［セキュリティ人材育成の現状と実践］

④ 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―

藤川真樹 | 工学院大学　小林良太郎 | 工学院大学
永宮直史 | 日本セキュリティ監査協会

工学院大学の取組み

セキュリティの人材不足が深刻度を増しており，サイバー攻撃が常態化している今日にあっては，最高学府としての大学は，セキュリティに関する知識・技術とともに実践的なスキルを学生に習得させることが望ましい．攻撃と防御は日々進化することから，最新の技術動向を教育に反映することも重要である．加えて，倫理やセキュリティに関する法を教育することも忘れてはならない．

安全・安心な社会は，法と倫理に則り，教養や訓練を通して獲得した能力（スキル）を持つ「人」によって構築・維持される．この原理原則は，いつの世においても不変である．インターネットがライフラインのような存在となり，あらゆるモノがインターネットにつながる時代を迎えようとしている今日にあっては，法と倫理に則り，サイバー空間とフィジカル空間を安全にするスキルを備えた「人」の存在が不可欠である．

実学に重きを置く工学院大学情報学部では，時代の要請に応えつつ特色ある教育を行うために，サイバーとフィジカルに関する包括的なセキュリティ教育（技術，法律，経営，心理，倫理など）を行い，実務者としてのスキルを備えた優秀なセキュリティ・エンジニアを世に送り出すことを目標として掲げた．具体的な施策として，セキュリティに関するカリキュラムを見直し，講義と演習の充実を図った．講義では，実習を織り交ぜつつ，情報処理安全確保支援士試験に定められたシラバスをカバーすることで，セキュリティに関連する有資格者数の向上を図る．一方，演習では「学生自身が演習環境を構築し，与えられたミッションを解決する」というスタイルの採用により，セキュアシステムの構築能力や問題解決能力の向上を図る．

本稿では，カリキュラムの中から特色のある講義と演習を１つずつ紹介する．特定非営利活動法人・日本セキュリティ監査協会（JASA）による寄附講義，および，サイバーセキュリティ演習について述べる．最後に，本稿を総括する．

寄附講義

背景

特定非営利活動法人・日本セキュリティ監査協会（以下，JASA）は，情報セキュリティの確実な運用を確保するための「情報セキュリティ監査」の普及促進を行っており，活動の一環として「情報セキュリティ監査人」の育成も行っている．当該監査人は，監査の対象となる企業・団体を訪問し，適切

な情報セキュリティ対策を講じているか否かを監査するとともに，監査結果をもとに企業・団体に対して指導・助言を行う．

JASA では，情報システムに関する実務経験のある社会人を中心に情報セキュリティ監査人を認定しているが，監査の重要性の理解を学生にも広げるために，2017 年から工学院大学情報学部コンピュータ科学科の 3 年生に対して寄附講義（科目名：「企業経営と情報セキュリティ」）を行っている．

シラバスの設計

基本的な考え方

シラバスの作成に際しては，次の考え方を基本とした．

- JASA が販売している『情報セキュリティ内部監査の教科書』をベースに，情報セキュリティ監査を体系的に理解させる
- 社会経験のない学生に，事例を通して組織のマネジメントを理解させる
- 第一線の専門家の経験を伝えることで，学生に問題意識を持たせる
- グループワークと演習を取り入れることで「学生が熟考できる」講義にする
- 演習を通じて監査プロセスを理解し，実務知識を身につけられるようにする

一般的なセキュリティの講義では 1 名の教員がすべての講義を担当するが，寄附講義では担当教員はアサインされているものの講義は実施せず，毎回異なる講師のサポートを行っている（たとえば，音響・映像装置の操作，アンケート用紙の配布と回収など）．毎回講師が異なることから，学生にとっては新鮮な印象を持てる講義となる．

シラバスの内容

表 -1 に，シラバスの概要を示す．寄附講義の狙いは，企業の経営層を支援できる人材を育成することである．講師は，筆者および JASA 会員企業において第一線で活躍する技術者や幹部社員である．

講義ではまず，情報セキュリティマネジメントと情報セキュリティ監査の実態を踏まえ，経営者が考えるガバナンス・マネジメントを解説する．次に，内部監査の実務に焦点を当て，(1) 監査基準や管理基準等の考え方，(2) 監査組織の体制や効率的な進め方の枠組み，(3) 具体的な監査手続きの詳細や技術的検証を理解させる．これにより，経営層を支援する人材，つまり「内部監査要員に求められる知識体系」が身につくことから，学生は JASA が定める「情報セキュリティ内部監査人」としての能力認定を得ることができる．なお，講義において組織（国，地方公共団体，企業，大学）の担当者による情報セキュリティマネジメントと監査の事例紹介により，より深い理解を促した．

講義の進め方

講義の構成

講義は 1 コマ 105 分のため，75 分を座学，30 分を事例紹介とした．座学は，学生の集中力を維持するために 3 つのセッション（レクチャー，グループワーク，ラップアップ）から構成される．座学と事例紹介では，教科書を参照することは基本的にはせず，講師が各回のテーマに沿って作成した講義資料を投影しながら解説した．

グループワーク

グループワーク（図 -1）では，講師が各回のテーマに合わせて課題設定を行う．課題の例として「有価証券報告書を読んで，○○社の情報セキュリティ

表 -1　シラバスの概要

(1) 情報セキュリティマネジメントと監査
(2) 事例に学ぶ情報セキュリティ監査の必要性
(3) 情報セキュリティの基準とその活用
(4) 企業経営と情報セキュリティ監査（ガバナンス，マネジメント）
(5) 情報セキュリティを取り巻く法律，個人情報・プライバシ
(6) クラウドの監査，情報セキュリティ人材のキャリアパス
(7) 情報セキュリティ監査の実務
(8) 情報セキュリティ監査演習
(9) 学習の振り返りと試験

リスクの記載内容を調べなさい」などがある．与えられた課題に対して，学生は数名単位のグループを作って議論を行い，その内容を発表する．

事例紹介

事例紹介では，講師の組織で行われている情報セキュリティマネジメントや具体的な監査の取組みが紹介された．例として，ある講師は社内教育用のビデオを紹介し，セキュリティインシデントとその経験を踏まえた対策の見直しを学ぶ機会を学生に提供した．

実務演習

講義の終盤4回は，情報セキュリティ監査のプロセスを学んだあと「認証情報の管理」を具体的な監査テーマとして取り上げ，組織内で適切に運用されているか否かを評価する演習を行った．演習はグループ討議で行った．討議結果の発表，講師の講評後，模範回答と結果を比較することを通じ，気付きを与えるものである．

1つ目の演習は「監査手続の作成」である．グループ内の学生は，組織の規定等を閲覧したあとに被監査人に対して「どのような質問をし，事実を確認するのか」を討議する．2つ目の演習は「組織の評価」である．具体的には，監査人と被監査人に分かれて模擬的な質問を行い，事実確認をしながら組織の評価を行う．

図-1　グループワークの風景

学生の声

学生アンケートの結果

学生による講義アンケートの結果を見ると，寄附講義は3.51（4点満点）であり，コンピュータ科学科3年生を対象とした全講義の平均（3.23）を上回る評価であった．また，JASAが実施したアンケートの満足度は4.1点（5点満点）であり学生にとって満足できる講義であったといえる．

具体的な感想

講義に対する学生の感想（趣旨）を以下に示す．寄附講義の狙い（内部監査要員に求められる知識体系の習得）が達成されたものと考えられる．

1）**事例について：**「企業で行われている対策や事例を聞く機会が得られて大変よかった」「セキュリティ監査の重要性がよく理解できた」「組織によってセキュリティ対策が違うことが分かった」
2）**演習について：**「グループワークや実務演習により，講義を深く理解できた」「企業が公開している資料を参照しながら情報セキュリティリスクについて考えることができ，理解しやすかった」
3）**全体として：**「監査には知識だけでなく，十分な事前準備が必要であることが分かった」「監査人には観察力，すなわち，被監査人に対するインタビューの中で，色々な情報を得る必要があることが分かった」

サイバーセキュリティ演習

背景

セキュリティ人材の教育は，知識習得のための座学と技術習得のための演習に分かれる．産業界での取組みに注目すると，サイバー攻撃において攻撃側と防御側の演習を可能とする環境（サイバーレンジ）を用意し，顧客あるいは自組織に対して当該レンジを用いた実践的なセキュリティ教育を提供するサービスが展開されている．たとえば，CISCOの「シスコサイバーレンジサービス」，NECの「NEC

サイバーセキュリティ訓練場」，DNP による「サイバーナレッジアカデミー」の設立，NTT データ先端技術による「ADI Cyber Range」など，さまざまなサービスが提供されている．

産業界以外でも，高度なセキュリティ人材教育プログラムが提供されている．たとえば，文部科学省「成長分野を支える情報技術人材の育成拠点の形成（enPiT：エンピット）」に採択された「情報セキュリティプロ人材育成短期集中プログラム（ProSec）」，総務省所管の情報通信研究機構による「CYDER」などがある．

演習の概要と指導方針

まず工学院大学情報学部のカリキュラムにおける，サイバーセキュリティ演習の位置づけを示す．本学部では，セキュリティにかかわる技術を基礎と応用に分ける．1～2 年次ではプログラミング演習，情報学実験，コンピュータ科学実験を基礎技術として修得する．3 年次ではサイバーセキュリティ演習を応用技術として修得する．以降では 3 年次に学修するサイバーセキュリティ演習の概要を説明する．

本演習の特徴をひとことで述べると「まっさらな状態」から演習が始まる点にある．演習の冒頭，学生には以下の機材が与えられる（図 -2 には主要な実験機材を示す）．実験指導書などの資料は存在せず，パソコン等の機材は初期状態のままである．

図 -2　主要な実験機材（左上から順に，デスクトップパソコン，ノートパソコン，Raspberry Pi）

デスクトップパソコン，ノートパソコン，Raspberry Pi，各種ケーブル（LAN ケーブルや HDMI ケーブルなど），スイッチングハブ，電源タップ

また，学生には以下の指示が与えられる．

- 学生自身で実験内容（テーマ，目的，実験方法，役割分担など）を決定する．
- 学生自身で上記機材を用いてサイバーレンジを構築する．

教員は，学生に上記の指示を与えたあと，学生の能動的な学修をサポートする．学生には自分自身で実験内容を考えた経験がないことから，「実験内容の例示を行う」，「適切なテーマを決める方法を提案する（たとえば，インターネットで検索するなど）」といったサポートを行う．また，最初から実験内容に完璧さを求めることはせず，「スモールスタート」の考え方をもとに小規模な演習からスタートし，演習中に PDCA（Plan, Do, Check, Act）サイクルを回すように指導を行う．

演習では，問題解決に長時間を要することは珍しくない．たとえば，攻撃用プログラムのインストールや設定がうまくいかず，問題解決に 1 時間以上を要することがある．事前に教員が演習環境を準備しておけば上記問題は発生せず，より高度なサイバーレンジの構築が可能となるだろう．しかし演習では，事前に用意された問題と正解が存在しない状況下で，学生が自分自身の手で問題解決に挑み，その能力を向上させることに重点を置いている．

なかには「演習が予定通りに進まず，サイバーレンジが構築できない」状況に陥ることもある．しかし演習では，学生が諸問題にあきらめることなく取り組み続ける限り「演習に失敗はない」ことを強調している．たとえば，仮想マシンの設定がうまくいかず，演習最終日までにサイバー攻撃の再現ができなかったとしても，「進捗を明確にする」，「問題解決のために行った取組みや考察をまとめる」などを行えば，演習は成功であるとしている．

実践事例

図 -3 は演習時の様子である．学生は与えられた機材で独自のサイバーレンジを構築し，お互いに協力しながら自らの力で演習を進めていく．以下に，2018 年度に実施した演習において学生が自ら設定したテーマを紹介する．演習の自由度の高さと学生の発想の幅を垣間見ていただけるものと考える．なお，本演習では，演習で得た知識を学生が悪用しないための「倫理教育」を行っており，また，マルウェアへの感染に備え，ネットワークの隔離や PC 等の監視を行っている．

- **DNS Water Torture 攻撃の再現と観測：**DNS Water Torture 攻撃をエミュレートするプログラムは教員が提供しているが，サイバーレンジの構築は学生が行う．
- **Web サーバへの HTTP get flood 攻撃の再現と防御：**攻撃には負荷テストツールを使用する．防御は iptables によるフィルタリングである．
- **Easy File Management Web Server への脆弱性攻撃の再現とその対策の検討：**攻撃には Metasploit を使用する．
- **自作プログラムによる DDoS 攻撃の再現とその観測：**サーバ上で文字列を受け取るだけの疑似的なサービスを稼働させ，それに対し DDoS 攻撃を行う．サービスや攻撃を行うプログラムは学生が C 言語で作成する．
- **SQL インジェクションの再現とその対策：**データベースは非常に簡単なもので，SQL インジェクションの再現に必要な最小構成となっている．
- **脆弱性攻撃の振舞いの違いの検証：**Metasploit を用いて，Windows 7 あるいは Windows 10 搭載のパソコンに対して複数の脆弱性攻撃を試みる．
- **マルウェアの動作確認：**インターネットやハニーポット等で入手できるマルウェア，あるいは Metasploit で作成した疑似マルウェアを対象とする．
- **キーロガー検知手法の提案と実装：**Web ページ上に挿入されている JavaScript キーロガーを対象とする．

図 -3　演習風景

今後の予定

本演習は「まっさらな状態」から開始するという特徴を持つ．そのため，学生の設定するテーマに対応する機材やツールが入手できないといった問題や，学生が何をすればよいのか分からなくなるといった問題が発生する．これらは，演習を実施しながら機材の拡充や指導方法を見直していくことによって対応する予定である．なお，2019 年度以降は IoT セキュリティなど対応可能な分野を拡充していく予定である．

特色あるセキュリティ教育を目指して

寄附講義

寄附講義では，第一線で活躍する実務者による講義がオムニバス形式になっているため，学生にとっては毎回の講義が新鮮に映っているようである．講師による事例の紹介や監査の演習では，真剣なまなざしでノートを取ったり，ディスカッションをしたりしている姿（主体的な学びの姿勢）が印象的であった．公認情報セキュリティ監査人としての資格を得た学生が卒業後，企業や団体においてセキュリティの維持向上のために活躍する姿を，教育者として想像せずにはいられない．

サイバーセキュリティ演習

サイバーセキュリティ演習では，演習環境を一から構築するという画期的な試みであったため，当初の予想通り，ネットワークに関するスキルの違いによって演習環境が早く構築できたグループとそうでないグループができた．しかしながら，グループ間で助け合うなどの好事例が見られ，演習後にグループ内で改善点をディスカッションする様子が印象的であった．攻撃や防御といった基本的なスキルを得た学生の中から将来，ホワイトハッカーが生まれることを祈念してやまない．

今後の取組み

本稿では，工学院大学情報学部におけるセキュリティ教育のうち，特色のある寄附講義と演習を紹介した．いずれも新しい試みであることから，より良い内容にするために，講師陣とディスカッションを行いながら試行錯誤を続けている．寄附講義の場合，2018 年度までは「(5) 情報セキュリティを取り巻く法律，個人情報・プライバシ（表 -1 参照)」について 2 週に渡って座学を行ったが，学生の反応がやや食傷気味であったことから，2019 年度は 1 週に減らし，残りの 1 週は監査の基本である「リスクアセスメント」に置き換えた．また，「学生の声」で紹介した講義アンケートとは別に，毎回の寄附講義終了前にアンケートを実施した．当該結果は各講師にフィードバックされており，講義資料の改良（たとえば，文字や図を大きくする，実務演習の内容を充実させるなど）に活かされている．このように，PDCA サイクルを絶えず回していくことにより，内容の充実とともに，最新の技術動向を寄附講義や演習の中に含めていきたい．

現在，文部科学省では，大学において実践的な教育を行うことを目的として，実務家などの学外の人的資源を参画させることが検討されている．寄附講義は当該検討の方向性と合致しており，ユニークな試みであることから，特色あるセキュリティ教育といえる．

工学院大学情報学部では，今後もサイバーとフィジカルに関する包括的なセキュリティ教育を行い，実務者としてのスキルを備えた優秀なセキュリティ・エンジニアを世に送り出す決意である．

(2019 年 6 月 4 日受付)

藤川真樹（正会員） fujikawa@cc.kogakuin.ac.jp
博士（工学）．1998 ～ 2016 年綜合警備保障（株），2016 年工学院大学准教授，現在に至る．本会論文賞，特選論文等受賞．

小林良太郎（正会員） ryo.kobayashi@cc.kogakuin.ac.jp
工学博士．2000 年名古屋大学助手，2008 年豊橋技術科学大学講師，2017 年工学院大学准教授，2019 年同大学教授，現在に至る．

永宮直史 nagamiya-ta01@jasa.jp
特定非営利活動法人日本セキュリティ監査協会事務局長，公認情報セキュリティ主席監査人．野村総合研究所，金融機関等を経て現職．2015 年情報セキュリティ文化賞受賞．