Practice of Training Security Engineers Desired in Cyber Society

● Kosetsu Kayama ● Shinichiro Yamashita ● Masayuki Okuhara

The training of security engineers with advanced technical skills has been a key issue both in Japan and overseas and various reference models have been proposed for it. Meanwhile, for vendors of information and communications technology (ICT) with a wide variety of security-related operations in their corporate group, such as Fujitsu, it was difficult to use the conventional models for security engineers, as they were, in the systematic training of engineers with skills required to perform these operations. Accordingly, Fujitsu defined its original program for the human resources of security engineers, called Security Meister, and started implementing a human resource certification system based on it in January 2014. In addition to the security division, we have formulated models for security engineers including those for systems development, ICT operation, corporate and other divisions. They can be used to define human resources required for the respective divisions, discover human resources and provide training programs. This paper presents the details of the activities in the respective organizations based on these human resource models and the results.

1. Introduction

Training security engineers with advanced technical skills has been a key issue for some time both in Japan and overseas.

In Japan, the Skill Standards for IT Professionals (ITSS)[1] has been developed by the Ministry of Economy, Trade and Industry (METI) and the Information-Technology Promotion Agency, Japan (IPA). It states that, as part of business and IT strategies, companies need to provide training opportunities to secure personnel dedicated to planning and operating information security strategies (measures), and they have prepared and been operating a systematic certification scheme, the Information Technology Engineers Examination (ITEE).

In the USA, the National Institute of Standards and Technology (NIST) has developed a training program on cyber security, the National Initiative For Cybersecurity Education (NICE), in response to the White House Cyberspace Policy Review, June 2009.[2] This program offers a structural framework for skill development based on the National Cybersecurity Workforce Framework.[3]

As globally recognized standards, the International Information Systems Security Certification Consortium[4] provides a program, the Certified Information Systems Security Professional (CISSP), which has been certified with the American National Standards Institute (ANSI) ISO/IEC 17024. Major businesses in healthcare services and other major industries make it mandatory that their information security staff have this CISSP. As of March 2015, there are 97,000 CISSP holders across the world.

These institutions among others provide reference models for security engineers with the level of competence required of today's cyber society, and the models are playing a significant part in ensuring safety and security in society. Meanwhile, some vendors in information and communications technology (ICT), such as Fujitsu, perform diverse security-related tasks within their corporate groups. Training engineers to acquire the required skills in these operations would need something more than what the conventional training model of security engineers can offer. The reasons are as follows.

1) ITSS and CISSP are formulated inclusively for all

levels of security engineers, lacking detailed schemes for developing various skills required in practice.

2) NICE has developed well-formulated skill categories, which would bypass the problem just mentioned, but the definitions are based on a U.S. business model, and so there are some difficulties in applying it in a Japanese context.

3) The business management require certain information to make business decisions, and someone needs to convey this, bridging between the management and on-site reality. Thus, training programs must cater to the different elements required in security engineers for different work sites.

For these reasons, Fujitsu developed its own program for training security engineers, drawing on those existing models. We made this applicable both in Japan and abroad. Fujitsu thus established a unique certification scheme, a program called Security Meister, based on this model, and started operating it in 2014. In this paper, we explain the concepts in the ideal security engineer model, and the operation of the certification program.

2. Model staff as security engineers

It is not only the information and security departments that engage in security-related tasks in a company. In order to competently handle the cyber threats of today, businesses must develop a portfolio of personnel dedicated to the management of these threats, which in turn necessitates a review of the company's overall security practices. For example, it is not sufficient to provide security department staff with high-level training; it is necessary to clarify the concepts for a capable security engineer for each department within the company, and train them accordingly. Such model staff should also be defined for divisions of systems development, ICT operation and corporate functions. Other staff should be provided with training on not only system operation, legal matters, and business management, but also security issues. This practice will enhance the overall security competence of the company as a whole, and make a significant contribution towards lowering business risks.

To achieve this, Fujitsu developed Security Meister, a program to define and train security engineers competent in unique areas within the Group. The program defines security engineers in three areas and fifteen categories.

Figure 1 illustrates the program. The areas are defined by the degree of involvement in security-specific tasks performed by security engineers. The three areas are High Master, Expert, and Field engineers, where the first has the highest degree of technical involvement.

1) High Master area

Security engineers who have acquired the security competency of the highest level in specific fields. They engage in dealing with sophisticated security threats that change on a daily basis.

2) Expert area

Security engineers who have acquired high security competence, and engage in providing countermeasure solutions against highly sophisticated cyber attacks.

3) Field area

Security engineers who apply high-level security technology in the fields of system development and service operations, serving to ensure safety and security in customers' business operations.

The categories of the staff models provide for different tasks required for different areas. These are prepared by drawing on the established schemes, such as NICE, while taking into consideration Fujitsu's own requirements. These are described in **Table 1**.

These categories give details of the skills, involved tasks, and recommended certifications concerning the security engineers in question. Some considerations have been given to prerequisites such as the attainment of the CISSP in view of the context of globalization. **Figure 2** illustrates the definition for the category of Security Incident Handler. These fine definitions help to develop highly specialized staff concepts, and facilitate the selection of the necessary training programs and their development.

The skills required of engineers in different categories may be grouped into three types: security core, ICT, and non-ICT. They are shown in **Figure 3**. In fact, security engineers need to have not only the skills in security core and ICT, but also skills in areas other than ICT.

For example, in security incident analysis, the engineer needs to consider the information prepared for the business management's decision-making, and

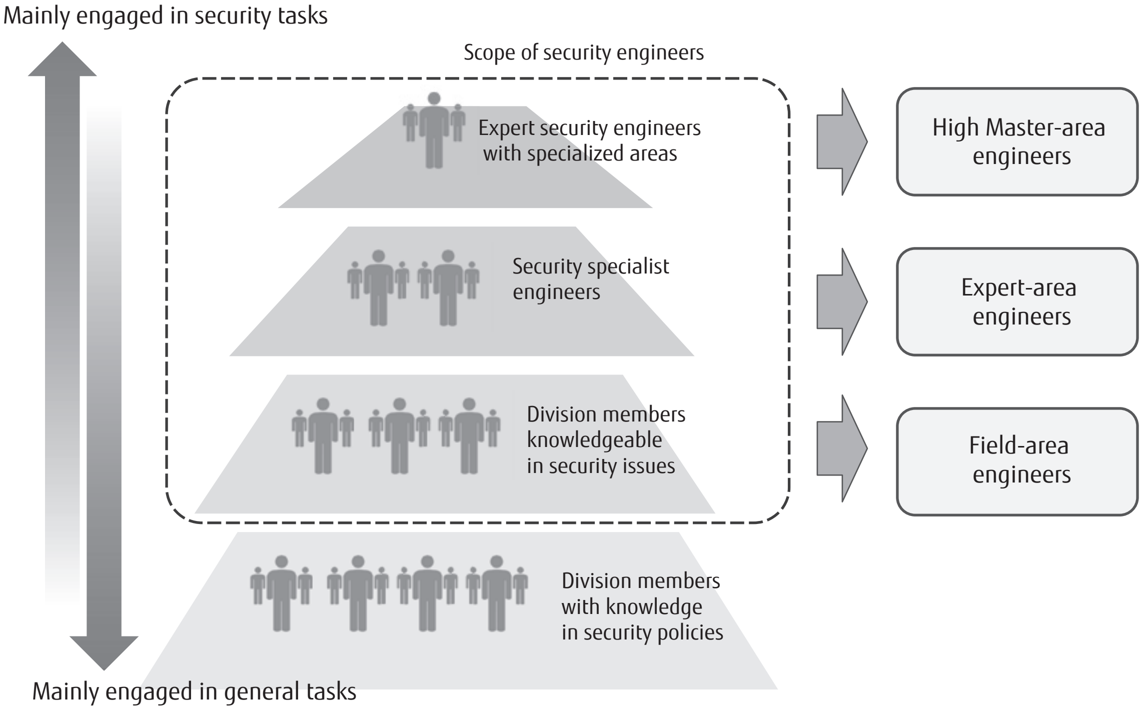

Mainly engaged in security tasks
Scope of security engineers
Expert security engineers with specialized areas
Security specialist engineers
Division members knowledgeable in security issues
Division members with knowledge in security policies
High Master-area engineers
Expert-area engineers
Field-area engineers
Mainly engaged in general tasks

Figure 1
Three engineer areas.

Table 1
Definitions of Security Meister skill categories.

Area	Category
High Master	• Code wizard • Computer wizard • Global white hacker • Senior security coordinator
Expert	• Security product expert • Security network coordinator • Cyber risk assessor • Penetration tester • Cyber researcher • Security analyst • Forensic engineer
Field	• System security engineer • Advanced system security engineer • Security incident handler • Advanced security incident handler

Table 2
Certification processes.

Area	Certification process
High Master	• Document-based assessment • Interview by certified High Master
Expert	• Mandatory external certificates • Mandatory training courses (4 to 7 days) • Document-based assessment
Field	• Mandatory training courses (2 days) • Training completion tests

this requires a well-balanced combination of skills described above.

3. Security Meister Certification Program

In this section, we explain the Security Meister Certification Program. This is a strategic training program for security engineers based on the above-stated model staff concepts and visualized in-group distribution of security engineers with their areas of security skills. The certification processes are described in **Table 2**.

One of the characteristics of this program is that it does not operate assessment tests within the program, unlike many certification programs in general. This is because a testing system would incur a significant cost, which makes it unrealistic for one company to manage. Instead, the program incorporates well-established external certificates such as ITEE and CISSP as prerequisites.

Regarding the High Master area, the nature of the required skills makes it difficult to standardize a

	Engineer description	Skill map	Basic theories		Database	
	Designs a system security operation and undertakes security tasks for the operation in the field from the security operation division		Algorithms and programming		Network	■
			Computer components	■	Security	■■
			System components	■	Service management	■■
			Software	■	System audits	
			Hardware		System strategies	
			Multi-media		Legal	
Main tasks	• Negotiates security operation requirements with customers during the defining stage of system requirements • Defines a system-wide security operation* and decision table during the designing stage of system operation • Checks the operability of designed security operation during the testing phase of the system • Reads log data of OSes, middleware, or other products, and separates and implements temporary measures for suspected security incidents according to the decision table					
Business contribution/ necessity	• Operational service quality (security) enhancement					
Standard skills	• Capable of responding to security inquiries • Capable of developing operational measures against possible security threats • Capable of designing security-sensitive system operation - Understands computer and system components - Understands Internet technology (IPv4, NAT, DNS, Proxy, etc.) - Understands material, technical and human threats against information properties - Understands major attack methods on Web services and threats/countermeasures of such attacks - Understands log data of major OSes, middleware, and other products • Capable of supervising the site affected by a security incident					
Recommended skills	• Obtained certificates of information security specialist or network specialist					

*Definition of log, trigger designing, patch operation design, etc.

Figure 2
Example of engineer areas (Security Incident Handler).

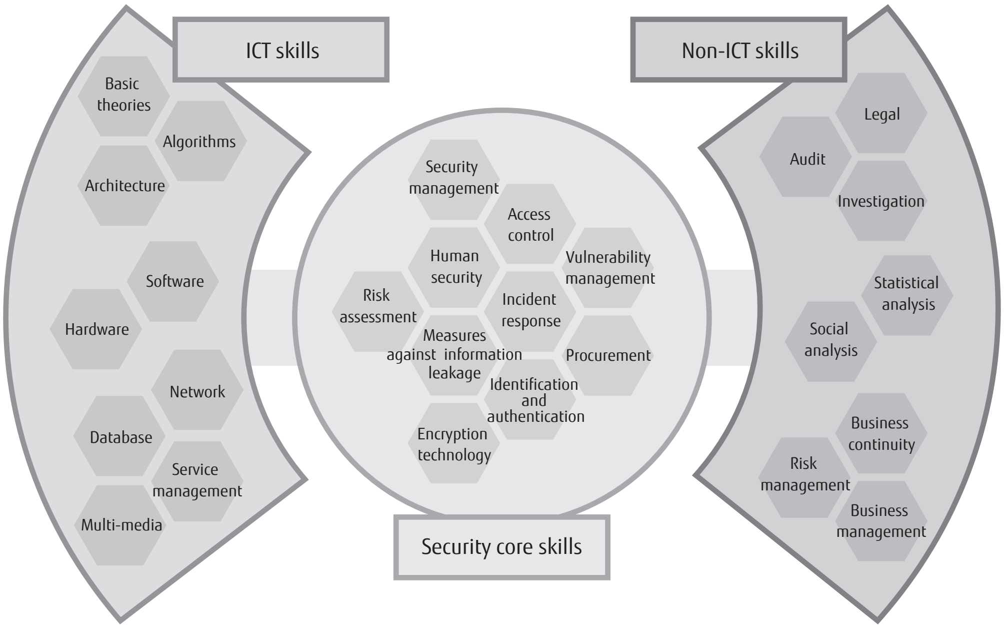


Figure 3
Skills of Fujitsu security engineers.

certification process. Therefore, a mandatory condition has been tentatively adopted, which is an interview by an existing High Master-area engineer. The program design is such that the candidate has to convince the High Master of his/her skills and experience in order to be certified.

Fujitsu has drawn up a plan to train engineers in each area with the following targets, and post them in various sections through a strategic and continued implementation of the program.

- High Masters - 20 people
- Experts - 100 people
- Field engineers - 580 people

These figures are based on the idea that 1 in 40 to 50 out of a total of 27,000 engineers at Fujitsu will become Security Meister-certified engineers. This proportion takes into account a good balance of organizations to accept certified engineers and development of engineers.

As of August 2015, approximately 400 engineers are certified with the Security Meister status, and they work towards developing and implementing cyber attack countermeasures in the field, or enhancing the area of organizational security measures.

4. Discovering and training engineers with potential

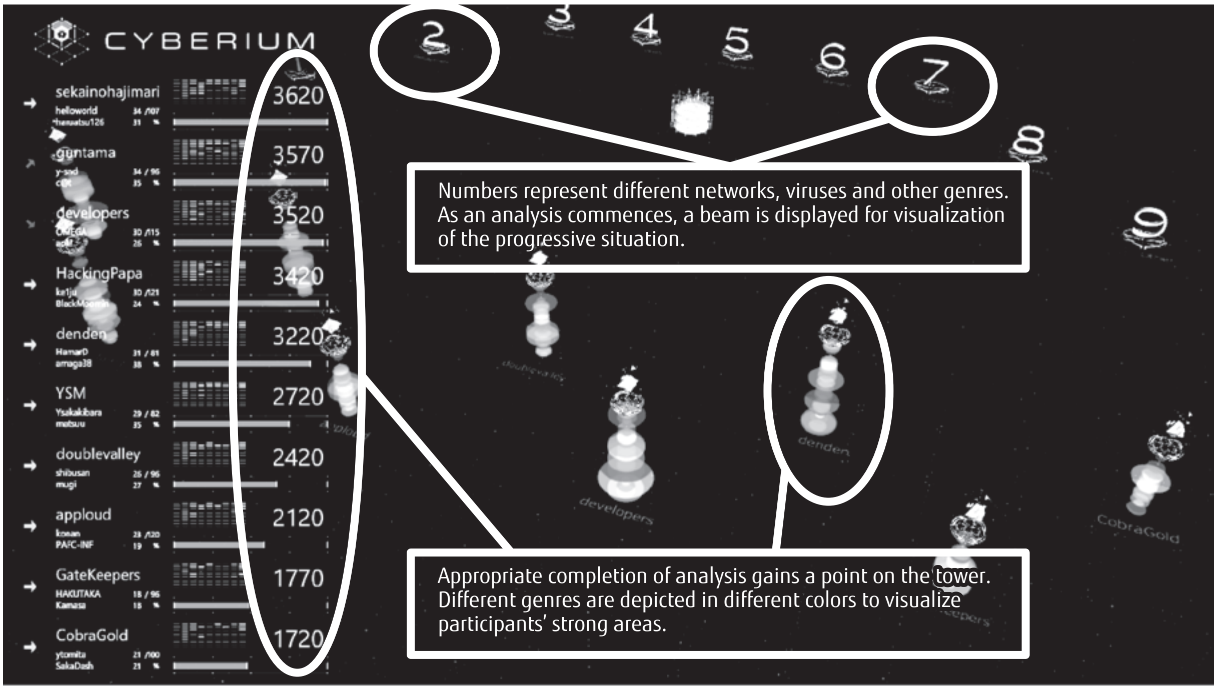
It is expected that the Security Meister Certification Program will help to find people with hidden talent who are capable of performing as security engineers by clarifying the model staff and visualizing the staff distribution according to these concepts. It is often the case that the development division has many members who are skilled and knowledgeable in networks and databases, while those adept at social analysis and risk management are often found in corporate divisions. Conventionally, security engineers would only train the members of their own division. But if engineers with potential abilities in security work are recruited from a cross-departmental perspective, education and training can be pursued more effectively.

In order to find capable members and to increase the number of security engineers, Fujitsu organized a group-wide security contest as part of the certification program. This in-house security contest took the form of a competition called Capture the Flag (CTF), where challenges entailed tasks to identify unauthorized accesses within the network communication. The contest also incorporated a dashboard, as shown in **Figure 4**, which visualizes participants' performance in real time. This helps to elucidate the skills each member has, making it easier to identify engineers with potential. This contest has been held twice a year since 2014. As a result, many skilled persons have been found in places other than the security division, such as the development and corporate divisions, helping to discover people with hidden talent within the Group who are capable of performing as security engineers.

The next step after discovering people with hidden talent is to train them as security engineers, through a program with a focus on practical capabilities. An effective program would provide opportunities for building up experience and attaining an overall understanding of cyber attacks, designed for those whose experience in security operations is not up to the mark compared to their on-site experience.

Thus, we drew on Fujitsu's know-how to develop a program that fully leveraged the practice based on a cyber range (virtual practice field). This is our unique training program for security engineers that combines a simulated environment reconstruction of problematic situations often encountered in the field, and the simulation scenario that postulates high-level attacks. With the practices characterized by the following seven points, the program gives the trainees overall practical experience. They are shown a security incident (network intrusion), and asked to maintain the operational continuity as much as possible, while conducting a series of actions from the initial response through to escalation and closing (completion). This training program is also available to our customers via Fujitsu Learning Media Ltd.

1) General network and server configuration that can be completely reproduced virtually using the virtual environment based on Fujitsu's core technology.
2) Mock experience of attack and defense as well as various verification processes in a simulated real business network environment.
3) Hands-on practice to understand a comprehensive picture of actual attacking tactics and processes.
4) A uniquely developed visual dashboard using 3D graphics helps the program trainees with their



Numbers represent different networks, viruses and other genres. As an analysis commences, a beam is displayed for visualization of the progressive situation.

Appropriate completion of analysis gains a point on the tower. Different genres are depicted in different colors to visualize participants' strong areas.

Figure 4
Visualizing dashboard for the in-house security contest.

understanding of the situations of attack and defense through visualization.

5) Practice of the preparation of an attack method timeline report based on the trainee's own analysis outcomes.
6) Practice on the escalation based on the timeline report for decision-making.
7) Simulations of not only temporary measures, but also permanent plans as part of practical exercises.

Once certified, security engineers are expected to continue improving their special skills and train subsequent engineer candidates. They can also communicate among themselves to exchange information and help one another to enhance their own skills further. With these points in mind, Fujitsu is undertaking the following activities in order to develop a community of Security Meister-certified engineers.

- Launch of a social networking service dedicated to Security Meister-certified engineers
- Provision of a mailing list for them
- Self-organized learning opportunities by highly skilled Meister engineers
- Regular meetings of Security Meister engineers so they can make connections with others

These activities are helping to change the perception about security—that it is not reserved for the security division, but it should be pursued with a group-wide effort. Generally speaking, there is often a discrepancy in certain opinions between the security and non-security divisions. The Security Meister certification program can help to address this discrepancy by encouraging exchanges of opinion and enhancing mutual understanding among engineers. We believe that the future cyber society will have a greater need for such personnel who can act as a bridging agent between company divisions.

5. Conclusion

This paper described the issue of training security engineers needed in today's cyber society, with an example from Fujitsu itself in terms of its Security Meister Certification Program. It also discussed a group-wide training program of security engineers and its effects by proposing model staff of security engineers needed not only by the security division but also by the company as a whole, so that various ideas of personnel education are used effectively to contribute toward further corporate maturity.

In this cyber society, security skills are indispensable for businesses. At Fujitsu, we believe that safety and security that support the human-centric intelligent society are delivered to our customers through our Security Meister engineers. Such engineers are capable of performing highly specialized security tasks as well as coordinating different internal organizations to raise the awareness of members of different parts of the corporation about the need for security.

References

1) Information-Technology Promotion Agency, Japan: Final report on surveys regarding needs and challenges for training IT human resources in information security (detailed version). March 2014 (in Japanese). *https://www.ipa.go.jp/files/000039527.pdf*
2) White House: Cyberspace Policy Review. June 2009. *https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*
3) NIST: National Cybersecurity Workforce Framework. *http://csrc.nist.gov/nice/framework*
4) (ISC)^2: IT Certification and Security Experts. *https://www.isc2.org/*

Kosetsu Kayama
Fujitsu Ltd.
Mr. Kayama is currently engaged in training initiatives in collaboration with external bodies as well as with group companies.

Shinichiro Yamashita
Fujitsu Ltd.
Mr. Yamashita is currently engaged in in-house security incident emergency response and information analysis.

Masayuki Okuhara
Fujitsu Ltd.
Mr. Okuhara is currently engaged in information security strategy development for Fujitsu Group and implementation of security measures.