【文部科学省】Society5.0に対応した高度技術人材育成事業
成長分野を支える情報技術人材の育成拠点の形成（enPiT）

Education Network for Practical Information Technologies

enPiT Pro Security

ANNUAL REPORT 2022

2022年度 事業報告書

企業・官公庁等のIT実務、OT実務、設計・製造実務における
情報セキュリティに関わるプロ人材育成コース

1．enPiT-Pro Security

1.1 本事業の目的

IT に対する需要は引き続き増加する見込みにも関わらず、労働人口の減少による人材供給力の低下から、IT 人材の不足は今後一層深刻化する可能性が高いことが予測されている。このような状況の中、大学教育改革により、情報科学技術分野の質の高い人材を多く輩出することや、産学連携によってすでに社会で活躍している同分野の人材の生産性を高めるための学び直しに貢献することが我が国の高等教育機関に求められている。このことを目的とした事業である文部科学省 2017 年度「成長分野を支える情報技術人材の育成拠点の形成（enPiT）enPiT-Pro」の公募の結果、「情報セキュリティプロ人材育成短期集中プログラム （ProSec）」（申請代表校：情報セキュリティ大学院大学）が 採択された。

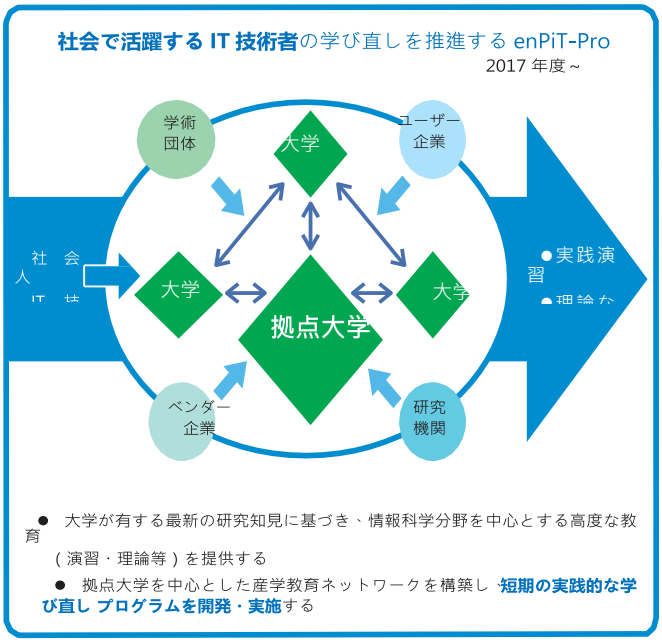
1.2 情報セキュリティプロ人材育成短期集中プログラム（ProSec）

情報セキュリティ人材のニーズは急速に高まっており、 活躍の場はセキュリティ製品・サービスを提供する IT 企業 だけでなく、非 IT 企業を含む全ての企業にとって自社の持つ情報やシステムのセキュリティを高める上で欠かせない 人材になっている。2016 年には国内の情報セキュリティ業務に 28.1 万人が従事しており、13.2 万人が不足し、今後も人材不足が増加すると推計されている。このため社会人の再教育による人材シフトが喫緊の課題となっている。また、大学院教育が生み出す人材と産業界が求める人材のミスマッチも指摘されており、大学院教育においても産業ニーズを意識した適切な人材育成を行うことへの変革が求められている。

申請は、「情報セキュリティ人材育成に関する調査研究」で提唱されたモデル・コア・カリキュラムを実践に移すため、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学が連携して社会人の学び直しを支援する高等教育の体制を 整えることで、さまざまな実務現場で情報セキュリティリーダーとして活躍できるトップ層の人材を育成することを目標としている。本プログラムでは、銀行システムの開発、自動車の製造部門やプラントの保守部門など、企業・ 社会の安全を維持するために不可欠な実務現場での情報セ キュリティのリーダー人材を育成する。本申請では、BP 認 定も可能な 120 時間超の学修を実施するメインコースと、必要な知識・技能のエッセンスを短期間（30 時間～60 時間）に学修可能なクイックコースを実施する。メインコースは大学院の enPiT で整備した既設講義に加えて、IoT や Fintech などのホットトピックスに対応した講義やサイバーレンジ等の演習科目を新設した魅力あるコース構成とし、クイックコースはメインコースを部分的に受講できる構成としている。

講義や演習の開講日時の配慮等により、社会人の学びやすさや地方都市の学修機会の確保に努め、 取得した単位は大学院入学時に履修単位の一部として認定するとともに、履修証明や BP 認定の取得も可能な仕組みとしている。また、日本ネットワークセキュリティ協会(JNSA) が開発した情報セキュリティ人材スキルマップをベースに改良して、各大学の講義内容がカバーしている知識セットを可視化することにより、連携大学が提供するコースが一定の水準に達していることを確認できるようにした。

図1：enPiT-Pro事業全体イメージ



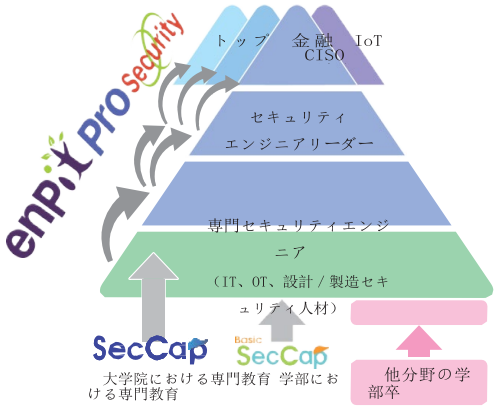


図2：セキュリティ人材育成における ProSec の位置づけ

全てのコースで全連携大学共通の枠組に基づくProSec-X 認定証を授与できる枠組みを構築している。これらの取り組みにより、水準の確保された質の高い教育を提供することに努めている。

▸産学連携体制

産業界との連携体制は、

(1) 企業の全国ネットワークを持つ団体との連携

(2) 地域の企業団体、個別企業との連携 の 2 層で構成している。全国ネットワークを持つ企業団体と連携して、産業界全体でニーズの高い人材の育成に注力する。具体的には、代表校 (情報セキュリティ大学院大学) が (特非) 日本ネットワークセキュリティ協会 (JNSA)、(一 社) サイバーリスク情報センター (CRIC) と連携して ProSec 運営委員会と協力して産業ニーズに応える教育コースの開発を支援する。JNSA は日本全国に 265 社を越える会員企業を擁し、企業に在籍する 20 名超の実務家教員 からなる登録制の講師データベースを維持している。これらと協力して進めることにより、産業界との調整、地域企業への社会人再教育プログラムの周知、連携大学への講師の派遣を実施する。他方、連携大学は各地域において地域の企業団体、個別企業と連携し、教育コースの充実、受講生の募集、企業研修としての活用促進を行う。

▸情報セキュリティ人材スキルマップ

大学が育成を目指す人材像と産業界が求める人材像のミスマッチがしばしば指摘されている。いわゆる企業の情報システム部門等における IT 実務だけでなく、社会インフラシステムの運用を担う OT (Operational Technology) 実務、家電製品から自動車や大規模プラント等の設計 / 製造実務まで、実務の内容によって期待されるプロ人材像が異なる。加えて、地域の地場産業の特徴も考慮すれば、求められるセキュリティのプロ人材像は更に多様となるであろう。連携大学が各地域の産業と連携して人材スキルマップで求められる人材像の認識を共有し、それぞれの産業ニーズにあった教育コースの開発によってミスマッチの解消を図っていく。

本事業においては、JNSA が策定・公表したスキルマップである SecBoK2016 を参照して、連携大学が提供する教育プログラムが SecBoK に記載されているスキル・知識をカバーするように配慮している。

連携大学が提供する内容をスキルマップ化し、SecBoK と対照させることにより、産業ニーズと提供する教育コースとのミスマッチを防ぐこととしている。2021～2022 年度にかけ、JNSA が 2019 年度に公表した SecBoK2019 をベースにしつつ、スキルマップを現場で運用されているアドバイザリーボード委員の方の意見などをとりいれ、スキルマップの改善を行った。SecBoK2019 は米国 NIST における同様の NICE Framework が改訂され、SP800-181 が規定されたなどの動向を踏まえたうえでの改訂である。情報セキュリティ分野の知識スキルは、SecBoK2019 に記載できていない詳細なスキル・知識もあると考えられることを想定しつつ、活用可能な部分については今後の提供コースに反映する事とした。また連携企業との意見交換を重ねた結果、2022 年度に 36 のスキル項目と 5 つのロールからなるスキルマップを提案した。このスキルマップは体系的な教育がカバーする範囲を大まかに確認すると共に、技術者が自分のスキルを確認するための仕様となっている。今後は、改善後のスキルマップをベースにコースの設計、提供、評価を行っていく予定である。

1.3 各分野の概要

▸提供するコースの概要

2007 年の学校教育法の改正により「履修証明制度」が創設され、大学院は履修証明プログラムを開設し修士号、博士号に加えて、その修了者に対して法に基づく履修証明書 (Certificate) を発行できるようになった。履修証明者は「職業能力証明書 (ジョブ・カード・コア)」として位置付けられており、客観的な証明書として利用できる。

ProSec では、実務家教員による授業や PC を使った演習授業を多く取り入れた実践的なコースを提供する。正規コースの大学院生に混じって 6 ヶ月から 1 年で修了するメインコース (履修証明プログラム) と、必要な知識・技能のエッセンスを短期間 (1週間～3 ヶ月程度) に習得できるクイックコースを提供する。メインコースは大学院の enPiT で整備した既設講義に加えて、IoT や Fintech などのホットトピックスに対応した講義やサイバーレンジ等の演習科目を新設した魅力あるコース構成とし、クイックコースはメインコースを部分的に受講できる構成としている。講義や演習の開講日時の配慮等により、社会人の学びやすさや地方都市の学修機会の確保に

努め、取得した単位は大学院入学時に履修単位の一部として認定すると共に、履修証明や BP 認定の取得も可能な仕組みとする。文部科学省「情報セキュリティ人材に関する調査研究」で提唱されたモデル・コア・カリキュラムに基づき、業種、職種や地域によって異なる産業ニーズに合わせ、多彩な教育コースを編成する。

教育コースは、メインコースとクイックコースの 2 種類のコース構成で提供し、実践的な演習や実務経験の豊富な企業在籍の教員による最先端の講義と、体系的な知識の習得を目指す大学院の正規科目を組み合わせたバランスのとれた教育コースとしている。修了者には、ProSec-IoT や ProSec-CSIRT 等の習得したコースに応じた修了証を発行する。また多様な受講ニーズに配慮し、クイックコースよりもさらに短時間のコースを開講した。

▸教育プログラムを通して育成する人材像

産業界や官公庁で、広く IT 実務、OT 実務さらに設計・製 造実務を担っている人材が、更にセキュリティ実践力と体系化されたセキュリティ知識を学修することにより、社会・経済活動の根幹に関わる情報資産および情報流通のセキュリティ対策を技術面・管理面で牽引できる実践的リーダーを育成する。例えば、セキュリティマインドをもつシステム開発技術者・データ解析技術者 (ProSec-Mind)、情報セキュリティの基盤理論に裏付けされた強い実践力を持つセキュリティ技術者 (ProSec-EC2 (Engineer of Crypto and Cybersec)) や、サイバー攻撃の脅威が大きい金融分野に特化した講義を通じて、金融情報システムの実務における情報セキュリティのリーダー人材 (ProSec-Fintech)、企業や官公庁の CISO (Chief Information Security Officer) として組織のセキュリティマネジメントを牽引できる実践 的リーダー (ProSec-CISO) などを育成する。

▸2022 年度の実施状況

2022 年度は 2021 年度に引き続き、各連携大学ともに新型コロナウィルス感染症 (以下、COVID-19) 対策として、コースのオンライン化 や、オンライン化できないコースについては感染対策を徹底した上で対面授業の実施など、工夫してコースを提供した (連携大学の実施状況についての詳細は、「2 連携大学の実施状況と計画」を参照)。

また連携大学間の情報共有とプログラム実施にあたって の意見交換の機会として、運営委員会と幹事会を月に 1 度 のペースで開催した。運営委員会の下にはワーキンググ ループを設け、産学連携を推進すると共に、各連携大学の 実施上の課題や地域ごとの産業界・社会のニーズなどに関 する知見の共有を図っている。ワーキンググループおよびメンバーは **図 3**

WG	サブ	メンバー
教務 WG	スキルマップ	山口（長県大）
	コース連携	大久保 *(情セ大) 砂原（慶應）
産学連携 WG		砂原 *（慶應）
評価WG		宮地 *（阪大）
FD WG		加藤 *（慶應）和泉（東北）
広報WG		内尾 *（和大）

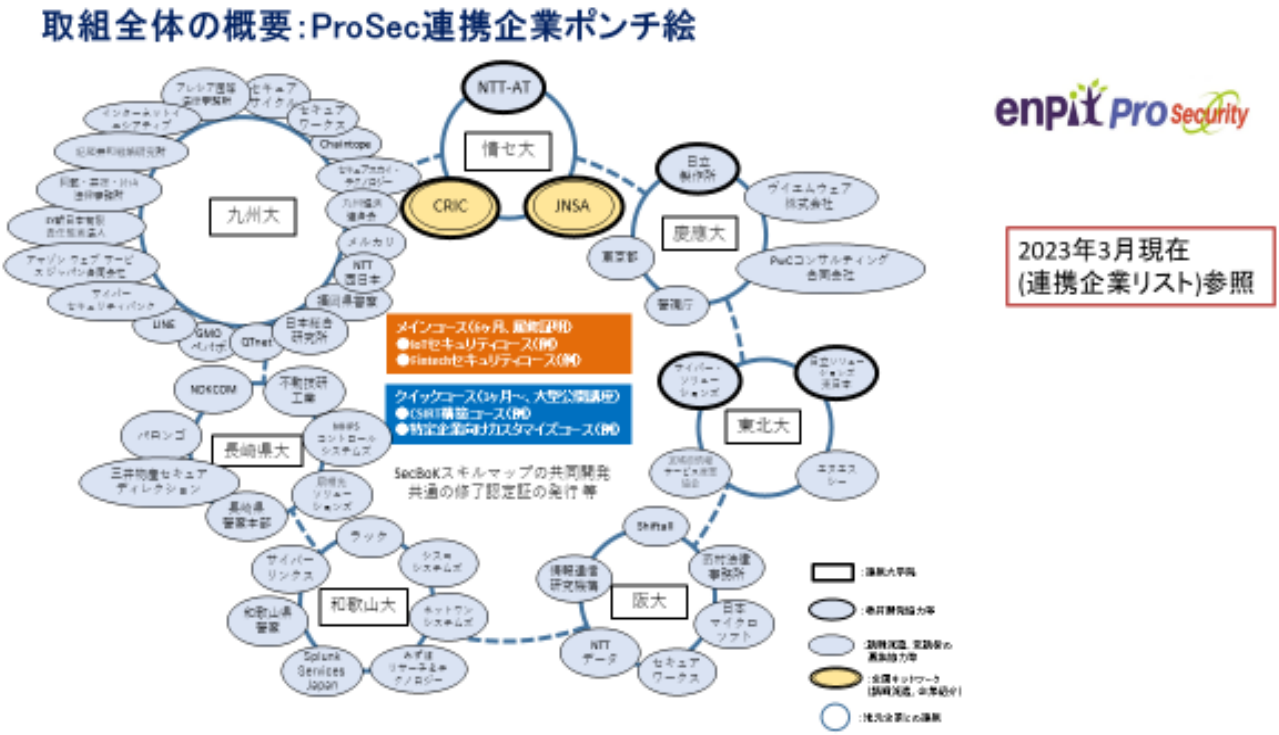
図 3：ワーキンググループ

* は主担当者

運営委員会では、意見交換と対応策の検討を行っている。また、 人材育成の方法の改善やプログラムを担当する教員の能力 向上に向けたファカルティ・デベロップメント（FD）の取り組みも行っている。2022 年度は、前年度に引き続き各連携大学の施設や演習実施方法等についてオンラインも含めた相互参観と意見交換を行うほか、短時間でコンパクトに学修したいというニーズに答えるため、ユニット制の導入と連携校間でのコースのコース組合せにより修了可能とするコース連携の仕組みや、育成効果の測定や適切なコース選択のためのスキルマップの整備、効果的な人材育成方法の確立に向けて演習教材の整備と蓄積、オンライン教育に使用するソフトウェアやツール類のノウハウの共有、オンラインで効果的に教育するための工夫の共有等によって、各連携大学の FD 活動の内容を詳細に共有することとし、各大学が提供するプログラムへのフィードバック・改善を図った。

また実践教育を実施できる教員の養成を図るため、各連携大学は、社会人等の実務家に演習の講師や非常勤講師を委嘱し、企業における研修や実務研修等の教育ノウ

ハウの吸収と共有を図っている。一方、各連携大学は、
　特任教員を採用したり専任教員を本事業に従事させたりしているが、 各教員は、本事業に参画することにより、それぞれの教員の研究内容や実務経験を活かしつつ各プログラムの講義や演習を実施することで、体系的な教育を実施するための教育を実践するスキルを身につけている。



2． 連携大学の実施状況と計画

2.1 情報セキュリティ大学院大学

取り組み概要

情報セキュリティ大学院大学は、2022 年度の enPiT-Pro Security（ProSec）の取り組みとして、以下の内容を実施した。

◦メインコース

履修証明プログラムに対応するメインコースとして、次のコースを募集した。

◦次世代 Fintech セキュリティとデータ・サイエンスメインコース

◦企業経営向けビッグデータ分析とリスク経営メインコース

次世代 Fintech セキュリティとデータ・サイエンスメインコースは、次世代の金融システムの設計開発とその情報セキュリティ対策のリーダー人材を育成するコースである。金融機関等の企業や官公庁等において、最新の金融システム開発やその情報管理業務に従事した経験を持つ情報技術者や管理系業務従事者、およびこれらの職種を志望される方々に向け、次世代 Fintech のコア技術の一つであるブロックチェーンの理論、事業リスクマネジメント実務においても重要なデータ・サイエンスに関する知識等、今後の経済社会が求める実践的な理論や知識をバランスよく習得していただくためのプログラムを提供する。

企業経営向けビッグデータ分析とリスク経営メインコースは、企業経営実務においてビッグデータ分析を技術面・管理面で引率できる実践的リーダーを育成するコースである。セキュリティマネジメント、リスク評価・マネジメント、セキュリティ経営、IT ガバナンス、人的要因等の業務遂行必要な知識、スキルを習得していただくためのプログラムを提供している。

◦クイックコース

クイックコースとして、次のコースを開講した。

◦セキュアシステム技術（基礎）クイックコース　−NW 攻撃とその防御および検知−

◦IoT セキュリティクイックコース

◦CSIRT 構築クイックコース（新設）

◦特別コース
クイックコースより短期間にエッセンスを学ぶことのできるコースとして今年度も特別コースを開講した。他の ProSec コースや他大学の ProSec コースと連携して修了を目指すことができるコースである。

◦CTF の基礎コース（オンライン）

セキュアシステム技術（基礎）クイックコースは、「ネットワーク経由の情報セキュリティ攻撃とその防御および検知」をテーマとし、攻撃者がどのようなツールや手段を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、実習を通じて理解を深めることを目指すコースである。
IoT セキュリティクイックコースは、IT 系、組み込み系の技術者が新たに考慮すべき IoT のセキュリティについて、講義と演習を行うコースである。
CSIRT 構築クイックコースでは、講義と演習を通じてインシデント対応の基本的な活動を理解する。また、インシデント発生時における様々な対処方法を習得する、実践力を高めるコースとなっている。
また特別コースとして開講した CTF の基礎コースは CTF(Capture The Flag) に関連する基本知識解説とクイズ形式の CTF を通して、受講者のサイバーセキュリティの技術力に関する課題を洗い出しながら実践力の強化を目指す企業研修に適したコースである。
その他、企業向けに IoT セキュリティコースの演習部分を中心としたカスタマイズコースとして、IoT 特別コースを開講した。

実施状況

2022 年度の受講者は 36 名（内、特別コースは 21 名）、修了者は 14 名であった。
メインコースは、大学院が提供するコースとしての特色を活かし、講義、実習、受講者同士の討議を取り入れた演習などの多様な方法により業務遂行に必要な知識、スキルを幅広く修得することができるように配慮している。セキュアシステム技術（基礎）クイックコース-NW 攻撃とその防御および検知-は、講義形式の解説と実習形式をミックスした形の授業により進行し、セキュリティについて基礎から知識を得られるとともに、Windows と Linux の OS を使用して実機による実習形式での演習も実施した。このことにより受講者は実践的な知識および能力を習得することができた。
IoT セキュリティコースは、今年度は対面で実施し、脆弱性検査や脅威分析の演習を受講することができた。
CSIRT 構築クイックコースは、CSIRT 構築に向けての基礎講座および技術演習コースを行い、受講生はセキュリティインシデント対応の基本的なプロセスやその対応策を解説と演習を通して修得することができた。

特別コースとして開講した CTF の基礎コースでは、CTF の基本講座として企業研修に最適なコースとして開設した。本コース受講生の内、1 名が他大学の連携コース「インシデントハンドリングコース」（慶應開講）を受講している。
IoT 特別コースは、特定企業の要望により、IoT セキュリティコースの演習部分を中心としたカスタマイズを行い、特別コースとして実施した。

なお、2021 年度で補助期間は終了しているが、本学では従来から社会人向け短期集中コースを実施してきているため、補助期間の終了の際に、これらの集中コースと統合して全体を ProSec コースとして開講することにより、受講者の確保を継続することができている。また 2022 年度は COVID-19 の感染状況も一段落したため、ほとんどのコースをオンサイト(一部オンライン)で実施した。併せて受講者の利便性を考慮し、今年度より主な ProSec コースを東京オフィス(丸の内)で開講した。

写真 1　IoT セキュリティコースの様子

来年度の計画

来年度は、システム以外の分野を含めた、より幅広いリスクへの対応を図るための講座として、IoT セキュリティコースの一部であった脅威分析講座を分離し、内容をさらに拡充した別コースの開講を予定している。これにより、受講者層のさらなる拡大を期待する。広報に関しては、横浜の産学公民連携推進組織である横浜未来機構の研修サイトに本学の各 ProSec コース案内を掲載いただき、一層の受講者開拓を目指す予定である。

募集情報

問い合わせ先: 情報セキュリティ大学院大学 ProSec 事務局
〒221-0835　神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail : prosec@iisec.ac.jp
Web: https://www.iisec.ac.jp/admissions/prosec/

2.2 東北大学

取り組み概要

東北大学では、2022 年度の ProSec の取り組みとして、引き続き以下の 1 つのメインコースと 2 つのクイックコースを実施した。

・セキュリティマインドメインコース
・セキュリティマインドクイックコース（セキュリティ）
・セキュリティマインドクイックコース（データ科学)
各コースは、情報セキュリティのマインドの学び直しをしたい現役システム開発技術者・データ解析技術者（20 代∽30 代）や産業界で情報系業務に従事している技術者を受講者として想定する。コースでは、ソフトウェアの設計・開発段階におけるセキュリティ対策やデータ解析、情報セキュリティマネジメントなどの知識を身につけるために座学や演習をそれぞれ 126 時間・45 時間・67.5 時間提供している。
コースを修了した受講者に対しては ProSec-Mind 認定証を発行するとともに、科目毎の履修も可能としている。今年度も新型コロナウィルス感染症対応として、遠隔教育・オンライン授業を中心に講義・演習を実施した。オンライン授業の実施にあたっては、Slack 等のコミュニケーションツールの活用やクラウド環境上における演習環境の整備により、質疑応答等の十分な指導及び受講者同士の意見交換の機会を確保するよう努めた。また、ProSec 科目の一部に参加するトライアルコースや、初学者向けの講義・演習科目やその一部に参加するエントリーコースを設置して、コース受講を検討する社会人に対し、具体的な授業内容や雰囲気を事前に把握することができる取り組みを実施した。

実施状況

今年度、東北大学では、以下の 8 科目を大学院情報科学研究科の正規科目として開講した。大学院科目を社会人に開放して行うコースのため、社会人受講者は大学院生とともに学ぶことができる。
①情報セキュリティ法務経営論（基礎講義、4 ポイント（22.5 時間）、遠隔配信有り）
②データ科学基礎（基礎講義、4 ポイント（22.5 時間））
③学際情報科学論（演習、4 ポイント（22.5 時間））
④ネットワークセキュリティ実践（演習、4 ポイント（22.5 時間））
⑤ビッグデータスキルアップ演習（応用講義、2 ポイント（12 時間））
⑥データ科学トレーニングキャンプⅠ（応用講義、2 ポイント（12 時間））
⑦データ科学トレーニングキャンプⅡ（応用講義、2 ポイント（12 時間））
⑧応用データ科学（応用講義、オプション（22.5 時間））

さらにメインコースとクイックコースに加えて、開講回数を部分的に聴講できるトライアルコースも用意したが、いずれのコースも参加者を得られなかった。その理由を検討すると、地域の産業界において ProSec に期待が寄せられていたものの、大学院相当の講義・演習科目への受講者派遣を具体化すると大学院生に相当する技術者の層がきわめて薄く、また受講者と所属勤務先にとって原則 15 週の講義に出席・派遣することに支障が少なくなく、さらに大学院生とともに演習に参加し課題をこなすことが容易ではないケースもあったと分析される。

これらの需要のある層とのミスマッチの問題は提案の時点で把握できていなかったが、補助事業期間をすぎたのでコア部分から修正を考えて 2023 年度以降に試行ないし実施することを計画している。

また、広報活動も積極的に推進し、学都「仙台・宮城」サイエンス・デイ 2022 などのイベントで本事業の取り組みの紹介をして、他分野の教員や企業の方々と意見交換するなど様々なかたちで広報を行った。

写真2　サイエンス・デイの様子

来年度の計画

上記の分析を踏まえて、大学院レベルの講義・演習は社会人向けコースとして当地ではマーケットが小さいので、新たに学部科目相当の講義・演習を追加提供することを計画する。例えば、情報セキュリティの基礎と実際を広く扱う講義の１～２科目を提供し、これを蓄積配信でも受講可能とすれば、受講しやすくなると期待できる。演習については教室で数日間にて実施する集中講義科目をいくつか提供することが考えられる。

この計画について、地域の需要とのマッチングを十分に調査して社会人向けのリスキリングコースとして実施することとしたい。これを試行として形式や内容を調整しつつ実施したのちに公式化することが適当と考えられる。

ほかに、ProSec で策定したカリキュラムや教材は学内の AI・数理・データ科学教育や今後のリカレント教育に連携していくことと、将来的にリスキリングコースを公式化した後には履修証明プログラムも検討できると期待する。

募集情報

問い合わせ先：東北大学 大学院情報科学研究科
実践的情報教育推進室
Email: tohoku@seccap.jp

2.3 大阪大学

取り組み概要

1. 基本方針

情報セキュリティは，情報セキュリティガバナンスという用語にみられるように組織全体で取り組まなければならない．一方，ビットコインなど，情報セキュリティ技術は経済活動にも大きな影響を与える．様々な業務で安全な情報利活用が必要となる社会人を対象として立ち上げた「情報セキュリティプロ人材育成短期集中プログラム　ム（ProSec）」において，大阪大学では，データの安全な利活用に必要なサイバーセキュリティ，リスクマネジメント，法制度，暗号技術の応用，ビットコイン・ブロックチェーン・IoT などの最新技術から，実務を支える理論として数学，アルゴリズム，暗号理論などのセキュリティ基盤技術までを幅広くカバーしており，社会システムにセキュリティ技術を安全に適用できる知識の獲得と現場知識の涵養を目指す．

2. 講義内容

講義は主に暗号技術及びサイバーセキュリティの 2 本柱において，それぞれの軸を基礎から発展まで構築することを目指している．これまでに構築した講義科目と PBL 科目を記載する．

○講義科目

・実践セキュリティ特論 I(1.5 単位), II(2 単位)
・先進安全なデータ設計特論（2 単位）
・実践離散数学と計算の理論（2.5 単位）
・先進情報セキュリティとアルゴリズム（2.5 単位）

○PBL 演習科目

・高度セキュリティ PBL（2 単位）
・高度セキュリティ PBL II, III（各 1 単位）
・高度サイバーセキュリティ PBL I, II, III（各 1 単位）

2022 年度には，演習内容を増強することで，一部の講義科目及び PBL 演習科目の単位数を増やして実施した．

また，受講者自身が学びたいことに合わせて選択できるようにコース設定を提供している．さらに，大阪大学で提供するコース（プログラム）を「職業実践力育成プログラム（BP）」に申請し，認定されており，さらに，教育訓練給付金制度　専門実践教育訓練の講座指定に採択された．

3. 連携企業

大阪大学のセキュリティコースの特徴である企業との連携による実用としてのセキュリティ技術の講義・演習として，NTT データ，セキュアワークスと連携し，高度セキュリティ PBL III を実施している．セキュリティの実践的技能を自ら主体的に判定する方法として Capture The Flag (CTF) 方式の問題がある．本 PBL においては CTF の基礎的な知識を演習形式で学習後，実際に CTF に取り組むという演習を実現した．また，Shiftall・苗村法律事務所とも連携し，セキュリティリテラシーに関する講義である，実践セキュリティ特論 I,II を実施している．

実施状況

実施状況について，今年度の受講者数，さらには各講義の受講者数の観点で報告する．

表 1: 大阪大学における 2022 年度各コース

コース名 / 科目名	メインコース（8 単位）			クイックコース（5 単位）				
	セキュリティ	暗号	サイバー	セキュリティ	暗号	サイバー	暗号実践	セキュリティ・サイバ
実践セキュリティ特論 I，II	必	必	必	必		必	選 F	選 F
実践離散数学と計算の理論	選 A	必	選 A		必		選 A	
先進情報セキュリティとアルゴリズム	選 A	必	選 A		必		選 A	
高度セキュリティ PBL	選 B	選 D	選 B	選 E	選 B		選 E	選 G
高度セキュリティ PBL II	選 B	選 D	選 B		選 B		選 E	選 G
高度セキュリティ PBLIII	必	選 D	必	選 E			選 E	選 G
高度サイバーセキュリティ PBL I	選 C		必	選 E		必	選 E	選 G
高度サイバーセキュリティ PBL II	選 C		必			必	選 E	選 G
高度サイバーセキュリティ PBL III	選 C		必			必	選 E	選 G
先進安全なデータ設計特論	選 H	選 H	選 H	選 H	選 H	選 H	選 H	選 G

※【必】必修科目【選 A】講義科目から選択 (2.5 単位上)
※【選 B】高度セキュリティ PBL 科目から選択 (1 単位上)
※【選 C】高度サイバーセキュリティ PBL 科目から選択 (1 単位上)
※ セキュリティメインコースでは上の条件に加えて未履修の科目から 2 単位取得
※【選 D】高度セキュリティ PBL 科目から選択 (2 単位上)
※【選 E】PBL 科目から選択 (2 単位上)
※【選 F】講義科目から選択 (1 単位上)【選 G】PBL 科目から選択 (4 単位上)
※【選 H】クイックコースを 1 つ以上修了していること

1. 受講者数

2022 年度前期受講生: 19 名

2022 年度後期受講生: 22 名（前期で修了が 2 名，後期から追加で 5 名が受講）

本年度も講義と演習をオンラインと対面参加のハイブリッドで実施した．また，各講義に Flipping 講義を導入し，事前学習，本講義・演習，事後学習を組み合わせた．これまで，本講義・演習で実施していた内容を事前学習に振り分けることにより，より深い知識の習得に繋がった．写真は PBL 演習の対面参加の様子（写真 3）を表す．

写真 3: PBL 演習の対面参加の様子

なお，各講義の受講者数は以下の通りである．

2.　　各講義の受講者数

実践離散数学と計算の理論: 8 名，実践セキュリティ特論 I: 12 名，実践セキュリティ特論 II:13 名，先進情報セキュリティとアルゴリズム: 8名，高度セキュリティ PBL: 9名，高度セキュリティ PBL II: 6 名，高度セキュリティ PBL III: 6 名，高度サイバーセキュリティ PBL I: 12 名，高度サイバーセキュリティ PBL II: 8 名，高度サイバーセキュリティ PBL III: 11 名，先進安全なデータ設計特論: 0 名

3.　　受講者の講義への意見

講義への意見をアンケートで収集した結果の一部を示す．

・情報セキュリティの基礎を学ぶのに最適な講義内容でした．今回全ての講義をオンラインで受講しましたが，充実した教材と講師の方々の配慮により，特に違和感なく講義に集中することができました．

・情報セキュリティの最先端で活躍されている先生方から，知識だけでなく，実際にあったインシデント事例の紹介やその考察などを学べました．座学形式の講義でありながらも，中には演習さながらの講義もあり，手を動かすことでさらに習得できたように思いました．

・バイナリ解析，具体的なツールの使い方など実際ハンズオンで試してみることで理解が深まりました．CTF について、書籍などは読むだけで，実際に書籍の内容を試してみる環境を整えようと思ってもうまくいかなかったりとなかなかハードルが高かったので，実際に体験ができて良かったと思います．

4.　　2022 年度修了生

2022 年は 5 名の ProSec メインコース認定と 23 名のクイックコース認定（重複認定者を含む），10 名の大阪大学大学院科目等履修生高度プログラム修了生を輩出した．ProSec 修了認定式（写真 4）を 2022 年 3 月 21 日に実施し，後に，立命館大学の上原 哲太郎教授及び大阪大学の猪俣 敦夫教授を交えて意見交換会（写真 5）を実施した．

写真 4：大阪大学 ProSec の修了認定式

写真 5：ProSec 修了者との意見交換会

自走後の計画

事業終了後においても，これまで通り，充実した教育プログラムの提供を目指す．最新セキュリティ特論 I, II，離散数学と計算の理論，実践情報セキュリティとアルゴリズム，高度セキュリティ PBL I，安全なデータ設計特論の演習内容を増強し単位数を増やした，実践セキュリティ特論 I, II，実践離散数学と計算の理論，先進情報セキュリティとアルゴリズム，高度セキュリティ PBL，先進安全なデータ設計特論を開講した．補助事業期間の終了と教育訓練給付金制度 専門実践教育訓練の講座指定に伴い，新たに実習等経費を 2023 年度から徴収する予定である．また，定期的な会報の送付や講義の合間に座談会を導入し，受講者間の情報交換を深められるように進めたい．

募集情報

問い合わせ先：〒565-0871 大阪府吹田市山田丘 2-1

大阪大学大学院工学研究科 宮地研究室

TEL：06-6879-4179

E-mail:myj-pro.seccap.staff@crypto-cybersec.comm.eng.osaka-u.ac.jp

URL:https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.ht

2.4　和歌山大学

取り組み概要

和歌山大学では，2022 年度の ProSec の取り組みとして，以下の内容を企画し，実施した．

・和歌山県警察本部サイバー犯罪対策課向け研修
(2022 年 8～9 月)

・遠隔ハンズオン(2023 年 2～3 月)

上記のハンズオンでは，サーバ・ネットワークの運用管理に係る情報セキュリティ事案、すなわちいくつかのインシデントをシューティングする．受講生となる社会人の職種は、金融系のセキュリティ部門の SE および，サイバー犯罪対策課の捜査員となる．金融系のセキュリティ部門の SE においては，運用管理上遭遇するインシデントを想定・経験し，解決策を想定することによって，ネットワークセキュリティに関する知見を高め，日々の業務に生かすためにハンズオンに参加している．捜査員においては，サイバー犯罪捜査の上で，必要な解析技術を身に着けるだけではなく，どのような条件(脅威と脆弱性)によってインシデントが構成されているかを知ることでどのようにサイバー犯罪に対処し，未然に防ぐことができるかを理解することができる．

実施状況

和歌山県警本部向け特別研修：

捜査員計 5 名に対して研修を実施した．本年度も JNSA の CSIRT 向けカードゲーム（マルウェアコンテインメント）を導入に用いた．加えて，ルータやスイッチを用いたネットワークの構築を繰り返し実施した．実際のネットワークの図面を確認してその通りに環境を再現する作業は，ネットワークやパケットの流れを理解し，把握する能力を高めたといえる．同時並行で行っていた Linux サーバ上での UNIX

コマンドや Web サーバのようなミドルウェアを利用する演習との相乗効果でより深い IT インフラへの理解を得ることができた．

次に，Basic SecCap 演習(8 月下旬 4 日間)の実施に必要な演習環境の構築とシナリオ(インシデント発生から終了条件に至るまでのトラブルシュートの過程を想定した演習の演目)の実施を反復練習する．この時，演習の運営側としての練習と，参加者としてトラブルをシューティングする練習の両方を行うことでセキュリティインシデントに対する理解を得ることができた．Basic SecCap 演習終了後，より深いシナリオへの理解を経て，SecCap 演習(NAIST 9 月下旬)に以前の演習と同様，運営として参加する．

最後に研修の集大成として，参加した捜査員が協力し演習のための新しいシナリオの作成を行った．これによって研修の教育的な効果の検証を行うことができた．

写真 6：和歌山県警本部向け特別研修の様子

遠隔ハンズオン：金融系のセキュリティ部門の SE2 名が参加者として，本学川橋研究室の学生(学部生 3 名，院生 2 名)が運営として演習を実施した．参加者は自宅から，運営は研究室から演習環境に VPN を用いて接続し同環境内で発生するインシデントに対応する．参加者は 5 つのシナリオに対応した．シナリオとして，辞書攻撃を用いた不正ログインによる Web コンテンツの改ざんや，sudo コマンドの脆弱性をついた攻撃，Slow HTTP DoS や Syn Flood のような DoS 攻撃，Memcached をもちいたリフレクション攻撃を行った．シナリオを一つ解くごとに，運営からの解説を行うことで，参加者はセキュリティインシデントの発生理由や，対処の方法を学ぶことができた．

来年度の計画

来年度も本年度と同じスケジュールと人数で実施する予定である．ProSec のメニューは本学においては，SecCap，Basic SecCap を有機的につないでいる中核的な存在であり，本メニューの充実はほかの演習の充実にもつながる．

募集情報

問い合わせ先：〒640-8510 和歌山県和歌山市栄谷 930

和歌山大学データ・インテリジェンス教育研究部門(ProSec 担当)

TEL: 073-457-7195

E-mail: dtier@ml.wakayama-u.ac.jp

2.5 九州大学

取り組み概要

九州大学においては 2018 年 4 月より学習時間 120 時間超の「ProSec-IT メインコース」および学習時間 60 時間超の「ProSec-IT クイックコース」を開講している。2022 年度はその 5 年目の受講生の受け入れになる。さらに戦略マネジメント要素を追加した教育コンテンツである SECKUN コースを ProSec-IT で選択可能なコースとして複数追加している．現在のコース形成は，全体で 8 コース（表 2）が選択可能になっている．各コースの受け入れ状況は表 1 の通りである．

表 2：ProSec-IT 受講者数および修了者数（人）

		受講者数			修了者数		
	コース名	在職者	その他	合計	在職者	その他	合計
ProSec-IT	ProSec-IT メインコース	6	5	11	6	5	11
	ProSec-IT クイックコース		3	3		3	3
SECKUN	ProSec-IT BASE	4	0	4	4	0	4
	ProSec-IT NEXT	13	0	13	10	0	10
	ヒューマンエレメント	11	0	11	9	0	9
	ビジネスイノベーション	6	0	6	5	0	5
	クライシスマネジメント	13	0	13	12	0	12
	セキュリティコンプライアンス	12	0	12	10	0	10
合計		65	8	73	56	8	64

全体で ProSec-IT/SECKUN 重複無しで時間数を数えると週末に約 70 日約 300 時間のハイブリッドで講義・演習を実施した．オフライン会場として，九州大学西新プラザ，大橋キャンパス，伊都キャンパス，東京，大阪，福岡での連携企業，東京，大阪，名古屋における貸し会議室等を利用して開催した．ハイブリッド実施により関西，関東からの受講生を集めることができ，また受講生の都合の付くタイミングで対面会場に足を運ぶことにより，受講生どうしの繋がり，交流形成にも配慮することができた（例；写真 7）．

写真 7 ： 連携企業のメルカリ本社（六本木ヒルズ）会議室でのハイブリッド講義の様子.

実施状況

（1）ProSec-IT

Web アプリケーションを代表とする情報システムの構築から、セキュアな運用、サイバー攻撃からの防御、実際にインシデント発生時の対応まで実践的に学べるカリキュラムである。さらに背景の理論や技術も深く学ぶことができる。座学だけではなく社会人受講生のニーズの高い演習科目に特に注力し、例えば、CTF ではゲーミフィケーションを活用したグループで協調して課題解決にあたるもの（NTT 西日本連携）と共に大阪大学と連携した本格的な競争型の CTF を準備し、スキルとチームワークの向上の両面からアプローチを実現している。また、入門（クラウドセキュリティ、Docker 技術）から Web アプリのセキュアプログラミング、IoT 演習、ARM64 アセンブラ演習、仮想計算機演習、サイバーレンジ演習等の高度な内容に段階を踏まえ無理なく、スキル向上ができるよう，他に無い講師独自の充実した内容で実施している．また、Web アプリ脆弱性診断スクリプト作成演習、フォレンジクス演習、ブロックチェーン演習では、第一線で活躍の実務家講師が対応し、高い実践力を修得できる。最先端の技術内容も SECKUN の「サイバーセキュリティ技術調査科目群」と共通であり、入門レベルから最先端に留まり続ける総合的な技術を修得可能にしている．SECKUN との共通科目では、情報倫理や個人情報保護法、組織マネジメント、法制度調査手法、デジタル新法講義、広告サービスと情報セキュリティに加え、サイバーセキュリティ俯瞰を配当し、広い視野と人脈および倫理観を兼ね備えた高度技術者の素養を研鑽している。

（2）SECKUN

世界の先端に留まり続ける技術者を育成する最先端の技術教育に加え、特に経営層や戦略マネジメント層などの組織の核となる人材にアプローチすることを目的に人間の脆弱性（心理学）、海外セキュリティ法則、BCP 体験型 TTX 等の内容も準備し、IT-BCP と組織全体の BCP とを総合的に担える人財育成を目指した。

ProSec-IT BASE では，ProSec-IT メインコースと同様の内容をより受講し易い公開講座の枠組みを使って展開した．これより受講生が大卒の資格が必要だったりすることなく，より簡易な手続きで受講できるようにした．また，ProSec-IT NEXT では，先端的な技術者らが共通して持つ、最新技術の一次文献を自ら調査・理解して追試や応用能力の開発を主眼に置き、先端技術（＝Moving Target Defense、クラウドセキュリティアーキテクチャレベルの脆弱性）の技術調査の方法や追試、応用の在り方を例示した。その他，SECKUN の各コースでは，フェイルセーフな組織（＝失敗しても壊れない組織）に欠かせないリスクマネジメント、経済安全保障と新規ビジネス投資，危機の現場で不動のリーダシップを発揮するため、セキュリティ心理学、医療機関でのインシデント発生時を想定した BCP 体験型机上演習、インテリジェンスと地政学などを，各コースの性質に合わせて組み合わせて学んでいる．

修了生や受講生は、自発的にオンラインコミュニティを構築し、例えば、連携大学の教育プログラムへのグループ参加等、全国へ活発な交流活動をしている．

また，ProSec-IT および SECKUN において，演習科目のひとつとして医療機関向け体験型演習を実施している．九州経済産業局と本プログラムが連携して，医療機関向け体験型演習を佐賀の実際の複数の医療機関が参加した演習の提供を行っている（写真 8）．

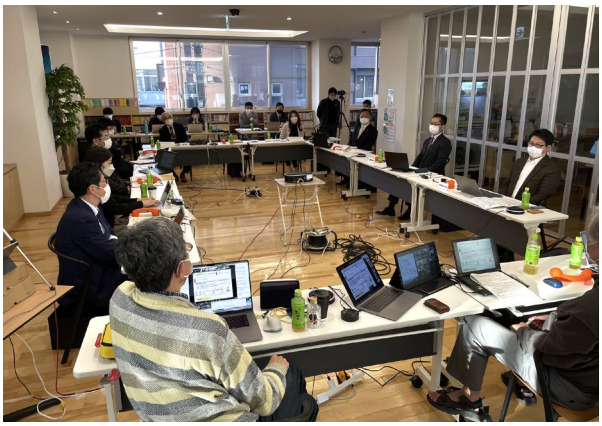


写真 8 ： 九州経済産業局と連携した実際の医療機関向け体験型演習の様子（2023/2/4）．

さらに，同様に九州経済産業局と連携して新しく「製造業向け体験型演習の開発」を行っている．今年度は SECKUN の受講生向けに演習の試行を行った他，製造業が集積している北九州市の複数の企業に集まってもらい，演習の試行までを行っている（2023/2/1 事前説明；3/8 体験型演習試行；写真 9）．

写真 9：九州経済産業局と連携した製造業向け体験型演習の様子（2023/3/8）．

来年度の計画

2022 年度は予算措置が無くなり自走体制の初年度であった．多くの周りからの協力のもとなんとか講義・演習を実施した．来年度以降にさらにより良い内容で事業を継続するため，体制構築のための期間として半年間使い，後期からより良い内容で開講する予定である．

募集情報

問い合わせ先：〒819-0396 福岡市西区元岡 744
九州大学 サイバーセキュリティセンター ProSec-IT 事務局
TEL：092-802-2671
E-mail：https://cs.kyushu-u.ac.jp/enpit-pro/info/
URL：https://cs.kyushu-u.ac.jp/enpit-pro/

2.6 長崎県立大学

取り組み概要

補助期間が終了した 2022 年度以降は、本学大学院の既定の制度である「科目等履修生」として受講者を受け入れることとした。教員の増員およびカリキュラムの変更に伴い、2022 年度に提供する科目は、地域創生研究科情報工学専攻の科目のうち、情報セキュリティコースの専門科目 9 科目と専攻共通科目から「ソフトウエア開発プロセス特論」を加えた 10 科目とした（下図）。

図：長崎県立大学 2022 年度提供科目

科目名	開講期
情報セキュリティリスクマネジメント特論	1Q
データセキュリティ特論	2Q
制御システムセキュリティ特論	2Q
現代暗号特論	2Q
ソフトウエア開発プロセス特論	2Q
生体認証特論	3Q
ネットワークセキュリティ特論	3Q
暗号数理特論	3Q
インターネット基盤セキュリティ特論	4Q
サイバーセキュリティオペレーション特論	4Q

これら 10 科目のうちから受講者が自由に選択し、6 科目を修了することでメインコースを認定、3 科目を修了することでハーフコースを認定するというコース設定とした。

また、受講生を派遣する側の企業・組織の意見を聴取して、取り組みの改善につなげるために、県下の企業・組織から委員を招集し、社会人情報セキュリティ学びなおしプログラム検討委員会と称する委員会を開催した。

◦実施状況

ハーフコースに県下の情報系企業から 1 名の受講者を迎え、修了した。この他、本学修士課程の学生で所定の科目の単位を修得した者に修了証を発行した。

2022 年度の募集に向けて、メインコースおよびハーフコースの募集要項を作り、本学 Web ページでの公開ならびに県の産業振興課などを通じて周知した（下図）。

3 月 14 日に社会人情報セキュリティ学び直しプログラム検討会議を開催し、県下企業および県警などから 7 名の委員が参加した。企業・組織側が人員を派遣しやすいように、広報の時期についての議論がなされた。また、社会人にとっては、ハーフコースでも科目数が多く、敷居が高いものとなっているとの意見があり、慶應義塾大学で取り入れられている unit 受講についての期待が挙げられた。

来年度の計画

2023 年度以降も、大学院情報セキュリティコースの科目を中心に 10 科目を提供し、そのうちの 6 科目を修了することでメインコース認定、3 科目を修了することでハーフコース認定するコース設定とする。また、2024 年度に向けて、unit 受講の導入を検討したい。

また、社会人情報セキュリティ学び直しプログラム検討委員会についても、これまで同様、県下の企業・組織の委員を招集して開催する予定である。

◦募集情報

問合せ先： 〒851-2195 長崎県西彼杵郡長与町
まなび野 1-1-1
長崎県立大学 大学院地域創生研究科 情報工学専攻
（ProSec 担当）
TEL：095-813-5153
E-mail：sun-prosec@sun.ac.jp

2.7 慶應義塾大学

取り組み概要

慶應義塾大学では、サイバーセキュリティの専門家の育成だけでなく、サイバーセキュリティについても理解するさまざまな分野のプロフェッショナルの育成が不可欠であると考えている。2022 年度は COVID-19 の影響が緩和される中、社会人の参加しやすさも考慮して引き続き講義での e-learning system の活用、演習のオンラインでの実施を進めた。

インシデントハンドリングメインコース/クイックコースの核となる演習であるインシデントハンドリング演習(インシデント対応コミュニケーション演習)でオンラインでの実施を行うと共に、同演習の中でグループリーダの育成を行うインシデントハンドリングリーダーシップ演習、演習のファシリテーションを行うことで組織管理の知識を学ぶ、インシデントハンドリングファシリテーション演習を並行して実施する仕組みを確立させるため、そのブラッシュアップを進めた。また、インシデントの分析を元に教材作成を行い試行する演習コースを実施し、セキュリティ人材育成のエコシステムの確立を進めている。講義については引き続き e-learning 教材を充実させ受講者の都合の良い時間に都合の良い場所から参加できるようにした。

これらはコースとして一括で受講するのではなく、各講義、演習を個々に都合の良いときに受講し認定証を発行する形態とした。コース修了はこれらを統合して授与する形式に変更している。今年度は各大学で実施しているコースの一部を同様に扱いコース間連携を進められるようにしている。

社会人の参加しやすさを考慮しオンラインを中心とすることで受講を容易にし、より広くサイバーセキュリティへの認識を高め社会全体のセキュリティインシデントへの強靭性を高めることを目指し人材育成を実施した。

実施状況

1. e-learning system による講義の実施

今年度も引き続き受講生の参加を容易にするために講義については e-learning system による実施とした。「セキュリティの基礎・対策・対応 (Unit 15)」を実施しており、履修の認定については単に講義を視聴するだけでなく、課題を出しその評価をもって行っている。今年度は教材の更新に注力したため参加は非公式に 1 名のみであったが、この参加が更新教材の評価につながっている。

2. オンライン演習と人材育成エコシステム

インシデントハンドリング演習について引き続きオンラインで 7/26(6 名), 2/24(5 名)に実施した(Unit 10)。これはインシデント発生時の組織内のコミュニケーションを訓練するための演習であるが、この演習の既修者を対象としてさらに演習内のグループをリードする訓練を行うインシデントハンドリングリーダーシップ演習(Unit 10, 7/26 2 名, 2/24 4 名受講)を並行して実施している。また、演習の運営側として演習全体のファシリテーションを行う訓練としての演習も行っておりこれによって組織全体の動きを把握する訓練としている(インシデントハンドリングファシルテーション演習 Unit 10, 7/27 1 名)。このように 1 回の演習で、レベルの異なる複数の人材育成を行うことで、効率よく効果的に人材育成を行えるようになる人材育成のエコシステムの確立を進めている。

3. 演習としての教材作成

インシデントハンドリング演習の教材は、実際に発生するインシデントに合わせて更新していくことが求められる。これまで実施側でこうした作業を行ってきたが、この作業そのものもセキュリティ人材育成に資することが明らかになってきた。そこで昨年度より、インシデント情報を収集し分析を行うインシデント分析演習(Unit 30), それを教材とするインシデントハンドリング教材作成演習(Unit 30)、インシデントハンドリング指導演習(Unit 15)を経て新教材を作成し演習に取り込んでいる。これによりインシデントハンドリングメインコースを 1 名が修了している。本課程も人材育成エコシステムの一部となっている。

来年度の計画

Unit 受講を導入したことにより柔軟な受講体制が整ったと考えられる。さらに、人材育成のエコシステムが確立しつつあることで効率よく効果的に人材育成を行うことが可能となってきた。今後、教材の評価を進めながら安定した質の人材育成が図れるようマニュアル等の整備を進めている。

来年度もこうした知見を活用し、Unit 受講を中核としてプログラムを連携組織の協力を得ながら進めていく予定である。

募集情報

問い合わせ先:

〒223-8526 神奈川県横浜市港北区日吉 4-1-1 協生館 2F

c/o 慶應義塾大学大学院メディアデザイン研究科/先導研究センタ内

サイバーセキュリティ研究センターProSec 担当

TEL: 045-564-2489

Email: keio@seccap.jp

3 大学間で連携した取り組み

■

教務 WG

【スキルマップ】

スキルマップについて 2022 年度末に立ち上げた slack を用いて、運営委員のほか企業・団体の方々を交えて意見交換を行った。その中で、技術者が自分のスキルを確認するためのスキルマップと、体系的な教育がカバーする範囲を確認するためのスキルマップでは、提示すべきスキルの粒度が異なるのではないかとの知見を得た。前者はスキルを細分化し周辺領域のスキルを確認できることが利便性につながるのに対し、後者は関連する技術や知識の教育が前提にあって、細分化することスキルマップの使いにくさにつながる。また、セキュリティに対する敏感さといった明示することの難しいスキルをスキルマップに含めるべきか否かといった議論がなされた。2022 年度版として、36 のスキル項目・5 つのロールから成るスキルマップを提案した。

図 5 スキルマップの一部画像

【コース連携】

ユニット受講をコアに各大学のコース連携を進めている。各科目単位で受講可能な Unit 受講を複数の大学が実施するコース連携に活用している。Unit 受講では、講義や演習にかかる時間(準備、予習、復習、課題実施にかかる時間を考慮)を基本として Unit 数を設定(1 時間 1 Unit)している。したがって、全体として 30Unit 以上が認定されるとクイックコース、120 Unit以上が認定されるとメインコースの修了として認定されることとなる。なお修了の認定は主としてコースを運営する大学から行うこととした。（（P3・図 4 教育プログラムのフレームワーク参照）。

■ 産学連携 WG

2022 年度も、COVID-19 の影響が残っており、オンラインとハイブリッドの両方の形式でのコース実施となった。

そのため、少しずつではあるが拠点間の連携等について進めてきている。

一方、オンライン化/ハイブリッド化を進めたことによる

当初カバーできていなかった地域の人材育成を図ることも可能となり、カバーエリアを広げつつある。また、産業ニーズに応えることができる社会人の再教育プログラムを提供するため、引き続き各拠点が地域の企業団体・個別企業等との連携を重視しながらコースを実施する。

来年度以降、オンライン化/ハイブリッド化で得られたノウハウを有効に活用しつつ、従来の対面でのコース実施を展開することにより、有機的な ProSec コースの展開において、複数拠点の連携等より全体が融合した体制を確立することを目指す。このため、全国ネットワークを持つ団体との連携だけでなく、これまでカバーしてこなかった地域の組織と連携し、本プログラムの特色を活かし連携できるような体制の構築を模索する。

■ 評価 WG

1．基本方針

評価 WG においては，これまでの大学院向けセキュリティコース SecCap，さらには現在進行中の学部向けセキュリティコース Basic SecCap における講義・演習の評価の経験をもとに，社会人向けコースの各講義・演習の評価を行う．具体的には，受講生への過度のアンケートを削減するため分野共通アンケートは実施せず，各連携大学において提供される講義・演習に対して受講者へのアンケートを実施し，そのアンケートの内容や結果を解析する．各連携大学で実施されている講義・演習アンケートについて報告する．

2．情報セキュリティ大学院大学でのアンケート

2-1. 講座内容の知識状況チェック（良 5～1 悪）

・IoT-1: IoT の特徴とセキュリティ, IoT デバイス, センサーと制御ネットワーク+産業用の IoT, IoT ネットワーク，車載セキュリティ, IoT セキュリティの運用, IoT の国際標準規格, IoT を取り巻く法制度

・IoT-2: 機能安全, 脅威分析手法, 脅威分析手法,
脅威分析(被害分析)演習, 脅威分析(攻撃分析)演習

・IoT-3: 脆弱性検査手法, 脆弱性検査演習,
脆弱性検査システム

2-2. 演習の評価

・内容のレベル（難 5～1 易）

・教員の講義・演習の仕方（良 5～1 悪）

・講座の総合評価（良 5～1 悪）

・講座に関する全体的なコメント

3．大阪大学でのアンケート

大阪大学では，講義開始前に知識や NW 環境の確認を行う事前
アンケート，講義毎の理解度を確認し，次の講義で質問に対する
回答をすることや，さらには次の講義の設計指針を立てるための
講義アンケート，最後に全講義に対する理解度を確認するための
事後アンケートの 3 種類のアンケートを実施している．なお，1 つの講義で複数の教員が実施する場合，全講義の最後に各教員の
評価を事後アンケートで実施している．

3-1. 事前アンケート（受講スタイル / NW 環境確認）

・金曜日開講の講義の受講形式について: 講義室（大阪大学吹田キャンパス）で受講 / 遠隔地から受講

・土曜日開講の講義の受講形式について：講義室（大阪大学吹田キャンパス）で受講 / 遠隔地から受講

・遠隔地から受講される場合について: 受講場所（会社，自宅など），LAN の種類，通信速度

3-2. 事前アンケート（事前知識）

・数学用語の事前知識について教えてください．

1. 素数・合成数，2. 倍数，3. 最大公約数，4. 整数，有理数，実数，複素数，5. 群・環・体，6. 離散数学，7. 初等整数論，8. バイナリ法，9. ユークリッドの互除法，10. 拡張ユークリッドの互除法

・暗号用語の事前知識について教えてください．

1. 公開鍵暗号，2. 共通鍵暗号

・プログラミングについて
Python を使用したことがありますか．プログラム経験はありますか．ある方は使用言語を教えてください．

3-3. 毎講義後のアンケート
・講義でもっとも勉強になった内容を教えてください．
・講義の内容ですでに知っていた内容があれば教えてください．
・講義の内容で追加説明が必要な内容があれば教えてください．
3-4. 講義終了後の事後アンケート
0. 年齢
20 代，30 代，40 代，50 代，60 代，70 代
1-1. 職業をお答えください．
管理職/ユーザー系/教育関係者/開発系/学びなおし/セキュリティ技術者/大学院生(情報系) /大学院生(情報系以外)/その他
1-2.「その他」の方は具体的にご記載ください．
2. 講義について教えてください．(各講師について 2-1～2-4 の質問をする)
2-1. 配布された講義資料は役に立ちましたか?
2-2. 講義は工夫されていましたか?
2-3. 講師は学生の質問に丁寧に回答してくれましたか?
2-4. 講義個別の内容について
1) 講義でもっとも勉強になった内容を教えてください．
2) 講義の内容ですでに知っていた内容があれば教えてください．
3) 講義の内容で追加説明が必要な内容があれば教えてください．
4) この先生の講義を他の学生に推薦しますか?
3. 講義の内容に関するご意見をお願いします．
4. 次年度に学習したい内容やもっと理解したい内容について記述お願いします．

4．和歌山大学でのアンケート

以下の項目について，5 段階で評価している．
1. 難易度　2. わかりやすさ　3. 現場向けノウハウ
4. 業務への利用　5. シラバスとの合致　6. 知識習得，技術力向上の動機　7. 満足度
また，自由回答のコメントの収集も行っている．

5．まとめ

各大学でのアンケート結果を自動的に取りまとめ，共有・ 分析することで，カリキュラムの改良に役立てるとともに，修了生に対する追跡アンケートについて検討する．

■ FD WG

概要

2022 年度の FD WG は、ハイブリッドでの演習実施を継続的に行っていくことを目的としたノウハウの共有を、隔月の全体ミーティングおよびメールにて実施した。

オンライン化からハイブリッドへの切り替え

2020 年度より取り組んだオンライン化から、これまで行ってきた COVID-19 以前の演習形態に戻す、ハイブリッドでの演習を実施した。実施演習を元にノウハウの共有を行った。これによりこれまでは物理的な距離に制約されていた演習への参加を緩和することが可能となっている。

様々なコミュニケーションツールの活用

現在は、Zoom や webex といったコミュニケーションソフトウェアの他に、持ち運びが可能な 360 度カメラや広範囲の音をインテリジェンスに集音し、コミュニケーションを実現するマイクツールが多く展開されている。これらを活用し、ノウハウを共有することでハイブリッドでの演習の実施を行うための知見を共有した。

今後の計画

今後も、COVID-19 による急激な社会情勢の悪化における演習形態の変更に柔軟に対応することが可能となるように、引き続き様々なノウハウの共有を行う。

■ 広報 WG

広報 WG の目的は、本事業を全国の情報系社会人技術者に広く認知してもらいコース受講につなげること、また関連する企業には事業の認知度向上に加えて連携企業としての参画につなげることである。
平成 29 年度から継続して行っている具体的な活動として
・Web サイトの運用（http://www.seccap.pro/）
・愛称、ロゴの活用
・Twitter アカウントの活用（@enpitprosec）
等がある。
継続的に本事業を実施するにあたり、今後も引き続き Web サイトを用いた本事業の周知が重要な活動であった。
そのため、広報 WG では、Web サイトのコンテンツ更新、情報発信を行った。また下記の対応を行うことにより本プログラムの普及活動を行った。
・Twitter アカウントを活用して、各連携校からの演習風景や各種イベント等の即時性のある情報発信（図 6 ）
・ProSecWeb サイトコンテンツの再構成（図 7）
Twitter 埋め込みの再配置、本プログラムや各連携校への連絡先、リーフレット、事業報告書の Web 公開

図 6：ProSec Web サイト（http://www.seccap.pro/）

図 7:Twitter アカウントによる情報発信

enPiT Pro Security

各大学のお問い合わせ先

情報セキュリティ大学院大学 ProSec 事務局	E-mail：prosec@iisec.ac.jp ＵＲＬ：https://www.iisec.ac.jp/admissions/prosec/
東北大学 大学院情報科学研究科 実践的情報教育推進室（ProSec 担当）	E-mail：tohoku@seccap.jp ＵＲＬ：http://www.esprit.is.tohoku.ac.jp
大阪大学 大学院工学研究科 宮地研究室	E-mail：myj-pro.seccap.staff@crypto-cybersec.comm.eng.osaka-u.ac.jp ＵＲＬ：https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html
和歌山大学 データ・インテリジェンス教育研究部門（ProSec 担当）	E-mail：dtier@ml.wakayama-u.ac.jp
九州大学 サイバーセキュリティセンター ProSec-IT 事務局	Email：prosec-it-staff@cs.kyushu-u.ac.jp ＵＲＬ：（ProSec-IT）https://cs.kyushu-u.ac.jp/enpit-pro/ （SECKUN）https://cs.kyushu-u.ac.jp/seckun/
長崎県立大学 大学院地域創生研究科 情報工学専攻（ProSec 担当）	E-mail：sun-prosec@sun.ac.jp ＵＲＬ：https://sun.ac.jp/siebold/sec/enPiT-prosec/
慶應義塾大学 大学院メディアデザイン研究科 / グローバルリサーチインスティテュート サイバー文明研究センター サイバーセキュリティ研究センター ProSec 担当	E-mail：keio@seccap.jp

www.seccap.pro