組織間連携による セキュリティ人財育成の 15年

砂原秀樹
慶應義塾大学
大学院メディアデザイン研究科 教授/
サイバー文明センター内
サイバーセキュリティ研究センター センター長

自己紹介

- インターネット研究
  - 1984年～1994年
    - JUNET
  - 1988年～現在
    - WIDE Project
- InternetCAR/InternetITS
  - 1996年～
- Live E!
  - 2005年～
- 情報銀行
  - 2013年～
- Software Defined Media
  - 2014年～
- Cybernetic Being
  - 2023年～

インターネットの叔父

インターネットの父

組織間連携によるセキュリティ人財育成

- セキュリティ人財
  - セキュリティ業務に関わる人財
  - セキュリティも理解する人財
- セキュリティ人財育成の課題
  - 理解するべき知識が多い
    - Computer Science関連知識
      - 数学(暗号、情報理論)、アーキテクチャ(アセンブラを含む)、オペレーティングシステム、プログラミング言語、コンパイラ構成論、アルゴリズム等
      - 最近では、AIや量子コンピュータなどの知識も必要
    - その他の知識
      - 法律、経営、心理学、倫理、最新情報の取得、現場でのオペレーション
  - 教育に携わることができる人財の不足
    - 各組織に少数の人数が所属
      - 専門がそれぞれ異なり、各組織に所属する人財のみではセキュリティ人財育成が難しい
- 複数の組織による連携人財育成

大学連携によるセキュリティ人材育成

大学院(修士課程)

2008～
(2007-2011)

IT Keys

NAIST

ISS Square

情セ大

2013～
(2012-2016)

SecCap

情セ大(enPiT全体は阪大)

2017～
(2016-2020)

Basic SecCap

東北大

学部(3,4年)
高専(本科4,5年)
(専攻科)

社会人(学び直し)

2018～
(2017-2021)

ProSec

情セ大

3つの知識の獲得

総合的知識

情報セキュリティに関する最新知識と法律面・倫理面・経営面などの実務に必要な知識

スキル・経験的知識

繰り返しセキュリティインシデントを体験することによる経験的知識、現場での実践的知識

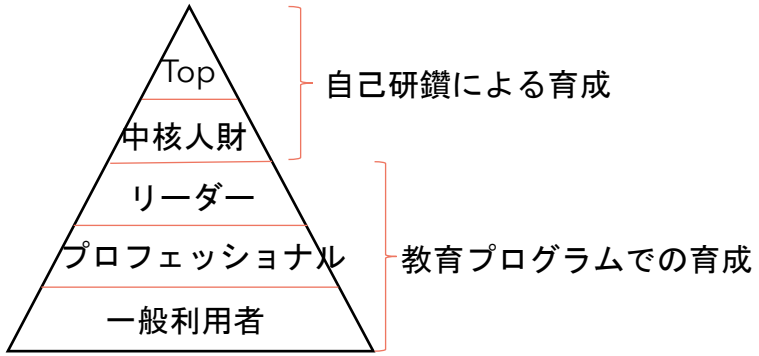
実践的セキュリティエンジニア

体系化された基礎知識

実践的な情報セキュリティ問題に関連した課題研究(修士論文に限定しない)

セキュリティ技術を体系立てて理解するためのネットワークを中心としたコンピュータサイエンスの知識

セキュリティ人財



課題
- 倫理感の醸成
- グローバル感覚
- 嗅覚
- 評価

トップ人財、中核人財の育成

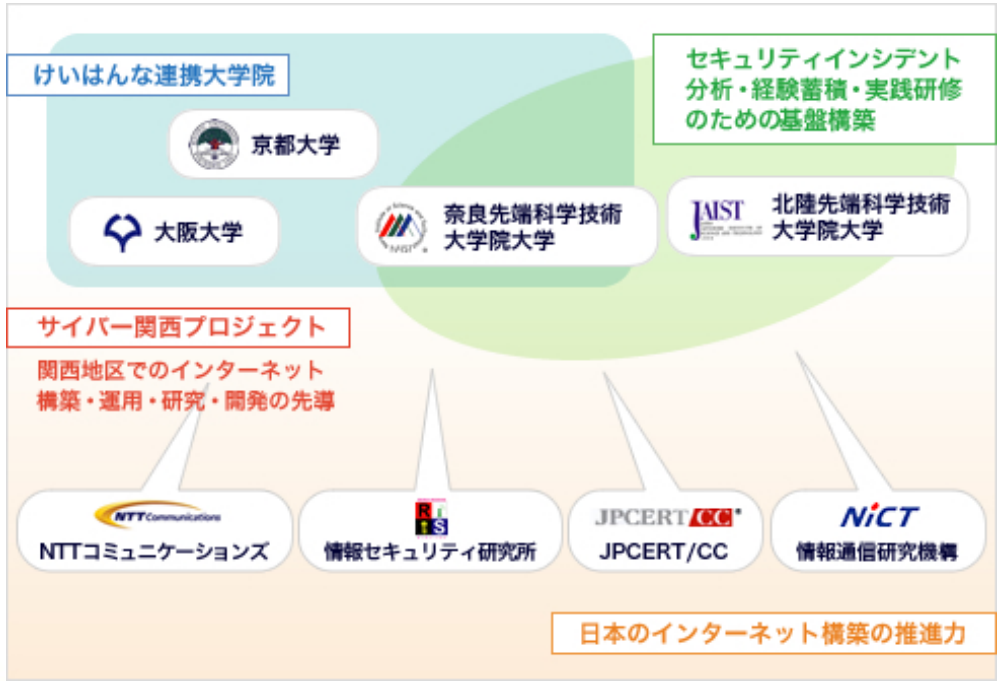
リーダーシップ人財

セキュリティの知識を持ったプロフェッショナル

正しいセキュリティの知識を持った一般利用者

IT Keys プログラム

- 文部科学省　平成19年度「先導的ITスペシャリスト育成推進プログラム」
  - 社会的ITリスク軽減のための情報セキュリティ技術者・管理者育成
  - IT-KEYS (IT specialist program to promote Key Engineering as securitY Specialist)
    - 情報セキュリティ対策の立案遂行を主体的に実施しうる実務者の育成
- 組織



2009年度
情報セキュリティ運用リテラシー

1. 猪俣敦夫　奈良先端科学技術大学院大学
   - 情報セキュリティ・運用リテラシーの概要からセキュリティリスク、国際標準、暗号危殆化問題、 情報セキュリティと法について、情報セキュリティ運用リテラシー講義を学ぶにあたっての知識習得
2. 歌代 和正　JPCERT/CC・代表幹事
   - 企業・組織で業務を適切に実行していく上で必要な知識とセキュリティ管理で必要なTipsを紹介し、体系化を目指す
3. 永見健一　(株)インテック・ネットコア取締役CTO
   - インターネットの現状やその構造を振り返り、世界そして日本のネットワーク統計情報を交えながら現状のインターネットの在り方と問題点についての把握と理解
4. 平林　実　NTTコミュニケーションズ（株）セキュリティマネジメント室 担当部長
   - 1組織として、特にNTTコミュニケーションズ(株)における情報セキュリティの状況と取り組みについて知る
5. 小山　覚　(株)NTTPCコミュニケーションズ 執行役員
   - 企業を取り巻く情報セキュリティの現状と課題について知る
6. 高橋 郁夫　IT法律事務所　弁護士
   - 昨今のサイバー犯罪事例をもとに裁判の判例などを紹介し、法律という視点からセキュリティマネジメントについて学ぶ
7. 丸山 満彦　監査法人トーマツ
   - IT内部統制について理解するために、財務報告の信頼性評価とIT内部統制について学習する。さらにIT内部統制の枠組みである「COBIT」について取り上げ、現状の問題点から議論する
8. 高木 浩光　産業技術総合研究所
   - インターネットで利用されている認証基盤のリスクを実例を取り上げて、その脆 弱性と対策について学習する。現代の情報社会において、リスクを考慮した本物 のセキュリティの在り方を模索する
9. 阪本　泰男　内閣官房内閣審議官・情報セキュリティセンター副センター長
   - 大学院生に知っておいて欲しい政府の役割と情報セキュリティの在り方

情報セキュリティ運用リテラシー （座学）

京都大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、大阪大学中之島キャンパス(講義会場)を結んだオンライン講義を実施。技術的知識だけでなく、社会的背景を考慮した情報セキュリティリスクマネージメントについての理解を目指す

最新情報セキュリティ特論

1.岡部寿男　京都大学

- PKI（公開鍵暗号）、IDS、ファイヤーウォールの仕組み、セキュリティリスク、ISMSの基礎等、最新情報セキュリティ特論を学ぶにあたり必須の基礎知識等の習得を目指す

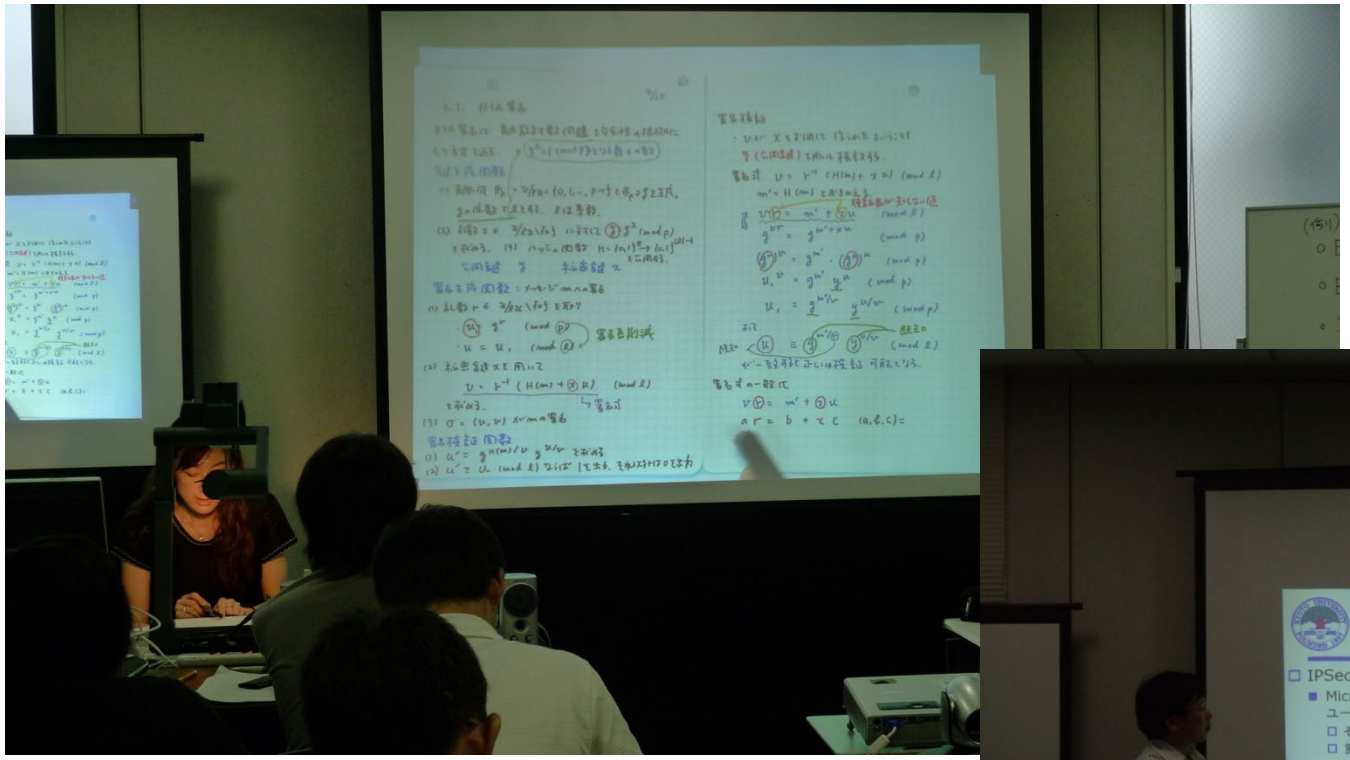
2.宮地充子　北陸先端科学技術大学院大学

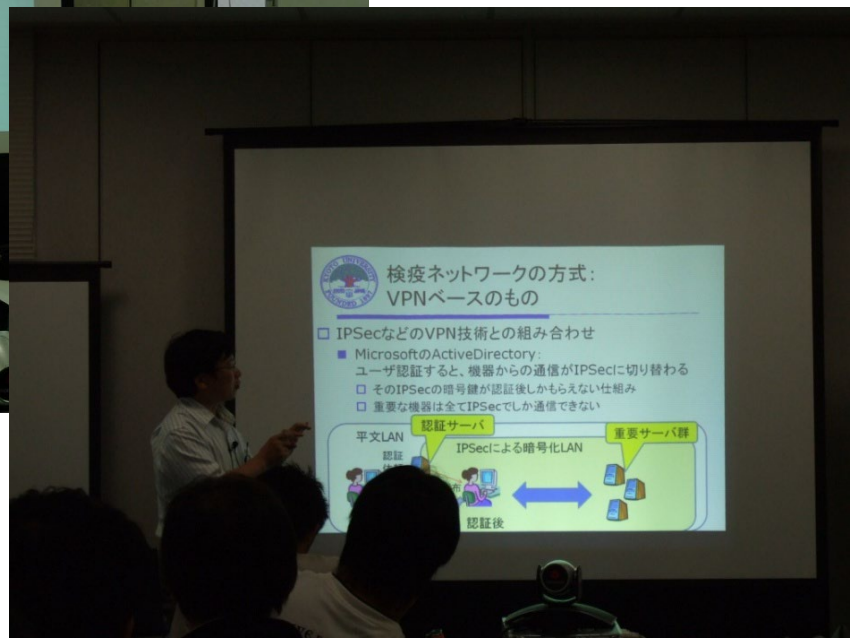
- 代数論の基礎、公開鍵暗号、デジタル署名の理論的仕組み、楕円曲線暗号の安全性について、主に暗号理論の習得を目指す。さらに、Mathematicaを利用して、暗号プロトコルの実装を行い、その仕組みを理解する

3.高倉　弘喜、上原哲太郎　京都大学

- ネットワークにおける管理技術とセキュリティ、攻撃の振る舞いの基礎について学習し、ネットワーク運用者としてその障害対応や対策手法を体系的に習得することを目指す

最新情報セキュリティ特論（座学）

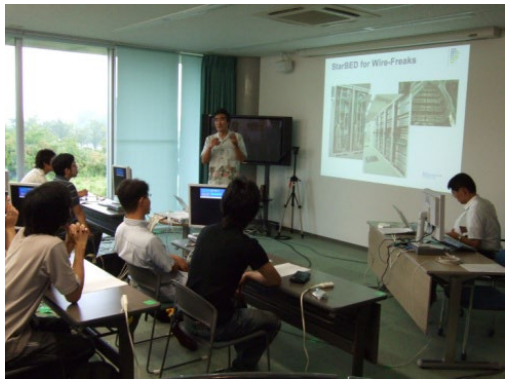




初等代数論から楕円曲線暗号など基礎から応用まで含めた暗号に関する理論的知識を習得する。また、ネットワークセキュリティとして基礎技術から運用者視点からのマネージメント技術など幅広い知識の習得をめざす

実践科目群（演習）

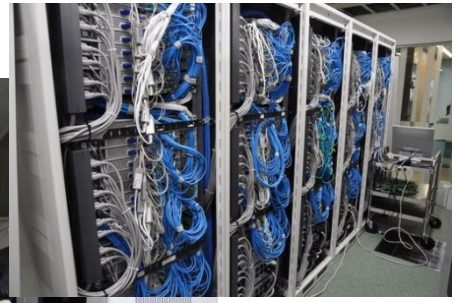
- 無線LANセキュリティ
  - 日程: 2009/6/13-14
  - 場所: 大阪大学：大阪府吹田市
  - 担当：　大阪大学
- インシデント体験演習
  - 日時: 2009/8/31-9/2
  - 場所: NICT北陸リサーチセンター:石川県能美市
  - 担当：門林雄基、樫原茂、篠田陽一、NICT北陸リサーチセンター
- リスクマネージメント演習
  - 日程: 2009/9/15-18
  - 場所: Telecom ISAC (Cyber Clean Center:CCC)：東京都港区
  - 担当：JPCERT/CC、IPA、TelecomISAC、NTTコミュニケーションズ
- IT危機管理演習
  - 日程: 2009/9/24-26
  - 場所: 和歌山県立情報交流センター（big-u)：和歌山県白浜町
  - 担当：NPO法人 情報セキュリティ研究所、和歌山大学、京都大学
- システム攻撃・防御演習　／　システム侵入演習
  - 日程: 2009/6/27-28　・　2009/11/21-22
  - 場所: 大阪大学：大阪府吹田市
  - 担当：　大阪大学



インシデント体験演習@北陸

- 独立行政法人　情報通信研究機構(NICT)北陸リサーチセンターの大規模汎用ネットワーク実証実験施設StarBEDを用いたセキュリティテストベッド上で、現実的な規模と複雑さを持つサイトへの様々な攻撃と、それらに対する監視・分析・防御・回避・復旧等の技術を習得
- 特徴
  - 本物のコンピュータウィルスの検体を用いたサイバー攻撃の仕組みを実践的に体験することが出来る

インシデント体験演習@北陸



掲載記事%インシデント体験演習

NTTコミュニケーションズ　経営課題とICT（ITトレンド）
「日本人だからこそできる「セキュリティ立国」に向けて

2009年1月22日　ITmedia エンタープライズに掲載
「標的型攻撃に備えよ！ただし抜本対策は見つからず」

リスクマネージメント演習@東京

- 情報セキュリティの現場において、予防対策や不正アクセス事故発覚時の対処（情報収集、関係各所との連携など）について、さらに動的マルウェア解析などより実践的な状況に即した体験的な学習を行う
- 特徴
  - 定常的に発生する不正攻撃やボット等の悪意のあるプログラムの振る舞いを、機械語レベルで仕組みを理解し、稼働中のシステムから問題を早期に発見するためのテクニックについて、その経験的手法を学ぶ

IT Keysスケジュール

2008年9月9日

	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	
9月16日（火）	準備	オリエンテーション（自己紹介、生活回り、注意事項等）10:30～ CCC概要説明(T-ISAC-J)	感染＆分析演習（T-ISAC-J）	休憩	感染＆分析演習（T-ISAC-J） ・4チーム ・実習 ・9月19日に発表				予備（発表準備、まとめの時間）	赤坂環境 赤坂会議室は期間中確保 インターネット環境有り 持ち込みPC使用可（指定場所） 入館は期間中許可設定 食事等は館外
9月17日（水）	準備	静的解析演習（JPCERT/CC）		休憩	静的解析演習（JPCERT/CC） ・4チーム ・実習 ・9月19日に発表			CCCの活動説明（T-ISAC-J）（4Fセミナールーム） ・H19年度成果等 マルウェア調査研究トピック（T-ISAC-J）	予備（発表準備、まとめの時間）	
9月18日（木）	準備	ウイルス等ネットワークにおける脅威の変遷と対策（IPA）（千石） ・説明 ・デモ		休憩 ・移動（30分）	セキュリティ関連企業見学 ・トレンドマイクロ社（新宿）13:30-15:00 ・LAC社（神谷町）15:30-17:00 ・各1時間～1.5時間程度見学＆説明 ・移動時間1.5時間程度				予備（発表準備、まとめの時間）	懇親会 （永田町：海運クラブ） ・18:30-20:30 ・立食形式
9月19日（金）	準備	発表準備		休憩 ・移動（15分）	発表準備（13:00-13:20） 発表（13:20-16:00） （虎ノ門：新虎ノ門実業会館） ・40分×4チーム ・感染＆分析演習＋静的解析演習			意見交換会 ・CCCへの提案 ・Q&A ・感想など	予備	

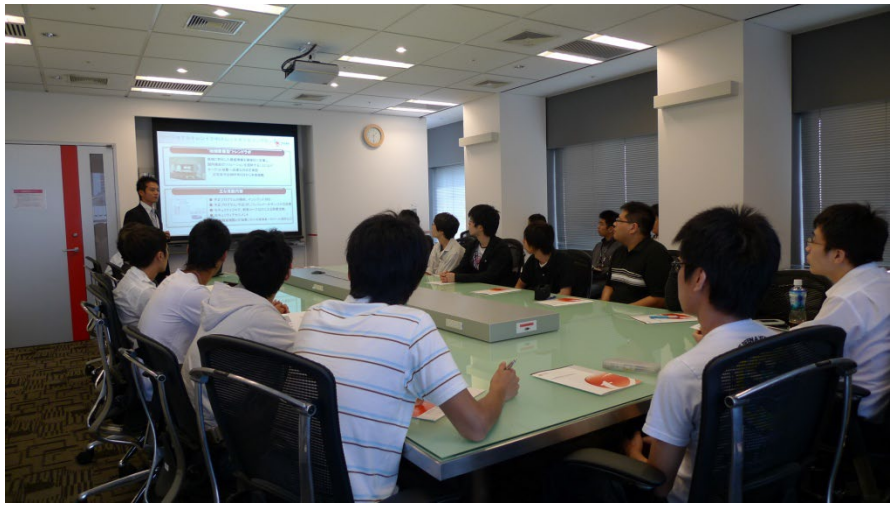
※黄色枠は赤坂会議室、橙色枠は4階セミナールーム、緑色枠は外部

リスクマネージメント演習@東京

外部機関で演習を行うために、受講生自身に
NDA（秘密保持契約）を理解してもらった上で実施

動的にマルウェアを機械語レベルで解析

リスクマネジメント演習@東京



トレンドマイクロ株式会社

LAC株式会社

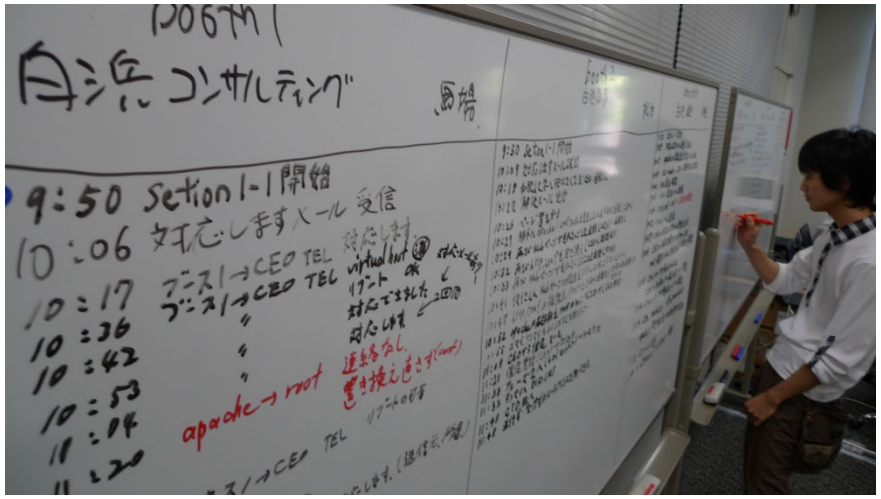
独立行政法人
情報処理推進機構(IPA)

各所、活発な質疑応答
受講生の関心度の高さ

IT危機管理演習@白浜

- 実際に起きうるインシデントとその事後処理について、情報システム管理者の立場でのロールプレイング形式での演習を行う
  - 各グループごとに仮想の1組織のネットワーク部署担当者として、ネットワーク障害などの技術対応だけでなく想定外の危機管理への対応など幅広い実践的な業務を体験し、運用者として様々なリスクへ対応できるようにすることを目指す

IT危機管理演習@白浜



実習オペレーションセンター
by 情報セキュリティ研究所、和歌山大学

受講生によるインシデント対応の場面

IT危機管理演習（白浜）

- ISS Squareとの連携
  - 情報セキュリティ大学院大学、東京大学、中央大学から合計6名の学生が参加し、IT-Keysの学生と一緒に合計30名での演習
  - 学生同士の大学を越えた新たなコミュニティの結成

CEOに向けた最終報告会

ISS Square中央大学
趙教授による質問

３つの演習@大阪大学

- 無線LANセキュリティ演習
  - 無線LANにおけるセキュリティ対策の現状を把握し、より安全に無線LANを利用するための対策を検討する
    - グループごとに異なる無線LAN機器によるネットワークを構築し、無線LAN上に流れているトラヒックを観測し、攻撃や盗聴について学ぶ
- システム侵入解析演習
  - 侵入されたシステムを発見したときの対処法について学習する。特に、システムで保持している情報漏洩の可能性やその対処法について検討する
    - 様々なポートスキャン攻撃を受けたときに送受信されるパケットを解析し、攻撃者の振る舞いを観測する。これによりポートスキャンを受けていることや、どのように攻撃の前兆を検出できるかの検討をグループごとに行う
- システム攻撃・防御演習
  - 脆弱性のあるシステムをインターネットに接続した場合、どのように攻撃されるのか、攻撃に対してどのように防御するのか等について学習する
    - セキュリティホールを利用した攻撃プログラムのソースコードを読み、攻撃の原理を理解する。実際に攻撃プログラムを実行し、攻撃が成功することを確認する。実際に、本物の各種攻撃ツールを用いて実験環境上のシステムペネトレーションテストを行い、発見された脆弱性への対策について検討を行う

無線LANセキュリティ@大阪大学

グループ検討課題一例

次のことについて調査・考察せよ。

1. アクセスポイントがもつ各種セキュリティ機能について調べ、それらの機能により本演習で行った攻撃（アクセスポイントへの侵入、DoS）が防げるか否かを確認せよ。
2. アクセスポイントがもつセキュリティ機能で防げなかった攻撃について、どのような対策が考えられるか？
3. WEP キーの解析に必要なパケット数、時間はどのくらいか？
   また、WEP キーが解析される危険性は、現実的にあるといえるか？
4. DoS 攻撃が成功したとき、攻撃を受けたアクセスポイントや端末はどのような動作をしていたか？送出されたパケットをキャプチャして解析せよ。

ISS Squareとの連携

CSS2009のセッションにてISS Squareとの連携成果の発表

ISS Square特別講義の遠隔講義（IT-Keysの4拠点にて遠隔受講）
各拠点の受講者ごとに議論を実施、評価のフィードバック

IT-Keysが目指す像

- 大学を越えた人的ネットワークの形成

第1期生の修了証授与式にて

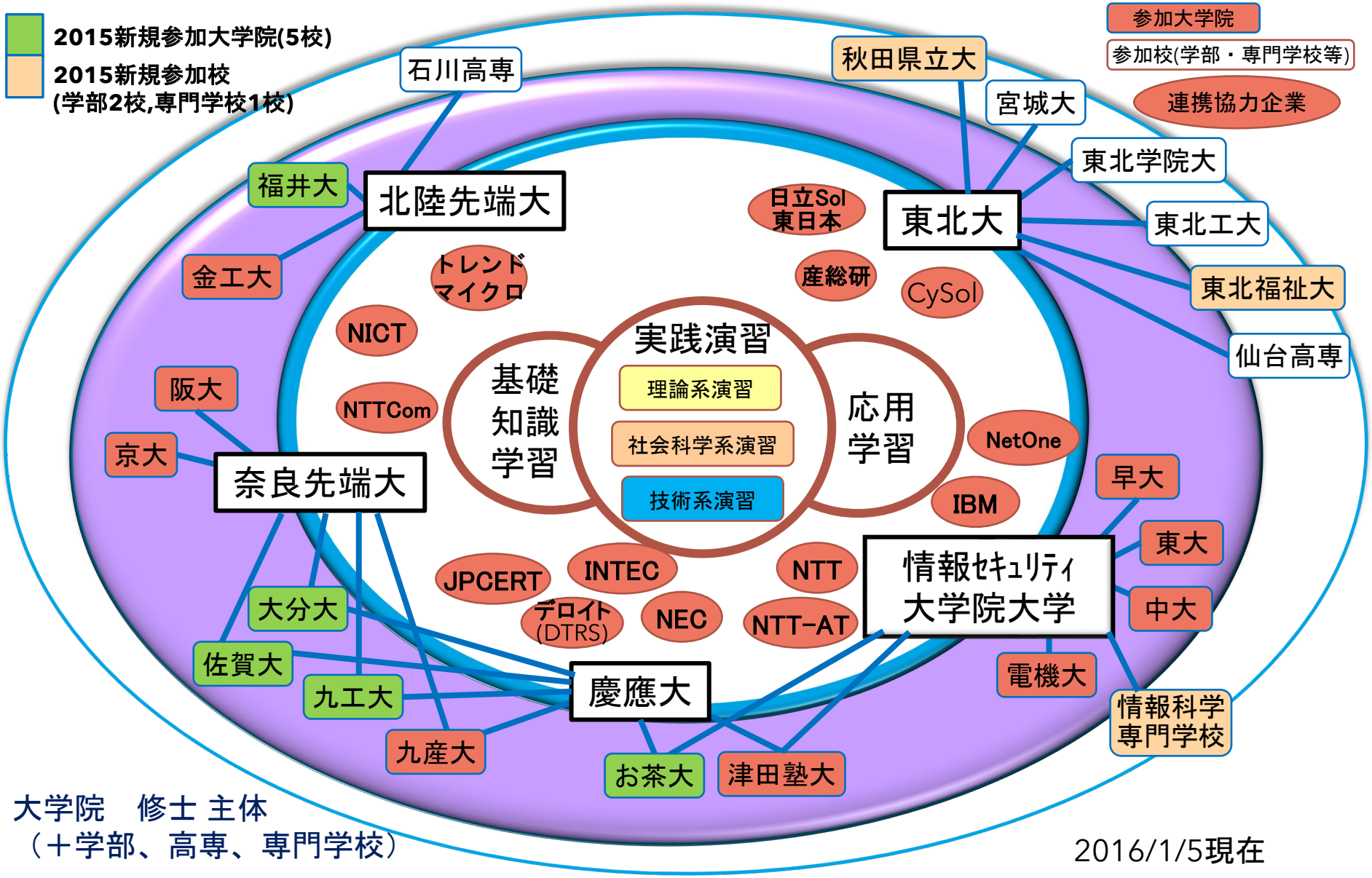
第2期生インシデント体験演習(北陸)にて

enPiT-Secuirty (第1期)

- 幅広い産業分野において求められている「実践的なセキュリティ技術を習得した人材（実践セキュリティ人材）の育成
- 実践セキュリティ人材：社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を，技術面・管理面で牽引できる実践リーダー
  - IT産業においてセキュリティ要求レベルの高いプロダクト開発に携わるIT技術者
  - ユーザ企業のIT部門において，セキュリティベンダーと協力して，自社のセキュリティシステムを構築できる技術者
  - CIO，CISOとして，組織のセキュリティ経営を担う経営者
  - IT技術者を育成する教育機関（大学，専門学校など）の教育者，等

参加大学，協力企業・組織との密な連携による講義と実践演習

SecCap



大学院　修士 主体
（＋学部、高専、専門学校）

2016/1/5現在

連携5大学が共同で開講：SecCapコース（2015年度）

暗号技術，Webサーバ・NWセキュリティから，法制度やリスク管理まで幅広く最新技術と知識を具体的に体験を通して習得

基礎知識学習

- 共通科目: **情報セキュリティ運用リテラシー**
- 基礎科目: 所属大学指定科目（各大学）

演習

理論系

- 情報セキュリティ演習

技術系

- セキュリティ基礎演習
- ネットワークセキュリティ技術演習
- Webアプリケーション検査と脆弱性対策演習
- デジタルフォレンジック演習
- Capture The Flag（CTF）入門と実践演習
- 無線LANセキュリティ演習
- システム攻撃・防御演習
- システム侵入・解析演習
- リスクマネジメント演習
- インシデント体験演習
- IT危機管理演習
- ハードウェアセキュリティ演習
- ネットワークセキュリティ実践

社会科学系

- インシデント対応とCSIRT基礎演習
- 組織経営とセキュリティマネジメント演習
- 事業継続マネジメント演習

先進科目

理論系

- 最新情報セキュリティ理論と応用

技術系

- 情報セキュリティ技術特論
- 先進ネットワークセキュリティ技術

社会科学系

- セキュア社会基盤論
- 情報セキュリティ法務経営論

その他の活動

- セキュリティ分野シンポジウム
- 企業インターンシップ
- 交流ワークショップ

enPiT-Security：SecCapの修了認定

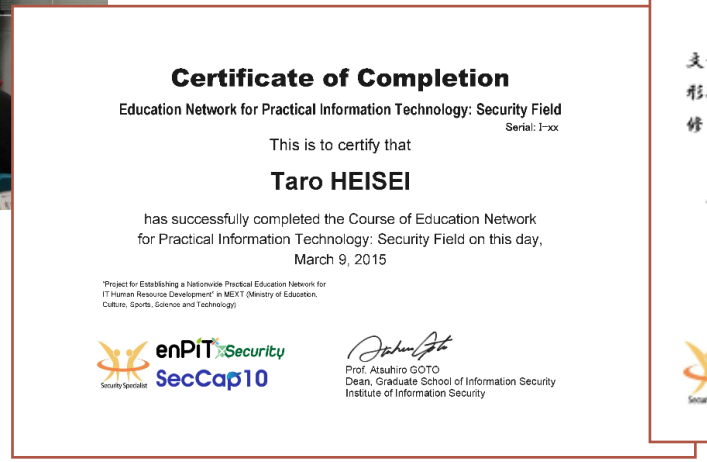
- SecCap修了認定：大学院修士（単位認定）約 120時間～
  - 共通科目：2単位
  - 演　　習：2単位
  - 先進科目：2単位（または演習2単位でも可）
  - 基礎科目：4単位（所属大学指定科目の中から選択）
- Associate-SecCap：学部、高専など（聴講生として認定）
  - 共通科目：2単位相当
  - 演　　習：2単位相当
  - 先進科目：2単位相当（または演習2単位相当でも可）
- SecCap10：“Security Specialist ”認定　約180時間～

  共通科目、演習、先進科目で10単位以上、および基礎科目4単位以上の合計14単位以上を取得できたものには「SecCap10」を授与し“Security Specialist”として認定する。

SecCap Certificate

所定の単位を取得した大学院修士の受講生に「SecCap認定」を授与

SecCapプログラムだけで1500名以上が修了



Certificate of Completion

Education Network for Practical Information Technology: Security Field

Serial: I-xx

This is to certify that

Taro HEISEI

has successfully completed the Course of Education Network for Practical Information Technology: Security Field on this day, March 9, 2015

"Project for Establishing a Nationwide Practical Education Network for IT Human Resource Development" in MEXT (Ministry of Education, Culture, Sports, Science and Technology)

enPiT Security SecCap10

Prof. Atsuhiro GOTO
Dean, Graduate School of Information Security
Institute of Information Security

第I-xx号

修 了 認 定 証

分野・地域を越えた
実践的情報教育協働ネットワークプロジェクト
セキュリティ分野

平成 太郎 殿

文部科学省「情報技術人材育成のための実践教育ネットワーク形成事業」に選定された掲記プロジェクトにおいて所定の課程を修了したことを認定する。

平成27年3月9日

文部科学省 情報技術人材育成のための実践教育ネットワーク形成事業
「分野・地域を越えた実践的情報教育協働ネットワーク」
セキュリティ分野

enPiT Security SecCap10

情報セキュリティ大学院大学
情報セキュリティ研究科長
後藤厚宏

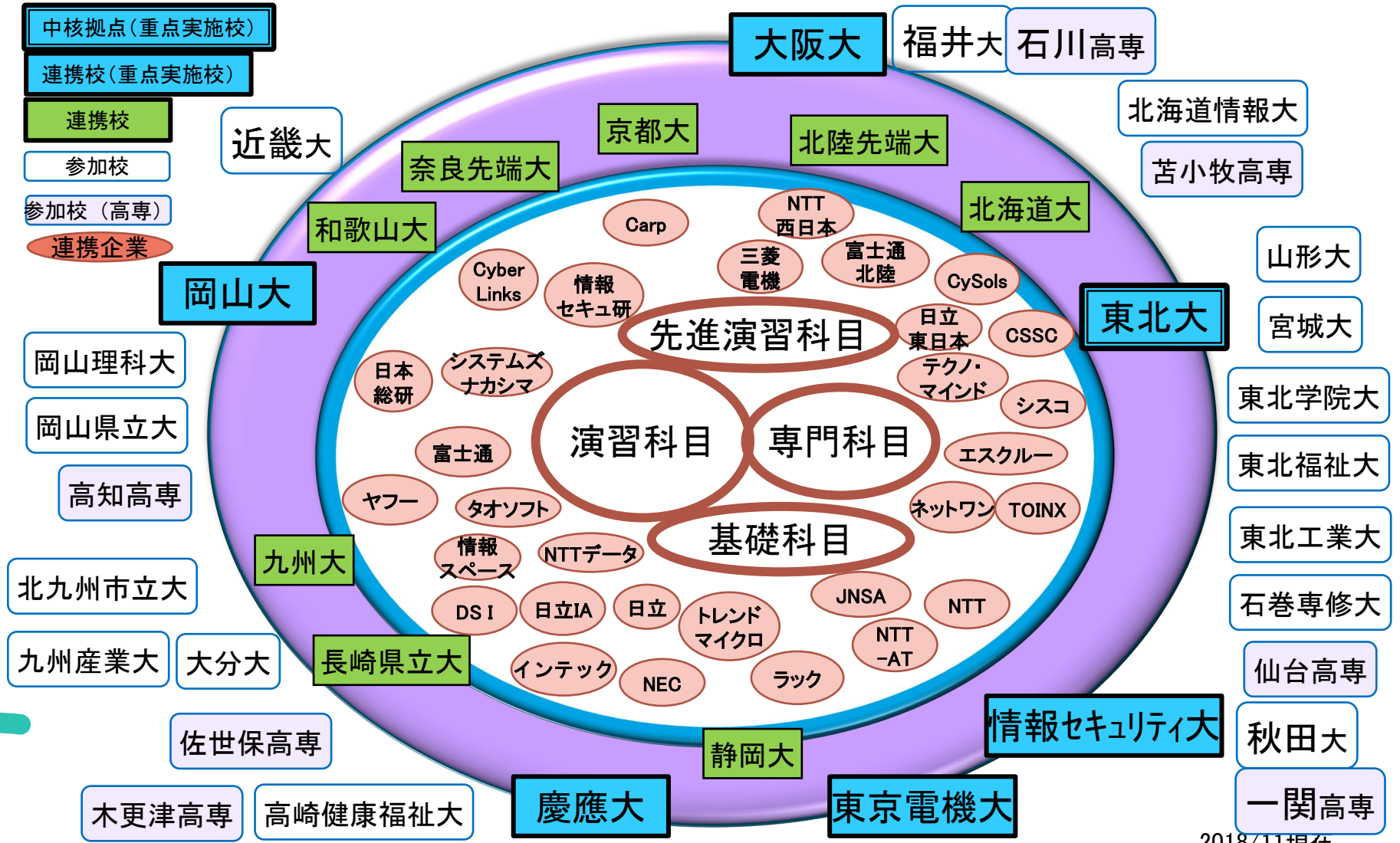
enPiT-Security （第２期）

- 実践人材の養成
  - 学部生向けセキュリティ分野の実践的スキルの基礎
  - Basic SecCapカリキュラムを協同で開講
  - 「Basic SecCap」コース修了(7単位以上)を認定
- 他大学・高専等・他学部との授業交流
  - 大学間で遠隔講義や集中講義（演習）を相互に提供
    - 多様な学生の中での実践的な人材育成
  - 専門科目の担当と履修運営は重点実施校6校が担当
- 幅のある演習
  - 多数のPBL演習により多様な経験の機会を提供してセキュリティ人材輩出の要請に対応
  - 高度な内容を扱う先進演習科目によりレベルと内容を多様化

enPiT-Security

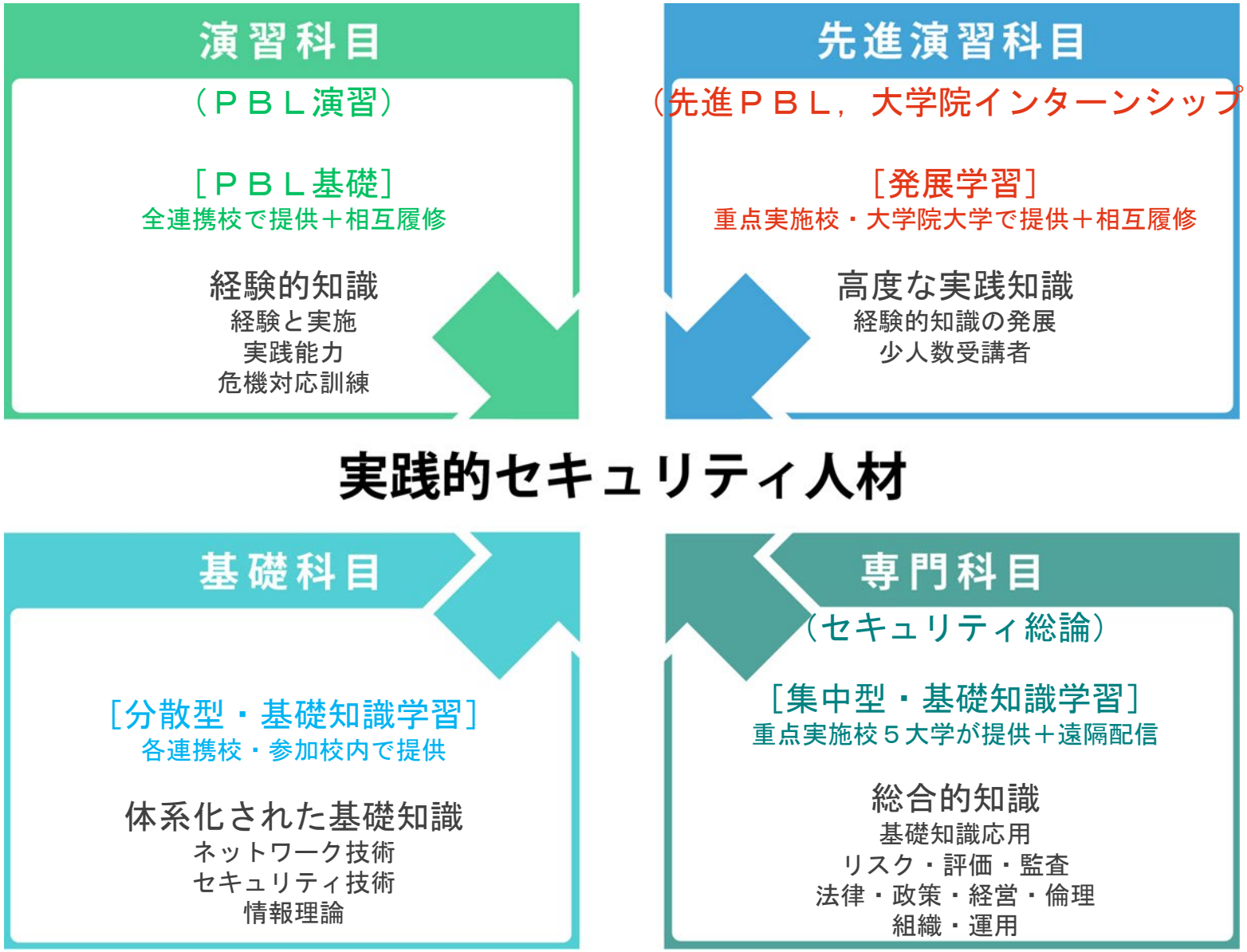
(2016年度～2020年度)

（スペースの都合のため社名・大学名の表示を短縮しています）



2018/11現在

実践的人材の育成のための
体系的，総合的，経験的知識と科目群



基礎科目

- 各大学で指定 (4単位，コース修了認定の要件)
  - 各大学の数科目（既存または新規開講）を申請し，認定
  - 教育水準とコース修了者認定の質を考慮して，モデルを提示

基礎科目の指定例

（東北大学工学部）
- 計算機学
- ディジタルコンピューティング
- 情報数学
- 情報通信理論
- アルゴリズムとデータ構造
- 計算機ソフトウェア工学
- 情報論理学
- システムソフトウェア工学
- ネットワークコンピューティング

（岡山大学 工学部 情報系学科）
- 応用数学
- 情報理論
- コンピュータハードウェア
- オペレーティングシステム
- ソフトウェア設計
- データ構造とアルゴリズム
- ネットワークシステム
- データベース

専門科目

- 専門科目7科目 (1科目2単位，コース修了認定の要件)
  - セキュリティ教育標準カリキュラムをターゲットにした統一カリキュラム
  - 重点実施校（５）が協働して実施提供
  - 内容を調整して内容の偏りを防ぎ，レベルの均質化を図って設定

セキュリティ総論A (東北大, 後, 水)

1 セキュリティリテラシー，2. セキュリティ攻撃の事例，3. セキュリティ防御の事例，4・5. プログラムのセキュリティリスク，6・7・8. ネットワークのセキュリティリスク，9・10・11. 暗号技術と実利用例，12. 情報セキュリティーポリシー，13. 情報セキュリティ対策体制，14. 情報倫理，15.まとめ

セキュリティ基礎論 (阪大, 前, 月)

1. 数理モデルから紐解く暗号理論，2. 代数学から構築する実践セキュリティ技術，3. 実用化暗号の安全性評価と実装演習，4. Pythonによるマルウェア解析，5. IoT機器とサイバーセキュリティ

情報セキュリティの基礎と暗号技術（セキュリティ総論）(電機大, 前, 木)

1. イントロダクション, 2. コンピュータウイルス, 3. アクセス管理技術, 4. 暗号の概要, 5. 共通鍵暗号, 6. 公開鍵暗号, 7. デジタル署名とPKI, 8. 暗号プロトコル, 9. 個人情報漏洩対策, 10. 不正コピー対策, 11. セキュリティポリシーとISMS, 12. ICTシステムの運用とセキュリティ, 13. デジタルフォレンジック, 14. ITリスクの考え方, 15. 考査と解説

セキュリティ総論D (慶應, 後, 水)

1. システム，2. 暗号の基礎， 3. セキュリティの基礎，4. 法制度と社会制度

セキュリティ総論E (岡山大, 後， 水)

1. イントロダクション，暗号の歴史と概要， 2. 暗号数学，3. 共通暗号鍵とデータ暗号化/公開鍵暗号と認証技術，4. 暗号計算のSW/HW実装，5. SW/HW実装に対する工夫と安全性評価，6. 階層型通信プロトコルモデル，7. データリンク層セキュリティ，8・9. ネットワーク層セキュリティ，10. トランスポート層セキュリティ，11. アクセス制御，12. メモリ脆弱性，13. 侵入検知，14. マルウェア検知，15. マルウェア解析

PBLテーマ（演習科目・先進演習科目）

- 演習科目・PBL 演習（１単位，コース修了認定の要件）
  - 多岐にわたるバラエティに富んだPBL を提供
  - 各連携校（大学院大学以外）が特徴的な内容で提供
    - 産学連携による企業インターンシップ等も提供予定
- 先進演習科目・先進PBL (1 単位)
  - ダイバーシティを高められるカリキュラムを設定
    - 受講者数を制限し選抜
  - 重点実施校が提供
  - 学部向けの企業インターンシップと最先端のPBL
- 先進演習科目・大学院インターンシップ (1 単位相当)
  - 高度な人材育成
  - 大学院大学が学部生を受け入れて学部生向け内容により演習

演習科目・先進演習科目

演習科目（PBL 演習）

- サイバーセキュリティ基礎演習 (北大, 2学期)
- クラウド・セキュリティ演習 (東北大, 6セメ集中)
- ビッグデータのプライバシー保護プロトコル演習 (阪大, 夏期集中)
- インシデントレスポンス演習 (和大, 夏期集中)
- 暗号ハードウェアセキュリティ演習 (岡山大, 後期集中)
- クロスサイトスクリプティング対策演習 (岡山大, 夏期集中)
- セキュリティエンジニアリング演習 (九大，夏期集中)
- サイバーセキュリティ演習 (九大, 夏期集中)
- ネットワークセキュリティ実践演習（セキュリティPBL）(電機大, 集中)
- セキュリティ先進PBL (電機大, 夏期集中)
- PBL演習 K (慶應, 8月集中)
- 不正アクセス解析演習 (京大，後期集中)
- Webアプリケーションファイアウォールによる攻撃検知演習 (長県大，後期集中)
- サイバー攻防基礎演習（仮）(静大，トライアル)

先進演習科目（先進PBL）

- 制御システムセキュリティ演習 (東北大, 5セメ集中)
- システム構築におけるセキュリティ機能実装とセキュリティ監視・運用について (阪大, 夏期集中)
- IoT機器向け安全な楕円曲線暗号の実装 (阪大, 後期集中)
- CSIRTとリスクマネジメント演習（先端セキュリティ）(電機大, 集中，1月)
- インシデントハンドリング演習 (慶應大, 集中, 2月)
- 安全性評価のための衝突型暗号攻撃演習 (岡山大，夏期集中)

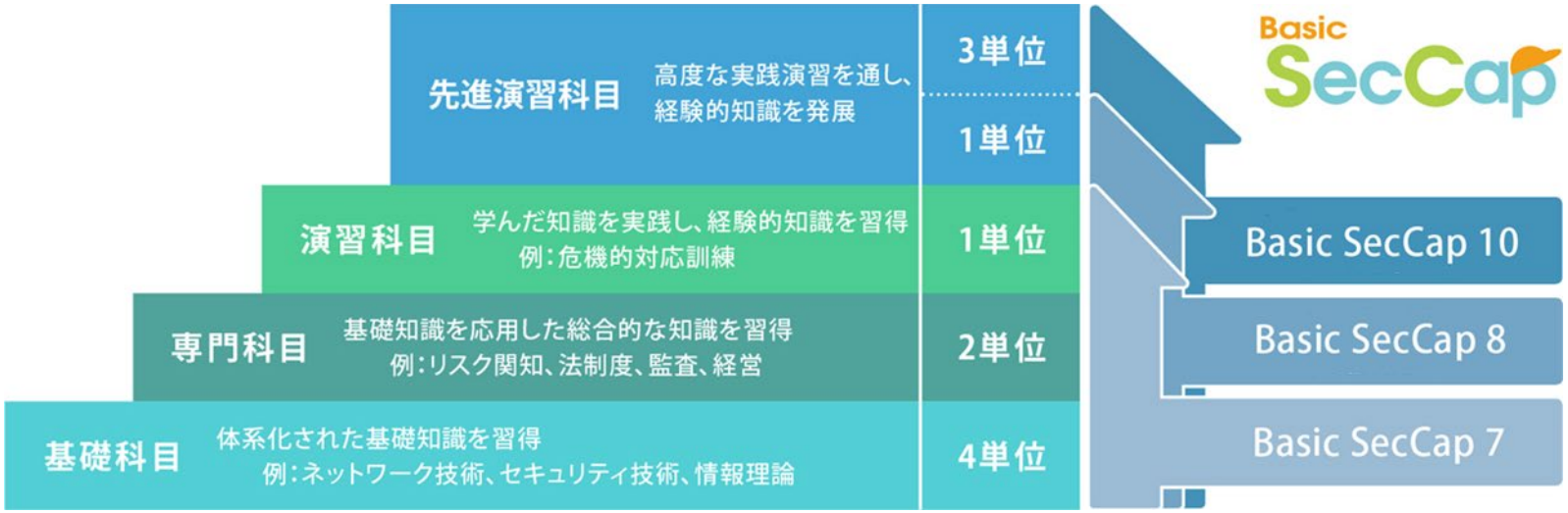
先進演習科目（大学院インターンシップ）

- セキュアクラウド理論演習 (JAIST, 夏期集中)
- 認証技術によるWebシステムのセキュリティ対策実践 (JAIST, 夏期集中)
- ハードウェアセキュリティ基礎演習 (NAIST, 夏期集中)
- 脅威分析演習 (情セ大, 集中, 8月)
- ハードニング基礎演習 (情セ大, 集中, 8月)
- 大学院インターンシップC (慶應)

コースの人材育成計画と修了認定

3つのレベルにより，到達目標と内容の多様化

- Basic SecCap 7 （専門科目2単位、演習科目1単位、基礎科目4単位の合計7単位以上）
  Basic SecCap 8 （7授与要件＋先進演習科目より1単位）
  Basic SecCap 10 （7授与要件＋先進演習科目より大学院インターンシップを含む計3単位）
- 参加拡大のため，専門科目及び演習科目のみの受講も受入れ



ProSec計画のポイント

情報セキュリティ分野の学び直しニーズ

情報セキュリティ人材のニーズの急速な高まり

非IT企業を含む全ての企業に自社情報システムのセキュリティを高める必要が生じており，平成28年情報セキュリティ従事者28.1万人（13.2万人が不足[1]）今後も増加傾向.

社会人の再教育による情報セキュリティ分野への人材シフトが喫緊の課題

- **産業ニーズに合った大学院教育の実践**
  理工系人材育成の在り方調査に基づき提案されたモデル・コア・カリキュラム[2]を実施に移す.
- **社会人の継続的な学び直しの場としての*大学院への変革*，社会要請に応える挑戦**

本計画のポイント

- 優位性
  - 人材不足が深刻な**情報セキュリティ人材**の育成を対象
  - enPiT1等で**実績**のある大学院が連携して社会人の学び直しを**全国規模**で支援する高等教育の体制を整える
    - ✓ **産業界・実務家との連携**が確立
    - ✓ 大学院**カリキュラム・演習科目が充実**
    - ✓ **大学間の密な連携**
      授業互換や遠隔講義が整備，多様性・レベルが維持
- 新たな挑戦
  - 社会人向け**モデル・コア・カリキュラム**[2]の実践
  - **人材スキルマップ**を活用した産業ニーズと教育コースの視覚化と連続的な改善プロセスの実践
  - 全大学共通のProSec認定証の発行(SecCap ⇒ ProSec)

連携7大学で統一された取り組み内容

① **メインコースとクイックコースの2種類のコース構成**

② 共通の枠組に基づいて高度情報セキュリティ人材教育コースの修了を示す**ProSec-X**(Xは実務領域)を認定する

例) ProSec-CSIRT,ProSec-IoT,ProSec-IT, ProSec-BigData経営…

③ 講義や演習の開講日時やポイント制の導入により，**社会人が受講し易いコースを開講**する

④ **講義科目を相互に提供**する（単位の相互認定），および修了認定の考え方を統一する

⑤ コース内容を**人材スキルマップ上で視覚化し、産業界が求める人材像に適合した教育コース**を開発する

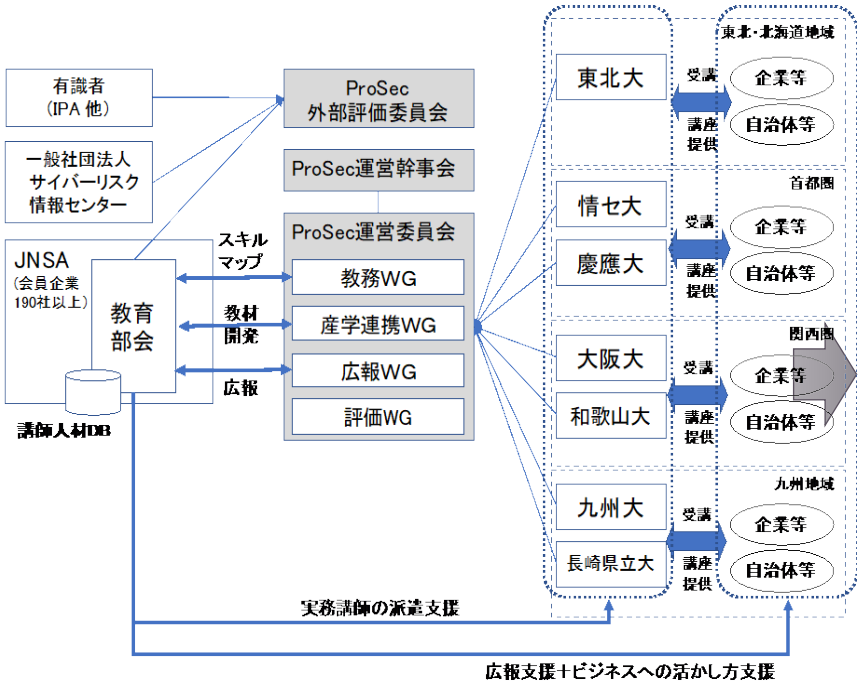
⑥ 産業界および個々の社会人向けに統一された広報

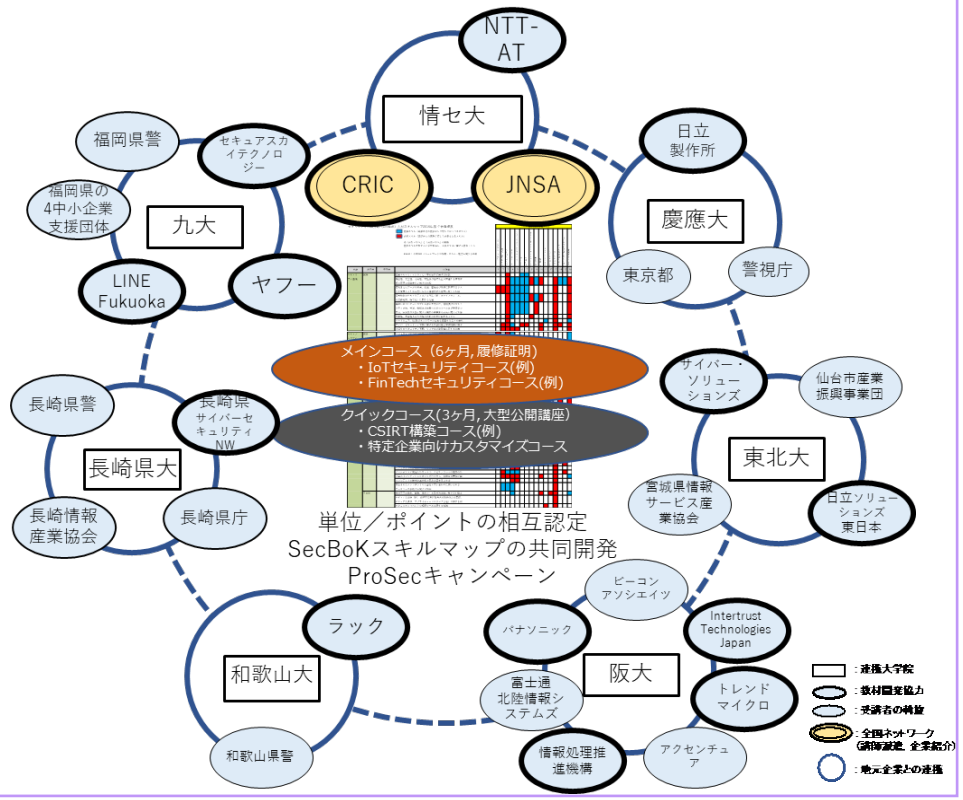
[1]経済産業省商務情報政策局情報処理振興課,"IT人材の最新動向と将来推計に関する調査結果," 平成28年6月10日.
[2]文部科学省,"平成28年度理工系プロフェッショナル教育推進委託事業 工学分野における理工系人材の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）成果報告書," 平成29年3月.

大学間・産業界との連携体制の構築

- enPiT1 Security等で**実績のある大学が連携**して社会人リーダー人材育成 “ProSec” を開発・実施
- 東北，関東，関西，九州に分散する7大学を拠点として，**地域企業28社・組織と連携**（2017年6月現在）
  - **ローカルループ**： 連携大学が地域企業群と連携し，各地域での産業ニーズにあった教育コースを独立に開発・発展させる
  - **グローバルループ**： enPiT1 Security等で実績のある大学連携を活用し，全国で統一のProSec認定，遠隔講義や授業互換で高度教育を全国規模で展開

※ enPiT1 Securityではグローバルループ（大学連携）が中心，enPiT-Proでは地域の産業ニーズに応えるローカルループを新たに構築





アウトプットとアウトカム

アウトカム

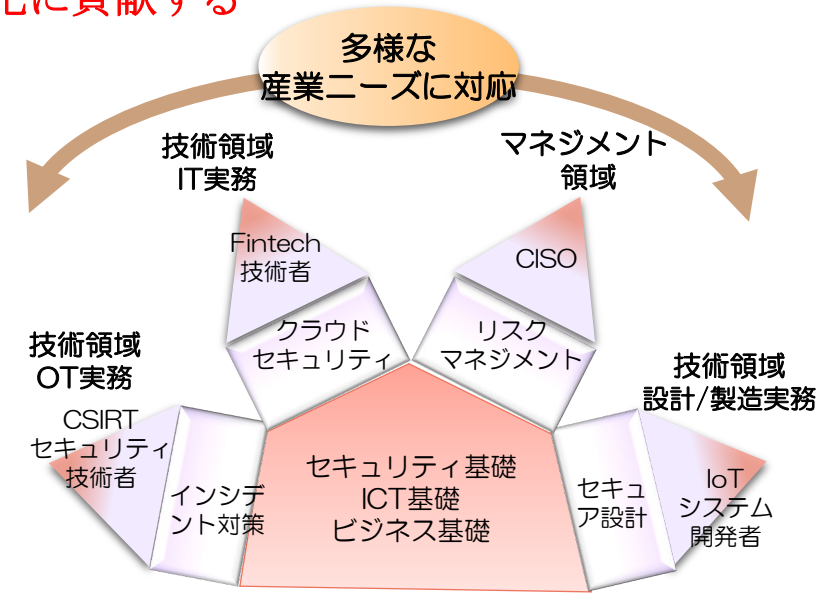
各連携大学が地域の産業界・自治体等と連携して、地域ニーズにマッチした人材教育コースを開発・実践し、人材ミスマッチの解消と地域活性化に貢献する

アウトプット

1. 産業ニーズに合わせて幅広い教育コースをメインコースとクイックコースの選択肢で提供

① クイックコース：
その時々の最新の専門知識や新しいサイバー攻撃に対応したスキルを短期集中で学ぶ

② メインコース：
修士・博士課程への橋渡しとなる単位取得を伴う120時間超のコース．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正規科目にある講義／演習を組み合わせた既設科目で構成



2. 各連携大学毎に，メインコースとクイックコースをそれぞれ1コース以上開講し，修了証（ProSec-X）を授与する実績を作る。ProSec-X=ProSec-CSIRT, ProSec-IoT, ProSec-IT, ProSec-BigData経営他

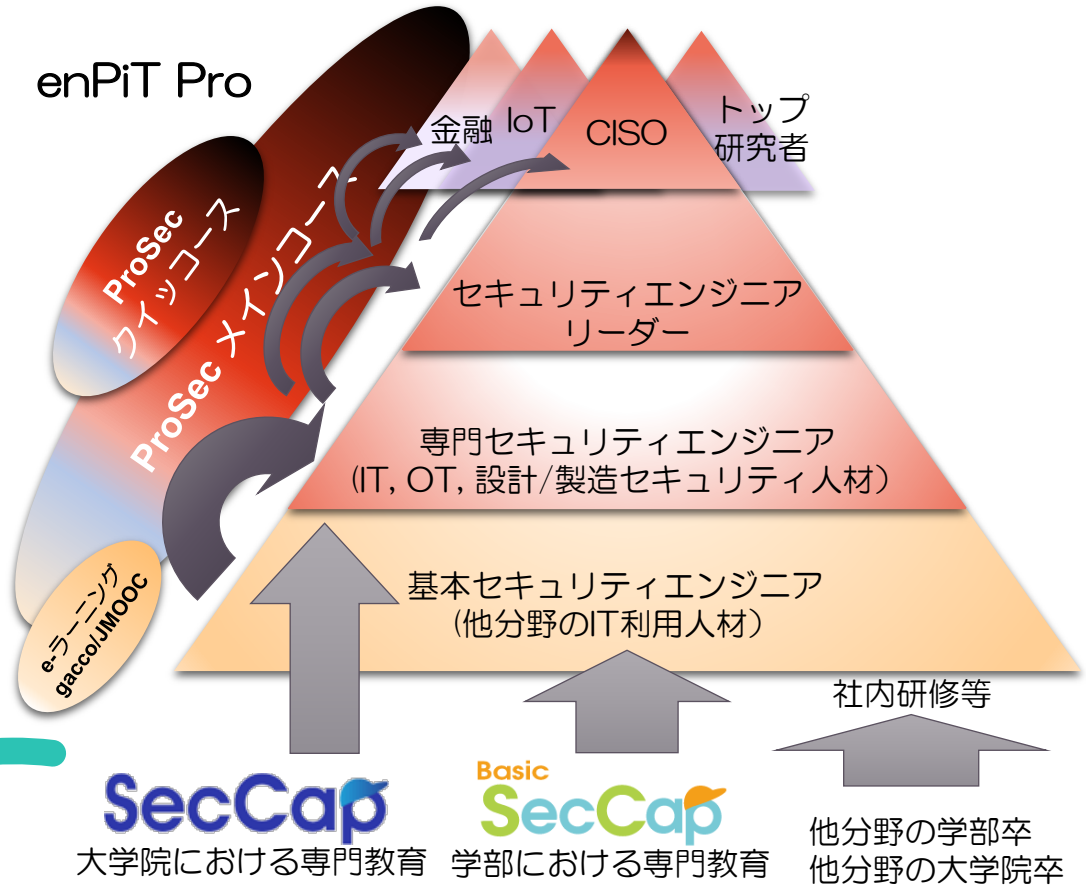
情報セキュリティプロ人材育成短期集中プログラム(ProSec) の描く将来像

情報セキュリティプロ人材育成短期集中プログラム(ProSec)は社会の人財教育の場としての大学院を活用する取り組み

1. キャリアステージ，技術分野に応じて，大学院が最適な教育コースを提供.
2. 企業のキャリアアップ評価や（中途）採用評価に活用可能な大学院での学修レベル.
3. 社会人の客観的な知識・技能の証明としてProSec認定証の定着

を通じて，「<u>社会の人財教育の場としての大学院</u>」を目指す.

セキュリティ人材の企業内キャリアパス



<u>企業ニーズにマッチしたセキュリティ人材育成は全産業における企業の経営課題</u>

「これまでは守りと考えられていたセキュリティ技術が、イノベーションの創発に必要不可欠の要素となっている」

アクセンチュア株式会社　セキュリティ推進事業本部
統括マネージング・ディレクター　市川 博久

「自社内で教育を実施できる教える側人材がいないため、外部の専門機関に頼らざるを得ない」

特定非営利活動法人日本ネットワークセキュリティ協会
教育部会　部会長　平山 敏弘

「セキュリティ技術は大手ITベンダーへの依存度が高く、地方IT企業が自社でセキュリティ人材を育成することは困難」

一般社団法人宮城県情報サービス産業協会
事務局長　穴沢 芳郎

「本プログラムで社内人財の教育の一部を実施するだけでなく、協力して社会の人財教育に資することに期待します。」

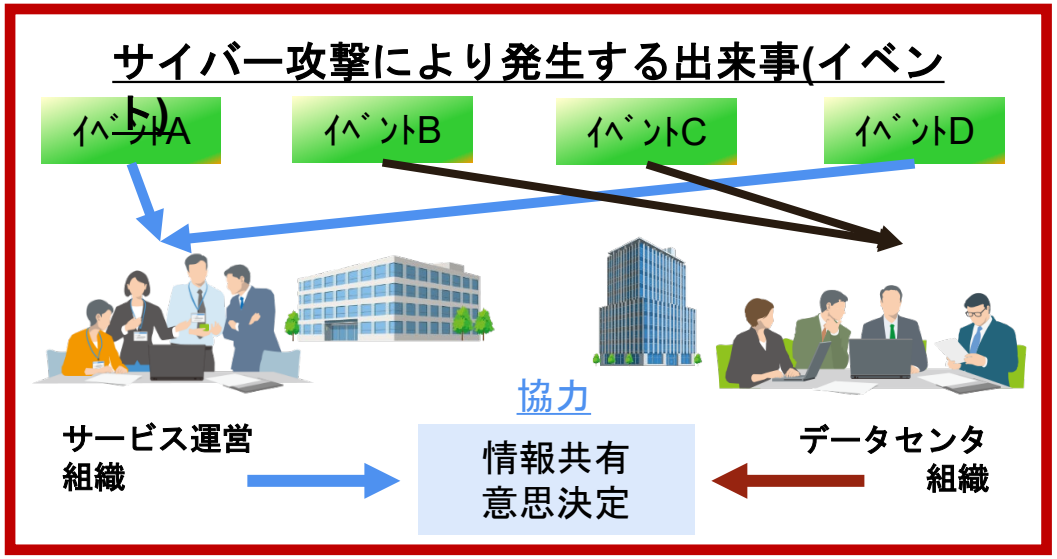
株式会社日立製作所　セキュリティ人財統括センタ
主管技師　川嶋 一宏

実環境に即した演習教材の作成

- シナリオ型演習
  - 実環境を用いた対応演習
  - インシデント対応のみならず人とのコミュニケーションの訓練を含む
  - 効果大、準備負荷大、育成人財数少
- カードゲーム型演習
  - インシデント発生はカードを選択することで置き換え
  - 対応についてもカードで実現
  - 判断の訓練
  - 効果中、準備負荷少、育成人財数大
- 複合演習
  - カードゲーム型をコアに、コミュニケーション訓練に注力
  - コミュニケーション部分は実環境で行う
  - 効果中、準備負荷中、育成人財数中

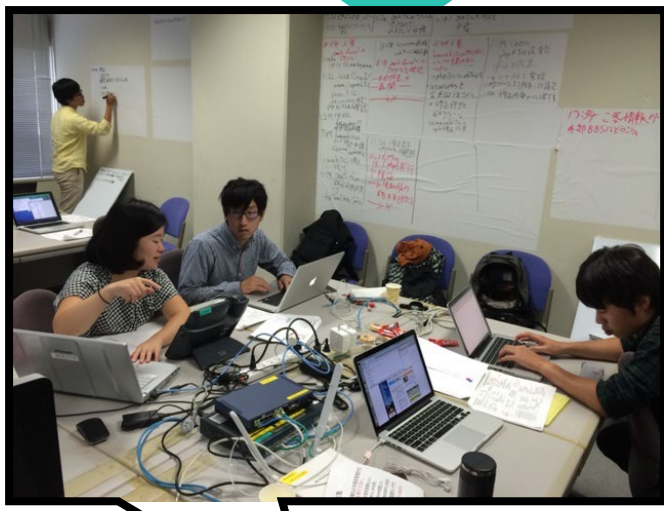
複合演習の狙い

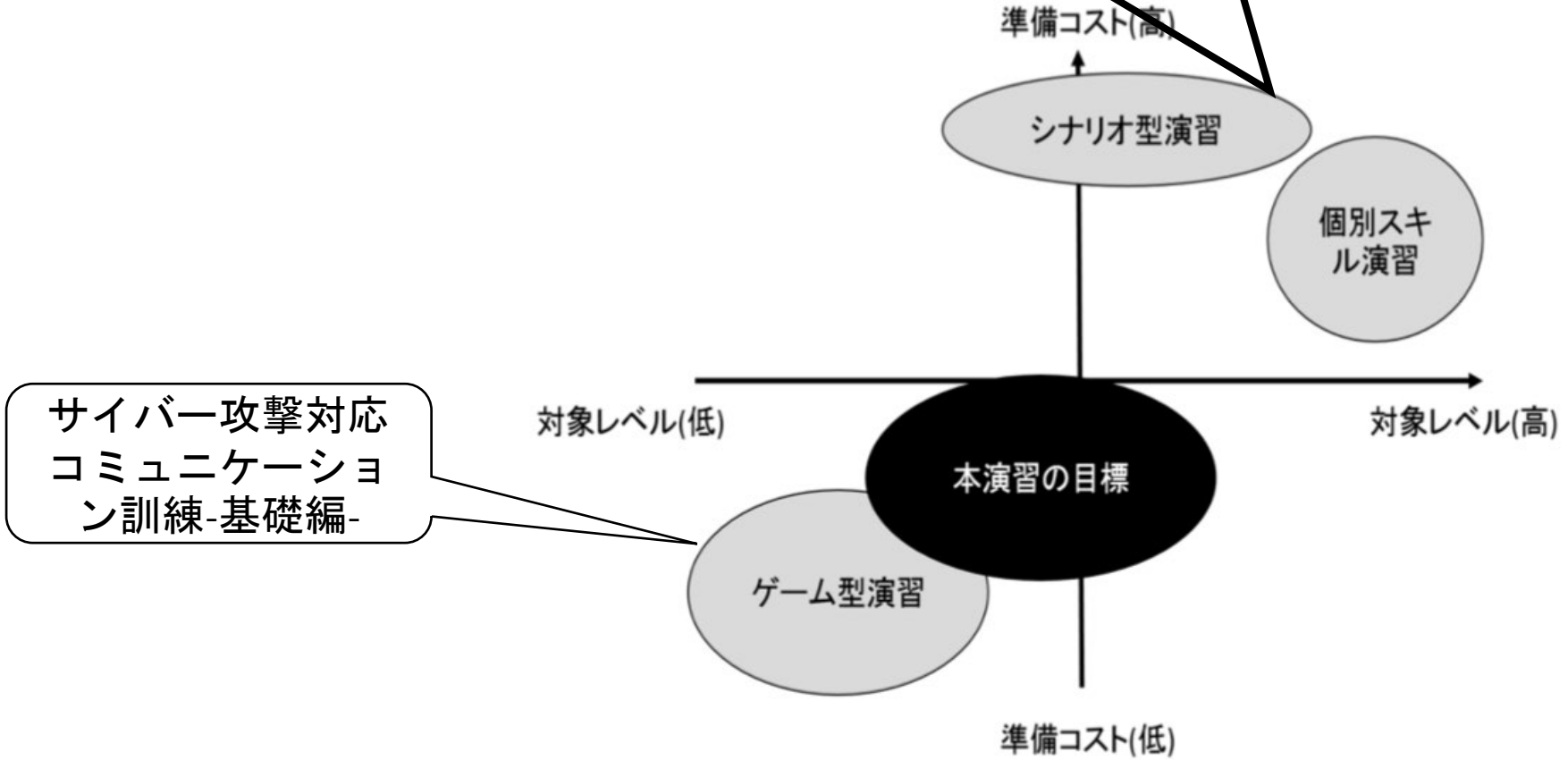
- 社内システムや製品サービスにおいてセキュリティインシデントが発生した際に、組織間において円滑に情報共有を実施し、組織間で協力してサイバー攻撃に迅速対応できるようになる
- 的確な報告・連絡・相談により、迅速なサイバー攻撃対応を行うための体験訓練
- 事前準備として何を行うべきかの気付きや確認を行う



本研修の位置付け

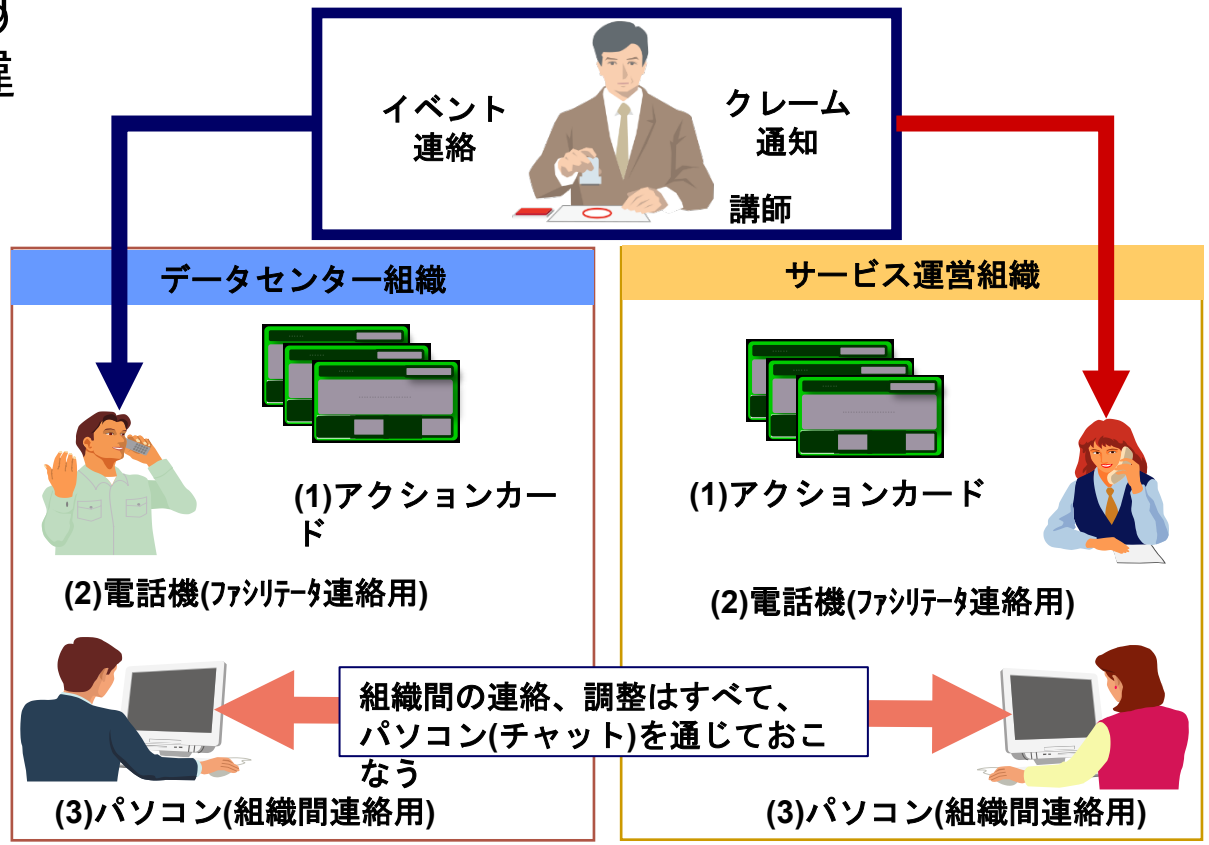
- 基礎編より有事(サイバーセキュリティインシデント発生時)に近い環境をシミュレーションすることで事業範囲の違いやバックグラウンドの違いによるコミュニケーションギャップを体験





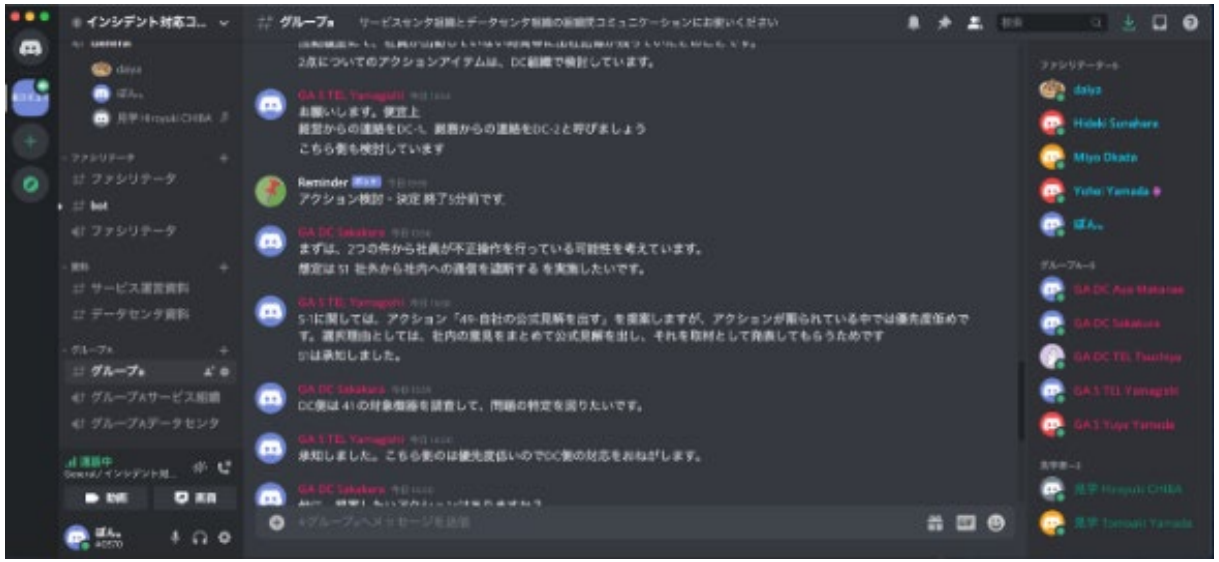
本研修のターゲット

- サイバーセキュリティインシデント発生時に共に対応する必要がある一方、事業範囲やバックグラウンドの違い等によりコミュニケーションギャップが生まれる組織
  - 経営本部 <-> 現場 (開発・トライアル済)
  - OT <-> IT(今年度開発したシナリオ)
  - 親会社 <-> 子会社
  - システム開発企業 <-> 顧客企業



オンライン複合演習

- 2020年度より実施
  - Discordを用いてオンラインで参加
  - 部署間でのコミュニケーションをエミュレート
  - 限定された環境でのコミュニケーション訓練



オンライン複合演習 2023年度

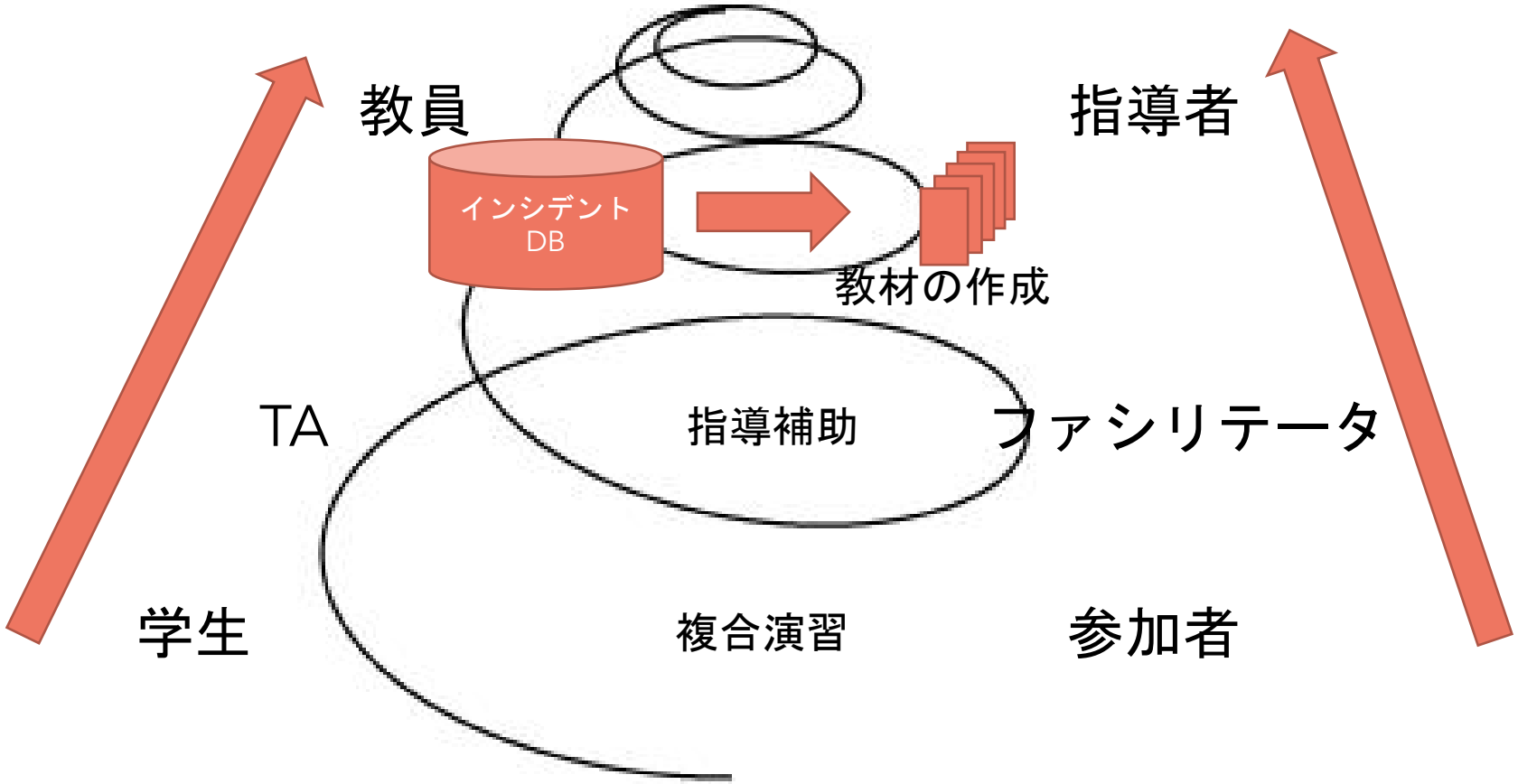
- 今年もやります
  - 参加費無料
  - 7月と2月に実施
- インシデントハンドリング演習(オンライン版)
  - 7/26午後
  - ProSec Unit10を付与
  - 募集予定: 16名
  - 申し込み: keio@seccap.jp
- 来年2月にも実施します
  - 7月に参加が難しい場合でも、案内を行いますのでご連絡頂ければ幸いです

keio@seccap.jp

人財育成の課題

- 人財育成に携わる人財の確保と育成
- 人財イメージ
- 人財育成の効果と評価
- 倫理感の醸成

人財育成のエコシステム



リーダーシップ人財と求められる能力

- リーダーシップ人財イメージ

組織リーダー
- 組織の方針決定
- 対策・対応計画の策定

統括リーダー
- 部署間の調整
- 進捗把握

部署リーダー
- 部署の意見の集約と
- 意思決定、意思の伝達

部署メンバー
- インシデント発生時に
- 事態を把握し対応を検討

部署A　　部署B

コミュニケーション

人材育成エコシステム

- グループメンバーとしての参加から教材作成へ人財イメージ

参加者を選定しながら
上位レベルの演習へ

教材作成
- インシデントの分析
- 教育ポイントの整理
- Up-to-dateな演習教材作成

ファシリテーター
- 演習の進捗管理
- 各グループの調整、アドバイス
- 演習実施者の育成

グループリーダー
- グループの意見の集約と
  意思決定、意思の伝達

グループメンバー
- インシデント発生時に
  事態を把握し対応を検討

グループA　グループB
コミュニケーション

教材作成演習

- Step1
  - 実際のインシデント事例の分析
    - それぞれにインシデントに対する対応と対策の整理
    - 対応、対策の重要なポイントを把握
- Step2
  - 実際のインシデント事例から
    - 演習で学ぶべきポイントを抽出
    - 既存カードの選定と新規カードのデザイン
- Step3
  - 演習シナリオの作成及びファシリテータ向けマニュアルの作成
- Step4
  - 作成したシナリオの実施

成果及び課題

- シナリオ(教材作成演習での成果)
  - IT部門、OT部門連携
  - ランサムウェア
  - 情報公開に関する議論
- 課題
  - 教材作成演習
    - 指導手順書の整備
  - ファシリテーターレベルから教材作成演習の間を埋める演習の必要性
    - ファシリテーターマニュアルの整備
    - 教材の構造を理解するための資料整備

提言1) 連携防御のすゝめ
深い情報共有による組織間連携防御態勢の整備

- 防御のためのFederationの形成
  - パートナー選定基準
    - 組織のReputation
    - リスクを定義・特定・測定することで目的を示し、連携による利益を共有できること
    - 組織間の契約とサービスへの落とし込みができること
  - 数が多ければいいわけではなく、組める相手を選別しFederationを形成
    - 数組織から10組織程度
- 共有情報
  - IOCよりもコンテキスト情報(定石やLive情報)を
  - パートナーシップに基づく相互での情報提供と信頼に基づく情報の活用
- ツールの活用
- 共有情報の教材化

育成人財の評価

- 人財育成プログラムの効果の測定
  - CTF
  - 課題提出
  - 実務環境での評価
- 共通の評価基準が必要
  - 知識だけでなく
  - スキルの評価

倫理感の醸成

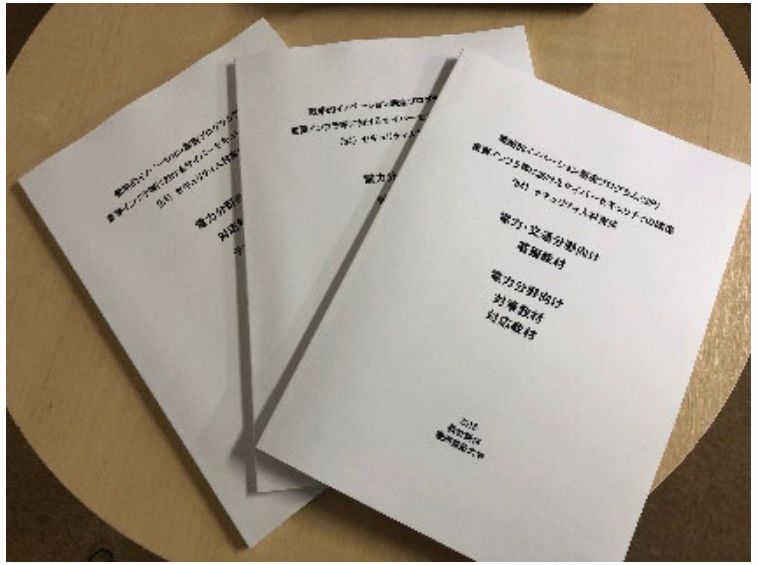
- 育成された能力の活用
- 育成プログラムの責任
- 人財への倫理感の付与
- 責任感の醸成
- 倫理的行動と人への評価

提言2)
サイバーセキュリティ業務/研究/教育における正当性の確保

- 各種法制度における正当性要件
  - 基本的に未定義
  - その結果として、業務等においてグレイゾーンがあり、逮捕されるといった状況も発生している
- セキュリティ業務における正当性
  - 正当業務行為の定義
  - マルウェアの所持、分析
  - マルウェアの挙動分析とその際に発生しうる事故
- セキュリティ研究における正当性
  - 研究に関して「正当業務行為」が定義されていない
  - 実環境での実験等のための準備に関する議論、事故発生時の報告方法、報告先、手段
- セキュリティ教育における正当性
  - 情報共有、教育側の責任範囲
    - 受講者によるインシデントの発生時の責任
  - 教育項目として倫理や制度に関する教育をどの程度行い、どのようにその成果を確認すればよいか
- 責任範囲の定義が不可欠である
  - ミスなどが発生した際において、どの程度の準備を整えておけば免責されるかといった議論
- 「正しく」業務/研究/教育を実施している従事者が安心してそれぞれにあたることができるような環境の整備
- 以上のような環境を構築するための議論の場を設けることを提案する

人財育成教材

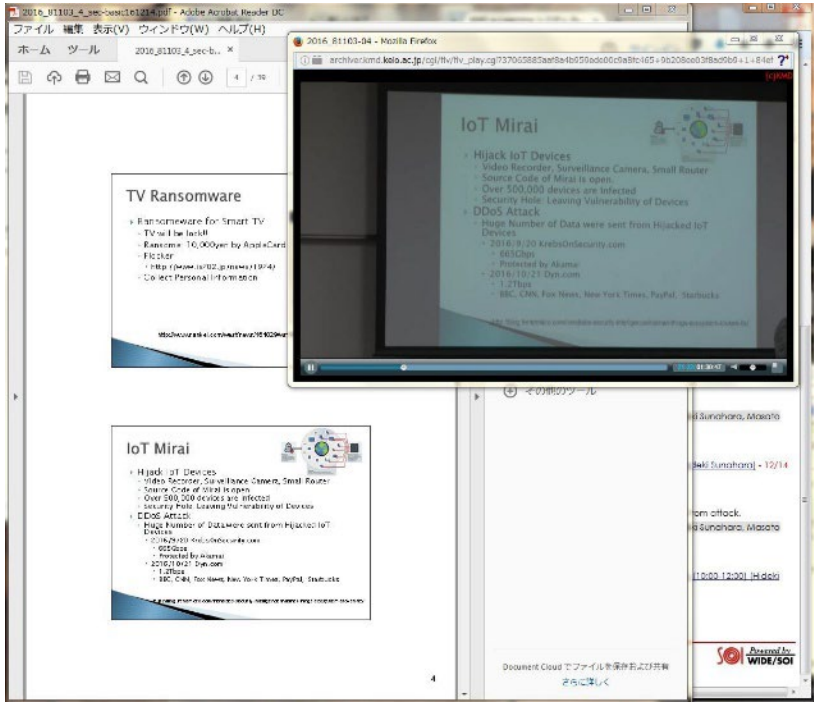
- 開発したカリキュラム及びそれに基づく講義・演習教材
- テキスト・スライドを核とした指導教材
  - テキスト、スライド、**指導要領**で構成
    - 指導要領で指導の仕方も提示
    - 加えて
      - カスタマイズマニュアル：各組織向けカスタマイズ
      - 演習課題例：理解度の確認用
      - **用語集：言葉の差異の吸収**
      - **事例集：身近に起こりうることを理解するための資料**
    - 電力分野版、交通分野版



テキスト

e-learing教材

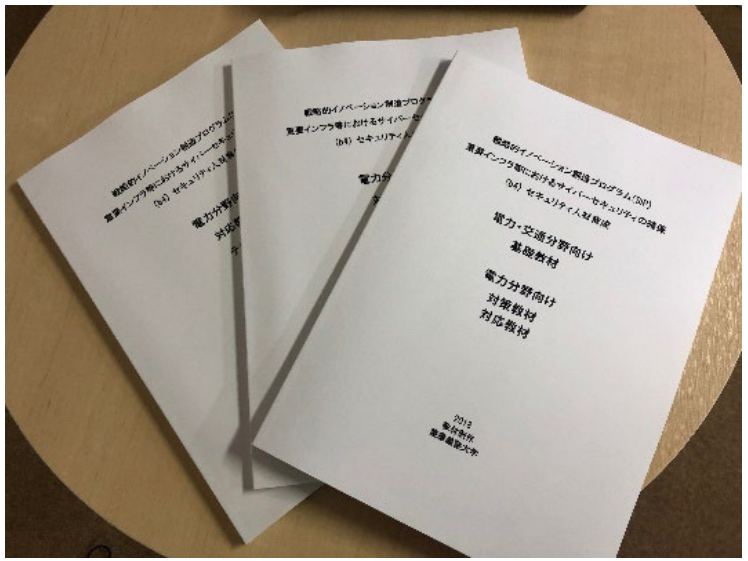
- e-learning
- 開発したテキストに基づく内容
  - 業務の合間に学びやすい形式での提供
  - 1単元 10～15分程度
- 学習の進捗状況を確認可能
- 課題等の提出、確認可能



e-learning教材

開発された教材も無償で配布中

- セキュリティの基礎・対策・対応
  - テキスト、スライド、指導要領、演習教材等
  - 講義等で利用したい方に配布中



教材に関する問合せ先: keio@seccap.jp