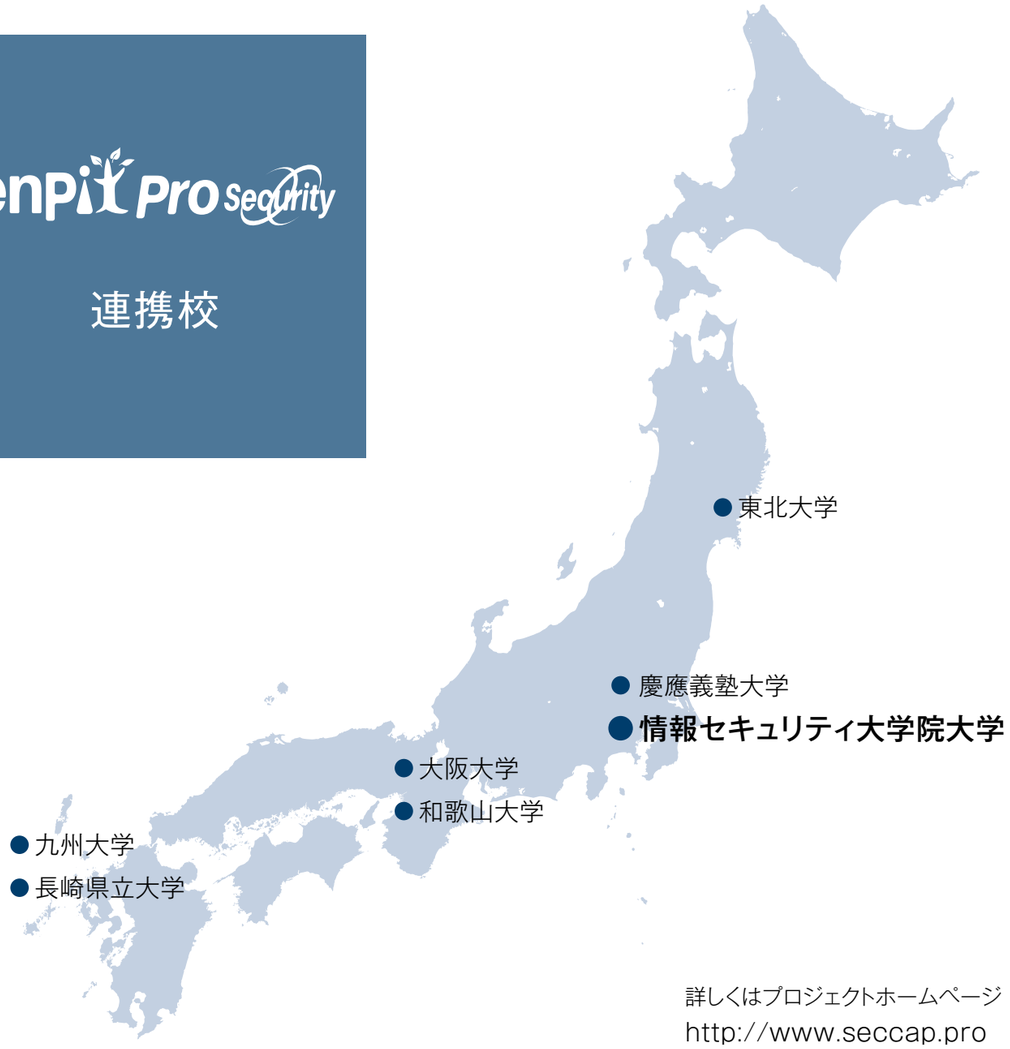
enPiT Pro Security

連携校



詳しくはプロジェクトホームページ
http://www.seccap.pro

連絡先

情報セキュリティ大学院大学 ProSec 事務局	E-mail：iisec@seccap.pro 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@center.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 ：cs-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 / 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	E-mail：keio@secccap.jp

201807

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

【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 2017

2017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、我が国の高等教育機関に求められていることは、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、産学連携により、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を目的とした公募型事業である。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（図1）。

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いるが、13.2万人が不足している。更に、今後も人材不足が増加すると推計されていおり、社会人の再教育による人材シフトが喫緊の課題である。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2」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と大学院6校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する（図2）。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にする。夜間・土曜日の開講や遠隔講義、単位の相互認定を通じて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。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、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する。これらの取組により、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）、（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190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（図3）。

▶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。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目指す（図4）。

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、自身の能力についての客観的な証明書として利用できる。

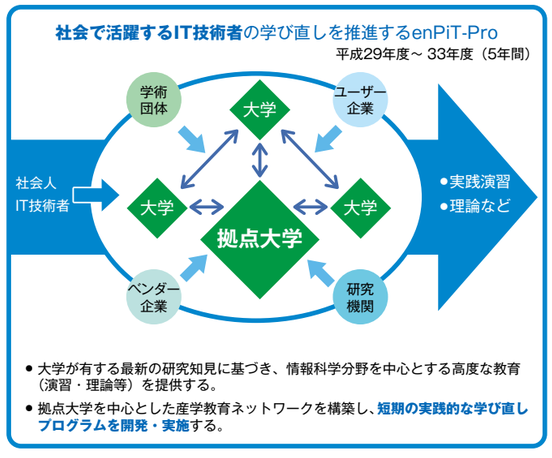


図1：enPiT-Pro事業全体イメージ

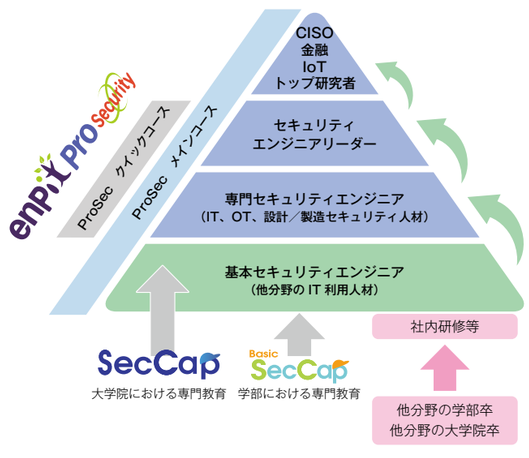


図2：Pro-Secの位置づけ

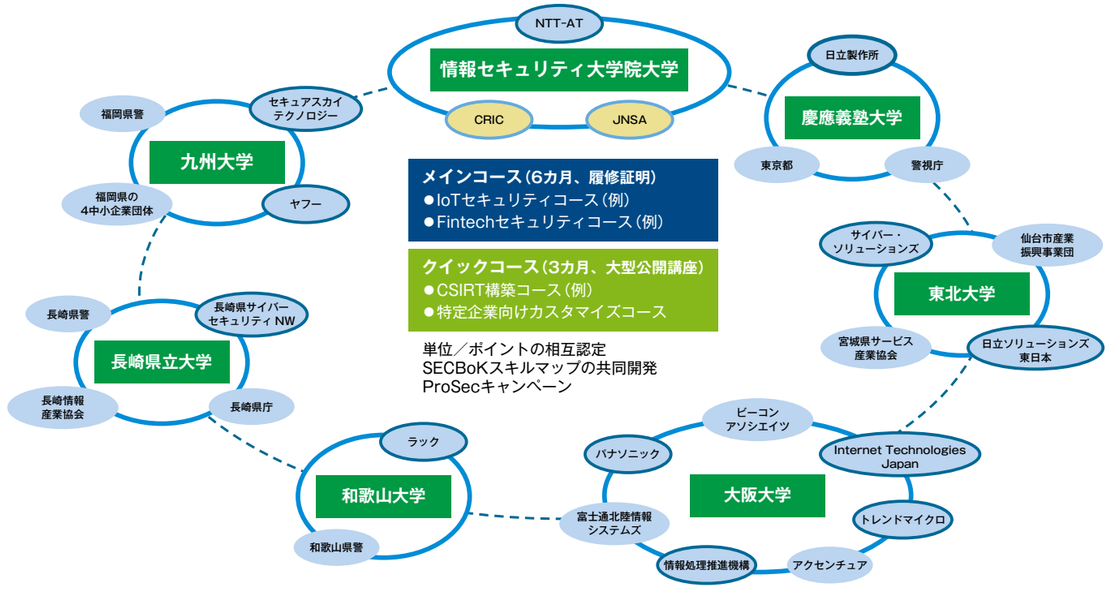


図3：教育プログラムのフレームワーク

情報セキュリティ人材スキルマップ（SecBoK）の概略

「CSIRT運営管理者向けメインコース」の主領域

			CSIRT運営管理者向けメインコース	iコンピティショナリディクショナリのスキル分類											
				メソドロジ						テクノロジ					関連知識
				戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016	基礎	工学基礎										※	※	※	
		ICT基礎	※		※	※			※	※	※	※	※	※	
		ビジネス基礎	※	※		※	※	※							※
	セキュリティ専門分野	セキュリティ基礎										※			
		セキュリティガバナンス													
		セキュリティマネジメント	◇	☆			☆	◇				◇			
		ネットワークセキュリティ	○						○			○			
		システムセキュリティ	○		☆				○	○		○			
		セキュアシステム設計・構築	◎		☆	☆			◎	◎		◎			
		セキュリティ運用	◎			☆	☆	◎	◎		◎	◎			
		暗号・認証・電子署名													
		サイバー攻撃手法	○									○			
		デジタルフォレンジック													
知識項目		法・制度・標準													

記号凡例　◎：演習を伴う実践的専門教育　○：座学中心の専門教育　※：基礎的／入門的教育　☆：状況に応じてケースバイケース　※：修得済みが受講の前提
［産］※［情］※で求めているスキル　［産］※のみで求めているスキル

※［産］：産業横断サイバーセキュリティ人材育成検討会人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］：情報処理安全確保支援士試験シラバスにおいて要求される知識に対応するスキル

コース名称	CSIRT運営管理者向けメインコース
コースの狙い	OT実務の現場で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。
履修（受講）資格	情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）。産業界で情報系業務に従事している技術者を想定する。 以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項で明示）。 ●コンピュータネットワーク（TCP/IP、無線LAN） ●コンピュータアーキテクチャ ●オペレーティングシステム（Windows及びUNIX系） ●プログラミング言語（C言語、アセンブラ）
修得できる知識・技術・能力等	下記テーマについて、業務遂行に必要な知識をする。 ●組織における標的型攻撃対策 ●企業ITシステムの運用段階におけるセキュリティ対策 ●CSIRT運営 ●デジタルフォレンジック
教育内容（授業科目等）・教育方法	講義及び演習により以下を実施 ●基礎講義1　セキュアシステム構成論（4ポイント） ●基礎講義2　ネットワークシステム設計・運用管理（4ポイント） ●基礎講座3　インターネットテクノロジー（4ポイント） ●基礎講座4　CSIRT運営とインシデント対応（4ポイント） ●演　　習　情報セキュリティ（CSIRT実装）（9ポイント）※CSIRT実践クイックコースと同じ ●応用講義1　ハッキングとマルウェア（4ポイント） ●応用講義2　組織行動と情報セキュリティ（4ポイント）
指導体制（教員）	大学院教員及び実務経験の豊富な企業在籍の客員教員
学習時間	演習9ポイント（54時間）と座学12ポイント以上（66時間以上）を含む120時間以上
修了要件	科目ごとの受講を可能とし、科目ごとの受講証を発行する。演習を含む科目を履修し、20ポイント以上履修した受講者に対してProSec-CSIRT認定証を発行する。
年間スケジュール	基礎講義、応用講義は科目等履修により前期または後期に受講する。演習は6月～8月の平日昼間に集中して行う。

図4：コースで学習できる知識と情報セキュリティ人材スキルマップの対応例

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にする。夜間・土曜日の開講や遠隔講義、単位の相互認定を通じて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、図5に示すように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（水色）とクイックコース（灰色）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する。修了者には、PorSec-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。

▶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。

	IT実務 （金融、ビッグデータ他）	OT実務 （CSIRT、SoC他）	設計／製造実務 （IoT、ITシステム開発他）
技術領域	Fintechセキュリティメインコース	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
	実践情報セキュリティ技術者 メインコース	CSIRT実践クイックコース	Secutity-by-Design基礎 クイックコース
	実践情報セキュリティ利活用 クイックコース	インシデントハンドラ実践 メインコース	セキュリティ開発者向け メインコース
	セキュリティマインドメインコース	インシデントハンドラ実践 クイックコース	情報システムセキュリティ・ 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）	インシデントレスポンス実践 メインコース	情報システムセキュリティ・ クイックコース
	セキュリティマインドクイックコース （データ科学）	インシデントレスポンス実践 クイックコース	
		短期セキュリティ 技術・管理・運用 習得クイックコース	
マネジメント領域	セキュリティ対策実践メインコース		
	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		
	CISO向けメインコース		

注　OT：Operation Technology　CISO：Chief Information Security Officer　CSIRT：Computer Security Incident Response Team　SoC：Security Operation Center

図5：ProSecで提供準備中のコースの全体像

2 連携大学の準備状況と計画

2.1 情報セキュリティ大学院大学

●取り組み概要

2004年の開学以来、技術、管理・運営、法制度、情報倫理等広範な領域を対象とする学際的総合科学として情報セキュリティを捉え、それぞれの分野の第一線で活躍する研究者および実務家の力を結集し、高信頼性社会の実現を担う高度で専門的な知識・技術と高い倫理観を備えたプロフェッショナルとして、情報セキュリティにおける技術面での対策を担う情報セキュリティエンジニアと情報セキュリティの運用・管理面でのリーダーとなる情報セキュリティマネージャを養成してきた。本取り組みでは、従来の修士課程、博士課程に加えて、半年程度で修了できる履修証明プログラム（メインコース）と、企業研修等で利用しやすい短期のクイックコースを開講し、社会の多様な人材育成ニーズに応える。

●準備の進捗状況

2017年2月にイスラエルIAI社のTAME Rangeを利用した実践サイバーレンジ演習を20名の社会人・学生を対象にトライアル実施した（協力：大日本印刷株式会社）。受講生からは「インシデントレスポンスにおいてチームワークがいかに重要かを強く実感することができた」等の意見があった。（**写真1**）。

写真1: 実践サイバーレンジ演習トライアルの様子

表1：CSIRT 運営管理者向けメインコース(CS-M2018)

必　修	CSIRT実践演習（CSIRT構築の手引き、NWセキュリティ技術、Webアプリ検査、デジタルフォレンジック）
選択 A	セキュアシステム技術演習 ――NW攻撃とその防御および検知――
選択 B	セキュアシステム構成論、インターネットテクノロジ、情報デバイス技術、ネットワークシステム設計・運用管理、セキュリティシステム監査

情報セキュリティ大学院大学では、2018年4月からCSIRT運営管理者向けメインコース（CS-M2018）を開講する（**表1**）。情報セキュリティの学び直しをしたい現役IT技術者、産業界で情報系業務に従事している技術者に向け、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運営等にかかわる業務遂行に必要な知識、スキルを習得するためのプログラムを提供する。本コース修了者はオプションで実践サイバーレンジ演習も受講可能である。

●来年度以降の予定

後期からIoTセキュリティメインコース（IO-M2018）、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（RM-M2018）の2コースを新たに開講する。詳しくはWebを参照のこと。

●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：iisec@seccap.pro
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

●進捗状況

東北大学では、IT実務に携わる人材を対象とする分野においてセキュリティマインドをもつシステム開発技術者・データ解析技術者の育成を目指したProSec-Mindコースの実施に向けて、開講の準備として運営・推進体制整備と演習環境構築等を行った。具体的には、演習環境構築として、講義の遠隔配信や遠隔講義の受講のための遠隔配信・受講システムと、ネットワークセキュリティの実践的演習のために必要となる機材を整備した。運営・推進体制整備とカリキュラム・講義科目の新設・改訂に向けて、担当予定教員及び教務委員会との協議を行い、法律や実務などの観点でのセキュリティを論じる座学の担当教員として地元企業の実務経験者や情報や法律の専門家と、また実務的なセキュリティ演習を提供するためにネットワークセキュリティを専門とした企業の社長に非常勤講師を依頼して、取組み体制を整えた。

また、（一社）宮城県情報サービス産業協会（MISA）の協力を得て企業の研修ニーズの開拓を行い、あるいは宮城県警が組織する宮城中小企業情報セキュリティ支援ネットワークに対して説明を行い、地元企業に対して受講生の募集広報の準備を行った。

さらに、国内外のセキュリティ技術・人材育成のイベントに参加し、セキュリティ技術の動向や企業におけるセキュリティ人材育成に関するニーズの調査を行った。

●来年度の計画

東北大学では以下の1つのメインコースと2つのクイックコースを10月以降に開講する予定である。

・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）
・セキュリティマインドメインコース

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。二つのクイックコースでは情報セキュリティマネジメントやデータ解析などの知識を身につけるために座学や演習をそれぞれ45時間提供する。セキュリティマインドメインコースでは、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総合的な知識を身につけるために座学や演習を126時間提供する。

履修証明プログラムとして提供するとともに、科目毎の受講も可能とする。さらにコースを修了した受講者に対してProSec-Mindの認定証を発行する。

各コースの内容と教材や環境を具体的に整備し、必要な学内手続きを進め、募集要項やシラバスを作成し、受講生の募集を行う予定である。

●募集情報

問い合わせ先：東北大学
E-mail：tohoku@seccap.jp

2.3 大阪大学

●取り組み概要

情報セキュリティは、技術部門の問題ではなく、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。大阪大学では、数学やアルゴリズム、暗号や情報セキュリティの基盤技術から、情報セキュリティガバナンスや法制度、セキュリティ脅威の分析から、マネジメントまでカバーし、社会システムにセキュリティ技術を適用できる深い知識の獲得と現場知識の涵養を目指したコースを提供する。

●準備の進捗状況

大阪大学大学院工学研究科において科目等履修生高度プログラムとして本コースを実施する大学内取組体制を明確化した。本コースにおいて大阪大学で提供する科目「セキュリティリテラシー」他を新規開設し、既存科目についても本コースに向けて改訂した。他部局科目についても本コース科目として提供するための調整を行った。来年度の科目開設および講義・演習の準備を行った科目について完了した部分的内容を大学院における講義に取り入れることでトライアルを実施し、講義・演習等の実施上の問題点の洗い出しとフィードバックにより、来年度以降の新規科目・改定科目における講義・演習を円滑化、効率化できた。

また本コースにおける教育実施のための外部講師の招へいといった他大学・研究機関および企業との連携体制を整えた。特に本コースでの新規開講科目のための、講義及びPBLの理念、ポリシー、知識単位などの構築を行い、さらに、必須単位となる科目であるセキュリティリテラシーについては、講義ポリシーに沿った講師陣を選定し、講師陣とのカリキュラムについて議論を重ね、講義の構築を行った、PBLについてもこれまでの実績を元に、教材開発を行った。連携企業および連携大学の協力を得て講義内容についての協議を行い、次年度以降の講義実施準備を進めた。また関連団体との連携を通じて中小企業向けセミナーに参加し、地元企業への本コースの広報活動および人的ネットワークの構築を行った。

●来年度以降の予定

今年度の準備に基づいて、本コースにおける教育（講義科目・PBL科目）を受講生に対して実施する。また引き続き連携企業・関連団体の協力の下、講義・演習内容およびカリキュラムについての改善を行い、教育プログラム実施のフィードバックや調査に基づいて社会人向け教育プログラムに対するニーズの把握や最新のセキュリティ技術動向に

関する調査に基づいてコース設計の改良を行う。

●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

和歌山大学においては、ネットワークおよびコンピュータシステムをレイヤシステムとして再認識し、各レイヤにおいて必要なセキュリティを確保、発生した事案を速やかに収束させる技術を提供し、その仕組みへの深い理解を講義・演習を通じて提供する。

演習の内容としては、実際にインシデントを特定の環境内で発生させて、この発生に必要な要件を意図的に揃えることの困難さを理解する。これは一方で、ネットワークおよびコンピュータシステムの設計および運用上の弱点を理解することになり、セキュリティの確保とインシデントレスポンスに有用である。一方で、インシデントレスポンスに必要な解析手法が、実際にどのような場面でどのように使用されるかという具体的な手法についても実践する。

●準備の進捗状況

和歌山大学では、2017年8月に和歌山県警のサイバー犯罪対策班の研修を受け入れ、実際のサイバー攻撃を構成する要件の理解と情報収集の手法、解析業務およびフォレンジックについて演習を提供した。併せて、研修の中でenPiT2 (BasicSecCap) における学部生への演習にも企画・運営として参加いただき、参加者にインシデントレスポンス“させる”ために必要なノウハウを提供した。

本学が考えているProSecの人材育成とは、「教える側の層を厚くする」ことである。このため、「～させる」視点でIT実務およびOT実務に広く携わる基礎知識と基礎体力を備えた人材育成に役立つカリキュラムを構築している。

本学では、2018年4月から、インシデントレスポンス実践メインコースを開講する。これは、実務をこなしてきた社会人の学び直しとして活用できるよう、また社内での人材育成に役立つよう、「～させる」上でのさまざまな工夫をしている。なお、本実践コースではいくつかインシデントのシナリオ (環境とレスポンスの手順など) を作成し、これをBasic SecCapのインシデントレスポンス演習や情報危機管理コンテストに採用する場合がある。

●来年度以降の予定

後期からインシデントレスポンス実践クイックコースを開講する。各コースでは参加希望の企業との打ち合わせを継続して実施し、講義・演習内容およびカリキュラムの改善を随時おこなう。複数のセキュリティベンダ製品による機能評価やセキュリティソリューションへの適用評価についても実施する。

●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@center.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、ProSecの教育プログラムの一環として、情報システムを構築する最新の技術、および、それらをサイバー攻撃から守るための発展的な技術について講義・演習を通じて、知識や技術・手法を習得させるProSec-ITを構築、実施する。演習の内容としては、企業等の協力を得て、実際に企業でも扱われている最新技術や最新のサイバー攻撃に関する情報を反映する。

●準備の進捗状況

九州大学においては、大学院システム情報科学府の正規科目として演習を中心とした科目として、「情報システムセキュリティ演習」と「セキュリティエンジニアリング演習」を新設した。また社会人が受講し易い特別科目として「情報システムとセキュリティ」を設計した。それらを中心として既存の大学院科目を含む履修証明プログラムであるProSec-ITを構成し、学内の承認手続きと受け入れ準備を行った。九州経済連合会および福岡県、福岡県警、4つの中小企業支援団体で構成されている中小企業サイバーセキュリティ支援ネットワーク等を通じて広報を行った。新聞等のメディアの取材も受け多くの社会人エンジニアに広報することができた。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) の協力を得て最新のサイバーセキュリティ技術を含む講義・演習を準備することができた。次年度以降に本格的に開始する演習等の開催に向け、社会人も参加するワークショップにおいてトライアル演習を実施し、演習教材や演習環境の改善を行った

写真2：実践サイバーレンジ演習トライアルの様子

(写真2)。本プログラムの主たる講義実施会場として、福岡市中心部に位置し交通至便な大橋サテライトを準備することができた。また学生事務組織の協力を得て受講生募集の手順や諸規則を作成し、受講生募集を実施し、審査、受け入れまでを実施した。

●来年度以降の予定

九州大学においては、クイックコースの募集を行い、審査、受け入れを実施する。連携企業の協力も得てProSec-ITのメインコースおよびクイックコースの講義・演習を土日開講や集中講義の形式で実施する。受講者や企業からのフィードバックを得て、カリキュラムや講義科目について改善や改訂を実施する。また、昨年度に引き続き企業や団体と連携して受講者のニーズを把握したり、セキュリティを含む情報科学に関連する実践的な教育の進め方、社会人エンジニアに対する情報教育のあり方について、海外調査および国内調査実施し、より良いコース設計を行う。

●募集情報

問い合わせ先：〒819-0396　福岡市西区元岡744九州大学事務局名：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：cs-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

2016年4月より、全国初の情報セキュリティ学科に改組し、情報セキュリティ人材育成の育成を開始している。当初より、社会人のための連続セミナーなどを開講しており、地域に根差しつつも、全国の学術機関と連携した情報セキュリティ人材育成を目指している。本学では、地方における最新の情報セキュリティ技術を習得する機会として、まずは幅広い知識を提供可能なコースを想定している。受講者の立場を、開発ベンダおよび利用者システム側とみなし、それぞれに適切なコースを提供することを計画した。また、地域の企業・組織からの要望を取り入れるために、本学内に4企業、1県警と本学教員から構成される「社会人情報セキュリティ学びなおしプログラム検討会議」(以降、学びなおし会議) を設置し、コンテンツや授業運営・運用に反映できるよう議論を継続している。

また、地方大学の事情として、受講生の通学への不便さが挙げられるが、本学も例外ではない。そこで、演習を除き、座学では積極的に遠隔講義を活用することを計画している。

●準備の進捗状況

長崎県立大学情報システム学部情報セキュリティ学科の教員は、現在大学院の教員も兼任しているが、情報セキュリティについての本格的な講義を準備中である。本プログラムにおいては、既述した学びなおし会議での優先的に必要とされている開発者向けコースを開講するべく準備中である。また、大学院の、履修証明プログラムとして開講可能かは検討中である。開発者向けコースは、セキュア開発技法Ⅰ、Ⅱ、ネットワークセキュリティ、データセキュリティの4科目から構成される。また、SMB (中小企業) セキュリティの実践も開講を予定している。科目によっては、前半、後半に分割することが可能なため、クイックコースとして構成することも可能である。なお、遠隔講義を実現するために動画とe-ラーニングシステムを統合するシステムを開発した。

●来年度以降の予定

学びなおし会議からのコンテンツへの要望等を取り込めるかを継続して検討していく。また、地域の企業等から受講生を派遣しやすいように、集中講義や遠隔授業の配信を実施していく。開発者向けコースの開講と平行して、利用者向けコースの開講についても、地域の要望を取り入れコースを設計、改良していく。また、学内事務との連携を深め、受講生の募集、受講料などを検討する。

●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、連携するさまざまな組織と協議を行い、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るに至った。こうした認識から、慶應義塾大学ではインシデントハンドラ実践メインコースの準備を進めるとともに、サイバーセキュリティファンダメンタルコースの準備を進めてきた。同時に、サイバーセキュリティを理解するために必要なコンピュータサイエンスの基礎知識コースを準備し、さまざまなメインコース／クイックコースに参加するための基礎知識を補うための仕組みの検討を進めてきた。

また、こうした各コースの修了認定に関しての相互連携について検討を行い、他大学が実施するコースとの連携を進めるための検討を行った。

こうした種々のコースを用意することで、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す。

●準備の進捗状況

各コースの実施のため慶應義塾大学ではエクステンションコースとしての実施設計を進め学内体制の整備を行った。また、インシデントハンドラ実践メインコースの実施のため特にロールプレイ型のインシデントハンドリング演習に関して、連携組織に属する社会人を対象に試行を行い、課題の整理とレベル調整を実施している。この演習は、実際に発生するインシデントを例にその対応について検討を行う演習であるが、電話でインシデント発生の連絡を受けたり、対応状況について逐一報告するなど、実際の状況に近い経験を行うことで、具体的な対応を理解できるようにされている。

また、ファンダメンタルコース及び基礎知識コース実施のための教育項目を整理し、実施へ向けた準備を進めた。特に、ファンダメンタルコースはサイバーセキュリティあるいはITに関する知識を持たない参加者も対象とするため、基礎的な知識を補うように配慮してある。また、こうした整理を元に基礎知識コースの設計を行った。

他大学との連携においては、運営委員会での議論を元に連携のしやすい体制の検討を進めている。特にファンダメンタルコースについては、各地域で必要になることを考慮し、地域連携を含めて実施できるように検討を行っている。

●来年度以降の予定

今年度の準備に基づいて、各コースを来年度後半より実施する。また、引き続き連携組織との協議を進め必要とされる内容の精査を進める。また、サイバーセキュリティの状況は日々刻々変化するため、こうした変化に合わせた演習等の新規開発を進める。さらに、大学間の連携を進めるための方策の検討を進める。

●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
E-mail：keio@secccap.jp

3 大学間での連携した取組

■コース評価

コース評価は宮地充子（大阪大学）、川橋裕（和歌山大学）、小出洋（九州大学）が担当する。宮地はこれまで、大学院生用のセキュリティコース、学部生用のセキュリティコースの評価を行ってきた。社会人コースにおける評価は、これらの経験を元に、構築する予定である。具体的には、大学院生、学部生の評価手法が、

1. 河合塾から提供されるコンピテンシー能力のコースの受講前後の違い
2. （大学院生）就職後の上司の評価
3. （学部生）配属の教員、あるいは担当教員の評価

となっており、どちらかというと社会性の評価を中心に展開している。

社会人コースにおいては教育コースの構築の観点から、社会性の評価に加えて、コースの内容の評価も展開する方向で、現在、各大学の講義の評価システムを収集している。また、予備調査として、各企業、企業社会人からの必要科目の情報の収集を行っている。

■コース連携

コース連携は、湯淺墾道（情報セキュリティ大学院大学）、砂原秀樹（慶應義塾大学）、曽根秀昭（東北大学）が担当する。コース連携は大学が相互に講義を提供することにより、一つの大学だけでは提供が困難な豊富な講義メニューを受講者に提供することを目的としており、これまで、大学院生向けenPiT1、学部生向けenPiT2では単位互換やネットワークによる遠隔講義を利用してコース連携を実現してきた。enPiT-Proにおいても同様の方法でコース連携の実現を模索しているが、enPiT-Proでは①講義時間や開催時期に統一性がないこと、②受講者が正規課程の学生ではないため単位互換などの仕組みが適用できないことなどの課題があり、これらの課題を克服する新たな枠組みの構築に向けて検討を進めている。

■教務

教務では、各大学が提供するカリキュラムが、情報セキュリティ人材の育成に適合しているかを検証し、不足した部分などを相互補完や追加し、最適なカリキュラムを提供しているかを常に検討していく。初年度は、まず日本ネットワークセキュリティ協会（JNSA）が（独）情報処理推進機構（IPA）が公表しているセキュリティ人材に関連するiコンピテンシディクショナリを参考として作成した「セキュリティ知識分野（SecBOK）人材スキルマップ（右表参照）」を活用し、これに各大学の科目の適合を検証することとしている。本WGは、長崎県立大学が中心となり、各大学の委員とともに実施している。

■認定・コース

認定・コースは、小出洋（九州大学）、砂原秀樹（慶應義塾大学）、山口文彦（長崎県立大学）が担当する。認定・コースは、各大学がそれぞれ実施している教育コースのProSecコースとしての認定方法を確立し、認定を行うことを目的としている。今回実施するenPiT-Proは現役の社会人エンジニアが新たに大学に来て教育を受けるという点で、大学がこれまでに連携して行ってきた教育プログラムである、ICT人材育成、enPiT-1、enPiT-2等と大きく異なり、コース認定という観点からは多くの解決すべき課題、考慮すべき課題が存在する。今後、それらの課題を洗い出して大学間連携を含むコース認定に関する制度をつくる。

今後はコース連携WG、スキルマップWGと連携することにより、ProSecコース要件の明確化を行い認定制度を設計する。

基礎	ICT基礎	情報理論 計算機ハードウェア ネットワークインフラ 通信プロトコル・サービス データ構造 データベース ナレッジマネジメント アルゴリズムとプログラミング オペレーティングシステム ソフトウェア システム開発 システム運用 エンタープライズアーキテクチャ アプリケーションとサービス その他
	工学基礎	工学基礎
	ビジネス基礎	ビジネス基礎
キュリティ基礎	セキュリティ基礎	セキュリティ基礎
セキュリティガバナンス	セキュリティガバナンス	セキュリティガバナンス
セキュリティマネジメント	セキュリティマネジメント	セキュリティマネジメント
ネットワークセキュリティ	ネットワークセキュリティ	ネットワークセキュリティ
	トラフィック解析	トラフィック解析
	侵入検知	侵入検知
	脆弱性診断	脆弱性診断
	フィルタリング	フィルタリング
	アクセス制御	アクセス制御
	VPN	VPN
	深層防御	深層防御
システムセキュリティ	システムセキュリティ	システムセキュリティ
セキュアシステム設計・構築	セキュアシステム設計・構築	セキュアシステム設計・構築
	セキュアプログラミング	セキュアプログラミング
	テスト	テスト
セキュリティ運用	セキュリティ運用	セキュリティ運用
	インシデント対応	インシデント対応
	セキュリティ運用の関連知識	セキュリティ運用の関連知識
暗号・認証・電子署名	暗号・認証・電子署名	暗号・認証・電子署名
サイバー攻撃手法	サイバー攻撃手法	サイバー攻撃手法
	マルウェア	マルウェア
	サイバー攻撃手法関連スキル	サイバー攻撃手法関連スキル
デジタルフォレンジクス	デジタルフォレンジクス	デジタルフォレンジクス
法・制度・標準	法・制度・標準	法・制度・標準