東京工業大学における
サイバーセキュリティ教育の取り組み

田中 圭介
東京工業大学 情報理工学院
サイバーセキュリティ研究教育センター

第8回ワークショップ「データサイエンスにおける
サイバーセキュリティ教育事例」
2024年3月22日

サイバーセキュリティ特別専門学修プログラム

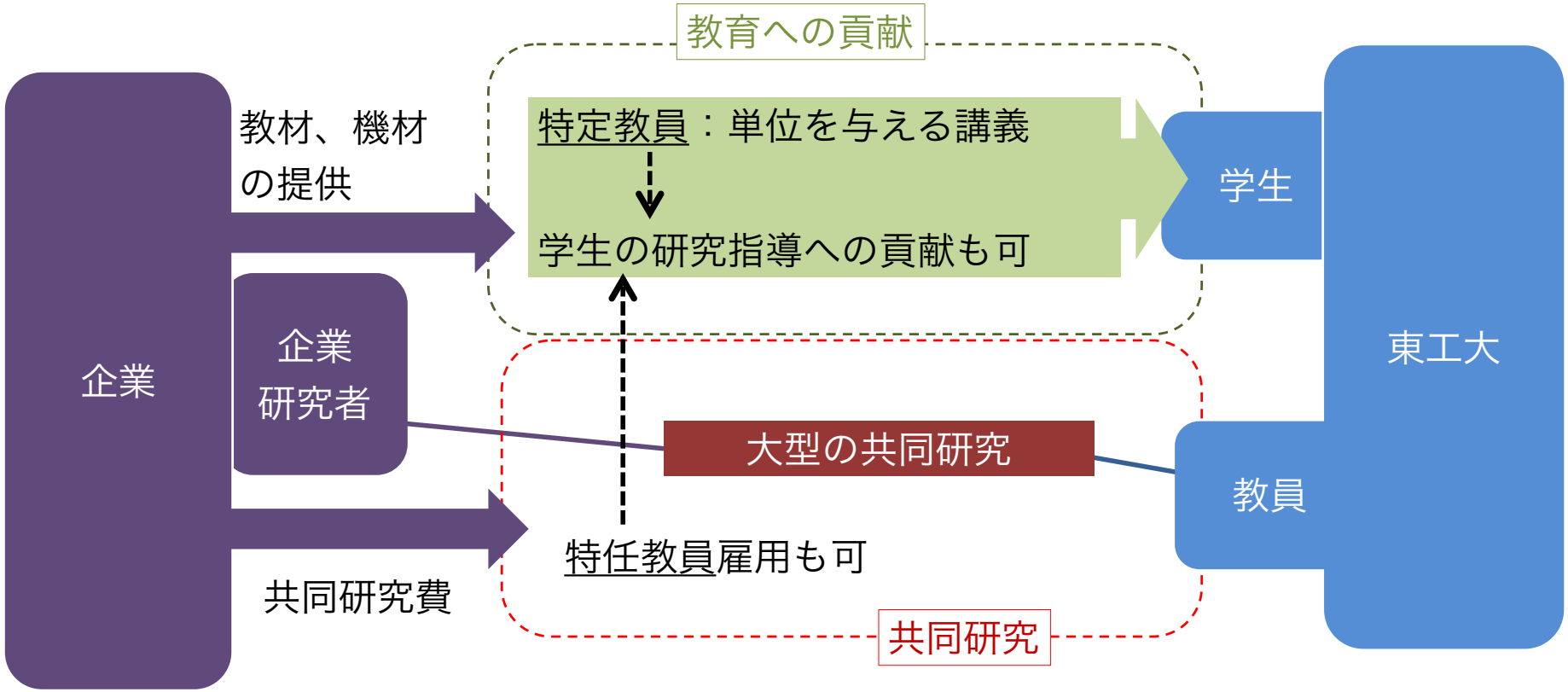
- 東工大の大学院特別専門学修プログラムの制度を利用
- サイバーセキュリティの実践的な内容を学ぶとともに、東工大の情報・通信分野の特色である理論分野の強みも活かし、理論的背景にある知識も同時に学ぶ
- NRI、楽天、NTT、産総研、内閣サイバーセキュリティセンターが協力
- 本日は、プログラム設置の経緯、東工大教育研究共創スキーム、カリキュラムの設計ポリシー、コアカリキュラム、授業内容を紹介します

特別専門学修プログラム設置の経緯

- 2015年2月: 東工大のサイバーセキュリティ分野に関連する教員17名が定期的に集まりグループを組織
- 2月: 経団連「サイバーセキュリティ対策の強化に向けた提言」
- 5月: サイバーセキュリティ研究推進体を学内に設置
- 6月: NRIから東工大への教育・研究協力の打診
- 9月: 楽天、NTT、産総研、NICTとテスト教育イベントの開催
- 2016年4月: NRI・東工大 サイバーセキュリティ教育研究共創プログラム、および、サイバーセキュリティ特別専門学修プログラムの設置
- 2017年4月: 情報理工学院サイバーセキュリティ研究センターの設置
- 2022年4月: 情報理工学院サイバーセキュリティ研究教育センターへ名称変更

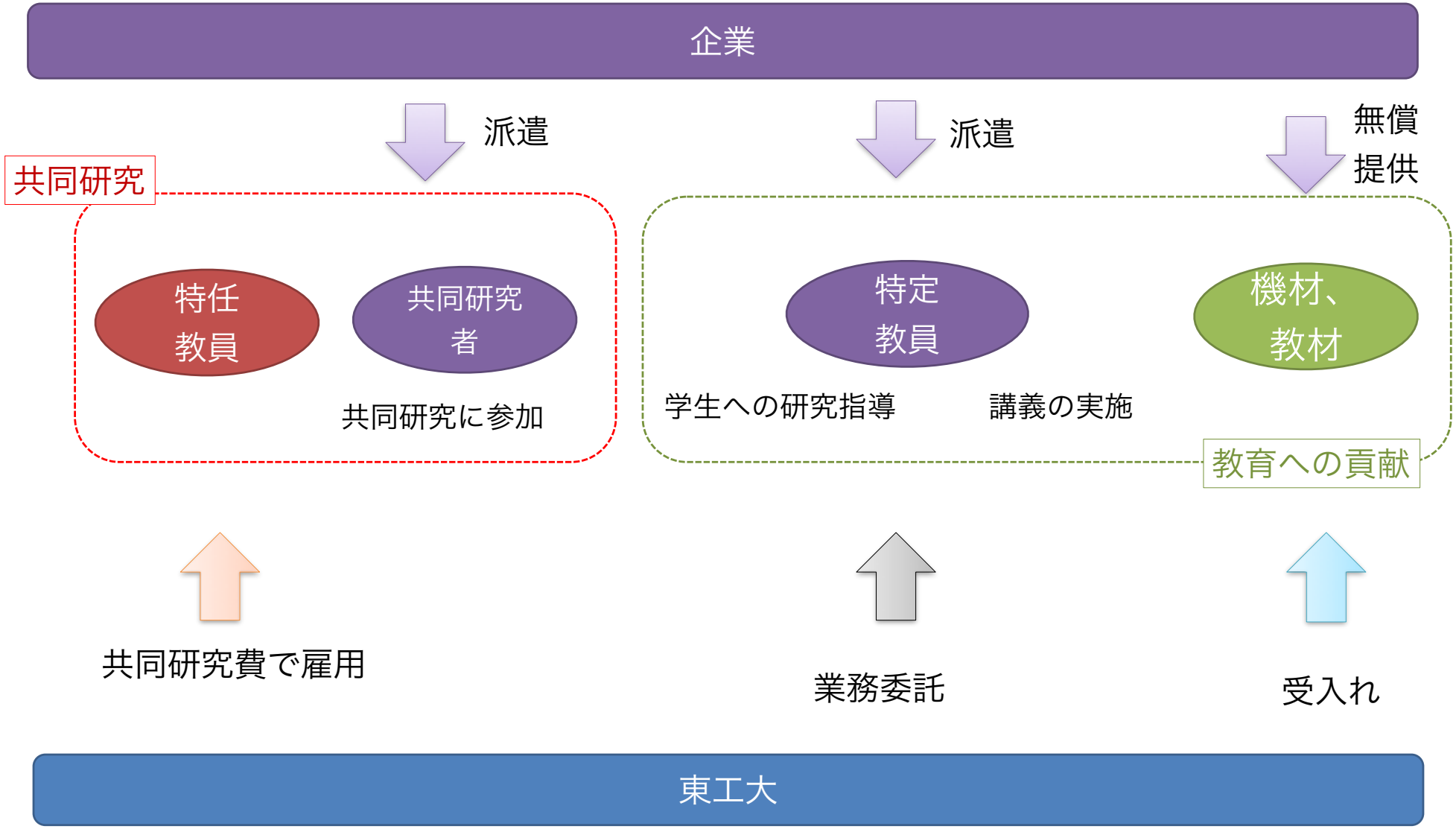
テスト教育イベントの様子
サイバーセキュリティ オータムスクール 2015年9月13-15日 箱根湯本ホテル

教育研究共創スキームのフレームワーク

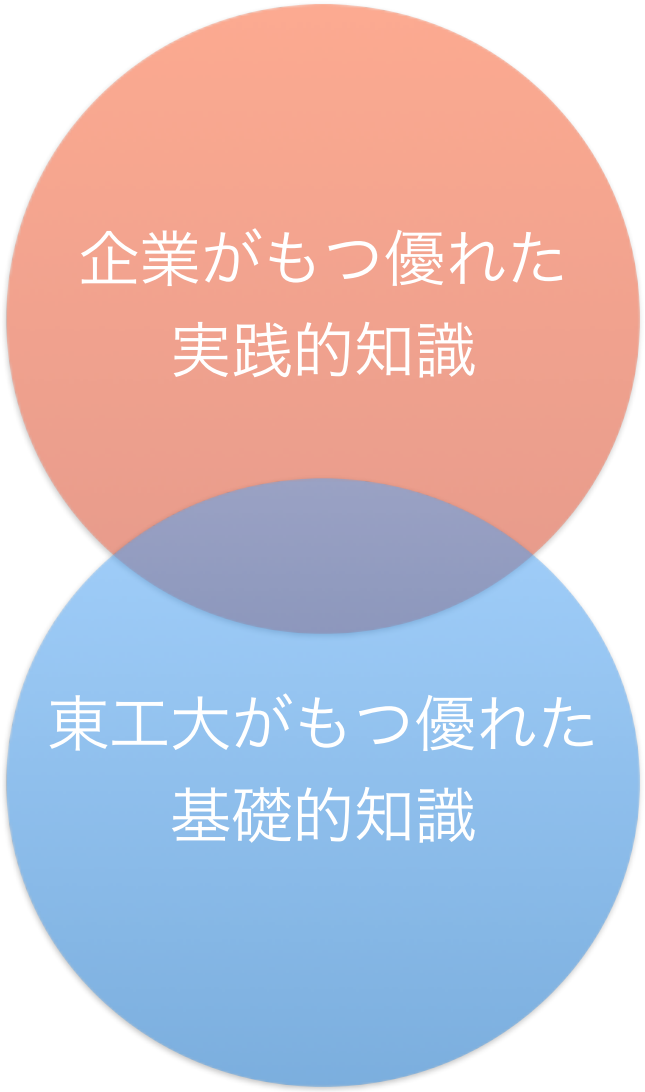


- 講義: 年間4単位以上
- 共同研究費: 年間1000万以上

教育研究共創スキームにおける契約関係



カリキュラムの基本コンセプト



- 東工大で用意している大学院特別専門学修プログラムの制度を利用
- 6科目12単位分のコアカリキュラム
  - 大まかには4科目12単位で修了できる
- 実践的知識と基礎的知識の相乗効果
  - 特に、基礎的知識を重視
- 短期的ではなく長期的な視点からの教育
- トップガンではなく橋渡し人材
- 東工大情報系学部卒業生レベルを想定
  - 授業の一部は情報分野以外の学生も理解しやすく設定
- 持続性を重視

コアカリキュラム

- サイバーセキュリティ概論（１Ｑ，２-０-０）
- サイバーセキュリティ暗号理論（３Ｑ，２-０-０）
- サイバーセキュリティガバナンス（３Ｑ，１-１-０）
- サイバーセキュリティ攻撃・防御第一（２Ｑ，１-１-０）
- サイバーセキュリティ攻撃・防御第二（2-３Ｑ，１-１-０，合宿形式を含む）
- サイバーセキュリティ攻撃・防御第三　（４Ｑ，１- １- ０）

の6科目を中心とする特別専門学修科目から構成

暗号理論が提供する機能

DNS
ホスト名
DNS (Domain Name System)

コアカリキュラム (1): サイバーセキュリティ概論

- 第1回: 講義全体の概要 (安永 憲司 (情報理工学院))、および、サイバーセキュリティの基本的概念 (松浦 知史 (学術国際情報センター))
- 第2回: ネットワークセキュリティの基礎 (北口 善明 (学術国際情報センター))
- 第3回: サイバーセキュリティの基盤理論としての暗号理論と計算の複雑さ (安永 憲司 (情報理工学院))
- 第4回: サイバーセキュリティの基本要素としての暗号理論 (尾形 わかは (工学院))
- 第5回: サイバーセキュリティにおける認証認可 (友石 正彦 (学術国際情報センター))
- 第6回: 並行システム、および、そのセキュリティ (西崎 真也 (学術国際情報センター))
- 第7回: ウェブセキュリティ (南出 靖彦 (情報理工学院))
- 第8回: マルウェア検知とIoTデバイスセキュリティ (一色 剛 (工学院))
- 第9回: 耐侵入コンピュータシステム (Xavier Defago (情報理工学院))
- 第10回: 暗号通貨・ブロックチェーン技術とサイバーセキュリティ (田中 圭介 (情報理工学院))
- 第11回: サイバーセキュリティにおける不正侵入検知 (小池 英樹 (情報理工学院))
- 第12回: 監視制御システムに対するサイバーフィジカルセキュリティ (石井 秀明 (情報理工学院))
- 第13回: セキュリティ情報の可視化技術 (脇田 建 (情報理工学院))
- 第14回: 形式的手法とセキュア・コンピューティング (渡部 卓雄 (情報理工学院))

コアカリキュラム (2)

- サイバーセキュリティ暗号理論
  - 協力: NTT、産総研
  - サイバーセキュリティの基本要素としての暗号理論
  - 特に、暗号理論におけるモデル、方式、安全性証明手法

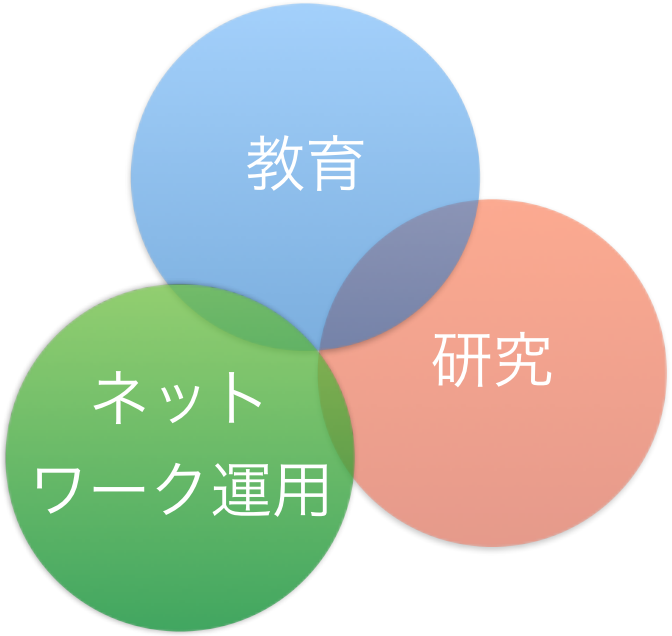
- サイバーセキュリティガバナンス
  - 協力: 内閣サイバーセキュリティセンター
  - 情報セキュリティに関わる管理施策の基本的なフレームワークを理解し、セキュリティに配慮した企業統治のための方法を習得
  - 情報セキュリティに関する計画の立案や、経営層への提言、支援、報告に関する方法の習得
  - ケーススタディでは、講師の実際に担当した事例も用いて「CISOは、どうあるべきか」、「スタッフは、どのようにCISOを支援すればよいか」を考える

コアカリキュラム (3)

- サイバーセキュリティ攻撃・防御第一
  - NRI
  - IT技術を情報セキュリティの側面からとらえる
  - システムやネットワークの開発・運用等において考慮すべきセキュリティの要素技術やその活用方法を習得
- サイバーセキュリティ攻撃・防御第二
  - 楽天
  - 3日間の合宿形式授業
  - 企業に関わる情報セキュリティの取り組み事例の紹介
  - Webセキュリティとフォレンジックに関するスキルの習得
- サイバーセキュリティ攻撃・防御第三
  - NRI
  - Web アプリケーションへの攻撃と防御方法
  - セキュリティに配慮したシステム開発・ネットワーク運用
  - インシデント対応時の調査手法 (フォレンジック) の基礎知識と調査手法

サイバーセキュリティ攻撃・防御第一・第二・第三の内容

- Webアプリケーションセキュリティ基礎
  - Webサイトの脆弱性に関する現状
  - セキュリティ診断の結果から
  - Webアプリケーションの仕組み
  - セッションIDの基礎
  - データの送受信の基礎
- 入出力値に関するもの
  - クロスサイトスクリプティング
  - SQLインジェクション
  - ディレクトリトラバーサル
  - コマンドインジェクション / ファイルアップロード
- ユーザ認証
  - 認証の種類と基本的な考え方
  - 認証に対する攻撃と対策
  - パスワードリマインダに対する攻撃と対策
- セッション管理
- アクセスコントロール
  - 権限昇格と対策
  - なりすましと対策
- ファイルシステム
  - 物理構造、バイナリデータ、ファイルシステム、FAT、NTFS、ディスクイメージ、暗号化
- メモリフォレンジック
  - メモリ、プロセス、ライブラリ、プロセス管理オブジェクト、メモリイメージ
- Windowsアーティファクト解析
  - ファイルカービング (削除ファイル復元、リストア機能)
- アンチフォレンジック
  - rootkit、タイムスタンプ
- フォレンジックツール
  - フォレンジックツール、IOC
- マルウェア解析

おわりに

- サイバーセキュリティでは、攻撃もAIを用い、防御もAIを用いるのが現在では普通
    - 数理・データサイエンス・AI教育を学生の研究室配属までに行ってもらうことは研究室でのサイバーセキュリティ研究の大きな助けになる
- セキュリティ人材に求められる具体的スキルも時代ともに変化していると考えられるが、基礎的な知識と能力をもった人材の重要性は変わらない
- 三日間の合宿形式授業では、学生や、企業からの講師、東工大教員同士でサイバーセキュリティ教育を含む様々な内容について意見交換ができ、おすすめです
- サイバーセキュリティ研究教育センターでは、大学における研究、教育、ネットワーク運用分野を一体的に考え、利点は大きい