enPiT SecCap: Comparison of Japanese Practical Security Education with one of the US

Takao Okubo

A new education program called enPiT in Japan has established in 2012. SecCap, a part of enPiT, is a set of practical security education. SecCap contains 21 lecture courses including 16 hands-on courses. This paper discusses the difference of practical security education between Japan and the US.

1 Introduction

Security attacks and incidents have spread widely and deeply over the society. Thus the human resource development on security is the urgent necessity for most of government agencies and enterprises. Japan had been behind in security education for a long time. enPiT SecCap [1]: the practical security education program has started in 2012. SecCap contains 3 security basic courses and 17 security practical exercise courses.

This paper discusses the status characteristics of Japanese security education and training mainly focusing on enPiT SecCap comparing with the security education in the US. Although most of the courses need to be improved, especially for online learning and education for young people, Japanese education has a few advantages such as course sharing.

The rest of this paper is organized as follows: Section 2 discusses the background of security education in Japan. Section 3 describes the enPiT and enPiT SecCap. 4 describes the education in the US. Section 5 discusses the comparison of Japanese education with the US and Section 6 introduces the related works. Section 7 describes the conclusion and future work.

2 Background

Although there are crucial requirements for human resources development on security, education institutes had not met the requirements sufficiently. There had been no security courses provided at most of the universities till 2010. The security incidents such as Gumblar and APT attacks have changed the situation. By 2014, several universities have started security lectures and hands-on courses. However, these courses would not be sufficient to meet the needs of industry. TABLE 1 indicates the security courses in representative universities.

Institute of Information Security (IISEC), which is the exception has provided 28 lectures and hands-on courses about security including cryptography, network security, software security, security and privacy, law and security management since 2004. Although it has succeeded to produce security experts in security vendors such as IBM and Trend-Micro, the impact on Japanese society is restrictive since the fixed total number of student is less than 100.

---

enPit SecCap: 日米の実践セキュリティ教育比較

Takao Okubo, 情報セキュリティ大学院大学, Institute of Information Security.

表 1 Security courses in Japan

University	number of courses	Representative course
University of Tokyo	1	security basics
Tokyo Denki University	1	network security
Tsukuba University	3	cyber risk
JAIST[†1]	4	security hands-on
NAIST[†2]	2	security PBL hands-on
The University of Electro-Communications	4	media security
Tokyo University of Technology	1	information security
Waseda University	6	security management

3 enPiT SecCap

enPiT is the one of education projects by Ministry of Education, Culture sports, Science and Technology (MEXT) for practical IT human resources. enPiT covers cloud computing, embedded systems, business applications and security. enPiT has started in October 2012 and continues till 2017.

3. 1 SecCap

SecCap is the security part of enPiT. Figure 1 indicates the organization of SecCap. Five universities and institutes (Institute of Information Security, JAIST, NAIST, Tohoku University and Keio University) are the organizers of SecCap. 15 universities in Japan participate in SecCap. Any students in these universities can attend a lecture courses provided by the organizer universities.

SecCap provides courses including 3 lecture courses and 17 practical exercises. The SecCap curriculum is shown in Figure 2.

Students in the universities in Fig. 1 can attend the online lectures with Polycom®. Practical exercises are not served online, thus students have to go to the universities where exercises are held.

SecCap students will be awarded “SecCap Certificate” after getting required credits within a year. In order to get credits, each student can choose exercise programs toward his/her own career target. SecCap provides social courses, theory courses, and technology courses. Students can choose only social courses, or they can choose courses from all categories.

3. 2 Practical exercises

One of the main characteristics of SecCap is practical hands-on exercise. VM (VMsphere®) clients are provided to students. Each student can use multiple VMs depending on the exercise contents. Fig. 3 indicates the exercise environment for the network security exercise. 6 VMs are assigned to each student. One VM plays as testing server, and other 4 VMs play a role for testing targets. The rest VM is used for administration work. The advantage of providing exercise environment as VM clients is maintenanceability. About 40 students in SecCap exercises, attend an exercise. They need the same environment except machine IDs and IP addresses. VM client environments are easy to clone and edit.

4 Education and training in the US

4. 1 National supports

In the US, there are National Centers of Academic Excellence, in Information Assurance Education (CAE/IAE), IA 2 year education (CAE/2Y) and IA Research (CAE/R) programs sponsored by National Security Agency (NSA) and Department of Homeland Security (DHS) [5]. 159 institutions are

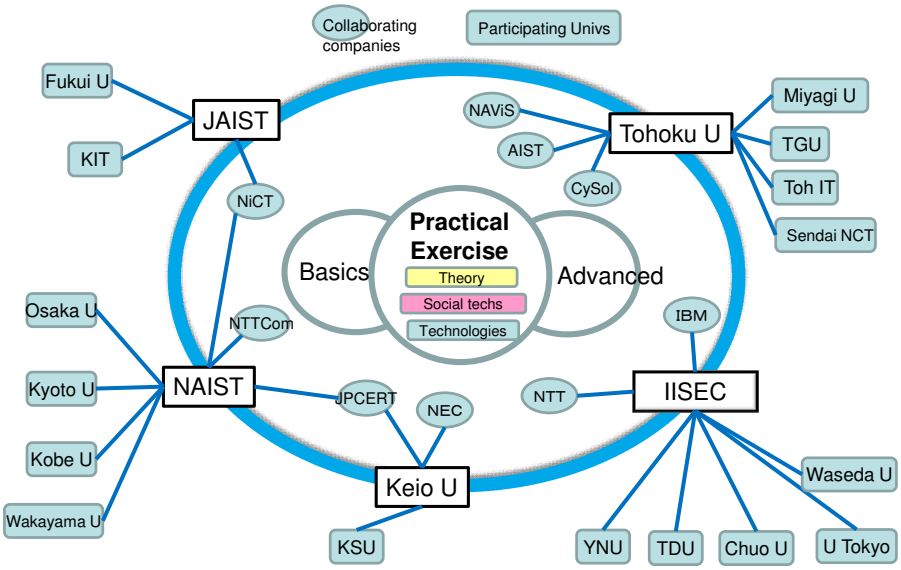

図 1　Organization of SecCap

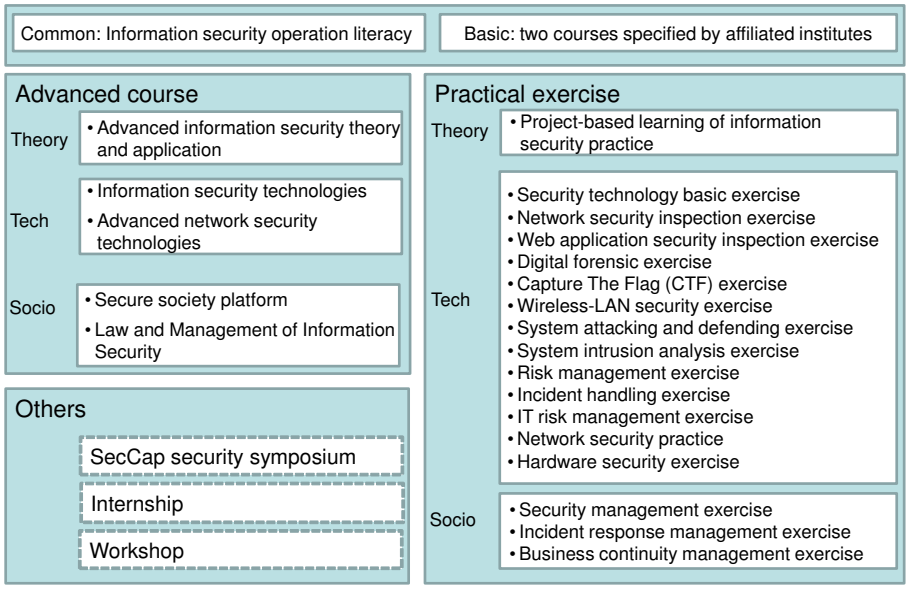

図 2　SecCap curriculum

certified as CAE.

NSA and DHS also define IA courseware Evaluation Program (IACP) for use of the national standards in information assurance education and training.

4. 2　UMBC / Maryland

University of Maryland, Baltimore Country (UMBC) is located near national agencies such as NSA / DHS and numbers of security related companies, where there are strong needs for security expertise development. Thus academia, federal a-

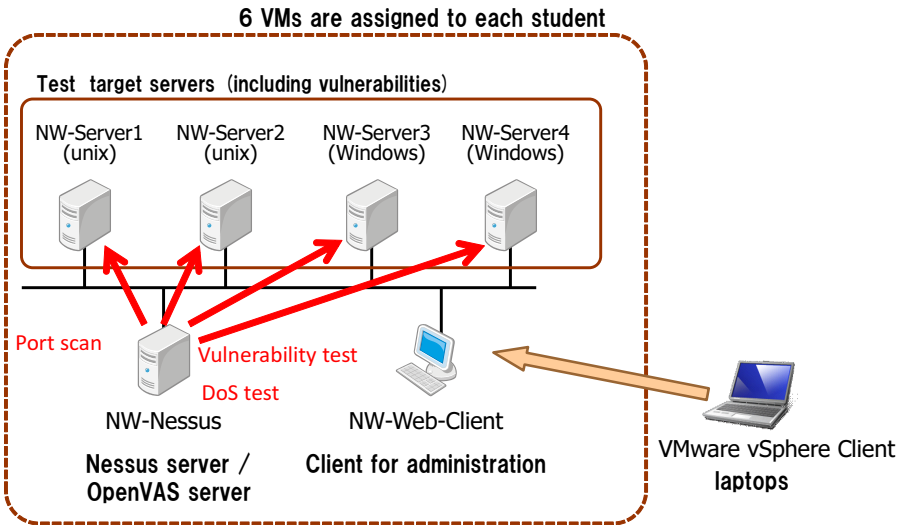

図 3 The environment for network exercise

gencies, and industry are strongly united as a community called "CyberMaryland"[†3]. For academia, the agencies and industry are sponsors, dispatching undertaking of students / trainees and also organizations to accept graduates.

Besides the academic courses, UMBC has a training center for expertise development for employees of agencies and companies.

4.3 CMU

CMU contains two important divisions: Software Engineering Institute (SEI) and Cylab. SEI has an essential role for training Computer Emergency Response Team (CERT) skills. SEI serves CERT programs for various stakeholders: system administrators, developers, researchers and managers. 17 CERT courses are listed in Table 2.

As shown in Fig. 2 the number of courses directly related with CERT in SecCap is 2 lectures, on the other hand the number of CERT is 5 lectures.

CMU provides open and free online courses called Open Learning Initiative (OLI)[†4].

CMU is also known as the university that obtains one of the best Capture The Flag (CTF) team in the world. There are some training activities for the team. Although there are CTF teams in Japan too and numbers of CTF contests have been held recent years, their level is not the same as teams in CMU and UMBC.

4.4 Educating white hackers

There are conferences for hackers in the US such as Blackhat, ToorCon, etc. sponsored by famous big IT companies e.g. Microsoft. ToorCon also holds boot camp for hackers called ToorCamp. These conferences are considered to develop young white hackers. UMBC holds CTF contests for high school students.

Japan has started similar activities for developing white hackers. Security Camp has started in 2004, sponsored by 30 companies. It is targeting the age under 22. Moreover, in 2014, CODE BLUE, the international conference for hackers has just began in Japan[†5]. The secure coding lecture will be pro-

†3 http://www.cybermaryland.org/
†4 http://oli.cmu.edu/
†5 http://www.codeblue.jp/en-index.html

表 2　CERT courses

Course
Overview of Creating and Managing CSIRTs
Creating a Computer Security Incident Response Team (CSIRT)
Managing Computer Security Incident Response Teams (CSIRTs)
Fundamentals of Incident Handling
Advanced Incident Handling
Malware Analysis Apprenticeship
Information Security for Technical Staff
Applied Cybersecurity, Incident Response, and Forensics
Managing Enterprise Information Security: A Practical Approach for Achieving Defense-in-Depth
Secure Coding in C and C++
Security Requirements Engineering Using the SQUARE Method
Software Assurance Methods in Support of Cyber Security
Introduction to the CERT Resilience Management Model
CERT Resilience Management Model Appraisal Boot Camp
CERT Resilience Management Model Users Group Workshop Series
Assessing Information Security Risk Using the OCTAVE Approach
Insider Threat Workshop

vided in the future. In Japan, NII have provided several online courses including formal methods[†6]. SecCap provides only live video streaming service.

5 Discussion

From a security educational point of view, Japan is behind the US. One of the disadvantages is the number of security education courses in the universities. The courses in universities even including SecCap are still insufficient for satisfying the needs of the government and industry. Another disadvantage of Japan is the lack of courseware standard such as IACP.

We consider the main reason of the disadvantages is the difference of military / homeland security motivation. CAE/CAR-R, IACP and CyberMaryland is promoted by NSA / DHS. On the other hand, there is few research or education program sponsored by military or security agencies in Japan. EnPiT is sponsored by Ministry of education.

However, we consider Japan takes a few advantages over the US. One is sharing security courses among multiple universities provided by SecCap. This sharing can reduce the cost and resources of each university for courseware development and lectures.

UMBC, CMU and SecCap provide online courses. However, the author has acquired knowledge by interviews that there is common understanding that online lecture is not appropriate for practical hands-on exercises. Students prefer offline style because they need quick helps and interactions with teachers. It is an obstacle for sharing lectures because of limitation of the venue. More interactive online style would be required for extending practical exercises.

†6 http://stream.edubase.jp/static_gadgets/view/13

6 Related works

Although there are numbers of computer educational researches, conferences and workshops, the researches for security education / training are not yet as many as other educational topics [4].

Hazeyama et.al. propose a learning process and a learning environment for software security process [2] [3]. Although it is one of the successful security education cases in Japan, unfortunately it is limited within one university, and limited to the education on secure software development.

The demand for cyber security education has emerged with the background of cyber threats recent years. NSA / DHS are going to enhance IACP for cyber security. The US National Science Foundation (NSF) asked ACM ' s Education Board to provide guidance to help university to and stimulate cyber security education. Schneider points that the cyber security education in universities is essential, but it is not sufficient and need to be improved [6].

7 Conclusion

This paper describes the current practical security education and training in Japan, focusing on enPiT SecCap, and it compares Japanese education with the one in the US. The author considers Japan has a few advantage to the US. One advantage is sharing lectures including exercises among multiple universities.

参 考 文 献

[1] enPiT: enPiT, 2014.

[2] Hazeyama, A. and Shimizu, H.: A Learning Environment for Software Security Education, *Secure Software Integration and Reliability Improvement Companion, IEEE International Conference on*, Vol. 0(2011), pp. 7–8.

[3] Hazeyama, A. and Shimizu, H.: Development of a Software Security Learning Environment, *2010 11th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Vol. 0(2012), pp. 518–523.

[4] McGettrick, A.: Toward Effective Cybersecurity Education, *IEEE Security & Privacy*, Vol. 11, No. 6(2013), pp. 66–68.

[5] NSA: National Centers of Academic Excellence, 2014.

[6] Schneider, F. B.: Cybersecurity Education in Universities, *IEEE Security & Privacy*, Vol. 11, No. 4(2013), pp. 3–4.