【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 2020

2020 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

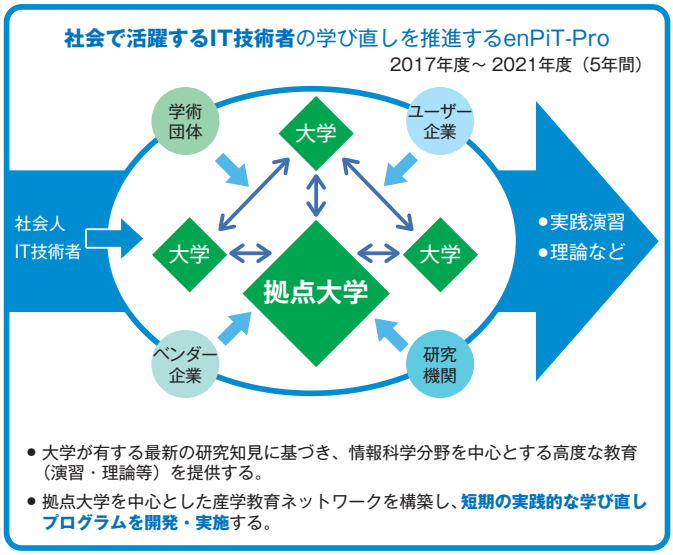

図 1：enPiT-Pro 事業全体イメージ

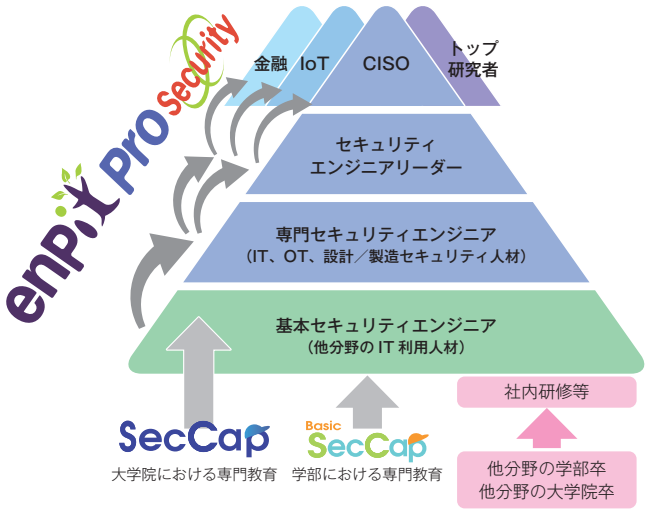

図 2：セキュリティ人材育成における ProSec の位置づけ

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250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。2020年度は、JNSAが2019年度に公表したSecBoK2019に対する充足を配慮しつつ、提供コースの検討を行い、実際に提供コースの改善や新規提供を実施した。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、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。

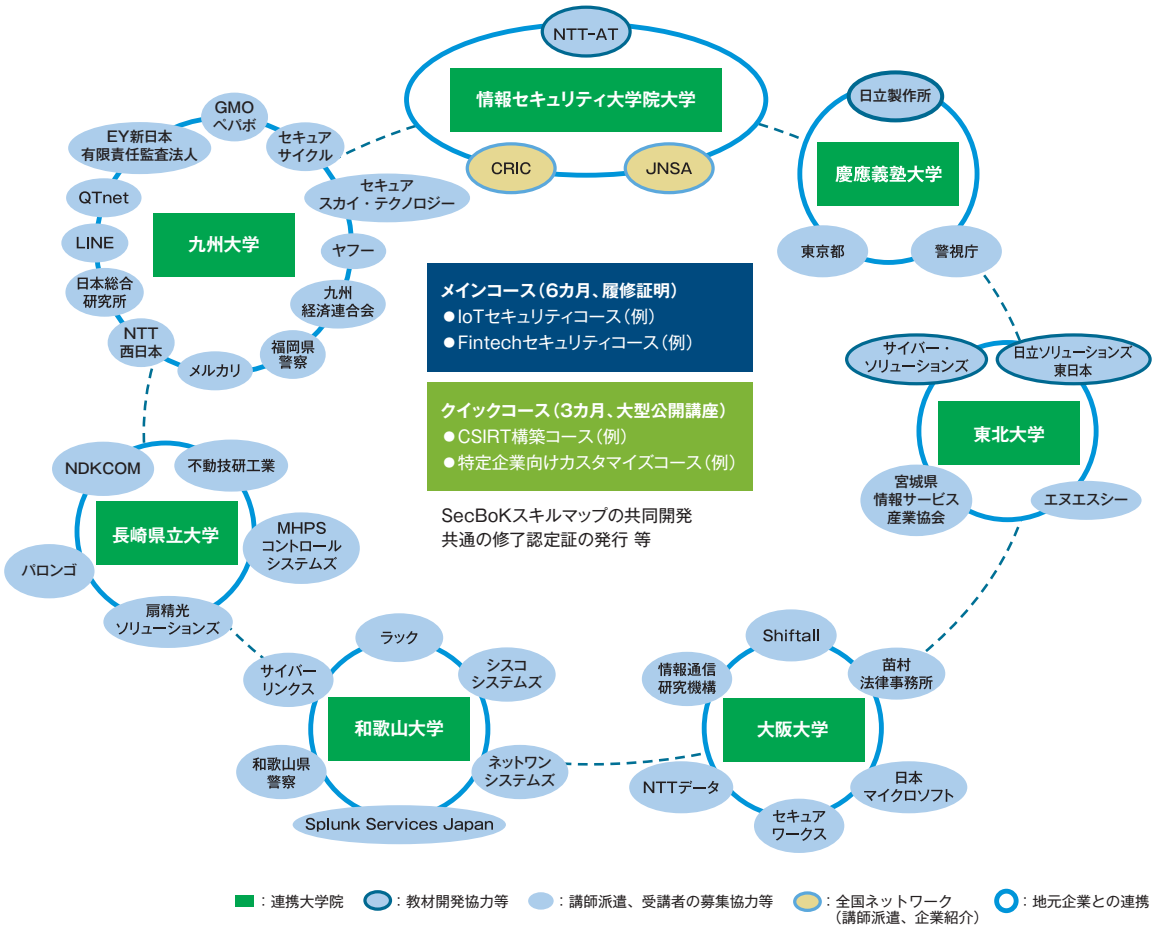

図 3：教育プログラムのフレームワーク

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。

▶ 2020 年度の実施状況

2020年度は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
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

2020年度はアドバイザリーボードを11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およびメンバーは図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。2020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、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。

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。

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		加藤＊（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

2020年度は、2021年3月18日に、2017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『AI&IoT時代の社会人育成』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。3月30日には各拠点と文部科学省との意見交換会をオンラインで実施する予定である。

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、2020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、2020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。

・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 —

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8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

写真１：セキュアシステム技術（基礎）クイックコースの様子

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（**写真1**）。

●DX推進者対象DX with Cybersecurity
3日間教育コース

クイックコースよりもさらに短時間で学びたいという声があることを受けて、今年度は3日間で学ぶ特別コースの施行を試みた。

DX推進者対象DX with Cybersecurity 3日間教育コースは、ITやセキュリティのバックグラウンドがないビジネスパーソンが、サイバーセキュリティに係る必要な知識や動向等を習得できるカリキュラムとして提供したものである。政府のサイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会では、7月より「DXに必要なプラス・セキュリティ知識を補充できる環境・人材育成」を政策課題に掲げ、検討を進めており、その政策動向と連携して「3日間特別教育コース」として開発した。

11月18日～20日の3日間ですべてZoomを利用したオンラインによって実施した。

●情報セキュリティ大学院大学2020オンラインセミナー
「ポストCOVID-19時代のサイバーセキュリティ脅威・対策・人財育成を考える」

ProSecの取り組みについて広報すると同時に、その成果を広く情報発信するため、オンラインパネルディスカッション形式で実施した。

●来年度の計画

来年度も今年度と同様のスケジュールで実施する予定であるが、COVID-19対策としてオンラインと対面形式を効果的に組み合わせて実施していく。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及びクイックコースよりもさらに短時間で学ぶコースの開設を検討する。また、連携大学間のコース連携を進め、受講生の利便性とコース受講者数の拡大を目指す。

●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
URL：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、2020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。

今年度は、COVID-19への対応として、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、対面授業に相当する教育効果を担保するため、連携大学や連携企業と意見交換を行い、同時双方向型のオンライン授業やオンラインでの演習環境の整備、Slack等のコミュニケーションツールの活用により、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。

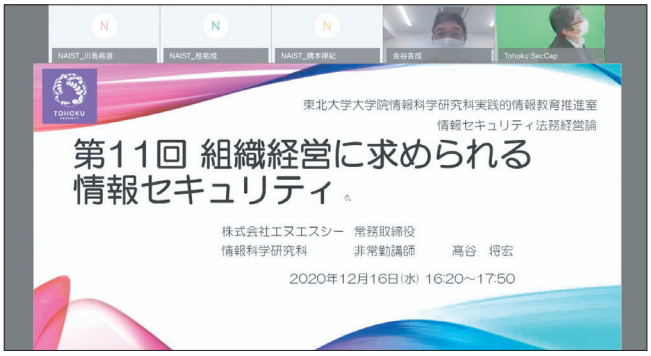

写真 2：同時双方向型のオンライン授業

●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、同時双方向型のオンライン授業で行った（**写真2**）。

演習科目であるネットワークセキュリティ実践では、クラウド上に受講者が個別に操作することができる仮想専用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。

また、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1名が受講した。今年度はコロナ禍の中、受講者の募集に苦慮したが、受講者からは、オンライン中心のため社会人として受講しやすいといった意見をいただいた。

●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。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。さまざま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 PBL Ⅰ、Ⅱ、Ⅲ
- 高度サイバーセキュリティ PBL Ⅰ、Ⅱ、Ⅲ

さらに、2021年度には「安全なデータ設計特論」を新たに開講する。

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、セキュアワークスおよび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

2020年度前期受講生：23名
2020年度後期受講生：22名

本年度はCOVID-19に影響を受けることなく、講義はオンラインと対面参加のハイブリッド、演習はオンライン、あるいはオンラインと対面参加のハイブリッドで実施した。今年度から、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、

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	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	必修	必修	必修	必修		必修	選必 D	選必 D
離散数学と計算の理論	選必 A	必修	選必 A		必修		選必 A	
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		選必 A	
高度セキュリティ PBL Ⅰ	選必 B	選必 B		必修	選必 B		選必 E	選必 F
高度セキュリティ PBL Ⅱ	選必 B	選必 B			選必 B		選必 E	選必 F
高度セキュリティ PBL Ⅲ	必修	選必 B	必修	必修			選必 E	選必 F
高度サイバーセキュリティ PBL Ⅰ	選必 C		必修	必修		必修	選必 E	選必 F
高度サイバーセキュリティ PBL Ⅱ	選必 C		必修			必修	選必 E	選必 F
高度サイバーセキュリティ PBL Ⅲ	選必 C		必修			必修	選必 E	選必 F

※【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）　※【選必D】講義科目から選択（1単位以上）　※【選必E】PBL科目から選択（3単位以上）　※【選必F】PBL科目から選択（4単位以上）

写真 3：PBL 演習の対面参加の様子

写真 4：オンラインで繋がる受講生

写真 5：コース認定授与式

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**）とオンラインで繋がる受講生（**写真4**）、また、演習日に実施したコース認定授与式を表す（**写真5**）。

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：8名、最新セキュリティ特論Ⅰ：11名、最新セキュリティ特論Ⅱ：8名、実践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 Ⅰ：8名、高度セキュリティ PBL Ⅱ：5名、高度セキュリティ PBL Ⅲ：11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：12名、高度サイバーセキュリティ PBL Ⅲ：7名

3. 受講者の講義への意見

- IoTについて講義形式で話を聴くことは多かったものの、実際にIoT製品を開発されている方からのお話を伺うことはなく、非常に良い経験となった。
- 定義したことのみを極力用いて証明を行う進め方は非常にわかりやすく、自らも身につけたいと感じた。
- ビットコインの仕組みについて理解することができた。
- 暗号資産がどのようなものであるか、非常に興味深く勉強になった。

●来年度の計画

新規科目「安全なデータ設計特論」（1単位）を開講する。本講義は産官学で活躍されるセキュリティ人材のセミナーおよびコース受講で習得した知識を用いて、セキュリティを社会に応用するシステム設計手法について学習する。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、2020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（2020年8～9月）
- 遠隔ハンズオン（2020年11月～2020年12月）
- 合同ハンズオン（オンライン2020年11月24日、25日）（現地2020年11月26日、27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4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（**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、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

写真 6：合同ハンズオンの様子

に、指定したSlackのチャンネルにWebhook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

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。2020年度はその3年目の受講生の受け入れになる。図6にこの3年間の受講生受け入れ人数を示す。

各コースの具体的な講義･演習内容を図7に示す。講義概要は昨年度まで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更新している。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。サイバーセキュリティの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、LINE、NTT西日本、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演習を中心とした内容としている。ProSec-ITに協力いただいている特別講師は主にこれらの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。

図 6：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	
	社会人	院生	社会人	院生
2020	17	8	0	0
2019	16	4	2	0
2018	10	0	7	2

図 7：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

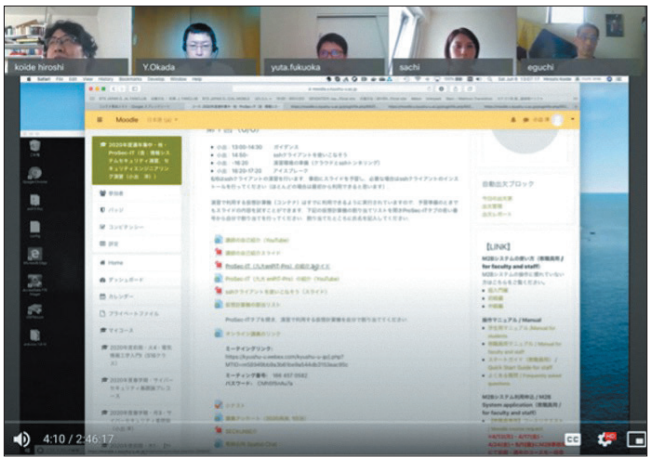

写真 7：初回講義・演習・ガイダンスの様子（2020/6/6）

●実施状況

本教育プログラムにおいてもCOVID-19のパンデミックの世界的な影響を受け、またそれに関連する受講生からの要望もあり、講義・演習のオンライン化を行った上で実施した。講義・演習のオンライン化の十分な検討と準備のため開講を二ヶ月遅らせ、初回講義を6月6日に実施した。初回の講義においては、ガイダンスとsshクライアントや仮想計算機に関する演習を実施した（写真7）。

6月13日には「サイバーセキュリティ業界の動向」について俯瞰する内容の講義を行った。次の6月20日にはWebアプリケーションのセキュアプログラミング、サイバーセ

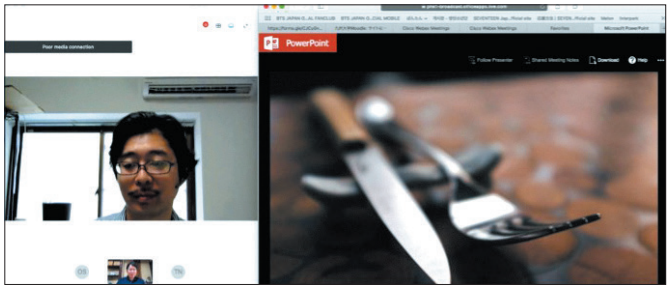

写真 8：「弁護士による情報法規・情報倫理」の様子（2020/7/4）

写真 9：「マイクロアーキテクチャ攻撃」の様子（2020/7/11）

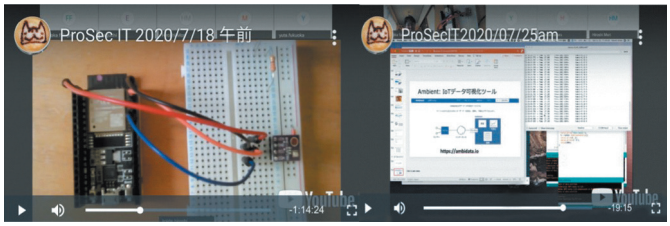

写真 10：「IoT セキュリティ演習」の様子（2020/7/25）

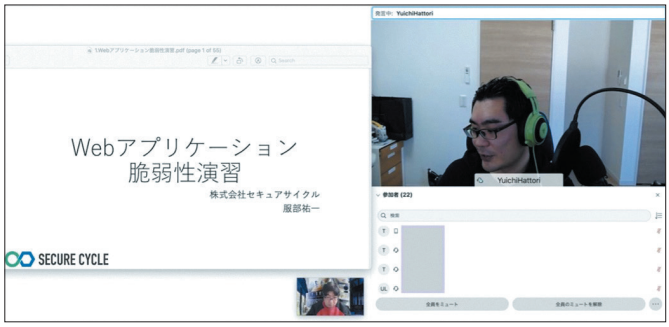

写真 12：Web アプリケーションの脆弱性を見つける簡易診断スクリプトの作成演習の様子（2020/12/5）

写真 11：CTF を使った実践的なセキュリティのゲーミフィケーションのハイブリッド演習・講義の様子（2020/11/21）

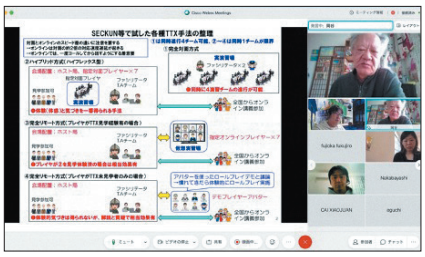

写真 13：サイバーインシデント対応のための机上演習（2021/1/16）

キュリティに関連する技術以外の要素について（文系サイバーセキュリティ）、7月4日には、現役弁護士による情報関係法規・情報倫理に関する講義を行った（**写真8**）。

7月11日および7月18日には、SpectreやMeltdown等で有名なCPUに対する攻撃である「マイクロアーキテクチャ攻撃」に関する講義・演習を行った（**写真9**）。さらに加えて、上記4回の講義において、セッション管理、各種のインジェクション、クロスサイトスクリプト、クロスサイトリクエスト強制等のWebアプリケーションのセキュリティについての演習も実施している。

7月18日、7月25日にはDockerコンテナに関する入門的な演習、ESP32によるIoTセキュリティ演習を実施している。これは実際の電子デバイスを利用するため本来はオンラインでの講義・演習が難しいものであるが、必要な電子デバイスを郵送したり、手元を撮影するWebカメラを用意したり、いろいろな角度からの写真を用意する等の工夫で実現した（**写真10**）。7月25日には加えてWebセキュリティに関する講義を行っている。

8月22日、23日、29日には、サイバーレンジを用いたオンライン演習を行った。また、9月26日、27日、10月3日には、セキュリティエンジニアリング演習としてセキュリティ by デザインに関する演習を行った。10月17日には広告サービスと情報セキュリティに関する講義。10月24日には、ARM64によるアセンブラ演習および個人情報とプライバシーに関する講義を行っている。さらに10月31日にはフォレンジクス演習、11月7日にはコンテナとそれに関するセキュリティ的な話題についての講義・演習を行っている。11月14日にはプライバシー保護に関する講義、11月21日はサイバーセキュリティ法制とイノベーション、CTFを使った実践的なセキュリティのゲーミフィケーションについてのハイブリッド講義・演習を実施した（**写真11**）。

12月5日には、Webアプリケーションの脆弱性を見つける簡易診断スクリプトの作成および脆弱性の修正演習を行った（**写真12**）。

年が明けて1月9日には、SNSにおけるフィルターバブルやマイクロターゲット広告等の課題を扱ったデジタル社会の深読みに関する講義を行った。さらに1月16日には、サイバーインシデント対応のための机上演習を行った（**写真13**）。

写真 14：
最終成果報告会を兼ねたオンラインシンポジウム（2021/2/21）

さらに1月23日および24日には、昨年度、一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。

また最後に今年度は2月21日に修了式を兼ねたオンラインシンポジウムを開催した (**写真14**)。

●来年度の計画

今年度は、COVID-19のパンデミックの世界的な影響への対応から、オンラインでの講義・演習 (一部ハイブリッド講義) への展開を行った。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委員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
TEL：092-802-2671
E-mail：https://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

長崎県立大学では、2020年度のProSecの取り組みとして、技術者・開発者などを対象に情報セキュリティに関連した学び直しを支援する以下の内容を企画した。

- メインコース・ハーフコースの授業提供
- 情報セキュリティ講演会 (2021年3月7日)
- サイバー攻撃対応トレーニング (2021年3月8日)

授業提供では、本学が本年度から導入したクォータ制に合わせ、第3・第4クォータにおいて、セキュリティ技術者・開発者向けに、セキュア開発技術・ネットワークセキュリティ・情報セキュリティとエコノミクス・データベース・量子情報処理の5科目を提供した。このうち5科目すべて (120時間) を修得するメインコースと、3科目 (72時間) を修得するハーフコースを設定し、受講生を募集した。これらは大学院に新設された情報工学専攻の正規科目として開講する科目を社会人に開放して行うコースである。

情報セキュリティ講演会は、サイバー空間の新たな脅威への対策をテーマに、企業の研究所などで活躍されている2名の方にご講演をいただくものであり、技術者だけでなく企業経営者などの一般の方々を対象としている。講演内容のうち一つは、量子暗号を中心とする暗号・認証技術の最新の研究動向に関するもので、研究開発の現場で量子計算機に対してどのような対策が考えられているのかを解説する。もう一つは、IoTの普及が進む中での制御セキュリティに関するもので、サイバー空間と現実空間の融合が進む中での安全・安心の確保に必要な制御セキュリティについて事例を踏まえながら紹介する。

サイバー攻撃対応トレーニングは、情報系の技術者を対象とする講習会である。COVID-19対策としてオンラインでの講習が可能な内容を選択した。サイバー攻撃対応を繰り返し経験する訓練を行うという内容で、同じ攻撃が繰り返されることで毎回少しずつ攻撃の状況を観測し、対処する方法を試すことができる。このような訓練によって、個々の技術者のインシデント対応能力の向上を図るものである。

●実施状況

今年度はCOVID-19感染拡大防止対策として、一部の授業がオンラインならびにオンデマンドでの実施となった。各コースの内容をまとめた広報用の資料を作成し、地元地域の企業を中心に受講生の募集を行ったものの、コロナ禍のなか受講生の募集に苦慮し、残念ながらメインコース・ハーフコースとも社会人の受講は無かった (ハーフコース相当の履修をした大学院学生は5名)。

情報セキュリティ講演会およびサイバー攻撃対応トレーニングを広報するための資料を作成し (**写真15**)、地元企業を中心に配布した。情報セキュリティ講演会は、コロナ対策のために人数を制限して開催し、会場へは22名の参加があった (**写真16**)。

サイバー攻撃対応トレーニング (**写真17**) には、定員を充足する8名の参加者があり、運営委員会後に視察も行った。

●来年度の計画

受講者の利便性と事業の継続を鑑みて、コース内容の改

写真 15：講演会および講習会の広報資料

写真 16：情報セキュリティ講演会の様子

写真 17：サイバー攻撃対応トレーニングの様子

善と拡充を図る。

本学が長崎市内から少し離れて立地していることなどから、以前より来学しての受講には時間的な負担が大きいとの指摘があった。オンライン講義の整備が進むことで改善される点もあると思われるが、セキュリティの特性上、オンラインでの演習が難しいこともある。そこで、科目履修の時間に受講者が選択できる自由度を持たせることを計画している。具体的には、通年で6科目を提供し、すべて履修するメインコースと、これらのうち3科目を履修するハーフコースを設置することを検討中である。本学では社会人の学び直しを支援する目的で、大学院の科目を昼開講だけでなく、夜の時間帯や集中講義などの形態で2回開講する取り組みをしている。こうした取り組みについても合わせて広報していくことで、社会人の受講生の確保につながるものと考えている。

また今年度から情報工学専攻が開講しており、enPiTで提供する科目がすべて同専攻で正規に開講されているものとなった。enPiTでの受講を科目等履修として整理することで、手続きや処理の負荷を軽減することを検討している。

●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 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。一方、2020年度はCOVID-19が大きく人財育成の環境も変えた。このような環境下において2020年度は講義と演習のオンライン化を図った。

まず演習についてであるが、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）をオンラインで実施できるよう開発を進めた。また、講義についても2019年度に開発したe-learning教材の充実を用いて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ている。また、これらを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。

このように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た。

●実施状況

今年度はCOVID-19禍においても広く多くの人に受講してもらえるようさまざまな工夫を行った。

以下に詳細を示す。

1. フルオンライン版演習

コースのコアであるインシデントハンドリング演習についてフルオンライン化を図った。同一組織内でもサービス部門とIT部門やOT部門やIT部門など、それぞれ異なる目的をもって活動している部門が存在する。インシデント対応時にはこうした複数の部門が連携してインシデント対応に当たる際の手順について学ぶことを目的とした演習が、インシデントハンドリング演習である。従来から、部門間のコミュニケーションは実際の状況を想定して電話やチャットなどを用いて演習を行っていたが、フルオンライン化することで部署内のコミュニケーションもTV会議ツールなどを通して行うこととなる。これは、オンライン

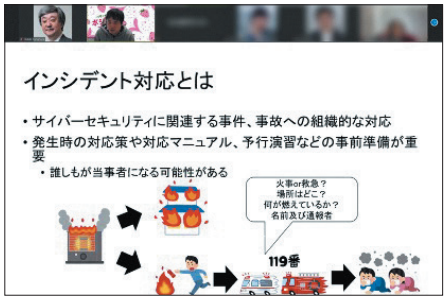

写真 18：フルオンライン版インシデントハンドリング演習

業務などにおいて現在発生している状況であるが、こうした中でインシデント対応を進めることについても学んで行くことが求められる。また、演習の進行にあたって時間管理などをする仕組みが必要となってくる。2020年度は、こうした演習教材の開発に努め9/17と2/9の2回で計18名の受講者が演習の受講を認定されている。

2020年度は、試行錯誤の部分も多く受講者からの意見も収集しつつ改善に努めた。特にTV会議ツールについては会社によって利用を禁止されているものもあり受講環境の整備にも課題があることが明らかになった。一方で、オンラインコミュニケーションツールに関するノウハウを収集し、より円滑の演習の実施のためのマニュアルの整備も行った。また、演習での経験から、本演習はグループにおいてリーダーシップを取るレベルの人財育成、ファシリテータとして演習を運営しているレベルの人財育成、本演習で利用する教材開発をするレベルの人財育成と複数のレベルの人財育成を実施していくエコシステムの確立にも活用可能であることがわかった。こうしたエコシステムを確立することで、さまざまなクラスのセキュリティ人財育成を図っていくことができることが明らかとなった。

2. e-learning system による講義の実施

今年度は、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。具体的には「セキュリティの基礎・対策・対応（15時間）」について実施している。また、修了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。

●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】

教育プログラムにおいて、受講者が修得できる能力を確認すること、提供される科目群の内容的な偏りを知る、もしくは偏りがないことを評価することが、スキルマップの役割である。また、情報技術などの移り変わりの激しい分野においては、受講者や業界の要請に応じて、適宜スキルマップを更新していく必要がある。一方で技術や知識を積み重ねた上で学習すべき内容については、基礎となる内容を教授できていることの確認もスキルマップの役割となると考えられる。

本年度の活動として、近年の国内外の情報セキュリティに関わるスキル標準などの動向を調査した。調査対象として、情報処理学会のJ17-CyS-report R3、米国のNICE Workforce Framework for Cybersecurity R1（SP800-181）、英国のCyber Security Body of Knowledge（CyBOK）、JNSAのSecBoK2019およびSecBoK2017が挙げられる。

この中で、NICEおよびSecBoKは、セキュリティ人材の

役割を分類し、役割ごとに必要とされる知識・能力に関する共通用語と、それら分類法を提供している。SecBoKではNICEによる役割との対応も示している。役割を明確にしていることは、受講者の視点から修得できる能力の確認を容易にするものと考えられる。一方で、委員の中からは、SecBoK2019がインシデント対応に偏った内容になっているとの指摘もあった。また、限られた時間内で提供される科目内容を、細かすぎる分類のスキルマップで評価することは困難であるため、スキルマップの策定においては、技術や知識の分類の粒度の設定も課題となる。

来年度は、主にSecBoKを参考として、カバーする範囲を広げ、大学院での授業内容を反映できる程度に粗粒度なスキルマップを作成する。合わせてProSecが提供する科目群の評価を行う予定である。

【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。

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た。

このような経緯を踏まえ、今年度は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た。

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。このため、今年度は複数大学およ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である「インターメインコース」を開講することとし、その準備を進めた。

ただし、実際には今年度のインターメインコースの開講は困難であった。これは、COVID-19対策として、各大学ともに春の緊急事態宣言下では学内の教職員や学生もキャンパスへの入構を禁止・制限され、他大学の学生等を受け入れられるような状況にはなかったことによる。その後も、学外からのゲスト講師も含め、学外者の入構の制限という大きな壁に直面した。

またオンラインによるコースの連携については、オンラインで利用する会議システムやLMS (Learning Management System) のライセンスの制限により他大学の学生に利用させることができないケースや、企業に所属する社会人学生の場合は勤務先のセキュリティポリシーにより特定の会議システムやオンライン上のツールの使用が禁止されている場合がある等の問題があることもわかった。

ただし将来的にインターメインコースとなりうる短時間の特別コースをオンライン形式で開講することができた。

来年度は、さまざまな問題点を踏まえながら、オンラインも含めた連携大学でのコース連携の実現性を検討し、可能なものから実践する計画である。

■ 産学連携 WG

2020年度は、COVID-19の影響で制限された中でのコース実施のための工夫を凝らしてきたため、拠点間の連携等については課題を残したが、オンライン化を進めたことにより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。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。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 (**図8**)。

■ 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

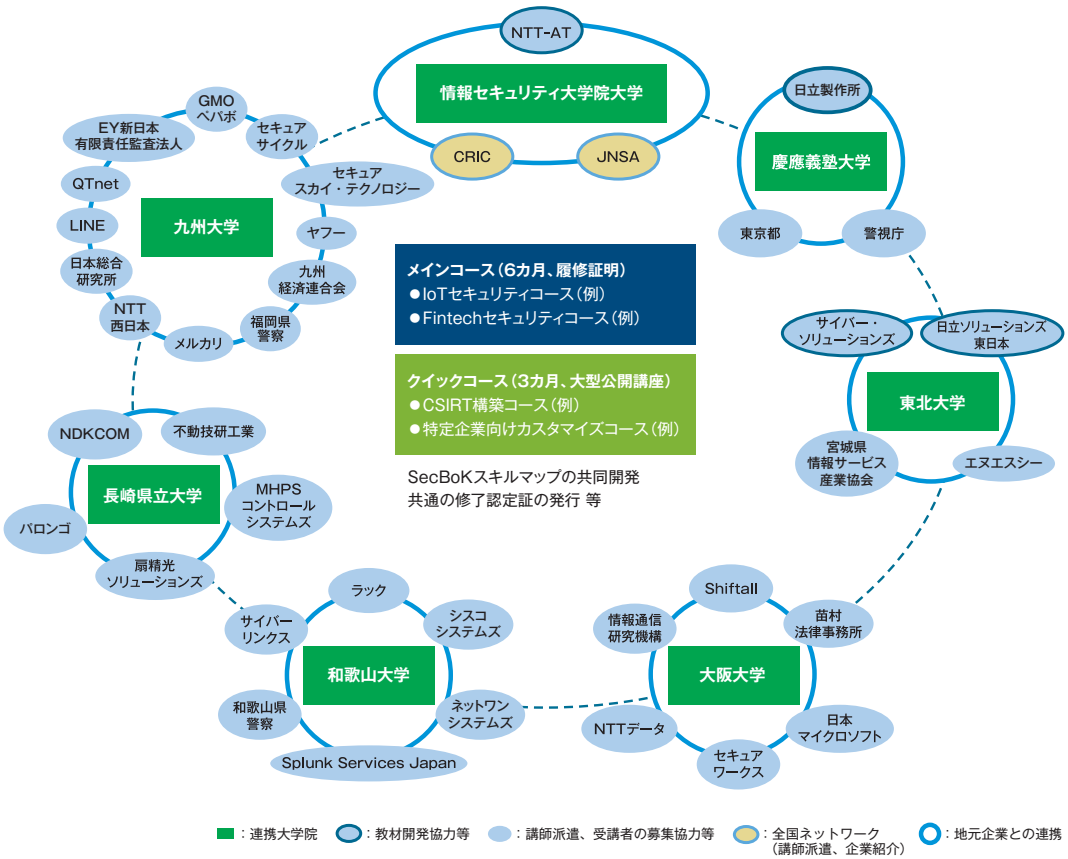

図 8：各拠点と連携組織

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。2020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（難5～1易）
- 教員の講義の仕方（良5～1悪）
- この講義の総合評価
- 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さらには次の講義の設計指針のための講義アンケート、最後に全講義に対する理解度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）／
  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

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

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
2. 講義について教えてください。
   (講義担当者別に実施, 5段階評価)
   2-1. 講義の内容の難しさについて教えてください。
   2-2. 講義中の演習課題の難しさについて教えてください。
3. 講義個別の内容について
   3-1. 講義でもっとも勉強になった内容を教えてください。
   3-2. 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。
   3-3. 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. 講義全体の内容に関するご意見をお願いします。
5. 講義の感想は今後講義を受講する際のよい目安になります。このため、感想の一部はHPや講義パンフレットに利用させて頂きます。利用時は上記１の職業＋姓の頭文字で掲載させて頂きます。利用を望まない場合は記載お願いします。
6. その他、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段階評価で実施する。

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

5. 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
- 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. 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、COVID-19の影響による講義、演習のオンライン化を行うために活用するツールや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。

主な共有内容

主な共有内容としては、

1. Zoom、Webex等のコミュニケーションツール、Slack、Discord等のチャットツールのアップデートやノウハウ、ツールの効率的かつ有効な利用方法
2. 演習環境を構築するためのクラウド環境やオンプレミス環境のノウハウや構築例の展開、また演習を実施するためのネットワーク環境
3. マイク、カメラ、オーディオインターフェース等の配信機材のノウハウ、提供する講義のクオリティ担保のための機材の組み合わせや利用方法
4. 1. 2. 3を活用して実施した講義および演習で実際に得られた知見

の４つが挙げられる。

これらの知見はProSecだけで得られたものではなく、コロナ禍における各大学全体での取り組みやSNS等で情報発信されているノウハウについても積極的に取り入れることでいち早く、数多くのオンライン対応への知見を蓄積し、講義および演習に反映することで高品質なオンライン講義、演習を実現することを目的とした。

得られた成果

FD WGにおける知見共有で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
- 既存の演習、講義をオンライン化するにあたってどのようなソフトウェアを活用することで演習、講義を実施可能となるのかという指針を立てることが可能となる
- オンライン化のニーズに合わせて日々行われている重要なアップデート情報を共有することで、できること、できないこと、できなくなったことを知っておくことで突

図 9：ProSec Web サイト（https://www.seccap.pro/）

図 10：Twitter アカウントによる情報発信

然講義が実施不可能になるという状況の回避

また、これらの成果を広く活用することを目的として、これまでの演習、講義の実施状況や知見を“オンライン授業・演習実施におけるノウハウの共有”として資料を作成した。本資料により講義、演習を新たにオンラインで実施する際の参考となることを期待している。

来年度の計画

ここまでの知見や得られた成果をもとに来年度は講義、演習をオンライン化するにあたってのガイドラインや参考となる資料を作成しProSec自体の取り組みとしてのみならず、産学を通して広く提供することを考えている。

また今年度は、コロナ禍に対応することを目的としてFDに取り組んだため、知見の共有や実施例の紹介などオンライン化を乗り切るための実務的な活動となったことも事実である。そこで来年度は実際に各拠点で提供しているオンライン講義、演習を教員、スタッフ間で体験するためのオンライン授業体験合宿（仮）を実施することを計画しており、これにより更なる高品質な講義および演習を提供するための能力開発および講義、演習の改善、向上に取り組む。

■ 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。

2017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9）
- 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10）

等がある。

2018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、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：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

202103