

# サイバーセキュリティ人材育成事業



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

一関工業高等専門学校 〒021-8511 岩手県一関市萩荘字高梨 TEL 0191-24-4700(代)  
 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)  
 石川工業高等専門学校 〒929-0392 石川県河北郡津幡町北中条 TEL 076-288-8000(代)  
 佐世保工業高等専門学校 〒857-1193 長崎県佐世保市沖新町 1-1 TEL 0956-34-8406(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

2020.10 作成



## 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も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な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ことが原因。**
- 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。**
- 教育情報システムや中学校の学内ネットワークが不正アクセスを受け、生徒や保護者、教職員の個人情報、成績関連情報などの外部流出が判明。**
- IT犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手できるようになり、情報モラルの低い若者によるIT犯罪が増加。**

## 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の最新ハードウェアやソフトウェ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できる高専生は、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

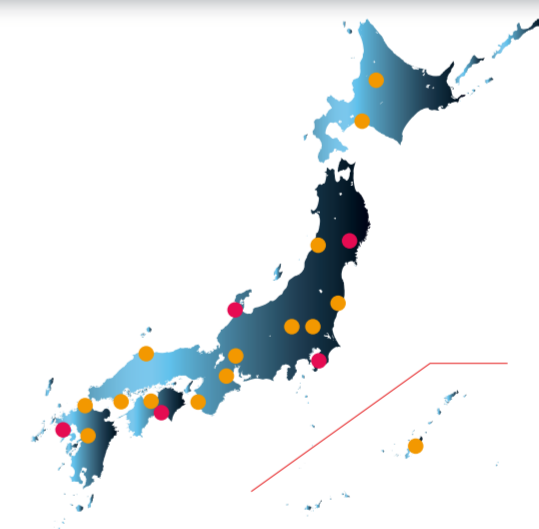
#### 体系的にセキュリティ知識を身につけた高専生(プラス・セキュリティ人材)

専門分野において「守るべきものは何か」を考慮す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ること、そして、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。

## 推進体制

全国を5つのブロックに分け、各ブロックの拠点校と実践校が、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** ● 拠点校：一関高専 ● 実践校：苫小牧高専、旭川高専、鶴岡高専
- 第2ブロック** ● 拠点校：木更津高専 ● 実践校：福島高専、小山高専、群馬高専
- 第3ブロック** ● 拠点校：石川高専 ● 実践校：岐阜高専、鈴鹿高専、和歌山高専
- 第4ブロック** ● 拠点校：高知高専(中核拠点校) ● 実践校：松江高専、大島高専、新居浜高専
- 第5ブロック** ● 拠点校：佐世保高専 ● 実践校：北九州高専、熊本高専、沖縄高専



## 主な活動

### 人材イメージとカリキュラムの作成

大学企業等接続先の要請を考慮した習得すべきスキルや習得レベルを定義することで、高専が輩出する人材のイメージを明確にしています。基盤教育とトップ人材、それぞれのスキルマップを整備し、サイバーセキュリティを学ぶためのカリキュラムと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5校と実践校5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。2018年度から10校の環境整備、再整備を行い、更なる教育環境の充実を図っています。

### (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全国規模のセキュリティコンテストを2016年度から毎年開催しています。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各ブロック内の学生を対象とした講習会等を企画し、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

サイバーセキュリティの課題や事例を理解する「情報教育担当教員向け講習会」と、より高度な専門的な知識や技術を習得する「情報系教員向け演習」を実施しています。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啓発のための講演や、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

セキュリティの基本を学ぶ「全学科向け基本教材」と情報技術をより深く学ぶための「情報系学生向け教材」を作成しました。「全学科向け基本教材」[各専門分野別教材]では、実社会で役立つセキュリティ知識を習得するために、事例に即した分野ごとの学習内容を用意しています。また、K-SEC公式サイトでは、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。クラウド環境で攻撃や防御を体験する演習、IoT分野でのボードゲーム形式の演習、カードゲーム等サイバーセキュリティを楽しみながら体験する教材を用意しています。

### 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、ブロック内活動を中心とした教員のコミュニティ形成に取り組んでいます。また、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。2018年度には、全国の高専に向けたメールマガジンの配信を開始しました。

### 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進め、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。

