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	E-mai：prosec-it-staff@cs.kyushu-u.ac.jp URL：https://cs.kyushu-u.ac.jp/enpit-pro/
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）	E-mail：sun-prosec@sun.ac.jp
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

201903

【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 2019

2019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平成29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。平成28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、様々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。

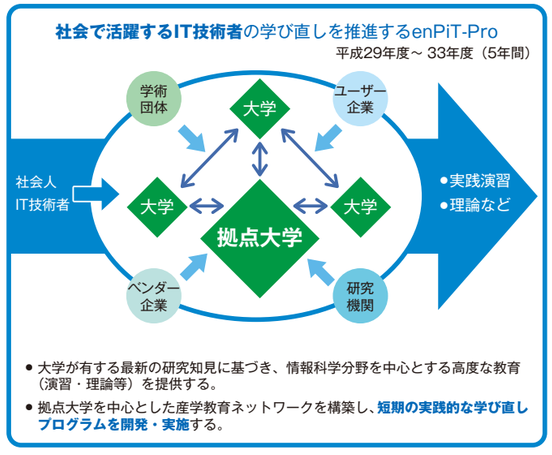

図1：enPiT-Pro事業全体イメージ

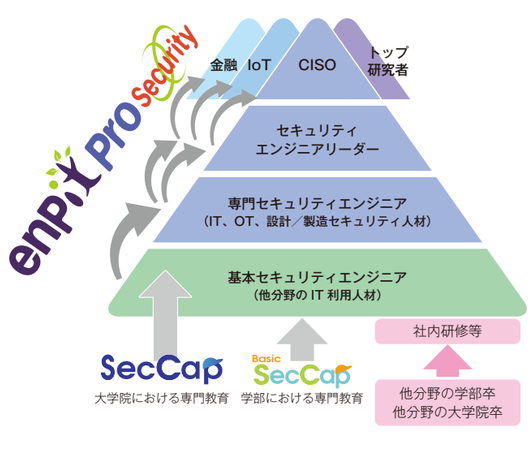

図2：セキュリティ人材育成におけるProSecの位置づけ

▶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教育に注力する。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240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。

2019年度は、JNSAが2019年度に公表したSecBok2019に対する充足状況を調査した。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、現状のSecBok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

平成19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。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

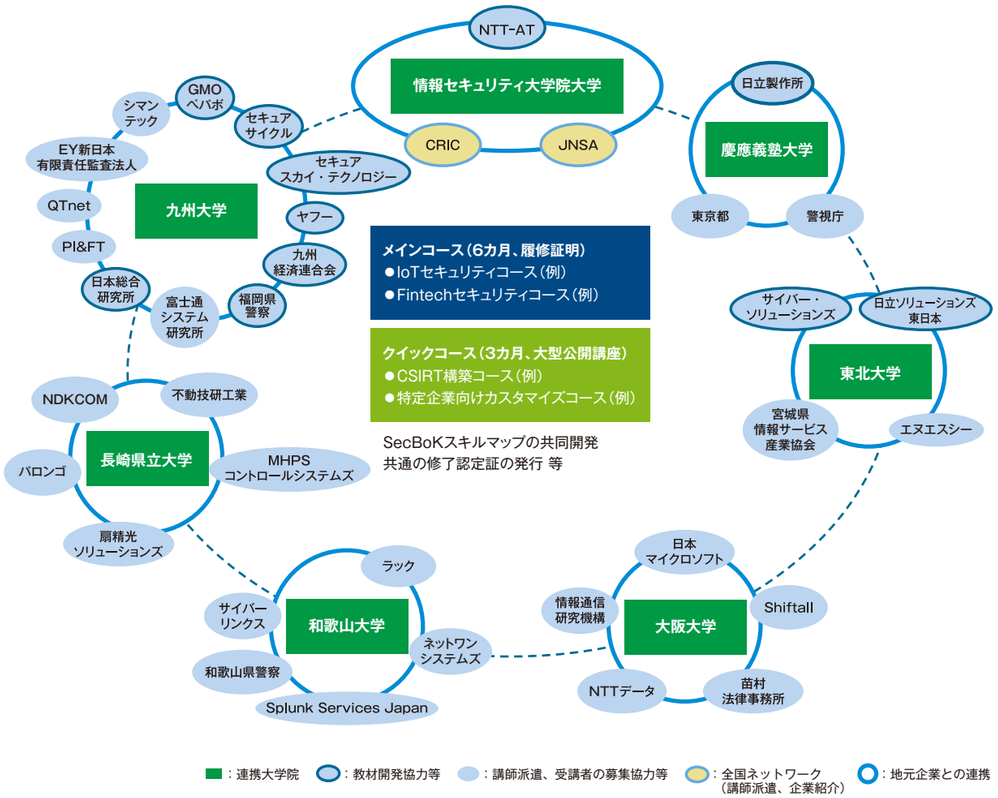

図3：教育プログラムのフレームワーク

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試行的に開講した。

▶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、さら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。

▶2019年度の実施状況

2017年度の各連携大学における準備を踏まえて、各連携大学は2018年度から本格的にコースの提供を開始し、2019年度はさらに提供するコースが充実した（各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
高畑　昌志	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

2019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。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及びメンバーは図4の通りである。

運営委員会では、当初予想していた以上に短期間でコンパクトに学修したいというニーズが強く存在すること、企業や社会のニーズに配慮しつつ大学院教育ならではの体系性を維持することなど、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。2019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相互参観と意見交換を行うほか、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、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。

2019年度は、2020年3月12日に、平成29年度文部科学省enPiT-Proに採択された5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enPiT-Pro 5拠点合同シンポジウム『Society5.0に向けた人材育成とDX』の開催を計画した。合同シンポジウムでは、各拠点によるコースの概要や取り組み内容の紹介、およびポスター発表形式による個別紹介・相談を実施する予定であったが、新型コロナウイルス感染症対策の観点から、関係者間でのオンラインによる意見交換を実施した。

図4：ワーキンググループ

WG	サブWG	メンバー
教務WG	スキルマップ	小松*（長県大）、小出（九大）、山口（長県大）
	コース連携	湯淺*（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		山内*（慶應）、和泉（東北大）
広報WG		内尾*（和大）、砂原（慶應）、奥村（阪大）

＊主担当者

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、2019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、次のコースを開講した。

●CSIRT 運営管理者向けメインコース
●IoT セキュリティメインコース
●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

CSIRT運営管理者向けメインコースは、IT実務の現場でセキュリティ対策を技術面・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。組織における標的型攻撃対策、ソフトウェアやネットワークシステムの設計・開発段階でのセキュリティ対策、セキュリティマネジメント、

CSIRT運営等に関わる業務遂行に必要な知識、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。

IoTセキュリティメインコースは、IoT機器やIoTサービスの設計・開発から運営に至るトータルなセキュリティ対策を技術面・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。IoTセキュリティ技術やSecurity-by-Designにおける脅威分析技術等について、業務遂行に必要な知識、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。

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―

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。

●実施状況

本学の今年度の受講者は、合計10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及び能力を習得することができた（**写真1**）。

●来年度の計画

来年度も、今年度と同様のスケジュールと人数で実施することを予定しているが、より短期間で集中的に学びたいという要望が強いことを受けて、クイックコースの充実を図ることを検討中である。また、各連携大学とのコース交流により連携したメニューを提供することも検討中である。

写真1：セキュアシステム技術（基礎）クイックコースの講義の様子

●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
TEL：045-311-7784（代）
E-mail：prosec@iisec.ac.jp
URL：https://www.iisec.ac.jp/admissions/prosec/
【事務取扱時間】平　日 9：00-20：00
　　土曜日 9：00-17：30

2.2 東北大学

●取り組み概要

東北大学では、2019年度は以下の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時間提供する。

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。

また、多様な受講者のニーズやレベルに対応するよう今年度より、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整備して、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、実践的なハンズオンを通じてさまざまなプロトコルやアプリケーションが有する脆弱性について確認し、それらの脆弱性が攻撃者による偵察行為や攻撃にどのように利用されるのかを知り、それらへの対策についての検討を行った（**写真2**）。

写真2：グループ演習で課題に取り組む受講者

また、各コースの内容と教材や環境を整備し、コースの詳細な内容をまとめて募集案内やシラバスを作成した。これらをもとに地元企業を中心に受講生の募集を行い、今年度はセキュリティマインドクイックコース（セキュリティ）を1名が受講した。授業評価アンケートでは、講義や演習で学んだ知識や技術について多くの部分が業務に使えるといった回答があった一方で、今後取り上げてほしいテーマや課題についての意見もあり、来年度以降の授業改善に役立てていく。

今年度は推進室のTwitterアカウント（@espritistohoku）を開設し本学の取り組みを発信するとともに、以下のイベントで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している。

●学都「仙台・宮城」サイエンス・デイ2019（2019/7/14）
●電気関係学会東北支部連合大会（2019/8/22-23）
●大学ICT推進協議会年次大会（AXIES）（2019/12/13）
●東北地域連携イノベーション展2020（2020/1/17）

●来年度の計画

これまでに得られた知見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、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。また、（一社）宮城県情報サービス産業協会（MISA）との間で地域高度IT人材育成における連携協力協定の締結、さらには行政や他の地元団体等と、高度IT人材育成に関するコンソーシアムの設立を目指す。

そして、引き続き、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、技術部門の問題でなく、今や、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むものである。一方、ビットコインにみられるように、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の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およ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）
- 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（各1単位）

- 高度セキュリティPBLⅠ、Ⅱ、Ⅲ
- 高度サイバーセキュリティPBLⅠ、Ⅱ、Ⅲ

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データ及びNICTと連携し、高度セキュリティPBLⅢ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、日本マイクロソフト、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、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

2019年度前期受講生：8名

2019年度後期受講生：16名

写真3：高度サイバーセキュリティPBLⅠの演習風景

写真4：高度セキュリティPBLⅢの集合写真

図5：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
最新セキュリティ特論Ⅰ、Ⅱ	必修	必修	必修	必修		必修
離散数学と計算の理論	選必A	必修	選必A		必修	
実践情報セキュリティとアルゴリズム	選必A	必修	選必A		必修	
高度セキュリティPBLⅠ	選必B	選必B		必修	選必B	
高度セキュリティPBLⅡ	選必B	選必B			選必B	
高度セキュリティPBLⅢ	必修	選必B	必修	必修		
高度サイバーセキュリティPBLⅠ	選必C		必修	必修		必修
高度サイバーセキュリティPBLⅡ	選必C		必修			必修
高度サイバーセキュリティ PBLⅢ	選必C		必修			必修

※【必修】必修科目
※【選必A】講義科目から選択（2単位以上）　※【選必B】高度セキュリティPBL科目から選択（1単位以上）　※【選必C】高度サイバーセキュリティPBL科目から選択（1単位以上）

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：5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：8名、高度セキュリティPBLⅠ：1名、高度セキュリティPBLⅡ：2名、高度セキュリティPBLⅢ：6名、高度サイバーセキュリティPBLⅠ：4名、高度サイバーセキュリティPBLⅡ：4名、高度サイバーセキュリティPBLⅢ：6名

3. 受講者の講義への意見

- 基本から最新の動向まで順を追って説明がありわかりやすかったです。
- 演習の内容が素晴らしいと感じました。実際に手を動かして学べるため、よい経験になったと思います。

●来年度の計画

定期的な会報の送付やセキュリティ関連招待講演やイベントの実施などにより、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、2019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（2019年8～9月）
- 遠隔ハンズオン（2019年11月～2019年12月）
- 合同ハンズオン（2019年11月27日、28日、29日）

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、ネットワークベンダのSE、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。ベンダ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。

上記の取り組みでは、基本的に座学で学ぶネットワーク、サーバの仕組みやセキュリティの知識をどのように活かすのか、知識の一つ一つの点を実践によって線で結ぶことを目的としている。

●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。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。

遠隔ハンズオン：

ネットワークベンダより1名、ソリューションベンダより6名、他市役所職員1名が参加した。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。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。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、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（**写真5**）。

写真5：合同ハンズオンの様子

●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、2017年度までに連携企業や連携機関とも打合せを行い、以下のメインコースとクイックコースの各コースの内容と教材や演習環境について具体的な検討を実施し、募集要項やシラバスの作成、履修証明プログラムの審議や社会人の入学に関連する事務手続きの流れを決める等の学内諸手続きを終え、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。2019年度はその2年目の受講生受け入れになる。

各コースの具体的な講義･演習内容を**図6**に示す。講義概要は昨年度のものと同一内容であるが、中に含まれる演習等の内容は昨年度から刷新している。情報システムを構築する最新の技術、および情報システムをサイバー攻撃から守るための攻撃する側の技術も含めた発展的な技術について、講義･演習を通じて、知識や技術的手法を習得する教育プログラムとしている。演習の内容は、企業等の協力を得て、最新技術や最新のサイバー攻撃に関する知見を反映させたものとしている。

講義内容を最新のものにしたり、演習内容を実践的なものにしたりするには、大学だけで検討しても中身を充実させることは難しい。脅威に関する最新の情報が集まり、常に脅威に直面し、その対策を行っているのは企業が中心である。このため、九州大学では、連携企業（ヤフージャパン、セキュアスカイ・テクノロジー、GMOペパボ、セキュアサイクル、日本総研、QTnet、EY新日本等）の現役エンジニアの協力を得て、その時点で現役エンジニアが最も興味を持つ技術についての講義や演習を含めた内容とした。日々の業務に追われる地方の現役エンジニアにとり、新しい技術を常に探求している連携企業の現役エンジニアによる自身の研究結果に基づく最新技術を含む講義を聞くことは、非常に良い刺激となり得る。

図6：九州大学 ProSec-ITの講義概要

サイバーセキュリティセンター提供科目（新設科目）
• 情報システムセキュリティ演習（Webセキュリティ等） • セキュリティエンジニアリング演習（サイバーレンジ、IoTセキュリティ等）
システム情報科学府提供科目（既存科目）
• 暗号と情報セキュリティ･同特論 • 情報ネットワーク特論
サイバーセキュリティセンター提供科目（履修証明プログラム科目）
• 情報システムとセキュリティ

●実施状況

今年度から産学連携の一環として、交通至便な福岡市内中心部に位置し十分なスペースの会議室をQTnetからお借りしてProSec-ITの講義・演習を実施している。昨年度からの変更点としては、講義開催1日あたりの時間数を増やし開講日数を減らしたこと、より理解に時間をかけた方が良いとアンケートにあった講義・演習項目の時間を増やしたこと、フォレンジクス等新しい講義・演習を追加したこと等が挙げられる。特別講師は主に連携企業から招聘し、各講師の独自技術や大学ではなかなか集まらない実際のサイバー攻撃に関する最新動向についての講義・演習を依頼・実施している。

写真6：初回講義・演習・ガイダンスの様子（2019/4/13）

写真7：ユーザ企業のセキュリティミッション（2019/6/29）

写真8：デジタルフォレンジクス演習（2019/7/20）

写真9：セキュリティエンジニアリング演習の様子

写真10：広告サービスとセキュリティ演習・講義の様子

写真11：パケット解析の重要性とハンズオン演習の様子

その後、組織マネジメントやサイバーインシデント危機管理演習、ユーザ企業のセキュリティミッション（文系セキュリティ）（**写真7**）、サイバーエコノミクス、デジタルフォレンジクス（**写真8**）といった講義・演習を行った。「セキュリティエンジニアリング演習（**図6**）」については夏期に九州大学伊都キャンパスで実施し、社会人現役エンジニアにとり、いつもとは異なる雰囲気の大学キャンパスで行った（**写真9**）。

さらに後半においてはWebアプリケーションの脆弱性、マイクロアーキテクチャ攻撃、IoTにおけるサイバーセキュリティに関する演習を行った。また連携企業のヤフーから「教育と啓発」「広告サービスとセキュリティ」「脆弱性診断」「個人情報とプライバシー」といった一連の講義・演習をしていただいた。例えば「広告サービスとセキュリティ（**写真10**）」は、マイクロターゲット広告やフェイクニュースなどの最新の話題も扱っている。また連携企業のシマンテックによる「パケット解析の重要性とハンズオン演習」は、情報システムに対する実際の攻撃を記録したパケット解析から攻撃者が何を行ったのかを解析する実践的な内容になっている（**写真11**）。

さらに講義演習の後半においては、昨年度に引き続き大阪大学と共催でCTF（Capture The Flag）と呼ばれている、いままで学習したさまざまなサイバーセキュリティ技術を総動員して技術的な競技を行う競技大会をクラウド技術等を駆使して遠隔で共同実施（**写真12**）し、受講生が切磋琢磨して互いにスキルを向上できる機会を用意した。

最終的に2020年2月にメインコース19名、クイックコース3名（うち4名がシステム情報科学科の学生、1名が福岡県警の公務員）が修了した。受講生の満足度も高く（最終アンケートの受講生の満足度に関するアンケート項目において、五段階評価で最上位の「満足」が93.3パーセント）、本プログラムを締めくくることができた（**写真13**）。2019年12月に来年度の受講生の募集を行う等、来年度の講義・演習の準備を行っている。

本教育プログラムは地域の企業や団体の協力が不可欠な取り組みである。協力いただいているコミュニティ間の連携をさらに強化する新たな試みとして、今年度、連携企業や団体、機関が共有する目的や課題を議論する「ProSec-IT

写真12：大阪大学と連携したCTFの様子

写真13：修了式の様子

写真14：ProSec-IT情報交換会

情報交換会」を2019年7月27日に開催した（**写真14**）。連携企業、情報関係企業、インフラ事業者等から80名以上の参加者が参加し、地域の課題や人材育成、社会インフラである情報システムのサイバー攻撃からの防御に関する活発な議論を行うことができた。

●来年度の計画

今年度は、本プログラムの主たる講義演習会場を本学大橋サテライトから、連携企業QTnetの本社会議室（天神）に移して実施することができた。この講義会場は交通至便でありスペースも十分で会場に関する受講生の満足度も高いため、今後も継続して利用させていただく予定である。また講義・演習内容についても講義アンケートや連携企業、アドバイザリーボード等からのフィードバックを受けて改善を行う予定である。

●募集情報

問い合わせ先：〒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
TEL：092-802-2671
E-mail：prosec-it-staff@cs.kyushu-u.ac.jp
URL：https://cs.kyushu-u.ac.jp/enpit-pro/

2.6 長崎県立大学

●取り組み概要

国際情報学研究科情報メディア学専攻における情報セキュリティ領域の教員により、2018年後期より4科目6か月で修了のメインコース、同じ期間であっても2科目を選択するクイックコースを提供している。受講料の徴収など学内の制度に合わせるため、当該大学院の科目等履修生として募集している。2019年度からは、情報理論や暗号分野などの理論から、プライバシー保護技術やブロックチェイン技術などを含むデータセキュリティ、さらに中小企業向け実践講座、社会科学や人間の心理の観点からの科目など多岐にわたる領域をカバーする科目8名の教員により提供している。**図7**に提供科目を示す。

図7：長崎県立大学 2019年度後期提供科目

科目		単位	開講期間	担当教員名
enPiT科目	大学院授業科目			
SMBセキュリティ対策の理論と実践	情報セキュリティ	2	2019年度後期	C.ソムチャイ
データセキュリティ	信号応用技術	2		松崎なつめ
計算量安全暗号	計算の複雑さ	2		穴田啓晃
情報理論的安全暗号	情報理論とその応用	2		吉田雅一
セキュア開発技術1	人工知能技術	2		山口文彦
セキュア開発技術2	数理科学とその応用	2		松田 健
ネットワークセキュリティ	ネットワークセキュリティ対策技術応用	2		加藤雅彦
情報セキュリティとエコノミクス	情報セキュリティと社会・個人	2		小松文子

本プログラムは、5つの県内企業・組織からなる、長崎県立大学情報セキュリティ学科社会人学びなおしプログラム検討会（以降検討会）によって、内容や運営について検討した。また、受講生が少数であることに対しては、有意義なコースであるが広報活動を積極的に実施すべきという意見があった。このため、後期からは募集用パンフレットを、長崎県情報産業協会（NISA）をはじめとした県内へ送付したり、教員によるコース紹介などを積極的に実施した。

●実施状況

2019年度の前期は、理論が中心だったため、残念ながら受講生希望者はいなかった。後期には、IT企業と医療機関からの受講生を受け入れている。前者は、企業からの派遣、後者は私費での受講である。前述した検討会にて、社会人が学びやすい講座運用について意見があり、特に、近年の働き方改革の影響で企業派遣の場合、夜間や休日の講義を避ける要望を受けている。また、社会人にとって、毎

写真15：「データセキュリティ」外部講師による講義

写真16：サイバー攻撃・防御のハンズオン演習

週の受講は本人と職場にとって負荷が高いことから原則として集中講義にて開講している。例えば、毎月1回を5か月継続する、集中3日間でのハンズアウト演習などである。

提供コースの担当教員は8名であるが、特にハンズアウト演習や最新の研究動向については、学外の研究者・実務家を招いている。**写真15**に「データセキュリティ」の講義において、明治大学教授 菊池浩明教授による講演を示す。受講生だけでなく、受講生の上司なども特別参加し、活発な議論を行った。

他にも、(株) ラックにおいて心理学の観点からセキュリティ行動を研究している鈴木遥氏が講義を提供した。また、2月には（株）パロンゴの技術者の支援により、サイバー攻撃・防御のハンズオン演習を実施した（**写真16**）。

長崎県においては、特に情報セキュリティをビジネスとして提供する企業はほとんどないため、実務的な講義を提供してもらう連携はできないが、情報産業やその他の製造業、また今年の受講生のような医療機関などの情報セキュリティを学びたい潜在的な受講生を期待できると考える。

●来年度の計画

本学は、2020年4月より、大学院が再編され、新たに地方創生研究科情報工学専攻セキュリティコースを開始する予定である。これに伴い、学内制度への位置づけを再度実施する。そして、これをベースに広報活動を積極的に進める。

●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。こうした認識から、2019年度は2つのことを実施している。一つは、インシデントハンドラ実践メインコース／クイックコースの実施のためe-learning教材の充実を図ることである。2018年度の実施において、業務や個人的事情によりやむなく参加を断念するケースがありこれらの問題を解決するためにe-learning教材の充実が不可欠であると判断し、その開発を進めた。もう一つは、より広くセキュリティの知識への理解を高めるため、参加しやすい形式のサイバーセキュリティトライアルコース（基礎）を実施した。

これらの経験から種々のコースを用意し、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た。

●実施状況

今年度はインシデントハンドリングメイン/クイックコースの実施のための準備、広報を進めるとともに、社会人の参加を容易にするためのe-learning教材の充実をはかるとともに、広くセキュリティの知識への理解を高めるため、参加しやすい形式のサイバーセキュリティトライアルコース（基礎）を実施した。以下に詳細を示す。

1. e-learning教材の開発

2018年度は、インシデントハンドリングクイックコースの中で講義として「セキュリティの基礎・対策・対応（12時間）」を用いているが、この実施にあたって4日間の講義への参加を必要としていた。しかしながら、参加者の中で業務や個人的都合で4日間全てに参加が難しかったケースが散見された。こうした経験から講義形式の授業に

写真17：e-learningコンテンツ例

写真18：サイバーセキュリティトライアルコース(基礎)

写真19：インシデント体験演習

関してできるだけe-learningで参加できるよう配慮を進めることとした。そこで今年度は、本講義のうちセキュリティにおける対策、インシデント発生時の対応について学ぶセクションに関するe-learning教材化を行った（**写真17**）。

内容を10分から15分程度に分割し、自分のペースに合わせて受講できるようにするとともに、指導側からは受講の進捗状況、課題提示と提出確認などを行えるようにしている。

2. サイバーセキュリティトライアルコース(基礎)

広くセキュリティの知識への理解を高めるため、講義「セキュリティに関する基礎知識（90分）」と「インシデント体験演習（30分 e-learning型）」を組み合わせたサイバーセキュリティトライアルコース（基礎)を実施した（**写真18**）。

本コースは、1/24（東京)、2/7（大阪）でそれぞれ2回ずつ実施し、全体で82名が修了している。講義ではセキュリティに関する基礎的知識を整理するとともに、対策の立て方と対応方法の方針について整理している。演習では、実際に起こりうるインシデントをWeb上で安全に体験するものとなっており、セキュリティインシデントを体感できるように作られている（**写真19**）。なお演習教材は情報セキュリティ大学院大学で開発したものを活用しており、本コースは慶應義塾大学と情報セキュリティ大学院大学の合同で修了証を発行している。

●来年度の計画

2020年度は、メインコース／クイックコースへの参加をより容易とするためコースを複数のブロックに分割し、個々に参加しながら全体としてコースを修了する仕組みの検討を進める。また、7大学がカバーできていない地域においてコースの実施の要望もあがっていることから、トライアルコースについてさまざまな地域での実施を目指す。

●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
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】

ここでは、産業界から要求されるスキルを、本事業が提供しているかを評価する手段として、NPO日本ネットワークセキュリティ協会（JNSA）が公表するスキルマップに対する充足状況を調査し、今後のカリキュラム提供の参考にすることを目的としている。

1．JNSAのスキルマップ

JNSAは、2019年3月にSecBok2019を公表した(1)。従来はスキル中心に知識を羅列したものであったが、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。SecBok2019の特徴は、新たに定義した16の役割（**図8**）とセキュリティ知識項目が3つのレベルごとに対応づけられていることである。

これらの16の役割に対して，知識のレベルを4レベル（L、M、H、P）（**図9**）役割ごとに要求されるスキルの種類（前提、必須、参考）を規定している（**図10**）。

(1) https://www.jnsa.org/result/2018/skillmap/

2．コース充足の状況

新たなJNSA SecBok2019に対して各大学機関が提供するコースがどの程度充足しているかを調査した（**図11**）。

本調査は、全大学機関を調査したものではなく、SecBok

図8：JNSA SecBokにおける16の役割のその定義

	役割（ロール）	役割定義（ユーザ企業におけるおもな役割）
1	CISO （最高情報セキュリティ責任者）	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。
2	POC（Point of Contact）	社外向けではJPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口、社内向けではIT部門調整担当社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、それぞれ情報連携を行う。
3	ノーティフィケーション	組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合にはIT部門と調整を行う。
4	コマンダー	自社で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。
	トリアージ	事象に対する対応における優先順位を決定する。
5	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。
	インシデントハンドラー	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。
6	キュレーター	リサーチャーの収集した情報を分析し、その情報を自社に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）とすることが多い。
7	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。収集のみで分析はしない。
8	セルフアセスメント	自社の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。
	ソリューションアナリスト	平常時にはリスクアセスメントを行う。インシデント対応時には脆弱性の分析、影響の調査等に対応する。
9	脆弱性診断士	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。
10	教育・啓発	社内のリテラシーの向上、底上げのための教育及び啓発活動を行う。
11	フォレンジックエンジニア	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。
12	インベスティゲーター	外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。
13	リーガルアドバイザー	システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する橋渡しを行う。
14	IT企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。
15	ITシステム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。
16	情報セキュリティ監査人	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。

図9：知識のレベル

L	低	（概ね経験3年未満でも対応可能）
M	中	（経験3年以上または関連する演習・トレーニング受講者なら対応可能）
H	高	（経験10年以上または高度な研修受講を前提とする専門実務経験者または「突出した人材」なら対応可能）
P	ペンディング	（情報収集・インテリジェンスに関するもの。今回はレベル付けの対象外）

図10：要求されるスキルの種類

1	前提スキル	（職務遂行の前提として有しておくべき知識・スキル）
2	必須スキル	（職務遂行の実施に際して必要となる知識・スキル）
3	参考スキル	（職務遂行に際して必須ではないが、あると望ましい知識・スキル）

図11：コース充足の状況

役割（ロール）	ProSecコース	充足度（ロールに要求されている知識・スキルのレベルに対する提供状況）
CISO（最高情報セキュリティ責任者）	情セ大：企業経営向けビッグデータ分析とリスク経営	58%
POC（Point of Contact）	情セ大：CSIRT運営管理者向け	68%
ノーティフィケーション	情セ大：CSIRT運営管理者向け	75%
コマンダー、トリアージ	情セ大：CSIRT運営管理者向け	85%
インシデントマネージャー、インシデントハンドラ	情セ大：CSIRT運営管理者向け	91%
トリアージ、コマンダー	和歌山大：インシデントレスポンス実践	66%
インシデントマネージャー、インシデントハンドラ	和歌山大：インシデントレスポンス実践	69%
キュレーター	和歌山大：インシデントレスポンス実践	77%
リサーチャー	和歌山大：インシデントレスポンス実践	76%
セルフアセスメント		
ソリューションアナリスト		
脆弱性診断士		
教育・啓発		
フォレンジックエンジニア		
インベスティゲーター		
リーガルアドバイザー		
IT企画部門		
ITシステム部門	情セ大：IoTセキュリティ	69%
情報セキュリティ監査人		
16すべての役割に対して	九州大：ProSec-IT	38% （全726項目中278項目）

との対応が可能かどうかの予備調査にあたる。

3．課題と今後の方針

各役割と大学機関のコースが提供する役割スキル充足度をみると、十分な数値ではないと考えられる。ひとつの理由としては、SecBokの定義時に、産業界でこれまで定義されていなかったサイバーセキュリティに関連する「インシデントレスポンス」に重点をおいた知識・スキル群であるからと考える。そのため、インシデントレスポンスに関連した項目の粒度が高いということがいえる。情報セキュリティ分野の知識スキルは、現状のSecBok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想定しつつ、活用可能な部分については提供コースに反映していくことが望ましい。

【コース連携】

コース連携サブWGでは、各大学でのコース連携の実現に向けた検討を行っている。

2017年度のサブWG活動において、ProSecが学部や大学院における正規課程科目としての開講とは異なることから、学部や大学院における単位互換等の制度を利用して各大学が開講するプログラムを横断的に受講することが難しいことが確認された。また、正規課程科目外の科目としての実施または継続のために必要とされる体制・制度が、大学によって異なっていることもわかった。

その後、2018年度から本格的に各大学がプログラム提供を開始し、各企業・機関との意見交換やプログラムの実施に際しての各大学への社会人からの問い合わせ等から、時間の制約のある社会人が、半年や1年という期間に120時間のプログラムに参加することは難しいという声が多いこと、社会人の仕事とProSecの学修との両立を図るための多様な受講方法を望む声があること、クイックコースよりも短いコースへの希望も存在することが確認された。

このため、コース連携にあたっては高等教育機関である大学が実施する教育プログラムとしての体系性を維持しつつも、受講者の利便性とProSecコース受講者数の拡大を図るための新たなスキームの検討を開始した。

具体的には、クイックコースよりもさらに短いコース（サイバーセキュリティトライアルコース）の試行的実施を行ったほか、興味のある講座をピンポイントで受講できるような仕組み、また、複数大学及び複数年にわたる受講履歴の加算によるProSec修了認定証を発行可能とするコース開講の可能性について検討している。

またアドバイザリーボードにおいても、コース連携についての意見をいただいている。アドバイザリーボードで指摘されたのは、次のような課題である。

- 社会人の実情を踏まえたプログラムの提供を行うこと。特に短期間で集中して学修するニーズがきわめて高いことから、それに対応するべきである。
- 実践的な内容を主眼としつつも、企業や民間団体が提供する研修コースとは異なる大学院レベルの体系的な内容・水準を維持すること。特に体系性を維持することが重要である。
- 他の地域で開講されているコースも受講できる枠組みを検討すること。
- 地域の実情や、地域企業のニーズに即したコースを提供すること。

このようなご指摘をうけて、短期間で集中して学修するニーズに応えること、他の地域で開講されているコースも受講できる枠組みを構築することについて、引き続き検討を進めることとしている。

■ 産学連携WG

ProSecの各コースの実施にあたって、すべての拠点が多くの企業・組織と連携している。その概要を図12に示す。産学連携は、(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・個別企業等との連携の2層から構成されるが、各拠点におけるコースの検討や実施にあたっては、地域の企業団体や企業と緊密に連携しながら行った。具体的には、講師の派遣、演習の実施支援、演習プログラムの開発等を行っている。また、参加者募集に関する広報にも連携先の企業・組織からの協力を頂いている。

来年度は、当初カバーできていなかった地域の人材育成に関する事情や実情を踏まえた上で、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。また、来年度以降のより有機的なProSecコースの展開において、複数拠点の連携等に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・および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

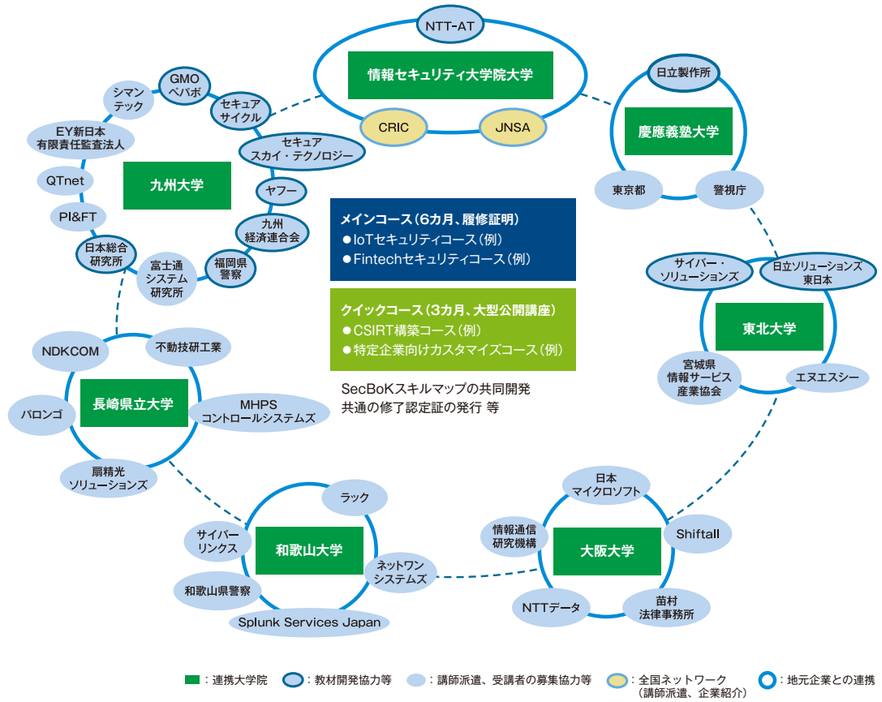

図12：各拠点と連携組織

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。2019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. 演習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

- 内容のレベル演習内容が自分に合っているか
- 教員の解説の仕方話し方、態度、教材、質問への対応、工夫など
- 全般的な有益性、面白さ等を考慮した総合評価
- コメント（自由回答）

3. 東北大学でのアンケート

3-1. ProSec受講者に対する質問

- 現場向けノウハウが含まれていましたか？
- 学んだ知識や技術は、業務に利用可能ですか？
- 今後取り上げて欲しいテーマ、課題、内容
- 講義・演習を実施する時間、場所等に関して
- コメント（自由回答）

4. 大阪大学でのアンケート

4-1. 事前アンケート(年度初め)

- 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）／講義室(中之島キャンパス)／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、ポリコムは利用可能ですか？

4-2. 事前アンケート（講義毎）

- 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。

4-3. PBL／講義アンケート（毎回講義・演習ごと）

- 講義でもっとも勉強になった内容に関して
- 講義の内容ですでに知っていた内容に関して
- 講義の内容で追加説明が必要な内容に関して

5. 和歌山大学でのアンケート

- 難易度
- わかりやすさ
- 現場向けノウハウ
- 業務への利用
- シラバスとの合致
- 知識習得、技術力向上の動機
- 満足度
- コメント（自由回答）

6. 九州大学でのアンケート

6-1. 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
- 説明が分かりにくかった部分はありますか
- 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

6-2. ProSec-IT全体の講義アンケート

- 講義全体の難易度
- 講義全体のわかりやすさ
- 現場向けノウハウについて含まれていたか
- その他（記述式）
- 講義全体におけるシラバスとの合致
- 講義全体において知識習得，技術力向上の動機
- 講義全体における満足度
- コメント（自由回答）

7. 慶應義塾大学でのアンケート

7-1. クイックコースアンケート

1. 問題点・改善点に関して
2. 取り上げて欲しいテーマ、課題、内容について
3. 場所、時間等に関して
4. その他ご自由にお書きください。

7-2. 講義アンケート

1. テキスト・スライド等の意見・改善点に関して
2. 取り上げて欲しい話題に関して
3. 場所、時間等に関して
4. e-learningに関して

8. 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

FDWGの目的は、各拠点における取り組み状況を視察することや広く一般の方へ紹介することでフィードバックやコメントを得ることにより教育の方法や質を向上することである。これまでのenPiT第1期やenPiT第2期の事業に比べて各拠点独立でコース設計、コース実施をしており、それらの知見を共有することが重要である。

講演などにより得られたフィードバックやコメントは運営委員会で全体へ共有している。また、運営委員会の開催を演習の開催日と合わせることで他拠点の演習視察を行いやすくする工夫をしている。今年度の活動実績を図13に示す。

■ 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サイトでの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サイトを活用して、コンテンツ更新、情報発信を行った。またシンポジウム対応のためのポスター制作、パンフレット作成、ProSecのTwitterアカウントのWebサイトへの組み込みなど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

図13：2019年度FD活動実績

実施日	実施内容	視察人数
2019年　5月　8日	宮城県警察本部にて『大学連携による実践的セキュリティ人材育成』の講演	―
5月13日	福岡県警察本部にて福岡県警察の人材育成におけるProSecの活用方法について意見交換	―
5月16日	ITRCにおいて『大学連携による実践的セキュリティ人材育成の紹介』の講演	―
5月16日	サイバーセキュリティ福岡スクラム令和元年で講演	―
5月21日	警視庁・東京都の会合で意見交換	―
5月29日	個人情報保護セミナーにおいて『実践的セキュリティ人材育成コースの紹介』の講演	―
7月14日	学都『仙台・宮城』サイエンス・デイ2019でProSecの紹介	―
8月　5日	人材育成ラウンドテーブルにおいてProSecの活動紹介と意見交換	―
8月22日	2019年度電気関係学会東北支部連合大会でProSecの紹介	―
10月26日	高度サイバーセキュリティPBLⅢ（高度セキュアネットワーク設計演習）の視察	1名
10月30日	セキュアシステム技術演習（基礎）クイックコースの視察	9名
11月29日	インシデントレスポンス実践クイックコース演習の視察	2名
12月13日	AXIES2019にてProSec紹介及び社会人エンジニアの学びなおしに関する議論	11名
2020年　1月17日	東北大学地域連携イノベーション展においてProSecの紹介	―
1月23日	enPiT第8回シンポジウムにてenPiT2の取り組みに関する発表視察	9名

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