【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 2024

2024 年度 事業報告書

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。情報セキュリティ業務に従事している人材は 2024 年には 48 万人まで増加しているが、サイバー攻撃の高度化や多様化が進み、また社会のデジタル化・DX（デジタルトランスフォーメーション）の加速が進んだことにより、守られるべき資産と範囲が増えたことにより、依然として情報セキュリティ人材は不足している。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。

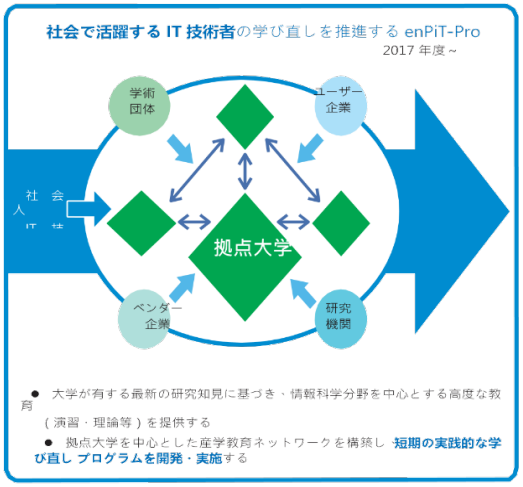

図 1：enPiT-Pro 事業全体イメージ

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。

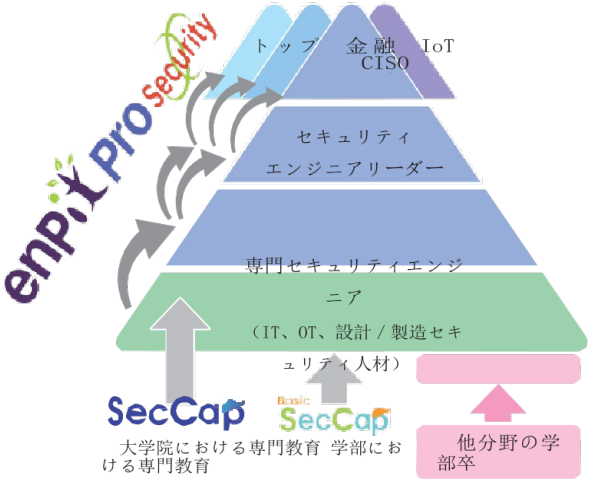

図 2：セキュリティ人材育成における ProSec の位置づけ

▸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 310 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。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が、2023 年にはその第一段階として、既存提供科目のスキルマップ各項目との対応付けを行い、コースとしての価値や十分性の確認を行った。

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（数日～ 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。

▶ 2024 年度の実施状況

2024 年度も引き続き感染対策を徹底した上で対面授業で実施した（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 2 か月に 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** の通りである。

WG	サブ	メンバー
教務 WG	スキルマップ	砂原（慶應）
産学連携 WG		砂原*（慶應）曽根・種茂
評価 WG		宮地*（阪大）
FD WG		加藤*（慶應） 和泉（東北）

図 3：ワーキンググループ　＊は主担当者

運営委員会では、さまざまなプログラム実施上の課題について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。2024 年度は、各連携大学がそれぞれ自走を行う中での課題について意見交換を行い、その改善を図った。また前年度に引き続き各連携大学の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を、、オンラインで効果的に教育するための工夫の共有等を行い、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。

その他、広報活動の一環として行っているサイエンス・デイや大学 ICT 推進協議会年次大会（AXIES2024）の企画セッションへの出展に向けての意見交換や情報共有を行った。

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、2024 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）-NW 攻撃とその防御及び検知-（45 時間）

・CSIRT 構築クイックコース（30 時間）

セキュアシステム技術(基礎)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。

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。

その他、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として開講している。

・IoT セキュリティコース（12 時間）

・CTF の基礎コース（6 時間）

・グローバルリスク分析コース（10.5 時間）

・デジタル製品セキュリティコース(14 時間)

IoT セキュリティコースは、サプライチェーンからホームセキュリティまでを対象に、SBOM、TEE などを安全保障の活用が見込まれる技術を紹介し、IoT セキュリティの新たな考慮すべき点を講義と演習を通じて学べるコースである。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として提供した。グローバルリスク分析コースは、セキュリティリスクに留まらず、グローバルにリスクを意識することを想定したリスク分析のためのコースとして提供した。デジタル製品セキュリティコースは、昨今対応が求められている欧州の CRA(サーバーレジリエンス法)を対象に、必要な対応について演習を含む講義を行うものである。

実施状況

2024 年度の受講者は 192 名（内、特別コースは 151 名）、クイックコース修了者は 22 名であった。

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―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（写真１）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。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習得することができた。IoT セキュリティコースは、講義で IoT システムサービスを運用するための広範囲な基礎知識を習得し、また演習では脆弱性検査の演習を受講することができた。今年度の IoT セキュリティコースは、受講希望者が定員を大幅に上回ったため、2 回に分けて実施した（写真２）。グローバルリスク分析コースでは、システムに対する脅威分析とリスク評価手法について、2 日間の座学と演習を実施し、受講生は実践的な脅威分析手法について習得することができた。

また、デジタル製品セキュリティコースでは、座学と演習やフリーディスカッションを取り入れた研修を実施した結果、受講生から講師への積極的な質問や、受講生同士で活発に議論を交わす様子が見られ、関心の高さをうかがわせた。

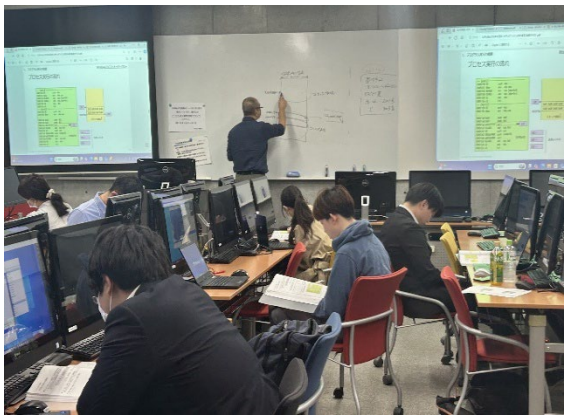

写真１：セキュアシステム技術（基礎）クイックコース演習風景

写真 2：IoT セキュリティコースの演習風景

来年度の計画

2024 年度は昨年度に引き続き、受講生がさらに増加した。来年度も同コース数を開講し、幅広い受講生のニーズに応えたい。広報に関しても引き続き、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 コース案内を掲載し、新たな受講者層の開拓を目指す。

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、2024 年度の ProSec の取り組みとして、継続して以下の 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。

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））

メインコースとクイックコースに加えて、受講者の様々な要望に対応するためにリアルタイムオンライン配信、LMS を利用したオンデマンド配信など様々な講義形態を用意した。大学院レベルの予備知識に達しない、あるいは 1 科目分の参加時間の確保が困難な社会人に対して、学部レベルの科目の要素を短時間かつオンデマンド形式で提供した。

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 2024 などのイベントで本事業の取り組みの紹介をして、様々な社会人の方々と意見交換を行った。（写真 3）

写真 3：サイエンス・デイ 2024 の様子（写真）

来年度の計画

運営体制の都合により 2026 年度以降の ProSec の実施が困難になる見込みであり、ProSec 受講者はおおむね 2 年度にまたがって履修することから、2025 年度は積極的な募集は控えることを予定している。

これまで 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（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(2 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）

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・西村あさひ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．

4. 実施状況

今年度はプロジェクト学習を行う「先進安全なデータ設計特論」において，2 つのプロジェクトの内容において，優秀研究賞の受章と国際会議論文での採択という大きな成果を挙げたので記載する．下線の学生が ProSec の受講者である．

-IPSJ CSEC 優秀研究賞 2024：「耐量子計算機暗号 LWE 暗号の亜種に関する調査報告」，城戸良祐，森本和邦，奥村伸也，宮地充子．

-22nd Annual International Conference on Privacy, Security, and Trust (PST2025)(採択)：“Privacy-Preserving Image Learning Across Trust Boundaries”，Yagishita, Hyohdoh, Boudvillain, and Miyaji.

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 2024 年度各コース

コース ＼ 名科目名	メインコース(12 単位以上)				クイックコース (6 単位以上)				
	セキュリティ	暗号	サイバー	総合	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
実践セキュリティ特論 I，II	必	必	必	必	必		必	選 B	選 B
実践離散数学と計算の理論	必	必		必		必		選 E	
先進情報セキュリティとアルゴリズム	必	必		必		必		選 E	
高度セキュリティ PBL	必	必	必	必	選 C	選 B		選 C	選 D
高度セキュリティ PBL II		必		必		選 B		選 C	選 D
高度セキュリティ PBLIII	必	必	必	必	選 C			選 C	選 D
高度サイバーセキュリティ PBL I	選 A		必	必	選 C		必	選 C	選 D
高度サイバーセキュリティ PBL II	選 A		必	必			必	選 C	選 G
高度サイバーセキュリティ PBL III			必	必			必	選 C	選 D
先進安全なデータ設計特論	選 S	選 S	必	必	選 S	選 S	選 S	選 S	選 S

※【必修】必修科目

※【選択 A】高度サイバーセキュリティ PBL I,II から 1 単位以上取得

※【選択 B】講義科目・PBL 科目から 1 単位以上取得

※【選択 C】PBL 科目から 2 単位以上取得

※【選択 D】PBL 科目から 4 単位以上取得

※【選択 E】講義科目から 2.5 単位以上取得

※【選択 S】クイックコースを 1 コース以上修了していること

受講者数

2024 年度前期受講生：28 名

2024 年度後期受講生：25 名（前期で修了が 3 名，後期から新規 2 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 4）を表す．

写真 4: PBL 演習の対面参加の様子

各講義の受講者数

なお，各講義の受講者数は以下の通りである．

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：13 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：9 名，高度セキュリティ PBL：10 名，高度セキュリティ PBL II：4 名，高度セキュリティ PBL III：5 名，高度サイバーセキュリティ PBL I：13 名，高度サイバーセキュリティ PBL II：10 名，高度サイバーセキュリティ PBL III：10 名，先進安全なデータ設計特論：4 名

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．

- 実運用・現場の視点からの話が多く，私自身，病院情報システムの運用を担当している立場でもあることから，全体的に非常にうなずける内容ばかりであった．特に，セキュリティ要求工学で紹介いただいた文献には目を通しておきたい．
- ログ解析や BOF 攻撃など，言葉として知っていましたが，実際にどうやるのか，どういうことが起こるのか，その中身について，これまで以上に理解することができました

（身近に感じることができるようになりました）．講義のペースも過度に早くなく，行き詰まったときもすぐにヘルプしていただき，初学者としても助かりました．

・実際に自身の手を動かして，リモートアクセス環境でコマンドを打ち込み，サーバーの設定をおこなう作業を初めて経験した．不慣れなコマンドライン操作に戸惑うことも多かったが，今後スキルアップを図る上で目標とすべきことの一つが見えた．

・暗号の基礎，暗号の仕組み，署名など基礎を学べた．

・リバースエンジニアリングの基礎と実践は，リバースエンジニアリングの実践力を高める上で非常に有益だった．逆アセンブル・逆コンパイルの違いや，それぞれの活用方法，スタックオーバーフローの概念と，それを悪用することで任意コード実行につなげる技術が学べた．

2024 年度修了生

2024 年度は 19 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 5）を 2025 年 3 月 23 日に実施し，意見交換会を実施した．

写真 5: 大阪大学 ProSec の修了認定式自走後の計画

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．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 年度から徴収した．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.html

2.4 和歌山大学

取り組み概要

和歌山大学では，2024 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（2024 年 8～9 月）
- 遠隔ハンズオン(2025 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，サイバー犯罪にどのように対応するか，どのような手法がサイバー犯罪を未然に防ぐことに有用であ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，初学者を対象としたネットワークインフラ構築を学習する演習を行った．

初学者を対象としたネットワークインフラ構築を学習する演習では，ルータやスイッチ等の基本的なネットワーク機器の働きを学習し，グループワークを取りいれたことで，協力して演習の問題を解決する演習となった．目標を達成できるように機器や LAN ケーブルのイラストを実際の部屋に見立てた図面に貼り付けることで，ネットワーク環境を再現する作業を行った．機器の使用用途を理解し，構築することで，サーバ，ネットワークを把握する能力を向上させた．ネットワーク構築に対する知識を身に付けた後に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．環境構築については，演習環境を提示し，実際のネットワーク環境におけるネットワークやパケットの流れを理解した後に図面通りに環境を再現する作業を行った．実際に環境を読み解き，構築することでサーバ，ネットワークを把握する能力を高めた．ネットワーク環境構築と同時に行った TCP/IP の座学や Linux サーバを用いた UNIX コマンド演習により，ネットワークの知識だけでなく，サーバに関する知識を補填することで IT インフラに対する理解を深めた．

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．この際，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深めた．Basic SecCap 演習終了後，演習の練習によるシナリオへの理解を経て，SecCap 演習(NAIST9 月下旬)に以前の演習と同様，運営として参加する．

また，SecCap 演習の練習を行うと同時に様々な脆弱性に触れるため，参加した捜査員 5 名で協力し，来年度に行う演習のための新しいインシデントシナリオの作成を行った．これにより，シェルスクリプトの理解や複数の脆弱性とその一時対策方法等の理解を深め，研修における教育的な効果の検証を行うことができた．**遠隔ハンズオン：**金融系のセキュリティ部門の SE7 名が参加者として，本学川橋研究室の学生(学部生 8 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(L2TP)を用いて接続し，同環境内に作成されたネットワーク及び，サーバに発生した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．シナリオでは，辞書攻撃を用いた不正ログインを行い，当該アカウントが運営しているサイトが別のページにリダイレクトするシナリオ，sudoedit の脆弱性をついた攻撃による特権昇格を行い，バックドアの設置などや任意のプログラムを実行するインシデントのようなサーバを中心としたインシデント，SQL インジェクションのようなアプリケーションの脆弱性をつきデータベースに不正アクセスしデータを編集するシナリオ，Slow HTTP DoS のような Dos 攻撃による異常なトラフィックを発生させるネットワークのインシデント対応を行った．一つ解くごとに，アブストラクトを用いて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センター(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

九州大学では技術中心の ProSec-IT として、2018 年度から受講生を受け入れ、また 2021 年度から厚生労働省からの予算を得て、技術以外のコンプライアンス、クライシスマネジメント、ビジネスイノベーション、ヒューマンエレメントなどの要素を取り入れた SECKUN という教育プログラムを展開している。60 時間から 120 時間の複数のコースとなっており、毎年 50 名以上、開講から現在までに延べ 259 名が受講している。

ProSec-IT

2018 年 4 月より学修時間 120 時間超で履修証明プログラムとなっている「ProSec-IT メインコース」および学修時間 60 時間超の「ProSec-IT クイックコース」を開講している．2023 年度はその 6 年目の受講生受け入れになるのだが、2023 年 10 月から 2024 年 9 月までの開講とした（図 4)。

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	17	4	1	0	22
2022	6	5	1	2	14
2023	4	0	0	0	4
合計	69	21	12	4	106

図 4:ProSec-IT 受講修了者の人数

SECKUN

SECKUN は令和元年度から令和 2 年度までに厚生労働省の委託事業として戦略マネジメント層を対象とする教育コンテンツを連携企業とともに追加したものである（図 3)．各コースは公開講座の枠組みで実施し，履修証明プログラムよりも受講生の手続きを簡単にすることができ受講し易くした．以下の（モデル）コースのうち ProSec-IT-BASE, ProSec-IT-NEXT，ProSec-IT-SECKUN は，ProSec-IT の内容やその一部を公開講座の枠組みで受講できるように開設したものである。

（モデル）コース名	2021	2022	2023
ProSec-IT-BASE		4	
ProSec-IT-NEXT	12	13	
ProSec-IT-SECKUN			13
ヒューマンエレメント	15	11	6
ビジネスイノベーション	7	6	6
クライシスマネジメント	15	13	8
セキュリティコンプライアンス	8	12	9

総計	57	59	42

図 5:SECKUN の受講修了者の人数

実施状況

今年度は継続可能な自走体制を模索するために，2023 年 10 月からの 1 年間の開講とし，図 6 に示すように同様の講義内容と規模で開講をした．例年同様 ProSec-IT と SECKUN のモデルコースを概観すると，サイバーセキュリティの技術面とそれ以外の要素である，コンプライアンス，人間要素，ビジネスイノベーション，危機管理といった各側面を体系的に学ぶことができ，高いレベルで経営層や経営マネジメント層を含む社会人を対象に学べる内容になっている．また安価な受講料，すべてオンラインやアーカイブ受講で学べ，なおかつハイブリッド対面講義に参加できれば受講生どうしの交流も可能で切磋琢磨できる環境が整っている．技術を扱う ProSec-IT/ProSec-IT-SECKUN では，受講生からの要望を踏まえて演習が非常に充実した内容になっている．事業継続演習 BCP 体験型演習などの実践に基づく演習が充実している等の良いポイントはすべて継続して行った．

モデルコース	時間数
ProSec-IT-SECKUN/ProSec-IT	126
セキュリティコンプラインスモデルコース	63
クライシスマネジメントモデルコース	48
ビジネスイノベーションモデルコース	49
ヒューマンエレメントモデルコース	53

図 5：各モデルコースの講義・演習時間

以上の教育プログラムに含まれる内容は、サイバーセキュリティの技術にのみ焦点を当てるのではなく、技術以外の要素である、法制、機器管理、ビジネスイノベーション、ヒューマンファクタも体系的に学ぶことが可能なものなっており、さらに、受講生、講師、大学、地域のコミュニティ形成を支援することができるものとなっている。例えば、その一環として 2024 年 9 月 21 日には、修了式を兼ねコミュニティ形成を目的とするシンポジウムを開催している。これにより社会人が貴重な時間を削って参加する価値のある学の場とすることができる（写真 6)。

写真 6:貴重なライフタイムを共有する価値のある学びの場

来年度の計画

本教育事業は多くの社会人からの需要が高いため，継続のための工夫を行い来年度以降も実施して行く予定であるが、現在のところ十分なスタッフが確保できない状況であり、多くの土日開講、ハイブリッド会場の確保、27 名程度の学外講師や 50 名程度の受講生の対応が困難になってきている。そのため、九州工業大学が立ち上げた社会人向けリカレント教育を支援することを目的とする特別目的会社である KyutechARISE と連携して実施することを計画している。

募集情報

問い合わせ先：九州工業大学･入試･教育接続課　リカレント･リスキル教育推進係

TEL: 093-884-3320

E-mail：eCampus@jimu.kyutech.ac.jp

URL:https://www.kyutech-arise.co.jp/course/special/cyber-security/

2.6　長崎県立大学

取り組み概要

2024 年度も、例年通り、大学院情報工学専攻の科目の科目等履修を介して、enPiT ProSec として科目を提供した。開講科目のうち、6 科目を修得することで認定されるメインコースと、3 科目を修得することで認定されるハーフコースの 2 コース体制とした。なお、本年度開講の 9 科目を表 2 に示す．また，両コースの周知のため，本学 Web ページでの案内も実施した。

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

表 2　2023 年度 enPiT ProSec 開講科目一覧

実施状況

本年度は、本学在学の学生が大学院科目履修の一環で enPiT Pro に参加をし、生体情報特論、インターネット基盤セキュリティ特論、ソフトウェア開発プロセス特論、サイバーセキュリティオペレーション特論などの受講を経て、4 名がハーフコースを、一方、3 名がメインコ

ースを修了した。なお、ハーフコース修了者のうち2名は、本学学部生が大学院進学を念頭に大学院生向けの科目を受講できる先取履修制度を利用して履修を行った学部4年生である。

なお、当プログラムの周知のため、長崎県庁職員に向けた案内を県学事振興課への依頼、長崎県情報産業協会の会員向けの周知を行った。

写真7：

図2 講義の様子

来年度の計画

来年度も、今年度の事項を継続し、科目等履修生制度を介した enPiT ProSec 科目の提供やその広報を継続して実施したいと考えている。

募集情報

問い合わせ先：〒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 情報システム学部情報セキュリティ学科(ProSec 担当)

TEL: 095-813-5153

E-mail: sun-prosec@sun.ac.jp

2.7　慶応義塾大学

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。2023年度は COVID-19 が5類感染症に移行され、原則として平常通りの活動ができるようになったが、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継続してきた。

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)は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し、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しつつある。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なっている。

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てきた。

実施状況

2024年度は、これまでの実施状況を振り返り、教材のブラッシュアップに注力した。

1. e-learning system による講義教材

e-learning system の講義教材も作成してから時間が経ち内容の精査が必要になってきた。そのため参照資料の更新や新しいセキュリティ状況への対応を行い次年度へ向けた準備を行った。

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の教材についても、更新を行い、その試行を8/27に実施し11名が参加し教材の有効性を確認した。エコシステムについても特に上位レベルの人材育成のための検討を行い次年度へ向けた準備を整えた。

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。今年度は、1名の参加者が一連の演習の一部を修了しており、これによりインシデントハンドリングクイックコースを修了している。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

2025年度は、更新された教材を用い、これまでの知見を活用し、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/先導研究センター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.j