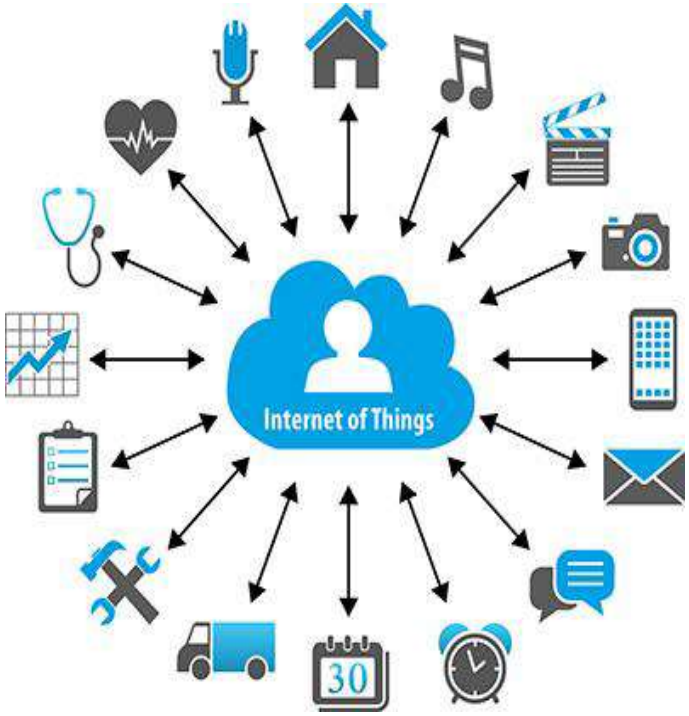
IoT時代に求められる
サイバーセキュリティ対策と人材育成

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

目　次

IoTがもたらす価値創造とリスク

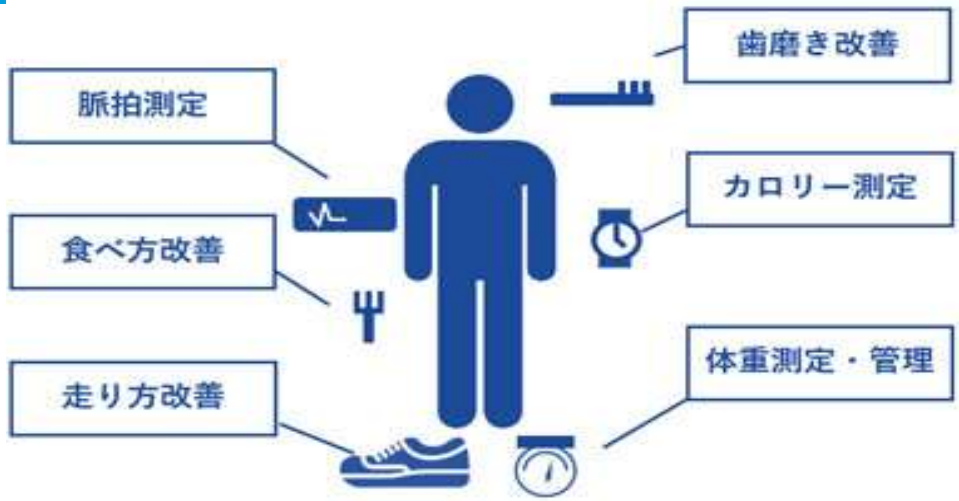


あらゆる「モノ」がネットワークで相互に接続
コンピュータによりインテリジェントな機能を発揮
新たなサービスを実現する価値創造のビジョン

https://www.altera.co.jp/solutions/technology/system-design/articles/_2014/internet-things-drive-innovation.html

IoTの応用事例

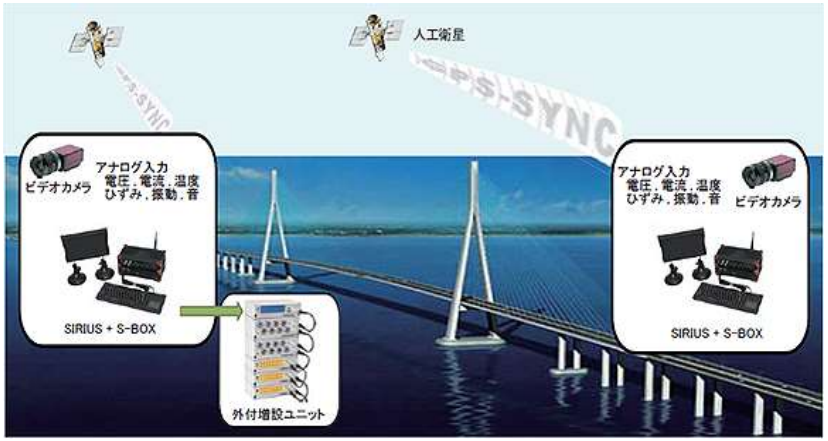
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



ヘルスケア用ウェアラブル機器

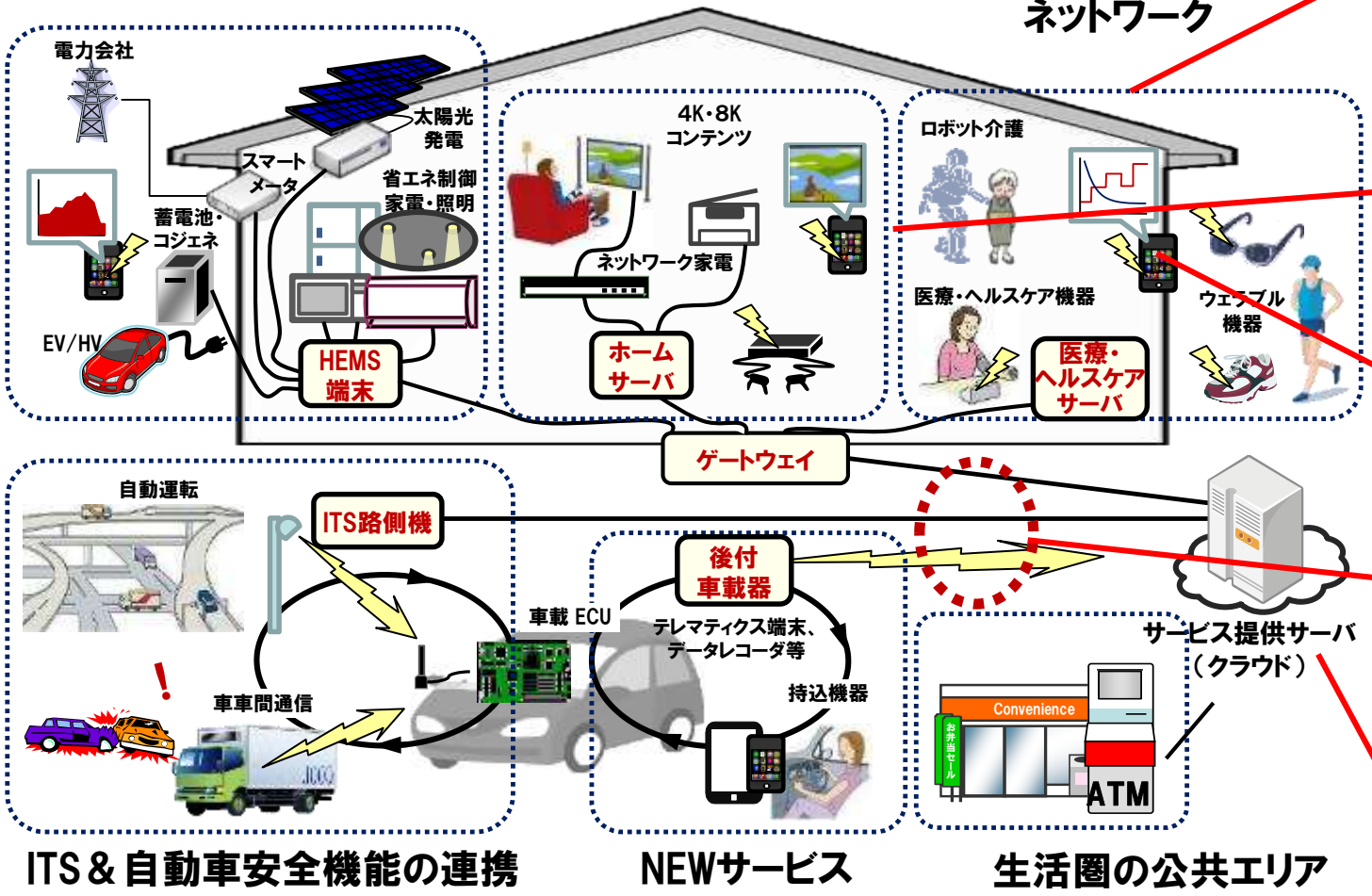
スマートホーム

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

つながるIoTサービス　－　リスクも拡大



何がつながっているか
分からない
＝脆弱な生活機器が
攻撃の入口に

分野ネットワーク間の連携
ができていない
＝他分野の生活機器の
思わぬ動作が影響

いたる所で生活機器と
モバイルデバイスが接続
＝モバイルデバイスが
脅威の運び役に

多くの生活機器が
サーバと通信
＝プライベートに係る情報の
漏えい、改ざんの危険性

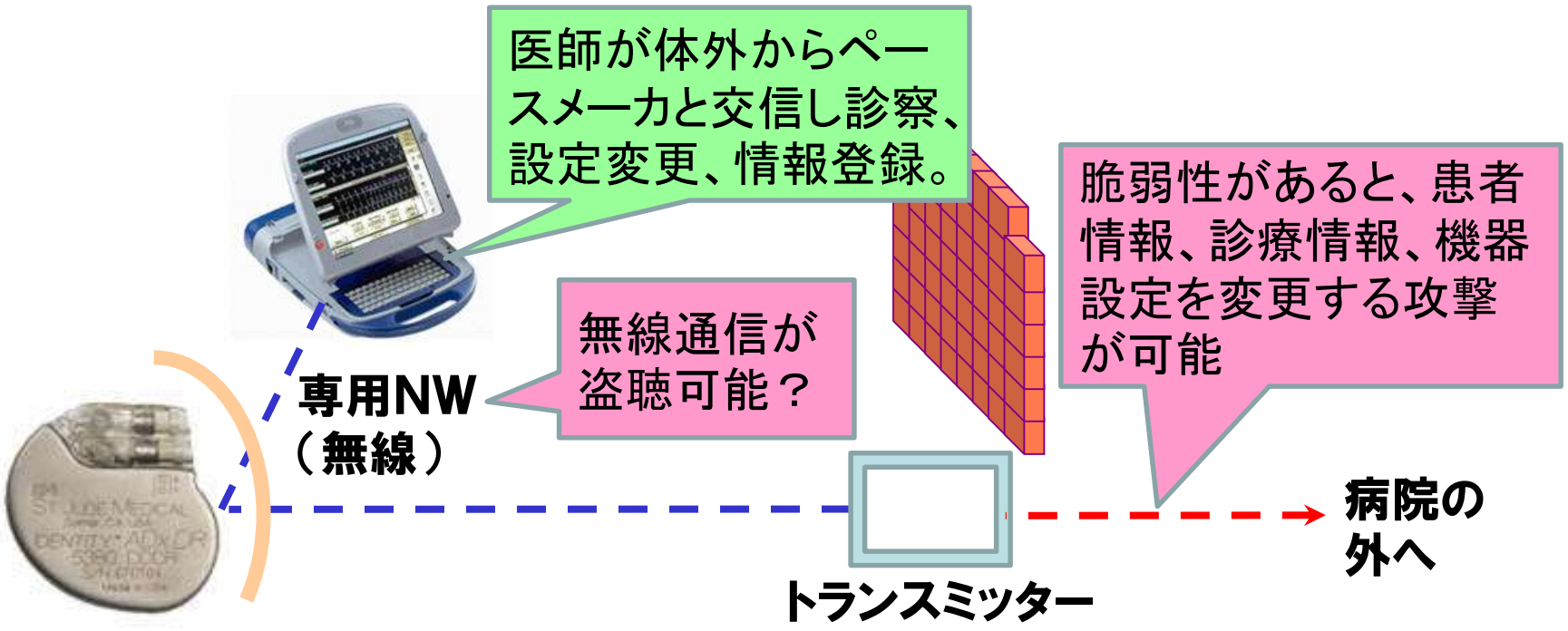
生活機器を遠隔から監視、
操作するサービスが増加
＝遠隔サーバの乗っ取りに
よる生活機器への攻撃も

出典：一般社団法人重要生活機器連携セキュリティ協議会 提言

ペースメーカー/ICD
不用意なネットワーク接続
2008年 IEEE Symposium on Security and Privacyにて報告

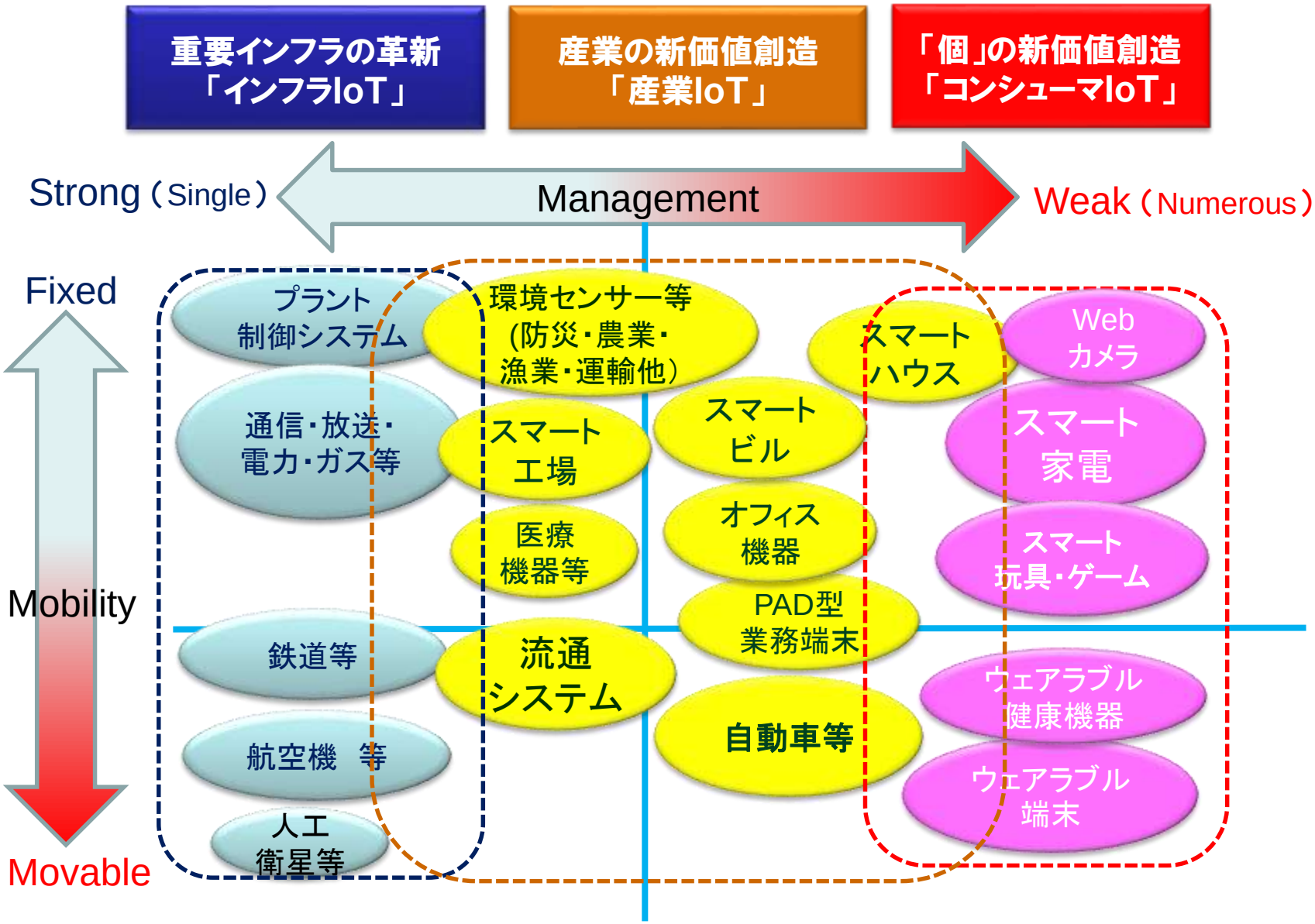
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 対象機器: ペースメーカー/ICD(埋め込み型除細動器)
  Medtronic Maximo DR VVEDDDR model #7278 ICD
- ワイヤレストランスミッタを用いれば、遠隔にデータ送信可能



出典: http://www.medtronic.com/us-en/healthcare-professionals/products/cardiac-rhythm/pacemakers/adapta.html

IoTの多様性


重要インフラの革新
「インフラIoT」
産業の新価値創造
「産業IoT」
「個」の新価値創造
「コンシューマIoT」
Strong（Single）
Management
Weak（Numerous）
Fixed
Mobility
Movable
プラント
制御システム
環境センサー等
(防災・農業・
漁業・運輸他)
スマート
ハウス
Web
カメラ
通信・放送・
電力・ガス等
スマート
工場
スマート
ビル
スマート
家電
医療
機器等
オフィス
機器
スマート
玩具・ゲーム
PAD型
業務端末
鉄道等
流通
システム
ウェアラブル
健康機器
航空機　等
自動車等
ウェアラブル
端末
人工
衛星等

Miraiの事案（2016）
IoT機器が社会インフラへサイバー攻撃

■ 脆弱性のあるIoT機器（ノラIoT）が大規模DDoS攻撃の踏み台

- 攻撃規模：600 ギガbps～テラbps
- Botの規模は10万台以上？
- 家庭用ルータ、監視カメラ、他の遠隔管理機能が悪用された模様

【事例1】 マネージドDNSサービス DynへのDDoS攻撃（2016/10）

- 約6時間にわたりサービスが不安定に
- PayPal, Twitter, Amazon, Netflixなども影響を受けた

【事例2】 DT（ドイツテレコム）のSpeedportルータをマルウェア感染させる攻撃（2016/11）

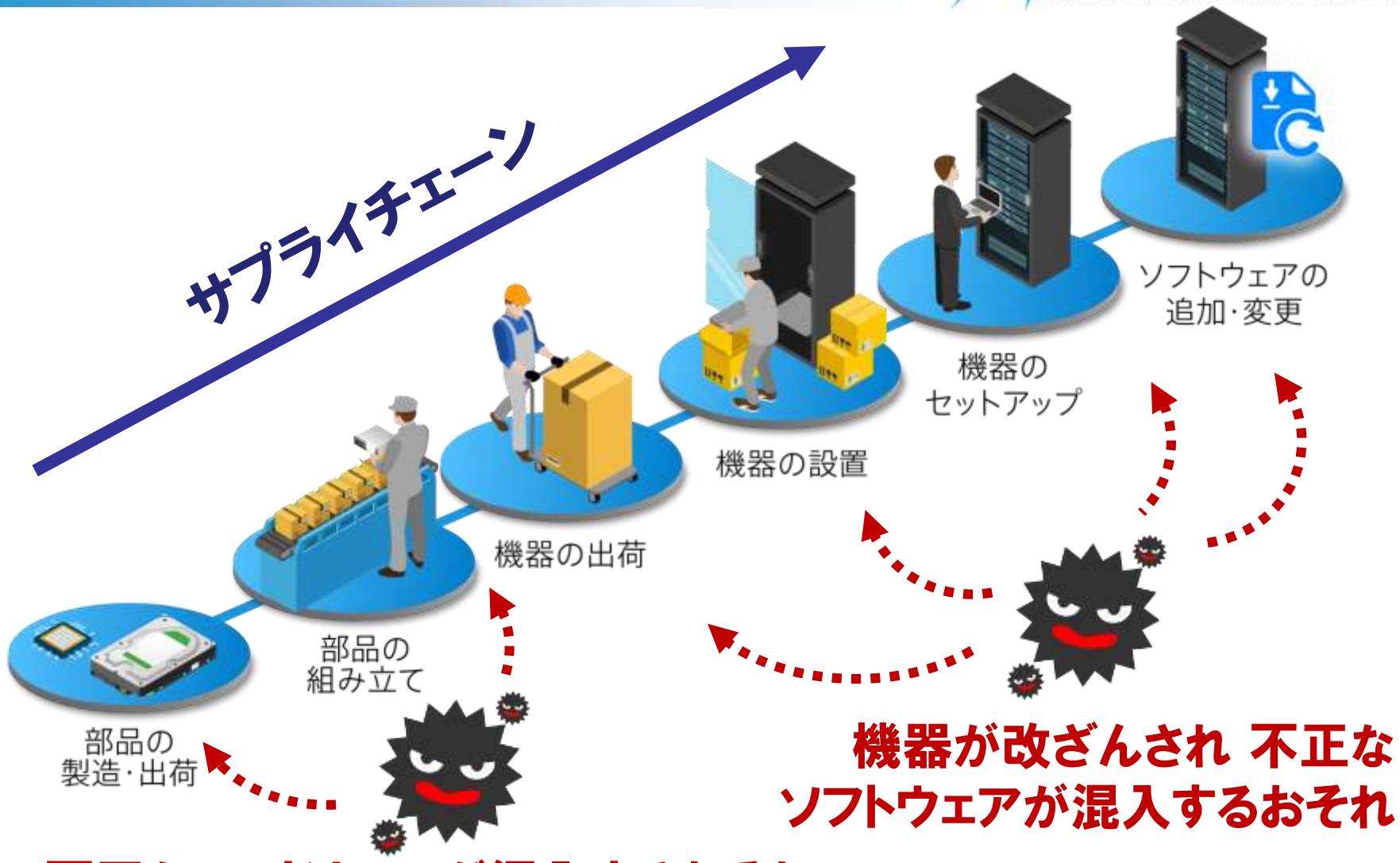
- 攻撃は失敗したが90万人が影響を受ける

JEEPハッキング事例（BlackHat2015）

- Chryslerのコネクテッドカーシステム「UConnect」の脆弱性
- リコール140万台で数十億円規模の損害が発生
  - Chryslerではパッチ提供して対応（USBまたは整備工場での更新）
- IoTシステム・サービスとしての課題
  - 通信サービスを提供する通信会社のシステムに脆弱性？
  - Jeep車載器に脆弱な通信サービスに備えた対策が備わっていなかった？

画像.ブレーキ不能で溝に(出典:WIRED)

サプライチェーンのリスク



IoTセキュリティと
サプライチェーンセキュリティ

内閣府SIP「第2期」での取組み

IoT社会に対応したサイバー・フィジカル・
セキュリティ

IoTリスクとサプライチェーンリスク

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リスク：サイバー攻撃の脅威が、あらゆる産業活動に潜む

世界のサイバー犯罪による経済損失は6,000億米ドル（世界のGDPの0.8%相当 ⇒日本では**約3兆円**）

IoTによるフィジカルとサイバーの融合により、サイバー攻撃がフィジカル空間まで到達し、**経済損失がさらに拡大**するリスク

サプライチェーンリスク：セキュリティ確保が調達要件になる動き

米国：サイバーセキュリティフレームワークv1.1に、『サイバーサプライチェーンリスクマネジメント』を明記。

防衛調達の全参加企業にセキュリティ対策（SP800-171の遵守）を義務化

欧州：ネットワークに繋がる機器の認証フレームの導入検討。

EUの顧客データに新たな義務（GDPR）2018年から

IoT機器が大規模DDoS攻撃の踏み台（MIRAI 2016）

コネクテッドカーシステムの脆弱性(JEEPハッキング事例 2015, 2016)

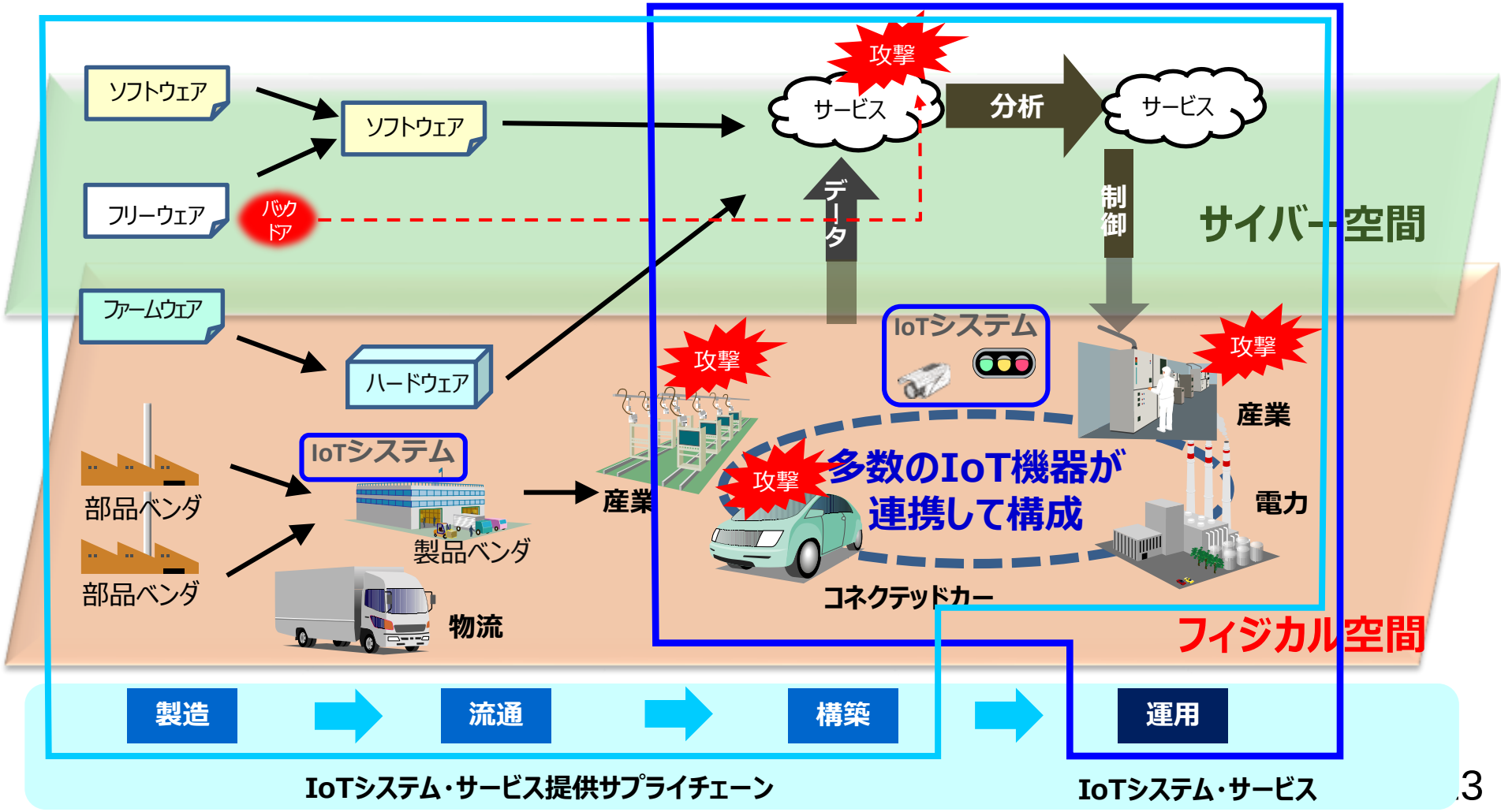
携帯電話用フラッシュメモリのファームウェアに仕込まれた不正プログラムが見つかる（2016）

サイバーフィジカル高度融合システムの課題

複雑につながるサプライチェーン
⇒ 影響範囲が拡大

フィジカルとサイバーの融合 ⇒
- **サイバー攻撃がフィジカル空間まで到達**
- **フィジカルから侵入しサイバー空間への攻撃も**
- **フィジカルとサイバーの間の情報伝達への攻撃**

大量のデータの流通・連携
⇒ データ管理の重要性が増大



IoTサプライチェーンセキュリティへの取組み

部品・システム・組織のそれぞれのレベルで「信頼の基点」作り

IoTサプライチェーンの「信頼チェーン」の構築・維持

開発・調達・運用時のセキュリティ確認（信頼の確認）の仕組みとグローバルな連携

内閣府SIP第2期
“IoT社会に対応したサイバー・フィジカル・セキュリティ”

総合科学技術・イノベーション会議 CSTI

1. 政府全体の科学技術関係予算の戦略的策定

2. 戦略的イノベーション創造プログラム （SIP）

総合科学技術・イノベーション会議が府省・分野の枠を超えて自ら予算配分して、基礎研究から出口（実用化・事業化）までを見据えた取組を推進。

3. 官民研究開発投資拡大プログラム（PRISM）

4. 革新的研究開発推進プログラム （ImPACT）

戦略的イノベーション創造プログラム（SIP）第２期（2018～2022年度）

- ビッグデータ・AI を活用したサイバー空間基盤技術
- フィジカル空間デジタルデータ処理基盤技術
- IoT 社会に対応したサイバー・フィジカル・セキュリティ
- 自動運転（システムとサービスの拡張）
- 統合型材料開発システムによるマテリアル革命
- 光・量子を活用したSociety5.0実現化技術
- スマートバイオ産業・農業基盤技術
- 脱炭素社会実現のためのエネルギーシステム
- 国家レジリエンス（防災・減災）の強化
- AI（人工知能）ホスピタルによる高度診療・治療システム
- スマート物流サービス
- 革新的深海資源調査技術

SIPサイバー・フィジカル・セキュリティ　研究開発のねらい

Society5.0の実現によりもたらされる価値創出

約90兆円(2025年) を支える

産構審 新産業構造部会「新産業構造ビジョン」(H29.5)
http://www.meti.go.jp/committee/sankoushin/shin_sangyoukouzou/pdf/017_05_00.pdf

複数の産業分野に跨るIoTシステム・サービス

とサプライチェーンのセキュリティ確保

（『サイバーフィジカルセキュリティ対策基盤』を確立）

製品・サービスのセキュリティ品質向上とコストの削減と、国際競争力強化に貢献（**輸出主体の製造業の国際調達に参入機会の確保**）

海外展開には国内で産業分野間で連携した取組みが重要

SIPサイバー・フィジカル・セキュリティ「信頼のチェーン」

実証実験　対象分野：製造・流通・ビル等

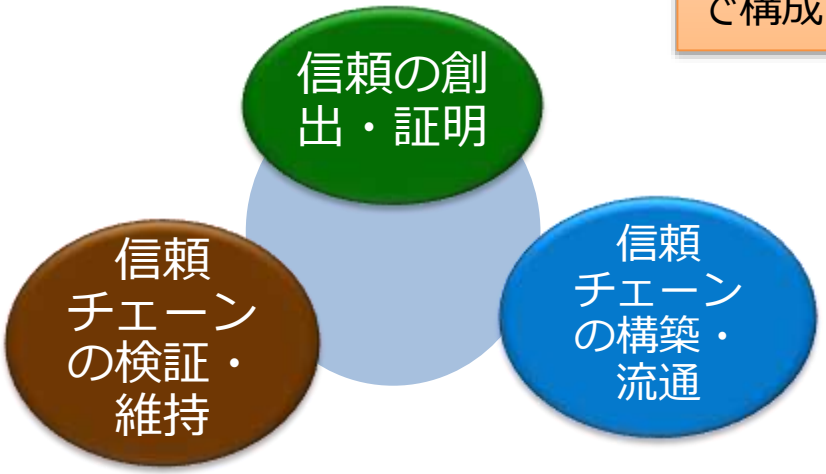
IoTシステム・サービスのセキュリティ確保

サプライチェーンのセキュリティ確保

信頼の基点をIoTシステムの構成要素に実装。それを起点とする信頼チェーンを多数のIoT機器、ネットワーク、クラウド等で構成

信頼のチェーン

サプライチェーンを構成するプロシージャの信頼の証明を実現し、それを起点とする信頼チェーンをサプライチェーンの構成要素（人、組織、製品、システム、サービス、データ等）で構成



SIPサイバー・フィジカル・セキュリティ：技術開発の取組み

A.信頼の創出・証明

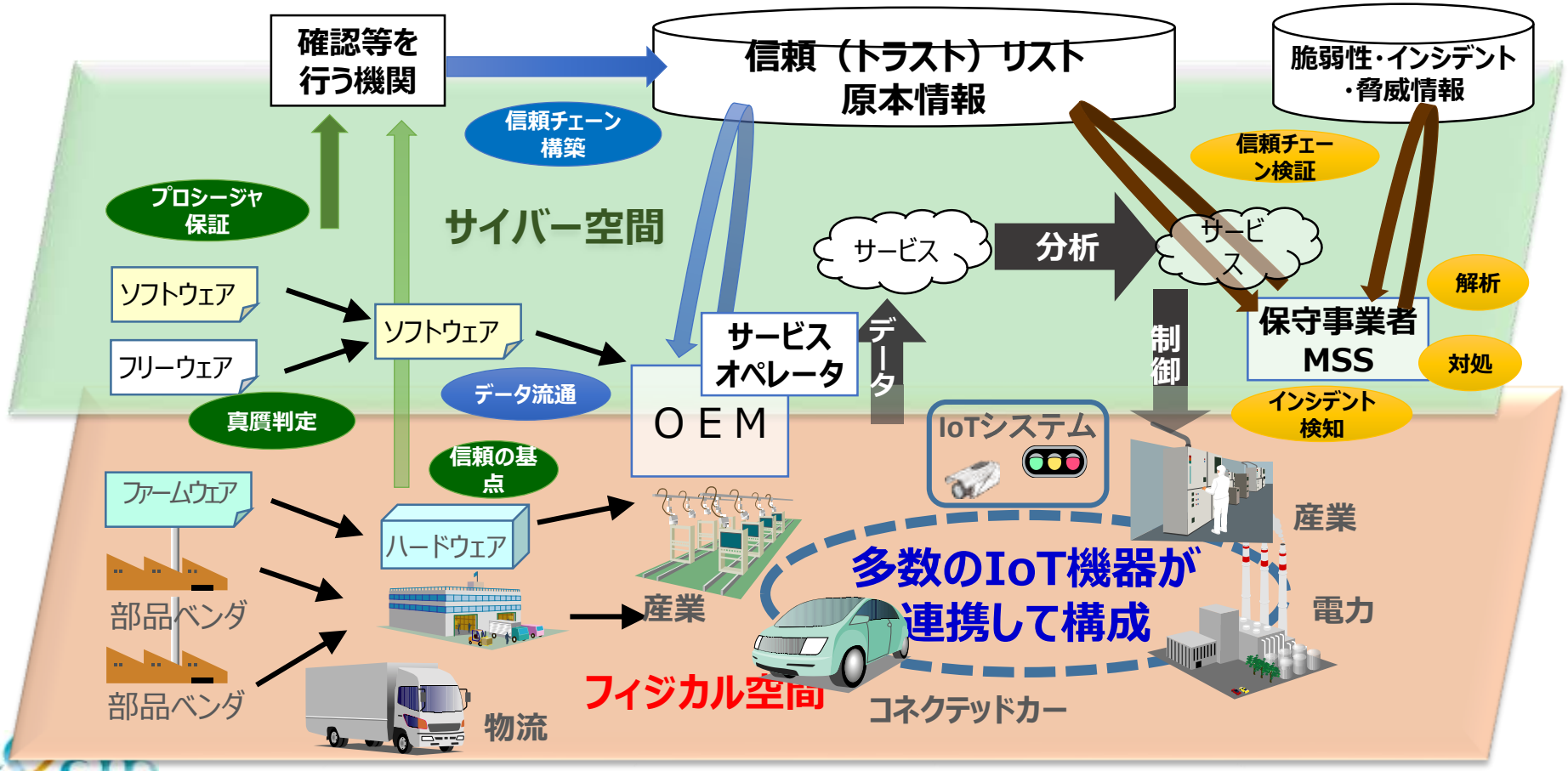
多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

B.信頼チェーンの構築・流通

信頼チェーンを構築し、必要な情報をセキュアに流通させる技術

C.信頼チェーンの検証・維持

信頼チェーンが安全に運用されていることを検証し、維持することを可能にする技術



信頼の創出･証明から構築･流通、検証･維持

信頼の創出・証明

- 暗号エンジンを活用した信頼の基点と保護
- 多種・大量の小型IoT機器の真贋判定（証明）
- プロシージャの適格性保証（証明）

信頼チェーンの構築・流通

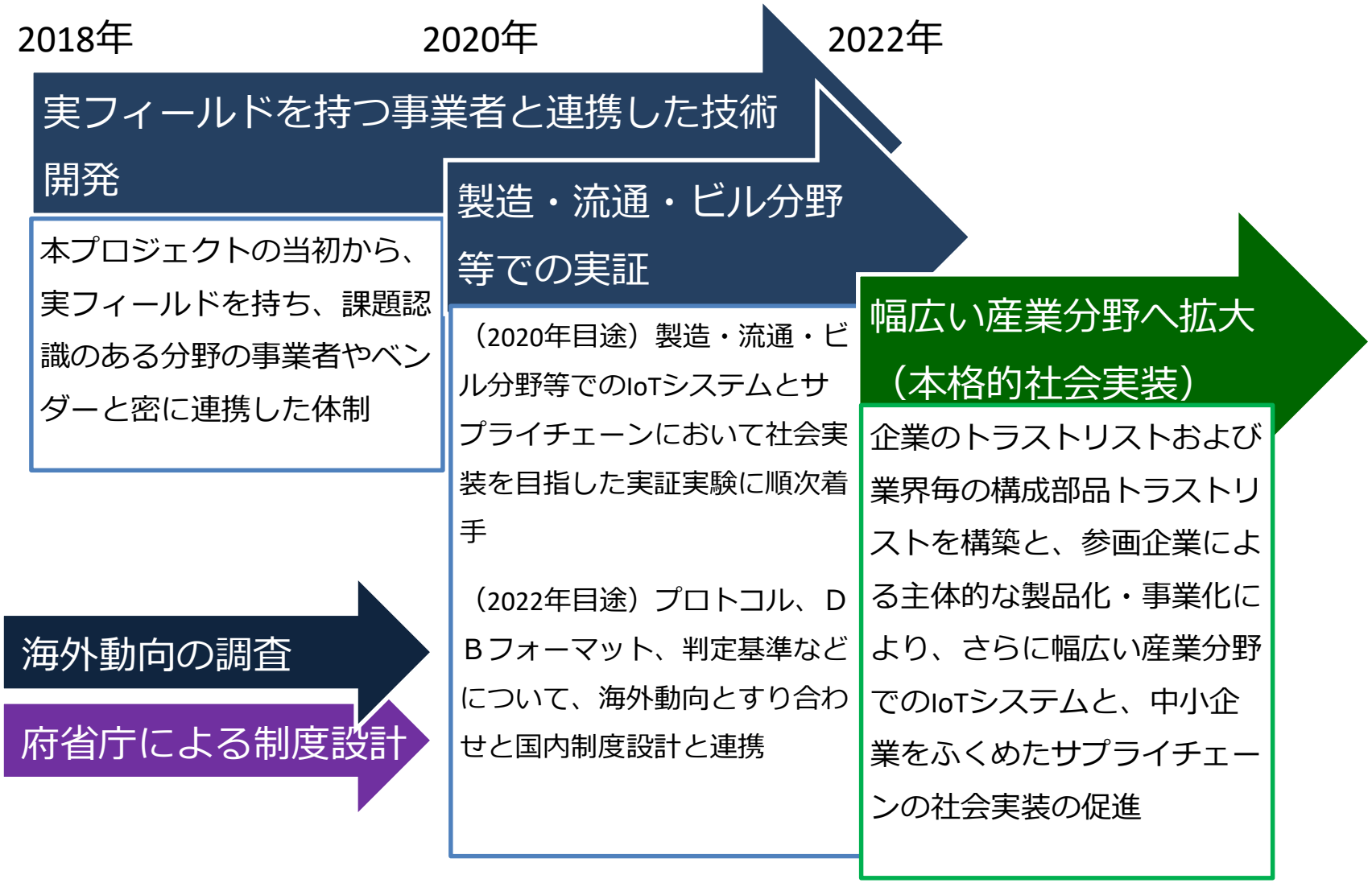
- 信頼の証明の繰り返しにより信頼チェーンを構築するプロトコル
- 信頼チェーンで流通する情報のデータセキュリティ確保

信頼チェーンの検証・維持

- 検証：信頼チェーンのトレーサビリティ
- 維持：信頼チェーンの運用時の保護と異常検知・対処

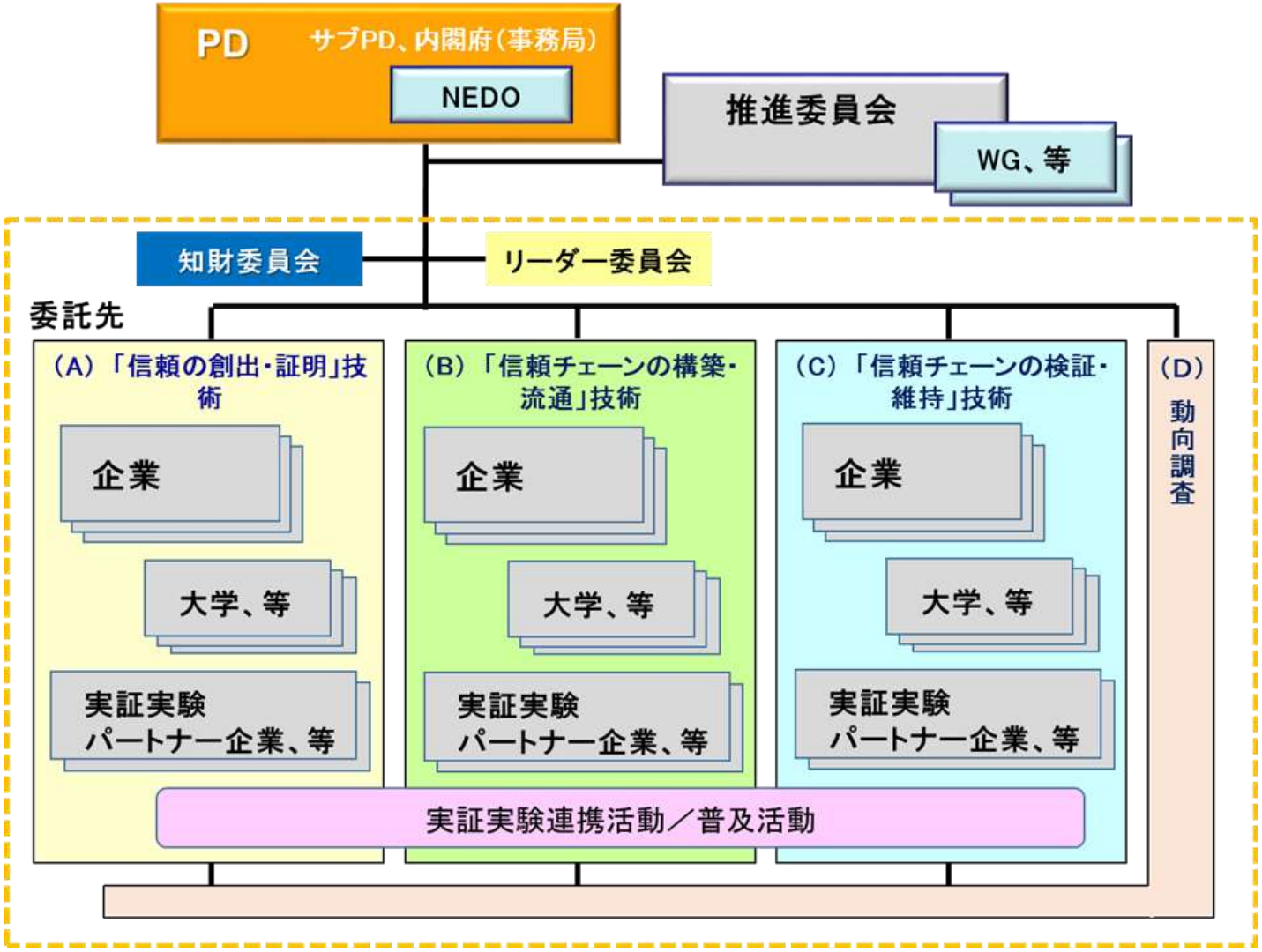
SIP

SIPサイバー・フィジカル・セキュリティ：社会実装に向けて



SIPサイバー・フィジカル・セキュリティ：実施体制

- 研究開発の成果を主体的に**実用化・事業化できる企業を中心**に、先進技術を有する大学やベンチャーを含む産学連携のプロジェクト実施体制を構築。



SIPサイバー・フィジカル・セキュリティの取組み

実証実験から社会実装へ

- 効果測定：実証実験において実用性や実効性の効果測定調査
- 海外発信：国際シンポジウムの開催
- SIPの課題間、他国プロ等との連携

技術成果の継続性・発展性の確保

- 参画企業による事業化（製品化）と各産業分野へ導入推進
- 共用検証センター（自主評価用）等の立上げ

普及のための方策

- 技術動向および政策動向調査
- 関連府省庁の規制・制度改革等における施策連携
- 国際連携：米国NIST, 欧州ENISA等へ積極的な提言

IoTセキュリティをめぐるグローバル動向

米国

- NIST&DHS　Strategic Principles for Securing the Internet　of Things
- NIST Cybersecurity Framework, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)
- Industrial Internet (IIoT）

欧州

- EU GDPR
- ENISA　Baseline Security Recommendation for IoT
- UK NCSC DCMS/Code of Practices
- ECSO/ECSC

日本

- NISC 安全なIoTシステムのためのセキュリティに関する一般的枠組
- IoT推進近ソーシアム　IoTセキュリティガイドライン
- IPA IoT開発におけるセキュリティ設計の手引き, つながる世界の開発指針 他

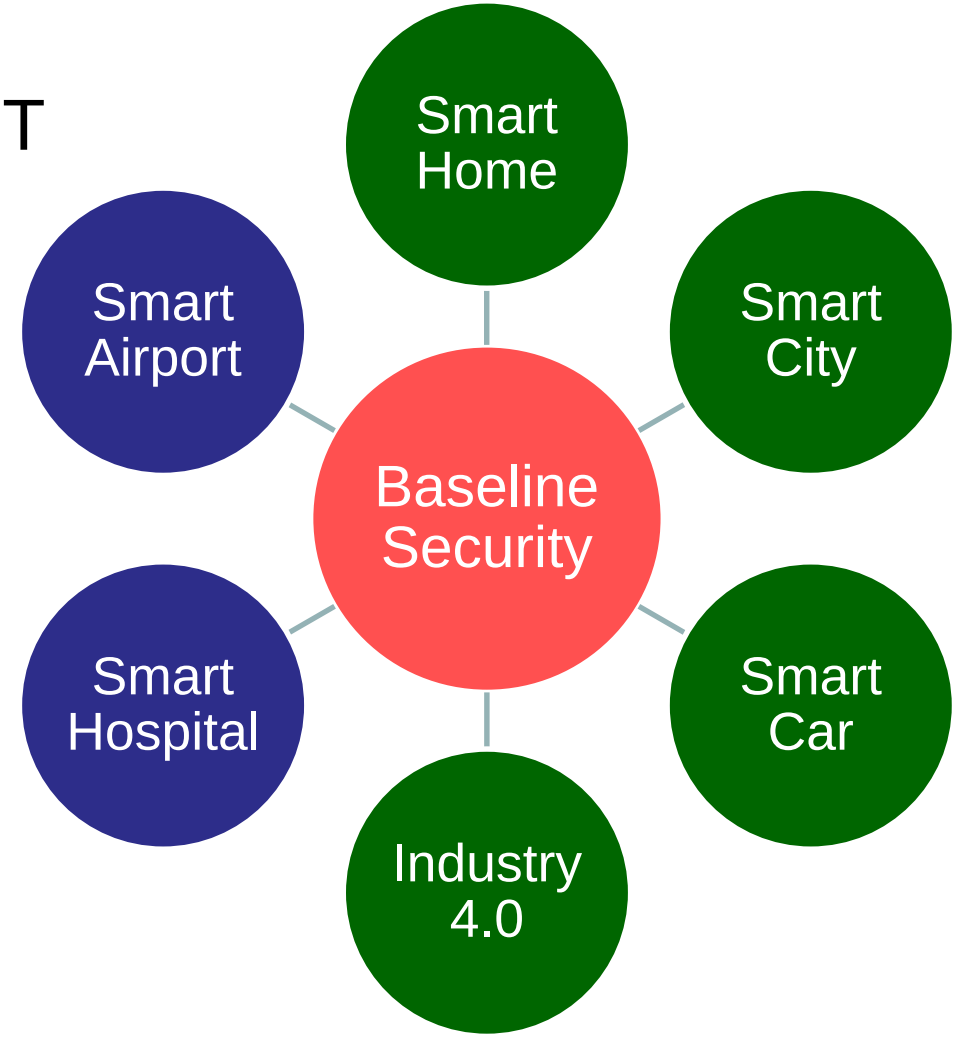
米国 NIST

- Draft NISTIR 8228: Considerations for IoT Cybersecurity and Privacy Risks
- NIST Cybersecurity White Paper: Internet of Things (IoT) Trust Concerns

Cybersecurity Framework

ENISA IoT Security

■ Baseline Security Recommendations for IoT



英国 DCMS IoT Code of Practices

- 消費者向け IoT 製品のセキュリティに関する行動規範（2018年10月）
  - DCMS “Secure by Design: Improving the cyber security of consumer Internet of Things: Report”（2018年3月）
- 対象：インターネットやホームネットワーク（両方またはその一方）と関連サービスに接続する消費者向け IoT 製品
- 対象読者
  - デバイスメーカー　、IoT サービス提供事業者
  - モバイルアプリケーション開発事業者、小売業者
- 実証と普及活動
  - 協力企業：　HP，Centrica Hive
- グローバルマッピング
  - 世界中のガイドライン（100以上）のIoTセキュリティとプライバシー推奨事項との対応付け

英国 DCMS IoT Code of Practice

1. **初期パスワードを設定しない　No default passwords**
2. **脆弱性に関する情報の公開方針を導入する**
   Implement a vulnerability disclosure policy
3. **ソフトウェアを定期的に更新する Keep software updated**
4. 認証情報とセキュリティ上重要なデータを安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時のシステムの復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスを容易に設置してメンテナンスできるように配慮する
13. 入力データを検証する

IoTセキュリティ人材の育成

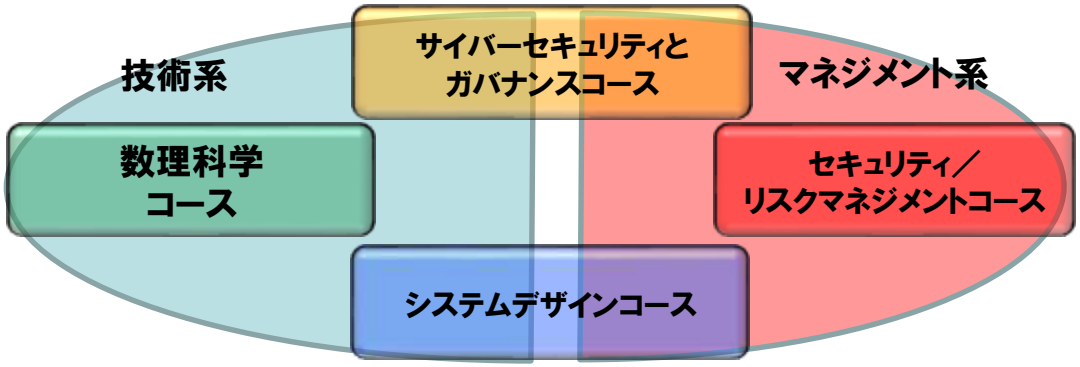
情報セキュリティ大学院大学

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

■本学は2004年に開学し、新しい学問の体系化と専門家の育成を旗印に、情報セキュリティ専門の独立大学院として教育と研究に携わってきました。

■2018年9月末までに、修士(情報学)366名、博士(情報学)33名の修了生が日本の情報セキュリティに関する中核的業務を担っています。

総合科学:情報セキュリティカリキュラム



本学の特色

約8割が社会人学生(2017-2018実績:ウィングアーク1st(株)/NECフィールディング(株)/NTTコミュニケーションズ(株)/NTTテクノクロス(株)/エヌ・テエ・ティ・コムウェア(株)/沖電気工業(株)/海上自衛隊/海上保安庁/外務省/(株)アイネス/(株)エヌ・ティ・ティ・エムイー/(株)サーバーワークス/(株)静岡銀行/(株)JR東日本情報システム/(株)タツノ/(株)東陽テクニカ/(株)日立システムズ/(株)日立製作所/(株)Beyondsoft Japan/(株)本田技術研究所/(株)読売新聞社/金融庁/警察庁/警視庁/(公社)日本医師会/埼玉県警察/CsSoft(株)/ジェイアール東海情報システム(株)/昭和シェルビジネス&ITソリューションズ(株)/(独)国立印刷局/(独)日本学術振興会/東日本旅客鉄道(株)/法務省/防衛省/モルガンスタンレーグループ/横浜市役所　など　)

情報セキュリティ大学院大学

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）・・・366名**（2006年3月～2018年9月）

博士（情報学）・・・33名（2007年8月～2018年9月）

情報セキュリティ大学院大学　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Ⅰ
- 情報セキュリティ輪講Ⅱ
- Presentations for Professionals

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

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
- **実践的IoTセキュリティ**

サイバーセキュリティとガバナンス

- サイバーセキュリティ技術論
- セキュアシステム構成論
- 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
- 特設講義（サイバー・インテリジェンス）
- 特設講義（ハッキングとマルウェア解析）

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
- AIと機械学習

ハンズオン

- 情報セキュリティ技術演習
- セキュリティ実践Ⅰ ＆セキュリティ実践Ⅱ（SecCap演習）
  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

IoTセキュリティ講座の開発

- IPA「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」として、IoTの安全安心な技術開発と運用を行う人材育成のための情報セキュリティ教材の開発
  - IPA「つながる世界の開発指針」
  - 大学院の講義として開講しながら、教材やハンズオン演習を開発　（2017年度～）
  - 今後、社会人向け講座など、広く横展開（2019年度～）

IoT機器の実機を用いたハンズオン演習と
IoT関連技術に加え、法制度までカバーする
IoTセキュリティ講座は世界でも類を見ない先進事例

プロジェクト体制

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

IPA

情報セキュリティ大学院大学

全体統括	教授　松井俊浩
教材作成・授業実施	専任教員　他
教材作成・演習補助	特任助手　他

◆ カリキュラムの作成
◆ 教材の開発と改良

カリキュラム会議

座学教材

技術演習教材

技術演習環境

授業の実施

受講生

開発支援

外部講師

アドバイス

アドバイス

教育効果測定

IoT教育開発連携機関（拡大中）

- 教材に盛り込むべき事項をアドバイス
- 講義を担当

自動車関連企業

半導体メーカー

重要インフラ事業者

電機メーカー

重要生活機器連携セキュリティ協議会　CCDS

組込みシステム技術協会 JASA

組込みシステム産業振興機構 ESIP

連携大学　　教授・准教授

IoT教育アドバイザリ委員会

- 教材と授業を評価し、改良をアドバイス

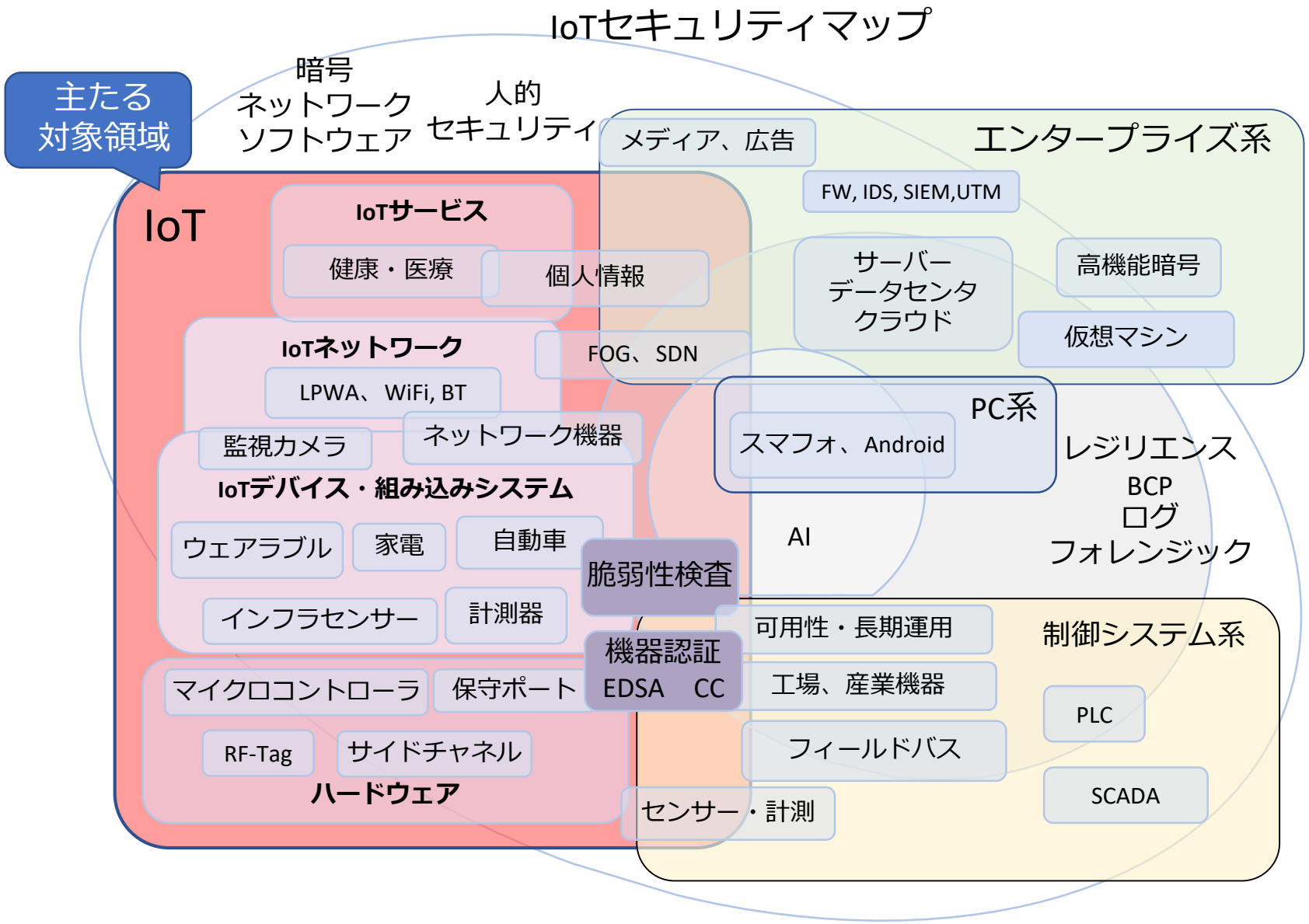
名古屋大学 教授	高田広章（委員長）
長崎県立大学 教授	小松文子
産総研　情報技術研究部門 副部門長	宝木和夫
セコム 常務顧問	小松崎常夫
JASPAR	橋本雅人

IPA「つながる世界の開発指針」

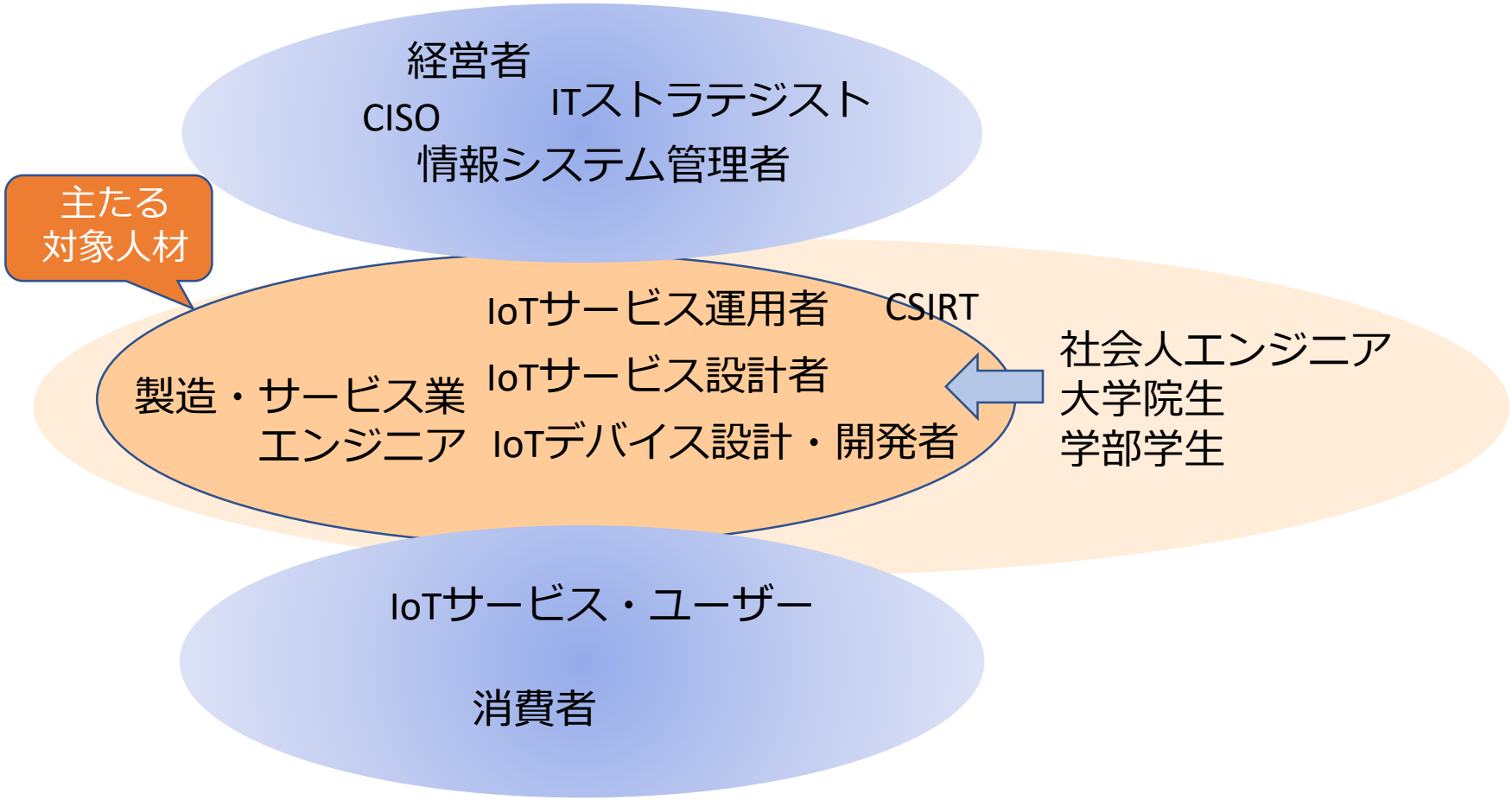
大項目		指針	
方針	つながる世界の安全安心に企業として取り組む	1	安全安心の基本方針を策定する
		2	安全安心のための体制人材を見直す
		3	内部不正やミスに備える
分析	つながる世界のリスクを認識する	4	守るべきものを特定する
		5	つながることによるリスクを想定する
		6	つながりで波及するリスクを想定する
		7	物理的なリスクを認識する
設計	守るべきものを守る設計を考える	8	個々でも全体でも守れる設計をする
		9	つながる相手に迷惑をかけない設計をする
		10	安全安心を実現する設計の整合性をとる
		11	不特定の相手とつなげられても安全安心を確保できる設計をする
		12	安全安心を実現する設計の検証、評価を行う
保守	市場に出た後も守る設計を考える	13	自身がどのような状態かを把握し、記録する機能を設ける
		14	時間がたっても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	15	出荷後もIoTリスクを把握し、情報発信する
		16	出荷後の関係事業者に守ってもらいたいことを伝える
		17	つながることによるリスクを一般利用者に知ってもらう

対象とする技術分野・セキュリティ課題

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



想定する受講者


経営者
CISO
ITストラテジスト
情報システム管理者
主たる
対象人材
IoTサービス運用者
CSIRT
IoTサービス設計者
製造・サービス業
エンジニア
IoTデバイス設計・開発者
社会人エンジニア
大学院生
学部学生
IoTサービス・ユーザー
消費者

実践的IoTセキュリティ2018後期講義計画

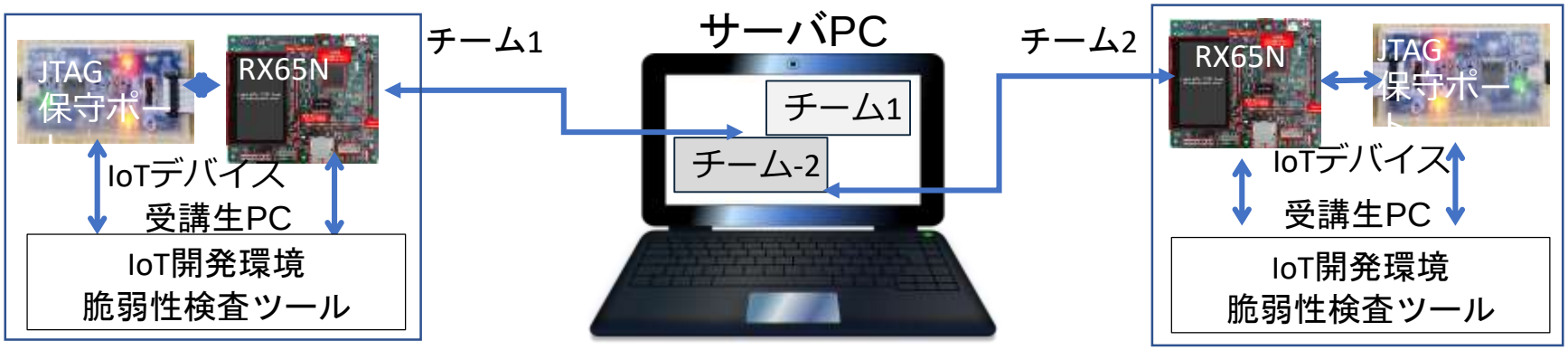
明日の信頼を創ろう。
情報セキュリティ大学院大学
JRITY

回	日付	テーマ	項目	担当教員
1	10月4日(木)	IoTのビジョンとIoTセキュリティ	IoTの特徴、5層アーキテクチャ、インシデント例 エントリポイント、ITとIoT	松井
2	10月11日(木)	IoTデバイスとリアルタイム機能	組込システム、センサ、デバイスインタフェース リアルタイムOS、JTAG	松井
3	10月18日(木)	制御システムセキュリティ	制御系、フィールドバス、PLC、SCADA	松井
4	10月25日(木)	IoTネットワークとエッジコンピューティング	blueborne, WPA2, Bluetooth-LE, LPWA、フォグコンピューティング	松井
5	11月8日(木)	車載エレクトロニクスのセキュリティ	コネクティッドカー、車載ネットワーク(CAN, LIN, FlexRay等)、テレマティックス、ITS、ECU、OBD-II	井上（広島市大）
6	11月15日(木)	ハードウェアセキュリティとセキュアデバイス	サイドチャネル、電力解析攻撃、侵襲攻撃、耐タンパー性、信頼の基点、TSIP	松井、石黒（Renesas）
7	11月22日(木)	IoTデバイスセキュリティ(演習)	組込システム開発、暗号通信、暗号鍵の保存、機器認証、セキュアアップデート	松井
8	11月29日(木)	IoTの機能安全	リスク分析、脅威モデル、CVSS、STRIDE、セキュリティ開発ライフサイクル	大久保
9	12月6日(木)	IoTの脅威分析	アタックツリーとハザード分析,要求分析	大久保
10	12月13日(木)	IoTのセキュリティ・バイ・デザイン	セキュリティ設計、モデル検査、セキュリティテスト、機器認証	大久保
11	12月20日(木)	IoTの脅威分析(演習)	スマートホームの脅威分析、IoTデバイスの脆弱性検査計画	大久保
12	1月10日(木)	IoTの脆弱性検査（演習）	スマートホーム、Wi-Fiルータ、スマートスピーカの脆弱性検査	荻野 (CCDS)
13	1月17日(木)	IoTの脆弱性検査（演習）	スマートホーム、ショッピングボタンの脆弱性検査	荻野 (CCDS)
14	1月24日(木)	IoTを取り巻く法制度、まとめ	IoTの情報資産、PL法、個人情報保護法、通信保護、マルウェア作成罪、ガイドライン	湯淺
15	1月31日(木)	IoTセキュリティの運用・保守と規格・認証	ログ、アップデート、情報共有、認証機関、相互承認、CSMS、CCとEDSA認証	松井

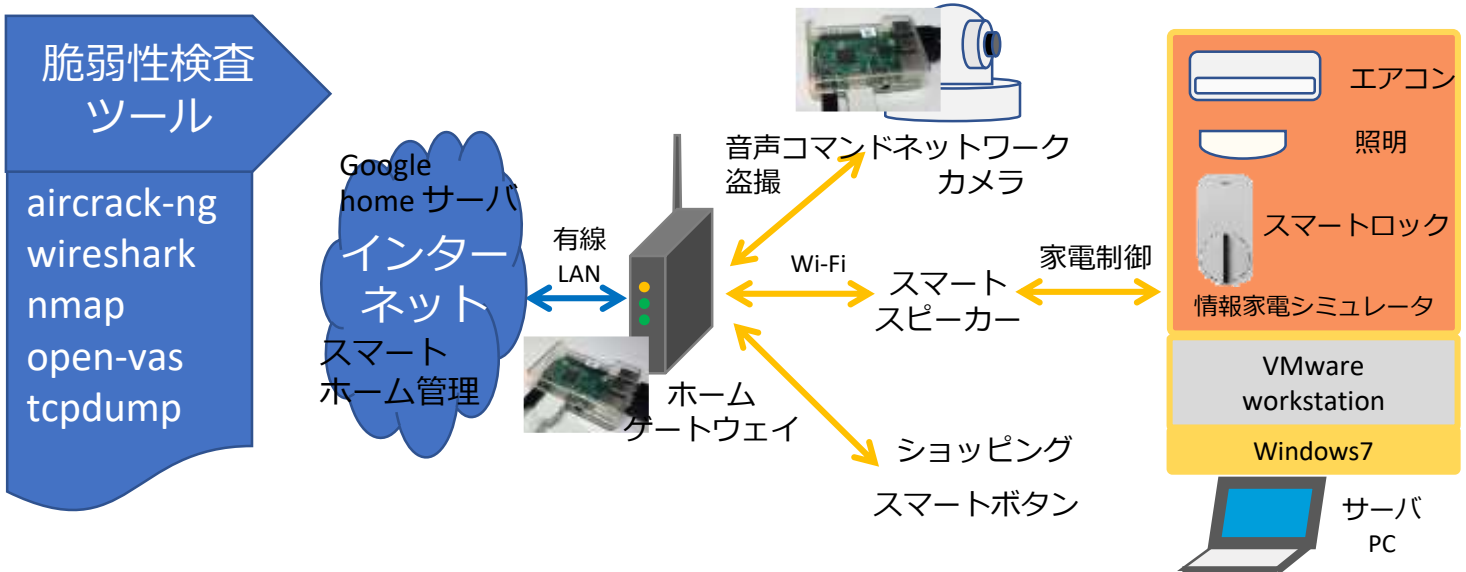
IoTセキュリティの演習授業

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

演習1：ソフトウェア暗号化では、暗号鍵を奪って相手チームになりすますことが可能だが、ハードウェア暗号機能を使うとなりすませないことを体験



演習2：スマートホームのWiFiルータ、Webカメラ、スマートスピーカなどに侵入可能な口がないかツールを使って探索する



2018年度講義の
つながる世界の開発指針との対応

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

大項目		指針		講義
方針	つながる世界の安全安心に企業として取組む	1	安全安心の基本方針を策定する	①IoTのビジョン ⑭法制度 ⑮規格・認証
		2	安全安心のための体制人材を見直す	⑮(運用・保守)
		3	内部不正やミスに備える	⑭法制度 ⑨脅威分析
分析	つながる世界のリスクを認識する	4	守るべきものを特定する	⑧機能安全 ⑩セキュリティバイデザイン
		5	つながることによるリスクを想定する	④IoTネットワーク ③制御システムセキュリティ ⑤車載エレクトロニクス
		6	つながりで波及するリスクを想定する	⑨脅威分析
		7	物理的なリスクを認識する	②IoTデバイス ⑤車載エレクトロニクス ⑥ハードウェアセキュリティ
設計	守るべきものを守る設計を考える	8	個々でも全体でも守れる設計をする	①IoTビジョン、⑩セキュリティバイデザイン
		9	つながる相手に迷惑をかけない設計をする	⑦IoTデバイス演習 ⑮規格・認証
		10	安全安心を実現する設計の整合性をとる	⑧機能安全 ⑨脅威分析 ⑮規格・認証
		11	不特定の相手とつないでも安全を確保できる設計	⑦IoTデバイス演習 ⑮規格・認証
		12	安全安心を実現する設計の検証、評価を行う	⑫⑬脆弱性検査演習 ⑮規格・認証
保守	市場に出た後も守る設計	13	自身がどのような状態かを把握し、記録する機能	⑮運用・保守
		14	時間がたっても安全安心を維持する機能を設ける	③制御システム ⑮運用・保守
運用	関係者と一緒に守る	15	出荷後もIoTリスクを把握し、情報発信する	⑭法制度、⑮運用・保守
		16	出荷後の関係事業者に守るべきことを伝える	⑮運用・保守
		17	つながるリスクを一般利用者に知らせる	①IoTビジョン、⑮運用・保守