

セキュリティ人材育成におけるセキュリティマインド教育の教材開発と実践

金谷 吉成 飯田 勝吉 小谷 大祐

enPiT-Security では、PBL 演習を中心にセキュリティ人材育成の取り組みを進めているが、実践的演習で得た知識やスキルを悪用しないよう、受講者に法律や倫理に関するセキュリティマインドを身に付けさせることが不可欠である。こうした問題意識に基づき、報告者らはセキュリティマインド教育の教材と確認テスト及び解説を作成し、14 の連携大学がそれぞれ実施する演習において統一した教材を用いてセキュリティマインド教育を実践するとともに、確認テストの結果や受講者・外部有識者による意見を踏まえ、教材及び確認テストの改善を行った。これにより、担当教員や演習内容にかかわらず均質なセキュリティマインド教育を実現することが可能となった。

In enPiT-Security, we have been working on the development of security professional with the educations at PBL seminars. It is essential to make the students acquire "Security-Mind" about law and ethics so that they do not misuse the knowledge and skills acquired in the practical seminars. Based on this awareness, we developed materials for Security-Mind education, questions for a proficiency test, and explanations. And we practiced this education using the same teaching materials at each PBL seminars in 14 partner universities. The materials and questions were improved based on the results of the proficiency test and the opinions of the students and external experts. As a result, we were able to realize a homogeneous Security-Mind education regardless of the teacher or the contents of the seminar.

1 はじめに

Society 5.0 [8] でも提唱されているように、サイバー空間と現実世界とが高度に融合した超スマート社会においては、サイバーセキュリティの確保はこれまで以上に重要となっている。サイバー空間を脅かす悪意ある攻撃は市民生活のみならず経済・社会活動にまで影響を及ぼし、国家の安全保障に対する脅威にもつながっている。しかし、サイバーセキュリティを実現

するための人材は質的にも量的にも不足しており [4]、セキュリティの実践的スキルを習得した人材の養成が喫緊の課題となっている。

enPiT-Security [5] では、こうした課題に対応するため、14 の大学が連携して学部学生を対象としたサイバーセキュリティ人材育成のための教育プログラム (Basic SecCap コース) を立ち上げ、先進技術の知識に加え、理解・応用できる実践的能力を持つ ICT 技術者・経営者となり得る人材の育成に取り組んでいる。

Basic SecCap コースは、基礎知識学習のための基礎科目、サイバーセキュリティに関する総合的な知識の学習のために少数の連携校が全参加校を対象に開講する専門科目、連携校が各々の特徴を生かし提供する多彩な PBL (Project Based Learning) 演習のための演習科目及び発展学習のための先進 PBL と大学院インターンシップを含む先進演習科目で構成される。各科目は、連携校相互及び各地の参加校に提供され、多くの学生が、幅広いセキュリティの最新技術や知識を、具体的に体験を通して習得することができる。

Teaching Materials Development and Practice of Security-Mind Education.

Yoshinari Kanaya, 東北大学大学院情報科学研究科, Graduate School of Information Sciences, Tohoku University.

Katsuyoshi Iida, 北海道大学情報基盤センター, Information Initiative Center, Hokkaido University.

Daisuke Kotani, 京都大学学術情報メディアセンター, Academic Center for Computing and Media Studies, Kyoto University.

コンピュータソフトウェア, Vol.38, No.1 (2021), pp.38-44. [研究論文 (レター)] 2020 年 3 月 30 日受付.

Basic SecCap コースで行う演習の中には、サイバー攻撃の検知・防御技術を学ぶために実際にネットワークパケットをキャプチャして分析したり、サーバーの脆弱性を突いてアクセス制御機能による認証を回避したり、暗号技術を理解するために暗号解読を行ったりするものがある。PBL 演習を中心としたこのような教育はセキュリティの実践的スキルを習得するために必要かつ効果的なものであるが、一方で、演習受講者がそこで得た知識を現実のサイバー空間において悪用した場合、受講者自身が刑事責任や民事責任を負うだけでなく、演習担当者が犯罪の教唆や幫助を行ったものとされ、あるいは共同不法行為として被害者から損害賠償請求をされる可能性が否定できない。また、演習担当者及び教育機関の責任として、演習で身に付けた知識やスキルを悪用しないよう注意することは必須であるが、それだけで十分な注意義務を果たしたと言えるかは必ずしも明らかではない。

このような実践的セキュリティ人材育成における問題を解決するには、演習で身に付けた知識やスキルを現実のサイバー空間で悪用しないこと、セキュリティに関連する法律や技術者倫理及び過去のインシデント事例を学び、他者と共存するための規範意識(これを「セキュリティマインド」と定義する)を身に付けさせることが不可欠であり、そのための教育(これを「セキュリティマインド教育」と定義する)を演習の際に受講者に対して行うことが必要である。

enPiT-Security では、運営委員会内にセキュリティマインド・タスクフォース(以下「セキュリティマインドTF」という)を設置して、セキュリティマインド教育の実施方法の検討、テーマ選定、教材作成、理解度を測る確認テストの検討を行い、2019 年度を試行期間として実施することとした。

本論文では、2 節でセキュリティマインドTF による取り組みと PBL 演習での実施について述べる。3 節では教育効果を確認テストの正答率から測り、受講者アンケート及び外部有識者であるアドバイザー委員からのコメントを示して、教材と確認テストの改善を検討する。4 節でまとめに加えて、今後取り組むべき項目と課題を示す。

2 セキュリティマインドTF による取り組み

2.1 先行教育プログラムとの比較

セキュリティ教育において、法律や倫理に関する教育を行っている事例は他にも存在する[2][6][9][11]-[13]。セキュリティ・キャンプはセキュリティ・キャンプ協議会が主催する学生を対象とするセキュリティ関連のイベント群である[11][12]。その中心的なイベントである全国大会では、初日に法律や倫理の講義が行われている。NICT が主催する 25 歳以下の若手セキュリティイノベーター育成プログラムである SecHack365 [9][13] では、現役の弁護士や検事によるサイバーセキュリティ研究の法律上の注意点の講義が含まれている。工学院大学情報学部では、講義と演習を組み合わせたセキュリティ教育がなされており、座学で情報セキュリティを取り巻く法律について講義されている[6]。Webb らは判断が難しい問題について事例ベースで議論することによりセキュリティ倫理教育を行う科目の実践について報告している[2]。

このようにセキュリティ教育プログラム、特に実践的な演習を行う場合に法律や倫理について教育を行う重要性は認識されており、需要が大きい。しかし、その教育方法は文書化されておらず、各プログラムに適した方法を手探りで検討することになる。そこで、本論文では Basic SecCap コースで導入したセキュリティマインド教育の要点を記載する。

Basic SecCap コースのセキュリティマインド教育の特徴は、セキュリティ専門家だけでなく他の分野を専門とする ICT 技術者や経営者となり得る人材に、セキュリティマインドを身に付けさせることである。また、座学による講義だけでなく確認テストを併せて実施する点にも特徴がある。これにより、受講者にとって興味を持ちにくい法律や倫理の講義にも真剣に取り組むといった効果が期待できる。また、連携校がそれぞれ実施する PBL 演習において統一した教材を用いてセキュリティマインド教育を行うことができるため、担当教員や演習内容にかかわらず均質な教育を実現することが可能となる。

2.2 セキュリティマインド教育の実施方法の検討

演習担当者及び教育機関の責務として、「演習で得た知識やスキルを現実のサイバー空間で悪用しません」というチェックボックスにチェックを入れさせ、誓約書や同意書に署名させるだけの対策ではまったく不十分である^{†1}。受講者自身のセキュリティマインドを醸成させ、適切な判断と的確な実践を主体的に行えるような人材を育てることが重要である。

セキュリティマインド TF ではそのための教材と確認テストを作成し、それを FD (Faculty Development) により演習担当教員間で共有し、各 PBL 演習において実施することにした。Basic SecCap コースの演習科目は、多くの科目が 1 単位の集中開講であるため、セキュリティマインド教育に割ける時間には限りがある。セキュリティマインド教育の内容は、2.3 節に示すようにセキュリティに関連するいくつかの法律や技術者倫理、過去のインシデント事例の紹介など多岐にわたるが、各演習の内容に応じて教材や確認テストを抜粋して利用することとし、教員による講義、確認テストの実施、解説の配布を 25～30 分程度で行えるよう設計した。

2.3 テーマ選定

セキュリティマインド教育で扱うテーマと内容を、法律・倫理・事例ごとに表 1 に示す。

限られた時間の中ですべてのテーマに触れることはできないが、本教育の目的は演習の受講者のセキュリティマインドを涵養することにあるので、セキュリティに関連するテーマをなるべく幅広く、具体的な事例を交えつつ提示することにした。

2.4 教材の開発

セキュリティマインド教育のための教材として、講義スライド、確認テスト及び解説を作成した。作成した講義スライドの例を図 1 に、確認テスト及び解説

表 1 セキュリティマインド教育で扱うテーマ

分類	テーマ	主な内容
法律	通信の秘密 (憲法 21 条 2 項, 電気通信事業法, 有線通信事業法, 電波法等)	ネットワークパケットをキャプチャして分析, 暗号通信を暗号解読により傍受等。
	不正アクセス 禁止法違反	パスワード解読, 脆弱性攻撃, フィッシングサイトの作成・誘導, 無線 AP の無断利用等。
	コンピュータ・ 電磁的記録対 象犯罪	電子計算機損壊等業務妨害罪 (刑法 234 条の 2), 電子計算機使用詐欺罪 (同 246 条の 2), 電磁的記録不正作出罪・供用罪 (同 161 条の 2), 不正指令電磁的記録作成罪・供用罪 (同 168 条の 2) 等。 マルウェアの仕組みや動作, その検出と駆除方法, 「正当な理由」の解釈等。
	著作権, 知的 財産権	著作権の保護, 私的使用, 引用, コピーガードの回避, リバースエンジニアリング等。
	故意・過失	刑事責任における故意と過失, 未必の故意, 保護法益, 不法行為による民事責任等。
	その他関連する 法律	不正競争防止法, 個人情報保護法, 特定電子メール送信適正化法, プロバイダ責任制限法等。
倫理	技術者倫理	ACM Code of Ethics and Professional Conduct [1], 情報処理学会倫理綱領 [7], 電子情報通信学会倫理綱領 [3], 技術士倫理綱領 [10] 等。
	技術者倫理が 問われる事例	顔認証技術のリスク (プライバシーの侵害と民主主義の自由を損なう可能性), 脆弱性情報の開示方法等。
事例	事例紹介	ウェブページの改ざん, 不正に入手した ID・パスワードによるログイン, マルウェアの作成, クレジットカード情報の盗用, 高度匿名化技術の利用等。
	グレーゾーン	情報通信技術や情報セキュリティ関連技術の発展に法規制が追いついていないケース, 規律があっても解釈が難しいケース等。

^{†1} 現時点でセキュリティ分野での裁判例は存在しないが, スキューバダイビング講習会主催会社と同講習会受講者との間で作成された免責同意書の内容が公序良俗に違反し無効であるとされた事例として, 東京地判平成 13 年 6 月 20 日判タ 1074 号 219 頁がある。

の例を図2に示す。

講義スライドは、2.3節に示したテーマについてセキュリティ実務の現場で想定される攻撃・防御を想定しつつ、報道資料を引用するなど具体的な事例を紹介し、受講者が身近な問題として捉えられるような内容を目指して作成した。法律を扱う場面では、正確を期するために条文を引用しなければならないこともあるが、セキュリティ演習の受講者の多くは理系の学部学生及び高等専門学校専攻科の学生であり、こうした受講者が身近な問題として理解しやすいよう、具体例を示したり要点を図示したりといった工夫をした。

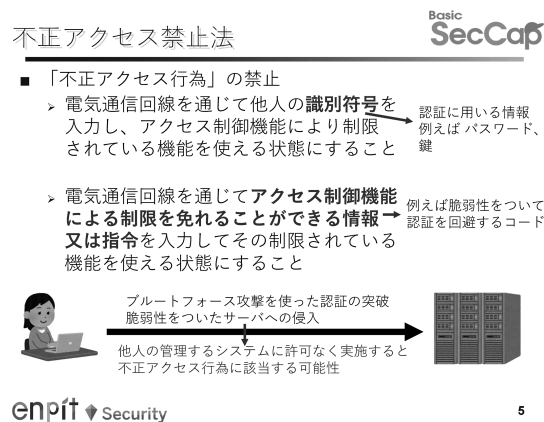


図1 講義スライドの例

確認テストは、講義の理解度を測るものとして情報セキュリティマネジメント試験、ITパスポート試験及び応用情報技術者試験の問題も参考にしながら9題を作成した。確認テストの内容を表2に示す。確認テストは、技術の理解を問うものではなく、技術に関連した法律に関する理解に加え、実例に近い例を法律や技術者倫理に基づいて判断できるかを問う内容となっており、これにより講義を通じてセキュリティマインドを身に付けることができたかを評価することができる。なお、解答方法は○×形式での正誤問題または四者択一問題とした。また、確認テスト実施後に配布する解説は、正答を示すだけでなくなぜそうなるのか、法的にどう考えられるのか、関連する論点にどのようなものがあるのかを示し、受講者が時間外学習の時間に復習できるようにした。

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 (パスワード解説)

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、自宅ですらに聞くと、無線 LAN の WEP キーを解説・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。

図2 確認テスト・解説の例

表2 確認テストの内容

	内容
Q1	無線 LAN セキュリティ (パスワード解説)
Q2	暗号解説
Q3	パケット監視
Q4	マルウェア (コンピュータ・ウイルスなど)
Q5	攻撃に対する反撃
Q6	不正アクセス禁止法
Q7	記憶媒体を介してのマルウェアの侵入
Q8	不正指令電磁的記録に関する罪
Q9	コンピュータ・ウイルスの作成

2.5 PBL 演習での実施

セキュリティマインド教育は2019年度を試行期間としていたが、全国の連携校で開講されたほぼすべての演習科目及び先進演習科目において、演習開始時に講義と確認テストが実施された。

3 教育効果と評価・改善

3.1 確認テストの正答率とその考察

夏季に行われた PBL 演習で講義とともに実施した確認テストの正答率の平均値 (m) と標準偏差 (σ) を表3に示す。確認テストは各演習の内容に応じて抜粋して利用できるようにしたので、問題ごとに実施した科目数、回答者数が異なっている。

問題ごとに正答率を比較すると、Q2 (暗号解説) や

Q5 (攻撃に対する反撃) の正答率が高く、Q4 (マルウェア) の正答率が低いことがわかる。これは、セキュリティマインド教育により通信の秘密や過剰防衛に関して受講者のセキュリティ意識が向上したと言える一方で、常識的な判断により正答しやすい問いだったとも言える。問題ごとに難易度を平均化させ、教育効果を測定可能とすることが今後の課題である。次に、演習科目 (PBL 演習) と先進演習科目 (先進 PBL と大学院インターンシップ) で正答率を比較すると、Q5~Q9 で発展学習となる先進演習科目の正答率が高くなった。確認テストは、Q1~Q5 が判断の難しいグレーゾーンの問題、Q6~Q9 が情報処理技術者試験の問題としており、既に PBL 演習でセキュリティマインド教育を受けた者やセキュリティに関する学習意欲の高い者が先進演習科目を受講していることを考えると、受講者にセキュリティマインドがしっかり浸透していることがわかる。セキュリティマインド教育は、何度も繰り返し行うことで受講者のマインドにセキュリティ意識を浸透させることができるのであるから、今後も改善しながら取り組んでいくことが必要である。

表 3 確認テストの正答率

	科目数	回答者数	全体 $m(\sigma)$	演習 $m(\sigma)$	先進演習 $m(\sigma)$
Q1	5	59	57.8% (20.8%)	78.9% (9.9%)	45.3% (3.1%)
Q2	5	114	98.3% (1.5%)	100.0% (0.0%)	97.7% (1.7%)
Q3	10	90	53.6% (22.8%)	61.3% (12.6%)	40.3% (31.1%)
Q4	6	15	12.8% (14.8%)	16.4% (16.0%)	6.8% (7.5%)
Q5	8	118	85.5% (9.1%)	81.1% (4.2%)	100.0% (0.0%)
Q6	7	63	69.2% (15.5%)	66.7% (16.2%)	84.6% (3.8%)
Q7	6	36	51.4% (18.5%)	49.2% (16.3%)	80.0% (0.0%)
Q8	4	33	73.3% (6.4%)	72.5% (5.8%)	80.0% (0.0%)
Q9	5	42	76.4% (11.4%)	74.0% (6.0%)	100.0% (0.0%)

3.2 受講者アンケートとその考察

セキュリティの実践的スキルの習得を目指して演習を受講した学生にとっては、比較的難しく興味を持ちにくい分野とも思われたが、予想に反し、真剣に講義を聴いている様子が見られた。演習後に実施した受講者アンケートでは、「……自分を守るため、また自分が他人に害を加えないようにサイバーセキュリティのスキルとインターネットの利用に対する倫理を養いたいと思った……」といった意見が寄せられている。

3.3 アドバイザー委員からのコメント

演習を視察した enPiT-Security のアドバイザー委員からは、「倫理に関しての内容を、必須にしたのは良い判断だったと思います」「(セキュリティマインド教育に関して) 均質な教育が、違うところでやっているけれどもできている」「小テストの内容について、よく練られており、グレーゾーン (判断の難しい) を問題にしている点は特に効果的だと感じた」というようなコメントをいただいており、外部有識者からも高い評価を得ていると言える。

3.4 正答率の低い確認テストの改善

Q4 (マルウェア) の正答率が極端に低かったこと、Q3 (パケット監視) に関して、受講者から問題文に利用規約の言及がないので解答できないとの意見があったことから、補足的な説明を追加するなど、確認テストの改訂を行った。教材については、確認テストや受講者アンケートの結果をフィードバックし、最新のセキュリティ事例をフォローするなどの改善を行っていく。

4 まとめと今後の課題

本論文では、セキュリティ人材育成におけるセキュリティマインド教育の必要性を明らかにし、そのための教材開発と実践、確認テストによる教育効果の測定と評価・改善について述べた。近年、サイバー攻撃のリスクはますます高まっており、幅広い産業分野においてセキュリティ人材が求められる状況を考えれば、今後も人材育成を推進していく必要があり、そうした人材には、しっかりとしたセキュリティマインドを身

に付けさせていく必要がある。

今後は、セキュリティマインド教育に IoT や AI などの新たな視点を盛り込んでいくこと、継続的なセキュリティマインド教育の実施を通じて、教育効果の評価と教材の改善を行うことが課題である。

謝辞 Basic SecCap コースにおいてセキュリティマインド教育の必要性を表明され、本論文の執筆を促していただいた東北大学の曾根秀昭教授に感謝します。セキュリティマインド教育のあり方や教材内容について議論いただいた enPiT-Security 分野運営委員会の皆様に感謝いたします。そのほかセキュリティマインド TF の活動にご協力いただいたアドバイザー委員、学生の皆様に感謝いたします。

参考文献

- [1] Association for Computing Machinery: ACM Code of Ethics and Professional Conduct, <https://www.acm.org/code-of-ethics> (2020 年 3 月 18 日閲覧)。
- [2] Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N. C., Campbell, R. H., and Bashir, M.: A Case Study-based Cybersecurity Ethics Curriculum, in *Proc. Workshop on Advances in Security Education (ASE'18)*, Baltimore, MD, USENIX, 2018.
- [3] 電子情報通信学会: 電子情報通信学会倫理綱領, <https://www.ieice.org/jpn/about/code1.html> (2020 年 3 月 18 日閲覧)。
- [4] 独立行政法人情報処理推進機構: 情報セキュリティ人材不足数等に関する追加分析について (概要), <https://www.ipa.go.jp/security/fy23/reports/jinzai/> (2020 年 3 月 18 日閲覧)。
- [5] enPiT-Security: 分野・地域を越えた実践の情報教育協働ネットワーク (セキュリティ分野), <https://www.seccap.jp/> (2020 年 3 月 18 日閲覧)。
- [6] 藤川真樹, 小林良太郎, 永宮直史: 大学におけるセキュリティ人材育成事例—工学院大学情報学部におけるセキュリティ教育—, *情報処理*, Vol. 60, No. 10 (2019), pp. 990–995.
- [7] 情報処理学会: 情報処理学会倫理綱領, <https://www.ipsj.or.jp/ipsjcode.html> (2020 年 3 月 18 日閲覧)。
- [8] 内閣府: 第 5 期科学技術基本計画, <https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html> (2020 年 3 月 18 日閲覧)。
- [9] NICT: 若手セキュリティイノベーター育成プログラム SecHack365, <https://sechack365.nict.go.jp/> (2020 年 3 月 26 日閲覧)。
- [10] 日本技術士会: 技術士倫理綱領, <https://www.engineer.or.jp/c.topics/000/000025.html> (2020 年 3

月 18 日閲覧)。

- [11] セキュリティ・キャンプ協議会: セキュリティ・キャンプ, <https://www.security-camp.or.jp/> (2020 年 3 月 26 日閲覧)。
- [12] 園田道夫: 実践形式によるセキュリティ人材育成の取り組み, *情報処理*, Vol. 60, No. 10 (2019), pp. 996–1001.
- [13] 安田真悟: 社会におけるセキュリティ人材育成事例 (1)—NICT におけるセキュリティ人材育成事業—, *情報処理*, Vol. 60, No. 10 (2019), pp. 976–981.



金谷 吉成

1994 年東北大学法学部卒。学士 (法学)。(財) 仙台応用情報学研究振興財団研究員, 東北大学法学部助手, 同法学研究科講師・准教授, 同法学研究科法政実務教育研究センター講師を経て, 2019 年 1 月より同情報科学研究科特任准教授 (研究)。専門分野はサイバー法・法情報学。高等教育機関におけるセキュリティポリシーの策定, 実践的セキュリティ人材育成などの研究に従事。



飯田 勝吉

1996 年九州工業大学情報工学部電子情報工学科卒。1998 年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了。2000 年九州工業大学大学院情報工学研究科博士後期課程中退。博士 (情報工学)。奈良先端科学技術大学院大学情報科学研究科助手, 米国カリフォルニア大学アーバイン校計算機科学科客員研究員, 東京工業大学学術国際情報センター講師・准教授を経て, 2016 年より北海道大学情報基盤センター准教授。情報ネットワーク, ネットワークセキュリティ, 性能評価に関する研究に従事。電気通信普及財団・テレコムシステム技術賞など受賞。2017~2018 年度電子情報通信学会インターネットアーキテクチャ研究専門委員会委員長。2017 年より電子情報通信学会英文論文誌 (B) 編集委員。

**小谷 大 祐**

2016 年京都大学大学院情報学研究科
知能情報学専攻博士後期課程修了。
同年より京都大学学術情報メディア
センター助教。京都大学博士 (情報

学)。インターネットアーキテクチャ，ネットワーク
セキュリティの研究に従事。情報処理学会，電子情報
通信学会，ACM, IEEE 各会員。