Environmental improvements for developing operation technicians who have gained knowledge regarding security at a provider of critical infrastructure

**Characteristics**

1. Scalable development of human resources
   - Curriculum and guidelines corresponding to each operation site (human resource development curriculum).
   - Shareable lecture and practice materials that cover everything from awareness to basic knowledge, handling, countermeasures, and reports (lecture and practice materials).

2. Continuous human resources development
   - A flexible learning environment is implemented (e-learning system).
   - Shapes a community in which trained workers constantly acquire the latest information in order to be able to acquire response capabilities (community formation support system).

**Overview**

1. R&D of curriculum
   - From awareness, to basic knowledge, handling, countermeasures, and reports.

2. R&D of learning and lecture materials
   - Customized curriculum A
   - Customized curriculum B
   - Ability checking

3. e-learning system
   - Flexible learning environment
   - Understanding of progress

4. Community
   - Interchange of the newest technology
   - Self-learning environments

**Types of Workers and Development Model**

- **Top leaders**
  - About 100 people
- **Leaders, instructors**
  - About 1,000 people
- **Core engineers**
  - About 10,000 people
- **General engineers**
  - About 100,000 people

Creating shareable lecture and exercise materials that can train about 1,000 leaders and instructors

**Curriculum**

- **Mechanism for implementing teaching that suits each environment**

- **Training of human resources**
  - Guidelines
  - Guidelines
  - Guidelines
  - Guidelines
  - Customized materials
  - Customized materials
  - Customized materials
  - Customized materials
  - Teaching materials
  - Teaching materials
  - Teaching materials
  - Teaching materials

- **Curriculum**

**Implementation Status**

In 2016, guidelines were created as R&D of curriculum.
Also, four types of exercises were attempted as R&D of the teaching materials for lectures, and hearing surveys from students and the like were implemented.

**Schedule**

By the end of FY2018, there are plans to create a learning curriculum for leaders and instructions and shareable lecture and exercise materials.
In 2020, curricula, lecture and practice materials, e-learning systems, and environments for community formation support systems and the like will be prepared, with the aim to realize the TOP plan by making it possible to continuously develop human resources in each organization after the year 2020 as well.
### Development of Curriculum

- Creating guidelines
  - Reference textbooks
    - Power control system security guidelines (Japan Electric Association)
    - Smart meter system security guidelines (Japan Electric Association)
  - Guidance procedures
    - How are textbooks used for teaching?
    - Facilitation of practice and the like
    - Examples students are familiar with
  - Broad view and concentrated view
    - Ability to anticipate the entire system from a broad view
    - Detailed knowledge of each problem
  - Image of human resources
    - Security management
    - Incident handlers
    - Incident response

### Implementation Status of Trial Exercises (1)

- Wireless LAN security exercises
  - Date of implementation: August 2, 2016
  - Venue: Hiyoshi Campus, Keio University
  - Number of students: 5
  - Summary: Cracks and coping strategies of WEP utilizing tools for wireless LAN devices

- System attacks/defense exercises
  - Date of implementation: August 3, 2016
  - Venue: Hiyoshi Campus, Keio University
  - Number of students: 11
  - Summary: Attacks against systems using buffer overflow and the coping strategies thereof

### Implementation Status of Trial Exercises (2)

- Exercises of incident response and CSIRT fundamentals
  - Date of implementation: August 4, 2016
  - Venue: Institute of Information Security
  - Number of students: 9
  - Summary: Launching of CSIRT and basics of security incident response

- Industrial Control System Security Workshop for CSIRT
  - Date: Sept. 27, 2016
  - Venue: Bld. No.16, Nagoya Institute of Technology
  - Participant: 30 managers and experts
  - Overview: Basic training of cyber incident response connected with field operations to keep the safety of critical infrastructures

### Summary of Practice

Hands-on practice regarding attacks (wireless LAN security, defense against system attacks)

- The majority of participants are not in charge of the contents of exercises
- However, participants have answered that it is beneficial to be knowledgeable about the vulnerabilities of access technology, wireless technologies, and the perspectives of attacks, even for items for which they are not directly in charge of
- Also, many participants said that they were able to concretely experience vulnerabilities from mere knowledge by executing specific attacks
- In general, there is a large need for comprehensively learning about many attack methods and the coping methods thereof
- Incident Response Exercise
- As a reference for building and operating CSIRT/SOC, satisfaction of participants is very high.
- The exercise framework is highly valued as being useful for organization construction and manual development

### Countermeasures should be considered based on protecting targets, not on cyber attack methods

A cyber attack comes up with new vulnerabilities, even if it is predicted. A cyber attack to ICS is considered as a malicious operation or malfunction. Fail-Safe and Fool-Proof, that are conventional safety measures, should be thoroughly effective for cyber attacks. Practical tactics against cyber attack should be prepared based on safety assessments. Even if an attack can be detected at an early stage, when the detectors take a time to confirm it, the damage of the attack becomes serious and the recovery will be prolonged. Collaboration with internal and external organizations is important for emergency response.

### Customization of Cyber Exercise for each Business Sector

In critical infrastructures, accidents caused by cyber attacks differ depending on business operations, such as railway, electric power, and broadcasting.

A person who knows what to protect against attacks should make a practical plan and practice it.

It is necessary to develop an exercise template for each business sector and train personnel capable of customizing the template in his/her field.

Our proposed template allows us to assign undergraduate students as the exercise facilitators.