資料２

国立高専・木更津高専における サイバーセキュリティ人材 育成の取組み

木更津工業高等専門学校
丸山真佐夫
（KOSEN サイバーセキュリティ教育推進センター運営校）

木更津工業高等専門学校
NATIONAL INSTITUTE OF TECHNOLOGY, KISARAZU COLLEGE

国立高専セキュリティ教育の到達目標

- 「モデルコアカリキュラム」（MCC）＝ 国立高専の教育におけるミニマムスタンダード
  - 全学生が学ぶ「工学基礎」と専門分野（情報工学科は「情報系分野」）ごとに設定
  - 「工学基礎」「情報系分野」にセキュリティに関する項目
- MCC Plus＝各校の特色を活かしたカリキュラム編成の参考指針
  - セキュリティ分野はSecBok等を参考に作成
    - サイバーセキュリティに関する24 項目とその他ソフトウェア工学，システム設計など9項目

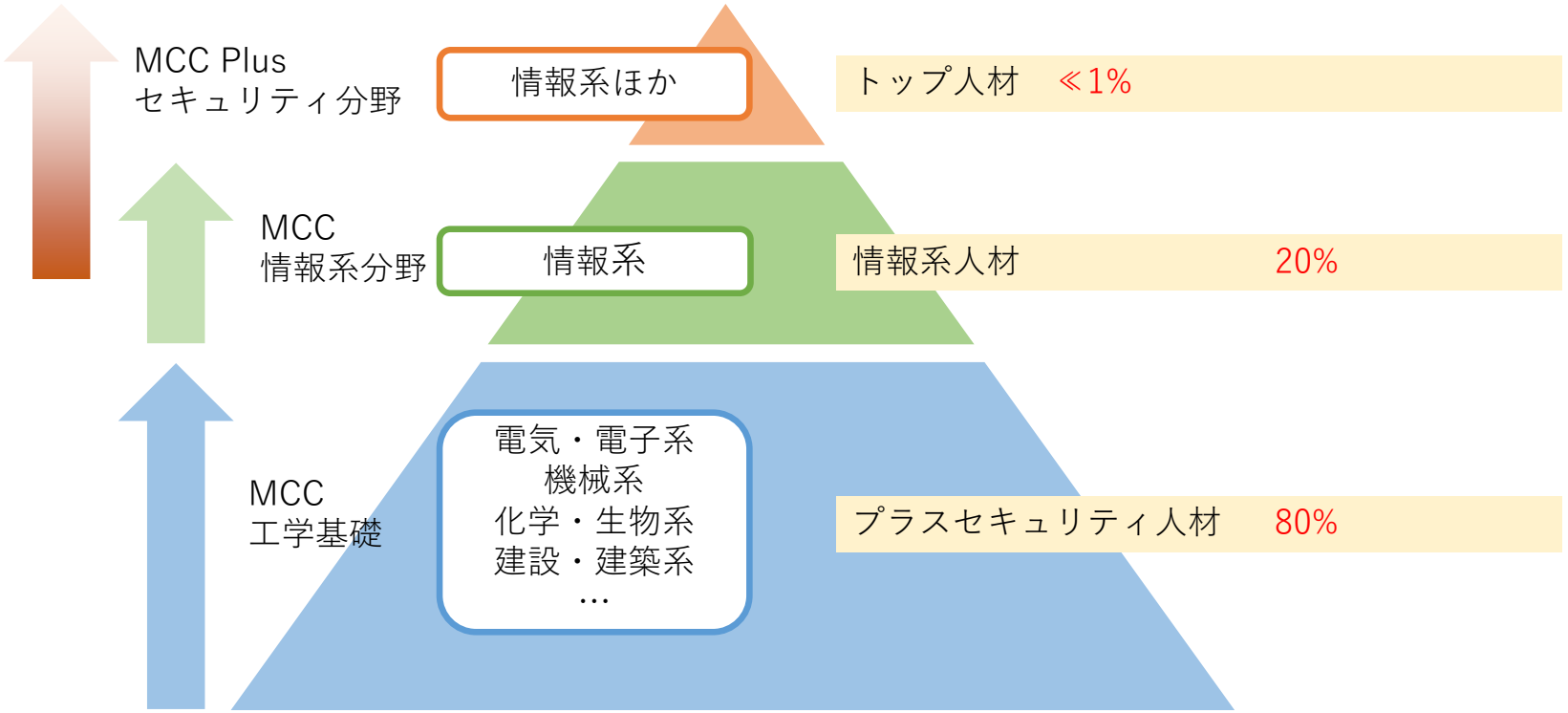
MCC「工学基礎」のセキュリティ項目（リテラシーレベル）

到達目標	到達目標
情報セキュリティの必要性を理解でき対策について説明できる。	情報や通信に関連する法令や規則等と、その必要性について説明できる。
情報セキュリティを支える暗号技術の基礎を説明できる。	情報社会で生活する上でのマナー、モラルの重要性について説明できる。
情報セキュリティに基づいた情報へのアクセス方法を説明できる。	情報セキュリティを運用するための考え方と方法を説明できる。

MCC情報分野のセキュリティ項目　MCC Plusセキュリティ分野（一部）の到達目標

	到達目標	学習の目安となる項目
MCC	サイバーセキュリティの重要性を理解し，その必要性を説明できる	脅威・攻撃手法の多様化，サイバーテロ，暗号・セキュリティ技術の輸出入規制，リバースエンジニアリング
	ネットワークにおける安全な通信方法と，基礎的な環境構築に必要な技術を説明できる	通信の安全，ファイアウォール
	ネットワークの稼働状況や通信の証跡を確認する基礎的な対応方法を説明できる	ネットワーク解析，ログの分析
	ネットワークに接続したシステムで発生しうる脆弱性と，その診断・対策方法を説明できる	システムの脆弱診断，ペネトレーションテスト
MCC＋	ネットワーク層における一般的な攻撃手法について知っている	DoS攻撃、 DNS リフレクション攻撃
	ディジタルフォレンジックに関する調査技法（ツール、実施方法など）について知っている	ハードウェア、OS 、ネットワーク、フォレンジック、フォレンジックサポートツール(VMWare、Wireshark など)、デジタルフォレンジクスにおけるフットプリント、バイナリ解析、不揮発のデータの種類と収集
	セキュリティインシデントが発生した際に、ログなどの様々な情報を用いて、インシデントの原因を解明する方法について説明できる	システムログ、相関ツール、状況の把握・分類、解決策検討、インシデント検知
	ネットワークに接続したシステムで発生しうる脆弱性を理解し、診断・対策を実施することができる	脆弱性診断（ペネトレーションテスト等）、システムの脆弱性（バッファオーバーフロー、 XSS 、 SQL インジェクションなど）

国立高専セキュリティ教育の育成人材像とMCC/MCC Plus

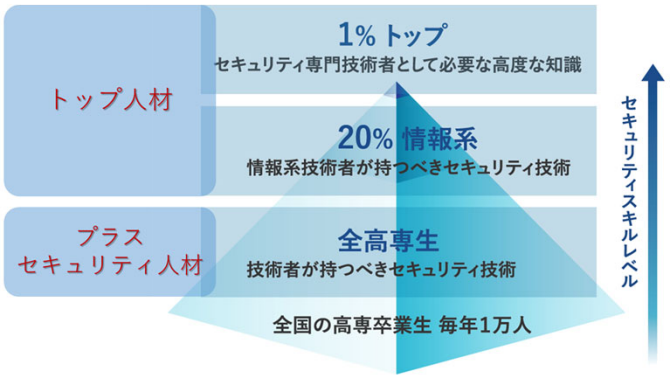


KOSENサイバーセキュリティ教育推進センター

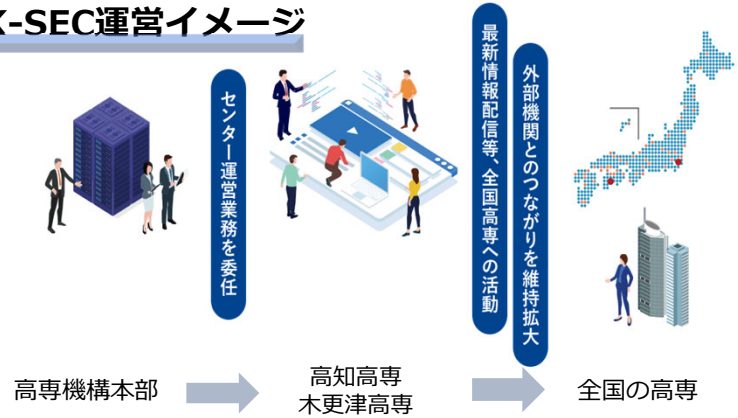
（K-SEC : KOSEN Security Educational Center）

設置：2023年12月（サイバーセキュリティ人材育成事業（旧K-SEC，2016～2023）を継承）
目的：高専で行われてきたサイバーセキュリティ教育を更に高度化し、(1) サイバーセキュリティ人材育成のためのエコシステム構築、(2) 産学連携による高度なサイバーセキュリティ教育とプラスセキュリティ教育の実践、(3) 地域企業との連携及び貢献のために、地域のサイバーコミュニティ等と高専の連携をこれまでの取組や、外部機関の連携を最大限に活かしつつ、組織的・一元的に推進するために設置
運営校：高知高専、木更津高専

高専が継続的に輩出する人材



K-SEC運営イメージ



＜ミッション＞
1.サイバーセキュリティ人材育成のためのエコシステム構築
　→到達目標（MCC、MCC Plus）の構築を通じた全高専展開（特にプラスセキュリティ人材）
2.産学連携による高度なセキュリティ教育のとプラスセキュリティ教育の実践
　→外部機関とのトップ人材育成と非情報系学科に対応したプラスセキュリティ人材育成
3.地域SECUNITY（セキュリティコミュニティ）の推進
　→地域連携、地域貢献等

KOSENサイバーセキュリティ教育推進センター
（K-SEC：KOSEN Security Educational Center）

取組事例

分野融合教育の実践（船×サイバーセキュリティ）

IoT&K-SEC 連携事業
海事サイバーセキュリティ演習

COMPASS5.0 サマースクール2024

- 低学年のセキュリティ初心者を対象に「CTF長入門講座」を開催
- セキュリティ人材育成の裾野を広げた

NECセキュリティエンジニアとの情報交換会

全国高専教員

- 全国高専教員とNEC専門技術者が定期的に情報交換を実施
- 最新のサイバー攻撃の動向やセキュリティトレンドを共有
- 毎月第3火曜日の17時からZoomにて開催中．どの分野からも参加可能．参加希望は木更津高専へご連絡ください．

NECによる女性エンジニアワークショップや最新動向提供

- NECグループの女性エンジニアとのキャリアワークショップ
- アプリの脆弱性診断を行うテクニカルワークショップ

https://jpn.nec.com/cybersecurity/topics/2024/20240920.html

産学官連携への取り組み

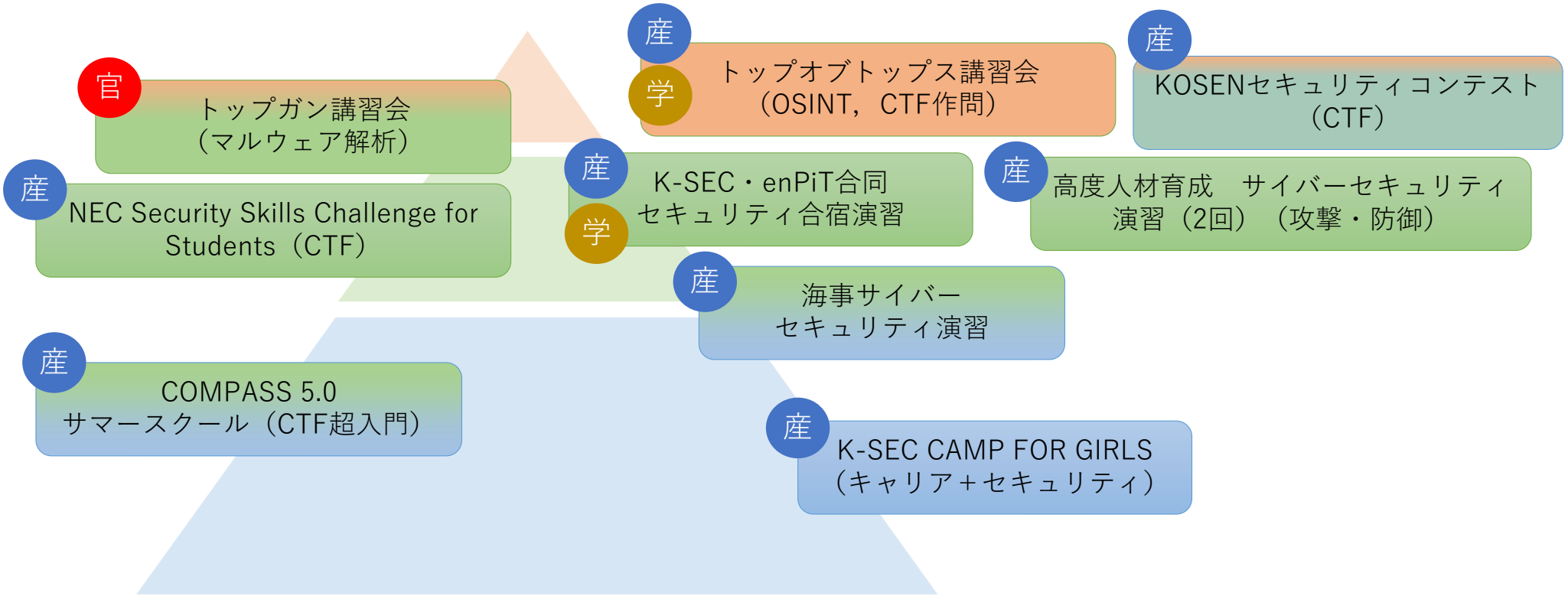
- 千葉県警とのサイバーボランティア連携の検討
- 日立製作所とのトップ人材育成の検討
- 防衛省・航空自衛隊と高専の連携検討
- 第14回おおた研究・開発フェアにてサイバーセキュリティ教材を紹介
- 順天堂大学健康データサイエンス学部・加藤教授とサイバーセキュリティ教育の連携について意見交換

高度人材育成「サイバーセキュリティ演習」

- サイバー攻撃の発見と防御の基礎学習を企業エンジニアがオンライン指導

産業界等との連携による学生向けイベント（2024年度の例）

参加者は全国高専から公募（トップオブトップス講習会は招待）



2026からの木更津高専のセキュリティ教育（コース新設）

支援2　高度情報専門人材の確保に向けた機能強化の構想について
令和6年度　高等専門学校　木更津工業高等専門学校

事業計画名　木更津工業高等専門学校における学修者と社会の期待に応えるサイバーセキュリティ教育推進基盤強化事業

基本情報	
改組内容	学科・コース等の設置・増員
所在地	千葉県木更津市
増員する情報系組織名	機械工学科, 電気電子工学科, 電子制御工学科, 環境都市工学科の4学科にプラスセキュリティコース, 情報工学科にAI・データサイエンス情報コースとセキュリティ情報コース
入学定員増数及び増員時期	【R8増員】改組前40名 → 改組後80名

＜社会や地域のニーズ・課題＞

1. 企業からの「情報処理技術者」,「専門技術＋セキュリティ技術を有する人材」輩出の要望, 千葉県警との連携教育からは「サイバーセキュリティ人材」の要望
2. 木更津高専「技術振興交流会」(約300社)からは、リカレント教育の要望
3. 地域産業界が抱える業務改善や技術継承に関する課題解決のための、AI・数理データサイエンスを駆使した協働教育や共同研究実施の要望
4. 地域社会の生涯学習機会の拡充に向けた、本校と自治体で締結している包括連携協定等を活用した一般市民向け最新の情報技術、セキュリティ技術の講習会開催の要望

＜学科等の体制強化の概要・コンセプト・特徴など＞

情報工学科には①AI・データサイエンス情報コース, ②セキュリティ情報コースの2コースを設置
① AI・データサイエンス情報コースでは, AI・データサイエンスの最先端かつ実践的技術を身につける
② セキュリティ情報コースでは高度なサイバーセキュリティ技術を身につける

機械・電気電子・電子制御・環境都市の4学科にプラスセキュリティコースを拡充設置
従来の4学科の基礎および専門科目にプラスセキュリティ科目を設け、専門技術＋情報セキュリティ技術を身につける

＜教育内容・育成する人材像＞

情報工学科
① コンピュータサイエンス・情報工学の知識を土台として、その上に情報分野の先端技術となっているAI・データサイエンス技術分野を切り開く<Top of topsの人材の育成コース
② ICT分野における高度なセキュリティ技術を身につけた人材の育成コース

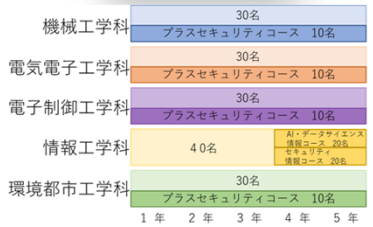
機械工学科, 電気電子工学科, 電子制御工学科, 環境都市工学科
各学科の基盤技術を身につけ、その分野において守るべき対象と方法を理解し、必要なセキュリティ技術を身につけたプラスセキュリティ人材の育成コース

＜初中段階・他大学・高専・企業・自治体等との連携＞

1. 「サイバーセキュリティ教育推進センター(K-SEC)」の運営校として、サイバーセキュリティの教育研究環境を整備し、全国高専と連携したセキュリティ人材の育成
2. K-SECの取組として、共同イベント/シンポジウム、サマースクール等を開催し、学生と企業人材との交流を通じたサイバーセキュリティ人材の育成
3. 横浜国立大学、情報セキュリティ大学院大学との連携、警察庁、千葉県警、NEC、三菱重工業等との連携を通じたK-SEC活動成果物を活用した高度情報専門人材の育成
4. 海外のモンゴルおよびタイの高専、ナンヤンポリテクニック、リパブリックポリテクニック等と連携したサイバーセキュリティに通じたグローバル人材の育成

＜女子学生、社会人学生、留学生等の確保＞

1. 女子学生確保
   女子学生の関心が高い分野の企業等と連携した授業の拡充
   キャリアパスについてOG等を活用した女子中高生や保護者向け説明会開催
2. 社会人学生確保
   大学、企業と連携した情報技術、セキュリティ技術に関する実践を重視した授業の開設
   専門分野および関連分野における情報セキュリティを活用した授業の開設
3. 留学生確保
   モンゴルおよびタイの高専、シンガポールのナンヤンポリテクニック、リパブリックポリテクニック等と連携した課題解決型インターンシップの実施



コースと育成人材像

プラスセキュリティコース
情報以外の4学科内に各10名

専門分野の基盤技術に加えて，各専門で必要なセキュリティ技術を身につけた，プラスセキュリティ人材

セキュリティ情報コース
情報工学科のうち20名

ICT分野における高度なセキュリティ技術を身に着けた人材

2026年度入学生のセキュリティ科目

科目	学年	非情報４学科		情報工学科		主な内容
		専門コース	セキュリティ	AI・DS	セキュリティ	
情報基礎	1	○	○	○		情報リテラシー
情報セキュリティ基礎	2	○	○	○		リテラシーレベルのセキュリティ
情報セキュリティ演習A	3		○	△		LINUX等の必要スキル修得
情報セキュリティ演習B	4	△	○	△	○	攻撃／防御演習等
情報セキュリティ演習C	5	△	○		△	IoTセキュリティ
総合セキュリティ	5	△	○	△	○	法，心理等を含む多面的なトピック
情報セキュリティI	4			○	○	攻撃／防御演習等
情報セキュリティII	4			△	○	攻撃／防御演習等
科目数		○2　△3	○6	○3　△4	○6　△2	

★　○必修科目　△選択科目

★　情報工学科は４年次からコース分け

★　　外部人材（セキュリティ技術者・研究者）による講義

高専での人材フレームワーク活用

- 高専卒業生に期待される人材像
  - 企業等のニーズを知りたい
    ⇒　人材フレームワークを介して採用側と学校側の認識すりあわせ
    - 業種別・職種別のニーズ
      - セキュリティ企業，情報系企業，製造業…
        それぞれの業種でどんなセキュリティ人材が求められている？
      ※ 現状で「セキュリティエンジニア」職の求人は少ない
- 高専 MCC・MCC Plus の指針
  - 高専生が習得すべき知識・スキルとレベル
    ⇒　MCC＝ミニマムスタンダードでカバーすべき項目とレベル
      - 高専でセキュリティにあてられる授業時間数は概して多くない　⇒　項目・レベルの精査
      - 変化の速いセキュリティ分野では不断の見直しが必要
  - MCC Plus をベースとした学校ごとの特徴あるカリキュラムの設計と評価
    例：職種の要求スキルのカバー率
- セキュリティ教育の認定制度
  - 高専＋大学のセキュリティ教育プログラム（またはプログラム修了生）の認定制度の設計に活用