一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

Ethical Education on Information Security Mind for Practical Security Learning

Yoshinari KANAYA † Daisuke KOTANI ‡ Katsuyoshi IIDA * and Hideaki SONE ‡

† Graduate School of Information Sciences, Tohoku University
‡ Academic Center for Computing and Media Studies, Kyoto University
*Information Initiative Center, Hokkaido University
‡ Cyberscience Center, Tohoku University, Aramaki Aoba 6-3, Aobaku Sendai, 980-8578 Japan
E-mail: ‡ sone@cc.tohoku.ac.jp

Abstract : Practical education on information security may cause trouble if any student in the course tries the new education against actual networks or services intentionally or negligently. Education on occupational ethics and relating legal system on unauthorized access, privacy protection, and copyright infringement must accompany such practical classes.

The authors developed an education material package for “security mind” education to be used in PBL classes on practice subject. The package contains explanatory slides and tests. This report illustrates the background and need for the education on information security mind, as well as development of education material, samples and result from evaluation.

Keywords : Practical security learning, information security, ethical education, information security mind, Basic SecCap Course

1. Basic SecCap Course

Practical education including exercise lessons on realistic practice subjects is an important part in human resource development for present-day IT technology. One of such projects in Japan is enPiT2 (Education Network for Practical Information Technologies) project for undergraduate students which started in 2016 as a funded project by Japanese government MEXT. The enPiT2 project has four IT fields; Big-Data AI, Security, Embeded System, and Business System Design, and the enPiT2 Security Field operates Basic SecCap Course [1] with 14 collaborative universities in the coalition as well as additional 27 participating universities / colleges (as of September 2020) to develop the education course by the collaborative network [1]. The Basic SecCap course provides five Specialized subjects (lectures) and 34 Practice Subjects (practical trainings) in field of information security for 400 undergraduate students every year.

Each collaborative university provides various PBL classes on Practice Subject (or Advanced Practice Subject) to educate sufficient number of personnel with wide coverage from fundamental of information security, practical system / network security engineering, to social management of security incident. A PBL class is typically a two-days training program on a specified problem, and some titles are listed in Table 1. Some part of Practice Subjects are carried out by collaboration with industries to deal on practical problem, or bring actual system into each practice subject.

Table 1 Practice Subjects (part).

[Practice Subjects]
Cybersecurity Fundamental
Cloud Security
Privacy Protection Protcol for Big Data
Incident Response
Cryptographic Hardware Security
Security Engineering
CSIRT and Risk Management
Information Security
Attack Detection by Web Application Firewall
Cyber offence / Defense Fundamental
[Advanced Practice Subjects]
Control System Security
Secure Public Key Cryptography Design and Decipher
Physical Security Attack and Countermeasures
Incident Handling
Collision Attack and Cryptography Safety Evaluation

[1] https://www.seccap.jp/basic/

2. Need for Ethical Education on Information Security Mind for Practical Security Learning

Practical education on information security may cause trouble if any student in the course tries the new education against actual networks or services intentionally or negligently. Education on occupational ethics and relating legal system on unauthorized access, privacy protection, and copyright infringement must accompany such practical classes. A simple method to use a webform with a checkbox "I understand / agree …" or signature on a pledge / consent form is inadequate for this purpose.

Although practical training in practice subjects are the essentials and effective program, possible abuse by the students in the class may cause civil or criminal problems. The educator of the subject might be acquitted on a soliciting charge on such illigal abuse. Responsibility of educational institutes and educators in these fields naturally includes education to give advice students not to abuse the information and skills learned in the practice.

To cope with the problem in practical training courses in information security, the course should extend the program to include appropriate and effective "ethical education on information security mind" to teach the students laws and ethical standards in information security and that the knowledge and skill learned in the practice must not abused in real cyber space.

3. Development of Education on Information Security Mind

3.1. Background

Security Mind Taskforce in Steering Committee of the the Basic Security Course was started in 2019 to study on implementation of security mind education, selection of topics, and development of education material. Three of the authors are members of the Taskforce.

There are related cases on education of laws and ethics in information security courses, notably in practical subjects, and the importance is widely known. Some examples are Security Camp[2], SecHack365[3], and a class in a university, and those cases are lectures on laws and ethics, or legal notice on cyber security research. Webb et al reported on a case study-based cybersecurity ethics curriculum by discussion on case examples in gray area [2]. Though there are many cases, educational methods are not well documented, and each program will find a suitable method with great effort. The Security Mind Taskforce has developed a document as an education material.

3.2. Purposes

The purpose of this education is to develop security mind of student who will become a personnel who takes the initiative in appropriate decision and accurate expertise.

Education on information security mind in the Basic SecCap course has a characteristic that students in the class are human material who will become security specialists as well as ICT engineers in different categories or business managers. Thus the security mind education cannot assume the students have learnt basic knowledge in information system and communication network engineering.

Another feature of the education in the Basic SecCap course is check test which follows classroom lectures. A program which has such a test may encourage students to learn in a serious manner even on uninteresting lectures on law and ethics

Standardized education material of security mind education helps achievement of quality guarantee of the education in any PBL class on practice subject and by any teacher at each collaborative university.

3.3. Method

The Taskforce built a plan to develop and apply the education of information security mind.

(1) The TF develops a package of education material and check test.
(2) The TF shares the package with teachers of practice subjects by way of faculty development (FD).
(3) Each teacher performs the education in the beginning of a practice class.

Typical practice subject class in Basic SecCap is a two or three days intensive classes, and time for information security mind is limited. The education on information security mind includes a wide variety of topics from introduction of many related laws, occupational ethics, to incident examples. The TF designed to include all the variety range in the education package, and each teacher can select and extract topics suitable for program of the practice subject. Expected time for the lecture, check test, and explanation by a teacher is 25-30 minutes.

4. Framework of Education on Information Security Mind

4.1. Selected topics

List of topics selected in the education on information

[2] https://www.security-camp.or.jp/

[3] https://sechack365.nict.go.jp/

security mind is shown in Table 2. The list is not intended to include all the topics within a limited time in the class. The Taskforce shows wide variety of security-related topics as well as specific case examples to cultivate security mind of the students in the practice subject class.

These topics in law field are derived from Constitution of Japan, Telecommunications Business Act, Radio Act, Act concerning the Prohibition of Unauthorized Computer Access, Penal Code, etc. The ethic field referred ACM Code of Ethics and Professional Conduct[4], Code of Ethics of the Information Processing Society of Japan[5], Code of Ethics of the IEICE[6], Code of Ethics of Professional Engineers[7], etc.

Table 2 Topics in education on security mind.

[Law]
Privacy of communications
Illegal access
Crime on computer / electromagnetic record
Copyright / intellectual property right
Guilty intent / negligence
Related laws
[Ethic]
Engineer ethics
Case exmple
[Incident example]
Case example
Gray range

4.2. Education material

The Taskforce developed lecture slides, check test, and explanation for the test as package of education material for information security mind. An example slide is shown in Fig. 1, and sample test followed by its explanation is in Fig. 2.

Each slide was designed to help students to understand the topic as an immediate problem, and a possible attack / protection in a practical business was explained along with specific case examples by referring news coverage.

Questions in the check test were designed to measure understanding of the students in nine subjects listed in Table 3. Style of answer is a true or false question or a choice between the four.

Explanation of test which is circulate after the check test shows not only the right answer but also the reason, legal picture, and relating issues to support review study.

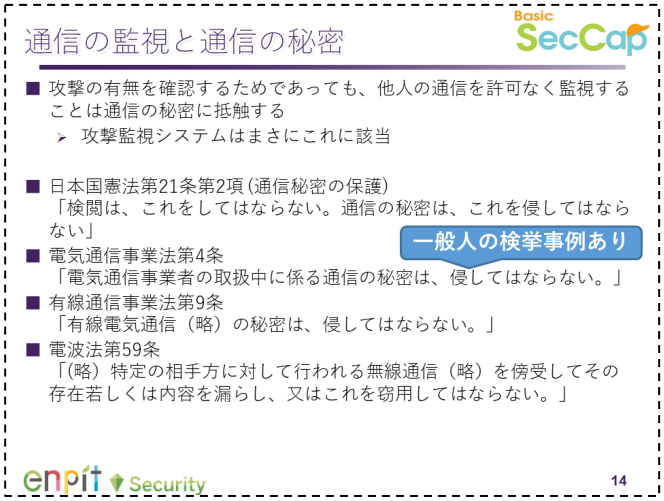
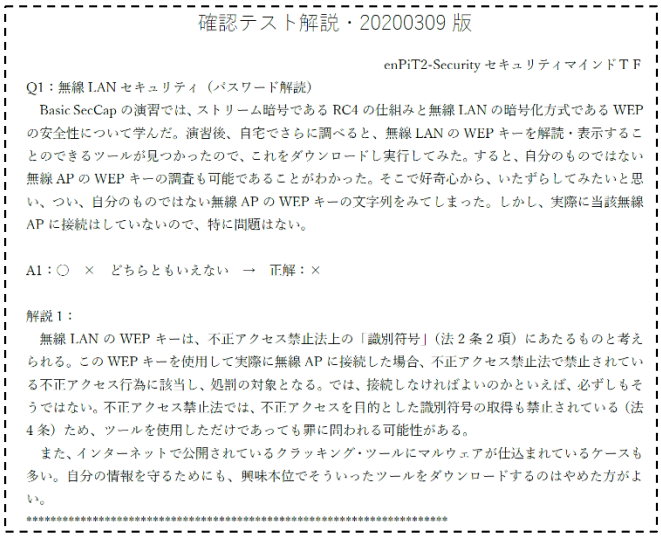


Fig. 1 An example of slide
(Monitoring and privacy of communication)


確認テスト解説・20200309 版

enPiT2-Security セキュリティマインドＴＦ

Q1：無線 LAN セキュリティ（パスワード解読）

Basic SecCap の演習では、ストリーム暗号である RC4 の仕組みと無線 LAN の暗号化方式である WEP の安全性について学んだ。演習後、自宅でさらに調べると、無線 LAN の WEP キーを解読・表示することのできるツールが見つかったので、これをダウンロードし実行してみた。すると、自分のものではない無線 AP の WEP キーの調査も可能であることがわかった。そこで好奇心から、いたずらしてみたいと思い、つい、自分のものではない無線 AP の WEP キーの文字列をみてしまった。しかし、実際に当該無線 AP に接続はしていないので、特に問題はない。

A1：○　×　どちらともいえない　→　正解：×

解説 1：

無線 LAN の WEP キーは、不正アクセス禁止法上の「識別符号」（法２条２項）にあたるものと考えられる。この WEP キーを使用して実際に無線 AP に接続した場合、不正アクセス禁止法で禁止されている不正アクセス行為に該当し、処罰の対象となる。では、接続しなければよいのかといえば、必ずしもそうではない。不正アクセス禁止法では、不正アクセスを目的とした識別符号の取得も禁止されている（法４条）ため、ツールを使用しただけであっても罪に問われる可能性がある。

また、インターネットで公開されているクラッキング・ツールにマルウェアが仕込まれているケースも多い。自分の情報を守るためにも、興味本位でそういったツールをダウンロードするのはやめた方がよい。

Fig. 2 Sample test and explanation
(Wireless LAN security – Password decipher)

Table 3 Questions in check test

Q1: Wireless LAN security (Password decipher)
Q2: Cipher breaking
Q3: Packet monitoring
Q4: Malware (Computer virus etc.)
Q5: Counterattack
Q6: Unauthorized computer access law
Q7: Malware intrusion through storage media
Q8: Crime of computer virus and malware
Q9: Computer virus development

[4] https://www.acm.org/code-of-ethics
[5] https://www.ipsj.or.jp/ipsjcode.html
[6] https://www.ieice.org/jpn/about/code1.html
[7] https://www.engineer.or.jp/c_topics/000/000025.html

5. Implementation and evaluation

Practical subject classes in Basic SecCap course in School Year 2019 were planned as trial term for education of information security mind, but almost practical subject held at collaborative universities implemented the new education and lecture and check test are performed at the beginning of the class.

Result of check test of practical classes in summer, 2019, is listed in Table 4 where average accuracy rate *m* is shown for each question. Number of classes and answers for each question differs because each class selected questions related to its topic.

Table 4 Result of check test

	Classes	Answers	*m*
Q1	5	59	58%
Q2	5	114	98%
Q3	10	90	54%
Q4	6	15	13%
Q5	8	118	86%
Q6	7	63	69%
Q7	6	36	51%
Q8	4	33	73%
Q9	5	42	76%

The average accuracy rate is high for Q2 (Cipher breaking) and Q5 (Counterattack), while low for Q4 (Malware (Computer virus etc.)). The high rates can be effect of the education which raised awareness on privacy of communication and excessive defense, or easy questions to get right answer by commonsense judgement.

The students in classes were observed listening seriously to the lecture. There were highly-motivated comments in student questionnaire that remark on self-defense and harm or skill and ethics sense on cyber security.

Outside advisor committee on visit inspection of PBL class on practice subject classes gave high evaluation and positive comments that mandatory education on ethics is a good decision, uniformed education is well performed in different universities, or test questions are well polished.

The Taskforce is continuing study to equalize difficulty level of questions and establish evaluation method for effect of the education. Some questions have been revised to add supplemental explanation. Slides were improved by reflecting result of test and student questionnaire and following-up the newest information security cases.

6. Conclusion

This report introduced the Basic SecCap Course operated by enPiT2 Security Field and its practice subject training classes. Following discussion showed that ethical education on information security mind for practical security learning is necessary to cope with the problem in practical training courses in information security,

The Taskforce team developed the education method for information security mind to educate variety of students from different fields as a combination of classroom lecture and check test. Standardized education material of security mind education helps achievement of quality guarantee of the education. The product is a package of education material that includes lecture slides, check test, and explanation for the test. The evaluation after classes in summer, 2019, showed effectiveness and good results of the education method for information security mind. The Taskforce and Basic SecCap course are continuing improvement of the education.

Acknowledgement

The plan and development as well as implementation and evaluation were supported by Steering Committee of Basic SecCap course and teachers and students who joined the Course from collaborative universities and participating universities / colleges. The authors would like to express their sincere thanks to all of them and advisor committee for their collaboration in realizing the valuable results.

Reference

[1] Hideaki Sone, Satoru Izumi, “Basic SecCap, Practical Education for Information Security by University Cooperation (Poster Presentation),” IEICE Tech. Rep., Vol. 117, No. 299, IA Workshop IA2017-36, pp. 33-34, KMUTT, Thailand, November 2017.

[2] Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N. C., Campbell, R. H., Bashir, M.: “A Case Study-based Cybersecurity Ethics Curriculum,” Proc. Workshop on Advances in Security Education (ASE’18), Baltimore, MD, USENIX, 2018.