Cross-ministerial Strategic Innovation Promotion Program (SIP)

Nagoya Institute of Technology

3-4 Programs of Human Resources Development for Improving Organizational Incident Response Ability

Social implementation technologies

Proposal for an exercise system for achieving highly resilient organizational collaboration for response to unexpected and unavoidable cyber incidents

What is organizational collaboration required for responses to cyber incidents?

- •Taking measures as an organization rather than calling for a superhero
- •Increase in the ability of a response to unexpected incidents on the assumption that not all incidents can be avoided
- •Multilayered versatile security measures for preventing complete disruption although part of the infrastructure is damaged
- •Collapse of business continuity is caused by all related AND conditions (in many cases of concerned parties)
- •What should be done in an emergency is shutting down the communication and performing manual operation independent of automatic systems.
  - •The instruments are configured to secure safety in case an incident is noticed and a response is initiated.
  - •When and where to shut down for localizing the damage and achieving early recovery?
  - •What kind of detection is required to shut down the communication and what actions should be taken after shutdown?
  - •If communication shutdown enables business continuity, early shutdown is a possible option.
- •OT for risk management of the operational systems and response to on-spot accidents
  IT is the core for monitoring the communication systems and tool management.

⇒ Repeat exercises (simulated experiences) with which required collaboration can be visualized.

Increase in resilience is important

Consideration from safety viewpoints

- ・Safety- Ⅰ Ability to not cause accidents
- ・Safety- Ⅱ Ability to suppress unexpected accidents
  Resilience

A cyberattack is one of the causes of security compromise

- • Impossible to assume all methods of cyber attacks
  (Vulnerabilities are also invented by attackers)
- • Even if a risk source is cyber attack, an incident that occurs depends on the control target.

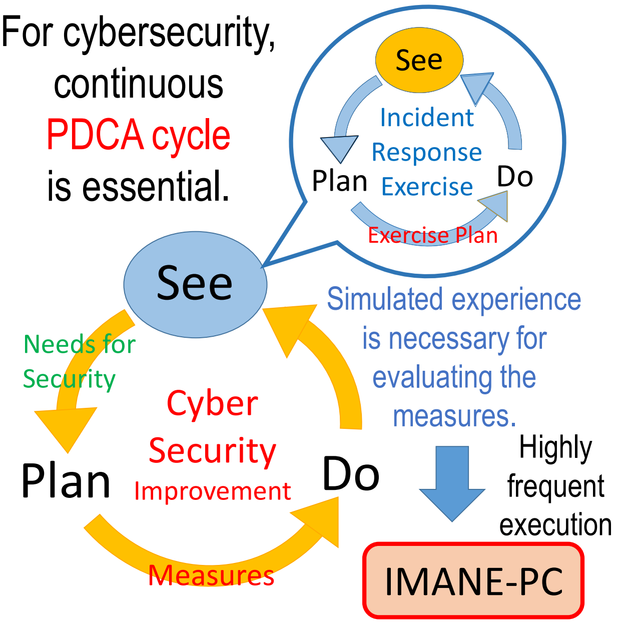
⬇

Assign personnel who can become aware of unexpected attacks and establish an organizational system that can lead the awareness to optimal measures.

⬇

To become aware of unexpected incidents, imagination is important. Simulated experiences (exercises) using multiple scenario are effective.

For cybersecurity, continuous PDCA cycle is essential.



We have developed the exercise for understanding organizational collaboration, **IMANE (Incident MANagement Exercise) series**.

EX-1: IMANE-DEMO	Exercise for making those who do not want to participate become involved
EX-2: IMANE-CARD	Exercise for sharing problem awareness on the spot without requiring preparation for the exercise
EX-3: IMANE-PC	Exercise for experiencing the simulated organizational collaboration using computers

T-1: IMANE-DRAW	Tool for editing scenarios for incident exercises and synthesizing data for CARD and PC
T-2: IMANE-DB	Database for data for implementing IMANE-PC and for accumulation and search of the implementation results

Cross-ministerial Strategic Innovation Promotion Program (SIP)

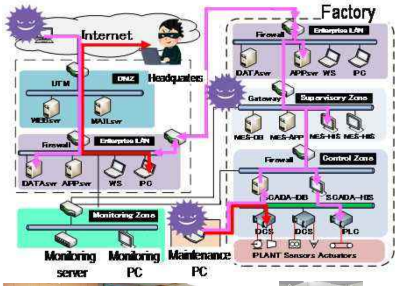
Nagoya Institute of Technology

3-4 Programs of Human Resources Development for Improving Organizational Incident Response Ability

Developed exercise system, IMANE (Incident MANagement Exercise)

IMANE-DEMO

- Build a control system to understand the structure.
- Attack the built control system by themselves using Kali Linux.
- Monitor the communication under the situation of being attacked, and consider how to defend against the attack when it is detected.

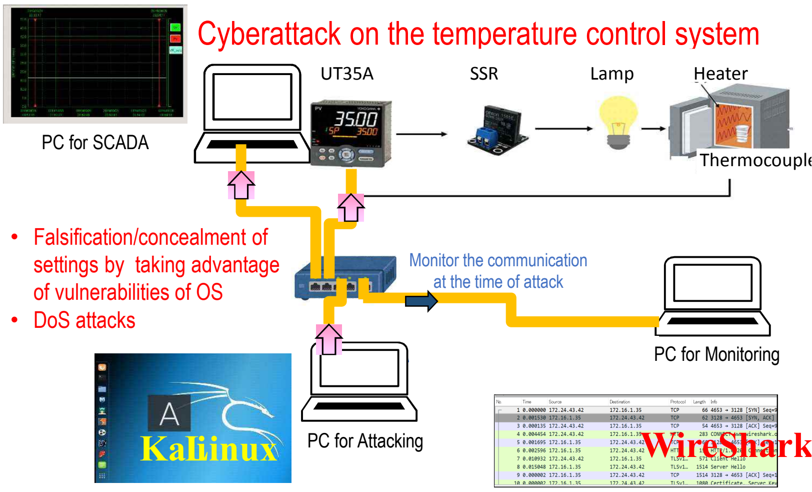


Understand that once the control network is compromised, not only SCADA and local controllers can be operated by the attacker but also unnoticed attacks can be launched, and that attacks can be visible when monitoring the communications.

Control Room

Local Control

Plant.



Cyberattack on the temperature control system

- Falsification/concealment of settings by taking advantage of vulnerabilities of OS
- DoS attacks

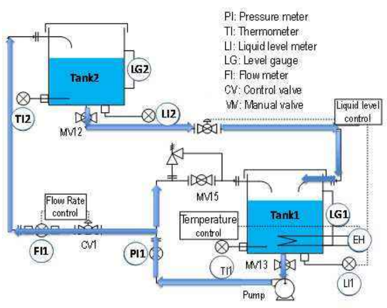
Feasible with only three PCs, one controller, and HUB.

IMANE-CARD

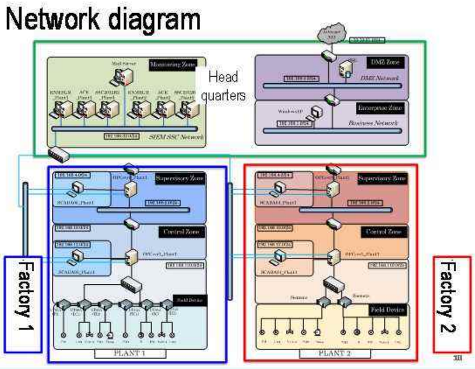
(i) Check the incident response system for the exercise.

(Unnecessary when the participants understand the role through the office’s scenario)

･Check the plant and organization to protect and the network structure.



Network diagram



(ii) Check the flow of responses to incidents for the exercise.

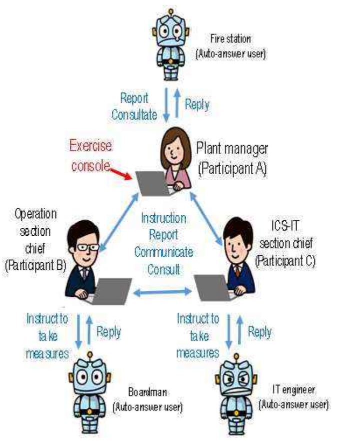
Unnecessary when the participants understand the role through the incident scenario.

Discuss what the situation is and what collaboration is necessary while placing cards.

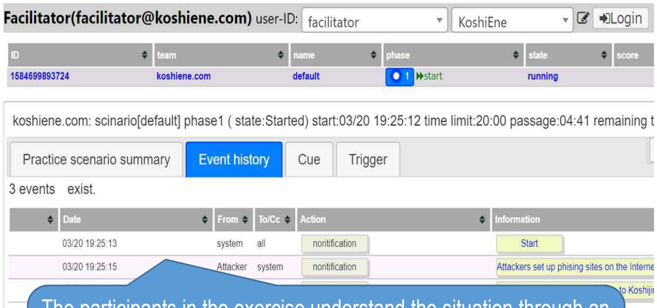
This is not about how correctly the cards are placed, but about how extensively to visualize the situation in the event of an incident by placing the cards while checking the content.

IMANE-PC

(i) Exercise using a computer



Exercise console



Facilitator(facilitator@koshiene.com) user-ID: facilitator ▾ KoshiEne ▾ Login

ID	team	name	phase	state	score
1584699893724	koshiene.com	default	1 start	running	

koshiene.com: scinario[default] phase1 (state:Started) start:03/20 19:25:12 time limit:20:00 passage:04:41 remaining t

3 events exist.

	Date	From	To/Cc	Action	Information
	03/20 19:25:13	system	all	noritification	Start
	03/20 19:25:15	Attacker	system	noritification	Attackers set up phising sites on the Interne
					to Koshiji

The participants in the exercise understand the situation through an email-like screen by which they can proceed with the exercise after selecting items from menus, entering text, and communicating with concerned parties including auto-answer.

The human interface is simple, which therefore is likely to fit a variety of types of offices and scenarios and be able to provide more exercise opportunities.
It is possible to review the exercise immediately after performing it based on specific activities.

Exercise scene

(Quiet exercise time – keyboard typing sound only)

(Review the exercise immediately after performing it)