資料５－４

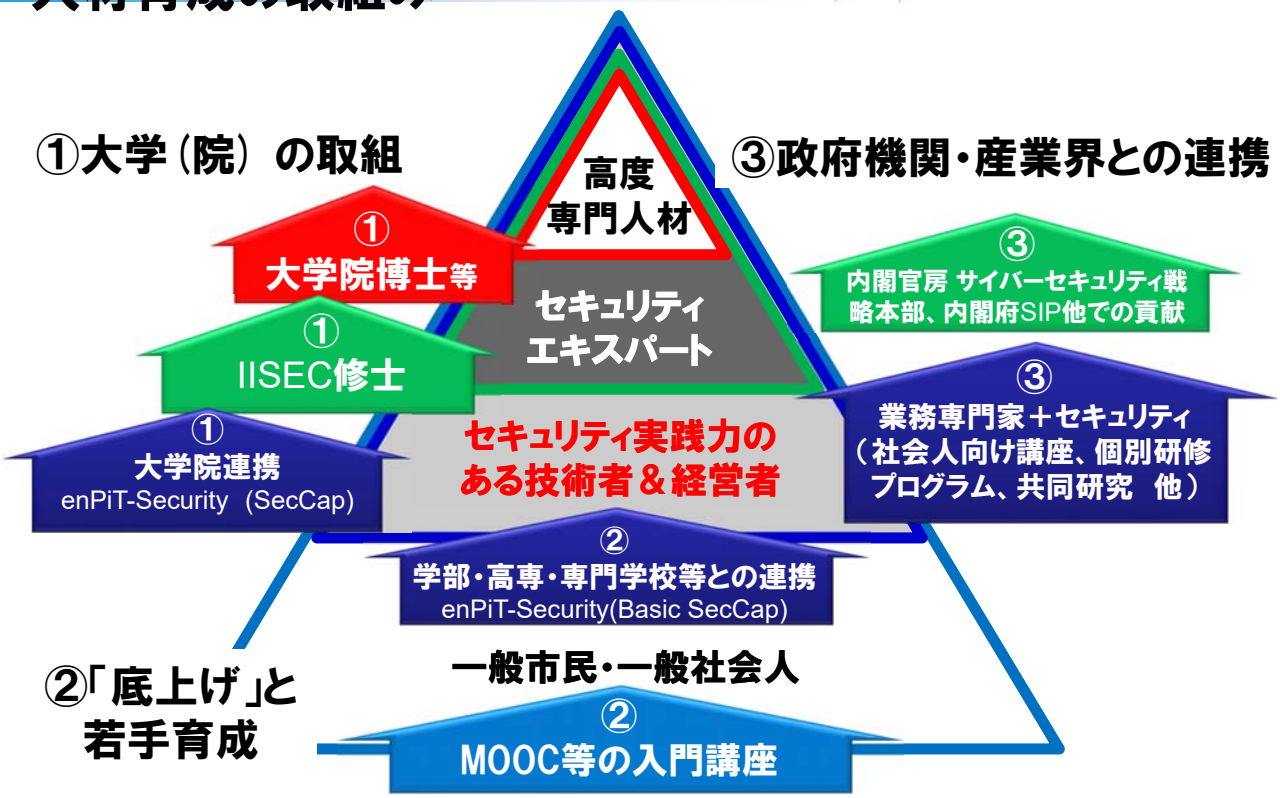
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoT時代を支える
サイバーセキュリティ人材育成

学校法人 岩崎学園　情報セキュリティ大学院大学
内閣府 SIP プログラムディレクタ(PD)
後藤 厚宏

情報セキュリティ大学院大学
人材育成の取組み

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



①大学院の取組

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- **情報セキュリティ専門の大学院大学： 修士(情報学) 博士(情報学)**
- **技術・管理・法制、セキュリティ総合教育のカリキュラム**
- **将来のCIO/CISOを育成する実務指向教育と深い専門研究成果の蓄積**
- **横浜市神奈川区鶴屋町2-14-1（横浜駅きた西口徒歩1分）**

	博士前期課程 [2年制]	博士前期課程 [1年制]	博士後期課程
標準修業年限	2年	1年	3年
所要単位	30単位以上 専攻科目24 (含必修4) 研究指導6	46単位以上 専攻科目42 (含必修4) プロジェクト研究指導4	8単位以上 博士専門8 (含必修8)
学位論文等	修士論文	リサーチペーパー	博士論文

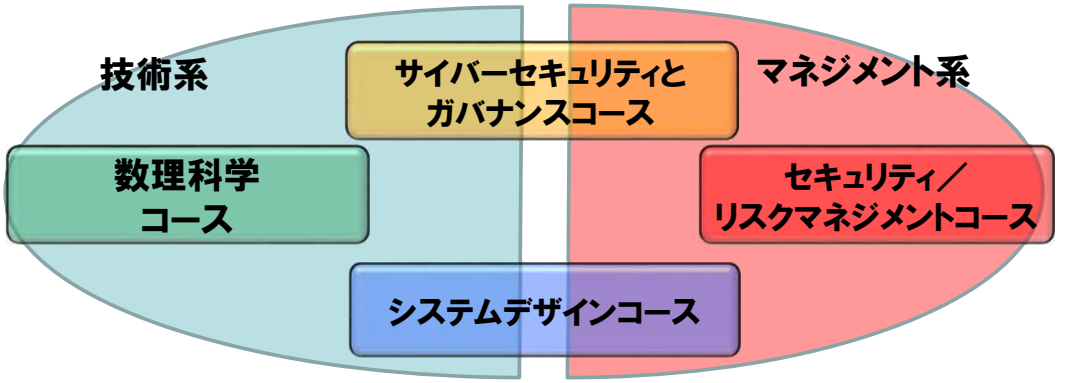
cf.**学位授与状況** **修士(情報学)・・・339名**(2006年3月～2017年3月)

博士(情報学)・・・30名(2007年8月～2017年3月)

①総合科学：情報セキュリティカリキュラム

http://www.iisec.ac.jp

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



倫理観を持って、現実の課題解決を担う高度な専門技術者・実務家、及び、将来方向をリードする創造性豊かな研究者を育成

社会人学生の所属組織(2016-2017実績)

アイテル(株)／ウィングアーク1st(株)／NECフィールディング(株)／NTTコムウェア(株)／NTTテクノクロス(株)／沖電気工業(株)／海上自衛隊／海上保安庁／(株)アーク情報システム／(株)アイネス／(株)サーバーワークス／(株)JR東日本情報システム／(株)ジョイント・システムズ・サービス／(株)日立システムズ／(株)日立製作所／(株)Beyondsoft Japan／金融庁／警察庁／警視庁／埼玉県警察／ジェイアール東海情報システム(株)／静岡銀行／ソニー(株)／(独)国立印刷局／東日本旅客鉄道(株)／フォレストソフト(株)／富士通(株)／ベライゾンジャパン合同会社／防衛省／法務省／三菱重工業(株)／モルガンスタンレーグループ／横浜銀行／横浜市役所／読売新聞社 など

①大学院の取組 IISEC カリキュラム

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

総合学習

- 情報セキュリティ特別講義
- 情報セキュリティ輪講
- Presentations for Professionals
- 情報セキュリティ運用リテラシーⅠ・Ⅱ

数理科学

- 暗号・認証と社会制度
- 暗号プロトコル
- アルゴリズム基礎
- 数論基礎
- 暗号理論
- 計算台数

セキュリティ／リスクマネジメント

- 情報セキュリティマネジメントシステム
- セキュリティシステム監査
- セキュリティ管理と経営
- 組織行動と情報セキュリティ
- マスメディアとリスク管理
- リスクマネジメント
- リスクの経済学
- 統計的リスク管理
- 統計的方法論
- セキュリティ監査
- 国際標準とガイドライン

①大学院の取組 IISECカリキュラム

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

サイバーセキュリティとガバナンス

- ハッキングとマルウェア解析
- 不正アクセス技法
- セキュアシステム構成論
- サイバーインテリジェンス
- セキュア法制と情報倫理
- 法学基礎
- 知的財産制度
- セキュリティの法律実務
- 個人識別とプライバシー保護

システムデザイン

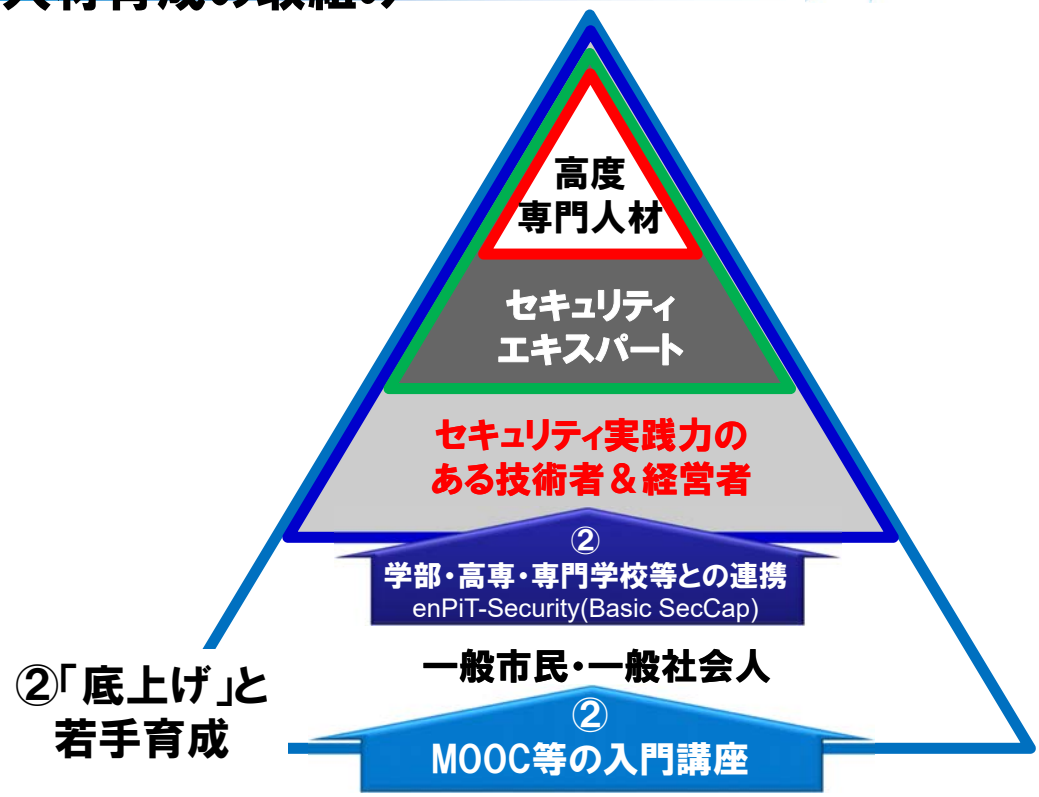
- インターネットテクノロジ
- ネットワークシステム設計・運用管理
- 情報デバイス技術
- 情報システム構成論
- オペレーティングシステム
- セキュアプログラミングとセキュアOS
- プログラミング
- ソフトウェア構成論
- IoTセキュリティ特論

ハンズオン

- セキュアシステム実習
- セキュリティ実践Ⅰ ＆セキュリティ実践Ⅱ
  NWとWebアプリのセキュリティ検査と対策演習、デジタルフォレンジック演習、
  Capture The Flag (CTF)入門と実践演習、インシデント対応とCSIRT基礎演習
- Windowsセキュリティ

情報セキュリティ大学院大学
人材育成の取組み

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



②「底上げ」と
若手育成

②MOOCによる幅の拡大と普及啓発

Massive Open Online Course

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 一般社会人・大学生・専門学校生向け情報セキュリティの「超入門」講座。
2015年5月13日～7月16日

⇒約1万人が受講

■ 情報セキュリティ「超」入門のステップアップ版。
企業研修を想定。
2015年10月8日～12月16日

⇒約5,000人が受講

http://gacco.org/

『超』入門コースの構成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティの常識(リテラシー)

1週目
1. 実社会におけるサイバー攻撃の脅威と要因、対策に必要な考え方(佐藤)

2週目
2. サイバー攻撃の仕組みとシステムや機密情報を守る対策技術(佐藤・大久保)

3週目
3. 情報セキュリティの基礎を支える暗号技術(土井)

4週目
4. 情報セキュリティを取り巻く法律や制度(湯淺)

情報セキュリティの知識を総まとめと標的型攻撃(後藤)

各コマ、合計で90～120分(＋確認テスト)

初級コースの構成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

1週目
1.情報セキュティ基礎知識(佐藤)

2週目
2M. 情報セキュリティマネジメントのフレームワーク(後藤)
2T. 情報セキュリティを支える暗号技術の基礎と応用(土井)

3週目
3M. 情報セキュリティのリスクマネジメントとリスクコントロール(後藤)
3T. ネットワークを守る認証技術とシステム技術(佐藤・土井)

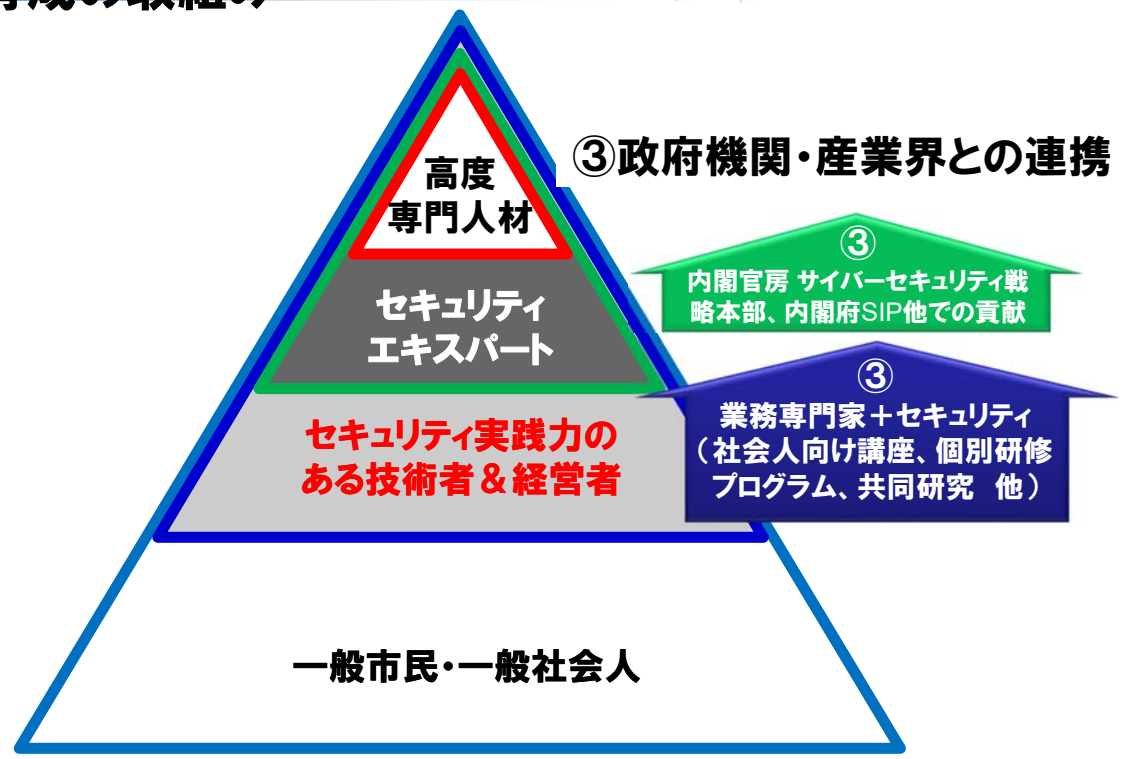
4週目
4M. 情報セキュリティの関わる法律の基礎知識(湯淺)
4T. 企業の情報ネットワークシステムのセキュリティ(佐藤)
ソフトウェアのセキュリティ課題と対策(大久保)

5週目
5T. Web・データベース・クラウドのセキュリティとCSIRT(大久保)

各コマ、合計で90～120分(＋確認テスト)

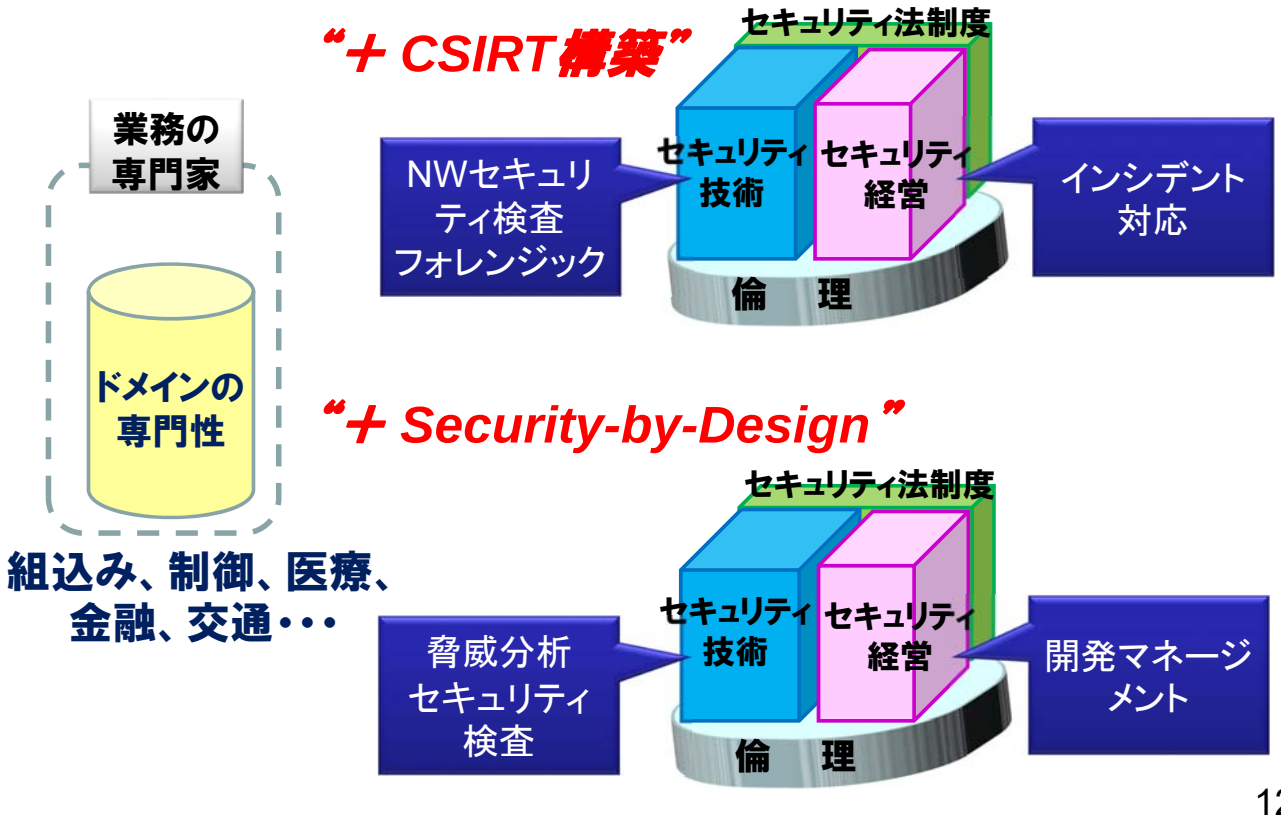
情報セキュリティ大学院大学
人材育成の取組み

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



③情報セキュリティ大学院の
社会人向け集中コース

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



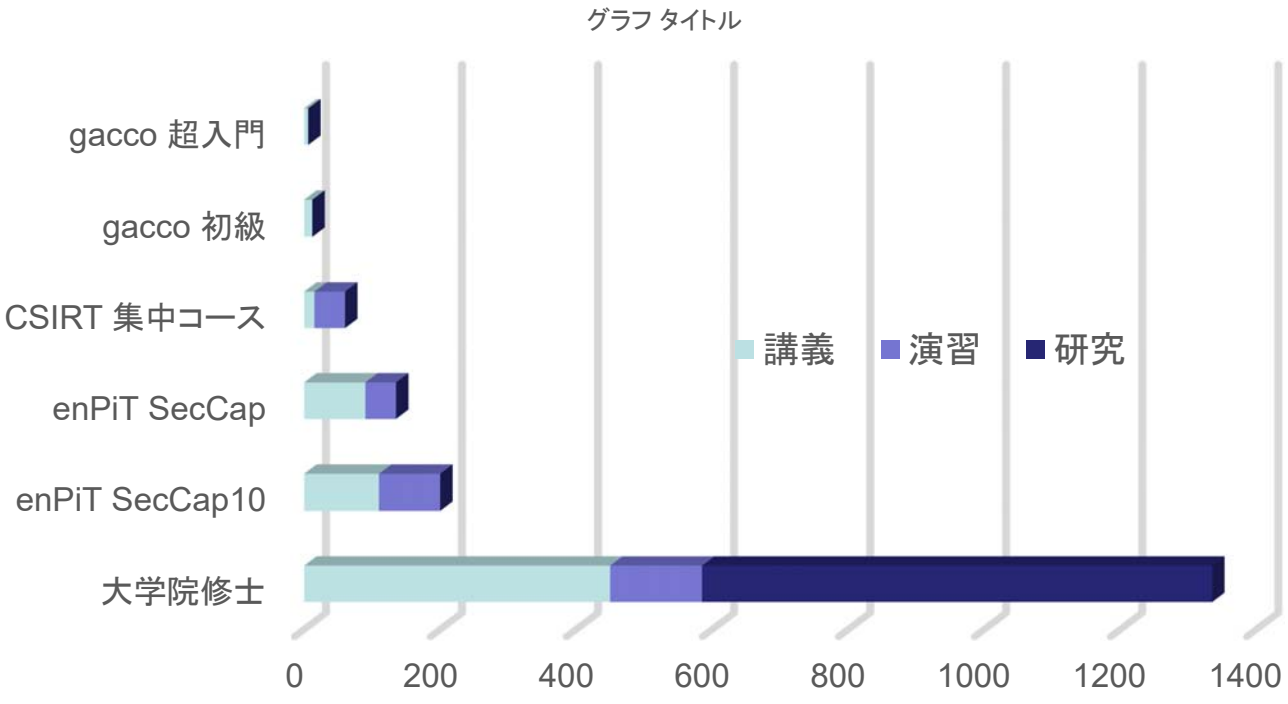
③情報セキュリティ大学院の社会人向け集中コース（2017年下期）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 2017年5～7月：CSIRT構築に向けた集中コース
  - CT-1 CSIRT構築の手引きコース（2日間, 8 units）
  - CT-2 ネットワークセキュリティ技術演習（2日間, 8 units）
  - CT-3 Webアプリケーション検査演習（2日間, 8 units）
  - CT-4 デジタルフォレンジック演習（4日間, 16 units）
- 2017年6月：Security-by-Designの集中コース
  - SD-1 Security-by-Designの基礎（2日間, 7 units）
- 日程調整中：実践サイバーレンジ演習コース（エキスパート向け）
  - 3コース×3日間（講義1、演習2）

セキュリティ人材育成への「時間」投資

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



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育成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）

◆ 調査の目的と体制

- ４つの部会で議論し、有識者会合でとりまとめ

◆ 情報セキュリティ教育の現状と社会的ニーズ

(1) 我が国における情報セキュリティ教育の実施状況

- 概況調査
  - 情報セキュリティ専門的教育の受講者数　1 年あたり 1,200 名弱程度
  - 情報セキュリティ関連科目を受講可能な人数　1 年あたり 20,000 名程度

  ⇒　5 年前の IPA 調査と比較して約 2 割の増加
- 東北地方を対象に深掘調査（理工系学部等の情報分野を網羅的に）
  - 13 機関中 12 機関で何らか情報セキュリティに関する内容を教育
    - ただし、産業界が期待する内容・レベルとは異なるものも多いという課題も指摘
  - 聴取した大学教員のほぼすべてが情報セキュリティ教育の必要性を認識
    - 教育方針の優先度等により、十分な情報セキュリティ教育を実施できない大学が依然として存在

      ⇒ 他分野専門の教員が講義のなかで使えるような数時間程度の隣接・関連学科向け補助教材が役立ちそう

(2) これまでの情報セキュリティ教育に関する取組

- モデル・コア・カリキュラムが対象とする学士課程、修士課程及び社会人学び直しのそれぞれについて先行する事例あり
- 実践的教育や産学連携等の実施を通じて産業界が求める人材を育成するための工夫

(3) 海外における情報セキュリティ教育の動向

- ◆ 米国、EU、英国、イスラエルのそれぞれに、大学を巻き込んだ形の情報セキュリティ人材に関する政府機関主導の育成プログラム
- ◆ 情報セキュリティ人材のスキルを測定・評価するための指標を提供

  ⇒ 後述の例示③大卒程度の学生（または受講中の学生）が自身のレベルを確認するためのスキル評価があると良い

(4) 大学における情報セキュリティ教育に対する産業界からの要望

- 情報セキュリティの現場で直ちに必要となるような知識やスキルに関する要望
- 基礎力・ファシリテーション力・コミュニケーション力などへの期待
- 経済や心理との関係など、企業が手を出しにくい学問分野（社会科学系教員も参画）に関する教育への期待

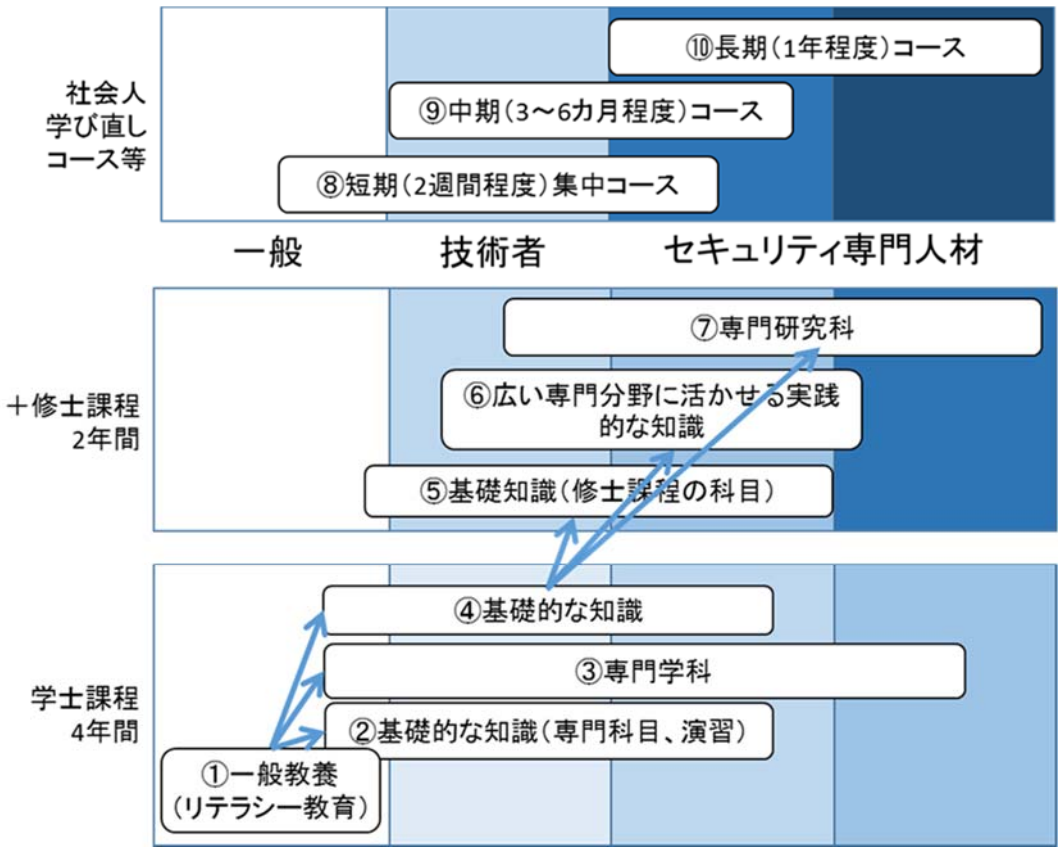


図　モデル・コア・カリキュラム 10 例示の位置づけ

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム

表　モデル・コア・カリキュラムの構成案

区分	例示ごとの定義	育成しようとする情報セキュリティ人材像	対象者（凡例参照）		
			専門人材	技術者	一般
区分1 学士課程４年間で卒業し社会に出ることを想定した区分	①一般教養としての情報セキュリティに関する講義を対象とするもの	日常の社会生活を営む上で必要なセキュリティに関する知識を備えた人材	○	○	◎
	②学士課程卒業後就職を予定している広く理工系に近い学生を対象とするもの	情報セキュリティに関する基礎的な知識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	○
	③情報セキュリティを専門とする学科等を対象とするもの	情報セキュリティに関する基礎的な知識・経験と意識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	△
区分2 学士課程４年間＋修士課程２年間の６年間の課程を経て社会に出ることを想定し、リテラシー教育が終了した学生（主に学部3年～修士1年）を想定した区分	④修士課程に進学予定の情報系学士課程の学生を対象とするもの	情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材	◎	○	－
	⑤情報セキュリティに関する単独の科目を対象とするもの	情報セキュリティに関する基本的な知識を備えた人材（セキュリティ分野への就職は前提としない）	△	○	○
	⑥専門とは別に情報セキュリティを学ぶコース等を対象とするもの	習得した知識・実践的経験を自らの専門分野のセキュリティ対策に活かせる人材	△	◎	－
	⑦情報セキュリティを専門とする専攻等を対象とするもの	情報セキュリティに関する専門的な知識と実践的な経験、及び意識を備えた人材（セキュリティの専門性をある程度発揮できる環境への就職等を想定）	◎	○	－
区分3 情報セキュリティに関して体系的に学び直したいと考える現役IT技術者（就職後10～15年程度（30代中～後半）の技術者）を想定した区分	⑧短期（２週間程度）集中コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	○
	⑨中期（3～6ヶ月程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	△
	⑩長期（1年程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	◎	△	－

◆ 今後のモデル・コア・カリキュラム活用の方向性

- 「社会で役に立つ人材の育成」という観点からの情報セキュリティ教育の意義
- 幅広い対象に向けた情報セキュリティ教育の必要性
- 国際的に通用する情報セキュリティ教育の実施
- 教科書の整備等と連動させることによる普及の促進

戦略的イノベーション創造プログラム（SIP）

重要インフラ等におけるサイバーセキュリティの確保

研究開発のねらい

国民生活及び社会経済活動を支える重要インフラ等へのサイバー攻撃の脅威に対し、強固なサイバーセキュリティを確保することにより、世界で最も安心・安全な社会基盤を確立する。

研究開発の背景

◆ 重要インフラ等の制御ネットワークシステムに対するサイバー攻撃の脅威が顕在化
ウクライナでは140万世帯が停電／復旧まで6時間

◆ 2020年オリパラでは重要インフラが最大の標的

制御ネットワークシステムの特徴

◆ サービス継続性重視
機密性よりも可用性、完全性を重視
セキュリティパッチ等の適用は最小限

◆ 数十年単位のライフサイクル
導入年代の異なる新旧機器が混在

制御ネットワークシステムを取り巻く状況

◆情報系ネットワークと同等のリスクの高まり
多様なルートでの情報系ネットワークとの接続
オフラインでの情報のやりとり
オープン化の流れ（汎用製品、標準プロトコルの採用）

◆ 効果的な対策が存在しない既存のリスク
製造～構築時（サプライチェーンリスク）や保守・運用時、
内部犯行等による機器／ソフトウェアのすり替え

◆ 技術トレンドへの追随
爆発的な数の（非力な）IoT機器の接続
仮想化技術の採用

◆ サイバー攻撃の高度化・巧妙化
⇒ 重要インフラ事業者間・分野間の情報共有
⇒ 重要インフラに加えサイバーセキュリティのスキル・知識を併せもった運用人材の育成

SIPにおける取組

制御ネットワークシステムのセキュリティ対策技術

真贋判定： 機器/ソフトウェアのすり替え対策（1-1）
動作監視・解析/防御： 新旧機器混在、仮想化技術（1-2a, 1-2b）
サイバー攻撃発生時も可用性担保（1-3）

ダイナミックマップ（データベース）インフラのセキュリティ強化 － SIP課題間連携（追加テーマ）－

⇒ *最新AI技術の活用により新たなサイバー脅威にも対応*

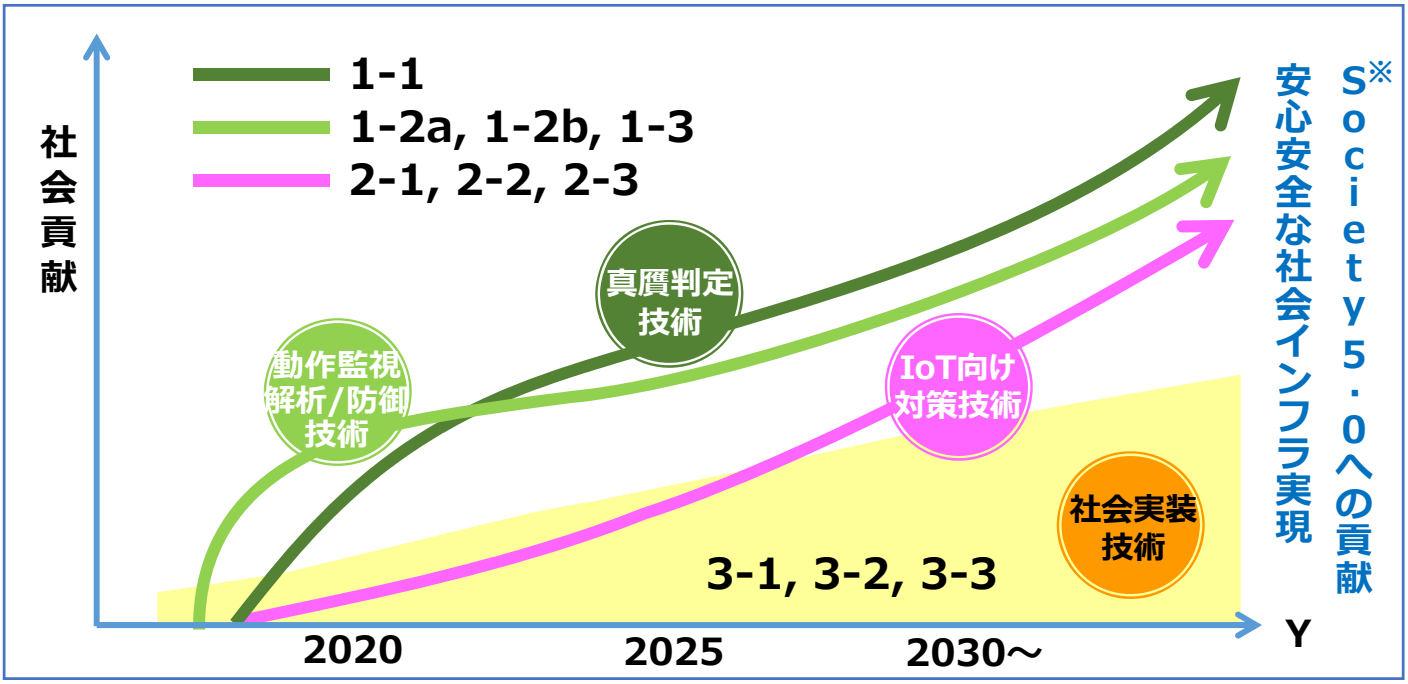
IoTシステムの普及拡大に先行したセキュリティ対策技術

新旧機器混在、爆発的なIoT機器増加（2-1）
非力なIoT機器（2-2）（2-3）

重要インフラのセキュリティを確保する社会実装技術

研究成果の社会実装を促す適合性確認のあり方（3-1）
情報共有を促進する仕組み（3-2）
サイバーセキュリティ人材育成（3-3）

■社会インフラへの貢献ロードマップ



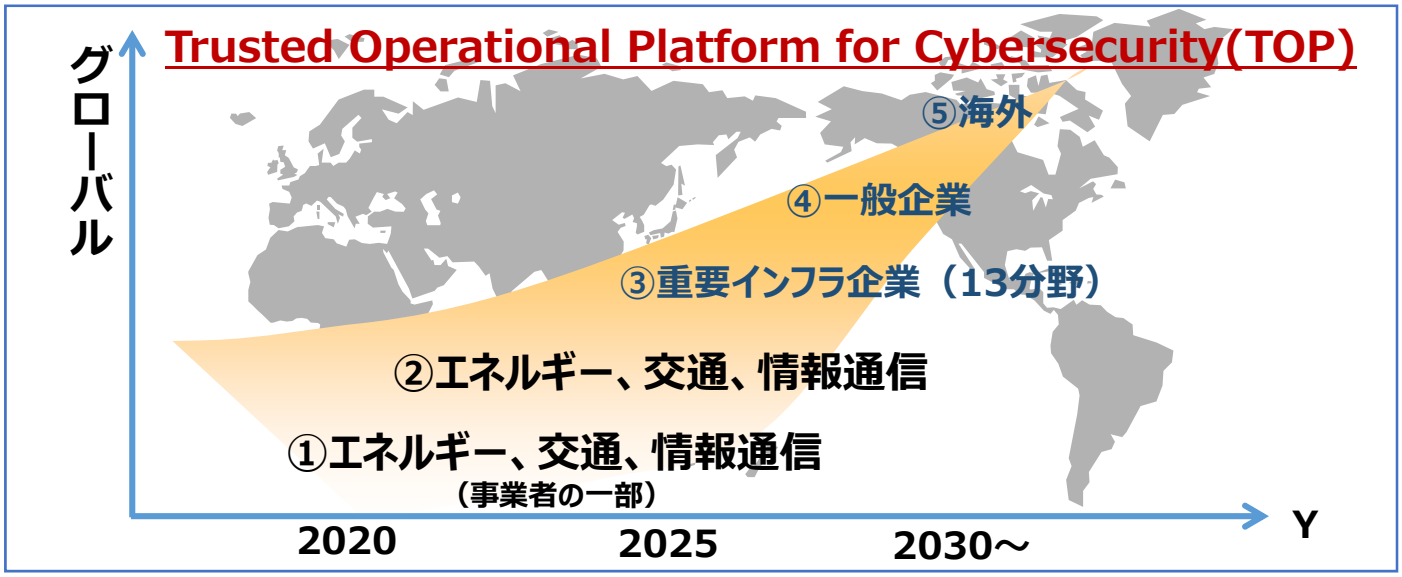
※ Society5.0： サイバー空間とフィジカル空間を高度に融合させ、経済的発展と社会的課題の解決を両立させた人間中心の社会
【「科学技術イノベーション総合戦略2016」（平成28年5月24日閣議決定）】より

戦略的イノベーション創造プログラム（SIP）

重要インフラ等におけるサイバーセキュリティの確保

■市場展開ロードマップ

オリンピックへの貢献を契機とし、重要インフラ企業を中心に国内のセキュリティ向上を支えるプラットフォームを提供し、将来的には重要インフラ企業以外の一般企業や海外への普及を目指す



Trusted Operational Platform for Cybersecurity（TOP）

- ◆ サイバーセキュリティの技術・導入・運用手順から人材までをセットで
- ◆ 国内外の優れたセキュリティ技術・ノウハウの受け皿になれる枠組み

本計画　（2016年1月～ 2019年度　予定）

コア技術

- 真贋判定技術
- 動作監視・解析・防御技術
- IoT向け暗号実装技術

社会実装技術

- 適合性確認のあり方
- 評価検証
- 情報共有
- 人材育成

【慶應義塾大学・名古屋工業大学】

サイバーセキュリティ人材育成

社会実装技術

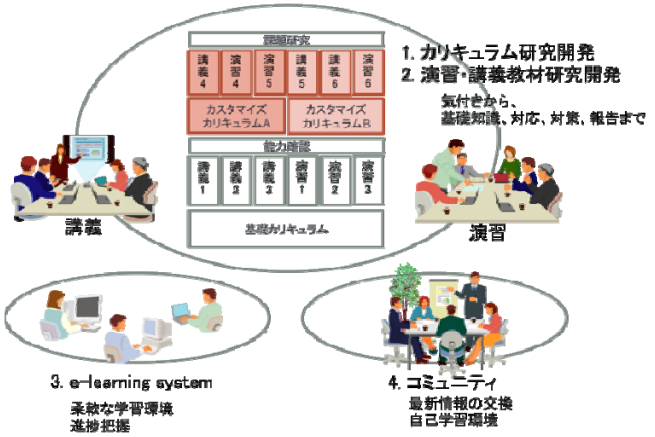
重要インフラ事業者において、セキュリティの知識を身につけた運用技術者を育成するための環境整備

特長

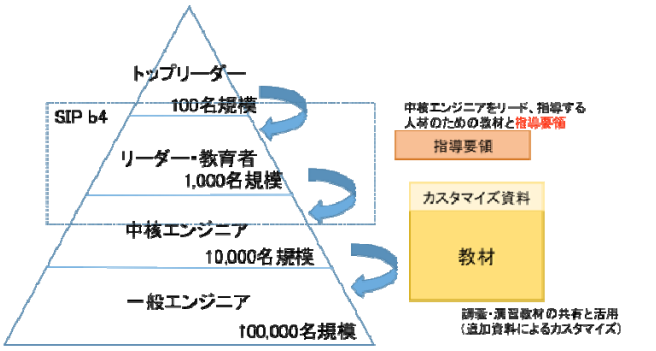
① スケーラブルな人材育成
各運用現場に対応したカリキュラム及び指導要領(人材育成カリキュラム)。
気付きから基礎知識、対応、対策、報告までを網羅した共有可能な講義・演習教材(講義演習教材)。

② 持続的な人材育成
柔軟な学習環境の実現(e-learning system)。
育成された人材が常に最新の情報を取得し、対応能力を身につけるコミュニティ形成(コミュニティ形成支援システム)。

概要



人材像と育成モデル



1,000名規模のリーダー及び教育者の育成と共有可能な講義・演習教材の作成

カリキュラム

実施状況

2016年度は、カリキュラムの研究開発として指導要領を作成。

また、講義演習教材の研究開発として4つの演習を試行し、受講者等からのヒアリング調査を実施。

スケジュール

2018年度末までに、リーダー及び教育者の育成カリキュラムと共有可能な講義・演習教材を作成する計画です。

2020年には、カリキュラムや講義演習教材、e-learning system、コミュニティ形成支援システム等の環境を整え、2020年以降も各組織における持続的な人材育成を可能とすることで、TOP構想の実現を目指します。

【慶應義塾大学・名古屋工業大学】

サイバーセキュリティ人材育成

カリキュラムの研究開発

指導要領の作成
・参考教科書
　電力制御システムセキュリティガイドライン（日本電気協会）
　スマートメーターシステムセキュリティガイドライン（日本電気協会）
・指導の手順
　教科書を使ってどのように教えるか？
　演習などのファシリテーション
　身近に感じる実例
・鳥の目と蟻の目
　俯瞰して全体を見通す力
　各問題に対する細やかな知識
・人材イメージ
　セキュリティマネジメント
　インシデントハンドラ
　インシデントレスポンス

試行演習の実施状況（1）

・無線LANセキュリティ演習
　実施日：2016/8/2
　会場：慶應義塾大学日吉キャンパス
　受講者数：5名
　概要：無線LAN機器に対してツールを用いたWEPのクラックと対処方法

・システム攻撃・防御演習
　実施日：2016/8/3
　会場：慶應義塾大学日吉キャンパス
　受講者数：11名
　概要：バッファオーバーフローを用いたシステムへの攻撃とその対処方法

試行演習の実施状況（2）

・インシデント対応とCSIRT基礎演習
　実施日：2016/8/4
　会場：情報セキュリティ大学院大学
　受講者数：9名
　概要：CSIRTの立ち上げ及びセキュリティインシデント対応の基礎

・制御系サイバーセキュリティ・ワークショップ CSIRT編
　実施日：2016/9/27
　会場：名古屋工業大学16号館
　受講者数：30名
　概要：制御系企業を対象としたセキュリティインシデント対応の基礎

演習のまとめ

＊攻撃体験型演習（無線LANセキュリティ、システム攻撃防御）＊
ほとんどの参加者は演習内容は担当外

ただし、直接担当していなくてもアクセス技術の脆弱性と無線技術や攻撃者の視点について知ることは有益だったと回答

また、具体的な攻撃を行うことで単なる知識から、具体的に脆弱性を体験できたことが大きいという声も複数あり

全般に、多くの攻撃手法とそれらへの対処方法を網羅的に学ぶことへの欲求が大きい

＊インシデント対応演習＊
CSIRT/SOCの構築や運用について参加者の満足度は非常に高く、組織の構築やマニュアル作成などのためのフレームワークとして高い評価

重要インフラのサイバー攻撃対策は、守るべきものをもとに考慮すべき

攻撃を想定しても、新たな攻撃は、たいてい想定外

ものに対するサイバー攻撃は、悪意の誤動作・悪意の誤操作とみなせる。従来より、安全対策として検討されたフェールセーフ・フールプルーフを徹底すればサイバー攻撃にも有効なはず。
安全検討をもとに、サイバー攻撃対策を立案する

攻撃の変化が早期検知できたとしても、検知者がみきわめてから他に知らせるのでは、被害が深刻化して、復旧も長期化する。
社内だけでなく社外も含めた組織的な連動も重要

防御演習の各事業所向きのカスタマイズ

重要インフラにおいて、サイバー攻撃で発生しうる事故は、鉄道、電力、放送など事業者によって異なる

守るべきものを知る者が、防御および攻撃を受けたときの対応のための演習を主体的に企画・実施すべき

各事業省用にカスタマイズできるテンプレートを開発して、そのテンプレートのカスタマイズを実行できる人材を事業所内に育成することが必要

各社での展開を考慮し、講師およびファシリテータに大学4年生を起用

テンプレート案による演習を9月27日に名古屋工業大学において施行