# 情報技術・人文・社会科学を含む体系的な社会人向け サイバーセキュリティ教育プログラム SECKUN の開発

藤岡福資郎 [1)], 小出洋 [2)]

1)九州大学　サイバーセキュリティセンター
2)九州大学　情報基盤研究開発センター
fujioka.fukujiro.843@m.kyushu-u.ac.jp
koide.hiroshi.934@m.kyushu-u.ac.jp

# Development of SECKUN, a Systematic Cybersecurity Education Program for Working People including Information Technology, Humanities, and Social Science

Fukujiro Fujioka [1)], Hiroshi Koide [2)]

1) Cybersecurity Center, Kyushu University
2) Research Institute for Information Technology,Kyushu University

**概要**

九州大学サイバーセキュリティセンターでは、厚生労働省教育訓練プログラムの開発（2 年開発コース）【区分名 ICT 技術を活用した分野】により、「世界の最先端に留まり続ける高度な技術力」と共にサイバーセキュリティ基本法第3条（基本理念）で指摘されている「イノベーションの創出、経済社会の活力の向上」を担う人材を育成する人文科学・社会科学を含む技術に限らない総合的な教育訓練プログラムを開発した。本論文では、同教育訓練プログラムの教材・カリキュラムの内容及び策定までの経緯を説明し、試行を通じて明らかになった課題と対策を検討し、今後のサイバーセキュリティ教育の在り方について議論する。

## 1　はじめに

最新かつ高度なサイバーセキュリティ技術の修得を目的とした教育訓練プログラムは、情報処理推進機構（IPA）の中核人材育成プログラム[1]や情報通信研究機構（NICT）の CYDER[2]等が存在する。主に技術者及び関連する管理者を中心に社内情報システムを守る高度人材を育成することを目的としている[3]。 しかし、「世界の最先端に留まり続ける高度な技術力」と共にサイバーセキュリティ基本法第3条（基本理念）で指摘されている「ノベーションの創出、経済社会の活力の向上」を担う人材を育成できる人文科学・社会科学を含む技術に限らない総合的な教育訓練プログラムは、存在しない。そこで、九州大学サイバーセキュリティセンターでは、厚生労働省教育訓練プログラムの開発（2 年開発コース）【区分名　ICT 技術を活用した分野】により、情報技術・人文・社会科学を含む体系的な社会人向けサイバーセキュリティ教育プログラム「SECKUN」を開発した。受講生 86 名に対して、令和 2 年 9 月より令和 3 年 3 月までの期間で試行中である。(https://cs.kyushu-u.ac.jp/seckun/)

具体的には、セキュリティ高度技術科目群、ブリッジ科目群、マネジメント科目群から成り立つカリキュラムを策定し、受講生の目的に合った4つのリカレント教育コースを設け（①CISO コース、②先端技術者コース、③マネージャー技術者コース、④サイバーセキュリティ技術経営戦略コース）提供している。さらに、複数の提供方式（①ハイフレックス方式、②オンデマンド方式、③スクーリング方式）により、教材の最適化を図るとともに運営面・コミュニケーション面の知見の体系化と集積を目指している。

本論文では、最先端技術と市場を熟知し、情報技術・人文・社会科学を含む一次情報の調査力を兼ね備えた高度なサイバーセキュリティ人材育成の教材・カリキュラムの内容及び策定までの経緯を説明する。

例えば、大学は、社会人教育と共に e-learning 等の環境整備が期待されている。カリキュラムは、受講生の実務的な課題解決と共に意思決定権者（＝経営者層等）の経営課題解決になる内容が求められる事が明らかになった。また、試行を通じ、音響等ハード

面だけでなく、ソフト面では、例えば、ハイフレックス方式は、オンラインと会場の受講生との同時並行のコミュニケーションを講師が行う事が難しく、一体感の醸成に課題が生じた。対策は、入念な事前準備に加え、Slack 上での事前の質問受付やセミナー情報等の話題提供、オンデマンド教材による復習環境整備、第三者が情報を整理することで講師の集中を途切れさせない事等が挙げられる。最後に今後のサイバーセキュリティ教育の在り方を議論する。例えば、高度な技術力と一次情報調査力を備えた修了生等が自律的にイノベーションを阻害するルールを発見・パブリックコメントにより改善を提言するエコシステムの実現により「イノベーションの創出、経済社会の活力の向上」を目指す(図1)。

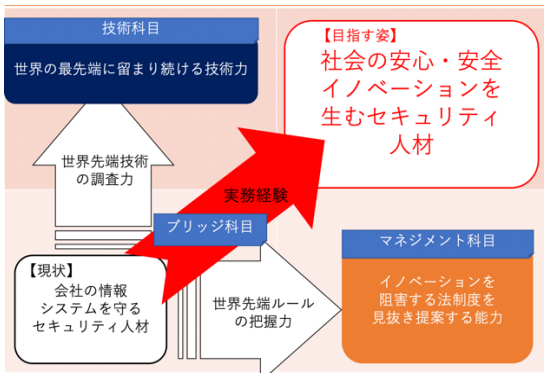


図 1:SECKUN の目指す姿

## 2　カリキュラムの作成

### 2.1 カリキュラムの作成方法

カリキュラムの策定にあたっては、九州大学サイバーセキュリティセンターで策定したカリキュラムを専門的な産官学が連携し、複合的な見地から検討する検討委員会(10 名)を設置した(表 1)　。

表1:検討委員会メンバー所属先組織

| ご所属 |
|---|
| 一般社団法人　九州経済連合会 |
| 株式会社Qtnet |
| GMOペパボ株式会社 |
| 情報セキュリティ大学院大学 |
| 株式会社セキュアスカイ・テクノロジー |
| 株式会社ディアイティ |
| 東京都立産業技術高等専門学校 |
| 株式会社日立システムズ |
| 富士通株式会社 |
| ヤフー株式会社 |

検討委員会は、令和元年度は、3 回開催(12 月、1 月、3 月)した。令和 2 年度は、3 回開催(5 月、7 月、9 月)した。検討委員会に加え、外部専門家を招いたワーキンググループを開催した(3 月)。

令和元年度第1回検討委員会では、「受講生のペルソナを想定し、明確なゴールを定める」ため、サイバーセキュリティ人材に企業や社会の期待をヒアリング等により、明確にすべき旨の指摘があった。そこで、九州経済連合会と連携し、九州・山口の会員企業 1,050 社対象にサイバーセキュリティに関するアンケートを実施し 42 社より回答を得た。(期間:令和 2 年 3 月 1 日～3 月 13 日)九州大学に期待する役割は、①セミナー・勉強会の開催が最も多い。次いで②セミナー型 e-learning、演習教材・演習、③小冊子・PDF 資料、講師派遣と続いた。高等教育機関として、教育を行う役割と共に、学習環境整備の期待があることが分かった(図 2)。

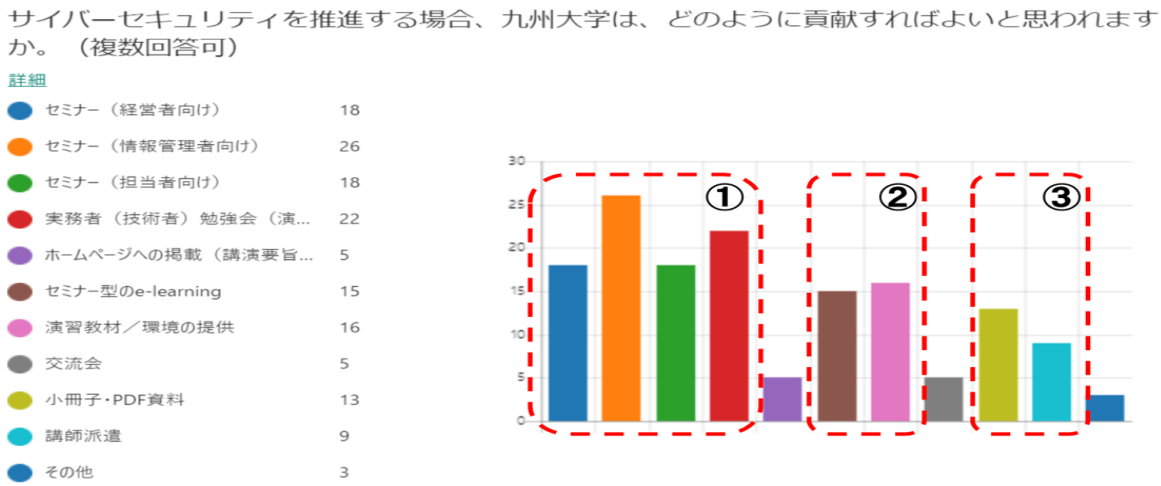


図 2:アンケート結果

令和元年度第2回検討委員会では、「優秀な受講生が集まるカリキュラムの作成」には、教育内容が受講生（＝技術者）の実務的な課題解決に役立つともに、意思決定権者（＝経営層、財務担当）の中長期的な経営課題解決にもつながる内容にすべき旨の指摘があった。そこで、事業継続計画（＝以下、「Business Continuity Plan,BCP」と言う。）を担当する経営企画部等のスタッフ等も対象とした内容を検討すべく、高度な技術の視点に加え、人文・社会科学も含め必要なスキルの洗い出しを行いカリキュラム策定することとした[4] [5]。セキュリティの専門家の育成を柱とし、医療・製造・金融などのユーザ企業の業務知識に精通した人材がセキュリティ分野へジョブチェンジできるリカレント教育の視点も含めることに留意した。

令和元年度第3回検討委員会では、「教育コンテンツ策定（4つのペルソナ／コースと選択科目／レビュー方法）」を検討した。ハイレベル技術者、マネージャー技術者（部下を持つ技術者）、CISO、経営戦略層の4つのペルソナを策定した（図3）。

| コース名 | 目指す人材像と開発する能力 |
|---|---|
| CISOコース | 【セキュリティのラストマンとして組織を牽引】<br>• 最新の技術をフォローできる技術力・調査力<br>• 組織責任者としての意思決定力、BCP構築・運営力 |
| マネージャ技術者コース | 【高い技術力とマネジメント力でチームを牽引】<br>• リーダーとして部下を指導できる高い技術力<br>• 所属組織、顧客の目標を把握・達成するコミュニケーション力 |
| 先端技術者コース | 【最先端技術で社会イノベーションを牽引】<br>• 世界の最先端に留まり続ける技術力<br>• 一次情報からの調査力 |
| サイバーセキュリティ技術経営戦略コース | 【BCP及びイノベーション成長基盤の構築を推進】<br>• サイバーセキュリティ技術経営戦略の企画・実行力<br>• CISO、CIO、経営層への進言・調整力 |

図3：コース名と目指す人材像と開発する能力

セキュリティ高度技術科目群の策定にあたっては、「世界の最先端にとどまり続けることのできる技術者を育成」すべく、最先端の学術研究を題材に一次情報の調査力の醸成に力点を置いた。正解のない問題に対して、正しく問題の所在を設定し、一次情報を調査し、自分の頭で考え行動し一定の答えを追求できる能力を研鑽につながる内容となるよう留意した。

ブリッジ科目群策定にあたっては、例えば、システムを継続運用しサービスを提供したい立場であるCIOとシステムを迅速に停止させ切り離し、原因究明と復旧を目指したいCISOは、危機時に役割が衝突する場面が想定される。そのため、立場の異なる当事者と調整を通じた合意形成を担える「橋渡し型」人材の育成につながる内容となるよう留意した。

マネジメント科目群策定にあたっては、例えば、金融機関、医療機関等各業界のビジネスプロセスや対応するBCPを理解し、サイバーセキュリティとの関係を整理し、円滑な事業継続に資するリーダを育成する点に留意した。

令和2年度第1回検討委員会では、「科目の具体的な内容と留意点」について検討を行った。特にマネジメント科目群のガバナンス、リスクマネジメント、コンプライアンス、インテリジェンス（以下、「GRCI」と言う。）について、専門知識に加え、受講生が主体的に新しいGRCI 態勢構築の提案能力を研鑽できるアフターコロナのビジネス環境変化を捉えた教材を策定すべき旨の指摘があった[6] [7]。また、サイバーセキュリティを危機管理の側面だけでなく、平時からイノベーションを生む投資の側面から捉え、経営層に対して具体的に進言する能力を研鑽するための講義・演習が必要な旨の指摘があった[8]。

令和2年度第2回検討委員会では、「オンライン型コンテンツを策定する際の留意点」を検討した。受講生向けの教材に加え、講師や事務局むけのマニュアルを策定することとした。講師や事務局側のノウハウの蓄積に加え、オンラインだから実現できる受講生メリットを明確にする趣旨である。また、全国の受講生からアンケート等を通じて、講義・演習の内容で自分の経験と反していたところや、言葉の定義，概念の定義で違和感を持ったことも意見収集し、リカレント教育の充実を図ることとした。教材は、受講者のバックグラウンド（受講動機、業務経験、背景）を踏まえ策定する。難易度は、落とさず受講生の自助努力を最大限行ってもらうなかで自らが学び取ってもらう内容になるよう留意することとした。以上から策定したSECKUNのカリキュラムの全体像は、（図 4）に示す通りである。

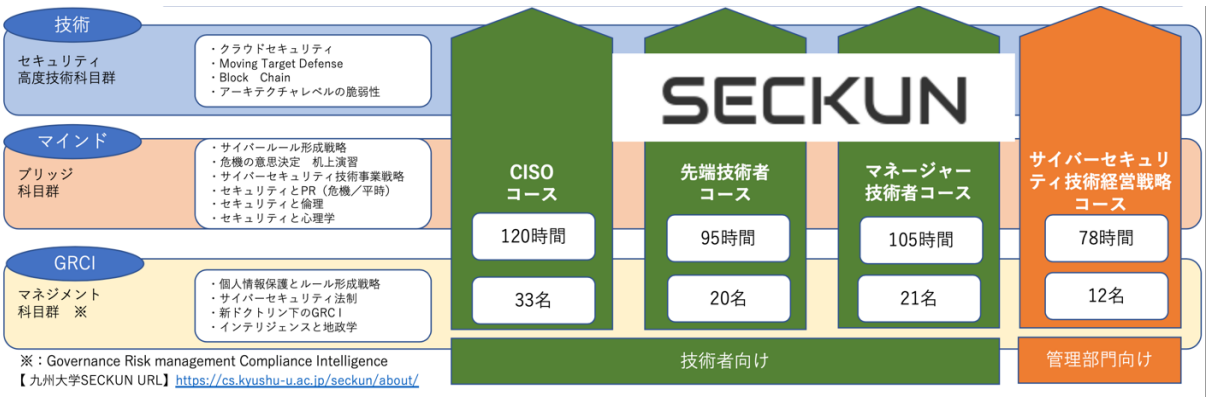


図 4:SECKUN のカリキュラム全体像

## 2.2 カリキュラムの内容

SECKUN は、セキュリティ高度技術科目群(5 科目 42 時間)、ブリッジ科目群(5 科目 42 時間)、マネジメント科目群(8 科目 44 時間)の合計 120 時間から成り立つ。CISO コースは、全科目 120 時間、マネージャー技術者コースは、105 時間、先端技術者コースは、95 時間、技術系科目以外を履修するサイバーセキュリティ技術経営戦略コースは、78 時間を習得する。

セキュリティ高度技術科目群は、実務でのニーズが存在するクラウドセキュリティ、コンテナ技術の実装と設計思想を修得する。最先端のサイバーセキュリティ関連技術研究の調査・考察を実施し、一次情報から自ら高度な技術とそれを習得し続けるための技能を研鑽する(表 2、図 5)。

表 2:セキュリティ高度技術科目群

| 科目名 | 時間数 |
|---|---|
| SECKUN概論 | 4 |
| サイバーセキュリティ技術調査 I<br>【Moving Target Defense】 | 8 |
| サイバーセキュリティ技術調査II<br>【Block Chain】 | 8 |
| サイバーセキュリティ技術調査III<br>【アーキテクチャレベルの脆弱性】 | 8 |
| 情報システムセキュリティ講義/演習 | 14 |
| 合計 | 42 |

図 5:セキュリティ高度技術科目位置づけ

ブリッジ科目群は、高度技術科目やマネジメント科目で習得した高度な知識やスキルを遺憾なくサイバーインシデント発生時に発揮するためのマインドを育むための科目群である。セキュリティと人間を理解するための心理学や倫理を出発点にステークホルダーとの関係を危機・平時の両場面で築いていくためのパブリックリレーションズ戦略に加え、実際に危機が発生したことを想定したサイバーインシデント机上演習を準備している。また、サイバーセキュリティ基本法が定める技術イノベーションを生むという観点を実現するために「サイバーセキュリティ技術経営戦略」を配置した。分野横断的なセキュリティ技術の視点を応用して、具体的な事業課題を解決しイノベーション創出に必要な捉え方を習得する(表 3、図 6)。

表 3:ブリッジ科目群

| 科目名 | 時間数 |
|---|---|
| サイバーインシデント机上演習 | 8 |
| 専門用語・知識をわかりやすく的確に社会へ伝えるPR平時の備え | 5 |
| セキュリティとPR戦略 | 5 |
| セキュリティと倫理 | 5 |
| サイバーセキュリティ技術事業戦略 | 6 |
| セキュリティ心理学 | 5 |
| 合計 | 34 |

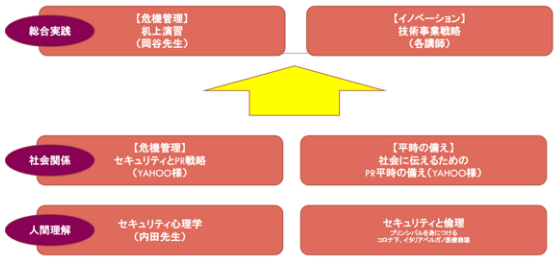


図 6:ブリッジ科目群位置づけ

マネジメント科目群は、サイバーセキュリティ法制やコンプライアンス経営をテーマとした包括的な法制度の一次情報調査力を醸成するとともにデジタルプラットフォーマ規制や個人情報保護法制といった実務的な最先端の課題に取り組む。現在の法制度がイノベーションを生む阻害要因になっている点はないかを自らが調査し、改善案と共にパブリックコメント等で発信できる能力をサイバーセキュリティとイノベーション（＝ルール形成的思考から学ぶ新規ビジネス創出の在り方）で研鑽する点に特徴を有する[9]。

セキュリティ心理学、インテリジェンスと地政学の分析系科目とリスクマネジメントの対策系科目を俯瞰して教材を策定し一貫性を高めた。セキュリティとガバナンスは、災害時の危機管理や BCP を踏まえた内容[10] [11]とし、サイバー攻撃をきっかけとしたインシデント対応に対応できる包括的な視野と専門知識を身につけることができる点が特徴である（表 4、図 7）。

表 4:マネジメント科目群

| 科目名 | 時間数 |
|---|---|
| サイバーセキュリティとイノベーション～ルール形成的思考から学ぶ新規ビジネスの創出の在り方 | 8 |
| 個人情報保護法制 | 5 |
| サイバーセキュリティ法制 | 5 |
| デジタルプラットフォーム規制とセキュリティ～EUの競争政策の実務を中心に | 5 |
| セキュリティとガバナンス | 6 |
| セキュリティとリスクマネジメント | 5 |
| セキュリティとコンプライアンス経営 | 5 |
| インテリジェンスと地政学 | 5 |
| 合計 | 44 |

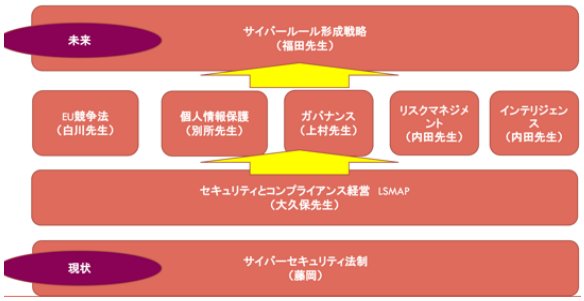


図 7:マネジメント科目群位置づけ

## 3 カリキュラムの試行

### 3.1 受講生の属性

受講生の募集は、令和 2 年 6 月 23 日から同年 7 月 20 日に実施した。募集にあたっては、SECKUN のホームページへ募集要項を掲載するとともに、オンデマンド方式の説明会を開催した（図 8）。

図 8:オンデマンド説明会模様

説明会は、掛け合い形式（教員2名）で実施し、双方向感を醸成した。はじめに SECKUN が想定している人材像を説明した上で、受講生が目指すゴールの実現のために4つのコースと3つの科目群を準備している点などの特徴を中心に説明した。さらに女性を含む幅広い層の受講を促すため、九州大学の enPiT-Pro セキュリティの修了生に出演いただいた。受講中の家庭との両立の方法等をお話いただき不安解消につなげるコンテンツを提供した(図 9)。

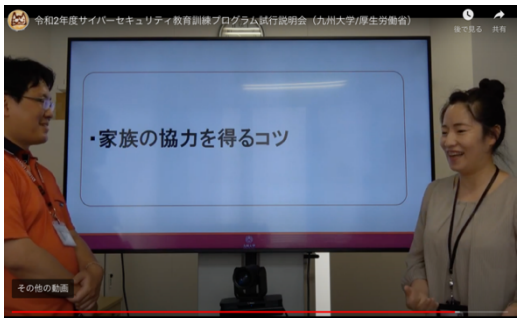


図 9:受講体験談模様

また、検討委員会のメンバーへ所属の企業・組織での周知をお願いしご協力いただいた。九州経済連合会のホームページに掲載いただいた。(https://www.kyukeiren.or.jp/news/index.php?id=3189)YAHOO 株式会社のホームページ「ステークホルダーダイアログ 2020」でご紹介いただいた。(https://about.yahoo.co.jp/csr/report/015.html)

結果として、ミスマッチのない 86 名の受講生を確保できた。SECKUN の受講生の年齢層は、20 代～60 代と幅白く、平均年齢は、40 歳であった。居住地域は、福岡県が 53 名で全体の約 6 割を占める。関東圏(東京・神奈川・千葉)が 21 名。大阪府、愛知県、兵庫県、広島県に受講生が存在する。職種は、医療・電力・通信・金融・製造・ベンチャー企業経営者・司法官憲・高等教育機関教員まで幅広く在籍している。コース別では、CISO コース 33 名、マネージャー技術者コース 22 名、先端技術者コース 21 名、サイバーセキュリティ技術経営コース 15 名であった。

### 3.2 試行結果（ハイフレックス方式）

ハイフレックス方式で実施した「SECKUN 概論」及び「Moving Target Defense 演習」(以下、「MTD 演習」という。)の結果を説明する。「SECKUN 概論」は、ガイダンスとして各科目の概要、スケジュールやツールの活用方法等を紹介した(図 10)。

図 10:SECKUN 概論講義模様

ガイダンスながら、三密回避のため、全員の顔合わせができず講師と受講生の一体感の醸成に課題があった。そこで、以下の施策を試行した。

- 開講前に Slack 上で自己紹介を実施。また、質問に対しても開講前から対応した。
- 講師への質問を予め募り、会場で講師が答えることで、双方向性を醸成した。
- 講義中のチャット上の質問を講師が随時応対し、会場とオンラインの場の共有を図った。

実施後の課題としては、以下の点が挙げられた。

- Slack が投稿により随時更新されるので、情報のフォローに苦慮する受講生が複数名いた。
- 講義中の会場やオンラインから質問・コメントの情報の整理を行わないと講師が講義に集中できない懸念があった。
- 会場の音響設備とオンライン配信用の機材の干渉でエコーノイズが発生し対応に苦慮した。

ハイフレックス方式は、会場の模様を一方向で配信する方式と異なり、双方向性が強みだが、会場とオンライン上の受講生の一体感・空気感を醸成しながら、講師が集中できる環境づくりが重要であることが分かった。受講生が「試行」の意味を理解し、受講生も SECKUN を共に創り上げる当事者意識をもってもらうことに成功した。現在では、受講生が自発的に「勉強会・講演会情報の告知」、「オンライン懇親会の開催」、「講師・教材づくりへの参画の申出」、「受講生同士のフォロー」を提案するなど活況を呈している(図 11)。

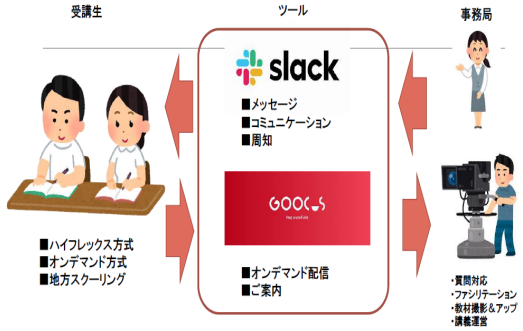


図 11: SECKUN 運用体制

「MTD 演習」は、セキュリティ技術研究の最先端テーマのカーネルレベルの MTD、ネットワークレベルの MTD を含む演習教材を開発した(図 12)。MTD とは除法システムの変更可能なパラメータを変更することにより、攻撃側の攻撃のためのコストを増大させる比較的新しい防御手段である[12]。

図 12:MTD 演習の模様

難易度が高い最先端のテーマであることに加え、受講生のレベルが分散している点に課題があった。そこで、以下の施策を試行した。

- 教材を受講生に予め配布しテーマの理解を深めてもらった。さらに環境設定用の映像教材(約20分)をオンデマンド方式で提供した(図13)。

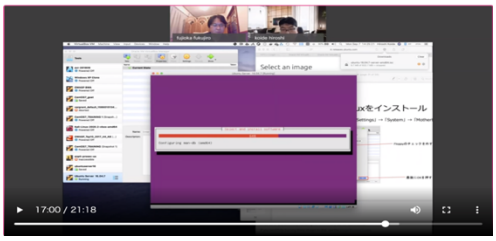


図13:環境設定用の映像教材

- MTDの環境設定が十分でない受講生のフォローのため、専任TA(1名)を配置し、専用のオンラインミーティングチャンネルを開設し対処した。
- 会場やオンラインの疑問を随時講義で取り上げ一体感を醸成し、理解度の向上を目指した。また、講義録画をオンデマンド提供して、欠席フォローおよび疑問点の繰り返し視聴環境を整備。

実施後の課題としては、以下の点が挙げられる。

- 事前準備及び授業中のフォローは、充実していたが、難易度が高く感じた旨の申出があった。

申出のあった受講生は、その後、オンデマンド教材を見直し、講師や受講生に自発的に質問を通じ教材を理解し課題提出レベルに自ら到達した。高度な内容の教材を技術レベルが分散している受講生に提供する場合、オンデマンド教材の提供と質問フォローの充実により、受講生のレベルを引き上げ、教材のレベルを下げずに対処できることが分かった。

### 3.3 試行結果（オンデマンド方式）

サイバーセキュリティ法制は、高度な法的知識を身につけ、法制度の構造や関連、位置づけの調査能力研鑽を目的とした教材である(1時間×5回)(図14)。

図14:サイバーセキュリティ法制配信画面

第1回目は、サイバーセキュリティ「関連」法制を洗い出し、箇条書きにするというテーマとした。第1回の実施後の課題としては、以下の点が挙げられた。

- IoTは、製造物責任が関連となり整理が難しい。
- ソーシャルエンジニアリングは、判断が難しい。
- ソースにより関連の範囲が異なり調査が難しい。

サイバーセキュリティ関連の法制度に関する講義や演習は、現場での問題解決や紛争予防を目的として、主に近時のトピックスを事例として取り上げ提供されている。「関連」は、所与のものとして、専門家から専門書やセミナー通じ知識として吸収されているが、自らスコープを持ち一次情報から関連を定義づける能力は研鑽の余地がある事が明らかになった。

## 4 考察

技術関連科目では、一次情報調査に重点を置き演習を行い受講生の主体的な調査力の向上に資した。同様のアプローチは、ブリッジ系科目やマネジメント系科目でも有用である。例えば、サイバーセキュリティ関連の法制度は一つの法典はなく、関連から成り立っており、本来は、業界や業種により異なる。一次情報である目次や条文から構造を捉え、一般法との比較を通じ、自ら「関連」する法制度を捉える力を育成すれば、現場を知るセキュリティ技術者等が自社に最適な対応を経営企画部や法務部などと連携し経営層に進言することが可能になる。更に法制度が海外と比べて整備されていない部分や改善点をパブリックコメントにより政府に提言しイノベーションを促進する法制度を自律的に産むエコシステム創出も視野に入れ受講生の実務課題解決と共に意思決定権者(経営層等)の中長期経営課題解決に役立つ内容を追求したい。

## 5 今後の検討課題

試行運営上の課題と対策の概要を表5に示す。今後の検討課題は、ソフト面は、受講生・講師が集中できるコミュニケーション環境を生み出すことであり、自由発言や一体感を生み出しつつも規律ある運営ルールが求められる。設備・音響のハード面の課題は、事前に実際の会場でテストする事が挙げられる。授業運営では、PDF資料からプログラムコードをコピーすると

エラーが生じる事をアナウンスする。コピー用のコード集を準備するなどオンライン特有の配慮を洗い出す事が求められる。受講生メリットを追求した教育訓練の在り方を今後も検討・研鑽し続けたい。

表 5:試行運営上の課題と対策の概要

| カテゴリー | 課題 | 対策 |
|---|---|---|
| 音響・装置 | 会場音響とオンライン機材の干渉 | 事前の試行。会場音響に頼らない |
| | WEBEX動画配信で音が伝わらない（＝画面共有） | 事前の試行。マイクで拾うなど代替手段を準備 |
| | 環境ノイズとマイク設置位置 | 必要な箇所に集中して配置。臨場感とのバランスをとる |
| コミュニケーション | 会場とオンラインの一体感 | Q＆Aを書き込む場所を指定しつつ、会場とオンラインが分かれないよう配慮(例)会場の様子を専用カメラで放映 |
| | 会場受講生のメリットの醸成 | 直接質問ができる点を活かす(例)質疑応答は、カメラに入ってもらう |
| | タイムマネジメント | 大きな時計を置くなど話者同士で時間間隔を共有。 |
| 授業運営 | PDF資料からのコピー＆ペーストによるエラー発生 | 直打ちまたは、必要なコードは、一覧にして配布 |
| | 講義時間 | 60分ごとに切る。 |

## 謝辞

本論文の作成にあたり、厚生労働省教育訓練プログラムの開発（2年開発コース）【区分名　ICT 技術を活用した分野】の委託を受けている。また、隔月にて開催している同プログラムの検討委員会メンバーの井上隆男（一般社団法人九州経済連合会，敬称略。以下同様）、江川哲也（株式会社 Qtnet）、近藤宇智朗（GMO ペパボ株式会社）、湯浅墾道（情報セキュリティ大学院大学）、長谷川陽介（株式会社セキュアスカイ・テクノロジー）、山田英史（株式会社ディアイティ）、竹迫良範（東京都立産業技術専門学校）、折田彰（株式会社日立システムズ）、佳山こうせつ（富士通株式会社）、日野隆史（ヤフー株式会社）、同委員会・WG 等にオブザーバーとして参加していただいている岡谷貢（元内閣官房、元防衛省）、福田峰之（多摩大学客員教授）、内田勝也（情報セキュリティ大学院大学名誉教授）、上村章文（RRPF 地域創生プラットフォーム代表）、松本照吾（アマゾンウェブサービスジャパン株式会社）から貴重な意見・提案を頂いた。

## 参考文献

[1]独立行政法人情報処理推進機構，中核人材育成PG,https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html（2020 年 10 月 14 日アクセス）

[2]国立研究開発法人情報通信研究機構、実践的サイバー防御演習「CYDER」,http://cyder.nict.go.jp（2020 年 10 月 14 日アクセス）

[3]内田勝也,サイバーセキュリティ教育・訓練の提言,情報処理学会研究報告コンピュータセキュリティ（CSEC）88 巻 2 号,pp.1-7(2020)

[4]内田勝也,欧米企業の現役 CIO/CISO が集う名門サイバーセキュリティ教育コースの中身,https://it.impress.co.jp/articles/-/17405（2020 年 10 月 14 日アクセス）

[5]林紘一郎,情報セキュリティの社会科学的側面,安全工学 54 巻 6 号,pp. 479-485（2015）

[6]横浜信一,経営とサイバーセキュリティ,日経 BP 社,pp.220-245（2018）

[7]佐々木良一,木下翔太郎,「つながる世界」のサイバーリスク・マネジメント,東洋経済新報社,pp.53-86(2020)

[8]大河内智秀,竹内文孝,伊藤潤,決定版　サイバーリスクマネジメント,NTT出版,pp.53-86（2019）

[9]國分俊史,福田峰之,角南篤,世界市場で勝つルールメイキング戦略,朝日新聞出版社,pp.134-162（2017）

[10]上村章文,自治体の危機管理マニュアル,学陽書房,pp.214-259（2008）

[11]林紘一郎,田川義博,淺井達雄,セキュリティ経営,勁草書房,pp.8-19（2011）

[12]Sushil Jajodia,Anup K. Ghosh,Vipin Swarup,Cliff Wang,X. Sean Wang,Moving Target Defense: Creating Asymmetric, Uncertainty for Cyber Threats (Advances in Information Security Book 54) (English Edition) ,Springer,pp.29-47 (2011)