebook. On March 21st, the official website is recovered, and a new webpage is explicitly created to report about the cyber-incident, and provide the contacts of the public relations personnel.

In the first two weeks after the incident, the company kept a transparent behavior, providing updates on the website and social media (post count on Twitter: 13, Facebook: 8) regarding the operation status. At this stage, the company used the re-tweet function of Twitter to acknowledge the good behavior and creativity of the employees. In early April, the count of social media posts totaled 11 for Twitter and 3 for Facebook. The first Youtube video [8] highlighting the operational personnel's effort was released on April 2nd. On April 9th, the company releases on the official website an article titled 'Employees find creative solutions in response to cyber-attack' [1], and publicizes it on social media. In late April, the count of social media posts decreased to 7 for Twitter and 3 for Facebook, and a second Youtube video [9] was released on April 16th. Finally, on April 30th a preliminary report [2] is published on the official website, while the official report for Q1 2019 is delayed to June 5th, due to the cyber attack impacting the availability of several systems and data. Consistently with the transparent behavior of the company, the report contains the estimated financial and operational loss.

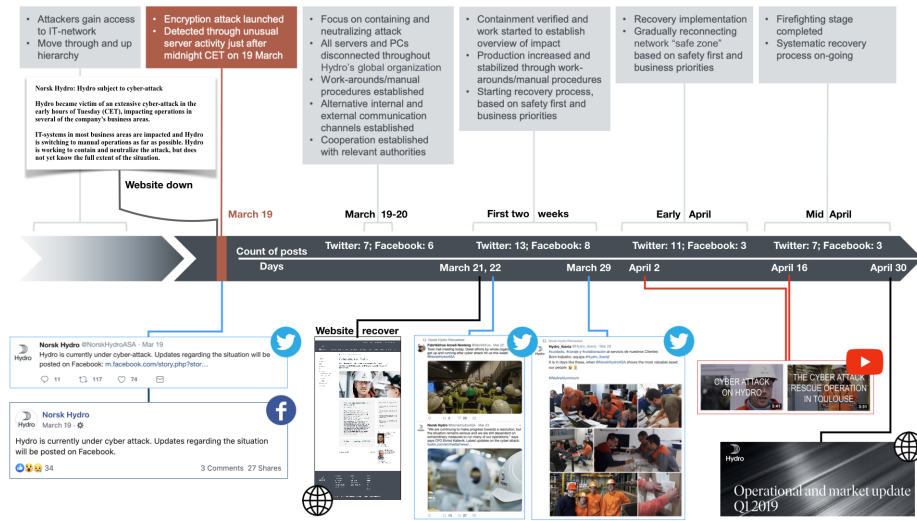


Fig. 2. Timeline of the Norsk Hydro incident [2] (top panel, modified by the author) and the reconstructed highlights of the organizations crisis communication (bottom panel).

4 Lessons Learned

The Norsk hydro case highlighted the benefit of incorporating social media as the medium of crisis communication. During the incident response, the organization continued to show its agility, transparency, and acts of positive reinforcement.

Agility. When the website became unreachable, the organization was quick to determine the alternative platform for communication (facebook and twitter). During the event, multiple platforms were used, including social media and web services. The organization seemed to have a good understanding of each platform; the audience, type of interactions, and its shortcomings. The responding organization has to incorporate the agile process management during the demanding cyber incident response. Agile organizations allow the sharing of information on different levels and between different disciplines, which increases situational awareness and effectiveness [14].

Transparency. Periodic updates on operational status and short documentary videos featuring operators showed honesty and openness. Cornelissen defined transparency as “the state where the image or reputation of an organization held by stakeholder groups is similar to the actual and projected identity of an organization [5]”. Transparency creates, maintains, or repairing trust between the organization and stakeholders.

Positive Reinforcement. In the area of psychology and organizational behavior, numerous research has addressed ways to enhance motivation by creating success-focused environments. Interestingly, Norsk Hydro used social media to communicate with the employees. The organization acknowledged the contributions of the employees by retweeting them and created articles and videos highlighting the operators and responders as heroes. Sveen et al. have studied this mechanism in the security incident reporting system in an organization. The result indicates that the increased number of reporting indicates high information security awareness among the system users, and the increase in user motivation causes an increase in the reporting rate, and vice versa [13].

5 Conclusion

In this paper, we studied the Norsk Hydro case from the perspective of crisis communication. From our analysis, we find that risk communication is not only about apologizing or meeting a reporting duty. Instead, it is crucial to promote good behavior of employees by acknowledging their effort. Moreover, by keeping a transparent communication, lessons learned during the recovery operations can be shared with the community.

In the past, information regarding cyber security incidents was shared internally or with close allies. It is because protecting private information is commonly considered as a critical aspect of cyber incident management. Here, we advocate that companies should be more open about sharing information. Haas et al. [7] suggest that Information Sharing and Analysis Organization (ISAO)s create an atmosphere of transparency and inclusion while emphasizing that information sharing, similar to social networking activity, is a group activity and requires active and frequent involvement. In the Norsk Hydro case, in the two weeks following the incident, the company provided updates about the cyber incident with a frequency of at least one post per day, either on Twitter or Facebook.

Undoubtedly, it is still a challenge to ensure the right balance of disclosing and protecting information to defeat an immediate attack and to prepare for long-term security [6]. For this reason, companies should design protocols about what can be shared and what cannot.

The Norsk Hydro demonstrated that agility, transparency, and positive reinforcement are essential principles to promote the good behavior of employees, facilitate cooperation with the relevant authorities and managing reputation.

References

1. Employees find creative solutions in response to cyber-attack (Apr 2019), <https://www.hydro.com/en-NO/about-hydro/stories-by-hydro/employees-find-creative-solutions-in-response-to-cyber-attack/>
2. Operational and market update q12019 (Apr 2019), <https://www.hydro.com/Document/Index?name=Hydro%20Q1-2019%20Update&id=42133>

3. Cimpanu, C.: Protonmail ddos attacks are a case study of what happens when you mock attackers (Jun 2018), <https://www.bleepingcomputer.com/news/security/protonmail-ddos-attacks-are-a-case-study-of-what-happens-when-you-mock-attackers/>
4. Coombs, W.T.: *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications (2014)
5. Cornelissen, J.P.: *Corporate communication*. The International Encyclopedia of Communication (2008)
6. Goodwin, C., Nicholas, J.P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Mas-sagli, A., Mckay, A., Mckitrick, P., Neutze, J., et al.: *A framework for cybersecurity information sharing and risk reduction*. Microsoft (2015)
7. Haass, J.C., Ahn, G.J., Grimmelmann, F.: Actra: A case study for threat information sharing. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. pp. 23–26. ACM (2015)
8. Hydro, N.: Cyber attack on hydro magnor (Apr 2019), <https://www.youtube.com/watch?v=S-ZlVUM0we0>
9. Hydro, N.: The cyber attack rescue operation in hydro toulouse (Apr 2019), <https://www.youtube.com/watch?v=o6eEN0mUakM>
10. Kulikova, O., Heil, R., van den Berg, J., Pieters, W.: Cyber crisis management: A decision-support framework for disclosing security incident information. In: *2012 International conference on cyber security*. pp. 103–112. IEEE (2012)
11. ProtonMail: A brief update regarding ongoing ddos incidents (Jul 2018), <https://protonmail.com/blog/a-brief-update-regarding-ongoing-ddos-incident/>
12. Steelman, T.A., McCaffrey, S.: Best practices in risk and crisis communication: Implications for natural hazards management. *Natural hazards* **65**(1), 683–705 (2013)
13. Sveen, F.O., Sarriegi, J.M., Gonzalez, J.J.: The role of incident reporting in reducing information security risk. In: *Twenty Seventh International Conference of the System Dynamics Society*. The System Dynamics Society (2009)
14. Van Veelen, B., Storms, P., van Aart, C.: Effective and efficient coordination strategies for agile crisis response organizations. *Proceedings of ISCRAM 2006* (2006)
15. Veil, S.R., Buehner, T., Palenchar, M.J.: A work-in-process literature review: Incorporating social media in risk and crisis communication. *Journal of contingencies and crisis management* **19**(2), 110–122 (2011)
16. Von Solms, R., Van Niekerk, J.: From information security to cyber security. *computers & security* **38**, 97–102 (2013)
17. Weiner, D.: Crisis communications: Managing corporate reputation in the court of public opinion. *Ivey business journal* **70**(4), 1–6 (2006)

A.3 TRAINING CYBER SECURITY EXERCISE FACILITATOR: BEHAV-
IOR MODELING BASED ON HUMAN ERROR

Training Cyber Security Exercise Facilitator: Behavior Modeling based on Human Error

Shiho Taniuchi, Tomomi Aoyama, Haruna Asai and Ichiro Koshijima

Nagoya Institute of Technology, Bldg.16 305 Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan

Abstract. Exercise facilitators are essential in the field of cybersecurity trainings. They provide a useful insights to the exercise participants, while guiding the group discussion. During the exercise conducted at the Nagoya Institute of Technology, the variation of exercise deliveratives were observed due to the uneven facilitation. In this paper, facilitation error was studied by modeling the error behavior as the error of omission and commission. The quality of the facilitation was evaluated based on the error occurrence.

Keywords: Cyber security · tabletop exercise · facilitation · Human error · Omission error · Commission error

1 Background

1.1. Increasing cyber risk awareness

Cyber threat is no longer ignorable for critical infrastructure operators. In the modern connected world, Industrial control systems (ICS) which are widely used in the automated process are vulnerable to the threat. The consequence of a cyber attack targeting ICS may result in damaging health, safety, and environment (HSE) factors of the organization.

Cybersecurity process can be grouped into three phases - prevention, detection and response [1]. Conventional mitigation procedure was focused heavily on first two phases; however, the past incidents taught us that the sophisticated cyber attack may be difficult to prevent and detect.

In order to increase the response capability, response planning and communication management are essential. Response activities should be coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies [2]. These capabilities can be established and managed by conducting response exercise and trainings.

1.2. Developing cyber incident response exercise

Nagoya Institute of Technology has developed a table-top exercise to simulate an incident response process and communication [3], promoting to increase cyber risk awareness among ICS security stakeholders [4].

The exercise is designed to encourage the stakeholders to explore the necessity of the organization-wide collaboration in response to a cyber-attack targeting ICS [5]. The exercise scenario is divided into three phases [6] according to the progress of the cyber attack.

Phase X - Detection : Ensure the safety of a chemical plant system from a suspicious cyber attack

Phase Y - Response : Review the incident response procedure with the business risk mindset

Phase Z - Recovery : Organize a recovery plan from the incident

Exercise participants engage in the exercise as a group of four to six people. In each phase, participants create a swimlane diagram to identify who in the organization is responsible for which action. The output visualizes the participants' perspective on the ideal command and communication structure of the incident response.

During the exercise, a facilitator is assigned to each group. The role of a facilitator is to guide the discussion of the group, while providing an additional explanation to the exercise scenario [4].

1.3. Facilitators' effect on exercise participants

In the past exercises, variations of deliverables were observed. It has been thought that the fluctuation is a result of participants' difference in their background experiences. However, since the facilitator leads the discussion of the group, it is possible that they are influencing the group decision making.

In fact, although facilitators were provided with a general idea of their role in the exercise, there was no guidance of the execution method. Their performance has heavily relied on their empirical knowledge. It is necessary to review their performances to understand their differences, and provide consistent facilitation regardless of the facilitator.

2 Establish the Facilitation Error Model

2.1. Defining Facilitation

Facilitation is defined as 'an act of helping other people to deal with a process or reach an agreement or solution without getting directly involved in the process, discussion, and so on[7]. Its concept is adopted in many fields from education[8] to business meetings[9].

The role of facilitator in the above mentioned exercises is similar to that in learning facilitation.

The purpose of learning facilitation is to guide learners to the predefined destination of learning. The role of a facilitator is to guide the learner by utilizing the knowledge of the learning contents and the presentation skill-set [10]. Schwartz defined facilitation

tion as a process to improve the group's ability by improving problem definition, problem solving and decision-making methods in the group [11].

From the literature review ([11,12,13]), the fundamental facilitation process and the seven core capability indicators are determined.

2.1.1. Fundamental facilitation process

Boyd's OODA loop [12] breaks down the decision making and action process with four steps: sensing yourself and the surroundings (Observation), familiarize the situation based on the complex filters of genetic heritage, cultural predispositions, personal experience, and knowledge (Orientation), decide the courses of action (Decision), and finally testing the selected act by implementation (Action) [13].

Correspondingly, the fundamental facilitation process can be explained with this framework. Firstly, the facilitator collects the remarks and observes the group in order to understand the situation (Observation), assess the situation (Orient), decide the method to interfere the situation based on the pre-defined role (Decision), then approach to the group (Action).

2.1.2. Core capability indicators

In order to perform the above mentioned activities, the following seven capabilities are required.

Neutrality - avoid showing preferences and biased opinion

Emotion control - manage own emotions and be aware of the participants' mental state

Observation - monitor the participants' actions, verbal and non-verbal expression, and shift of emotions

Sharing - convert one person's learning into the group learning

Descriptive - comprehend and summarize the group opinion, supplement the details with the knowledge of the contents

Trust building - create an environment for active discussion

Learning - accumulate knowledge from the past facilitation experience

2.2. Error model of the facilitation

Even if facilitation is performed according to the fundamental facilitation process, the facilitator does not necessarily take the same action in each process phase due to the difference in core capability. The execution method may vary depending on the context of the situation. Therefore, in this paper, the authors explore the behavior model of the exercise facilitator by identifying the improper action as an error.

Human error is defined as "deviation from required performance" [14]. In other words, the facilitation error is defined as a deviation from "guide learners to the pre-defined destination of learning" where the facilitator "should perform", and the facilitator error is extracted from observation.

Swain studied the human performance reliability by dividing error factors into two categories: error of commission and error of omission. Two error modes are defined as following [15].

Error of commission - incorrect performance of a system-required task or action, given that a task or action is attempted, or the performance of some extraneous task or action that is not required by the system and which has the potential for contributing to some system-defined failure.

Error of omission - failure to initiate performance of a system-required task or action. Swain's taxonomy is applied in the context of the performance error in exercise facilitation. In this study ECOM and EOM are redefined as following.

Facilitator's error of commission (ECOM) - facilitator's incorrect performance by interfering or influencing participants' decision making and learning.

Facilitator's Error of omission (EOM) - facilitator's failure to initiate necessary involvement with participants' discussion, in order to induce the participants' leaning.

3 Research Methods

3.1. Qualitative Analysis of audio recordings

During the exercise, facilitator intervenes the participants' discussion. Their conversation is ad-hoc, and non-scripted. In order to understand the nature of facilitation error without interfering the nature of the exercise, the research was conducted by recording the facilitators' utterance. The recordings were transcribed to text format to conduct a qualitative analysis.

3.2. Data Collection

The data were gathered from the recordings of the two exercises, consists of two phases. Four facilitators (Facilitator A, B, C, and D) participated the experiment. Table 1 shows the detail of each recording.

Table. 1 Details of the Recording

Recording no.	Date (YYYY/MM/DD)	Exercise phase	Facilitators subject to analysis
1	2017/11/22	X	B, C, D
2	2017/11/22	Y	B, D
3	2018/1/12	X	A, B, D
4	2018/1/12	Y	B, D

4 Analysis

4.1. Identifying error from the core capability indicators (Exercise Phase X)

Exercise Phase X (Recording No. 1, 3) is the first phase of the exercise. Therefore, facilitator spends most of the time explaining the detail of scenario. The explanation should be consistent and thorough. Also, facilitator answers the questions raised by participants. In this process, it is a challenge to keep the neutrality.

From these perspective, the utterance that lacks the neutrality or description was extracted from the recording of interaction between facilitators and participants during the exercise. The quality of facilitation was evaluated from the counts of error occurrences. The relation between the quality and experience was examined.

4.2. Analysing deviation from the learning goals (Exercise Phase Y)

As a result of revisiting the definition of human error in the Section 2, it revealed the structural problem of the exercise, that is to say, the performance requirement for the facilitator was not defined in detail by design. Meanwhile, experienced facilitators have acquired the empirical knowledge of participants' learning goals.

In the exercise phase Y (Recording No. 2, 4), participants discuss the organizational responses to a cyber attack from multiple perspectives of safety, security and business continuity. To that end, the learning goals of this phase is relatively complicated than other phases.

In the interest of this study, participants' learning goals were extracted to a list of 18 items, by analysing the deliverables of the multiple exercises, and conducting an interview to experienced exercise facilitators. With this list of learning goals, the role of facilitator is defined to guide participants to achieve the defined learning goals.

The analysis was conducted in the process shown in Fig.1. EOM can be identified by analysing the gap between the list of learning goals and participants' deliverables, and the dialogue. In order to identify ECOM, the recording was examined to determine whether the corresponding remark was initially mentioned by the facilitator or the participants. Among them, ECOM was identified based on whether the facilitator mentions the learning goal directly or not. When the facilitator avoids revealing the listed items on learning goals, by guiding the discussion organically, it is not considered as error.

The occurrence of error was noted to evaluate the performance of facilitators, and its relation to their experience.

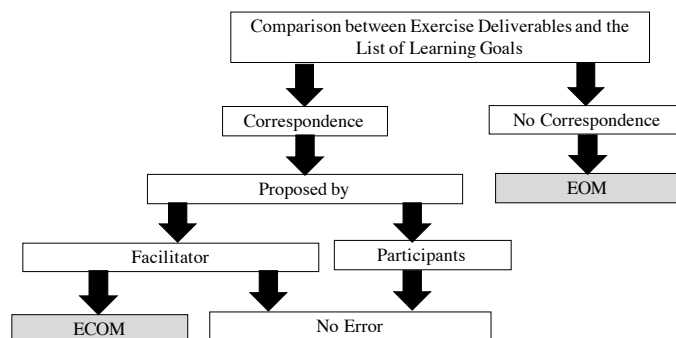


Fig. 1. Error identification process

5 Results

5.1. From the core capability indicator (Exercise Phase: X)

Table 2 shows the observed facilitation errors and its corresponding remarks which are extracted from the utterance of facilitators. ECOM were identified as the lack of neutrality, such as favoring particular opinion and providing judgment. Lack of explanation and misdirection were classified as EOM. As the result, four EOM and seven ECOM were identified. Facilitator D, who is the most experienced, did not perform any facilitation error. Meanwhile, facilitator B, who participated twice, provided a diverse error profile; two ECOM in the first, and three EOM in the second trial. This shift suggests that this facilitator tried to correct the past behavior in the second trial. For this reason, error profile can change over experience.

Table 2. Observed facilitation errors and corresponding remarks

Date	Facilitator	Utterance	Reasoning	Error Type
2018/1/12	A	"The safety control office is <u>not necessary</u> ."	Judgment of necessity	ECOM
		"It is <u>better</u> to contact all"	Judgment of necessity	ECOM
		"That is <u>good</u> ."	Agreement	ECOM
		"Cybersecurity skills are <u>necessary</u> for the Boardman and others to notice the attack"	Judgment of necessity	ECOM
2017/11/22	B	"It is <u>possible</u> that SCADA output is concealed"	Should be noticed by participants	ECOM
		"Since you can doubt the on-site panel, <u>you need to check</u> the level gauge"	Should be noticed by participants	ECOM
2018/1/12	B	"Please <u>assume</u> that head office IT is familiar with the site"	Lack of explanation	EOM
		"The factory side is busy during manual valve operation. Therefore <u>investigation is difficult</u> ."	Misdescription	EOM
		"Safety management office <u>manages safety</u> ."	Lack of explanation	EOM
2017/11/22	C	"Automatic control is carried out under normal conditions. ... <u>We doubt that the setting value has been changed due to a human error or the like</u> "	Misdescription	EOM
		"Information that IT has suspicious <u>communication should be developed</u> ."	Judgment of necessity	ECOM

In Fig.2, the count of facilitation error occurrence is compared by facilitators' experience. From left to right, error count of each facilitator is arranged according to the number of the facilitation experiences. Each facilitator's experience is numbered in parentheses.

From Fig. 2 we can see the following;

- (1) ECOM decreases with experience,
- (2) EOM decreases with experience, and
- (3) error profile swings between EOM and ECOM centric.

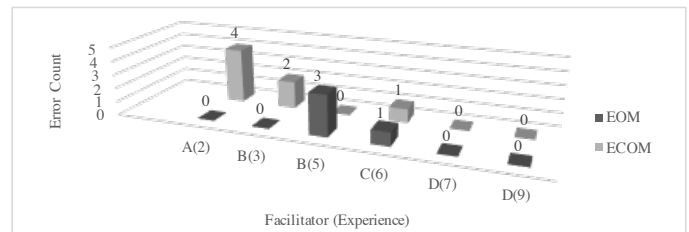


Fig. 2. Comparison of the count of facilitation error occurrence by experience (Phase X)

This fluctuation can be explained as the result of overcorrecting the past performance (Fig.3). It also suggests that the width of this swing gets smaller over time. Therefore, it can be said that facilitator naturally learns from the past mistakes, and performance gets better by experience.

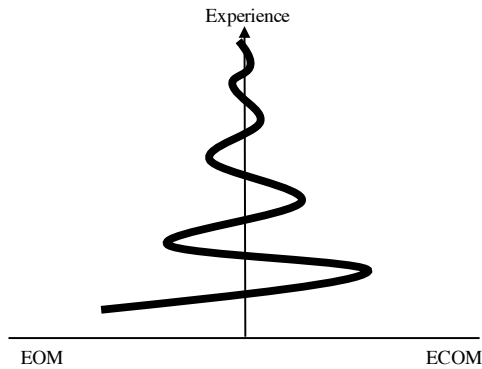


Fig. 3. Maturity model of facilitator

5.2. From the learning goals (Exercise Phase: Y)

Table3 shows the result of the error identification process explained in the fig. 1. Two facilitators with different proficiency (Facilitator B and D) were subjected to analysis twice.

In the Table, EOM (No correspondence to the learning goal list) is marked as '-', and items subjected to further utterance analysis to determine ECOM (item suggested by a facilitator) are indicated by 'X'. Since the item suggested by participants is not subjected to error categorization, the according cells is left bank (colored in gray).

Table. 3. The List of Learning Goals

conflict	items	Facilitator				Workflow	Fill in example
		B		D			
		2017/11/22	2018/1/12	2017/11/22	2018/1/12	no correspondence	-
SaKety-Security	1 Confirm factory	-	-	-	-	correspondence (Facilitator)	X
	2 Confirmation of SCADA screen values and operate	-	-	-	-	correspondence (Facilitator)	X
	3 Confirm the fire drill response sufficient	-	-	-	-	correspondence (Facilitator)	X
	4 Confirmation of input of elect 2	-	-	-	-	correspondence (Facilitator)	X
	5 Confirm impact of load office	-	-	-	-	correspondence (Facilitator)	X
	6 Safety survey of backup data before assertion	-	-	-	-	correspondence (Facilitator)	X
SaKety-Security	7 Network segmentation	-	-	-	-	no correspondence	-
Security-Business	8 Designation of forensic target equipment	-	-	-	-	no correspondence	-
Security-Business	9 Designation of internal equipment for forensic	-	-	-	-	no correspondence	-
SaKety-Business	10 Network segmentation location	-	-	-	-	no correspondence	-
	11 When to disclose information to customers	-	-	-	-	no correspondence	-
	12 When information should be reported to customers	-	-	-	-	no correspondence	-
Security-Business	13 When to communicate external reports	-	-	-	-	no correspondence	-
	14 How to communicate external reports	-	-	-	-	no correspondence	-
Communication	15 How to communicate technical terms	-	-	-	-	no correspondence	-
	16 Whether to adjust the granularity of information	-	-	-	-	no correspondence	-
Human	17 Who leads and responds	-	-	-	-	no correspondence	-
	18 Who decides whether to continue or stop	-	-	-	-	no correspondence	-

ECOM were identified as shown in the Table4. The remarks made by facilitator and the corresponding learning goal are listed. As the result, three ECOM were identified. ECOM occurs when a facilitator answers to a question raised by participants, and also

by failing to segue from other discussion topics. ECOM was avoided by suggesting in interrogative sentences. Especially, the experienced facilitator (D) tend to form a shorter question than the less experienced (B).

Table. 4. Identifying ECOM from the facilitators' utterance

Date	Facilitator	Relevant List Item No.	Utterance	Error / No Error
2017/11/22	B	3	"Manual valve operation can not be continued forever. Also, <u>a human error may occur.</u> "	ECOM
2017/11/22	D	4	"Would you like to contact them about cyber attacks?"	No Error
		5	"... Since production data is handed over to the head office through here, <u>I think that the production plan will be affected.</u> "	ECOM
		10	"What part of the network do you want to disconnect?"	No Error
		14	"What external people will you contact?"	No Error
2018/1/12	B	6	"Backups are being taken, <u>but possibly contaminated.</u> "	ECOM
		17	"Is CSIRT leading the entire operation?"	No Error
2018/1/12	D	5	"Do you mean to check if there is an influence?"	No Error
		10	"The influence varies depending on the cutting place. It is necessary to be confirm by someone."	No Error

The count of error occurrence of each facilitator was summarized into Fig 4. In spite of the difference of their experiences, both facilitators marked high counts of EOM. In addition, no improvement on EOM has observed on two performances of facilitator B. Moreover, even the most experienced facilitator omitted nearly 40% (7 EOM out of 18 items) of the learning goals. It can be concluded that EOM tends to occur repeatedly, since facilitator is not aware of causing EOM.

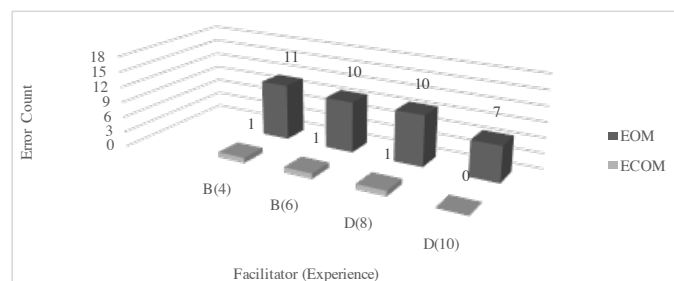


Fig. 2. Comparison of facilitation error counts by facilitator's experience (Phase Y)

6 Discussions

In this paper, facilitation error was studied by modeling the error behavior as the error of omission and commission. The error was identified with two approaches; compari-

son to the core capability indicators, and completeness of the list of learning goals. The quality of the facilitation was evaluated based on the error occurrence. As a result, it was found that less experienced facilitators are more prone to facilitation errors, and as gaining more facilitation experience, the number of error decreases. Also, it is more likely that facilitators are unaware of own EOM, therefore EOM is difficult to mitigate naturally. The results from section 5.1 suggested that facilitators learn natural learning path of facilitation. Although it is expected that facilitators would learn to perform better by empirical learning, a supporting mechanism may expedite this learning process. Learning by examples is an effective method to prevent future errors [18]. Each facilitator accumulates error cases by experiencing. However, this study revealed that facilitators are unaware of some of the error. Therefore, for the further error mitigation, it is important to have (a) a mechanism to detect errors and (b) a mechanism to generate more error cases to accumulate. In order to increase the error recognition, objective evaluation efforts, such as the list of the learning goals developed specifically for this study, may be useful. It can encourage facilitators to review the performance by themselves. Moreover, in order to gather more cases, it is better to share the cases among facilitators. They can learn the variety of error by reviewing the recordings of other facilitator's performance.

It is reported that the cybersecurity workforce gap is on pace to hit 1.8 million by 2022 [19]. In proportion to the expanding demand, the continuous growth of cybersecurity training and education market is expected. It is important to maximize the learning in each training. We conclude that the quality of facilitation should be reviewed to increase the quality of the training.

References

1. LaPiedra, J.: The Information Security Process Prevention. Detection and Response, Global Information Assurance Certification Paper, GIAC directory of certified professionals (2011)
2. Cybersecurity, Critical Infrastructure.: Framework for Improving Critical Infrastructure Cybersecurity. Framework 1, 11. (2014)
3. Ota, Y., Aoyama, T. and Koshijima, I.: Cyber Incident Exercise for Safety Protection in Critical Infrastructure. 13th Global Congress on Process Safety, San Antonio, USA, (2017)
4. Aoyama, T., Watanabe, K., Koshijima, I., Hashimoto, Y.: Developing a Cyber Incident Communication Management Exercise for CI Stakeholders. 11th International Conference on Critical Information Infrastructures Security, pp.13-24. Paris, France (2016)
5. Ota, Y., Aoyama, T., Davaadorj, N., Koshijima, I.: Cyber incident exercise for safety protection in critical infrastructure. Int. J. of Safety and Security Eng, Vol.8, No.2, pp.246--257. (2018)
6. Hirai, H., Aoyama, T., Davaadorj, N., and Koshijima, I.: Framework for Cyber Incident Response Training, Safety and Security Engineering VII, pp.273--283. Rome, Italy, (2017)
7. "Facilitation." Cambridge business English dictionary, <https://dictionary.cambridge.org/dictionary/english/facilitation>.

8. Hmelo-Silver, C.E., Howard, S. B.: Goals and strategies of a problem-based learning facilitator. *Interdisciplinary Journal of problem-based learning* 1.1, 4. (2006)
9. Miranda, Shalla M., and Robert P. Bostrom.: Meeting facilitation: process versus content interventions. *Journal of Management information systems* 15.4, 89–114. (1999)
10. Shirai, Y., Washio, A., Shimomura, T.: Role of Facilitators in Group Learning in Higher Education. (in Japanese) pp.109–118. (2012)
11. Roger, S.: *The Skilled Facilitator: A Comprehensive Resource for Consultants, Facilitators, Managers, Trainers, and Coaches* (2002)
12. Hori, K.: *Organizational change facilitator*. (Japanese) Toyo, Keizai(2006)
13. Donald, V.M., Deborah, D.T.: *Basics of Learning facilitation*. (Japanese) Kazuaki, K. translation (2015)
14. Boyd, J.R.: The essence of winning and losing. Unpublished lecture notes 12.23, 123-125. (1996)
15. Osinga, F.B.: *Science, strategy and war: The strategic theory of John Boyd*. Routledge, (2007)
16. James, R.: *Human error*. Cambridge university press. (1990)
17. Swain, A.D.: Accident sequence evaluation program: Human reliability analysis procedure. No. NUREG/CR-4772; SAND-86-1996. Sandia National Labs., Albuquerque, NM (USA); Nuclear Regulatory Commission, Washington, DC (USA). Office of Nuclear Regulatory Research. (1987)
18. Nakamura, T.: Human error from psychological perspective. (in Japanese) pp.29–32 (2009)
19. Isc2.org. (2017). Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher. [online], <https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage> [Accessed 2 Mar. 2018].

APPENDIX: CASE STUDY FOR APPLYING PROPOSED FRAMEWORK

B.1 CASE STUDY: CRITICAL INFRASTRUCTURE INCIDENT RESPONSE EXERCISE BY NISC

From the exercise organizer's perspective, it is important to know which tier the participant belongs to, and aims at. It helps the organizer to design exercise at the suitable level. However, the designing is particularly challenging when the participating organization is plural, and their tier level varies.

One of the measures is to select one tier level as a standard level. The other measure is to select an exercise method applicable to many tier levels, customize the aim and according to the variation of the tier, and conduct the exercise of several tier levels in parallel.



Figure B.1: Exercise structure of CIIREX.

In this section, we use the proposed tier-specific exercise framework to understand the preparedness of the exercise participants from their method of participation and aims. In addition, we discuss how this table-top exercise can be adapted to several tier levels, by examining observed cases from CIIREX.

STYLE OF THE EXERCISE This annual exercise is a combination of a drill and a table-top exercise. Two important features of this exercise are (A) the attendance of majority of CI operators, authorities, and related organizations and (B) the exercise with the latest threat scenario. Correspondingly to these features, the participating organizations can (a) simulate the information sharing procedure by contacting the participating authorities via telephone and emails (drill), while (b) review the effectiveness of their incident response plan by discussing within the colleagues (table-top exercise).

Communication procedure is mostly standardized in each CI sectors; hence, regardless of their tier level, the participants share the same goal of demonstrating the procedure together with the authorities. On the other hand, because of the difference of their security capability and organizational culture, the maturity and style of their incident response plan varies between organizations. Therefore, the intensity of the exercise scenario is kept at the moderate level.

The exercise controller provides scenario injections to all participants simultaneously (e.g. "JPCERT/CC¹ released an alert regarding the DDoS² attack targeting domestic organizations"). Some of the injections are general, but others require tailoring (e.g. "Employee A from [Department X] has contacted [IT Department] that he cannot log in to [the core IT system]"). One participant in each organization plays the role of "sub-controller", and fills in the brackets ([]).

PARTICIPANTS AND THEIR AIM The exercise is held in several locations simultaneously; at the venues in three major cities ("on-site participation") and at participants' offices by accessing the system via the Internet ("remote participation"). Due to the capacity of the exercise venue, on-site participation from an organization is limited to 1 to 5 people. At the venue, a variation of participation style has been observed. It seemed that the maturity of participating organizations' security level is displayed by their participation style and their aim.

¹ Japan Computer Emergency Response Team Coordination Center

² Distributed Denial of Service

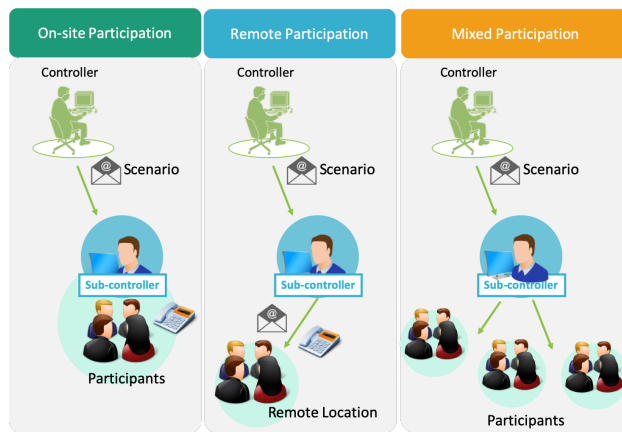


Figure B.2: Observed participation styles.

Case 1: Single participant on site, *without* additional remote participants

- **Participation:** The on-site attendant represents the organization.
- **Aim:** The attendant's goal is to familiarize with the exercise settings. He/she experience how the threat affects the organization (*Awareness*), while simulating the information sharing procedure (*Technical skills*).
- **Preparedness:** The participant seemed to be in charge of finding solutions to implement security into the organization. Most likely the organization has limited risk awareness, and doesn't own more than one personnel to work on security. Therefore the organization of this case belongs to *Tier 1*. From the lessons learned in the exercise, the organization may increase the awareness, and develop a risk management process. The participation to this exercise can trigger the transition from *Tier 1* to *Tier 2*.

Case 2: Single participant on site, *with* additional remote participants

- **Participation:** The on-site attendant plays the role of the sub-controller. He/she communicates with colleagues via phone calls and emails. The remote participants partially join the exercise while operating their daily business routine. Few organizations participated in this method. The remote participants may be from a single department (often IT), or cross-sectional (such as

the involvement of the customer service, public relations (PR), and the management). In this case, the former type of remote involvement was observed.

- **Aim:** They simulate and verify the effectiveness of the predefined incident reporting procedure (*Technical Skill*) while discussing the improvements.
- **Preparedness:** The organization may not require more than one personnel to work on security at full-time, proportional to the business size. Otherwise, it may lack the organization wide risk awareness, and the full-time exercise attendance was not considered important compare to the daily operation. Therefore this organization belongs to *Tier 2*. Cross-sectional involvement may increase the organization wide awareness, be the stepping stone to *Tire 3*.

Case 3: A group from IT department

- **Participation:** Few people from IT department attended the exercise. The role of sub-controller is likely to be played by the most experienced personnel. Most of the organizations participated in this style.
- **Aim:** They simulate and verify the effectiveness of the predefined incident reporting procedure (*Technical Skill*) while discussing the improvements. Some groups were using this opportunity to transfer the know-hows from the experienced member to the other(*Non-technical Skill*).
- **Preparedness:** The team is prepared to operate the predefined procedure, but the lack of other departments' involvement suggests the lack of organization wide approach (*Tier 2*). The observation suggests that in this type of organizations, the knowledge is heavily concentrated in the most experienced personnel, and not easily transferred across organizations.

Case 4: Cross functional team

- **Participation:** The attendants were mixed group of several departments, such as IT, PR, and risk management.

- **Aim:** They simulate and verify the effectiveness of the predefined incident reporting procedure (*Technical Skill*) while discussing the improvements. They use the opportunity to understand the other department's operations, in order to coordinate in incident response procedure (*Non-technical Skill*).
- **Preparedness:** The involvement of several departments often requires the organization-wide risk awareness. Some organization actively communicate with other participants from the same group enterprise, or other CI operators. This type of organizations has a high adaptability to the situation. For this reason, they belong to *Tier 3* to *Tier 4*.

Observations of the above four cases show that the participating organizations' preparedness varies from *Tier 1* to *Tier 4*. The role of sub-controller is one of this exercises' characteristics. It allows each organization to customize the exercise scenario to their unique systems. Moreover, because the internally selected sub-controller takes over the role of controller, the participants can comfortably focus on the exercise with minimum interference from the exercise organizer (controller) who is an outsider. In addition, the combination variety of on-site and remote participation gives flexibility to participants, to adjust the exercise scope from individual to organizational.

SUGGESTIONS FOR THE EXERCISE IMPROVEMENT The exercise is successful owing to its customizable and generic scenario, and its parallel administration mechanism. However, considering the tier level of the participants, the exercise aim should include non-technical skills and resilience (Figure 4.1). For some capable organizations, the general scenario may not stimulate their learning enough. The exercise scenario should be familiar to the participants' business, and also adjustable by their aim. For example, for the *tier 4* organizations, the exercise scenario can include the interdependency of CI.

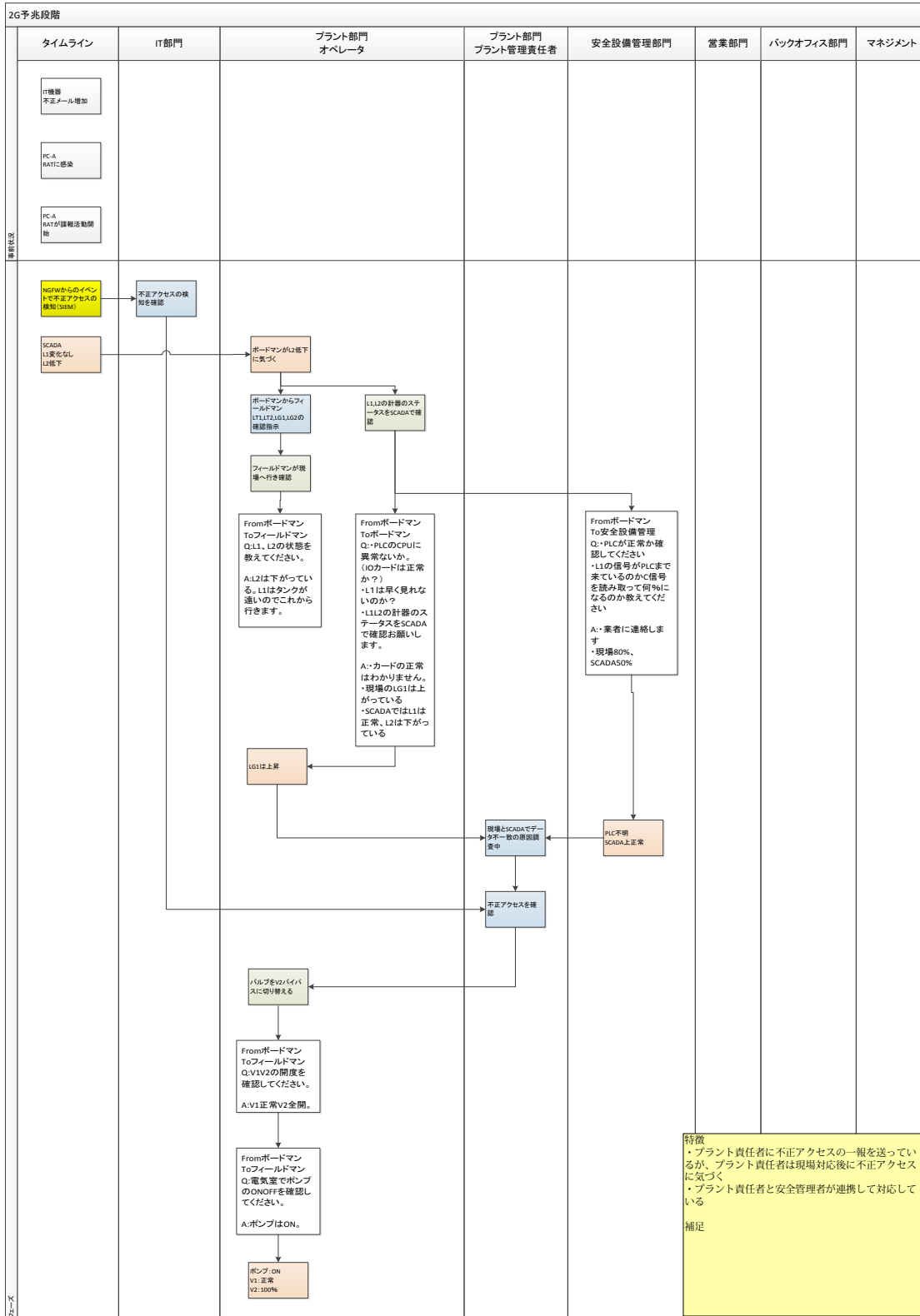
Additionally, due to the nature of the large scale exercise, the organizer cannot understand each participants' style and aim of participation. Consequently, the organizer cannot support the participants' learning opportunity. The concept of tier and the presented tier specific exercise framework is useful for participants to understand the

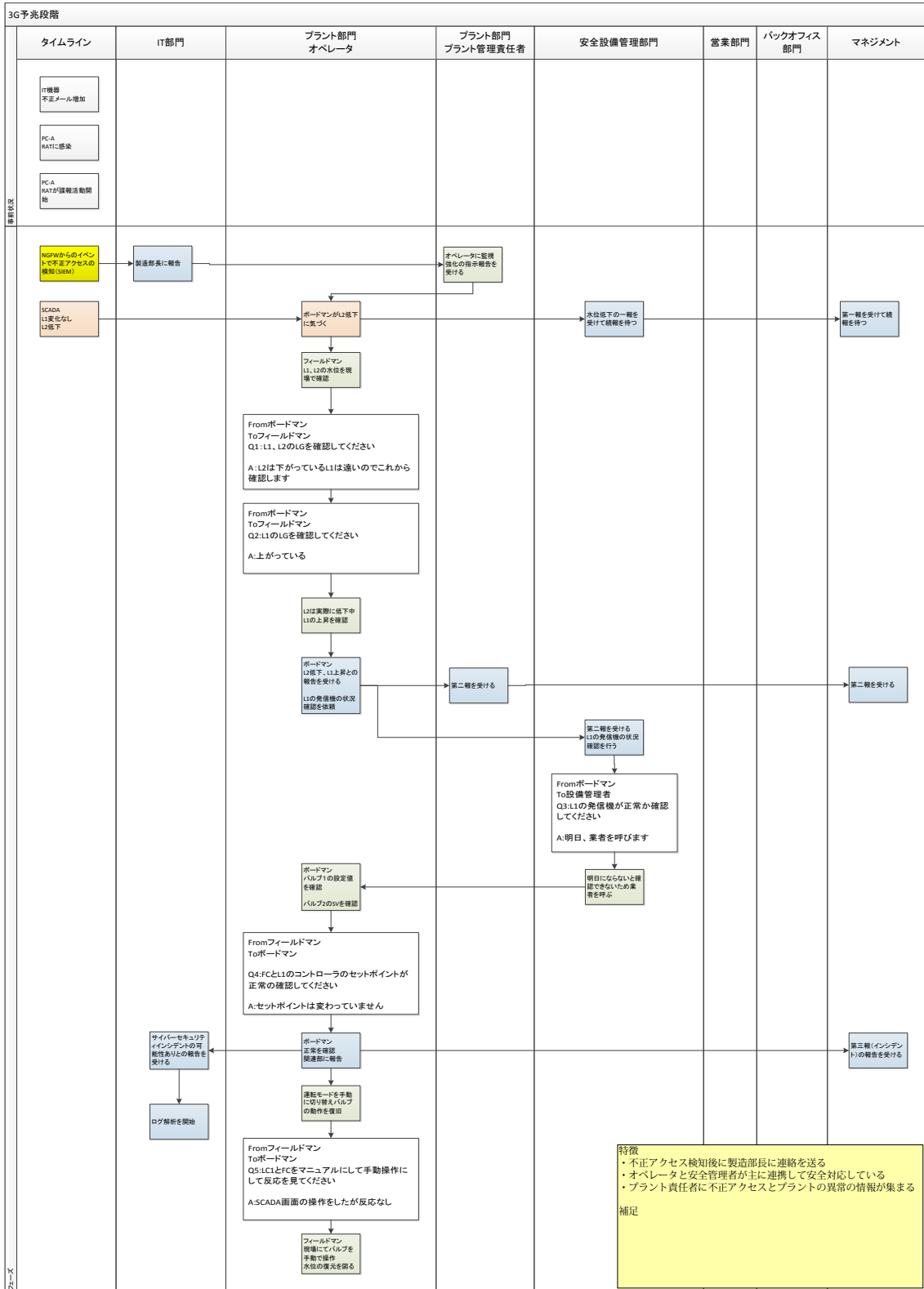
current preparedness, and what steps to be taken in order to enhance their capability. It is also helpful to share both common and unique usage of the exercise settings publically, as in the above cases.

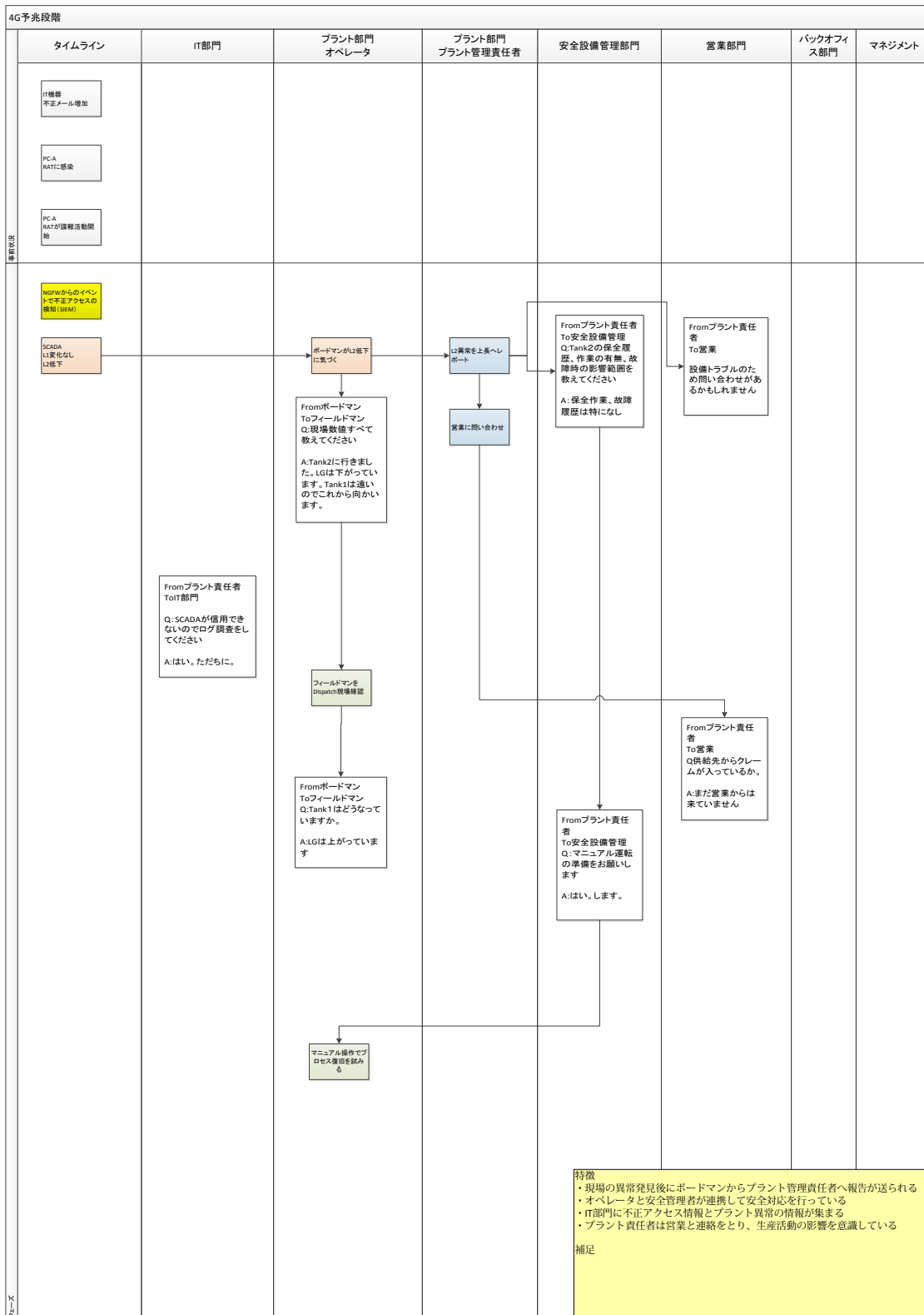
C

APPENDIX: EXERCISE MATERIALS

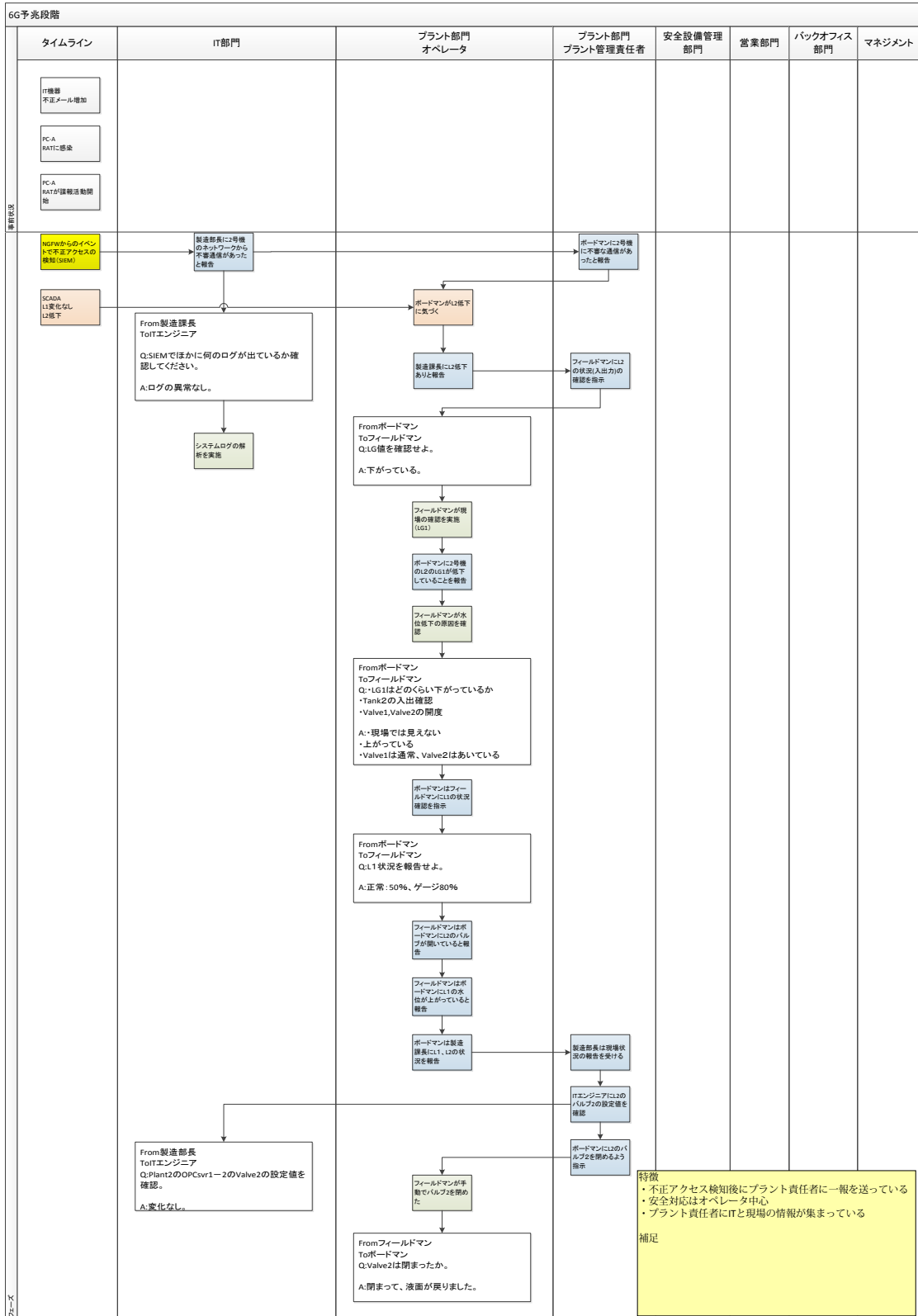
C.1 EXAMPLE OF TTX DELIVERABLE

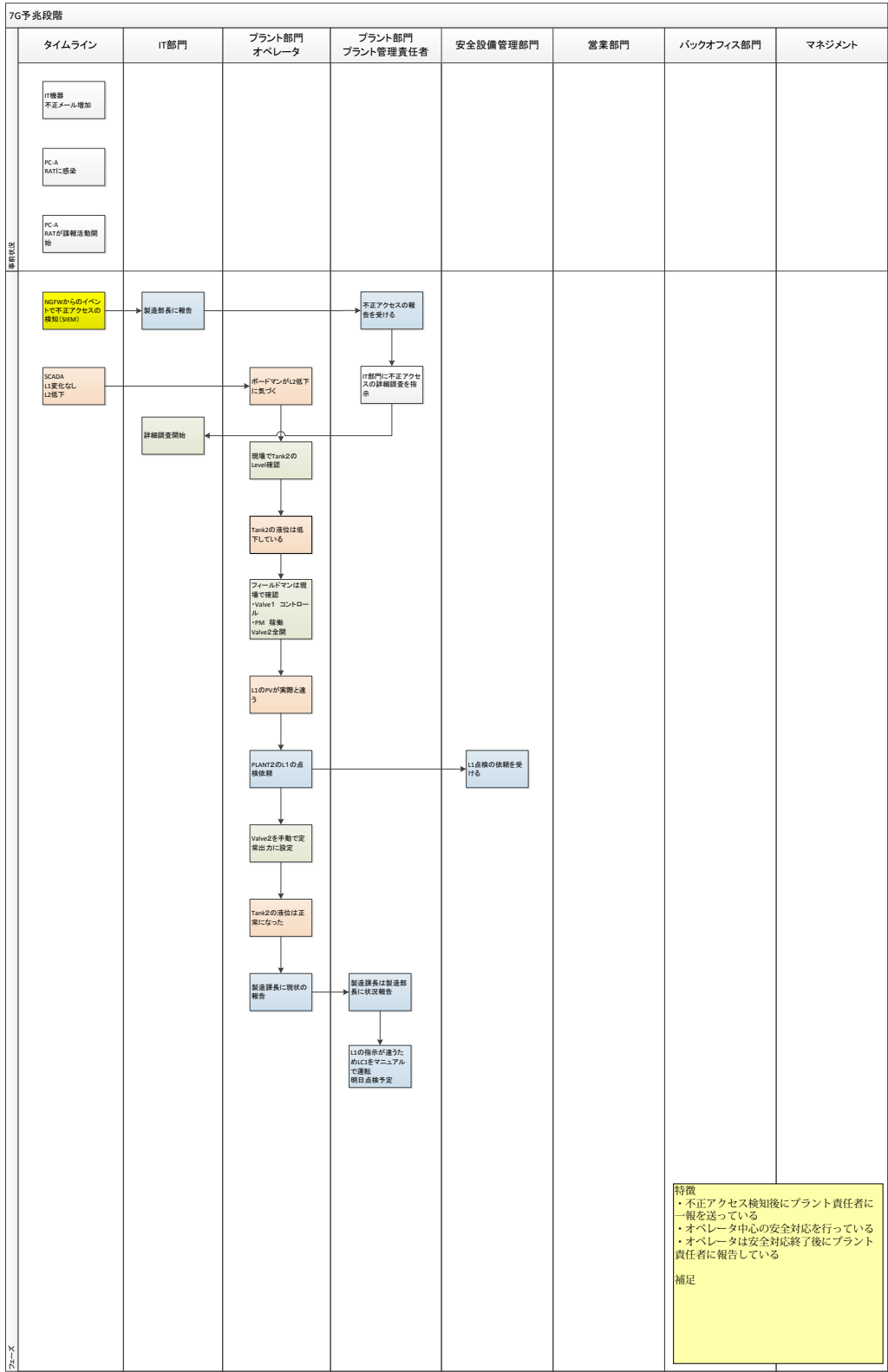


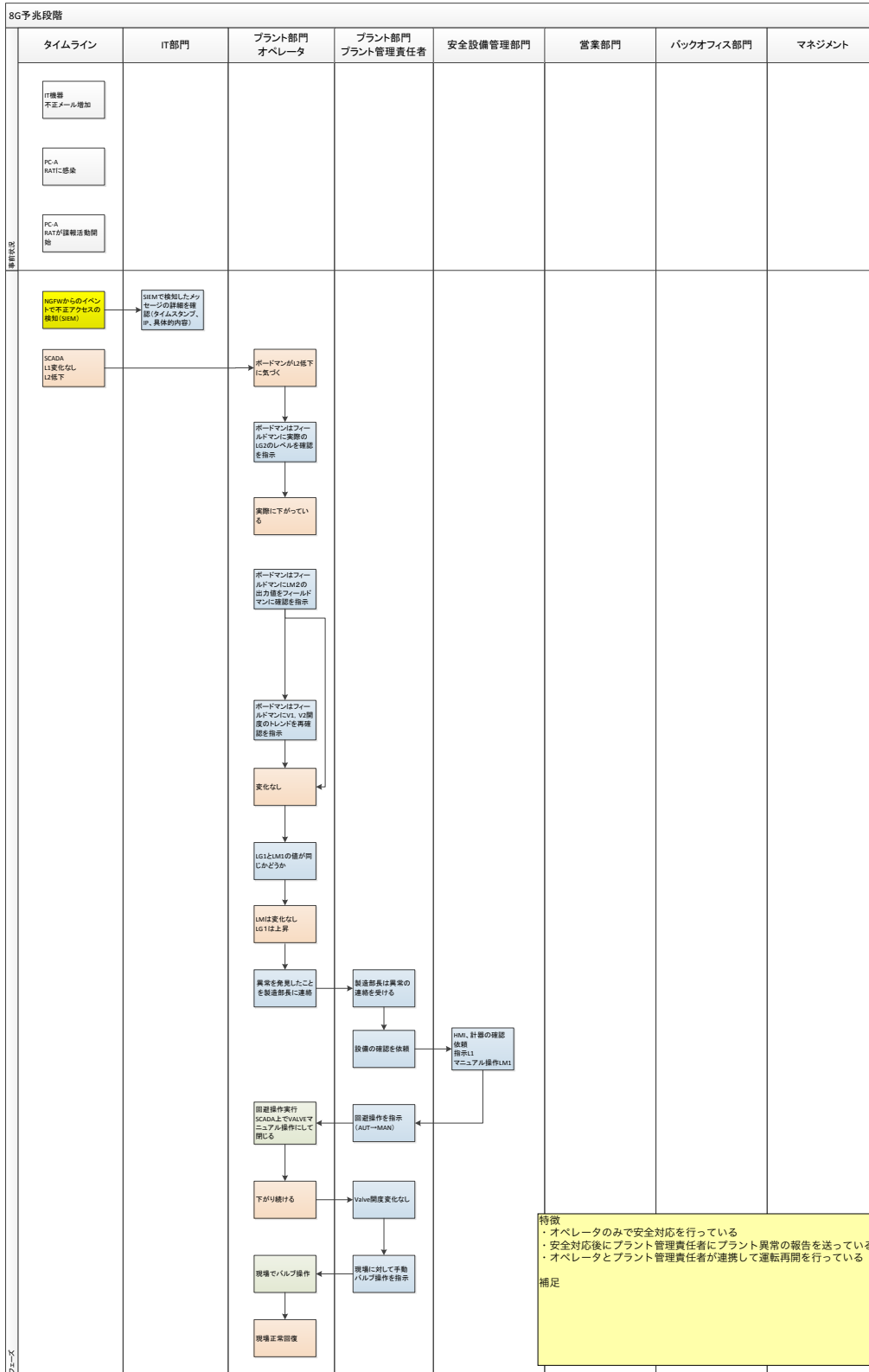


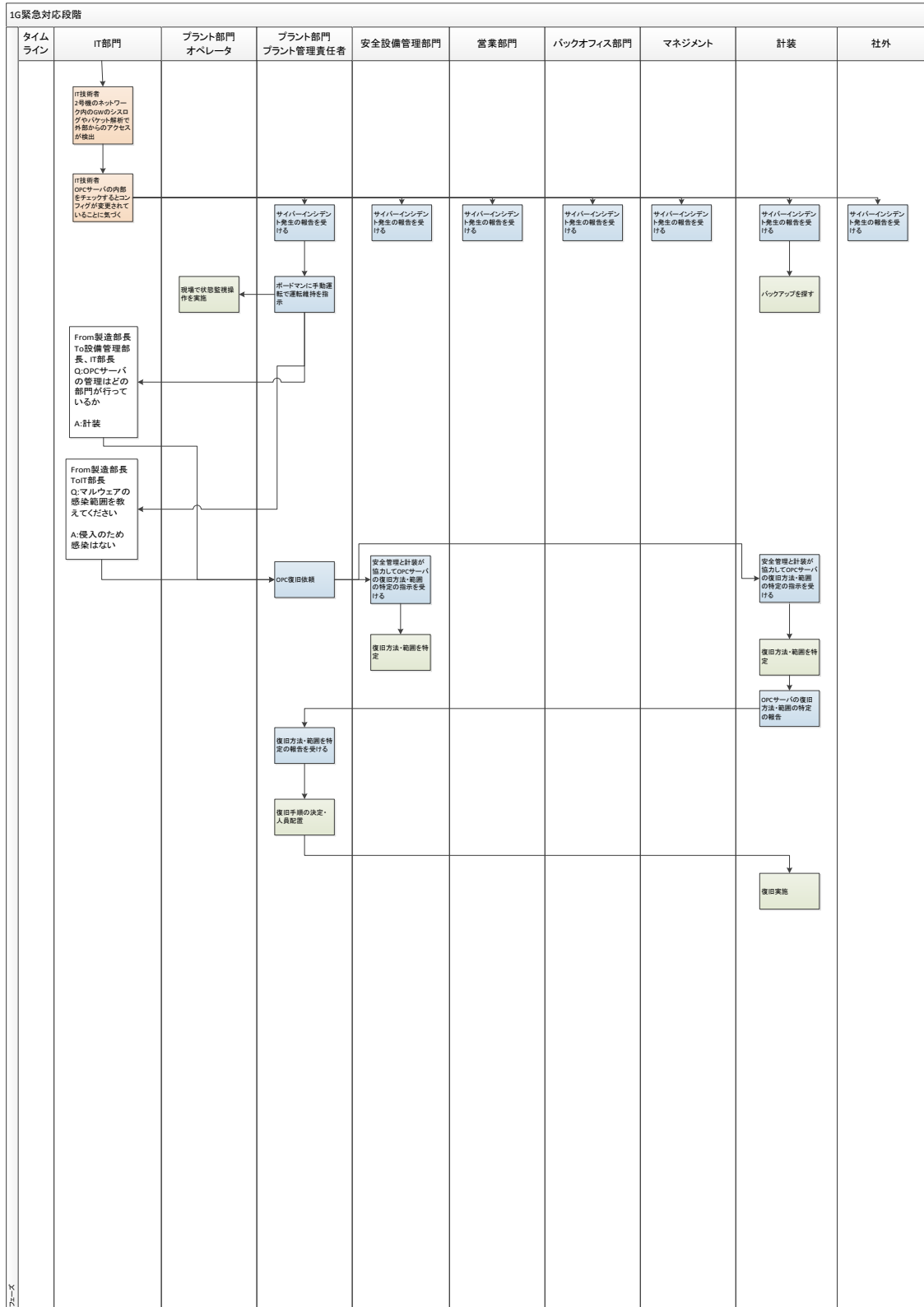


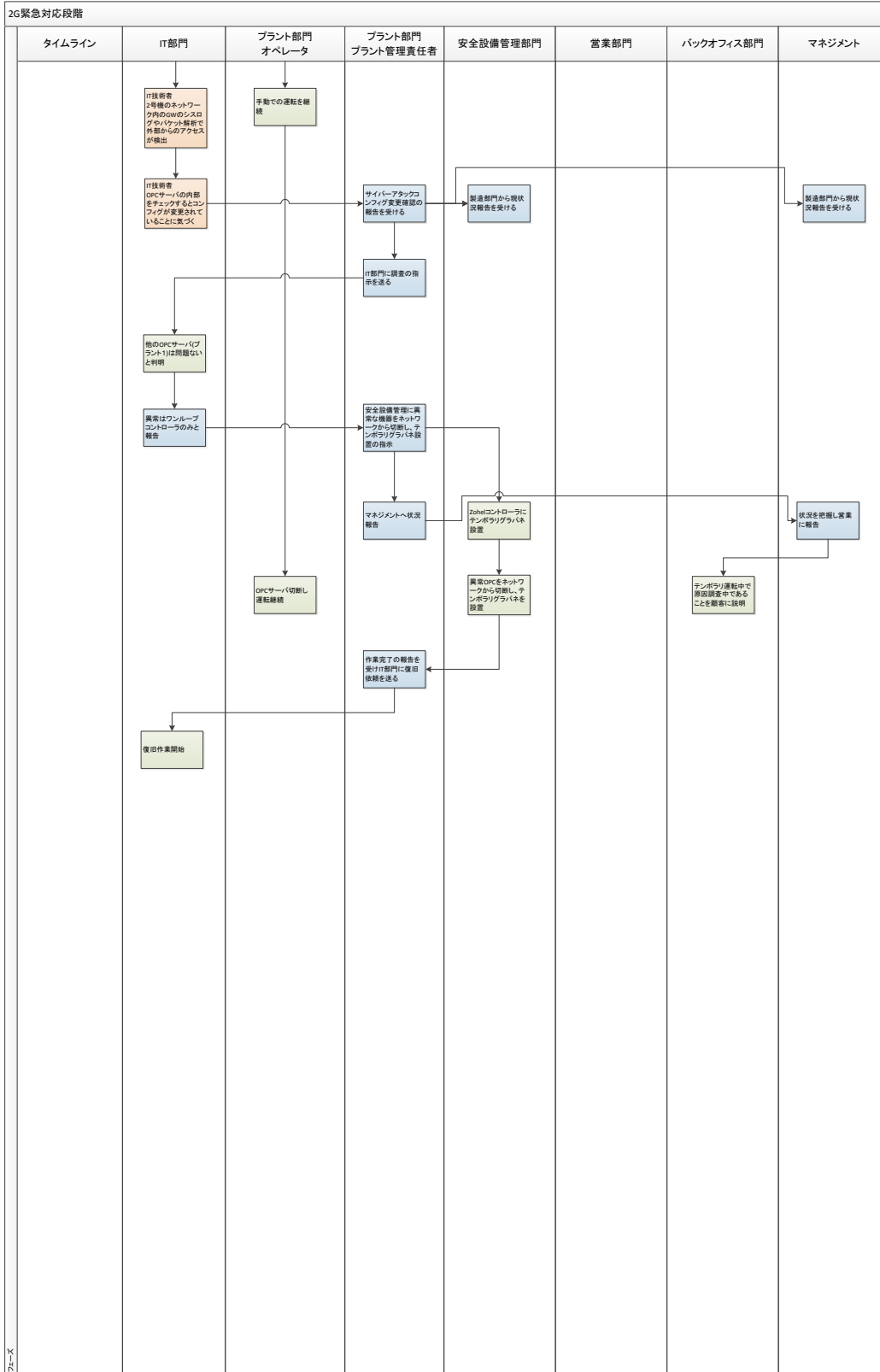
5G予兆段階							
タイムライン	IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	マネジメント
IT機器 不正メール増加 PC-A RATに感染 PC-A RATが稼働活動開始							
NDRWからのイベント 不正アクセスの 検知(SHEM) SCADA L1変化なし L2低下 プラント2(Y市) Q2が低下 プラント1異常なし バルブ全開 ポンプ運転中 不正なアクセスは 192.168.21.x	2号機ネットワーク に不正なアクセス 不正アクセスされて いるエリアを確認 From製造課長 ToIT部門 Q:不正アクセス により想定される 影響の範囲 はどこか A:(未返信)	ボードマンがL2低下 に気づく 現状確認 From製造課長 Toフィールドマン Q:バルブ2は手 動操作で調整で きるか ・L2はX市のプラ ントかY市のプラ ントか A:・できる ・Y市 From製造課長 Toフィールドマン Q:バルブ2の弁 解度と液位 A:タンクは液位が 下がっており、バ ルブ2は全開 From製造課長 Toオペレータ Q:LGの読み、差 異、どんな異常 か ・バルブ1・2の弁 解度 ・ポンプは動作し ているか A:・どちらのLGか 不明のため解答 できない ・バルブ1・2につ いてはSCADA上 では変化なし ・ポンプは動作し ている From製造課長 Toフィールドマン Q:バルブを閉め ることで手動で通 常の液位に戻し た時のその後の 液位 A:安定しました	2号機NWに不正な アクセスあり From製造課長 Toプラント1 Q:異常がない か A:今のところな し	From製造課長 To技術部門 Q:料倉の検知(動 作しているか) A:確かめるための 操作をしてください			
							特徴 ・不正アクセス検知後にIT部門からプラント管理責任者に一 報を送っている ・安全対応はオペレータが独立して行っている ・プラント管理責任者はオペレータ、IT部門と連絡を取り、 インシデントの原因究明を行っている 補足

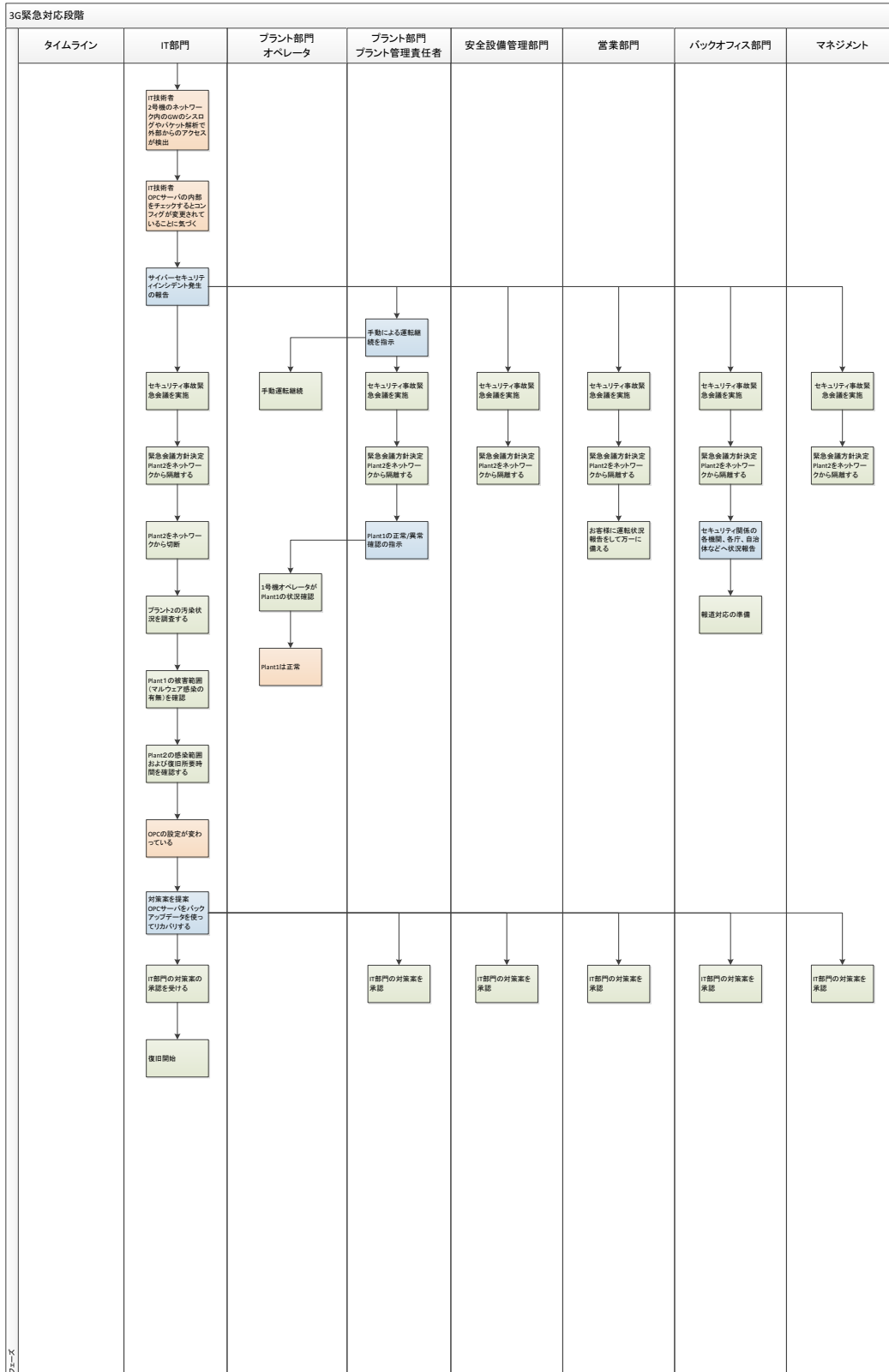


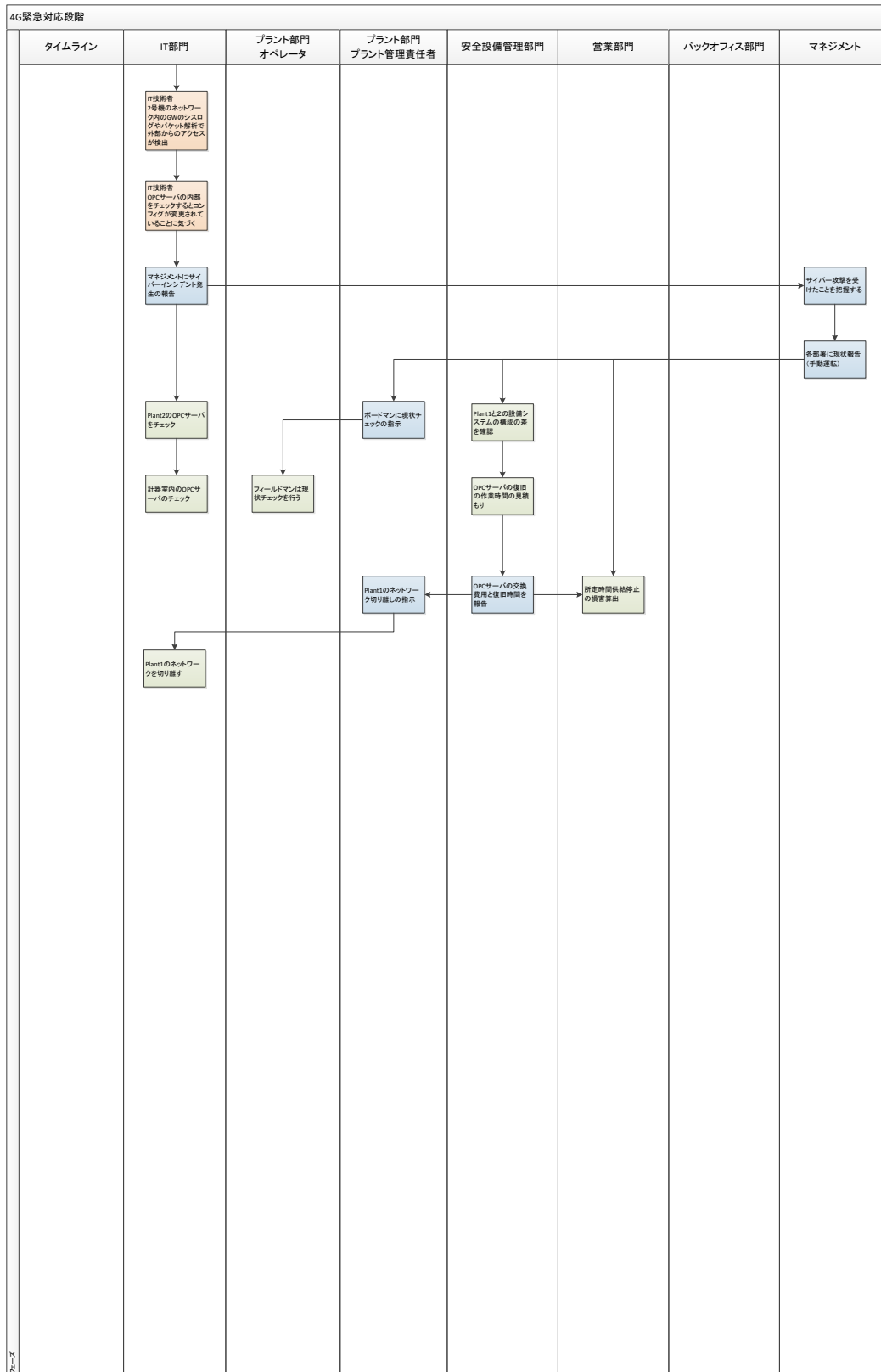


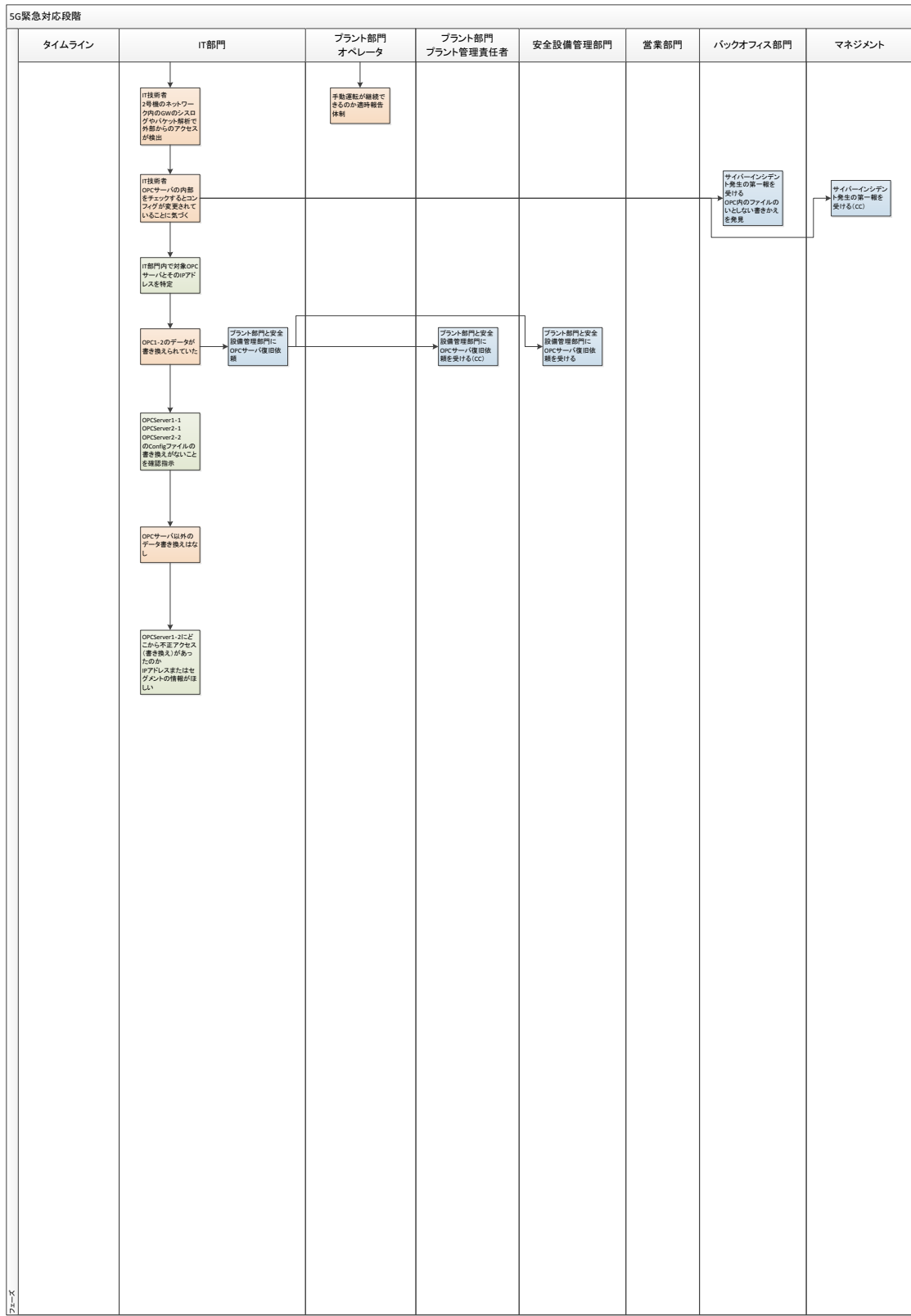


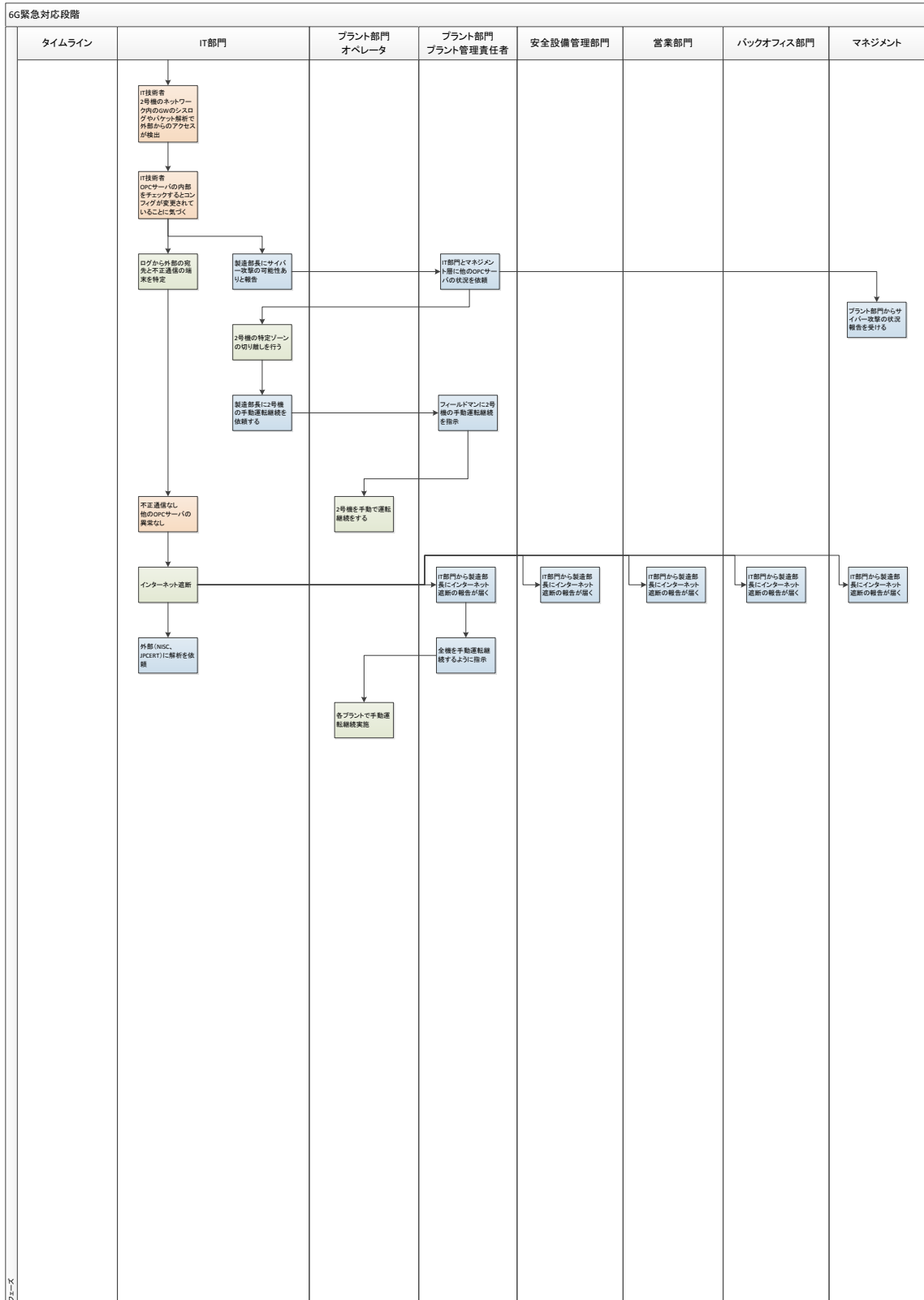


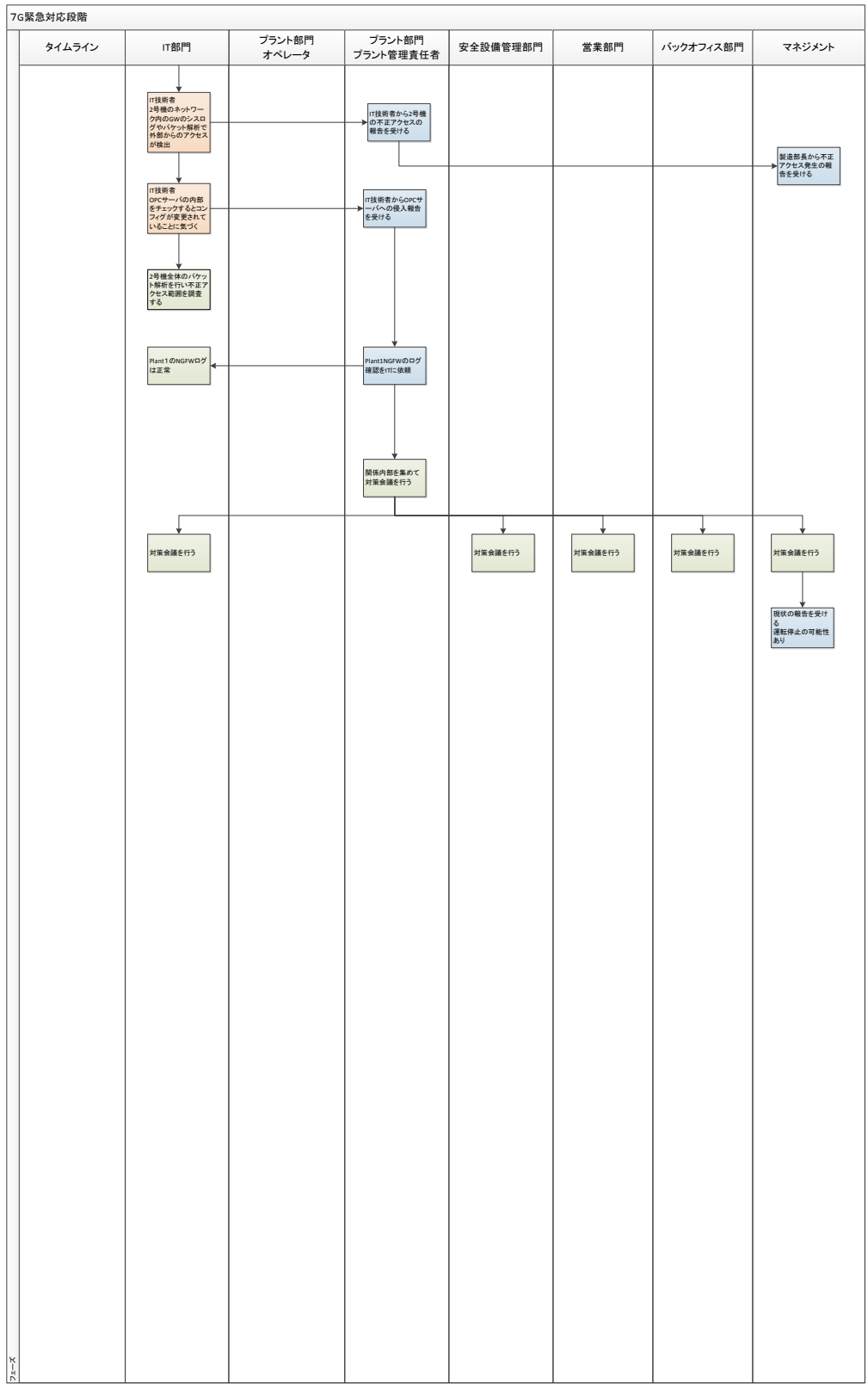


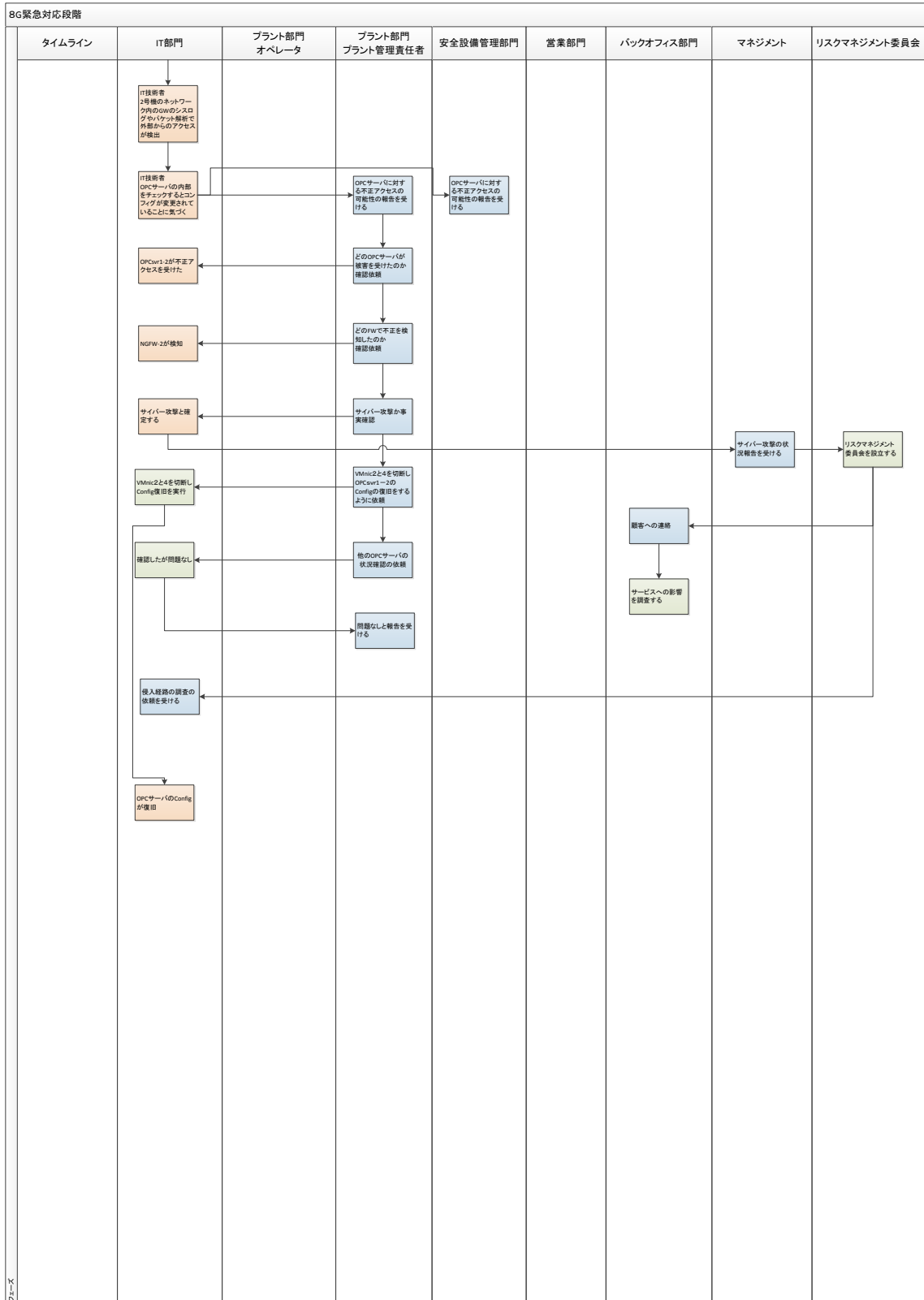


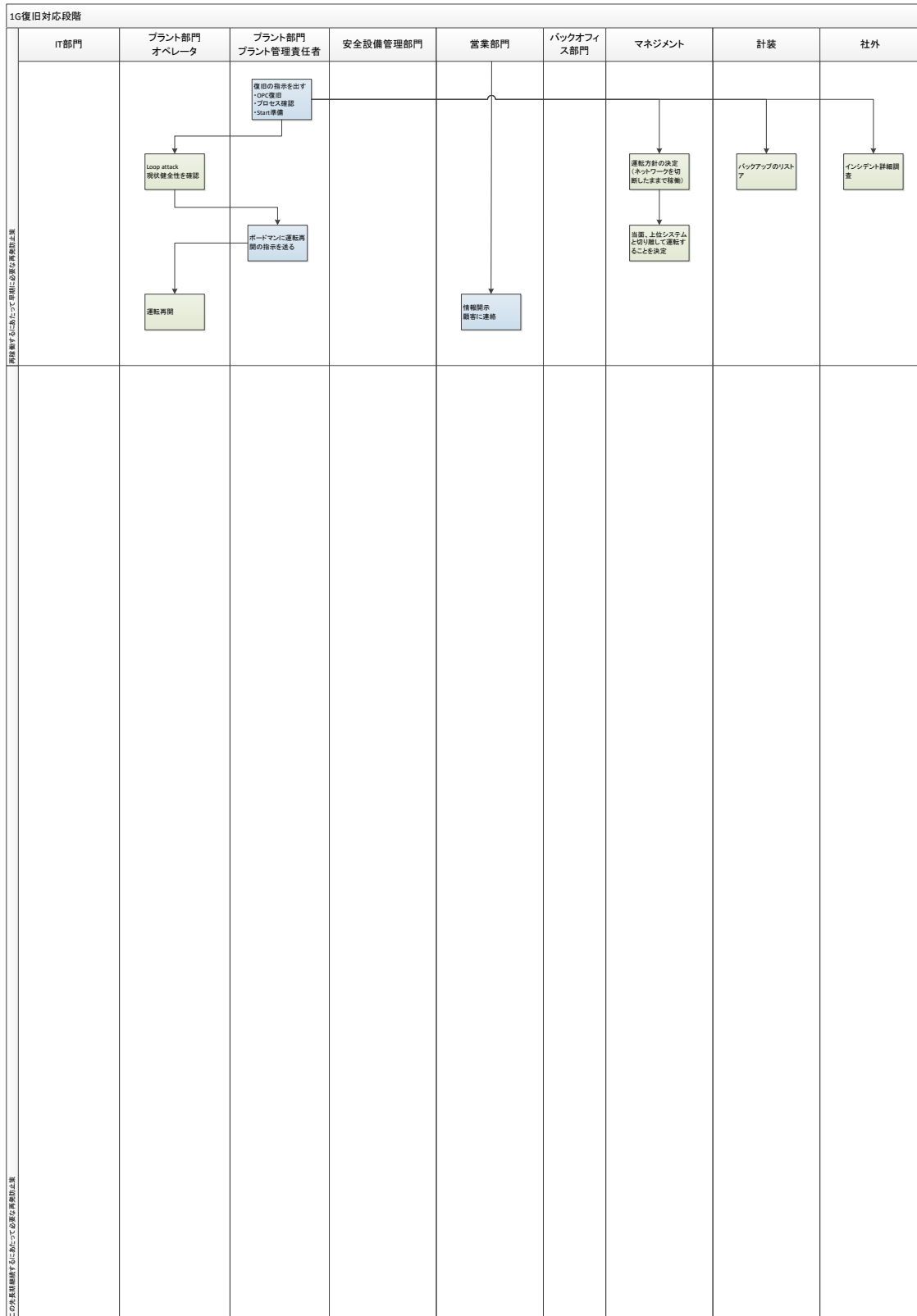








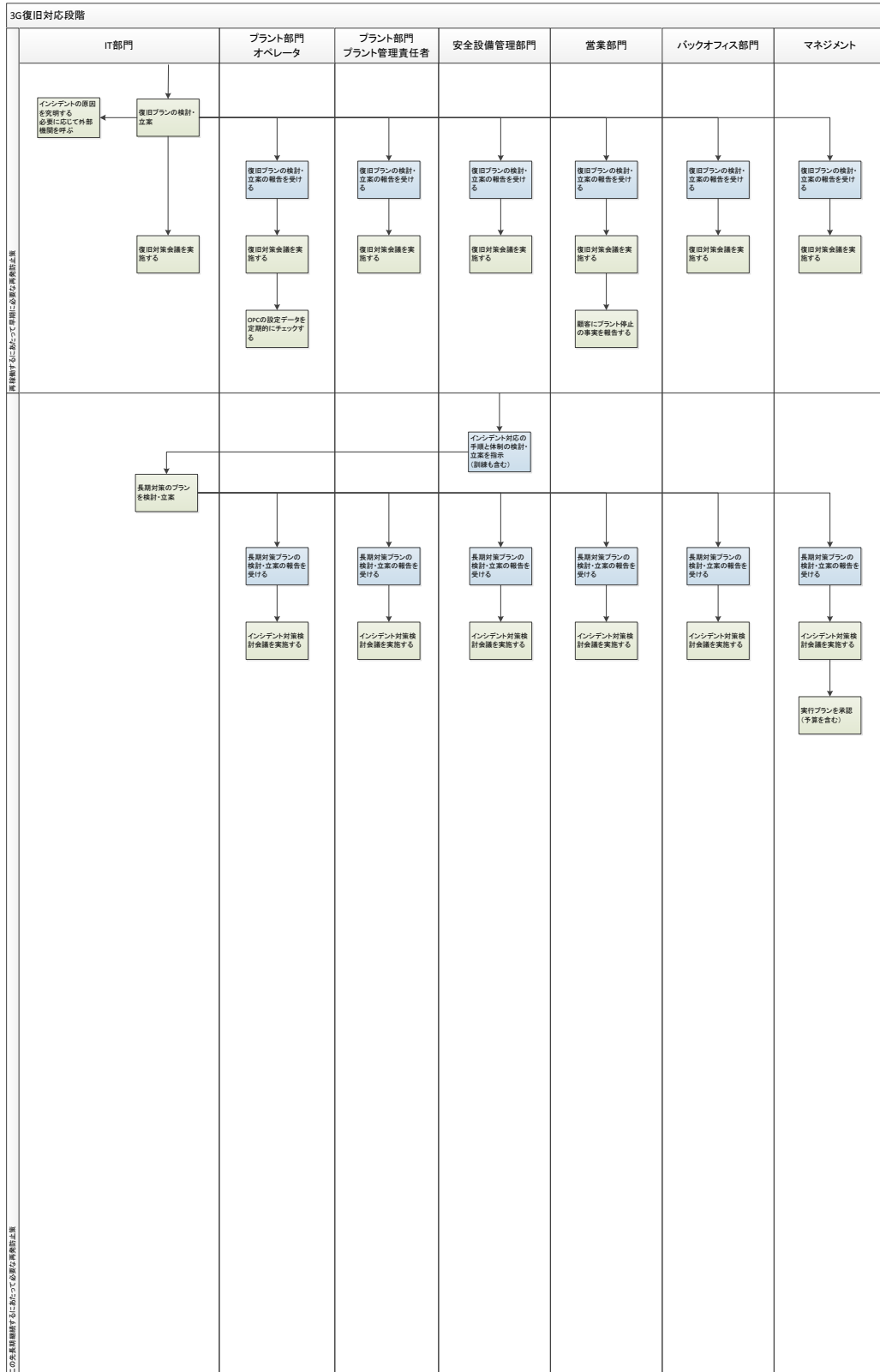




2G復旧対応段階						
IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	マネジメント
<p>opC復旧</p> <p>↓</p> <p>ビジネス系をクリーニング</p> <p>↓</p> <p>投入経路調査</p>		<p>リード</p> <p>↓</p> <p>ローカルで再稼働</p>				
<p>ネットワーク構成再検討</p> <p>↓</p> <p>ビジネス系とCSネットワークとはつながらない</p>			<p>インシデント対応社内体制の構築</p>			<p>CEO再教育</p>

再稼働するに当たって必要な業務の再評価は、

この作業は再稼働するに当たって必要な業務の再評価は、



4G復旧対応段階						
IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	マネジメント
上位ネットワークの 点検 ↓ 原因特定			OPCサーバー・PLC駆 入れ替え			
感応経路の特定		#ant1の再接続 (中期?)				

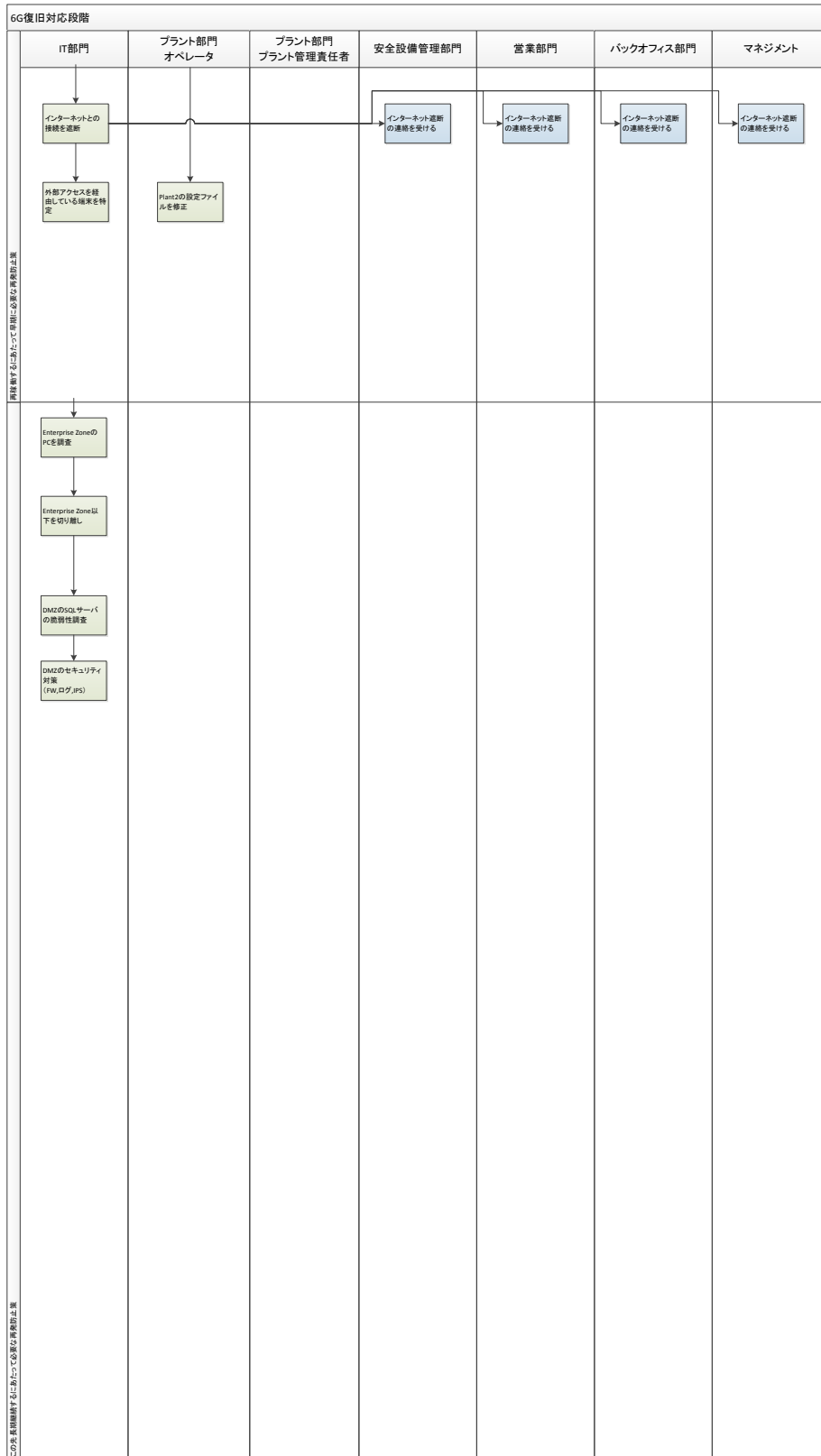
再稼働するに当たっては必要に応じて復旧の優先順位を決定

この作業は再稼働するに当たって必要の優先順位を決定

SG復旧対応段階						
IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	マネジメント
		↓ Plant2の制御システムが健全であることをチェック				
		↓ 各種復旧の条件を 合意する	↓ 外部からの攻撃手 法の調査 ↓ 他の端末が健全で ある証明			

再稼働するに当たって必要な復旧手順

この手順は再稼働するに当たって必要な復旧手順



8G復旧対応段階						
IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	マネジメント
ログ収集 (システムアクセス等) ↓ OA系とPlant2のクリ ーニング	動作確認 (ループチェック等)		インシデントの報告 書作成	客先への説明とお 返り	マスコミへの報告	記者会見
外部コンサルティ ングによる詳細実施 ↓ 詳細結果に基づ く対策計画の立案			インシデント発生時 の対応マニュアル 作成 ↓ セキュリティポリ シーの作成	今後の対応策説明 (再発防止策)		トップダウンによる 各部門への対応策 策

この作業は復旧対応するにあたって必要となる作業の概要を示す

C.2 KIPS+ OPERATION MANUAL

名古屋工業大学

コミュニケーション KIPS
ファシリテーターマニュアル

1. 演習概要

- コミュニケーション KIPS とは
KIPS(Kaspersky Interactive Protection Simulation)は重要インフラに対するサイバー攻撃の影響をゲーム形式で体験し、その対応策を学ぶ対サイバー攻撃演習である。コミュニケーション KIPS はサイバーインシデント状況下で、**社内における組織間の情報交換の重要性を体験するために**、従来の KIPS にチャットシステムを導入した改良型ゲームである。
- ゲーム内容
参加者は一つのチーム内で**本社グループ**と**現場グループ**に分かれ、**5ターン**に亘って制御システムのセキュリティ対策が記述されたカードを選択する。

2. 目標

- 本社グループ
企業の総収益をできる限り増やすこと。
Ex. 浄水場版：ゲームシステム内の最大総収益である 100 万ドルに近づけること。
- 現場グループ
プラントの安全を確保すること。
Ex. 浄水場版：サイバー攻撃によるプラントの影響を最小限にする。

3. 責任範囲

ファシリテーターは一人で一チーム分のゲーム操作を担当する。

4. 演習の準備

- 必要な物(1 チーム分)
 - ファシリテーター用 PC 1 台
ファシリテーターが担当チームのゲームを操作するために使う端末である。ファシリテーター用 PC には**ゲーム操作用コンソール**を開くためのブラウザ(推奨環境は Chrome)と、各グループに情報を送信するための**チャットシステム**、Slack をインストールしておく。
現場グループと本社グループにそれぞれ提供する情報を振り分けるために、ファシリテーター用 PC に**メッセージ(アクション結果)振り分けファイル**を入れておく。
 - 参加者用 PC 2 台
参加者がチャットを行うために使う端末である。本社グループと現場グループにそれぞれ 1 台ずつ用意する。**参加者用 PC**には、ファシリテーターから情報を受け取る、またはグループ間の情報交換を行うために Slack をインストールしてお

- く。
- アクションカード 1セット
参加者がゲーム内で利用する行動が記述されたカードである。アクションカードは**カード振り分けリスト**(7章参照)に基づいて現場グループと本社グループに分配される。
- ゲームボード 2枚
参加者がアクションカードを置くためのボードである。A0用紙に印刷しておく。
- 準備すること
 - 配置
運営者は現場グループと本社グループとの会話が聞き取れない程度の距離を空けて机を配置する。そして、**ファシリテーター**は参加者用PCとゲームボードを配置し、アクションカードを各グループの**カード担当者**に配分する。**ファシリテーター**は、**リーダー**を参加者用PCが操作できる場所に配置する。
 - チャットシステムへのログイン
ファシリテーターの指示で、**リーダー**はチャットシステムにログインする。(ログインするアカウントについては別紙参照)次に、本社グループ参加者用PCー現場グループ参加者用PC間、そして参加者用PCー**ファシリテーター**用PC間でチャットできることを確認する。
 - 操作用コンソールの立ち上げ
ファシリテーターはアクションカードを入力するための操作用コンソールを起動する。
- 5. 演習の進め方
 - 開始
初めに**ゲーム進行者**は前提条件、ルールを説明する。そして、**ゲーム進行者**の合図で**システム担当者**はアクションフェーズの開始ボタンをクリックする。
 - **メッセージフェーズ&アクションフェーズ**
アクションフェーズが開始されると、**アシスタントコンソール**の中央上部にターン1のメッセージが表示される。このメッセージをコピーし、担当チームの**本社グループの参加者用PC**に**slack**で(チャンネルはteam〈チーム番号〉_1ch)ペーストし、送信する。

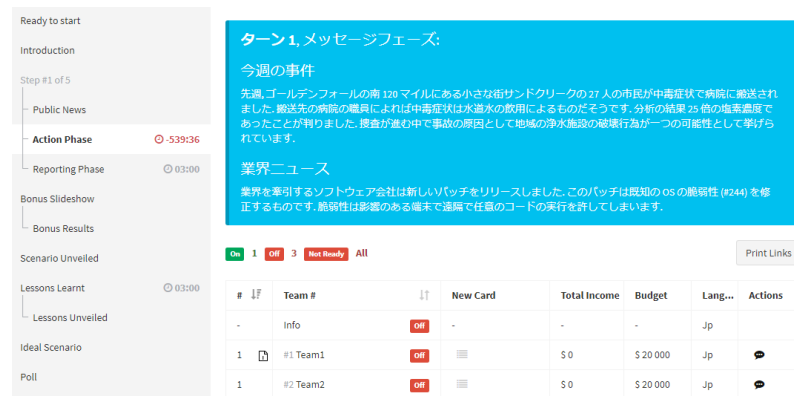


図 1 アシスタントコンソール

参加者がアクションカードを決定すると、担当チームの各グループから**アクションカード番号**が送られてくる。ファシリテーターは該当するアクションカードを**操作用コンソール**から選択し、画面右下の「送信」をクリックする。(カード選択の順番を守る)

ゲーム進行者は、**システム管理者**からの報告を受けて、アクションフェーズ終了 1 分前に全チームに残り時間をアナウンスする。

システム管理者は、**管理者コンソール**から全チームが「Ready」状態になったのを確認し、「Stop Action Phase」をクリックし、**ゲーム進行者**に報告する。そして、**ゲーム進行者**はアクションフェーズ終了をアナウンスする。



図 2 操作用コンソール

● レポートフェーズ

システム管理者はアクションフェーズ終了後、「Start Report Phase」をクリックする。ファシリテーターは、アシスタントコンソール右側にある Actions から担当チームの吹き出しマークをクリックする。担当チームのメッセージリストが表示されるので、結果を選択し、コピーする。

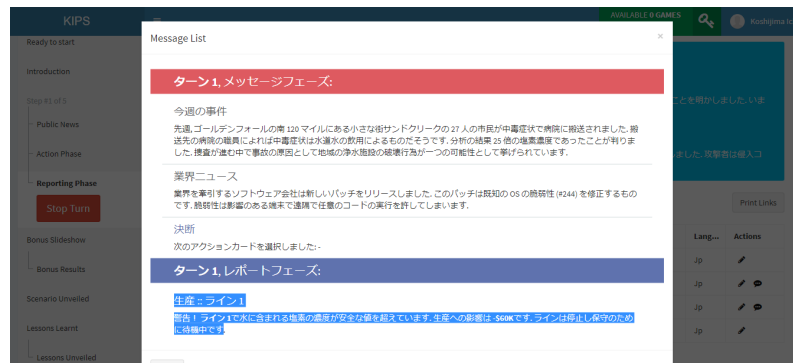


図 3 メッセージリスト

コピーしたメッセージをメッセージ(アクション結果)振り分けファイルの検索フィルタにペーストし、フィルタ検索することでメッセージはどちらのグループに送信すべきかが判明する。送信すべきグループが判明したら、該当するグループへ送信する。

カード配分者はアシスタントコンソールの New Card 項目から各チームに配るべきカードを確認する。該当するチームの**カード担当者**を呼び出し、追加のカードを渡す。すべて渡し終えたら、システム管理者に報告する。

システム管理者は管理者コンソールの New Card 項目から該当チームの Give card(矢印アイコン)をクリックする。

ゲーム進行者はインフォメーションコンソールをスクリーンに表示し、現時点での全チームの総収益を紹介する。5 ターン目のアクションフェーズ終了後、**ゲーム進行者**は5 ターンの総収益を紹介した後、ボーナスを加えた最終的な総収益を紹介する。

ゲーム進行者は**運営者**の作業化完了したことを確認した後、次のターンへ進める。

運営者は5 ターンを本章の手順で本演習を進行させる。

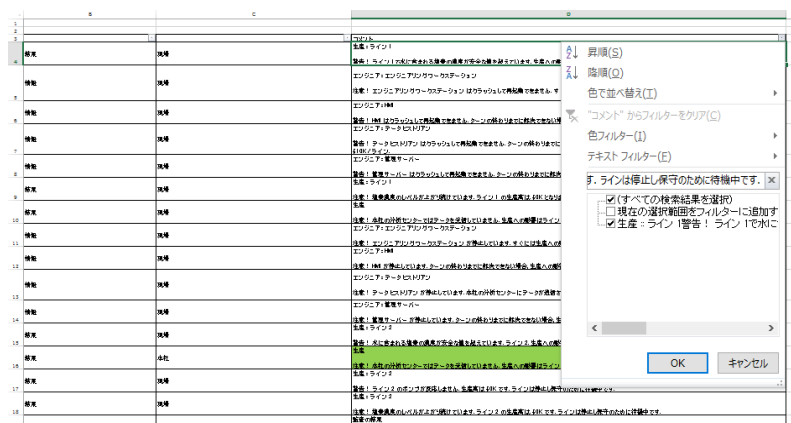


図 4 メッセージ (アクション結果) 振り分け画面

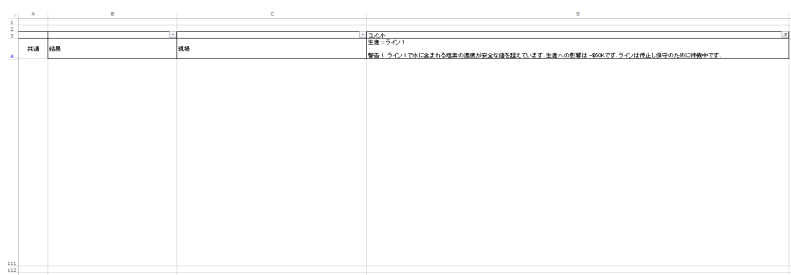


図 5 フィルタ検索結果

6. フェーズのサイクル

本演習では、**システム管理者**はフェーズの時間を以下のように設定する。

表 1 各フェーズの時間

ターン	時間(分)	
	メッセージ& アクションフェーズ	レポートフェーズ
1	10	6
2	7	6
3	5	6
4	4	6
5	3	—

7. 参考

● 演習関係者

- 参加者
コミュニケーション KIPS 演習を受講する人。
- 運営者
コミュニケーション KIPS 演習の準備に関わる全ての人。(ゲーム進行者、システム管理者、カード配分者、ファシリテーター等)
- ゲーム進行者
コミュニケーション KIPS の司会進行を行う人。ゲームのルール説明や、システム管理者からの情報からゲームの進行を行う。
- システム管理者
ゲームの進行を管理者コンソールから操作する人。管理者コンソールから各チームの状況を把握できる。
- カード配分者
ゲーム中に配るカードを管理する人。レポートフェーズ時にアシスタントコンソールからチームに配るカードを確認し、各チーム、各グループのカード担当者に、該当したカードを渡す。
- ファシリテーター
チームを管理する人。主にアクションカードの入力、担当チームの各グループへの情報送信、タイムキーパーを行う。
- リーダー
グループの最終的な意思決定者。チャットを行う。
- カード担当者
ゲーム中カードの管理を行う人。カード配分者から呼ばれた場合、追加のカードを取りに来る。

- コンソールの種類
 - 管理者コンソール

ゲームの進行を行うことができるコンソール。各チームの状態およびメッセージや結果を確認できる。システム管理者が扱う。
 - アシスタントコンソール

管理者コンソールと同等の情報が得られるコンソール。ゲームの進行はできないが、各チームの状態およびメッセージや結果を確認できる。ファシリテーターとカード配分者が扱う。
 - インフォメーションコンソール

全チームの総収益が表示されているコンソール。総収益は毎ターン更新される。ゲーム進行者が扱う。
 - 操作用コンソール

チームのアクションを入力するコンソール。ファシリテーターが扱う。
- チャットシステム(Slack)の操作
 - ログイン
 1. 別紙参照
 - ログアウト
 1. 管理画面上部にある「nitech_workshop」横のvマークをクリック
 2. 「Sign out of nitech_workshop」をクリック
 - メッセージの送信

メッセージ入力画面に文章を作成し、Enter を入力
 - メッセージの改行

メッセージ内の改行したい個所で Ctrl+Enter を入力
 - メッセージの削除
 1. 削除したいメッセージを選択
 2. メッセージ右側に表示される「・・・」をクリック
 3. 「Delete message」をクリック
 - チャンネルの切り替え

管理画面からチャンネルをクリック
 - チャンネルの種類

1ch : 本社グループアカウントとファシリテーターアカウントとの連絡用
 2ch : 現場グループアカウントとファシリテーターアカウントとの連絡用
 3ch : 本社グループアカウントと現場グループアカウントとの連絡用



図 6 Slack コンソール

- Slack アカウントごと役割



表 2 名工大用 Slack アカウント

アカウント名	チーム番号	役割
ws01	team1	本社
ws02	team1	現場
ws03	team2	本社
ws04	team2	現場
ws05	team3	本社
ws06	team3	現場
ws07	team4	本社
ws08	team4	現場
ws09	team5	本社
ws10	team5	現場
ws11	team6	本社
ws12	team6	現場
ws13	team1	ファシリテーター
ws14	team2	ファシリテーター
ws15	team3	ファシリテーター
ws16	team4	ファシリテーター
ws17	team5	ファシリテーター
ws18	team6	ファシリテーター
ws19	team7	本社
ws20	team7	現場
ws21	team7	ファシリテーター

- カード振り分けリスト(浄水場版)
以下の表はアクションカードごとに配分するグループを定義したものである。
○は演習開始前に該当するグループに配分するカードである。
☆はゲーム中にカード配分者が該当するグループに配分するカードである。

表 3 浄水場版カード振り分けリスト

カード番号	カード名	振り分け	
		本社	現場
1	インターネットからの切断	○	
2	パスワードの変更		○
3	サイバーセキュリティのトレーニング	○	
4	機器の監査		○
5	ファイアウォールのインストール	○	
6	SIEMのインストール	○	
7	ファイアウォールのログ分析	○	
8	パッチと脆弱性のチェック	○	
9	OSのネットワーク脆弱性にパッチを適用	○	
10	ネットワークセグメント分割の実行	○	
11	侵入テストの実施	○	
12	管理サーバにアンチウイルスをインストール		○
13	エンジニアリングワークステーションにアンチウイルスをインストール		○
14	HMIにアンチウイルスをインストール		○
15	データヒストリアンにアンチウイルスをインストール		○
16	PLC完全性モニタをインストール		○
17	PLCの完全性のチェックと修正		○
18	PLCの交換(ライン1)		○
19	PLCの交換(ライン2)		○
20	バックアップ復元サーバの導入		○
21	バックアップからノードを復元		○
22	ノードを初期状態から復元		○
23	ライン1を初期状態から復元		○
24	ライン2を初期状態から復元		○
25	OSのUSB脆弱性にパッチを適用	☆	
26	エンジニアリングラップトップにアンチウイルスをインストール		☆
27	ADSLモデムの取り外し		☆
28	ファイアウォールのパッチをインストール	☆	
29	PLCの認証情報のパッチをインストール		☆
30	PDFリーダーのパッチをインストール	☆	
	カード枚数	12	18
	合計		30

C.3 TSURUMAIGO OPERATION MANUAL



Tsurumai GO!!の操作説明

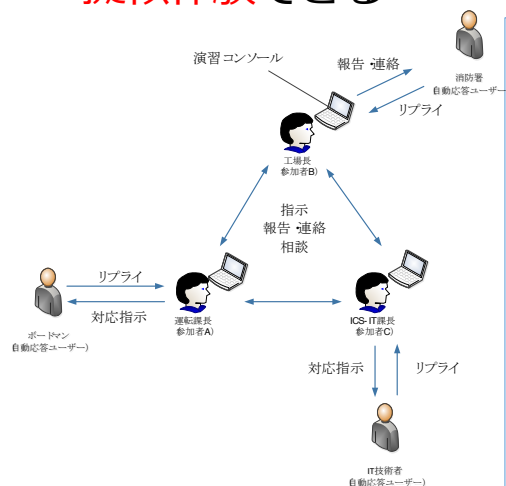
- 場所 文京グリーンコート
- 講師 国立大学法人 名古屋工業大学
橋本 芳宏
- 日時 令和元年10月30日

本日の目的



- シミュレーションを通じて、
「実行する」という観点を持って頂き、
これまでの議論を更に深めて頂くこと

参加者は**現実の役職**としてゲームに参加でき、**組織間連携**をゲーム内で**擬似体験**できる



- ゲーム内には、様々なロールを担う複数の**参加者**と、複数の**自動応答ユーザー**が存在
- 参加者は演習コンソールを用いて、他の参加者や自動応答ユーザーと様々な**コミュニケーション**を行うことでゲームを進行する
- ゲームの**ストーリー展開**は、参加者のコミュニケーション内容に応じて決まる

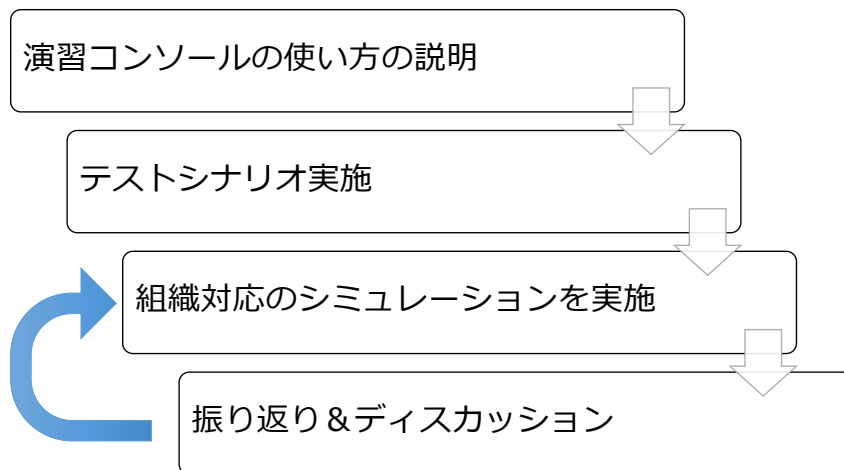
TsurumaiGO!!とは？



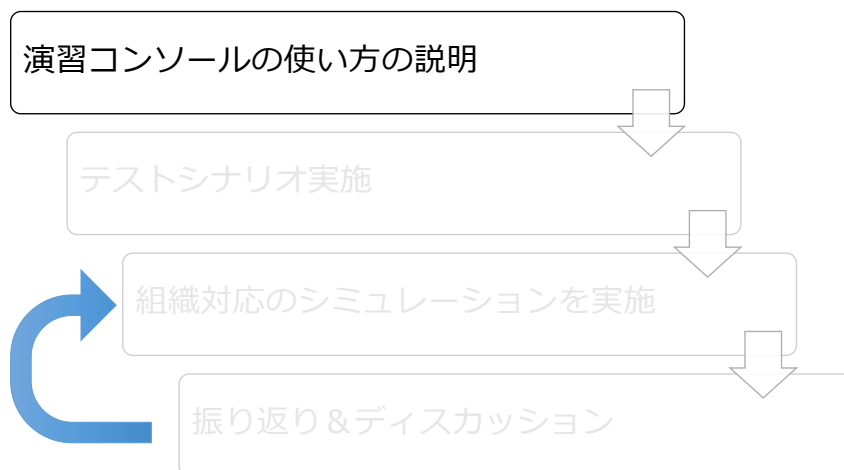
TsurumaiGO!!の二つの位置づけ

1. コンピュータゲーム形式のサイバーインシデント対応シミュレーション
 1. 参加者は**現実の役職**として演習に参加でき、**組織間連携**を**擬似体験**できる
 2. 結果(=対応フロー)はワークシートとして出力でき、演習の実施後**直ぐに評価**できる
2. 各社におけるサイバーインシデント対応演習の構築運用の支援システム
 1. ゲームは**簡単に構築・カスタマイズ**出来る
 2. 成果(ゲームデータ)を業界内で共有することで、**自社の演習構築に役立てることが出来る**
(**業界全体のセキュリティ向上**が期待できる)

演習の流れ



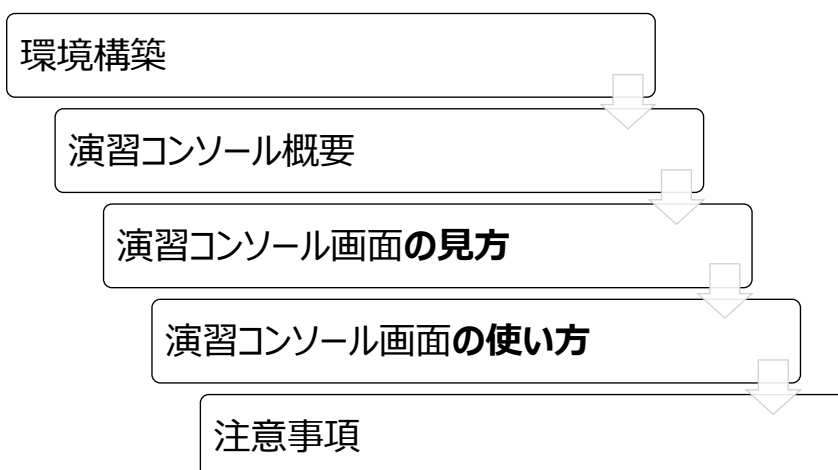
演習の流れ



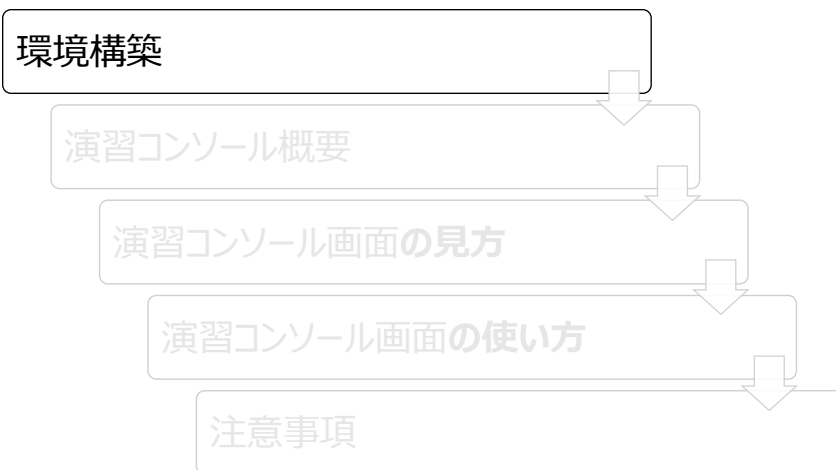


演習コンソールの使い方

説明の流れ



説明の流れ



環境構築 1/2



1. 有線LANをハブと接続
2. PCの有線LANアドレスを
192.168.1."2以上の数字"
として固定
(*アドレスが班内で競合しないようご
注意下さい)

環境構築 2/2



3. Google Chromeをシークレットモードで開く
4. 下記URLへアクセス
<http://192.168.1.1:8080/workshop/>
5. 下の画面が表示されることを確認

[演習参加者はこちらから](#)
[管理者/オブザーバはこちらから](#)

ログイン 1/3



1. 「演習参加者はこちらから」をクリック

[演習参加者はこちらから](#)
[管理者/オブザーバはこちらから](#)

2. 下の画面が表示されることを確認



ログイン 2/3



3. ユーザーを選択し、ログイン

(*ゲーム開始前に改めて役割決めを行うため、班内で競合しないよう仮決めして下さい。)

ません。 ユーザID: Company

ログイン 3/3



4. 下の画面の下線箇所を確認し、自身の役割が表示されていることを確認

製造課長(製造課長@sample.com) ユーザID: Company

イベント

日時	From	To/Cc	アクション	インテ
----	------	-------	-------	-----

説明の流れ



演習コンソールでできること



関係者とのコミュニケーション

①各ロール固有のアクション

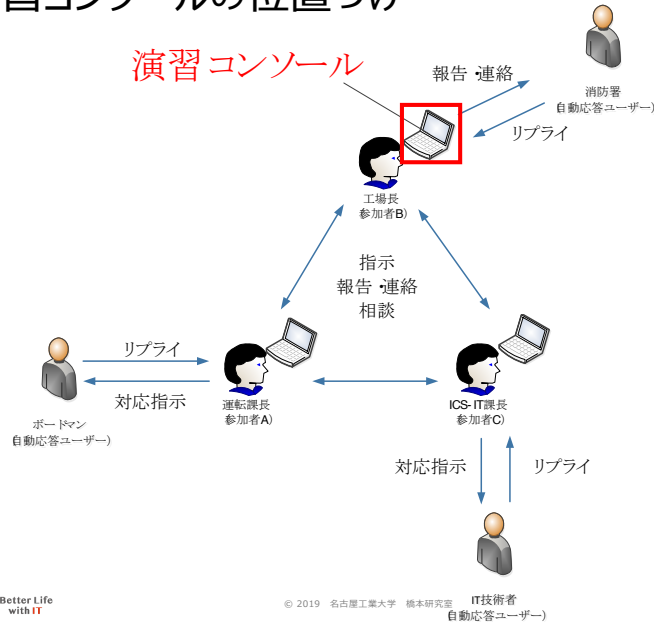
- ✓ 部下や上司、他部署に対して、対応の指示を行うこと
- ✓ 部下や上司、他部署へ報告・連絡を行うこと, etc..
- ✓ ゲームのストーリー展開に**影響あり**

②相談

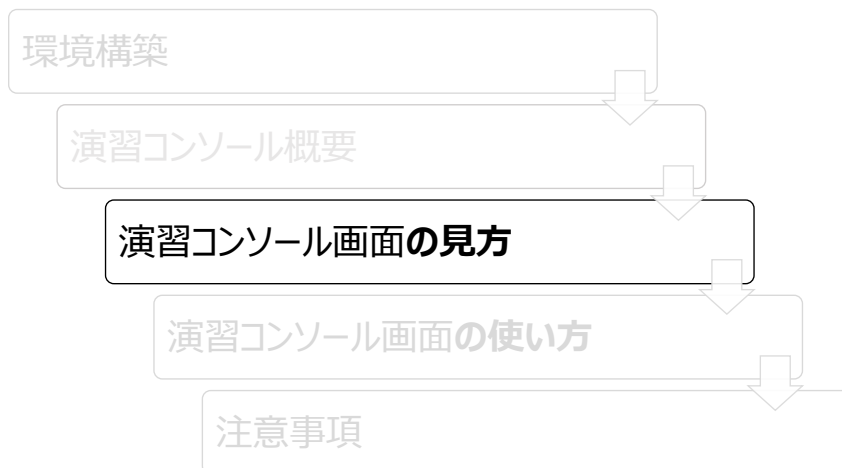
- ✓ 対応者間で状況認識や意思決定の在り方に関する相談を行うこと
- ✓ ゲームのストーリー展開に**影響なし**

以降は、上記の2点をまとめて「アクション」と呼びます。

演習コンソールの位置づけ



演習の構成



演習コンソールの基本画面



製造課長(製造課長@sample.com) ユーザID: 製造課長 Company ログイン ログアウト

ヘルプ: システム構成 組織と連絡ルート 役割とアクション

イベント sample.com: シナリオ(既定) フェーズ1 (状態Started) 開始06/08 11:09:23 制限時間20:00 経過04:45 残り15:14 スコア0 Q取り込み

ID	日時	From	To/Cc	アクション	インシデント情報	メッセージ
1	06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
1	06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少しています。
1	06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での運転可能性を知らせる		手動操作によって、圧力を戻すことができるか?
1	06/08 11:11:10	プラント運転員	製造課長	手動での運転が可能であることを報告	手動での運転操作可能	手動操作で圧力を戻すことが可能です。
1	06/08 11:11:38	IT課長	製造課長	報告・連絡	Qw2で不要な通信検出	
1	06/08 11:11:58	製造課長	プラント運転員	プラント運転員に外部通信する作業があったことを報告		いつもと異なる外部と通信する作業があったか?
1	06/08 11:12:05	プラント運転員	製造課長	異常なことを報告	製造課では外部と繋がる作業はしていません	特にありません。
1	06/08 11:12:18	製造課長	プラント運転員	プラント運転員に手動での運転継続指示		手動操作で運転継続を行ってください。
1	06/08 11:12:25	プラント運転員	製造課長	手動での運転継続完了	手動操作による運転継続開始	承知しました。手動操作で運転継続を行います。
1	06/08 11:12:44	製造課長	IT課長	IT課へプラント通信調整依頼		プラント通信の調整を行ってください。

イベントトレイ

イベントの種類



- ① システム通知(システムからの通知)
EX. 演習開始、演習終了
- ② 送信アクション(自身から他へのアクション)
EX. 部下への指示、他部署への報告・連絡
- ③ 受信アクション(他から自身に対するアクション)
EX. 同僚からの指示、他部署からの報告・連絡

ID	日時	From	To/Cc	アクション	インシデント情報	メッセージ
1	06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
1	06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少しています。
1	06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での運転可能性を知らせる		手動操作によって、圧力を戻すことができるか?
1	06/08 11:11:10	プラント運転員	製造課長	手動での運転が可能であることを報告	手動での運転操作可能	手動操作で圧力を戻すことが可能です。
1	06/08 11:11:38	IT課長	製造課長	報告・連絡	Qw2で不要な通信検出	
1	06/08 11:11:58	製造課長	プラント運転員	プラント運転員に外部通信する作業があったことを報告		いつもと異なる外部と通信する作業があったか?
1	06/08 11:12:05	プラント運転員	製造課長	異常なことを報告	製造課では外部と繋がる作業はしていません	特にありません。

イベントの見方 (1/7)



イベントの構成要素(画面の左から順に)

- ①送受信 ②日時 ③From ④To;CC ⑤アクション
⑥インシデント情報 ⑦メッセージ

①	②	③	④	⑤	⑥	⑦
送受信	日時	From	To;CC	アクション	インシデント情報	メッセージ
↓	06:08 11:09:25	システム	チーム全員	通知	異常開始	異常を開始します。
↓	06:08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少

①送受信

↓

送受信	日時	From	To;CC	アクション	インシデント情報	メッセージ
↓	06:08 11:09:25	システム	チーム全員	通知	異常開始	異常を開始します。
↓	06:08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少



受信



送信

イベントの見方 (2/7)



②日時

アクションを受信した日時、もしくはアクションを送信した日時

③From

アクションの送信者(自身が実施したアクションであれば、自身が表示される)

④To;CC

To:アクションの宛先(自身が受けたアクションであれば自身が表示される)
CC:アクションの知らせ先

② ↓ ③ ↓ ④ ↓

送受信	日時	From	To;CC	アクション	インシデント情報	メッセージ
↓	06:08 11:09:25	システム	チーム全員	通知	異常開始	異常を開始します。
↓	06:08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少

イベントの見方 (3/7)



⑤アクション:

- 固有のアクションの場合: コミュニケーションの内容
- 相談、通知の場合: コミュニケーションの識別子

↓

日時	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:09:39	ネット監視担当	IT課長	通信異常検知	Gw2で不審な通信検出	Gw2で通常でないIP133.68.1
06/08 11:11:38	IT課長	製造課長	報告・連絡	Gw2で不審な通信検出	
06/08 11:12:44	製造課長	IT課長	IT課へプラント通信隔離依頼		プラント通信の隔離を行って

イベントの見方 (4/7)



⑥インシデント情報

- イベントに付随する情報
 - 指示情報
 - プラント停止指示 等
 - 報告情報
 - プラントの運転状況 等

↓

日時	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:09:39	ネット監視担当	IT課長	通信異常検知	Gw2で不審な通信検出	Gw2で通常でないIP133.68.1
06/08 11:11:38	IT課長	製造課長	報告・連絡	Gw2で不審な通信検出	
06/08 11:12:44	製造課長	IT課長	IT課へプラント通信隔離依頼		プラント通信の隔離を行って

イベントの見方 (5/7)



⑦メッセージ

- コメント
- (返信/転送されたイベントの場合、) 返信元

↓

To/Cc	アクション	インシデント情報	メッセージ
チーム全員	通知	演習開始	演習を開始します。
IT課長	通信異常検知	Gw2で不審な通信検出	Gw2で通常でないIP133.68.111.20からIP192.168.111.10への通信を検知しまし
製造課長	報告・連絡	Gw2で不審な通信検出	
IT課長	IT課へプラント通信隔離依頼		プラント通信の隔離を行ってください。

イベントの見方 (6/7)



- 任意のイベント上で、**ダブルクリック**すると、Boxが開き、イベント内容を見ることが出来る

イベント

発生日時 2018/6/8 11:11:10

アクション **手動での復旧が可能であることを報告**

From プラント-運転員<プラント-運転員@sample.com>

To 製造課長<製造課長@sample.com>

Cc

インシデント情報 **手動での復旧操作可能**

メッセージ 手動操作で流量を戻すことが可能です。

閉じる

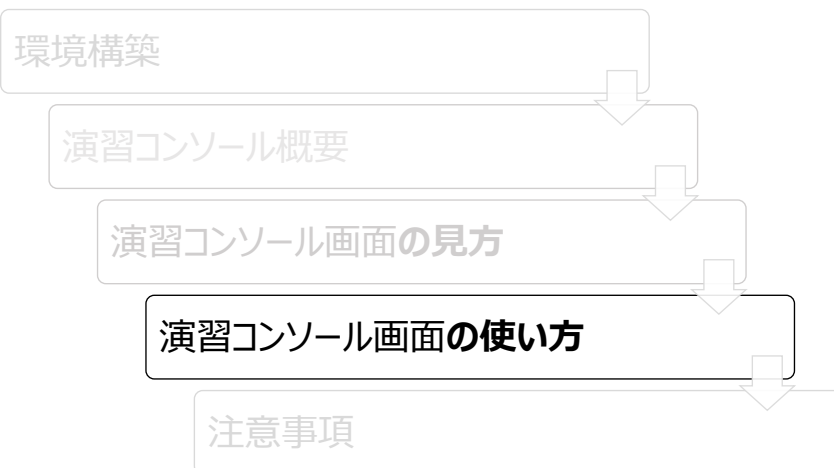
イベントの見方 (7/7)



- ・ 閲覧したいイベント上で、①**右クリック**し、②**表示**をクリックすると、Boxが開き、イベント内容を見ることが出来る

The screenshot displays the 'イベント' (Event) management interface. The table lists several events, with the third event selected. A context menu is open over this event, showing options like '表示' (Show), '返信/転送' (Reply/Forward), and 'マーク設定/解除' (Mark Setting/Unmark). The '表示' option is highlighted, and a detailed view window is open, showing the event's details, including the incident name, time, and a message.

説明の流れ



新規アクションの作成方法



- ・ イベントトレイの上にある「新規アクション」をクリック

製造課長(製造課長@sample.com) ユーザID: 製造課長 Company ログイン

新規アクション 返信/回答 一覧更新

イベント sample.com: シナリオ[既定] フェーズ1 (状態:Started) 開始:0

日時	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減少
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問...		手動操作によって、流量を...
06/08 11:11:10	プラント運転員	製造課長	手動での復旧が可能であることを報告	手動での復旧操作可能	手動操作で流量を戻すこと...

新規アクションの作成方法



- ・ 下のようなBoxが開く

アクション

アクション

To

Cc

返信元

インシデント情報

メッセージ

実行 キャンセル

Box作成手順



- ① アクションの選択
- ② Toの選択
- ③ CCの選択
- ④ 返信元の選択
- ⑤ インシデント情報の選択
- ⑥ メッセージの入力
- ⑦ 「実行」をクリック
- ⑧ その他

①アクションの選択(必須)



選択できるアクションは状況に応じて、どんどん増えます

- 3種類のアクションから一つ選択
 - 「(指示・報告連絡に関する)各ロール固有のコミュニケーション」
 - 「相談」

アクション一覧にある「報告連絡」は使用禁止！！

② Toの選択(必須)



アクションの宛先を指定

➤ Toに指定できるのは一人のみ

①で宛先まで記載された
アクションを選択した場合は
その宛先を選択してください

アクション	SCADAにおけるプラントの操業状態(サービスレベル,安全レベル)確認(30秒~1分)
To	事業所1)CS-IT技術者
Cc	
返信元	事業所1)CS-IT技術者
インシデント情報	事業所1)CS-IT課長
メッセージ	事業所1)ボードマン

③ CCの選択(任意)



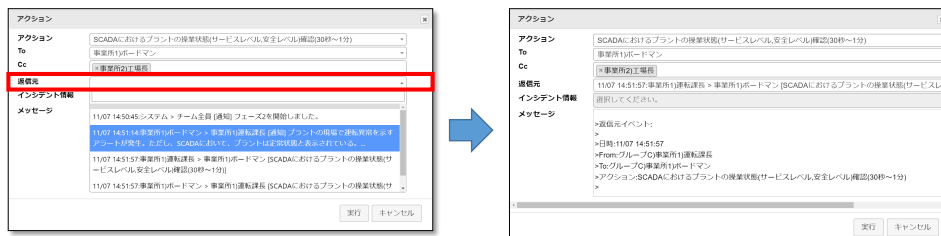
- アクションを知らせたい宛先を指定
- 何人でも指定可能

アクション	SCADAにおけるプラントの操業状態(サービスレベル,安全レベル)確認(30秒~1分)
To	事業所1)ボードマン
Cc	選択してください.
返信元	事業所1)CS-IT技術者
インシデント情報	事業所1)CS-IT課長
メッセージ	事業所1)ボードマン



④返信元の選択

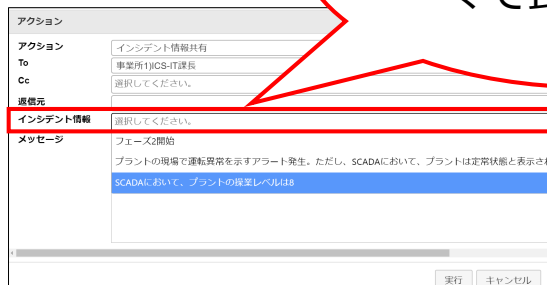
- 作成するアクションが、他者のアクションに対する返信の場合にのみ
その返信元を指定
- 選択すると、メッセージに自動で入力される
- **転送元**としても、利用可能



⑤インシデント情報の選択

- アクションとして「報告・連絡・相談」を選択
- インシデント情報をクリックすると、全てのインシデント情報が表示される
- 共有したいインシデントを選択

今回は自動で入力されるので、選択しなくて良いです。





⑥メッセージの入力

- アクションとして「相談」を選択した場合、**必須**
- 「相談」以外のアクションでも、必要に応じて入力可能
 - 部署間のプロトコル合わせ 等

「①アクションの選択」
時に
自動的に入力される場合
もあります！



⑦実行

- ①～⑥まで入力できたら、右下の「実行」を選択することでアクションを実行できる

⑧ その他



- 表示されるアクションは使用回数によって色が変わる
 - 緑色：未使用
 - 黒色：一回使用
 - 橙色：二回以上使用
- ※「相談」の色は黒から変化しない

アクション

アクション

To

Cc

返信元

インシデント情報

メッセージ

事業所内に最近越島エナジーに対する不審なメールが増加していることを報告

計装・設備課長へ外部と通信する作業があったかを問い合わせ

不審な通信があった為、サイバー攻撃の注意喚起

検知された不審な通信の原因究明を指示

報告・連絡

追跡

実行 キャンセル

返信/転送の作成方法 その1



① イベントトレイから返信/転送したいイベントを選択

- 濃いピンクに変わる

製造課長(製造課長@sample.com) ユーザID: 製造課長 Company ログイン

新規アクション 返信/回答 一覧更新

イベント sample.com: シナリオ[既定] フェーズ1 (状態:Started) 開始:0

目録	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001.PVの減少	SCADA上でFC001.PVの減少
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問...		手動操作によって、流量を...
06/08 11:11:10	プラント運転員	製造課長	手動での復旧が可能であることを報告	手動での復旧操作可能	手動操作で流量を戻すこと...

返信/転送の作成方法 その1



②返信/回答をクリック

製造課長(製造課長@sample.com) ユーザID: 製造課長 Company ログイン

新規アクション 返信/回答 一覧更新

sample.com: シナリオ(既定) フェーズ1 (状態:Started) 開始:0

日時	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001.PVの減少	SCADA上でFC001.PVの減少
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問...		手動操作によって、流量を調
06/08 11:11:10	プラント運転員	製造課長	手動での復旧が可能であることを報告	手動での復旧操作可能	手動操作で流量を戻すこと

返信/転送の作成方法 その1



③Boxが開く

- To及び返信元は、指定済み
- メッセージにも、返信元の情報が入力済み

アクション

アクション

To: IT課長

Cc: 選択してください。

返信元: 06/08 11:11:38:IT課長 > 製造課長 [報告・連絡]

インシデント情報: 選択してください。

メッセージ

>返信元イベント:
>>日時:06/08 11:11:38
>>From:IT課長
>>To:製造課長
>>アクション:報告・連絡

実行 キャンセル

返信の作成方法 その2



- 返信したいイベント上で、①右クリックし、②返信/転送をクリックすると、Boxが開き、イベント内容を見ることが出来る

①

②

その他：並び替え



イベントの(時系列順の)並びは、入れ替え可能

➤ 日時の▼をクリック

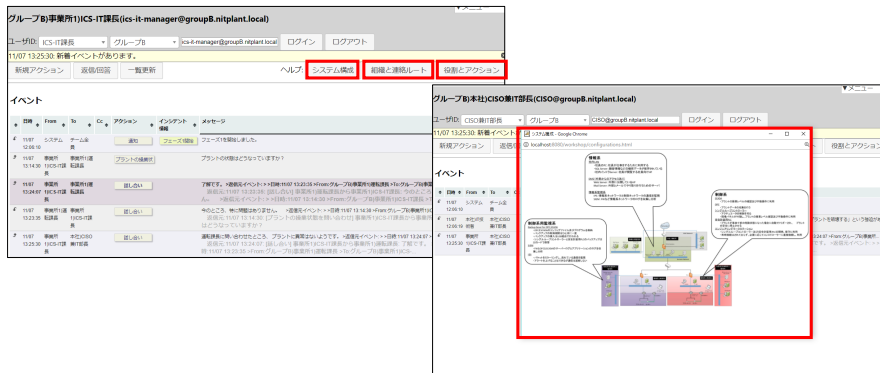
日時	From	To/Cc	アクション	インシデント情報	メッセージ
06/08 11:09:25	システム	チーム全員	通知	演習開始	演習を開始します。
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少	SCADA上でFC001 PVの減
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問...		手動操作によって、流量を
06/08 11:11:10	プラント運転員	製造課長	手動での復旧が可能であることを報告	手動での復旧操作可能	手動操作で流量を戻すこと

その他：前提条件の参照機能

ただし、本日は
「役割とアクション」を
利用しないでください
ヒントとなってしまう
情報が見えてしまいます

前提条件の参照が可能

- ▶ ヘルプ：「システム構成」「組織と連絡ルート」「役割とアクション」をクリックすると前提条件のBoxが開く



その他：マーキング機能



重要なイベントは、マークすることが可能

- ▶ マークしたいイベント上で①右クリックし、②マーク設定/解除をクリック

日時	From	To/Cc	アクション	インシデント情報
06/08 11:09:25	システム	チーム全員	通知	実習開始
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告	SCADA上でFC001 PVの減少
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問	手動操作によって、回
06/08 11:11:10	プラント運転員	製造課長	手動での復旧操作可能	手動操作で復旧も可能
06/08 11:11:38	IT課長	製造課長	報告・連絡	Gw2で不審な通信検出
06/08 11:11:58	製造課長	プラント運転員	プラント運転員に外部通信する作業があっ	いつと異なるが想定
06/08 11:12:05	プラント運転員	製造課長	未実施であることを報告	製造課では外部と繋がる作業はしてい

① 右クリック

② マーク設定/解除

その他：絞り込み機能



- 検索欄にワードや数字を入力すると、それに該当するイベントのみが表示される。

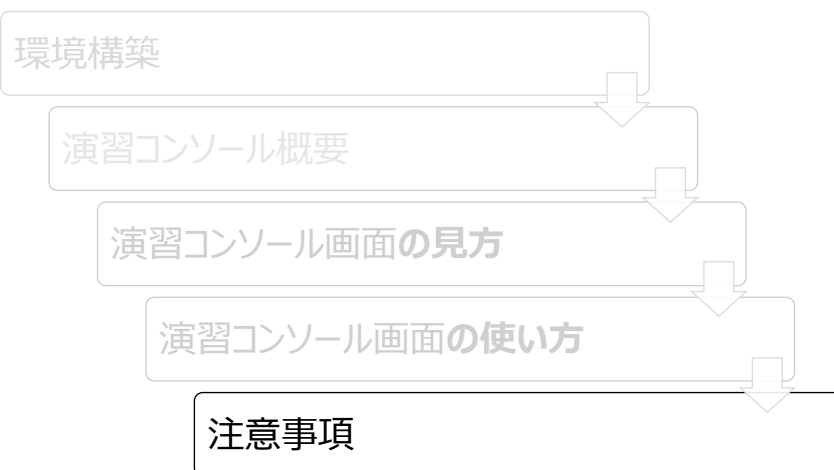
UID: 製造課長 Company ログイン ログアウト

ヘルプ: システム構成 組織と連絡ルート 役割とアクション

sample.com: シナリオ[既定] フェーズ1 (状態:Started) 開始:06/08 11:09:23 制限時間:20:00 経過:04:45 残り:15:14 スコア:0 **絞り込み**

アクション	インシデント情報	メッセージ
通知	異常開始	異常を開始します。
運転異常を報告	SCADA上でFC001.PVの減少	SCADA上でFC001.PVの減少しています。
プラント運転員に手動での復旧可能性を問...		手動操作によって、流量を戻すことができますか？
手動での復旧が可能であることを報告	手動での復旧操作可能	手動操作で流量を戻すことが可能です。
報告・連絡	Gw2で不審な通信検出	
プラント運転員に外部通信する作業があっ...		いつも異なる外部と通信する作業があったか？
未実施であることを報告	製造課では外部と繋がる作業はしていない	特にやってません。

説明の流れ



注意事項



- ブラウザの更新ボタンをクリックしないこと
 - イベントトレイ上の「**一覧更新**」をクリックする
 - もし、ブラウザの更新ボタンをクリックした場合は再度ログインしてください

製造課長(製造課長@sample.com) ユーザID: 製造課長 Compa

新規アクション 返信/回答 **一覧更新**

イベント sample.com: シナリオ[既定]

日時	From	To/Cc	アクション
06/08 11:09:25	システム	チーム全員	通知
06/08 11:10:00	プラント運転員	製造課長	運転異常を報告
06/08 11:11:03	製造課長	プラント運転員	プラント運転員に手動での復旧可能性を問...
06/08 11:11:10	プラント運転員	製造課長	手動での復旧が可能であることを報告
06/08 11:11:38	IT課長	製造課長	報告・連絡
06/08 11:11:58	製造課長	プラント運転員	プラント運転員に外部通信する作業があっ...

注意事項：アクションに関して



- 一度アクションを実行すると取り消すことはできない！！
 - 一つのアクションの実行がその後の対応に重大な影響を及ぼす可能性がある。
 - 迅速ながらも、慎重な意思決定を。
- アクションカードはどんどん増えます
 - イベントを受信した際には、注意深くアクションの欄の見てください。
 - 見落としが重大事故発生の原因になるかもしれません。
- **アクションカードの「報告連絡」は使用しないで下さい**

注意事項：自動応答ユーザーに関して



- CC:自動応答ユーザーに対して、指示、報告・連絡を行った場合
 - 自動応答ユーザーは返答しません
 - 自動応答ユーザーに返答を求める場合はToで指定してください
- To: 自動応答ユーザーに対して、相談を行った場合
 - 自動応答ユーザーは何も返答しません
- シナリオが想定していないアクションを自動応答ユーザーに対して行った場合
 - 「こちらの対応範囲外です。」と返答されます



振り返りシート

振り取りシート出力方法



右上のメニューより**振り取り**をクリックすると、ワークフローが表示さ
れる

The screenshot shows a software interface for a recovery process. At the top, there is a navigation menu with '振り取り' (Recovery) highlighted. Below the menu, there is a status bar indicating the system is in a 'Started' state. The main area displays a workflow with several steps, including 'システム', 'サイバー攻撃', '監視監視', 'ネット監視', '行調査', 'アラート監視', '監視', and '工場'. A timeline on the right side shows the duration of each step, starting from 06/08 11:09:23 and ending at 06/08 11:16:24.



セットアップ、ゲームデータ作成マニュアル



ゲームデータ作成

ゲームデータ作成インターフェースの機能と作成方法



ゲームデータ作成用EXCELファイル (Actorsシート)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	演習ゲーム用アクター登録シート		メンバー用json作成											
2														
3	参加者番号	99	0	1	2	3	4	5	6	7	8	9	10	11
4	Mode(選択)	System	Manual	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto
5	名前	System	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長	ネット監視担当	IT課長	総務	工場長	計測エンジニア	計測課長	設備課長	他工場長
6	役職	System	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長	ネット監視担当	IT課長	総務	工場長	計測エンジニア	計測課長	設備課長	他工場長
7	説明	system	facilitator											
8														
9	TeamAddress	koshiene.com												
10	TeamName	KOSHI-ENE												
11	DataDir	C:\workspace\作業用¥												
12														
13	type	Auto	Manual	Timer										
14	rolename=role													
15	email=role@team													
16	all	system	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長	ネット監視担当	IT課長	総務	工場長	計測エンジニア	計測課長	設備課長	他工場長
17	all	system	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長	ネット監視担当	IT課長	総務	工場長	計測エンジニア	計測課長	設備課長	他工場長
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														

ゲームのシナリオで出てくる人を
設定するためのシート



シナリオを基にしたゲームデータの作成(1) (Actorsシート)

	A	B	C	D	E	F
1	演習ゲーム用アクター登録シート		メンバー用json作成			
2						
3	参加者番号	99	0	1	2	3
4	Mode(選択)	System	Manual	Auto	Auto	Auto
5	名前	System	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長
6	役職	System	演習ファシリテータ	サイバー攻撃者	プラント運転員	製造課長
7	説明	system	facilitator			
8						
9	TeamAddress	koshiene.com				
10	TeamName	KOSHI-ENE				
11	DataDir	C:\workspace\作業用¥				
12						
13	type	Auto	Manual	Timer		
14	rolename=role					
15	email=role@team					
16						



Actorsシート:roleの設定1

- 参加者番号:1から順につけていく,基本的にはroleの人数に制限はなく、追加したい分セルを増やしてゆけば良い

※Systemと攻撃者はデフォルトのままにしておく

- Mode:Timer,Auto,Manualの3つが設定できる
 - Timer:ゲーム開始からの時間でコントロールし主に攻撃者に使う
 - Auto:参加者が担当しないroleに使う
 - Manual:参加者が操作するrole



Actorsシート:roleの設定2

- 名前:参加者の名前、自社でのその役職の呼び方
- 役職:正式なまたは一般的な役職名
- 説明:その役職がどういうことなのかなどを簡単に記載

※3つの区別はゲームの展開にあまり影響がないため名前と役職名に役職名を入力し、説明は入力しなくても良い



シナリオを基にしたゲームデータの作成(2) (Scenarioシート)

CardNo	Mode	name	message	Auto	Manual	共通入力
7	Timer	演習開始				
8	Auto	インターネットにフィッシングサイトを開設				
9	Auto	計装ベンダがアクセスし、コントローラ保守用PCがゼロデーのウイルスに感染				
10	Auto	Aプラントの複数のUT35Aのアップデートを計装ベンダ(Y社)に依頼する				
11	Timer	制御用ネットのPCがゼロデーウイルスに感染				
12	Timer	データサーバにVirusが感染し、FC01のUT35AのMVを100%にする攻撃を実施				
13	Auto	TC01のUT35AのMVも100%になりヒータがフルパワー				
14	Auto	SCADAで異常な温度上昇と液面低下に気づく				
15	Auto	SCADAでコントローラのMVの復帰を図るが、効果なし				
16	Auto	急速な温度上昇と液面低下を課長に報告				
17	Auto	現場の状況確認を指示				
18	Auto	高温になっているので、運転課長に停止を提言				
19	Auto	運転員にプラント停止を指示				

AutoかManualかTimer

Messageの要約

表示されるカード情報(改行禁止)

HELPで表示される内容

この欄が空欄だと、以下の行は読まない

必須 推奨 省略可

シナリオを基にしたゲームデータの作成(3) (Scenarioシート)

addstate-list	addstate-name-list	addstate-to	removestate-list	TriggerCondition	TriggerTime	delay	from	to	cc
1199000	01919	演習開始状態	製造課長が特定の指示(現場)		0		system	all	
2101001		サイバー攻撃者がフィッシングサイトを開設	system	11990010		5	system	system	
2117001		計装ベンダがアクセスし、コントローラ保守用PCがゼロデーのウイルスに感染	system	21010010		5	system	system	
2101002		Aプラントの複数のUT35Aのアップデートを計装ベンダ(Y社)に依頼する	system	170010		5	system	system	
2101003		制御用ネットのPCがゼロデーウイルスに感染	system	1080010		5	system	system	
11990020		データサーバにVirusが感染し、FC01のUT35AのMVを100%にする攻撃を実施	system	21170020		5	system	system	
21020010		TC01のUT35AのMVも100%になりヒータがフルパワー	system	21010020		5	system	system	
21020020		SCADAで異常な温度上昇と液面低下に気づく	system	21010030		5	system	system	
21030010		SCADAでコントローラのMVの復帰を図るが、効果なし	system	11990020		5	system	system	
21020030		急速な温度上昇と液面低下を課長に報告	system	21020010		5	system	system	
21020040		現場の状況確認を指示	system	21030010		30	system	system	
		高温になっているので、運転課長に停止を提言	system	21030010		5	system	system	
		運転員にプラント停止を指示	system	21020030		5	system	system	

左の行の解説

生成する情報コード

削除したいaddstate-listを記載

基本的にはtoと同じ。この欄が空だとAddstateを実行しない

Timerによる起動時刻(ゲーム開始がゼロ)

トリガー成立から実行までの遅れ

起動条件となる情報コード

メールでいうFrom, To, ccと同じ

必須 推奨 省略可

シナリオを基にしたゲームデータの作成(4) (Scenarioシート)

O	P	Q	R
15	16	17	18
Auto/Manual/Timer共通入力		Manual用入力	
attachment-list	attachment-name-list	roles-list	DisplayCondition
22990	演		
2201	インタ		
2202	ペンダがフィッシングサ		
2203	エンジン		
2204	用ネッ		
240	virusがPLCに		
22020070	ポンプが破損しました!!		
22010050	サイバー攻撃者がヒーターONのこ		
22020080	タンクの水温がサービス不能レベル		

ユーザー所有の情報カードの発行
Timerの時は必ず記述する

ユーザー所有の情報カードの名前

この行で示されるアクションを選択、実行できるアクターの情報
fromと同じroleが入る

カードを表示する条件
Attachment-listを入力することで制限する

必須 推奨 省略可

1. Scenarioシート

- cardNO:1から順に一番上からふっていく
※空欄や数字のとびがないか注意
- Mode:Actorsシートで設定したModeに合わせる
fromに入力したroleのmodeにする
- name:messageの要約
- message:アクションの内容
- description:コンソール画面でのHELPで表示される内容



2. Scenarioシート

- Addstate-list:アクション固有のコード、ゲームシステムは各アクションをこのコードで認識しこれを使って各roleのやり取りをコントロールしアクションの送受信を行っている
※エラーの原因となることが多いのでエラーの際はまずここを確認
- Addstate-name-list:Addstate-listの解説
- Addstate-to:toの宛先と同じものを入力



3. Scenarioシート

- triggercondition:アクションが成立するための条件つまりそのアクションがゲーム中に起こるための条件、成立条件となるアクションのaddstate-listを入力する
AND,ORなどでさらに制限をかけることもできる
※関係するのはTimer,Autoのアクション
- trigger-Timer:Timerモードのアクションが起こるまでの制限時間を設定する、ゲーム開始からカウントが始まる



4. Scenarioシート

※triggerconditionとtriger-Timerを併用した場合は
両方の条件が満たされたらアクションが起こる

- delay:アクションの成立条件が満たされてから実際に起きるつまりゲーム上で発生するまでの時間
- from,To,cc:送信者、主な受信者、副次的な受信者
※Toの宛先は一人、ccは何人でも可



5. Scenarioシート

- removestate-list:ゲーム上で認識されている
addstate-listをゲーム上から除外する
これでtrigerconditionの成立条件を崩し分岐など
をつくる事が出来る

※除外するaddstate-listは除外専用のもを作成
する、作成したaddstate-listをANDなどを使って
trigerconditionに付け加える



removestate-list用addstate-list 生成例

F6 : <input type="text" value="11990010,91990010,91990020,91990030"/>						
	A	B	C	D	E	F
1	シナリオに基づくゲームデータ作成シート			シナリオ用json作成	(注意:すべてのセルは、"文字列	
2						listは、でつないでく
3	1	2	3	4	5	6
4	CardNo	Mode	Auto/Manual			
5			name	message	description	addstate-list
6	1	Timer	演習開始	演習開始		11990010,91990010,91990020,91990030

演習開始などのシナリオには入らない内容のアクションカードを作成し、そのaddstate-listにremovestate-list用のものを入力。また、addstate-listは一つのアクションでいくつも作ることが出来る

※一つのアクションであまりにも多く入力するとエラーが起きやすくなるため注意



removestate-list用addstate-list 生成例

11030050	運行指令長が運行再開	運輸部長	99010020	11040050
11030061	運行指令長が運行見合わせ	運輸部長	99010010	11040060
11020010	運輸部長が運行再開判断	all		11030050,99010010,AND
11020020	運輸部長が運行見合わせ	all		11030061,99010020,AND

removestate-list用に作成したaddstate-listを上記の様に元の成立条件にプラスで加えることでremovestate-listが機能すれば成立条件を崩すことが出来るようになる



6. Scenarioシート

- attachment-list:そのアクションの情報(要約)に対する固有のコード、Manualでゲームに参加する参加者が選択できるアクションを制限するためのコード、相手(To,cc)に対してアクションを起こしたのと同時にこの情報コードも渡される
得たコードは自身のアクションに添付して展開も出来る(演習コンソール>新規アクションの中のインシデント情報で添付可能)
- attachment-name-list:attachment-listがもつアクションの情報(要約)の内容
- roles-list:そのアクションを行うroleを入力、fromと同じroleを入力



7. Scenarioシート

- displaycondition:そのアクションを参加者のアクション選択リストに表示するかどうかの条件
条件となるattachment-listを入力することで制限する、もしそのattachment-listを入手したら表示される

このリストに表示するかどうかをコントロールする



attachment-listとdisplaycondition

attachment-list

displaycondition

運行指令員	運行指令長	21040050	手動操作成功		
運行指令長	運輸部長	21030050	運行再開進言	運行指令長	21040050

運行指令員が運行指令長に対して手動操作が成功しましたという報告のアクションを行うとそれに付随して21040050(手動操作成功)という情報が運行指令長に送られる。その時、displayconditionに21040050が設定されていればこのとき初めて運行指令長のアクション選択肢に運行再開を進言するというアクションが表示され、選択できるということになる。前述したが、この運行指令長が得た21040050(手動操作成功)という情報はアクションを選択する画面にインシデント情報の欄で他の人にも展開することが出来る。attachment-listはTo,ccの相手ともに渡すことが出来る



ゲームデータ作成用EXCELファイル (Point用)

No	State-ID	name	point	state	col	multi	after	description
6	12010010	サイバー攻撃者がインターネットにフィッシングサイトを開設した状態						
8	12010020	サイバー攻撃者が対象事業所社員にアクセス催促メールを発信した状態						
1	12990010	手動操作をしていない状態						
2	12990020	Gw1を遮断していない状態						
3	12990030	Gw2を遮断していない状態						
4	12990040	Gw0を遮断していない状態						
5	22990010	演習開始						
6	12010010	サイバー攻撃者がインターネットにフィッシングサイトを開設した状態						
7	22010010	インターネットにフィッシングサイトを開設	初期ポイント	100			0	初期ポイント
8	12010020	サイバー攻撃者が対象事業所社員にアクセス催促メールを発信した状態						
9	22010020	対象事業社員にアクセスメール発信						
10	12010030	生産管理担当が誤ってアクセスした状態						
11	22100010	ご判断し、アクセス						
12	12010040	サイバー攻撃者が出来たトンネルを盗む、PCを攻撃し、SCADAに到達した状態						
13	22010030	サイバー攻撃者が出来たトンネルを盗む、PCを攻撃し、SCADAに到達						
14	12010050	サイバー攻撃者がコントローラにFC01.MV=0の指示を送った状態						
15	22010040	サイバー攻撃者がコントローラにFC01.MV=0の指示を送る						
16	12020040	ポンプが破損した状態						
17	22020070	ポンプが破損しました!!						
18	12010060	サイバー攻撃者がポンプ停止のコマンドを送った状態						
19	22010050	サイバー攻撃者がポンプ停止のコマンドを送る						
20	12020050	ポンプ停止が停止した状態						
21	22020080	ポンプが停止しました!!						

左の表はシナリオ用json作成ボタンをクリックすることで自動で生成、この値を参考にポイントを作成しても良いが、シナリオシートを直接参考することを推奨

Pointを付けるためのシート



Point(states)シート

name	point	state condition
BEST	100	11990010
GOOD	70	11990020
BAD	30	11990030
WORST	0	11990040

nameはscenarioシートで作成したポイントを付けたいアクションのnameをそのまま使用、stateconditionはそのアクションのaddstate-listを入力する
pointの点数は任意
ゲーム結果による総ポイントはファシリテータ画面で確認可
※現状はこの項目のみの使用でお願いします、申し訳ありません。



jsonの出力

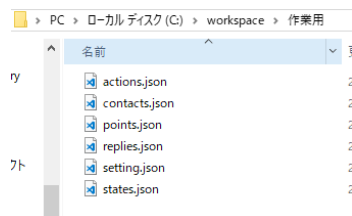
- 3つのシートが完成したら各シートにあるjson作成ボタンを全てクリック

メンバー用json作成

シナリオ用json作成

ポイント用json作成

- Actorsシートで設定したディレクトリにjsonがはき出される



注意点

- ManualからToの宛先にSystemを選択することはできない
- Toの宛先がManualのアクションのaddstate,removestateはゲームシステムが認識しないため、そのaddstateをtriggerconditionに入れたアクションは実行されない。またremovestateも機能せず指定したaddstateを除外しない。(今後改善していく予定)
- messageなどの文章を書く項目では改行してはいけない
- アクションのnameやmessageにはactorの名前を入れると誰に送れば良いかが分かってしまうため基本入れない(例外:誰に送るべきかを考える必要がないと意図しているアクションに記載するなど良い,etc...)
- 91xxxxxの形のコードはremovestateで取り除くためのコードとして使用する



addstate-listとattachment-listの番号のつけ方

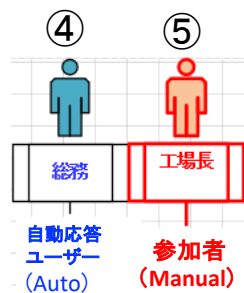
Attachment-listコード
Displayconditionに利用し、Manualの選択の表示を制御する

Addstate-listコード
TirggerConditionに利用し、Timer,Autoの挙動を制御する

情報コードのつけ方

11050020

- 1:addstate-list
- 2:attachment-list
- 9:*
- 1:特に意味なし
- 05:Actor番号
- 002:アクション番号
- 0:バリエーション



自動応答ユーザーの挙動は下記のどちらか
•TriggerCondition
•Timer

TriggerConditionではAND,OR,NAND,NOR,NOTを最後につけると2つ以上のコードに対して論理演算ができ、省略した場合はORになる

11010010,11010020,AND

「*」は、後述の用途で、成立前情報として用意

TrigerCondition (11050020)

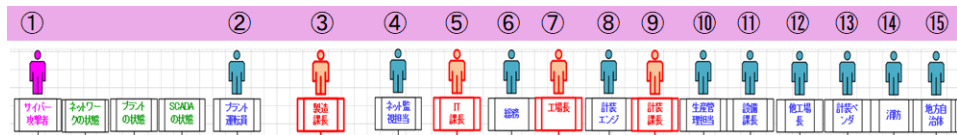
Aプラントの顧客の皆様へ、お詫びの連絡を指示

Addstate (11050020)

了解と返答



シナリオのカードから、EXCELの各行の設定(1)



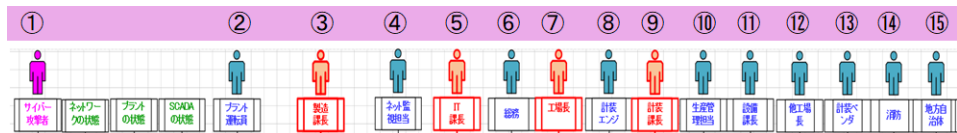
A1 Timer(system)により、時刻2に「A1: サイバー攻撃者①の攻撃」が始まる

Addstate-nameもattachment-nameもnameと同じに

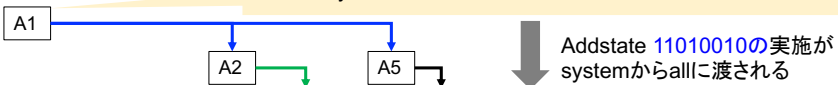
mode	name	Addstate	Add-to	trigger	time	from	to	attachment	Display
Timer	A1	11010010	all		2	system	all	21010010	



シナリオのカードから、EXCELの各行の設定(2)



Timer(system)により、時刻2に「A1: サイバー攻撃者①の攻撃」が始まる



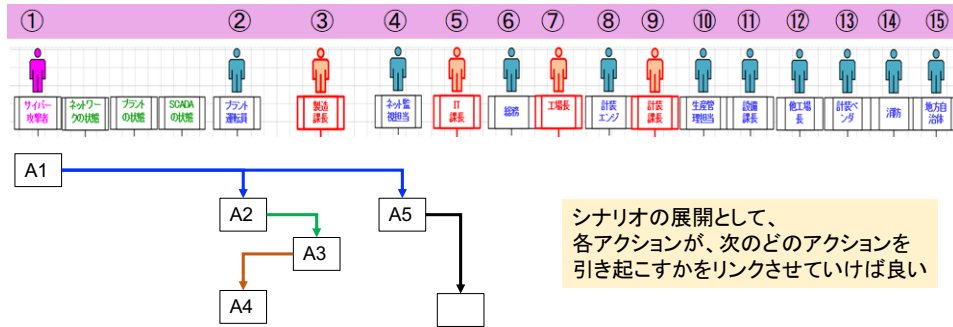
Addstate 11010010の実施が systemからallに渡される

「A2:プラント運転員②の反応」と「A5:ネットワーク監視担当④の反応」により、シナリオが展開する

mode	name	Addstate	Add-to	trigger	time	from	to	attachment	Display
Timer	A1	11010010	all		2	system	all	21010010	
Auto	A2	11020010	③	11010010		②	③	21020010	
Auto	A5	11050010	⑤	11010010		④	⑤	21050010	



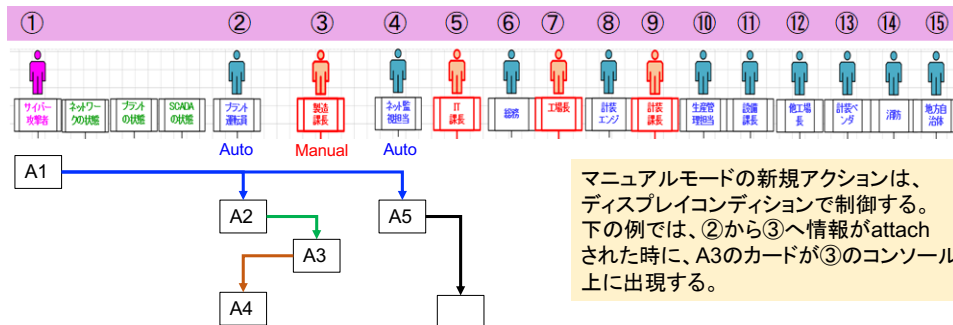
シナリオのカードから、EXCELの各行の設定(3)



mode	name	Addstate	Add-to	trigger	time	from	to	attachment	Display
Timer	A1	11010010	all		2	system	all	21010010	
Auto	A2	11020010	③	11010010		②	③	21020010	
Auto	A3	11030010	②	11020010		③	②	21030010	
Auto	A4	11020020	③	11030010		②	③	21020020	
Auto	A5	11050010	⑤	11010010		④	⑤	21050010	



シナリオのカードから、EXCELの各行の設定(4)



mode	name	Addstate	Add-to	trigger	time	from	to	attachment	Display
Timer	A1	11010010	all		2	system	all	21010010	
Auto	A2	11020010	③	11010010		②	③	21020010	
Auto	A3	11030010	②			③	②	21030010	21020010
Auto	A4	11020020	③	11030010		②	③	21020020	
Auto	A5	11050010	⑤	11010010		④	⑤	21050010	



実施タイミングでの条件分岐のつくり方

サイバー攻撃者①の攻撃A1は60分後に発生するがコントローラの停止(手動運転への切替)A2がそれ以前に行われていたか、まだ、コントローラが働いていたかで、A1攻撃の効果が変化する。この場合、攻撃が失敗するA11と成功するA12を用意し、A2が成立しているかの条件をA11,A12のTrigger Conditionに加える。

mode	name	Addstate	Add-to	Remove	trigger	Time
Timer	初期	91020010	system			0
Manual	A2	11020010	all	91020010		
Timer	A11	11010011			11020010	60
Timer	A12	11010012			91020010	60

Tsurumi GO!

シナリオへの追加

A1後にA5という条件を追加して、分岐後、またA4に戻る場合の変更

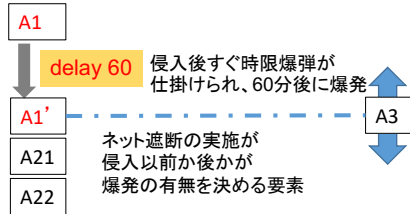
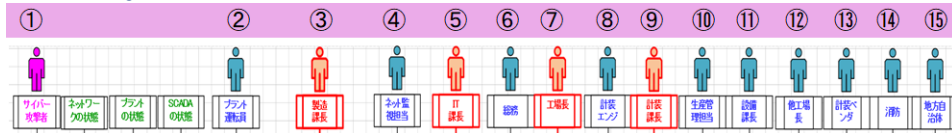
A5がA2の前に発生すると、A2の挙動が変化し、A6になる。A6はA3とは異なるが、A4に戻る

初期に、成立していないことを示すstateの定義とTriggerConditionにANDを追加してで条件分岐を作成するのは前例と同様

Name	Addstate	Remove	trigger	Time
初期	91010050, 91010060			
A1	11010010		分岐はAND	
A21	11010021	91010060	11010010,91010050, AND	60
A22	11010022		11010010,11010050, 91010060,AND	60
A3	11010030		11010021	
A4			11010030,11010060, OR	
A5	11010050	91010050	合流はOR	
A6	11010060		11010022	

Tsurumi GO!

Delayを利用する際の注意(1)



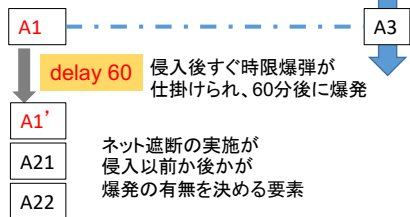
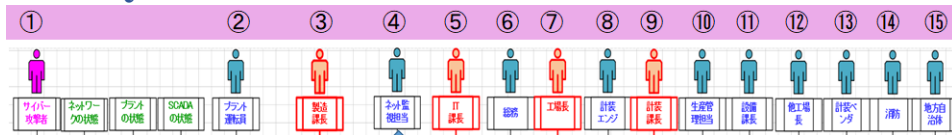
A1のタイミングでトリガーが成立してもdelayが設定されると、実行されるのは、delay時間後(A1')になる。

A1時刻以前に、他のイベントA2で、A1時刻に発生するイベントがA21とA22に分かれるとき

mode	name	Addstate	Add-to	Remove	trigger	Time	delay
Timer	初期	91030010	All			0	
Timer	A1	1010010	system			2	60
Manual	A3	11030010	system	91030010			
Auto	A21	11010021	system		1101010,91030010,AND		
Auto	A22	11010022	system		1101010,11030010,AND		



Delayを利用する際の注意(2)



A1のタイミングでトリガーが成立してもdelayが設定されると、実行されるのは、delay時間後(A1')になる。

A1時刻以前に、他のイベントA2で、A1時刻に発生するイベントがA21とA22に分かれるとき

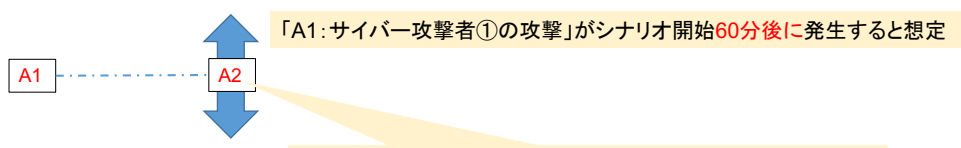
mode	name	Addstate	Add-to	Remove	trigger	Time	delay
Timer	初期	91030010	All			0	
Timer	A1	11010010	system			2	
Manual	A3	11040010	system	91030010			
Auto	A1'	11010011	system		11010010		60
Auto	A21	11010021	system		11010010, 91030010, AND		
Auto	A22	11010022	system		11010010, 11040010, AND		



以下、分岐に関する補足資料



実施タイミングでの条件分岐のつくり方(1)



「A1:サイバー攻撃者①の攻撃」がシナリオ開始60分後に発生すると想定

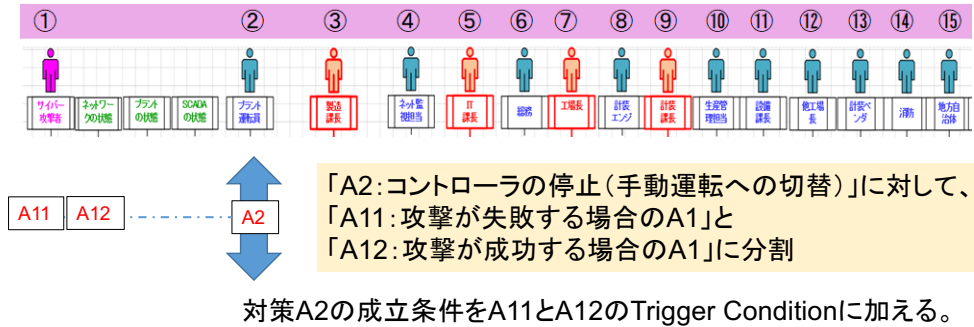
「A2:コントローラの停止(手動運転への切替)」がA1発生以前に行われていたか、まだコントローラが働いていたかによって、A1攻撃の効果が変化する場合(事故の発生など)を考える

シナリオの展開として、アクション間の相対的なタイミングにより変化する！

さて、どうやって表現しましょうか？



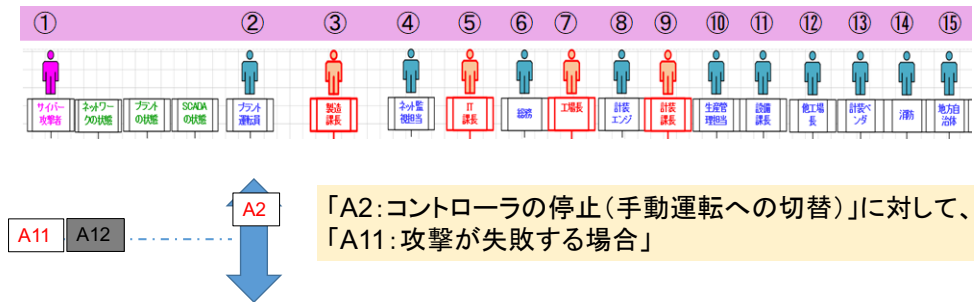
実施タイミングでの条件分岐のつくり方(2)



91020010をRemoveして
11020010を発生できるかが分かれ道

mode	name	Addstate	Add-to	Remove	trigger	Time
	初期	91020010	system			0
Manual	A2	11020010	all	91020010		
Timer	A11				11020010	60
Timer	A12				91020010	60

A2実施が間に合って、攻撃失敗の場合



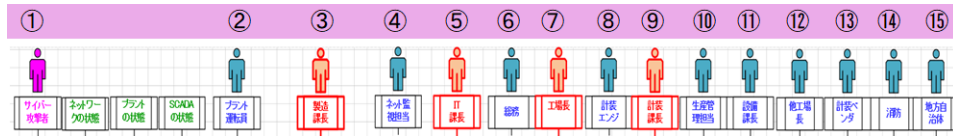
mode	name	Addstate	Add-to	Remove	trigger	Time
Timer	初期	91020010	system			0
Manual	A2	11020010	all	91020010		
Timer	A11				11020010	60

初期状態(A2実施前)は
91020010

A2実施が間に合い、
91020010がremove、
11020010となる

60分後、11020010が
トリガーでA11が発生

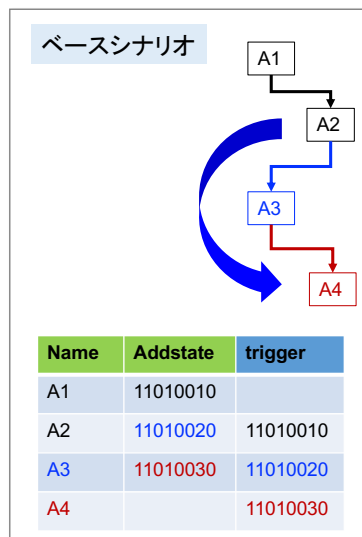
A2実施が間に合わず、攻撃成功の場合



「A2:コントローラの停止(手動運転への切替)」に対して、「A12:攻撃が成功する場合」

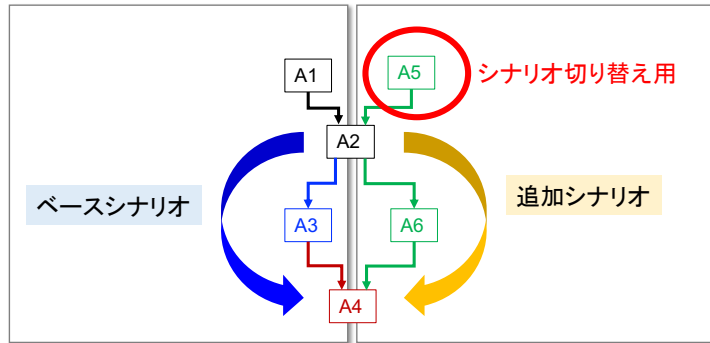
	mode	name	Addstate	Add-to	Remove	trigger	Time
初期状態(A2実施前)は 91020010	Timer	初期	91020010	system			0
A2が60分以内に未実施							
60分後、91020010が トリガーでA12が発生	Timer	A12				91020010	60

シナリオの追加(1)



ベースシナリオに対して、A2に条件を追加して分岐させた後、再びA4に戻るような別シナリオの追加を考える

シナリオの追加(2)



A5がA2の前に発生するかどうかでシナリオを切り替える

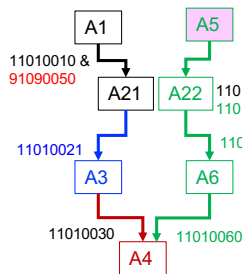
⇒A5発生により、A2の挙動が変化し、A3シナリオから、A6シナリオに

⇒A3もA6も異なるが、どちらもA4に戻る



シナリオの追加(3)

初期に、成立していないことを示すstateの定義と
TriggerConditionにANDを追加して
条件分岐を作成するのは前例と同様



A5を発生させれば
緑色のシナリオルートに
切り替わる

Name	Addstate	Remove	trigger	Time
初期	91010050, 91010060			
A1	11010010			
A21	11010021	91010060	11010010,91010050,AND	60
A22	11010022		11010010,11010050, 91010060,AND	60
A3	11010030		11010021	
A4			11010030,11010060	
A5	11010050	91010050		
A6	11010060		11010022	

単なる並列はOR



セットアップ

ツールの準備と環境構築



1. ツールの準備 (Windows, Mac共通)

- Webブラウザ: 必須
(Google chrome推奨)
- JAVA8以降インストール: 必須
(Oracle JDK推奨)
- テキストエディタ(json形式に対応したもの): 必須
(Visual studio code推奨)
- tomcat9,nkfフォルダ: 必須
(こちらで用意したものを配布)



2. 実行環境の準備1 (Windows,Mac共通)

- ローカルディスク(c:)にworkspaceフォルダを作成
- 作成したworkspaceフォルダ直下にtomcat9とnkfフォルダを配置
 - workspaceフォルダ直下に作業用という名前のフォルダを作成

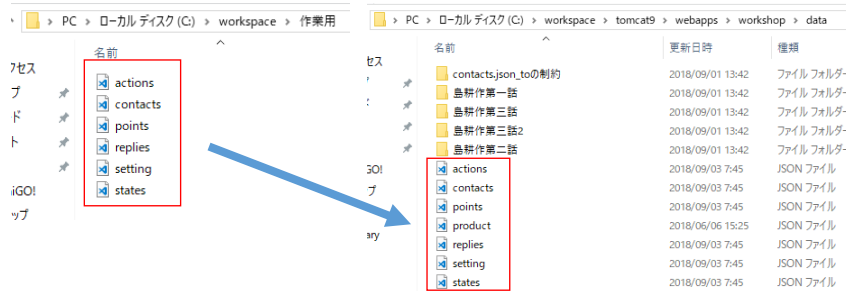


2. 実行環境の準備2

- JAVA-HOMEの環境設定
 - コントロールパネル>システムとセキュリティ>システム>設定の変更>詳細設定>環境変数
 - ※Windowsのみ必要、Macは必要なし
- ゲームデータの配置(jsonデータの配置)
 - C:\workspace\tomcat9\webapps\workshop\dataにExcelから作業用フォルダに出力されたjsonデータをコピーして貼り付け(Win,Mac共通)



ゲームデータの配置 (jsonデータの配置)



Excelから出力した作業用フォルダのデータをコピーしてdataフォルダ内のjsonデータを上書きして貼り付けする。

※product.jsonだけはもともともと置かれているものを使用

※使用するjsonデータのみdata直下におき、使用しない別シナリオのjsonデータは上記の様にフォルダにしまうことで残しておくことも可能。そのデータを使いたいときにフォルダから出し直下におけば別のシナリオを動かすことが出来る

※フォルダの名前は英語を推奨



2. 実行環境の準備3

- Windowsファイアウォールの設定(オプション)
 - 演習サーバへのリモートからのアクセスを許可するには、TCPポート8080の受信許可ルールを設定する
 - ※基本はデフォルトで使える
 - ※サーバとクライアントを同一PCで実行する場合、本作業は不要



3. ゲームの起動

1. rmBOM.batをたたく

- C:\workspace\nkf内にあるrmBOM.bat/shをたたく
(文字化け回避のため)

2. tomcat9の起動

- C:\workspace\tomcat9\bin内にあるstartup.bat/shを
たたく

※Macの場合はターミナルからこの手順を行う,Windowsはどちらの方法でも可能

※tomcat9がすでに起動している場合はshutdown.bat/shを行ってから再起動をかける



4. 演習コンソールアクセス1 (ファシリテータ用)

1. Google chromeを起動し「ctrl+shift+N」でシークレットウインドウを開く

2. <http://localhost:8080/workshop/>にアクセス

右記の画面が表示される

[演習参加者はこちらから](#)

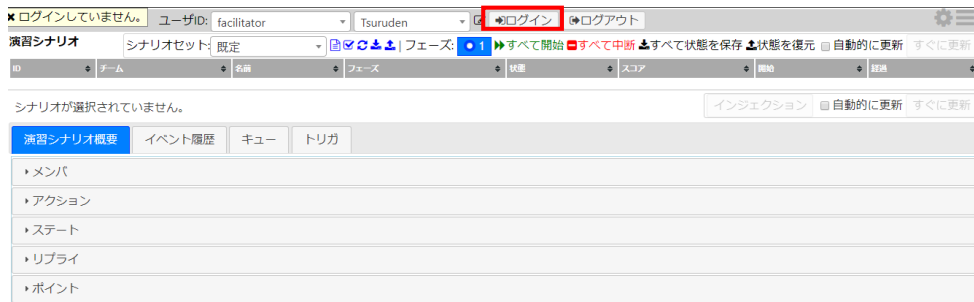
[管理者/オブザーバはこちらから](#)

3. ファシリテータは「[管理者/オブザーバはこちらから](#)」を選択する



4. 演習コンソールアクセス2 (ファシリテータ用)

1. 3を行ったら下記の画面が出てくる



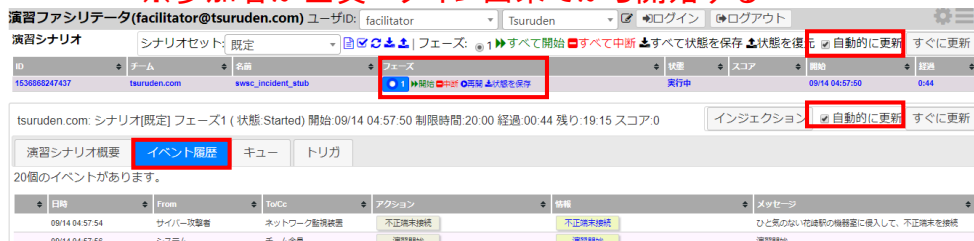
2. ログインを押す



4. 演習コンソールアクセス3 (ファシリテータ用)

- ログインし、新たに表示されたフェーズの青丸のを選択し、右の開始を選択でゲームが始まる
「イベント履歴で全てのやりとりを見ることが出来る、
「自動的に更新」でイベント履歴を自動で更新する

※参加者が全員ログイン出来てから開始する



4. 演習コンソールアクセス1 (参加者用)

- ファシリテータが立ち上げたサーバにアクセス
※シークレットモードでアクセス
 - [http://\[\]:8000/workshop/](http://[]:8000/workshop/)にアクセス
※[]の中はファシリテータPCのローカルアドレスが入る
例) <http://192.168.1.10:8080/workshop/>
- 下記画面の「演習参加者はこちらから」を選択

[演習参加者はこちらから](#)

[管理者/オブザーバはこちらから](#)

※参加者のこの後の操作や詳細は別資料に記載



注意点(エンジン操作時)

- ゲームが終わりもう一度ゲームを行う場合は
ファシリテータ、参加者ともにブラウザをおとし
tomcat9もシャットダウンし、その後再起動する



C.4 CARD-BASED TTX OPERATION MANUAL



カード演習作成方法

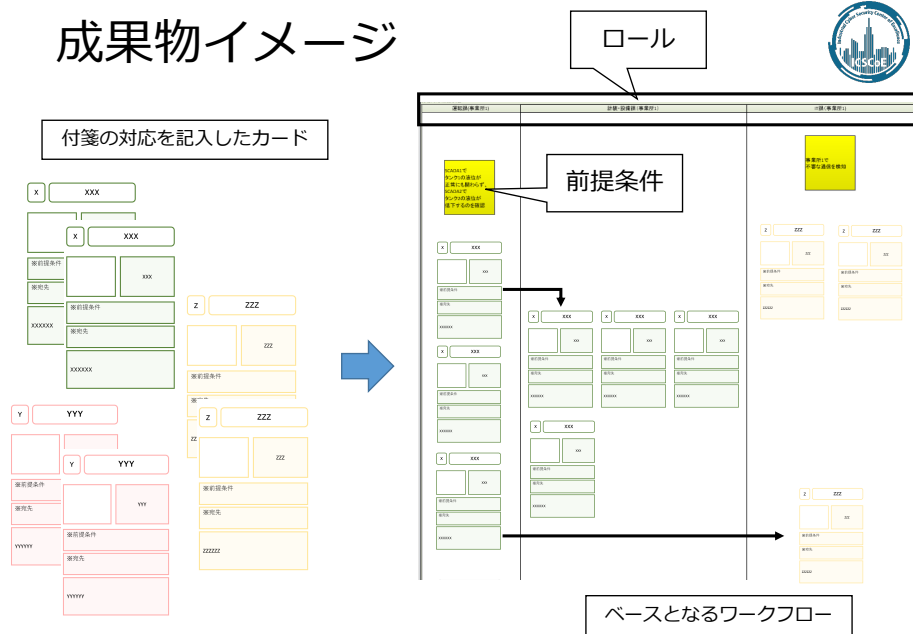
- 場所 文京グリーンコート
- 講師 国立大学法人 名古屋工業大学
橋本 芳宏
- 日時 令和元年10月28日

はじめに



- 本資料では、インシデント時の対応を記入した付箋からカード演習を作成していく手順について説明する

成果物イメージ



配布物

- カードテンプレート
- 前提条件記述用シート
- ワークフロー(A0用紙)
- マーカー

作成の流れ



1. ロールの再設定
2. 演習開始時の前提条件を設定
3. 付箋に書かれた対応をカードに落とし込む
4. 理想とするフローに並べる

1. ロールの再設定



- 作成した対応シナリオに出てくる各ロールを課や部ごとに括り、ロールを改めて設定する

※課や部で括れないロールはそのまま一つのロールとして設定する

※攻撃者は設定しない

運転課

- 運転課長
- ボードマン
- フィールドマン

IT課

- IT課長
- IT技術者

その他

- 営業
- バックオフィス
- 外部、 etc..

計装・設備課

- 計装・設備課長
- 計装技術者
- 設備技術者

工場長

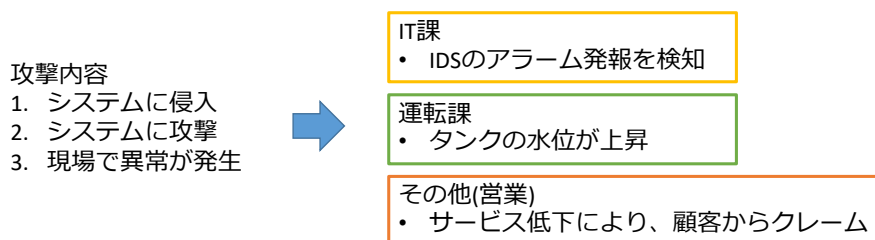
CSIRT

- 青文字は新たに設定したロールの例
- 工場長は課で括れないので一つのロールとして設定

2. 前提条件の設定



- 対応シナリオで想定した攻撃内容を基に演習開始時の各ロールの状況を設定する
 - 設定した前提条件を配布された紙に記述



3. 対応をカードに落とし込む

テンプレートの種類

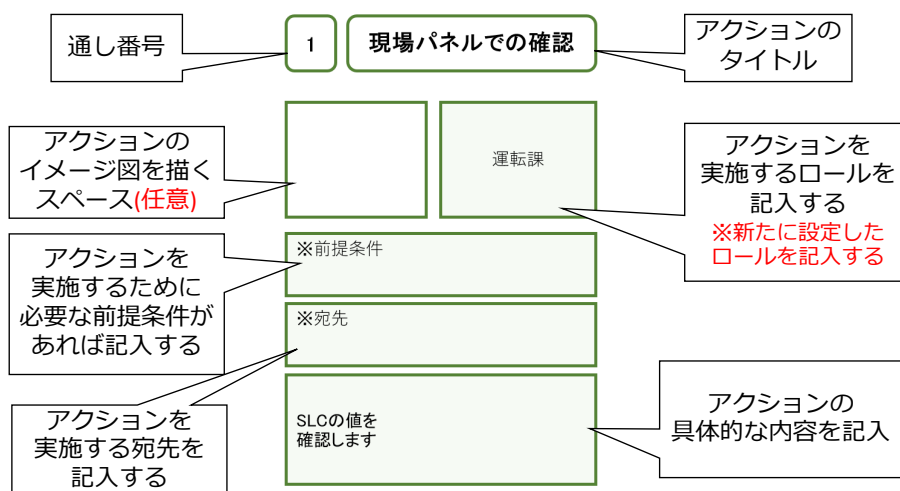


アクションカード：

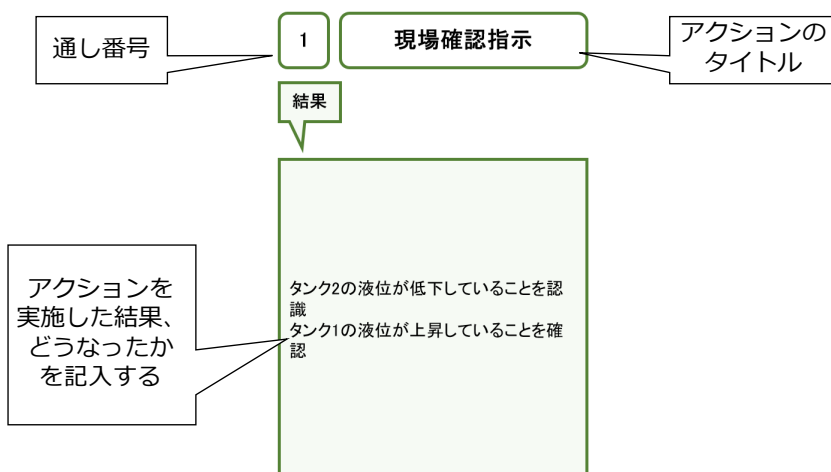
- ・ 付箋で作成した対応を記入していくカード
 - 緑色：現場での対応
 - 赤色：プラントの停止/再開
 - 黄色：本社での対応

1	現場パネルでの確認
	運転課
※前提条件	
※宛先	
SLCの値を確認します	

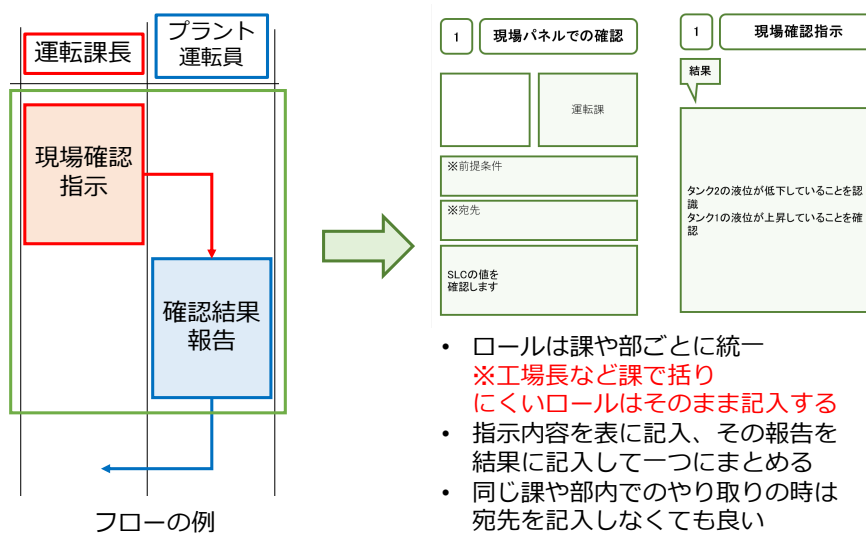
アクションカードの見方(表)



アクションカードの見方(裏)



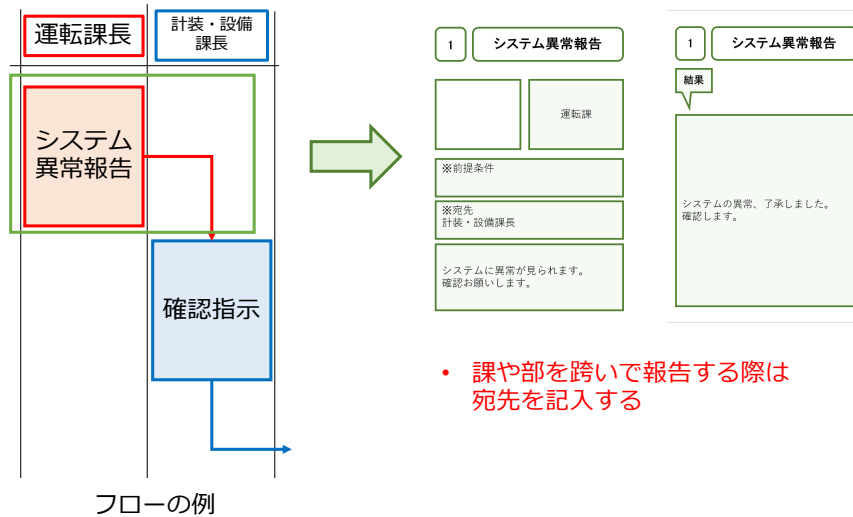
落とし込み方(例 1)



フローの例

- ロールは課や部ごとに統一
※工場長など課で括りにくいロールはそのまま記入する
- 指示内容を表に記入、その報告を結果に記入して一つにまとめる
- 同じ課や部内でのやり取りの時は宛先を記入しなくても良い

落とし込み方(例 2)

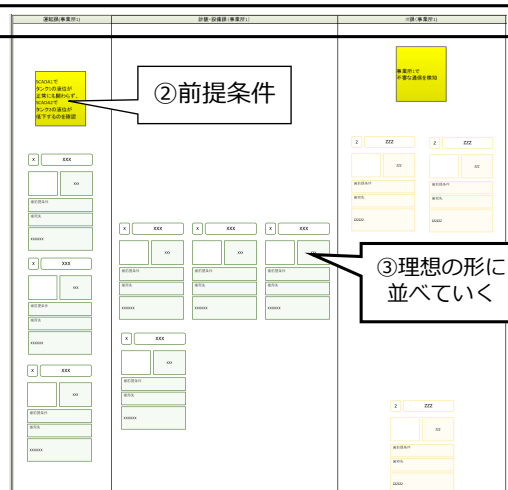


4. 理想のフローに並べる



①ロールごとに分ける

- ① 白紙のワークフローをロールごとのスイムレーンに分ける
※幅はロールごとに異なっても良い
- ② 前提条件を付与するロールに前提条件シートを置く
- ③ 作成したアクションを理想の形に並べてみる
※カードを繋ぐ線は書かずに並べるのみ



BIBLIOGRAPHY

- [1] N. Falliere, L. O. Murchu, and E. Chien. "W32. stuxnet dossier." In: *White paper, Symantec Corp., Security Response* 5.6 (2011), p. 29.
- [2] E. Byres. *Factory of the Future meets Stuxnet's Children: Egad!* 2012. URL: <https://www.tofinosecurity.com/blog/factory-future-meets-stuxnet%E2%80%99s-children-egad>.
- [3] K. Stouffer, J. Falco, and K. Scarfone. "Guide to industrial control systems (ICS) security." In: *NIST special publication* 800.82 (2011), pp. 16–16.
- [4] E. D. Knapp and J. T. Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.
- [5] J. Greenwood. *The third industrial revolution: Technology, productivity, and income inequality*. 435. American Enterprise Institute, 1997.
- [6] J. Frohm, V. Lindström, M. Winroth, and J. Stahre. "The industry's view on automation in manufacturing." In: *IFAC Proceedings Volumes* 39.4 (2006), pp. 453–458.
- [7] R. Shell. *Handbook of industrial automation*. CRC Press, 2000.
- [8] Z.-G. Wei, A. P. Macwan, and P. A. Wieringa. "A quantitative measure for degree of automation and its relation to system performance and mental load." In: *Human Factors* 40.2 (1998), pp. 277–295.
- [9] P. Troxler. "Making the 3rd industrial revolution." In: *FabLabs: Of machines, makers and inventors*, Transcript Publishers, Bielefeld (2013).
- [10] N. Falliere, L. O. Murchu, and E. Chien. "W32. stuxnet dossier." In: *White paper, Symantec Corp., Security Response* 5.6 (2011), p. 29.
- [11] The White House. *PPD-21, Critical infrastructure security and resilience*. <https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf>. 2013.
- [12] R. M. Lee, M. J. Assante, and T. Conway. "Analysis of the cyber attack on the Ukrainian power grid." In: *SANS Industrial Control Systems* (2016).
- [13] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies." In: *IEEE Control Systems* 21.6 (2001), pp. 11–25.

- [14] A. Boin and A. McConnell. "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience." In: *Journal of Contingencies and Crisis Management* 15.1 (2007), pp. 50–59.
- [15] D. Elliott, E. Swartz, and B. Herbane. *Business Continuity Management 2e: A Crisis Management Approach*. Taylor & Francis, 2010. ISBN: 9781134196883. URL: https://books.google.co.jp/books?id=Xqx%5C_AgAAQBAJ.
- [16] J. K. Ford and A. M. Schmidt. "Emergency response training: strategies for enhancing real-world performance." In: *Journal of hazardous materials* 75.2-3 (2000), pp. 195–215.
- [17] J. Borell. "Manage everything or anything? Possible ways towards generic emergency management capabilities." In: *Journal of Disaster Research* 10.2 (2015), pp. 246–251.
- [18] *Department of Homeland Security: Training available through ICS-CERT*. <https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT#workshop>. Accessed: 2019-07-09.
- [19] E. Sitnikova, E. Foo, and R. B. Vaughn. "The power of hands-on exercises in SCADA cyber security education." In: *IFIP World Conference on Information Security Education*. Springer, 2009, pp. 83–94.
- [20] E. Foo, M. Branagan, and T. Morris. "A proposed Australian industrial control system security curriculum." In: *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 1754–1762.
- [21] *European Network for Cyber Security: E.ON teams get trained on ICS and smart grid cyber security during the ENCS red team blue team course—ENCS*. <https://encs.eu/>.
- [22] M. Branlat. "Challenges to adversarial interplay under high uncertainty: staged-world study of a cyber security event." PhD thesis. The Ohio State University, 2011.
- [23] M. Branlat, A. Morison, G. Finco, D. Gertman, K. Le Blanc, and D. Woods. "A study of adversarial interplay in a cybersecurity event." In: *Proceedings of the 10th International Conference on Naturalistic Decision Making (NDM 2011). May 31st to June 3rd*. 2011.
- [24] T. Aoyama, H. Naruoka, I. Koshijima, and K. Watanabe. "How management goes wrong?—The human factor lessons learned from a cyber incident handling exercise." In: *Procedia Manufacturing* 3 (2015), pp. 1082–1087.
- [25] T. Aoyama, H. Naruoka, I. Koshijima, W. Machii, and K. Seki. "Studying resilient cyber incident management from large-scale cyber security training." In: *Control Conference (ASCC), 2015 10th Asian*. IEEE, 2015, pp. 1–4.

- [26] E. Luiijf and B. Te Paske. *Cyber Security of Industrial Control Systems*. Mar. 2015. DOI: 10.13140/RG.2.1.3797.4566.
- [27] J. D. Christopher. "Cybersecurity capability maturity model (C2M2)." In: *Department of Homeland Security* (2014).
- [28] *Cybersecurity Capability Maturity Model (C2M2) Program*. URL: <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0>.
- [29] J. Stevens. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)(Case Study)*. Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2014.
- [30] *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)*. URL: <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0/oil-and>.
- [31] P. Curtis, N. Mehravari, and J. Stevens. *Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0*. Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, 2015.
- [32] exida.com. *Resources*. URL: <https://www.exida.com/Resources/Term/IEC-62443>.
- [33] exida.com. *IEC 62443: Levels, Levels and More Levels*. URL: <https://www.exida.com/Blog/iec-62443-levels-levels-and-more-levels>.
- [34] M. Spear. "Industrial Cyber Security 101." In: *Honeywell Users Group Europe, Middle East and Africa* (2015).
- [35] P. WEF. "Risk and responsibility in a hyperconnected world." In: *Technical Report, World Economic Forum*. 2014.
- [36] National Institute of Standards and Technology (NIST) and United States of America. "Framework for Improving Critical Infrastructure Cybersecurity." In: (2014).
- [37] US Dept of Homeland Security and United States of America. *Homeland Security Exercise and Evaluation Program (HSEEP) Volume I: HSEEP Overview and Exercise Program Management*. 2007.
- [38] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good. "SP 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities." In: (2006).
- [39] *ISO 22398:2013 Societal security — Guidelines for exercises and testing*. Standard. Geneva, CH: International Organization for Standardization, Mar. 2013.

- [40] J. Rasmussen. "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models." In: *IEEE transactions on systems, man, and cybernetics* 3 (1983), pp. 257–266.
- [41] T. Grant and B. Kooter. "Comparing OODA & other models as operational view C2 architecture." In: *Proceedings of the 10th International Command and Control Research Technology Symposium*. 2005.
- [42] C. Eagle. "Using Capture the Flag Events as Training Opportunities." In: *Hitachi Review* 63.5 (2014), pp. 1–92.
- [43] *Kaspersky Interactive Protection Simulation*. 2017. URL: http://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf.
- [44] URL: <http://www.kaspersky.com/industrial-security-cip>.
- [45] *Introducing the Activities of Control System Security Center(CSSC)*. 2016. URL: http://www.css-center.or.jp/pdf/about_cssc_en.pdf.
- [46] *About Control System Security Center*. URL: <http://www.css-center.or.jp/ja/info/presentation.html>.
- [47] NISCchannel. *Enhancement of IT incident response capabilities in Critical Information Infrastructure (CII)*. 2016. URL: <https://www.youtube.com/watch?v=FL5CPiXXc3A>.
- [48] K. Watanabe. "Developing public–private partnership based business continuity management for increased community resilience." In: *Journal of Business Continuity & Emergency Planning* 3.4 (2009), pp. 335–344.
- [49] D. Noyes. "Cyber Security Testing and Training Programs for Industrial Control Systems." In: *Idaho National Laboratory (United States). Funding organisation: US Department of Energy (United States)* (2012).
- [50] E. Sitnikova, E. Foo, and R. B. Vaughn. "The power of hands-on exercises in SCADA cyber security education." In: *IFIP World Conference on Information Security Education*. Springer. 2009, pp. 83–94.
- [51] L. Martin. "Cyber kill chain®." In: URL: http://cyber.lockheed-martin.com/hubfs/Gaining_the_Advantage_Cyber_Kill_Chain.pdf (2014).
- [52] N. A. E. R. Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. 2010.
- [53] D. Kuipers and M. Fabro. *Control systems cyber security: Defense in depth strategies*. Tech. rep. Idaho National Laboratory (INL), 2006.

- [54] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne. "Vulnerabilities of Wireless Security protocols (WEP and WPA2)." In: *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 1.2 (2012), pp. 34–38.
- [55] J. Bergström, K. Petersen, and N. Dahlström. "Securing Organizational Resilience in Escalating Situations Development of skills for crisis and disaster management." In: *Proceedings of the third Resilience Engineering Symposium*. 2008, pp. 11–17.
- [56] J. LaPiedra. "The Information Security Process: Prevention, Detection and Response." In: *SANS Institute: Information Security Reading Room 20* (2001).
- [57] D. Murdoch. *Blue Team handbook: incident response edition: a condensed field guide for the cyber security incident responder*. CreateSpace Independent Publishing, 2014.
- [58] D. D. Woods and E. Hollnagel. *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC Press, 2005.
- [59] H. Palmqvist, J. Bergström, and E. Henriqson. "How to assess team performance in terms of control: a protocol based on cognitive systems engineering." In: *Cognition, Technology & Work* 14.4 (2012), pp. 337–353.
- [60] T. Aoyama, k. Watanabe, I. Koshijima, and Y. Hashimoto. "Developing ICS Security Training for Resilient Cyber Incident Management." In: *Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes (PSE Asia 2016)* (July 2016).
- [61] J. Borell and K. Eriksson. "Learning effectiveness of discussion-based crisis management exercises." In: *International Journal of Disaster Risk Reduction* 5 (2013), pp. 28–37.
- [62] US Department of Homeland Security and United States of America. *Homeland security exercise and evaluation program (HSEEP) volume I: HSEEP overview and exercise program management*. 2007.
- [63] H. Takagi, T. Morita, M. Matta, H. Moritani, T. Hamaguchi, S. Jing, I. Koshijima, and Y. Hashimoto. "Strategic security protection for industrial control systems." In: *2015 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. IEEE. 2015, pp. 986–992.
- [64] Y. Sheffi and J. B. Rice Jr. "A supply chain view of the resilient enterprise." In: *MIT Sloan management review* 47.1 (2005), p. 41.
- [65] G. A. Bigley and K. H. Roberts. "The incident command system: High-reliability organizing for complex and volatile task environments." In: *Academy of Management Journal* 44.6 (2001), pp. 1281–1299.

- [66] S. Converse, J. Cannon-Bowers, and E. Salas. "Shared mental models in expert team decision making." In: *Individual and group decision making: Current issues* 221 (1993).
- [67] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale. "Exploring a national cybersecurity exercise for universities." In: *IEEE Security & Privacy* 3.5 (2005), pp. 27–33.
- [68] R. Shumba. "Towards a more effective way of teaching a cybersecurity basics course." In: *ACM SIGCSE Bulletin*. Vol. 36. 4. ACM. 2004, pp. 108–111.
- [69] B. Lété and P. Pernik. *EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. German Marshall Fund of the United States, 2017.
- [70] F. B. Hare. "Private sector contributions to national cyber security: A preliminary analysis." In: *Journal of Homeland Security and Emergency Management* 6.1 (2009).
- [71] D. S. Henshel, G. M. Deckard, B. Lufkin, N. Buchler, B. Hoffman, P. Rajivan, and S. Collman. "Predicting proficiency in cyber defense team exercises." In: *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE. 2016, pp. 776–781.
- [72] E. Seker and H. H. Ozbenli. "The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation." In: *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE. 2018, pp. 1–9.
- [73] R. Ottis. "Light weight tabletop exercise for cybersecurity education." In: *Journal of Homeland Security and Emergency Management* 11.4 (2014), pp. 579–592.
- [74] A. Brilingaitė, L. Bukauskas, V. Krinickij, and E. Kutka. "Environment for cybersecurity tabletop exercises." In: *ECGBL 2017 11th European Conference on Game-Based Learning*. Academic Conferences and publishing limited. 2017, pp. 47–55.