【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 2021

2021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かかわらず、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。

本申請は、「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

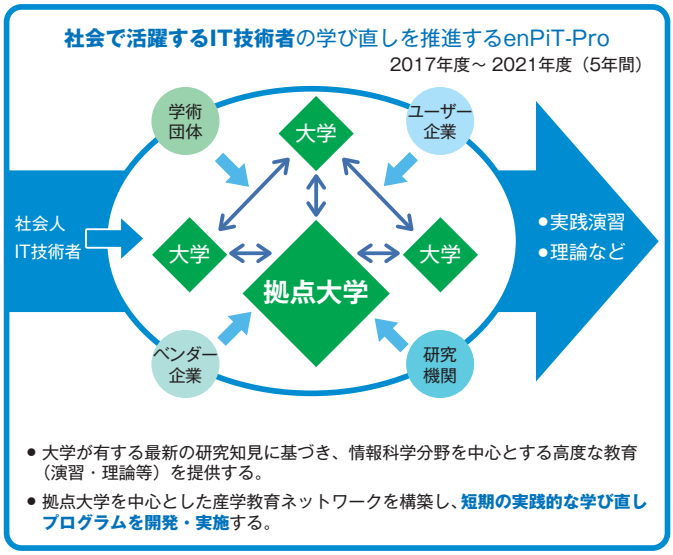

図 1：enPiT-Pro 事業全体イメージ

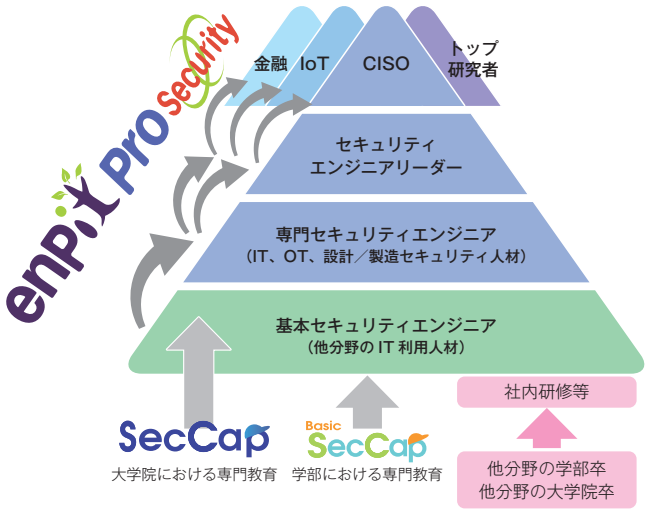

図 2：セキュリティ人材育成における ProSec の位置づけ

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。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262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年度は、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の委員の方の意見などを取り入れ、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、SecBoK2016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（2～3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。

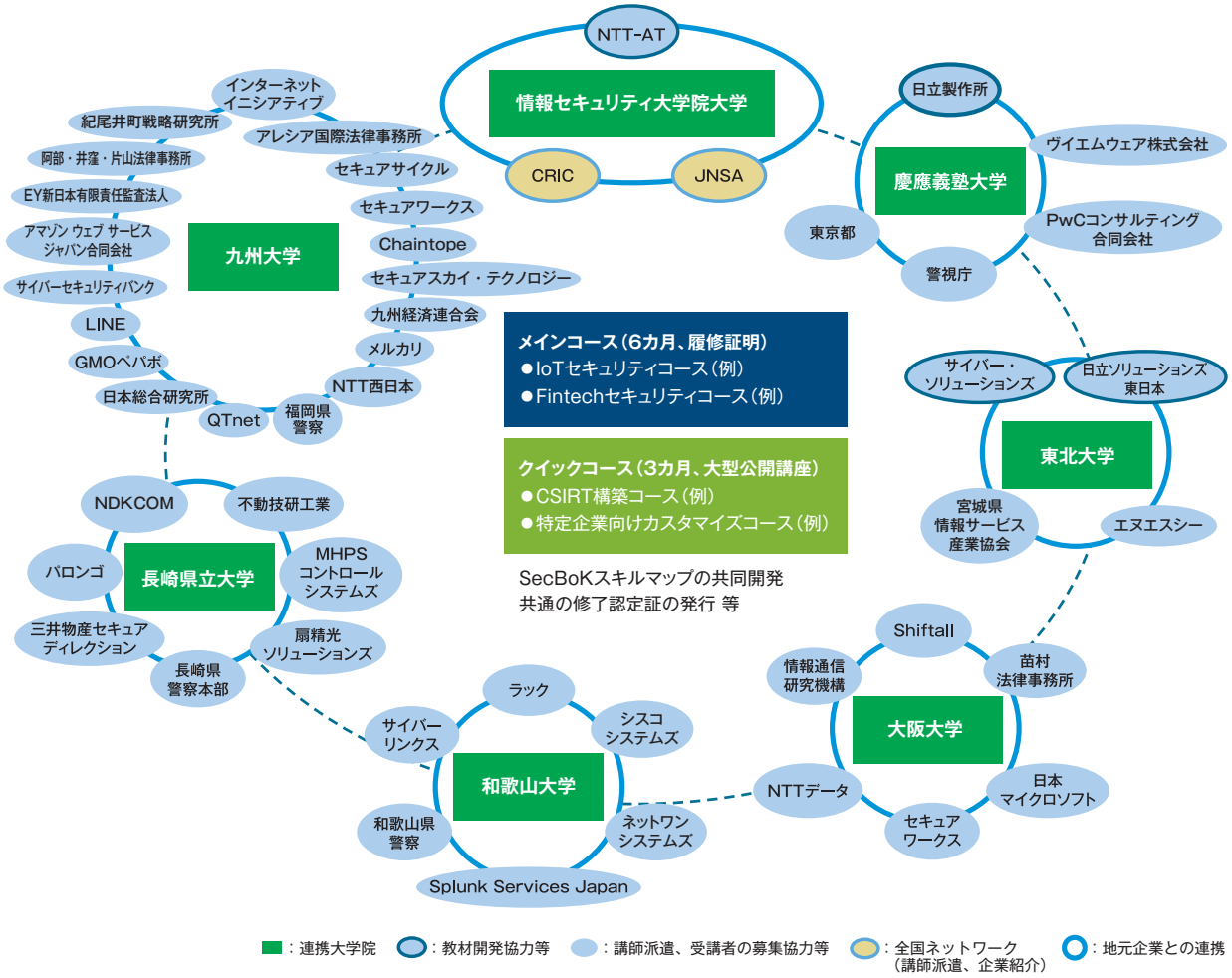

図 3：教育プログラムのフレームワーク

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。

▶ 2021 年度の実施状況

2021年度は2020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）。

提供しているコースやカリキュラムが社会・産業界のニーズに合致しているかどうかを評価していただくため、各方面で活躍されている専門家をメンバーとしたアドバイザリーボードを設けている。アドバイザリーボード委員は次の5名の方である。（敬称略）

金子 啓子　　大阪経済大学　経営学部
坂 明　　一般財団法人日本サイバー犯罪対策センター

図 4：各ワーキンググループの担当一覧

WG	サブ WG	メンバー
教務 WG	スキルマップ	山口*(長県大)、小松(長県大)、小出(九大)
	コース連携	大久保*(情セ大)、曽根(東北大)、砂原(慶應)
産学連携 WG		砂原*(慶應)、曽根(東北大)、種茂(情セ大)
評価 WG		宮地*(阪大)、内尾(和大)、小出(九大)
FD WG		加藤*(慶應)、砂原(慶應)、和泉(東北大)
広報 WG		内尾*(和大)、砂原(慶應)、奥村(阪大)

＊は主担当者

図 5：2021 年度 ProSec 担当教員一覧

教員名	所属大学名・肩書
大久保 隆夫	情報セキュリティ大学院大学 情報セキュリティ研究科 教授
曽根 秀昭	東北大学 大学院情報科学研究科 特任教授
和泉 諭	東北大学 大学院情報科学研究科 特任准教授
宮地 充子	大阪大学 大学院工学研究科 教授
奥村 伸也	大阪大学 大学院工学研究科 助教
内尾 文隆	和歌山大学 学術情報センター 教授
小出 洋	九州大学 サイバーセキュリティセンター 教授
藤岡 福資郎	九州大学 サイバーセキュリティセンター 学術研究員
小松 文子	長崎県立大学 大学院地域創生研究科 情報工学専攻 教授
山口 文彦	長崎県立大学 大学院地域創生研究科 情報工学専攻 教授
砂原 秀樹	慶應義塾大学 大学院メディアデザイン研究科 教授
加藤 大弥	慶應義塾大学 大学院メディアデザイン研究科 特任助教

寺井 理　　株式会社みずほフィナンシャルグループ
花田 経子　　岡崎女子大学　子ども教育学部
山岡 正輝　　NTTデータ先端技術株式会社

2021年度はアドバイザリーボードを10月に開催し、実施状況についてさまざまなご意見をいただいたほか、いくつかの演習をオンラインで視察していただいた。そのご意見を踏まえて、プログラムを改善していくこととしている。

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担当メンバーおよび本年度ProSec担当教員は**図4・図5**の通りである。

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。2021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のコースを組み合わせて受講すること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た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。

これらの取り組みの成果を全国に広く普及させるため、シンポジウムも積極的に開催している。

2021年度は、2022年3月1日に、enPiT-Pro5拠点（東洋大学「Open IoT 教育プログラム」、早稲田大学「スマートエスイー」、情報セキュリティ大学院大学「ProSec」、名古屋大学「enPiT-Pro Emb」、北九州市立大学「enPiT-everi」）による合同シンポジウム『社会人リスキリングに対する成果とこれからの高度情報技術人材のリカレント教育およびSDGs』をオンラインで開催した。合同シンポジウムでは、各拠点がそれぞれのコースの概要や取り組み内容を紹介し、ディスカッションも実施した。

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、2021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。なおCOVID-19拡大の影響により、2021年度は第1期 (4月開講分) メインコースの開講は見送らざるを得なかった。その後に開講した分については、オンライン化の検討を行い、講義を中心とした内容についてはZoomを利用したオンラインにより実施し、オンライン化が難しい実習内容等については感染症対策を徹底した上で対面授業を実施した。(**写真１**)

・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。

写真１：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のオンライン演習の様子

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 (新設)

●CSIRT基礎クイックコース (新設)

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基礎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。

●実施状況

2021年度の受講者は18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一は、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、コロナ禍のため演習も含めてオンラインで実施した。受講者はオンサイトと同様の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基礎クイックコースは、今年度は初の連携コースとして、慶應義塾大学の演習「インシデントハンドリング演習」(2/8オンライン開講) と組み合わせて実施した。これにより、コース連携する上での課題であった修了の扱い等の運用面においての土台を作ることができた。

また昨年度開講した「DX with Cybersecurity3日間教育コース」は、今年度開講した慶應の上記演習と組み合わせて「DX with Cybersecurityクイックコース」という連携コースとし、2名修了した。

●自走後の計画

【基本方針】

ProSecを企業向け集中コースと統合し、ProSecブランドとし、現コースは維持する。

【講義】

既存のメインコース、クイックコースは現状維持、連携校とのコース連携については各連携校と別途協議するものとする。

【受講手続】

メインおよびクイックコースについては、現状のProSecの手続を維持する。(応募書類、履歴書、修了証)。

●募集情報

問合せ先：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、2021年度のProSecの取り組みとして、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イ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))

このうち情報セキュリティ法務経営論では、情報セキュリティ技術を組織の中で利用するために必要な社会的側面を説明できる能力の修得を目的として、情報セキュリティ

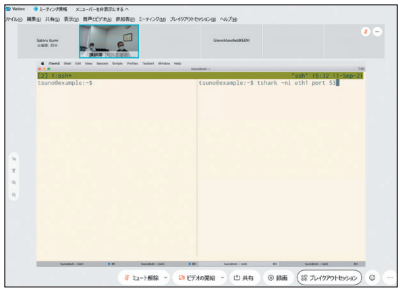

写真 2：ネットワークセキュリティ実践の様子

写真 3：仙台・宮城サイエンス・デイ 2021 の様子

に関する法務の基礎知識と関連法について解説するとともに、情報セキュリティを導入し定着させるために必要な経営上の意思決定方法について座学の講義を、同時双方向型のオンライン授業で行った。

演習科目であるネットワークセキュリティ実践では、クラウド上に仮想サーバと演習用ネットワーク環境を構築して、受講者がオンラインで実践的なハンズオンを行える環境を整備した（**写真2**）。

また、情報産業及びユーザ業界からのコメントをもとに各コースの内容や時間、受講料、シラバスなどをまとめて募集案内や広報用の資料を作成した。これらをもとに地元企業を中心に受講生の募集を行い、本年度はセキュリティマインドメインコースを2名が受講した。さらに広報活動も積極的に推進し、SNSやHPによる宣伝やオンラインで開催された学都「仙台・宮城」サイエンス・デイ2021（**写真3**）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。

●自走後の計画

今年度の開講した内容やアンケート結果などをもとにコースの内容の改善と拡充を図る。企業との協力に関しては、講義や演習の見学や意見交換を行って、企業側の視点による要望を調査し、また、これまでのオンライン講義や演習の知見も組み合わせて、社会人のニーズに合致し参加しやすいようコースの内容を改善・拡張させていく。地域高度IT人材育成に関しては、（一社）宮城県情報サービス産業協会（MISA）との連携協力をさらに推進する。

また、推進室のTwitterアカウント（@espritistohoku）やウェブサイト、各種イベントで本学の取り組みを発信して、募集案内をもとに地元企業に対して受講生の募集を進めていく。

●募集情報

問合せ先：東北大学 大学院情報科学研究科
実践的情報教育推進室
E-mail：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（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

- 最新セキュリティ特論Ⅰ、Ⅱ（各1単位）
- 安全なデータ設計特論（1単位）
- 離散数学と計算の理論（2単位）
- 実践情報セキュリティとアルゴリズム（2単位）

● PBL 演習科目

- 高度セキュリティ PBLⅠ、Ⅱ、Ⅲ（各1単位）
- 高度サイバーセキュリティ PBLⅠ、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

図６：大阪大学における各コース

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・サイバー実践
最新セキュリティ特論Ⅰ、Ⅱ	必	必	必	必		必	選 D	選 D
離散数学と計算の理論	選 A	必	選 A		必		選 A	
実践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 Ⅰ	選 B	選 B		必	選 B		選 E	選 F
高度セキュリティ PBL Ⅱ	選 B	選 B			選 B		選 E	選 F
高度セキュリティ PBL Ⅲ	必	選 B	必	必			選 E	選 F
高度サイバーセキュリティ PBL Ⅰ	選 C		必	必		必	選 E	選 F
高度サイバーセキュリティ PBL Ⅱ	選 C		必			必	選 E	選 F
高度サイバーセキュリティ PBL Ⅲ	選 C		必			必	選 E	選 F
安全なデータ設計特論	選 G	選 G	選 G	選 G	選 G	選 G	選 G	選 G

※【必】必修科目　※【選A】講義科目から選択（2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）
※【選D】講義科目から選択（1単位上）【選E】PBL科目から選択（3単位上）　※【選F】PBL科目から選択（4単位上）
※【選G】クイックコースを1つ以上修了していること 選択Gの単位取得済みかつコースを修了した場合、各コースのアドバンスの修了となる。例：暗号メインコース＋選択G→アドバンス暗号メインコースコース

写真４：PBL 演習の対面参加の様子

写真５：オンラインで繋がる受講生

義科目及びPBL演習科目の単位数を増やして実施する。

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、認定されている。

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、セキュアワークス及びNICT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や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、最新セキュリティ特論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。

1. 受講者数

2021年度前期受講生：22名

2021年度後期受講生：21名

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を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4**）、オンラインと対面参加の学生・講師が繋がる様子（**写真5**）を表す。

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

離散数学と計算の理論：4名、最新セキュリティ特論Ⅰ：9名、最新セキュリティ特論Ⅱ：9名、実践情報セキュリティとアルゴリズム：3名、高度セキュリティPBLⅠ：8名、高度セキュリティPBLⅡ：3名、高度セキュリティPBL Ⅲ：8名、高度サイバーセキュリティPBLⅠ：7名、高度サイバーセキュリティPBLⅡ：5名、高度サイバーセキュリティPBLⅢ：3名、安全なデータ設計特論：4名

3. 受講者の講義への意見

- 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については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。

●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PBLⅠ、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する。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

問合せ先：〒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.html

2.4 和歌山大学

●取り組み概要

和歌山大学では、2021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（2021年8～9月）
- 遠隔ハンズオン（2022年1月～2022年2月）
- 合同ハンズオン（2022年2月25日、28日、3月1日）（オンラインにて実施）

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、ソリューション系ベンダのSE、およびサイバー犯罪対策課の捜査員となる。ソリューション系ベンダのSEにおいては、運用管理上遭遇するインシデントを想定・経験し解決策を習得することによって、製品開発やソリューション提案における知見を得る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つけるだけでなく、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知ることで、どのようにこれを防御、予防することができるのか理解できる。電子的な証拠であるフォレンジックを実践的に学ぶことができる。

●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（セキュリティ人狼、マルウエアコンテインメント）を導入に用いた。本年は期間中に、サイバー犯罪対策課（配属直後）以外にも、現役の捜査員をスポットで参加させるなど、より実際の捜査に近いメンバーを対象に研修をおこなった。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する。特に実際の環境からネットワーク構成を調査、図面に描いて、次に概要図面通りに環境を再現する作業は、サーバ、ネットワークを把握する能力を高めた。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シュート過程を想定した演習の演目）の実施を反復練習する。同演習後、シナリオの仕込み（プログラミングと脆弱性の理解）を経て、さらなるトレーニングの後にSecCap演習（第1期

enPiT、NAIST、9月下旬）に参加する。先の演習と併せて、演習の運用を担当する。また、本年度からWindowsのデジタルフォレンジックについての演習を開始した。ガイドラインに基づいた初期対応やフォレンジックツールを使用した削除されたデータの復旧等を実施した。加えて、先述の各演習において利用するシナリオをオリジナルで作成して、シナリオの教育的な効果を検証した。

遠隔ハンズオン：

ソリューションベンダより4名、および本学川橋研究室の学生（学部生8名、院生4名）が参加して実施した。各自自宅や勤務先から和歌山大学内の演習環境にVPN（L2TP）接続し、同環境内にあるネットワークおよびサーバに発生するインシデントに対応する。シナリオはステージ1からステージ3まであり各ステージにはシナリオが3つずつある。シナリオには、辞書攻撃によりアカウントが破られ、当該アカウントを用いたコンテンツの改ざんや、Apache Struts2の脆弱性をつき任意のコードを実行され攻撃の踏み台にされた場合の対処などが含まれている。他にSlow HTTP DoS攻撃やMemcachedのリフレクションによる異常なトラフィックの発生など、ネットワークに症状が発生するインシデントも含まれる。DNSサービスを停止させられることで、ネットワーク基幹サービスの停止が、何に起因しているか調査するシナリオも実施した。VPN越しにシュートするには、ネットワークが切れると中断してしまうため、遠隔ハンズオンには常に運用スタッフが和歌山大学側で常駐する。

合同ハンズオン：

遠隔ハンズオンに参加しているメンバーが合同ハンズオンにも参加した（**写真6**）。初日はネットワークに関する法律とセキュリティ対応時における役割についての座学を実施した。次に、AWS（Amazon Web Service）のサービスおよびセキュリティ担当者によるサービス概要の説明を受け、AWSにおける最近のセキュリティ動向について説明を受けた。AWSを利用するユーザのアカウンタビリティーが侵害されて、AWS上のリソース（CPU、メモリ、ネットワークなど）が消費されてしまう事案が発生している。AWSでは、これを回避するために、リソースモニタに機械学習を加えることで、日常的なリソース消費を逸脱した状態を検知し、AWSのIAMユーザにこれを通知するなどのメカニズムを提供している。本演習の受講者は、同メカニズムの紹介を受けた。最終日は、AWSのリソースを他者が消費する事案を想定し、対策システムを構築・運用するというシナリオを想定し、同環境を構築する演習を実施した。

写真６：合同ハンズオンの様子

次に、パケットキャプチャの演習において、https通信の際に発生する一連の通信の流れをWiresharkを用いて確認をした。2日目はCisco社製ファイアウォールの既知の脆弱性を突いた攻撃を成功させるため、Pythonによるプログラムを完成させ、用意した閉鎖環境で実行した。3日目はSplunk社ソフトウエアを使用し、前日に実施した脆弱性を利用した攻撃のログのフォレンジックを実施した。ハンズオンを実施した後、特定の条件のログを検知した際に指定したSlackのチャンネルにWeb hook経由で通知を送信するチューニングを実施した。

●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他の演習の充実にもつながる。

●募集情報

問合せ先：〒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

• ProSec-IT

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。2021年度はその4年目の受講生の受け入れになる（**図7**）。

• SECKUN

また、令和元年度から令和2年度までに厚生労働省の

図 7：ProSec-IT の受講生の受け入れ人数

年度	メインコース		クイックコース		計
	社会人	院生	社会人	院生	
2018	10	0	7	2	19
2019	15	4	3	0	22
2020	17	8	0	0	25
2021	11	6	1	0	18
計	53	18	11	2	84

図 8：SECKUN の受講生の受け入れ人数

NO	コース名	人数
1	ProSec-IT NEXT	12
2	Human Element	15
3	ビジネスイノベーション	7
4	クライシスマネジメント	15
5	セキュリティコンプライアンス	8
計（延べ人数）		57

委託事業として、戦略マネジメント要素を追加した上位コースとなる教育コンテンツとしてSECKUNを藤岡福資郎（学術研究員）を中心に連携企業の全国拡大と共に開発した。令和3年度に職種別（4コース）から職能別（5コース）に再編し新たにProSec-ITで選択可能なコースとして追加した（図8）。

ProSec-ITとSECKUNの両方の講義・演習は、九州大学西新プラザ（ProSec-IT：令和3年11月20日、SECKUN：同年10月31日以降ハイブリット方式で活用）およびネットワーク会議システムを活用したオンライン方式で実施した。オンライン化により九州・山口と共に関東からの受講生を含め地域社会貢献と共に全国から仲間を募る礎を築くことができた。最終的に、ProSec-ITを基幹コースとし、全体で7コース（ProSec-ITメインコース＋クイックコース＋SECKUNの5コース）が選択可能になり、受講生のスキル向上のニーズに丁寧に応え、自走に耐えうるリカレント教育体制を構築・実装した。更にSECKUNにおける成果を踏まえた知見を当事業全体において活用し波及させることで、予算の効率化やプログラムの体系化に結び付けた。

●実施状況

(1) ProSec-IT（九大enPiT-Pro）

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講師書き下ろしの専用教材を開発した。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。

「サイバーセキュリティ技術調査科目群」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、Block Chain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。

「マネジメント科目群」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を準備した。

「ブリッジ科目群」では、危機の現場で不動のリーダシップ発揮するため、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を準備した。

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、九州・山口から全国へ活発な交流活動をしている。「地域セキュリティ講演」や「新しいセキュリティビジネス・キャリアシンポジウム」(120名参加)、有識者を招きBCPや危機管理の公開講演会(無料)等も開催した。

●自走後の計画

【基本方針】

セキュリティベンダやセキュリティ技術者をハンズオン技術演習にて育成するProSec-IT、ユーザ企業やCISO、戦略マネジメント層、先端技術に特化した上位コースとしてSECKUNの両ブランドを維持し、高度技術を中心に据えつつ全方位型の運営を行う。

【講義】

7コースは、維持しつつも大学卒業資格を持たない高度スキルを持つ技術者へ受講の裾野を広げるため、公開講座としてProSec-IT BASEの策定を検討。

【体制、費用】

自走後の運営事務は、専任の事務職員、TA、外部サポータの協力を得て実施する予定である。事務手続、講義謝金、人件費は、授業料収入及び企業寄付金から拠出する。

【受講手続】

現状の手続を維持する(応募書類、履歴書、修了証)。必要に応じて、2次募集等を行う。

【広報】

各連携校のサイトおよびSNS、イベント、企業連携、地域のコミュニティ連携等により広報を行う。

●募集情報

問合せ先:〒819-0395 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
E-mail:prosec-it-staff@cs.kyushu-u.ac.jp
URL:(ProSec-IT)https://cs.kyushu-u.ac.jp/enpit-pro/
URL:(SECKUN)https://cs.kyushu-u.ac.jp/seckun/

2.6 長崎県立大学

●取り組み概要

補助期間終了後の業務継続を踏まえ、enPiTとして提供する科目を大学院情報工学専攻の科目の科目等履修として整理した。2021年度は、開発者を対象とした6科目のメインコースと、6科目より3科目を自由に選択するハーフコースを設計・提供した。提供した科目は**図9**の通りである。

また、授業提供のほか、情報セキュリティ講演会を主催した。この講演会では、情報セキュリティ対策を業務として行っている企業の方を講師として迎え、仕事の内容や業務に必要となる技術や知識とはどういうものであるかについてお話いただいた。**写真7**はその広報用ポスターである。

また、本学におけるenPiTのWebページを刷新して、情報提供に努めた。

図9:長崎県立大学 2021年提供科目

科目名	開講期
暗号数理特論	1Q
データセキュリティ特論	2Q
ソフトウエア開発プロセス特論	2Q
ネットワークセキュリティ特論	3Q
情報セキュリティリスクマネジメント特論	4Q
人工知能特論	4Q

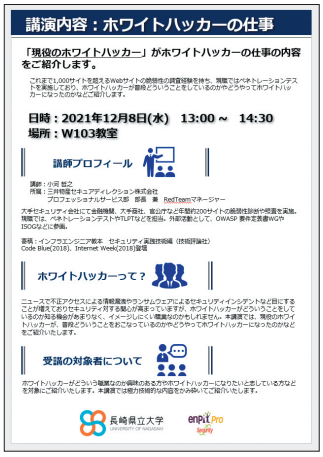

写真7:情報セキュリティ講演会広報用ポスター

写真8:情報セキュリティ講演会の様子

●実施状況

ハーフコースに運輸関係の企業から1名の受講者を迎え、修了した。令和元年度の医療関係者に続き、ユーザ企業からの受講者となった。

情報セキュリティ講演会「ホワイトハッカーの仕事」を12月8日に、対面とオンラインのハイブリッドの形態で開催した。本学学生のほか、enPiT ProSecの連携校学生など31名が聴講した。**写真8**は講演会の様子である。

2月11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10名の委員が参加した。オンデマンド授業の方が受講しやすいという要望があったほか、広報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った。県下のリカレント教育に貢献するため、来年度以降は本学の科目等履修生の制度と合わせてenPiT ProSecの広報を進めることを考えている。

図 10：長崎県立大学 2022 年度提供予定科目

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

●自走後の計画

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。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**図10**の10科目とする。

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。2021年度もCOVID-19の影響が大きく、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ている。

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している。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目指している。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。

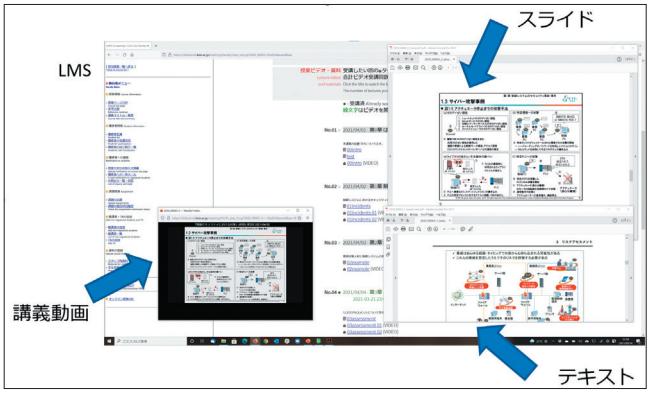

写真 9：e-learning system での受講の様子

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。

継続的にCOVID-19禍においても受講を容易にし、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靱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（**写真9**参照）。

今年度は82名が履修したが、履修認定を受けたのは19名となった。自由に受講できる反面、モティベーションの維持が課題であると考えられる。

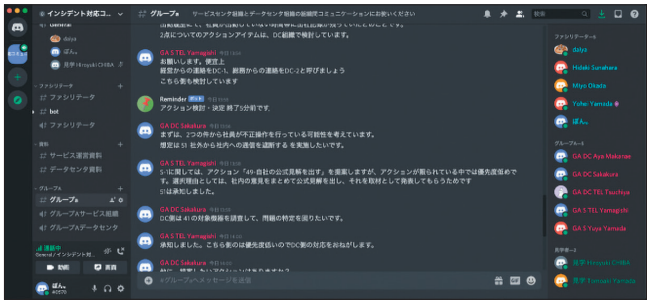

写真 10：インシデントハンドリング演習の様子（オンライン）

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7/27（4名）、2/8（10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、7/27 2名、2/8 2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リテーション演習 Unit 10、7/27 1名）（**写真10**参照）。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。そこで今年度は、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。

●自走後の計画

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。

自走後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

問合せ先：〒223-8526 神奈川県横浜市港北区日吉4-1-1 協生館2F
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
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】

スキルマップの一覧性や可用性に鑑みて、JNSAのSecBoK2017の中項目を基にスキルマップを試作した（**図11**）。このスキルマップでは、SecBoK同様に、セキュリティ人材の役割を16通りに分類している。スキル項目はSecBoK2017の中項目と同じ41項目である。役割ごとに、小項目が一つでも必須なら中項目を必須とした。

各連携校が、提供する各科目やコースに対応する項目にマークし、役割ごとにスキルをカバーしているか否かを可視化した。ここで、科目ごとにスキル項目の集計に算入するか否かを指定できるようにした。これにより、コースの中での選択科目の選び方ごとに役割に必要なスキルのカバーの様子を見ることができる。

図 11：スキルマップ例

引き続き、日本電気・日立・富士通による「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」のシラバスなどを参考に、スキルマップの検討を続けた。

12月9日に、みずほフィナンシャルグループのスキルマップ検討タスクのメンバーを交えて、情報セキュリティのスキルマップに関する意見交換会を開催した。この中で、人材の役割の分類の仕方を各企業の業態などに合わせて対応させる必要があることや、各役割が必要とするスキルも年々変化するといった意見が出された。これは、情報セキュリティという分野の進歩・技術革新の早さが原因の一つとなっているものと考えられる。

また、みずほフィナンシャルグループ・日立・JNSAの各担当者を交えての意見交換会を2022年3月7日に開催した。

【コース連携】

今年度は、慶應義塾大学を中心として、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する試みを行った。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＝1Unit）している。したがって、全体として48 Unit～60 Unit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。

今年度は、九州大学が実施するマイクロアーキテクチャセキュリティ演習（Unit 10）を慶應のインシデントハンドリングコースの受講生が、また慶應が実施するインシデントハンドリング演習（Unit 10）を情報セキュリティ大学院大学の複数のProSecコース受講生が受講している。

このような仕組みが実現したことで、各大学が実施する講義・演習で補完することでより高度な人材育成が可能となってきている。

■ 産学連携 WG

2021年度も引き続きCOVID-19の影響で制限された中で実施を展開してきた。拠点間の連携についてもUnit受講が確立してきたことで進められており、オンラインでの演習実施、e-learningによる講義の実施も進めてきたことになる。特に、オンライン、e-learningの活用は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った。

自走後についても、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していくことになる。また、Unit受講をさらに深化させ拠点間の連携を進めながら全体が融合した体制を確立さていくこととなる。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進める（P03・図3：教育プログラムのフレームワーク参照）。

■ 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、そのアンケート結果を解析する。2021年度は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

- 演習前と演習後にアンケート

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
- 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）

- 数学用語を知っているか教えてください.
  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

- 暗号用語を知っているか教えてください
  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. 講義毎の講義アンケート

- 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. 九州大学でのアンケート

- 講義毎の講義アンケート
- 今日の講義全体の満足度を教えてください
- 講義・演習で分かりにくかった部分はありますか
- 講義全体で良かったところはありますか
- 改善できるポイントはありますか

5. まとめ

今後、各大学でのアンケート結果を取りまとめ、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

今年度のFD WGは、昨年度より引き続き、COVID-19の影響による講義、演習のオンライン化を図ることを目的としたノウハウの共有を運営委員会およびメールにて実施した。

図 12：2021 年度 FD 活動実績

実施日	実施内容
2021年　6月20日	ダイヤモンドプリンセス号の危機管理講演を通じ国家危機レベルのBCPの在り方を講演およびProSecの紹介
2021年　7月18日	学都『仙台・宮城』サイエンス・デイ 2021にてProSecの紹介
2021年　8月10日	JNSA脅威研WGにてProSec-IT／SECKUNの紹介
2021年　9月28日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(福岡) 地域産業編 基調講演での社会人教育のPR
2021年 10月15日	JNSAの会員向け定期メールマガジンへ【前半】 「九州大学におけるサイバーセキュリティ人財育成「ProSec-IT/SECKUN」の取り組みについて【第一回】」を投稿
2021年 10月17日	教育データ利活用シンポジウムにてProSecの紹介
2021年 10月17日	教育データ利活用シンポジウムでの講演でProSecの紹介
2021年 10月28日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(福岡2) 海外ビジネス編 基調講演にて社会人教育のPR
2021年 10月29日	全国サイバーテクニカルアドバイザー意見交換会にてProSecの紹介
2021年 10月29日	放送受信障害解消Webセミナーにてオンライン講義・演習に関する講演
2021年 10月29日	JNSAの会員向け定期メールマガジンへの投稿【後半】・ 九州大学におけるサイバーセキュリティ人財育成「ProSec-IT/SECKUN」の取り組みについて【第二回】
2021年 11月10日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(大分) 宇宙産業編での基調講演での社会人教育のPR
2021年 11月22日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(佐賀) 医療薬局編にて基調講演での社会人教育のPR
2021年 12月17日	AXIES2021にて「セキュリティ人材育成と大学間連携」についての講演
2021年 12月17日	AXIES2021にて「大学連携による実践的セキュリティ人材育成」の企画セッション
2022年　1月28日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(熊本) 農業関連編　基調講演での社会人教育のPR
2022年　2月 9日	地域SECUNITY形成促進事業「サイバーセキュリティセミナー」(宮崎) 林業関連編　基調講演での社会人教育のPR

図 13：FD 活動実施総数

年度		2018	2019	2020	2021	計
実施内容	イベント実施、参加	3	6	9	11	29
	視察	1	4	0 *1	7	7
	講演、広報	4	9	7	17	36
実施総数		8	19	16	35	78

＊1：COVID-19 による社会情勢の大幅な変化により、イベントの開催および演習の視察について慎重な取り組みとなった。

また、オンラインにおけるセキュリティ演習の実施を様々な方面に講演、視察、イベントを通して共有を行った。

オンライン化についての実績

昨年度より取り組んだオンライン化のノウハウの共有をもとに各連携校で様々な講義のオンライン化が図られ、現在はほとんどの講義、演習がオンラインで実施可能になっている。また、今年度も継続しているコミュニケーションツールやソフトウェアの更新情報を共有することにより迅速な適応と新たな機能の追加を実現した。

また、オンラインでのセキュリティ教育の実績として、多方面からの講演依頼が増加し、本年度だけで17件実施した（図12）。

得られた成果

FD WGにおいて得られた主な成果を挙げる。

- ProSec全体として一定の品質を担保したオンライン講義演習の提供
- 2018から本年度まで、外部への演習視察、イベント、講演、計78件の実施（図13）。
- オンラインを前提とした演習の構築ノウハウの蓄積および共有。また、事項に示す自走期間における新規演習開発への活用。

自走後の計画

オンラインで実施することを前提として、引き続き視察、およびオンライン化のためのノウハウの共有を継続していく。

また、新規演習の構築や既存の演習の見直しを外部と連

図 14：ProSec Web サイト（https://www.seccap.pro/）

図 15：Twitter アカウントによる情報発信

携して実施することで、実社会、サービスでも活用可能な演習を継続して提供し続けるための連携を行っていく。

■ 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 (https://www.seccap.pro/) (図14)
- 愛称、ロゴの活用
- ポスター制作、パンフレット配布
- Twitterアカウントの活用 (@enpitprosec) (図15)

等がある。

平成30年度から本格的に実践的情報教育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では各連携校の開講コース等の情報を取りまとめ、CMS化したWebサイトを活用し、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。

- ProSecホームページのニュース記事に、各種イベント、お知らせ等の情報発信
- 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
- ProSecWebサイトコンテンツの再構成
  本プログラムや各コースの紹介、リーフレット、事業報告書のWeb公開、新規連携企業・団体の追記

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

202203