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 Security READY!!
IoTのセキュリティの特性と人材育成

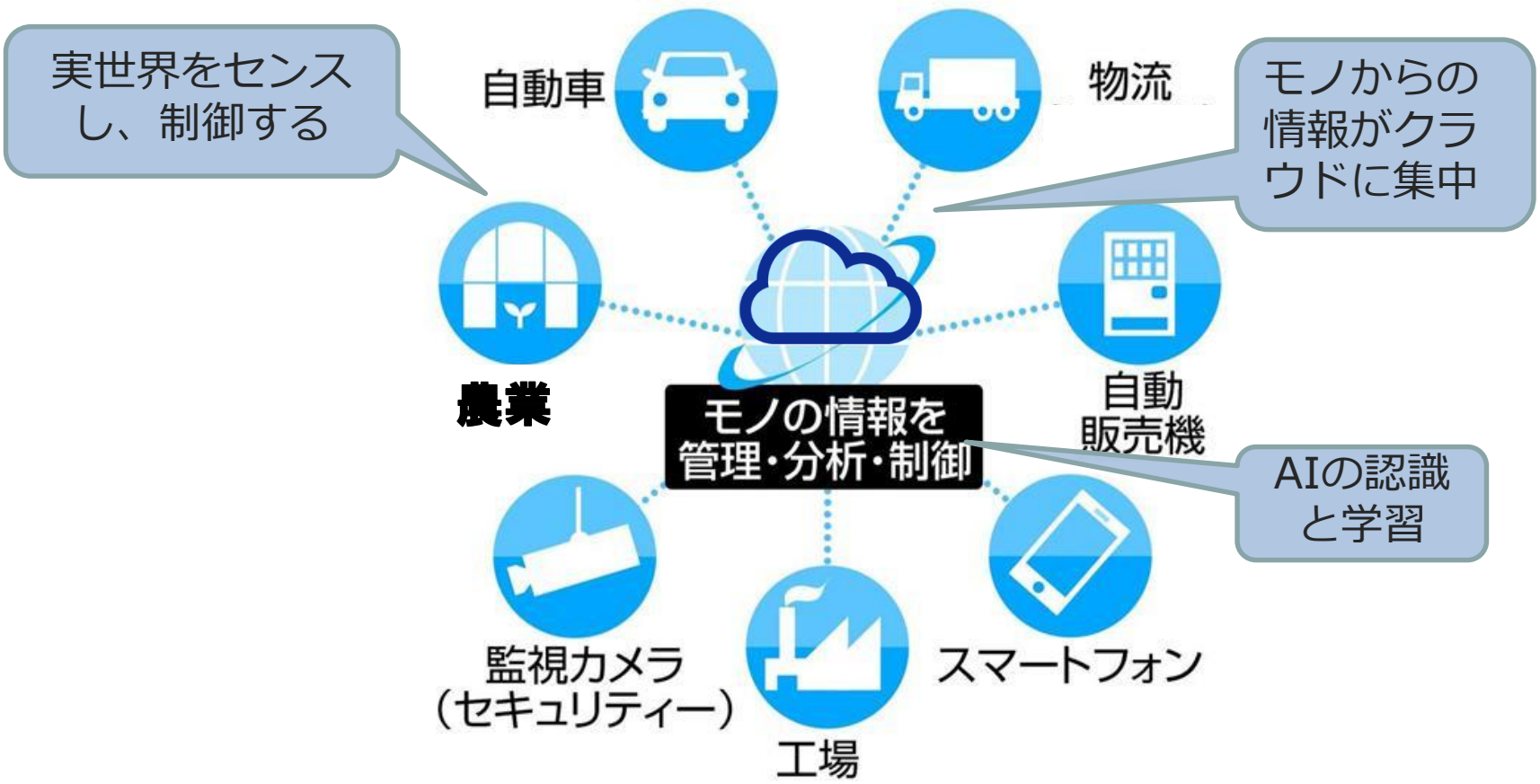
情報セキュリティ大学院大学　教授

国立研究開発法人　新エネルギー・産業技術総合開発機構　NEDO
技術戦略研究センター　電子情報機械システムユニット　フェロー

松井　俊浩

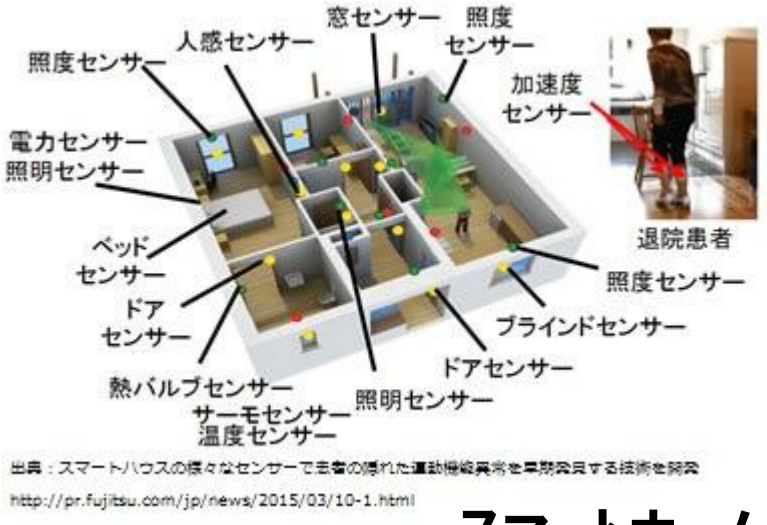
IoT（Internet of Things）とは

- P&G のKevin Ashton が、RF-IDの普及を指して初めて言った(1999)
- IDCは、「IP接続による通信を、**人の介在なし**にローカルまたはグローバルに行うことができる識別可能なエッジデバイス（モノ）からなる**ネットワークのネットワーク**」と定義



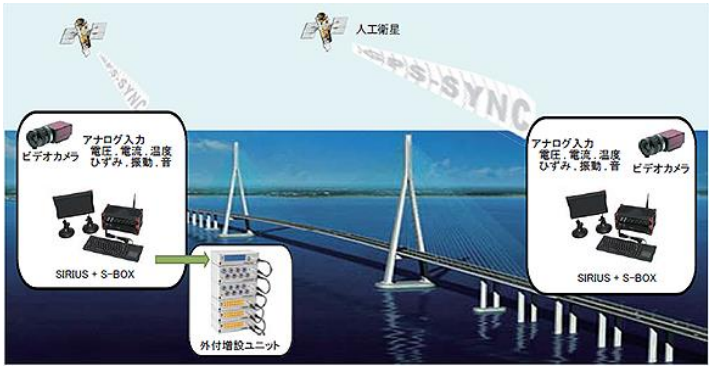
IoTの事例

ヘルスケア用ウェアラブル機器



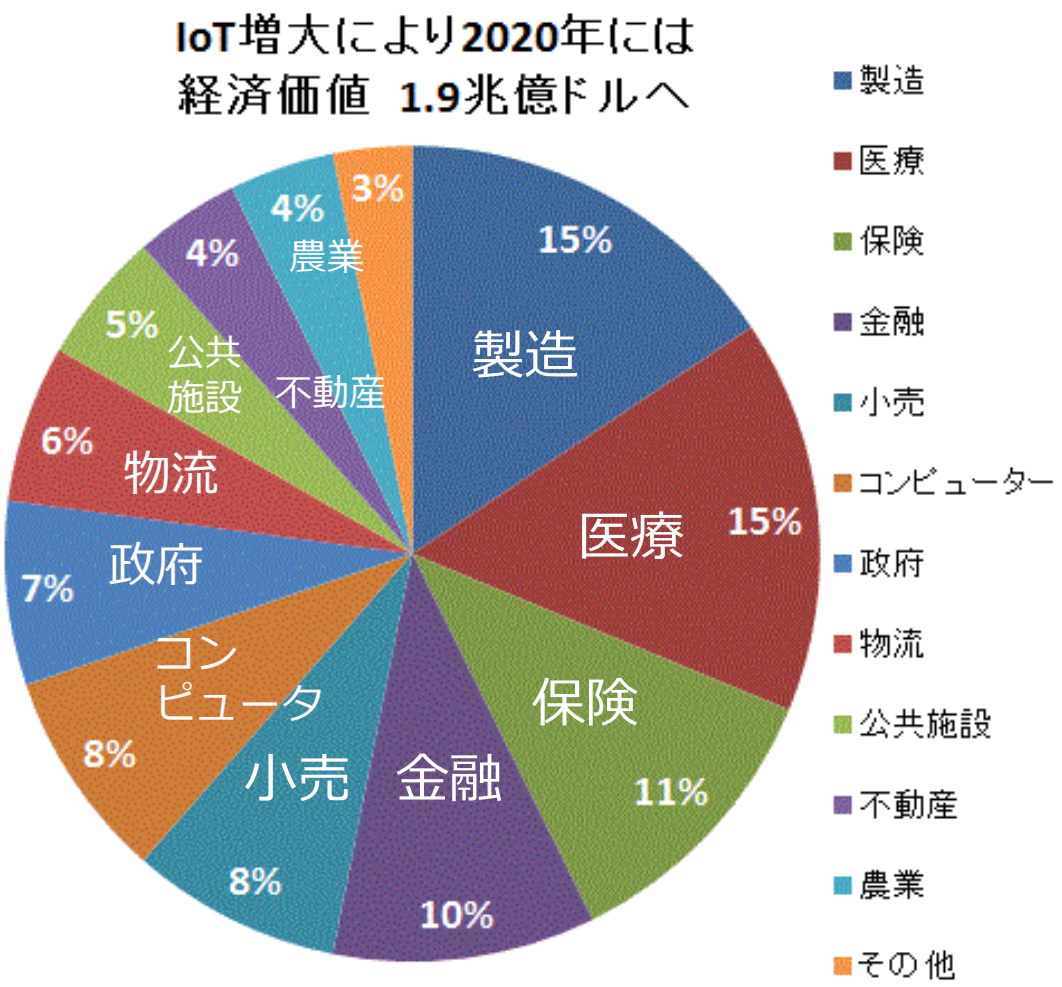
スマートホーム

産業機器の情報収集、メンテナンス



橋梁等インフラの老朽化センシング

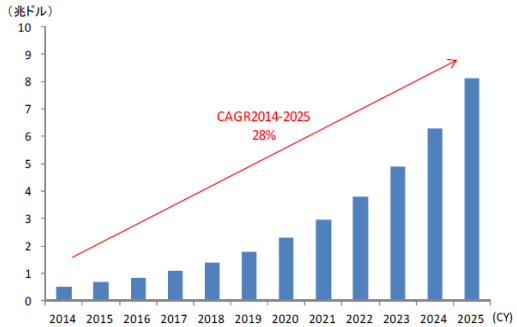
IoTの経済価値

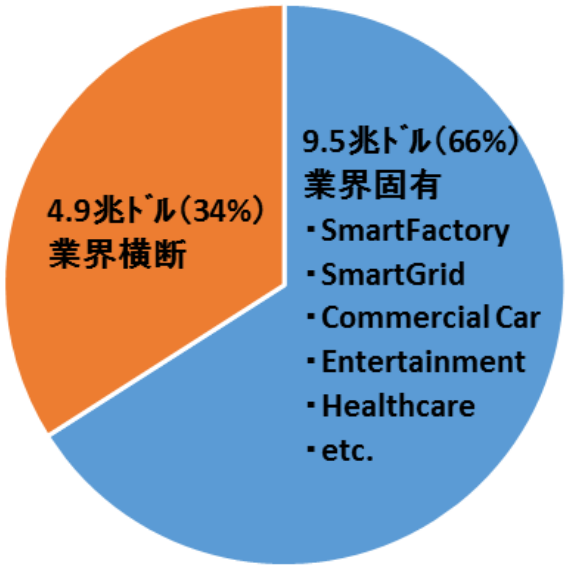


Gartner発表「Internet of Things Value」より作成

http://bdm.change-jp.com/?p=1790

年率28%の拡大





2022年IoE経済価値内訳

2017年のIoTテクノロジトレンド　トップ10
（ガートナー）

1. IoTセキュリティ
2. IoTアナリティクス　モノが収集する情報の解析方法
3. IoTデバイス（モノの健康）管理
4. 省電力・短距離ネットワーク
5. 省電力WAN
6. IoTプロセッサ　（暗号、省電力、ファームアップデート）
7. IoTのOS　(省電力、リアルタイム性、省メモリ、)
8. イベント・ストリーム処理　(大量データの並列処理)
9. IoTプラットフォーム　(ライブラリと開発環境)
10. IoT標準とエコシステム　（API）

IoTセキュリティ侵害の事例

家電
アイロン

BBC News - Russia: Hidden chips 'launch spam attacks from irons'
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337

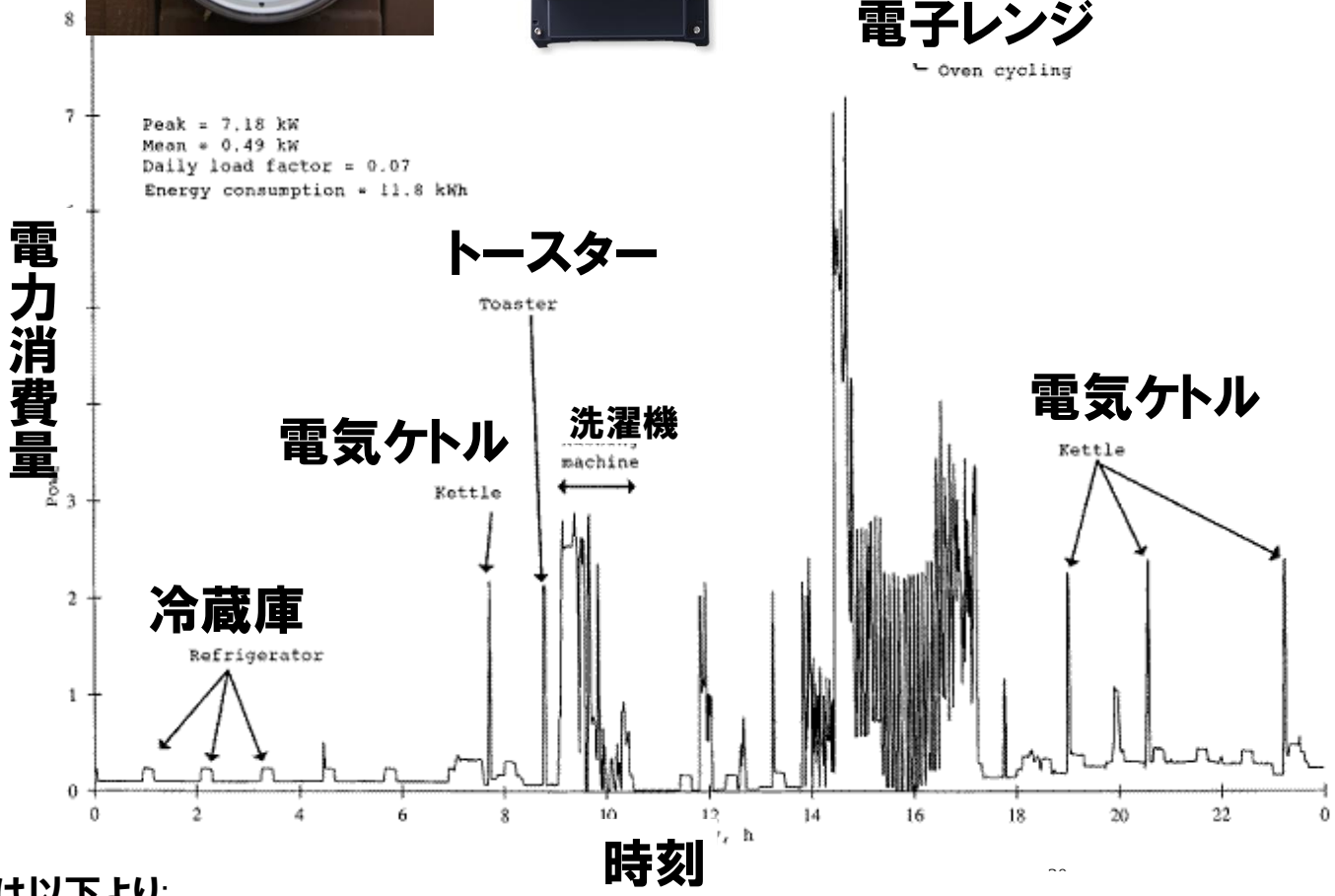
中国から輸入された電気式アイロンに隠されていたのは小さなチップ。このチップは半径200m以内で暗号キーなしで接続できるWi-Fiを利用しているPCに侵入し、ウイルスをまき散らすように設計されていたとのこと。

似たようなチップが中国製の携帯電話や自動車、カメラからも発見されており、専門家は「電化製品や自動車に隠されていたチップは、会社のネットワークに侵入しスパムメールを送信することに使用されていたものでしょう」と話しています。

- 2013年10月22日　英国BBC
- 電気ケトル、偽iPhoneからも発見された。
- WiFi経由でPCをマルウェアに感染させる。
- 仕様上の重量とわずかな差があったことから発覚した。

- 2014年1月、10万台以上のテレビや冷蔵庫、ネットワークルーターなどのスマート家電から、75万通以上の不正メールが送信された。「物のインターネット」を利用したサイバー攻撃の最初の事例(日本経済新聞 http://www.nikkei.com/article/DGXNASFK2000I_Q4A120C1000000/)
- 2016年1月、Insecamというサイトが、世界中の監視カメラの映像を配信、パスワードがデフォルトのまま。世界で75,000台、日本では1,800台が見える。スマフォカメラも同様の危険性あり。
  http://www.insecam.org/
- 2016年11月、家庭のIoT機器悪用、ルーター販売停止　スマートフォンやデジタルカメラからWifiで接続し、画像やメッセージを共有するWifiストレージポケドラが、ウィルスに感染し、情報を抜き取られたり、DDoS攻撃の踏み台にされる恐れがあるとして販売中止。 http://www.danshihack.com/2016/01/21/junp/website-insecam.html

例：スマートメータのプライバシ問題

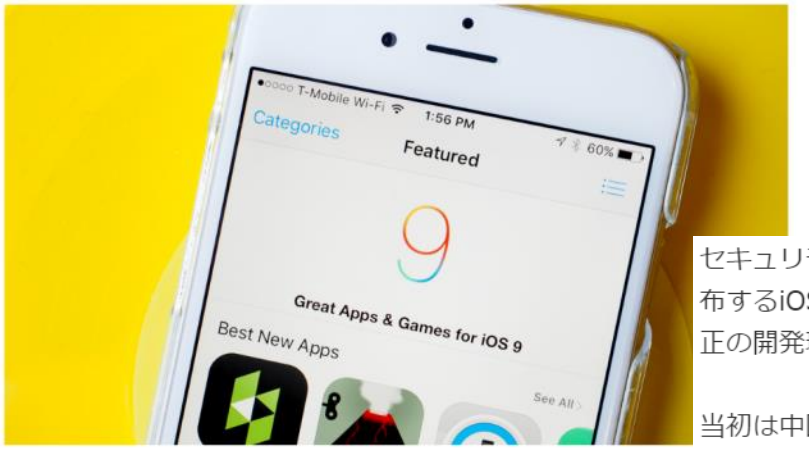


グラフは以下より:
NISTIR 7628, Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

9

App StoreのiPhoneアプリ多数にマルウェアが混入、パスワード盗難の危険。中国発の改竄コンパイラXcodeGhostが原因

BY MUNENORI TANIGUCHI • 2015年09月20日 21時10分 0



セキュリティ対策ソフトメーカーのパロアルトネットワークスが、中国のアップル App Store が配布するiOSアプリにマルウェアが混入しているものを発見しました。マルウェアは改ざんされた非純正の開発環 境 XcodeGhost を使って作られたことが分かっています。

当初は中国国内のみのわずかなアプリでしか見つかっておらず、端末から個人情報を抜き出すだけのものと思われていましたが、最新の情報ではすでに数十～数百の感染アプリがみつかり、WeChat など各国で配布される著名アプリにも感染が拡がっています。

App Storeでアプリを配布するには、アップルが提供する開発環境 Xcode を使って開発し、公開前には必ず審査を受けなければなりません。 にもかかわらずマルウェア感染アプリが多数出回った背景として、 パロアルトネットワークスは Xcode を改ざんした"XcodeGhost"が出回っていると指摘します。

Xcode はアップルが開発者に無料配布しているものですが、中国ではアップルの公式サーバとのネットワーク環境が極端に悪い場合があり、違法に二次配布配布を行うサーバーも点在しています。XcodeGhost はそうした転載サーバーに、通常のXcodeを装って登録されていました。

http://japanese.engadget.com/2015/09/20/app-store-xcodeghost/

IOTセキュリティの特性

IoTセキュリティガイドライン

総務省と経済産業省

① 脅威の影響範囲/影響度合いが大きいこと
- グローバルなインターネット、数が多い

② IoT機器のライフサイクルが長いこと、長寿命性
- 長期の機器保守に使われる、対象機器より長寿命

③ IoT機器に対する監視が行き届きにくいこと
- 小さくて多数、設置を忘れられる、監視機器の監視はしない

④ IoT機器側とネットワーク側の環境や特性の相互理解が不十分
- 専門家でなくても、誰でも使える

⑤ IoT機器の機能/性能が限られていること
- 最も安価なハードウェアを使用、暗号や認証が限定的

⑥ 開発者が想定していなかった接続が行われる可能性があること
- 動的社会、継続的な機能拡張

http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

IoTセキュリティ事情（松井）

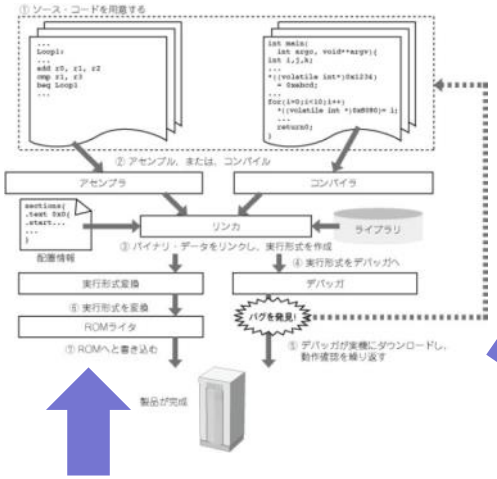
1. デバイス、ソフトウェアの多様性
   - 個別に対策が必要
   - セキュリティの非専門家が設計し、脆弱性が残る
2. M2M: 人が介在しない、装置同士の接続が行われる
   - パスワード認証が使えない→通信の偽装
3. 実世界性： 実世界の物理的実体を制御すること
   - データセンターに隔離できない
     - タンパー攻撃、リバースエンジニアリングが容易
   - 実時間制御を阻害するだけで致命的被害
4. 多数性： 実世界に多数が普及すること
   - 攻撃者の手の届く場所にあること
5. クラウドへのデータ集中

IoTデバイス=組込みシステム

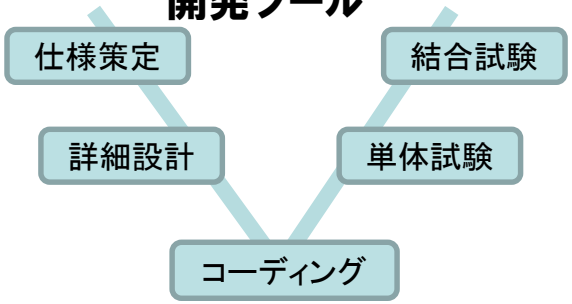
マイクロコントローラ

ECU (**電子制御装置**)

組込みソフトウェア



開発ツール



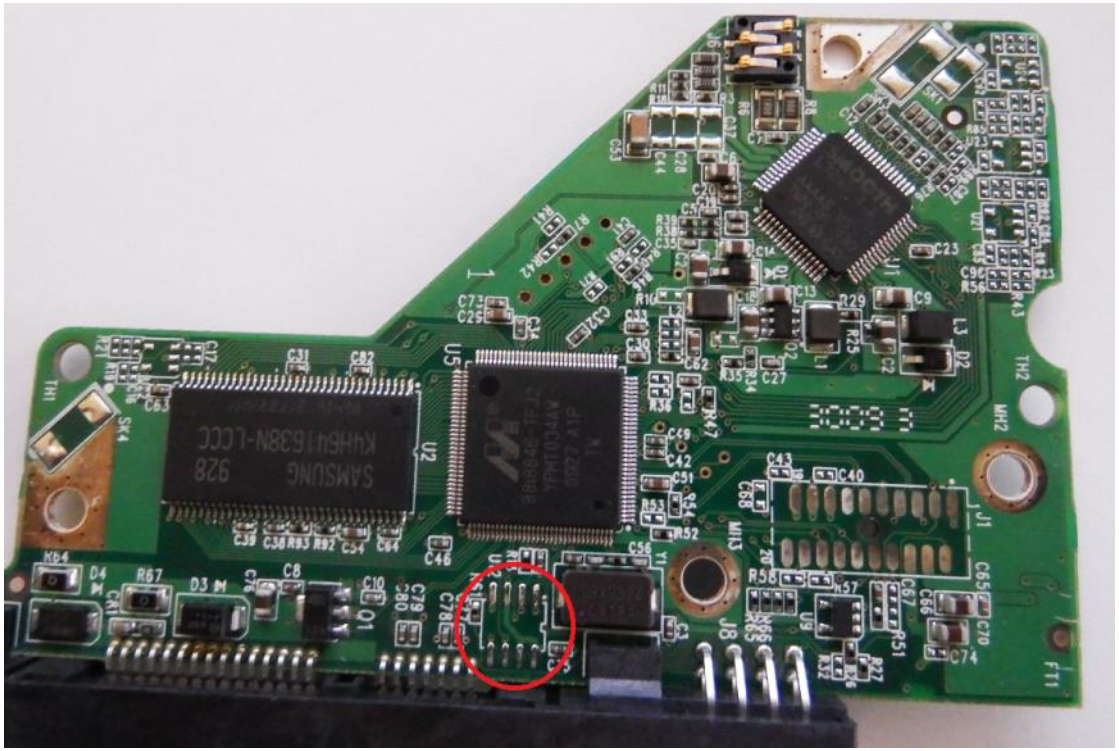
マイクロコントローラ

- Network インタフェース
- CPU
- メモリ
- デバイス インタフェース

IoTのイメージ

PCの主要部をワンチップ化

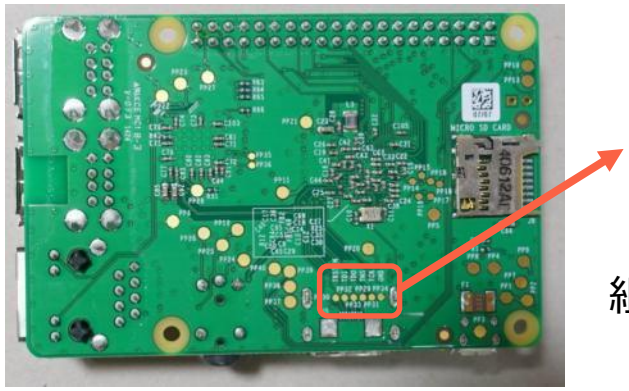
Test padsとOBD-2、JTAGポート



- OBD: On-Board Diagnostics, ISO-14230
- JTAG: Joint Test Action Group, IEEE-1149.1

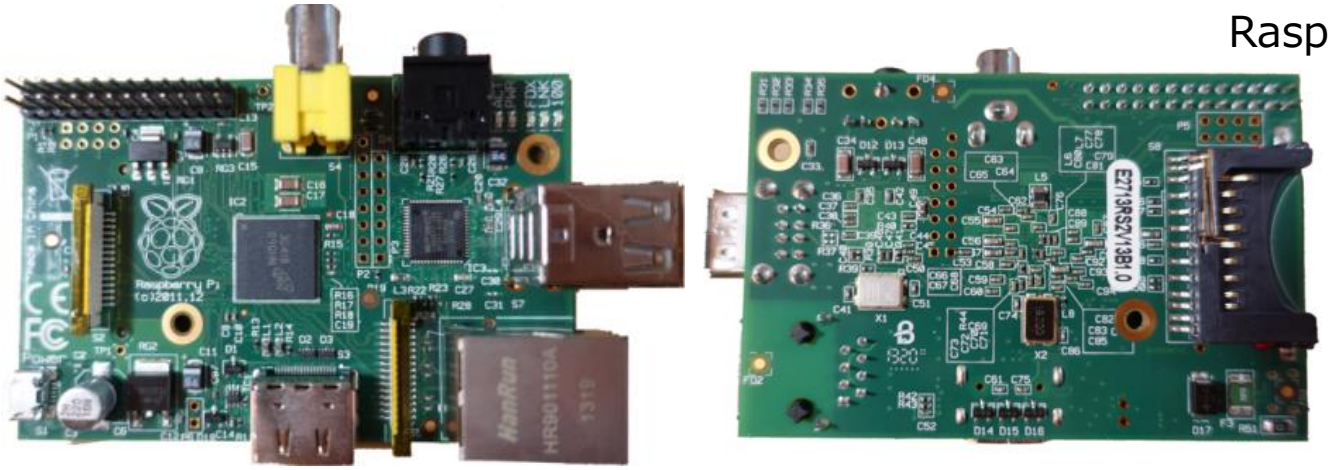
マイクロコントローラのデバッグ機能

- CPUエミュレータ
- ICE: In-Circuit Emulator
  - debug機能を備えたCPUを別途提供し、差し替え
- JTAG
  - IEEE1149.1、標準的な接続法
    - ◆TCK（クロック）
    - ◆TDI（データ入力）
    - ◆TDO（データ出力）
    - ◆TMS（状態制御）
  - ベンダー独自のインタフェースを使うと、内部メモリの読み書きやプログラムの解析が可能になる



組込システムの開発･保守ポート
組込学習ボードRaspberry Piのボード裏面にあるテストパッド。TRST, TDI, TDOなどは､JTAGの信号名。

Raspberry Pi-2



テストパッドは隠しても、LSIにはピンが出ている

組込機器のセキュリティ脅威

- JTAGから侵入、テストバッドから接続できることがある
- Bluetoothからデバッグポートに入れるモノがある
- デバッグポートから内部メモリの読み出しが可能
  - プログラムを解析して、脆弱性を発見される
- 内部メモリ(フラッシュ）に書き込みが可能
  - プログラムを改編してバックドアを付加
- 公開されることが多いアップデートプログラムからも侵入可能
- その他にもサイドチャネル攻撃
  - クロック・グリッチ攻撃
  - 電力解析
  - 電磁波解析　→　テンペスト攻撃
- たとえば自動車の修理工場や､公共の駐車場で攻撃者にさらされる
- 整備、補修用のポートは保護しにくい

IoTの特徴とセキュリティ脅威

- 現場の微小な情報がデジタル化、オンライン化される
  - 個人のプライバシー
  - 自動車のGPS情報
  - 工場の製造パラメータ
- ビッグデータがクラウドに収集、蓄積される
  - 大量の情報漏洩が起こりうる
- 人間が介在せず、M2M、C2Cの情報交換
  - スマートフォンが場所、移動経路、歩数などをアップロード
  - 車車間通信が、障害物の情報を交換
- 実世界のモノを動かす
  - 工場のロボット
  - 手術室や医療器具
  - 自動車
- PC以外の機器が、Wirelessでインターネット接続

機密性の問題

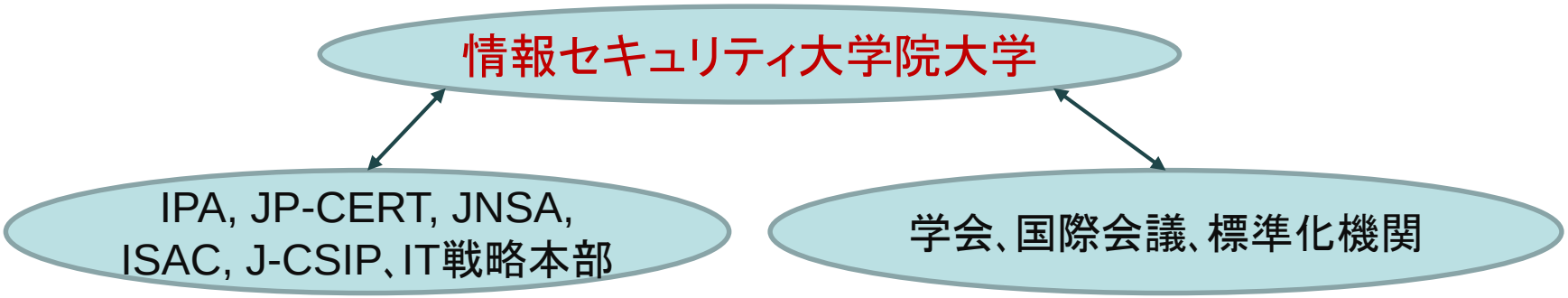
可用性、完全性の問題

IoTセキュリティを守る

- 使う人
  - パスワードを付ける、長いパスワードを使う
  - 認証された機器、ベンダーを使う　(CC、EDSA、CSMS、、、)
  - 部外者が触れないように物理的に保護
- 作る人
  - セキュリティ脅威を予測する
    - ◆リバースエンジニアリングされるかもしれない
  - セキュアな設計をする、セキュアなプログラム開発
  - セキュリティアップデート?
  - 多重の防護、回復策
  - テストする、認証を受ける

IoTセキュリティの課題と対策

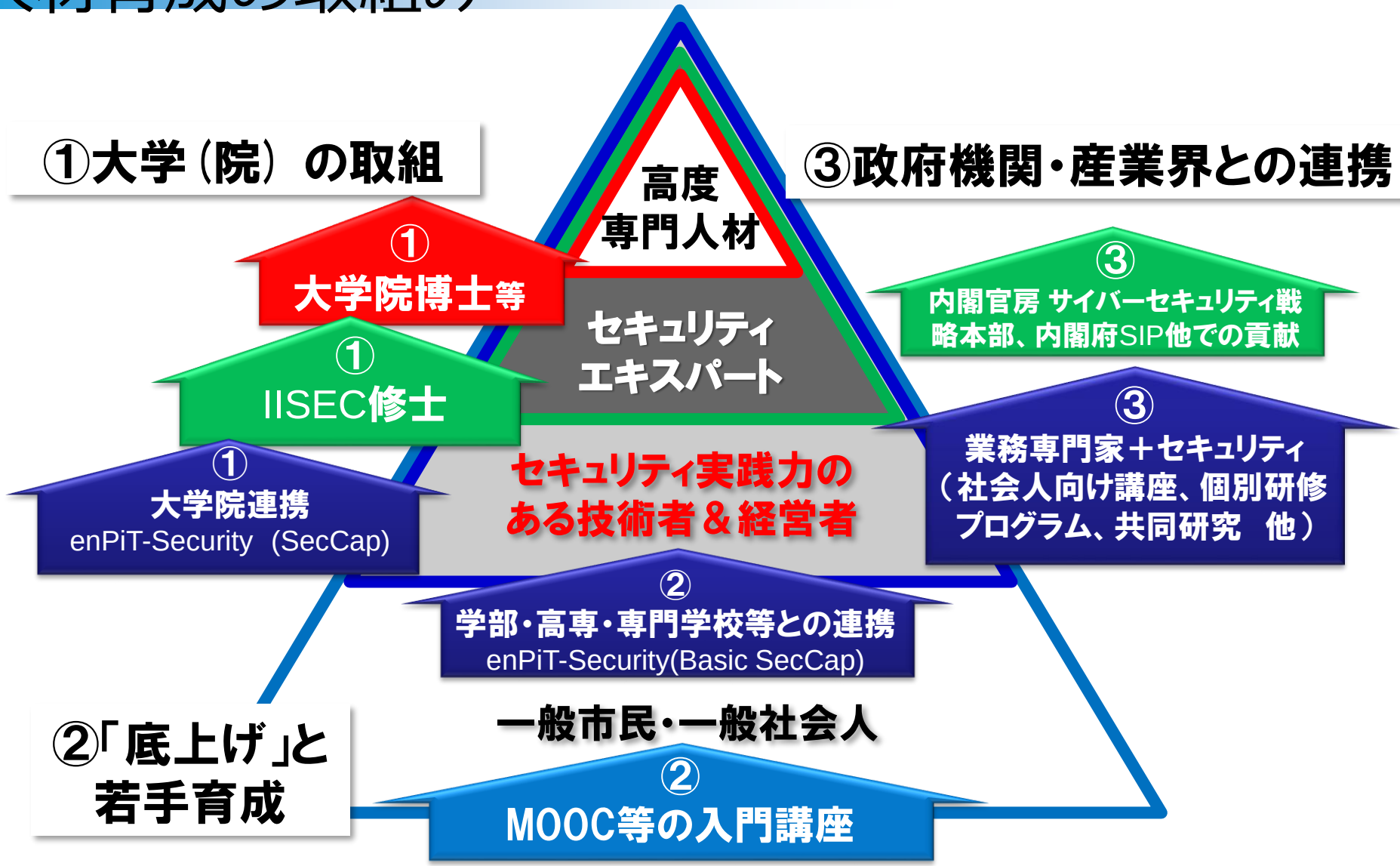
- 多様なデバイス、多様なサービス　←→　PC+Web
- それぞれについての情報が少ない
  - どういう技術が使われていて、何が起こっているのか?
- IoTセキュリティに関する産と学の情報共有
  - 事例のご相談
  - 学生としての人材派遣
  - 共同研究



情報セキュリティ大学院大学
(IISEC)
研究

情報セキュリティ大学院大学
人材育成の取組み

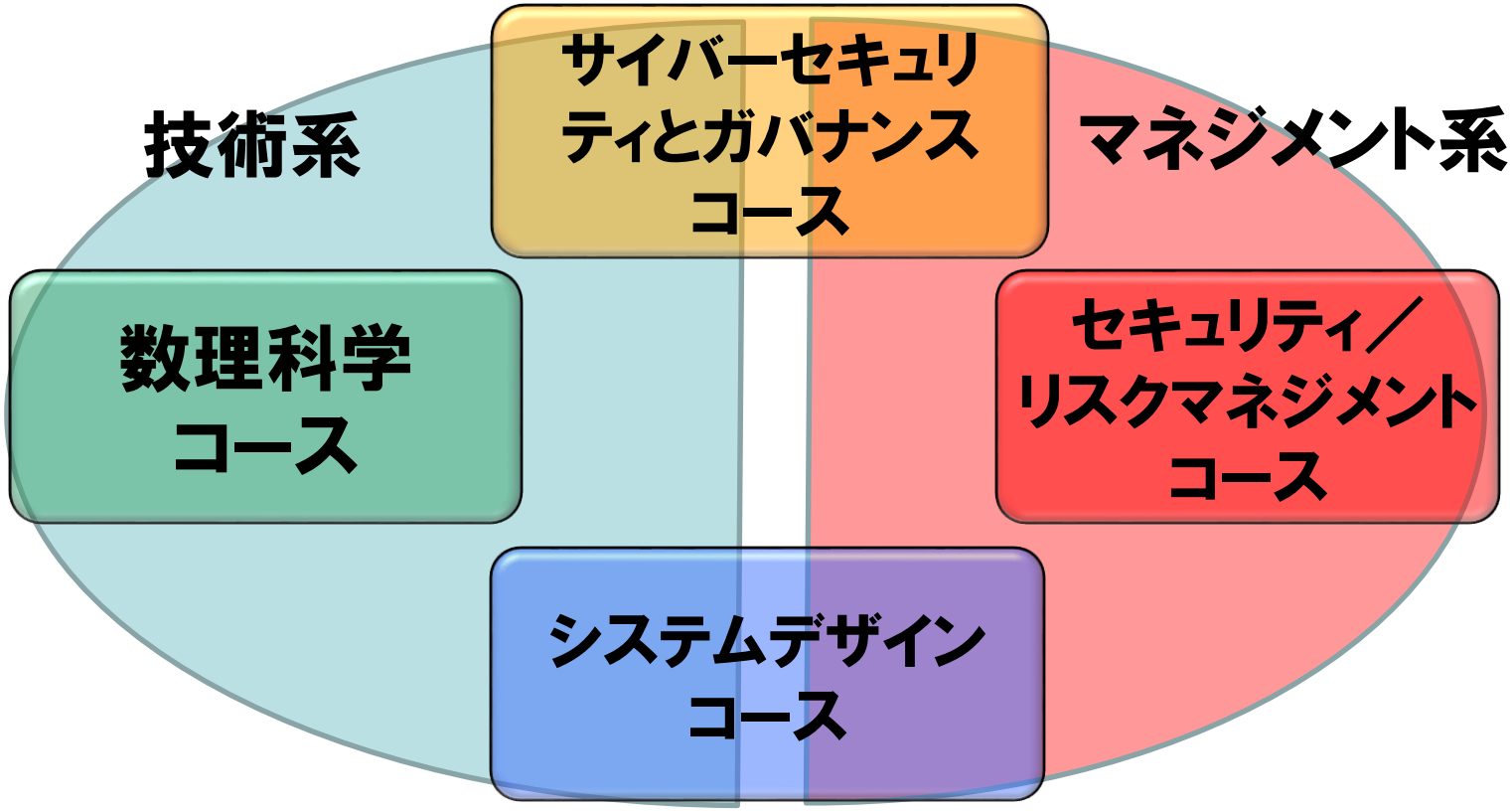
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



総合科学：情報セキュリティ力リキュラム

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

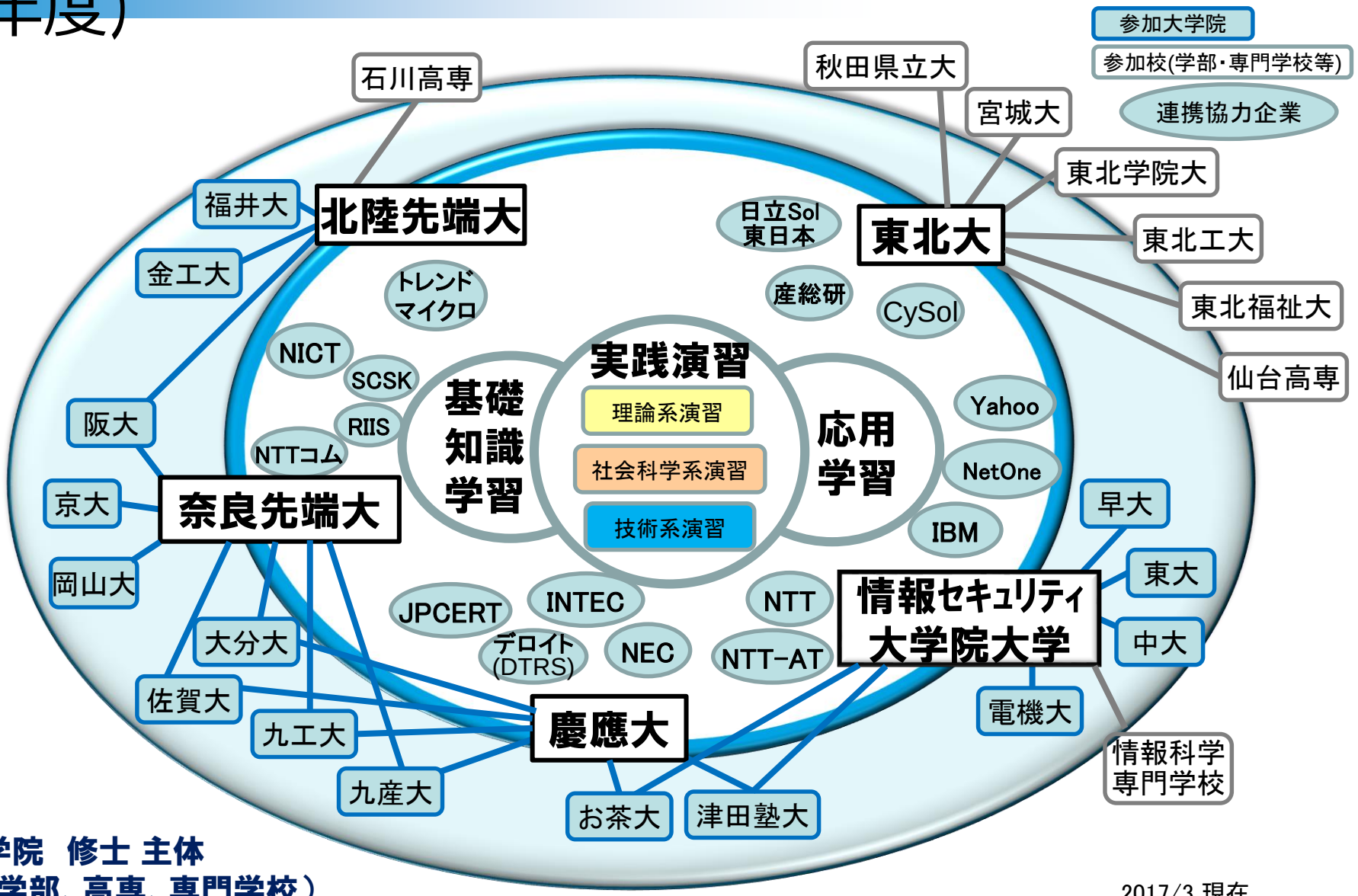


- 効率的な1-2年制の修士課程と、1-3年制の博士課程
- 数理、技術、法律、制度、国際標準など幅広い教授陣
- 社会人教育に強み
- 横浜市神奈川区鶴屋町2-14-1　（横浜駅きた西口徒歩1分）

情報セキュリティ大学院大学の実績

- 2016年度までに、339名の修士、30名の博士を輩出
- 情報セキュリティ教材開発の実績
  - 文部科学省2007年「先導的ITスペシャリスト育成推進プログラム」、ISSスクエア
    - ◆ 情報セキュリティ大学院大学、中央大学、国立情報学研究所他、企業・研究機関11社の産学連携による高度情報セキュリティ人材育成プログラム
  - 文部科学省2012年度「情報技術人材育成のための実践教育ネットワーク事業」enPiT-Security, SecCap
  - 文部科学省2016年度「高度IT人材を育成する産学協働の実践教育ネットワーク」enPiT-2
  - IPA2017年度「安全安心なシステムの設計・開発のためのIT人材育成教材等開発事業」
- 研究プロジェクト　JST_CREST,　SIP, 科研費など
- 社会人向けセキュリティ集中講座

参加大学と協力企業の拡大（2016年度）



大学院　修士 主体
（＋学部、高専、専門学校）

2017/3 現在

参考：IISECの修了生と本年度の学生

- 官公庁派遣（2割⇒**3割**）
  - 外務省、防衛省、海上保安庁、警察庁、警視庁、埼玉県警　他
  - 金融庁、国立印刷局
  - 横浜市、神奈川県

東京五輪対応？

金融インフラ

- 企業派遣および社会人自主（**5割**）
  - 通信キャリア系、大手ＩＴベンダー系
  - 機械、プラント系の製造業
  - 鉄道系および情報システム会社　**交通インフラ**
  - 金融系（Y銀行、E銀行、クレジット系、他）**金融インフラ**
  - 非ＩＴ系企業（**テレビ放送**、報道系、石油系、印刷系、他）
- 他大学の学部からの進学した学生（3割⇒**2割**）
  - セキュリティベンダー他
  - ＩＴ系企業、通信キャリア

人脈形成にも有効

IoT Security Ready!

- 後追い対応を余儀なくされることが多かったセキュリティ問題
- IoTでは、普及の前からセキュリティが注目されている
- 情報を共有して、事前に十分な対策を！