

# Training of Cybersecurity Human Resources to Support Future Social Development

● Masayuki Okuhara ● Kosetsu Kayama ● Tomohiko Mimura ● Takuya Suzuki

The training of security engineers with advanced technological capabilities to support future social development is a key issue, both in Japan and overseas. Securing and developing such human resources requires the formation of an ecosystem where organizations can cooperate broadly beyond corporate boundaries with the industrial world, public bodies, and educational institutions. Up until now, Fujitsu has trained security engineers in collaboration with various organizations. Examples include the establishment of the Fujitsu Specialist Training Research Division at Kyushu University, participation in the task of defining security human resources by the Cross-Sector Forum for Cybersecurity Workforce Development, and a hands-on seminar held jointly with Ehime University and Ehime Prefectural Police. This paper describes these three initiatives for training security engineers in collaboration with these organizations, and the results achieved.

## 1. Introduction

The training of security engineers with advanced technological capabilities is a key issue both in Japan and overseas. In Japan, the IT Skill Standard<sup>1)</sup> formulated jointly by the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency (IPA) states, "Companies should secure the human resources that will play a role in formulating and promoting information security strategies (measures) as part of their own corporate strategy and IT strategy, by methods such as training." In conjunction with the above, a scheme for the certification of information processing technicians, The Information Technology Engineers Examination, has been established.

The Fujitsu Group has defined its own human resource model, which is applicable both in Japan and abroad, using as reference existing human resource models in Japan and abroad. This human resource model defines roles and required skills with reference to the activities of people actually engaged in business within the Fujitsu Group in addition to the existing know-how of engineer skill models both in and outside Japan, and thus its definitions of human resources are predicated on actual practice. Furthermore, operation of the "Fujitsu Security Meister Certification System,"

which certifies security engineers' skills based on the above human resource model, began in 2014.<sup>2)</sup> Under this system, more than 4,900 security engineers have been certified as of September 2019, and the goal is to train and certify 11,000 engineers by the end of FY2021.

However, securing and developing such security engineers requires the creation of an ecosystem, i.e. a cycle for the continuous formation, hiring, and utilization of human resources, where organizations can cooperate broadly beyond corporate boundaries with the industrial world, public bodies, and educational institutions.

One of the reasons for this is that such an ecosystem is needed to raise awareness of security technology among the young people who have the potential to become security engineers in the future. According to a report from the National Public Safety Commission et al.,<sup>3)</sup> the number of persons arrested for violating laws prohibiting unauthorized access has been increasing year by year, particularly for 14- to 19-year-olds. It has been pointed out that many of the arrested cybercriminals obtained their knowledge on their own.<sup>4),5)</sup>

At the root of this problem is the danger that young people driven by curiosity can acquire on their

own skills that can then easily be used to commit crimes. This situation arises from the fact that the wealth of information freely available on the Internet allows people to acquire skills without the counterbalance of knowledge of laws, regulations, and morals, resulting in the undetected creation of a talent pool for cybercrime. To remedy this, it is necessary to involve young people early on in the society-wide ecosystem of security engineer development.

This paper describes the discovery and development of cybersecurity human resources, which the Fujitsu Group does through collaboration with organizations outside the Fujitsu Group, such as the industrial world, public bodies, and educational institutions. Additionally, as specific examples thereof, it introduces engineer development activities in collaboration with Kyushu University, the Cross-Sector Forum for Cybersecurity Workforce Development, and Ehime University and Ehime Prefectural Police.

## 2. Collaboration with Kyushu University

This section introduces the initiatives of the Fujitsu Specialist Training Research Division, which was established within the Kyushu University Cyber Security Center for developing cybersecurity human resources.

### 2.1 The Fujitsu Specialist Training Research Division

Kyushu University established the Cybersecurity Center in December 2014, and since then has been actively working on education and research for strengthening cybersecurity measures as roles that universities should take on. In particular, research and development, as well as the implementation, of educational courses that explain the basics of cybersecurity to students at all departments contribute to broadly raising the level of cybersecurity response capabilities.

In June 2016, the Fujitsu Specialist Training Research Division was established within the Cybersecurity Center with the contribution from Fujitsu. This research division is working to establish an education model for human resource development through the creation of educational methods related to cybersecurity and research and development of applied teaching materials. On the research side, we carry out R&D on frameworks and practical applications to create a safe cyberspace.

### 2.2 Aims of the Fujitsu Specialist Training Research Division

By establishing the Fujitsu Specialist Training Research Division (hereafter, Research Division), Fujitsu aims to further boost the cybersecurity research activities of Kyushu University and based on that accelerate the development of security human resources. In addition, Fujitsu aims also to raise the level of its security response capabilities by utilizing the educational methods, education models for human resource development, and educational effect assessment methods developed by the Research Division to train our own engineers. This will also allow us to provide applied examples of education models in companies to Kyushu University.

### 2.3 Initiatives to date

The Research Division has been offering courses designed to develop security human resources since October 2016. The major courses on offer are outlined below.

#### 1) Basic theory of cybersecurity

This is a basic education course on cybersecurity that is offered in common to all the departments of Kyushu University. The aim of this course is acquisition of the basics of cybersecurity in order to play an active role in the ICT society of the future. This course is available to all students, regardless of major and school year. Students cover a lot of ground, from basics such as password management and data management for familiar devices such as personal computers and smartphones, to laws and ethics. A total of 350 to 400 students take this course (offered as two classes) each year.

#### 2) Security engineering training

This course is aimed at students interested in digital manufacturing teaches about security engineering practices. In this course, students learn about the risk of cyber attacks on servers, networks, etc., and the need for protection.

In the section on IoT security, students can experience cyber attack methods and how to protect against them while also experiencing manufacturing that uses IoT. This course is offered to approximately 40 students at a time. **Figure 1** shows some of the training material used in this course. Students can learn about attack and protection methods for Wi-Fi routers, IoT devices, data collection servers, and the like, while programming self-running robots equipped with IoT devices



\* Uses Raspberry Pi (single board computer).

**Figure 1**  
Security training material.

such as sensors.

### 3) enPiT and enPiT-Pro PBL training

enPiT, which stands for Education Network for Practical Information Technologies, is an educational project started by Japan's Ministry of Education, Culture, Sports, Science and Technology in 2018 that consists of four fields: big data/AI, security, embedded systems, and business system design. As a university that is linked to the security sector, Kyushu University conducts project-based learning (PBL) training.<sup>6)</sup>

PBL training, which teaches the practice of security engineering, is available also to students from other universities besides Kyushu University. It is offered as a short-term intensive course, and like the security engineering training, it allows students to get hands-on experience with both security-related fabrication and cybersecurity.

For working people, we offer graduate-level courses as enPiT-Pro PBL training.<sup>7)</sup>

### 4) Information security education and training for teachers

The Research Division has been conducting e-learning courses on information security for all faculty members at the university since 2017. The content of the courses and verification tests includes incidents that tend to occur to teachers, taken from actual on-campus security incidents.

Drills for dealing with targeted attack emails are also run. These drills allow faculty members to experience actual targeted attacks by incorporating content

of malicious emails that have actually been sent to Kyushu University. As a result, whether links and attachments of malicious emails have been opened can be checked, and anyone who opens them receives cautions and the like as feedback. Both the education and the training content are designed to strengthen awareness about information security through the provision of meaningful on-point feedback to the participants.

## 2.4 Future initiatives

The Research Division aims to establish an education model for the development of security human resources through the creation of educational methods related to security and research and development of applied teaching materials. Going forward, it will work in collaboration with Kyushu University to develop, among other things, a system that supports education through the visualization of education effectiveness.

## 3. Collaboration with Cross-Sector Forum for Cybersecurity Workforce Development

This section describes the initiatives of the Cross-Sector Forum for Cybersecurity Workforce Development (hereafter, the Forum), which operates across industry boundaries and in which Fujitsu participates as a member.

### 3.1 Overview of the Forum

In February 2015, the Japan Business Federation released its "Proposal for Reinforcing Cybersecurity Measures."<sup>8)</sup> Human resource development was one of the issues that were emphasized in this proposal. In June 2015, the Forum was established as a forum for actually considering this issue. About 50 companies, consisting mainly of major companies in each industry and concentrated in important infrastructure fields, participate in the Committee.

### 3.2 Necessity of a cross-industry approach

In recent years, the activities of Information Sharing and Analysis Center (ISAC), which aims to share information on cybersecurity among private sector companies in the same industry and improve their ability to respond to cyber attacks, are gaining momentum. On the other hand, as every company and every thing is connected to networks, the scope of what needs to be

protected for each industry and company is expanding. The abundance of attack targets increasingly attracts interest from attackers around the world and motivates them to launch attacks, and a sense of crisis is rapidly spreading throughout the industrial world.

Thus, boosting security response capabilities throughout the industrial world and across industry and corporate boundaries is essential as a security measure. To achieve this, it is important to build cooperation systems for the industrial world, promote information sharing, and develop human resources capable of responding to new issues.

### 3.3 Promotion of industry-government-academia collaboration & cybersecurity seminars for students

By providing its various reference materials not only to industry but also to national and local governments, universities, and research institutions, the Committee aims to bring about more effective industry-academia-government collaboration. The following is an example of collaboration with universities and research institutions.

To increase the number of employees involved in security in the future, it is important to provide more students with opportunities to gain experience with the security required for ICT and get them interested in security. To this end, the Committee called out to universities with at least some interest in cybersecurity all over Japan and held seminars for students. The purpose was to present to students paths for becoming cybersecurity specialist, by introducing technical trends and the types of work done by security engineers active on the front lines. A survey conducted after the seminars found that 80% of the students felt that they were a good opportunity for getting interested in cybersecurity.

## 4. Human resource development activities in collaboration with Ehime University and Ehime Prefectural Police

In collaboration with Ehime University and Ehime Prefectural Police, Fujitsu runs security engineer development activities aimed mainly at young people in Ehime Prefecture. This section describes the Security Symposium Dogo Hands-on Seminar (hereafter, the Dogo

Hands-on Seminar), which is part of these activities.

### 4.1 Overview of the Dogo Hands-on Seminar

As part of the growth process of young people who wish to become security engineers, an appropriate place should be provided where they can experience security technologies. Especially if in their teens, an important period for personality development, young people fail to gain experience with security under good leadership, they risk taking the wrong path, partly out of curiosity. For the development of security engineers who have a sense of ethics, it is important to continuously provide young people with opportunities for positive hands-on experience with security from a young age.

The Dogo Hands-on Seminar started in 2017. In running this seminar, the aim was to create a place where young people could gain first-hand experience with computers and security so as to develop skills, hone their mind, and grow as persons. To this end, we offered Fujitsu's cyber range CYBERIUM as a virtual space where young people can experience, think, and share in the successes and failures of their predecessors.

Offering such a space only temporarily would be meaningless as success depends on continuous activities that are firmly rooted in the community. It is important that the seniors who grew up through activities in their respective hometowns establish an "intergenerational human resource development cycle" that fosters the next generation, and the Dogo Hands-on Seminar is no exception. Furthermore, young people can experience how wonderful it is to contribute to society through the acquisition of technology, and this can be expected to lead to regional revitalization as they find employment in their hometowns in the future (Figure 2).

### 4.2 Dogo Hands-on Seminar implementation and results

In February 2017, about 70 people including high school students, university students, and working adults participated in a Dogo Hands-on Seminar conducted in Matsuyama, Ehime Prefecture. In this seminar, by hacking a radio-controlled car and creating a program to make it go to the desired location, the

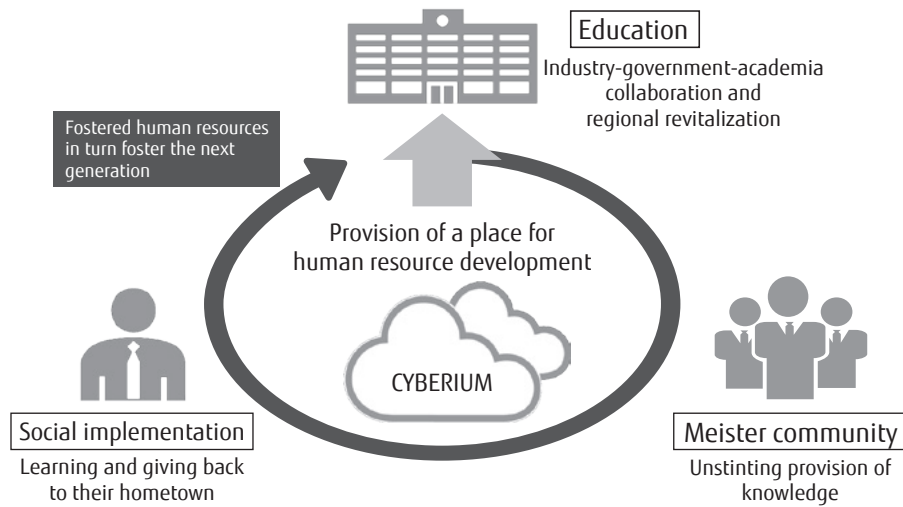


Figure 2  
Intergenerational human resource development cycle.

participants deepened their understanding of network vulnerability and gained first-hand experience of security technology.

According to a survey taken by the participants after this hands-on seminar, 98% of respondents said that this event gave them the opportunity to experience hands on security technology, indicating that the initiative was well received.

## 5. Conclusion

This paper described initiatives for the discovery and development of cybersecurity human resources by Fujitsu in collaboration with organizations outside the Fujitsu Group, such as industry associations and educational institutions.

In such manner, wide-ranging collaborations can form an ecosystem for the development of security engineer human resources. Fujitsu will continue to contribute to society through collaboration with many parties for the development of security engineers.

-----  
All company or products names mentioned herein are trademarks or registered trademarks of their respective owners.

## References

1) Information-technology Promotion Agency: Final Report on Survey of Needs and Issues on Information Security

Formation for IT Personnel (Detailed Version). March 2014 (in Japanese).

<https://www.ipa.go.jp/files/000039527.pdf>

2) K. Kayama et al.: Practice of Training Security Engineers Desired in Cyber Society. FUJITSU Sci. Tech. J., Vol. 52, No. 3, pp. 85–91 (2017).

<https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-3/paper13.pdf>

3) Minister of Economy, Trade and Industry: Reports of Status of the Occurrence of Acts of Unauthorized Computer Access, and Progress of Research and Development on Technology relating to Access Control Features Are Compiled. March 2018.

[https://www.meti.go.jp/english/press/2018/0322\\_001.html](https://www.meti.go.jp/english/press/2018/0322_001.html)

4) ITmedia NEWS: 17-Year-Old Compromises Education System with Attack Program Used for Illegal Access, Minister of Education, Culture, Sports, Science and Technology Hase “A Little Surprised by Ability.” (in Japanese).

<http://www.itmedia.co.jp/news/articles/1606/30/news092.html>

5) The Saga Shimbun: Miyazaki Prefectural Police: Third-year high-school student suspected of creating virus, self-taught.

<https://www.saga-s.co.jp/articles/-/79161>

6) Kyushu University: enPiT-Security—An advanced technology human resources development project that supports Society 5.0. (in Japanese).

<https://cs.kyushu-u.ac.jp/enpit2/>

- 7) Kyushu University: enPIT-Pro—Creation of a training base for information technology human resources that support growth fields. (in Japanese).  
<https://cs.kyushu-u.ac.jp/enpit-pro/>
- 8) Japan Business Federation: Proposal for Reinforcing Cybersecurity Measures.  
<https://www.keidanren.or.jp/en/policy/2015/017.html>



**Masayuki Okuhara**

*Fujitsu Ltd.*

Mr. Okuhara is currently engaged in cybersecurity human resources strategic planning.



**Kosetsu Kayama**

*Fujitsu Ltd.*

Mr. Kayama is currently engaged in cybersecurity human resources strategic planning.



**Tomohiko Mimura**

*Fujitsu Ltd.*

Mr. Mimura is currently engaged in cybersecurity human resources strategic planning.



**Takuya Suzuki**

*Fujitsu Ltd.*

Mr. Suzuki is currently engaged in security-related international standard strategy work.