

enpit Pro security

連携校

【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



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

連絡先

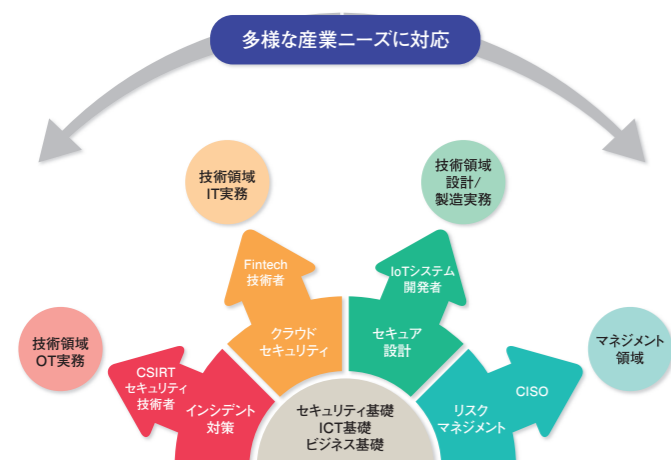
情報セキュリティ大学院大学 ProSec 事務局	E-mail : prosec@iisec.ac.jp URL : https://www.iisec.ac.jp/admissions/prosec/
東北大学 大学院情報科学研究科 実践の情報教育推進室 (ProSec 担当)	E-mail : tohoku@seccap.jp URL : http://www.esprit.is.tohoku.ac.jp
大阪大学 大学院工学研究科 宮地研究室	E-mail : myj-pro.seccap.staff@crypto-cybersec.comm.eng.osaka-u.ac.jp URL : 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-mail : 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

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

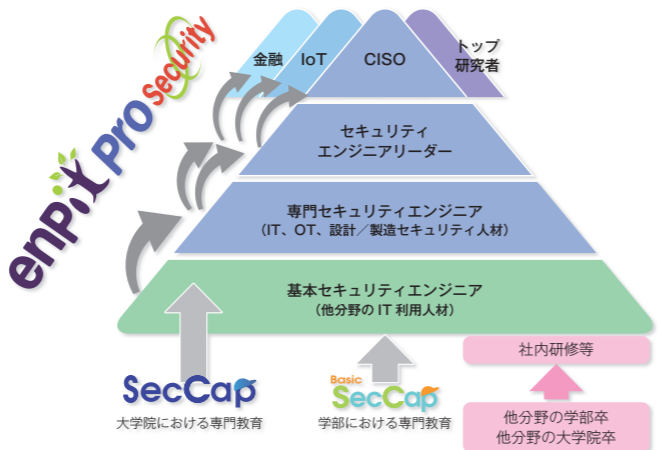
情報セキュリティのプロを育てる

情報セキュリティ分野では、CISO (Chief Information Security Officer) といった企業内のセキュリティに責任を負う経営層から、最先端のセキュリティ研究者まで多彩な人材が必要とされています。また、FintechやIoT、Big Dataなどの最先端の技術分野においてもセキュリティマインドを持つシステム開発技術者が求められています。

enPiT-Pro Security (ProSec) は、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、慶應義塾大学の7連携大学院が文部科学省「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・プログラムに基づき、社会人の学び直しを支援する高等教育の体制を整え、さまざまな分野で活躍する情報セキュリティ分野のリーダー人材を養成する短期集中プログラムです。



本プログラムでは、7連携大学院が、全国に会員企業を有する日本ネットワークセキュリティ協会 (JNSA)、サイバーリスク情報センター (GRIC) および各連携校を拠点とした地域の団体・官庁・企業と連携し、多様な産業ニーズに即した幅広い教育コースを開発するとともに、情報セキュリティ教育コースの修了を認定するProSec-X (Xは領域の名称) 認定証を発行し、全国規模で統一された情報セキュリティ教育を実施します。また、人材スキルマップを開発し、産業の求める人材スキルと教育コースが提供する知識・技術を共通のマップ上で視覚化することを通じて、効果の高い教育コースの開発を進めます。



受講対象者のイメージ

CISO等の経営層から、セキュリティポリシー設計等のマネジメント、サイバー攻撃から社内システムを守るオペレーションエンジニア、システムの設計/製造に携わるエンジニア、最先端のセキュリティ技術者・研究者などを想定しています。

FinTech、IoT、データマイニング等の最新技術に対応したセキュリティ技術など、多様な産業ニーズに対応した幅広いセキュリティ教育コースを提供します。情報セキュリティの基礎理論と実践技術を大学院で効果的に身につけたい社会人や、社内研修では達成が難しいプロ人材の育成を大学院がサポートします。

社会人が受講しやすい工夫

教育コースは、メインコースとクイックコースの2種類を提供しています。講義や演習の開講日時の配慮等により、社会人が受講しやすいコースを開講します。

【クイックコース】

その時々専門知識や新しいサイバー攻撃に対応した特定のスキルを短期間 (30~60時間) で学びます。

【メインコース】

IoTやFintechなどの最新の専門知識や新しいサイバー攻撃に対応した演習と、大学院の既設正規科目である講義/演習 (開講大学の科目等履修生として受講) を組み合わせた構成です (120時間以上)。修士・博士課程への橋渡しとなる単位取得も可能なコースです。

詳細は<https://www.seccap.pro/classes/> ※開講大学の履修証明プログラムとして設定されているコースの場合、修得者には開講大学より履修証明書が発行されます。



連携校担当教員からのメッセージ



情報セキュリティ大学院大学
情報セキュリティ研究科・教授

大久保 隆夫

Takao Okubo

情報セキュリティ大学院大学は2004年の開学以来、研究・教育を通じて産業界・社会のニーズに応えるため、さまざまなプログラムに取り組んで参りました。本プログラムは、サイバー攻撃防御、IoTセキュリティからDXセキュリティ、リスクマネジメントに至るまでの幅広い内容を、コンパクトに修得できるプログラムです。セキュリティの基礎から経営、サイバーレンジを使用する高度なハンズオン演習まで、多様なコースの中から実践的に学ぶことができます。



東北大学
大学院情報科学研究科・教授

曾根 秀昭

Hideaki Sone

東北大学では、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・データ解析技術者に主眼を置いてコースを計画しました。とくに、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、データ解析、情報セキュリティマネジメントについて業務遂行に必要な知識を習得しようとする技術者を歓迎します。



大阪大学
大学院工学研究科・教授

宮地 充子

Atsuko Miyaji

「安全なデータ活用のためのプロフェッショナル人材育成プログラム」では、セキュリティビジネスの実務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します。



和歌山大学
学術情報センター・教授

内尾 文隆

Fumitaka Uchio

和歌山大学では、情報セキュリティにおけるインシデントの発生する仕組みと解析、および対応方法の流れを理解し、業務に活かしたいエンジニアやマネージャの皆さまのために本コースを設置しました。利便性を確保しつつ、インシデント対応が容易で、かつセキュリティを向上させたバランスを図るシステム設計とスキルの向上を求める技術者を歓迎します。



九州大学
サイバーセキュリティセンター・教授

小出 洋

Hiroshi Koide

九州大学では、連携大学と様々な企業、機関と連携した教育プログラムであるProSec-ITを提供します。これは情報システムの構築、運用、サイバー攻撃からの防御、インシデントが起きたときの対応までを網羅的に学べるように計画しました。新しい技術や基礎知識、背景にある理論や技術を習得しようとする技術者を歓迎します。



長崎県立大学 情報システム学部
情報セキュリティ学科・教授

小松 文子

Ayako Komatsu

現代の社会経済を支える情報システムを開発する技術者だけでなく、利用する技術者にとっても、セキュリティや高度な情報科学の実践的能力は大切になっています。本学では、開発者、利用者のそれぞれの立場でセキュリティを学ぶ科目を本学の専門的な演習設備や遠隔授業なども活用し提供します。



慶應義塾大学
大学院メディアデザイン研究科・教授

砂原 秀樹

Hideki Sunahara

enPiT-Pro Security/ProSecでは、セキュリティの専門家を育成するだけでなく、セキュリティを理解する他の分野のプロフェッショナルを育成することを目指しています。また、社会人が参加しやすくなることやCOVID-19の影響を考慮し、オンラインを含めたさまざまな参加方法が選択可能です。セキュリティに関する知識を持たない方々から、セキュリティに関する知識や経験を深めたい方々まで、さまざまな方々の参加を期待しています。