2017年、サイバーセキュリティ人材育成事業の略称を「K-SEC」とし、併せて、ロゴマークを設定しました。サイバー空間をイメージした青色を配色し、Kの文字で、高専生の持つ技術力・先進性を表現しました。また、Kの文字を円で囲い安心感を表現し、加えて、小さな円で表現した大事なものを守ることで社会に貢献したいという想いを込めています。

K-SEC 公式サイト

https://k-sec.kochi-ct.ac.jp/

お問合せ先

拠点校

木更津工業高等専門学校　〒292-0041 千葉県木更津市清見台東 2-11-1　TEL 0438-30-4000(代)

高知工業高等専門学校　〒783-8508 高知県南国市物部乙 200 番 1　TEL 088-864-5500(代)

sec_edu_pj@kochi-ct.ac.jp

2022.09 作成

サイバーセキュリティ人材育成事業

KOSEN Security Educational Community

サイバーセキュリティの最新動向

IT化による高い利便性と引き換えに、多くのリスクを併せ持つ現代社会。セキュリティ・インシデントの発生について、ニュースや新聞紙面で取り上げられない日はありません。

- ウイルス「Mirai」の攻撃により複数の大手ネットサービスが長時間にわたって接続しにくくなるトラブルが発生。IoT機器がDDoS攻撃に加担してしまったことが原因。実在する氏名やメールアドレスを流用し正規メールへの返信を装う「Emotet」が感染拡大。
- ランサムウェア「WannaCry」の世界的感染が発生し、世界150か国で30万台以上のコンピュータが感染。国内でも、2000件の感染が判明。
- ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が窃取され、不正送金や不正利用の事例が発生。
- 近年、大学等の高等教育機関や研究機関などを対象とした高度サイバー攻撃(API攻撃)が増加。この攻撃により個人情報や知的財産や研究データ等の盗取や、組織内システムへの不正アクセスや不正使用が発生。
- 商品の開発、調達、製造、在庫管理、物流、販売といった一連のプロセス(サプライチェーン)の中で、セキュリティ対策の強固な大企業ではなく、セキュリティが脆弱な取引先や委託先等を攻撃し、それらを足掛かりとして標的の大企業の機密情報等を窃取する攻撃。

サイバーセキュリティの人材不足

上記のような脅威に対抗するために、サイバーセキュリティ分野に詳しい人材が求められています。しかし、経済産業省の「IT人材の最新動向と将来推計に関する調査結果」では、サイバーセキュリティ分野における人材不足は増加傾向にあり、2030年に向けて、一層深刻化することが想定されています。また、政府関係会議でも、「ITベンダーや企業・団体で、サイバーセキュリティに精通した者が必要である」ことに加え、「高度な専門性及び突出した能力を有する人材の必要性」も提起されています。

ITが隅々にまで普及した現代社会においては、サイバーセキュリティ確保への取り組みとサイバーセキュリティ分野の知識を身につけた人材の育成が不可欠です。

サイバーセキュリティに貢献できる高専生の可能性

ITの最新ハードウエアやソフトウエアに触れる環境があり、15歳の早い段階から専門教育を受けることが出来る高専生は、将来、サイバーセキュリティの分野で社会に貢献出来る可能性を持っています。

独立行政法人国立高等専門学校機構

サイバーセキュリティスキルを備えた人材の育成

高専が継続的に輩出する人材

質的向上

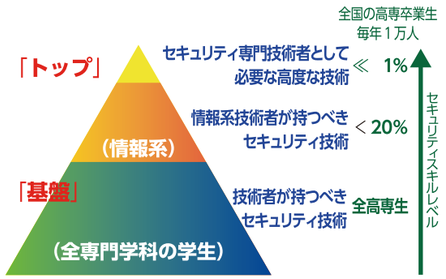
飛び抜けたサイバーセキュリティ人材（トップ人材）

サイバーセキュリティ専門技術者として必要となる高度な技術を持った高専卒のトップレベル人材の輩出を目指します。高専生がより高度な技術を身につけることができるように、外部のサイバーセキュリティ専門組織と連携し、最新動向やより高度な技術に触れる機会を作っていきます。

量的拡大

体系的にセキュリティ知識を身につけた高専生（プラス・セキュリティ人材）

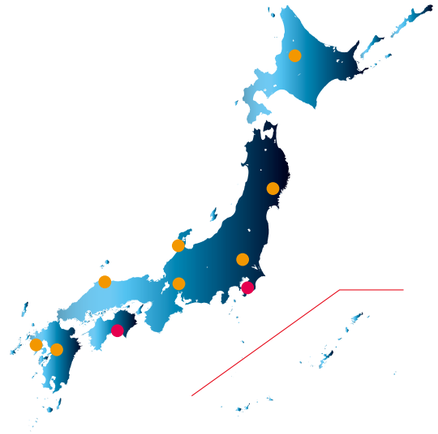
専門分野において「守るべきものは何か」を考えることができる技術者になるため、機械・建築・土木・電気/電子・材料生命など工学分野の技術者が持つべきセキュリティ意識や技術を身につけさせ、情報系技術者には、社会で必要とされているサイバーセキュリティ技術を身につけさせることを目指します。本来の業務を担いながらITを利活用する中で、セキュリティ技術も習得した人材（プラス・セキュリティ人材）の育成を図ります。



推進体制

拠点校と協力校が、サイバーセキュリティ人材の育成を推進しています。

第１ブロック	●	協力校：旭川高専
	●	協力校：一関高専
第２ブロック	●	拠点校：木更津高専
	●	協力校：小山高専
第３ブロック	●	協力校：石川高専
	●	協力校：岐阜高専
第４ブロック	●	拠点校：高知高専
	●	協力校：松江高専
第５ブロック	●	協力校：佐世保高専
	●	協力校：熊本高専



主な活動

人材イメージとカリキュラムの作成

高専の卒業生が活躍すると想定される職種を考慮し、習得すべきスキルを検討します。検討の結果に基づき、全分野の学生、情報系学科の学生それぞれを対象としたスキルマップを整備します。そしてサイバーセキュリティを学ぶためのモデルコアカリキュラムを構築していきます。また、カリキュラムを実現するためのシラバスの整理を行います。

セキュリティ演習拠点の整備

各ブロックでのサイバーセキュリティ教育の拠点として、拠点校と協力校、あわせて10校にセキュリティ演習環境の整備を行いました。これらの演習環境を活用した授業・課外活動、イベント等を通して、サイバーセキュリティ教育と人材育成の重要性を発信していきます。

〈学生対象〉コンテスト、高度人材育成講座等の開催

高専で身につけた情報科学の知識やサイバーセキュリティの技術を活かすことができる高専セキュリティコンテストを毎年開催しています。高専セキュコンの最優秀チームは、セキュリティコンテスト日本大会の出場権を獲得できます。また、長期休暇期間を利用した合宿形式での高度人材育成講座やオンライン講習会等を企画し、学生のスキルアップを支援しています。

〈教員対象〉講習会、ワークショップの開催

企業で活躍する実務家教員による特別演習の様子を参観できる授業見学会のほか、情報系分野だけでなく、他の専門分野の教員もサイバーセキュリティ教育を授業に取り入れることができるよう、教材の活用を支援する勉強会や授業見学会を行っています。また、全国の教職員を対象にしたサイバーセキュリティ意識を啓発するための講演や、教育現場で役立つ内容を紹介するワークショップを開催しています。

教材の作成と全国高専への展開

すべての学生がセキュリティの基礎を学ぶための基本的な教材から、情報技術をより深く学ぶ情報系学生向けの教材、また、情報系でない分野に進む学生の専門分野に合わせた教材など、多様な教材を開発しています。全国の国立高専からアクセスできるK-SEC教材サイトでは、教材の紹介のほか、教材とモデルコアカリキュラム(MCC)の対応や教材を活用した教育実践の紹介等を行っています。

セキュリティ演習教材の導入

サイバーセキュリティの必要性を実感してもらうために、実践を模した演習教材の導入を進めています。実際に近い情報システムに対する攻撃、防御を行うことができるサイバーレンジ教材、産業分野におけるサイバーセキュリティを実践的に学習できるPLC制御システム教材など、多様な演習教材を提供しています。

セキュリティに関するコミュニティ形成

質の高いサイバーセキュリティ教育の継続と教員同士の連携の活発化を目指して、教員等育成プロジェクト参加教職員を中心としたコミュニティ形成に取り組んでいます。また、高専セキュリティコンテストや学習イベント等を通して、学生同士の活発な交流を図っています。

セキュリティ関連外部組織との連携

セキュリティ知識を身につけた高専生、また高度なセキュリティ技術を身につけた人材の育成のために、企業、大学、公的機関等の外部組織との連携を進めています。外部組織の支援を得た講習会やコンテストの開催、インターンシップの実施などを積極的に行い、また、学生が習得すべき知識やスキルについての整理も進めます。