サイバーフィジカルセキュリティ研究センターの概要と戦略

2018年12月17日

国立研究開発法人 産業技術総合研究所
情報・人間工学領域

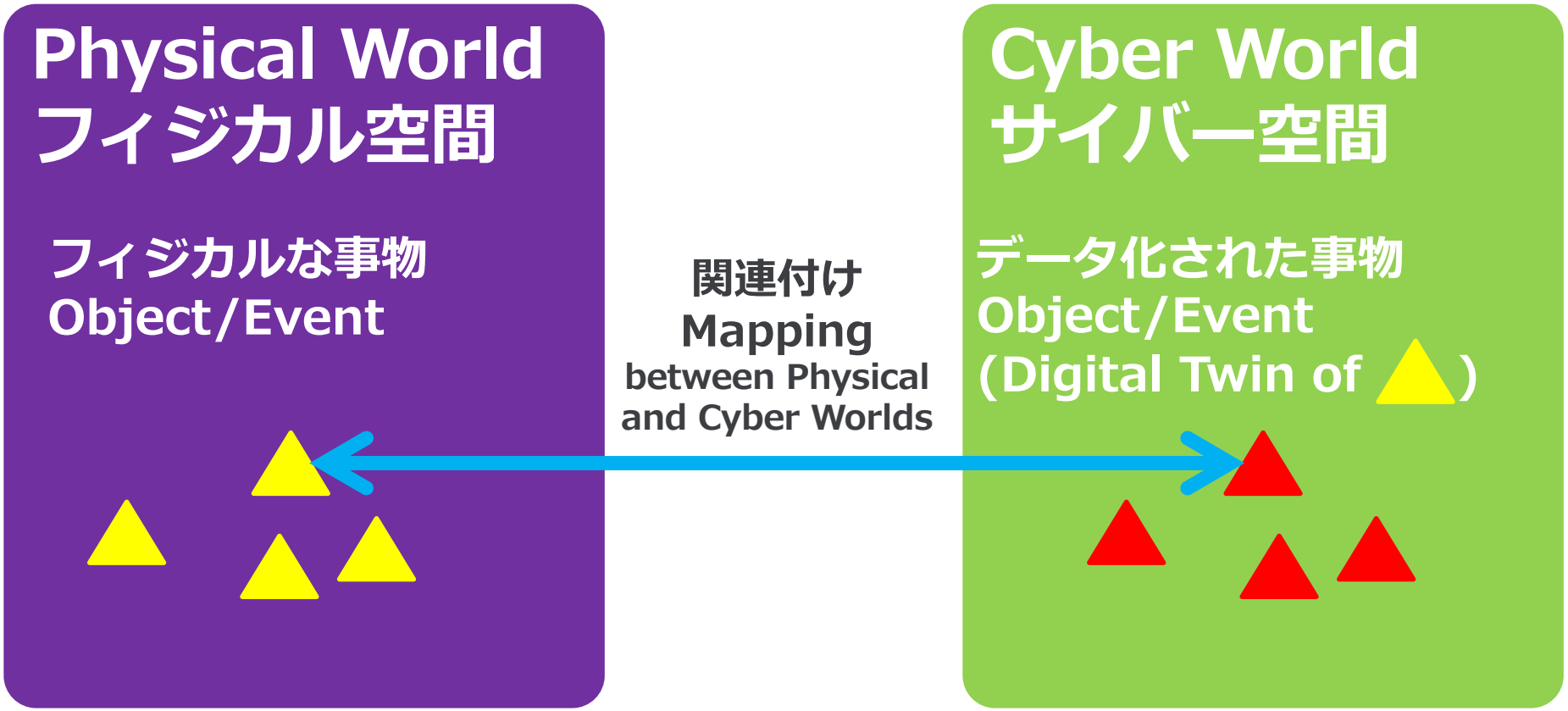
サイバーフィジカルセキュリティ研究センター長

松本　勉

サイバーフィジカルセキュリティとは

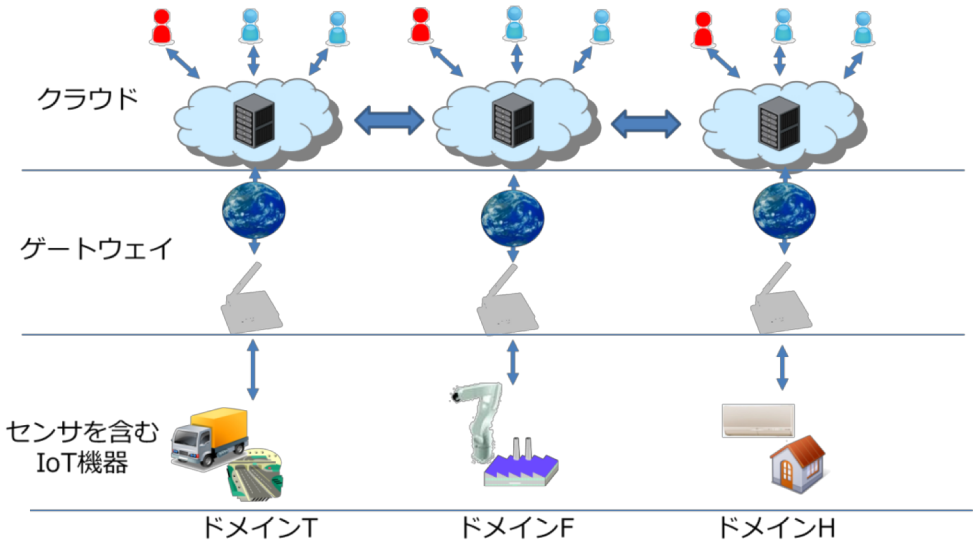
CPS(サイバー・フィジカル・システム) IoT(モノのインターネット)

～フィジカル空間とサイバー空間を関連付け、価値を創造～

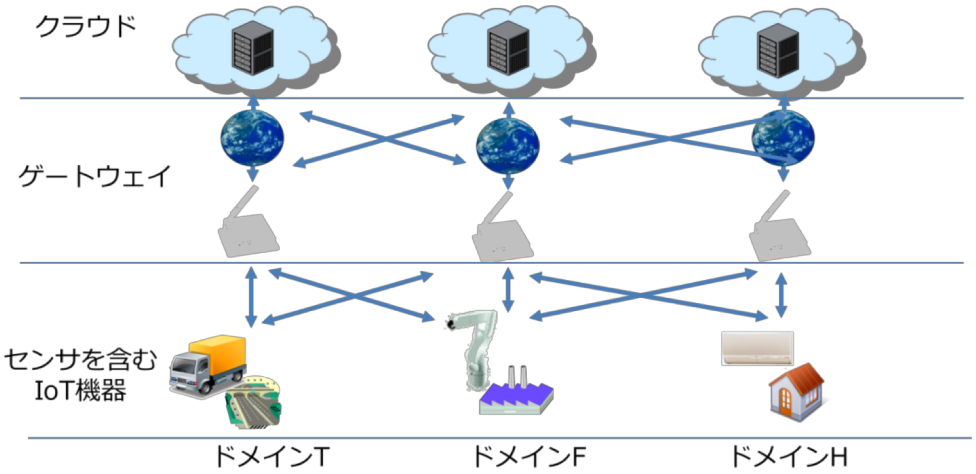


IoT（/CPS）アーキテクチャの展開（仮説）

1（2020年頃まで？）



2（2030年頃には）



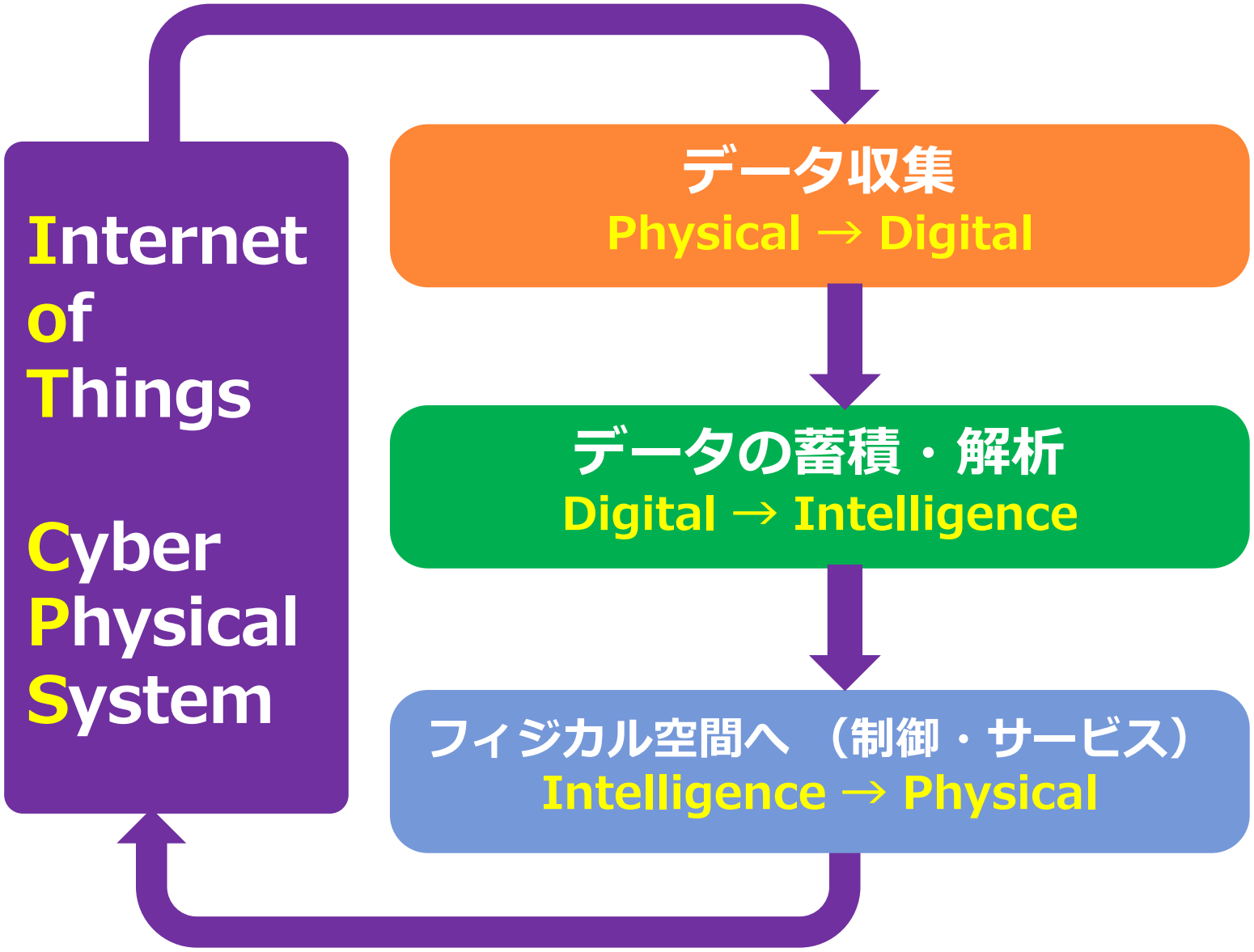
やや閉じたIoT

- 現在はドメイン、あるいは事業主毎に、垂直統合でIoTアーキテクチャが構成されている 。
- ドメイン間、あるいは事業主間で、クラウドを介した部分的な情報交換は行われる。

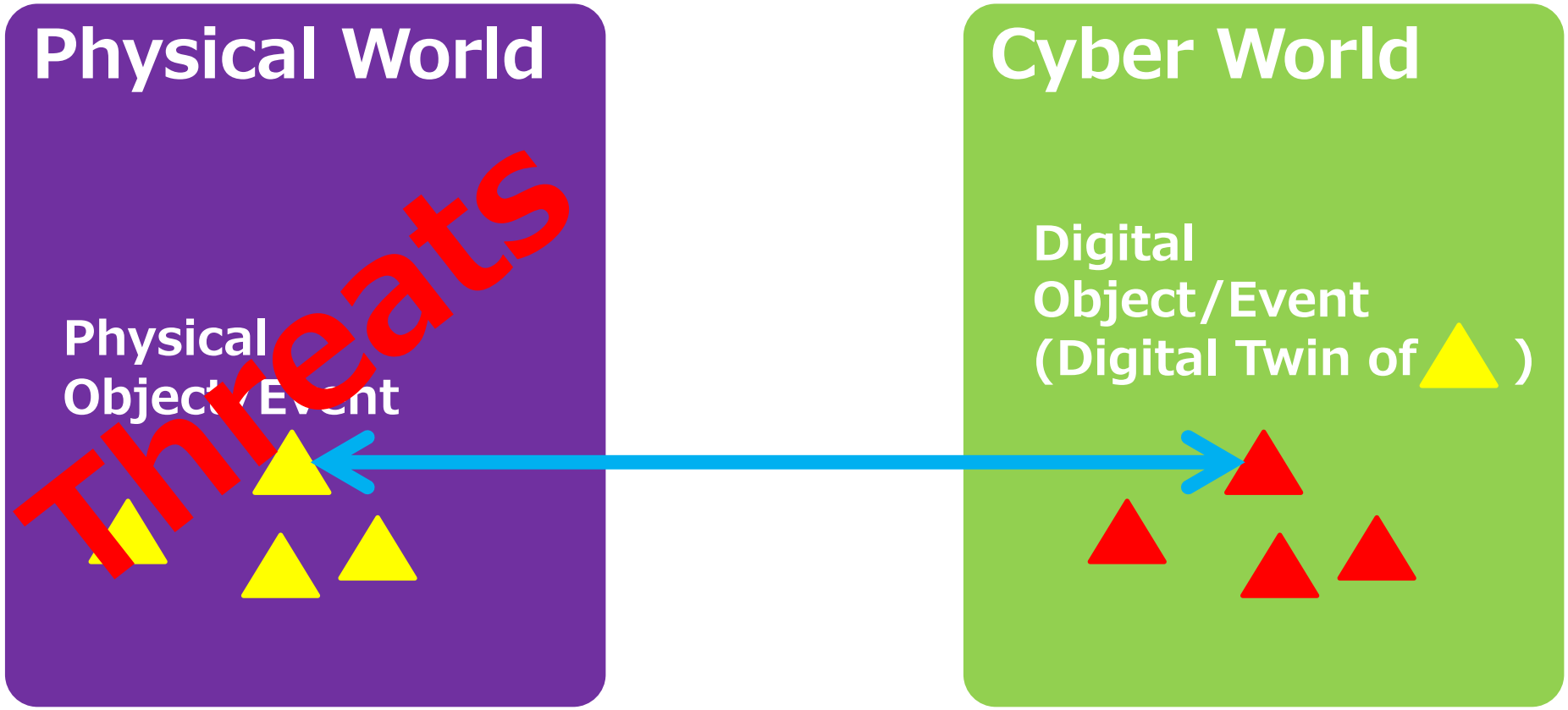
オープンなIoT

- ドメイン、事業主を問わず、IoTの様々なレイヤ間でデータ流通のメッシュ化、サービスの多層化、仮想化が進む。
- 複数のステークホルダーが多様に繋がる究極のIoTに向かって展開する。

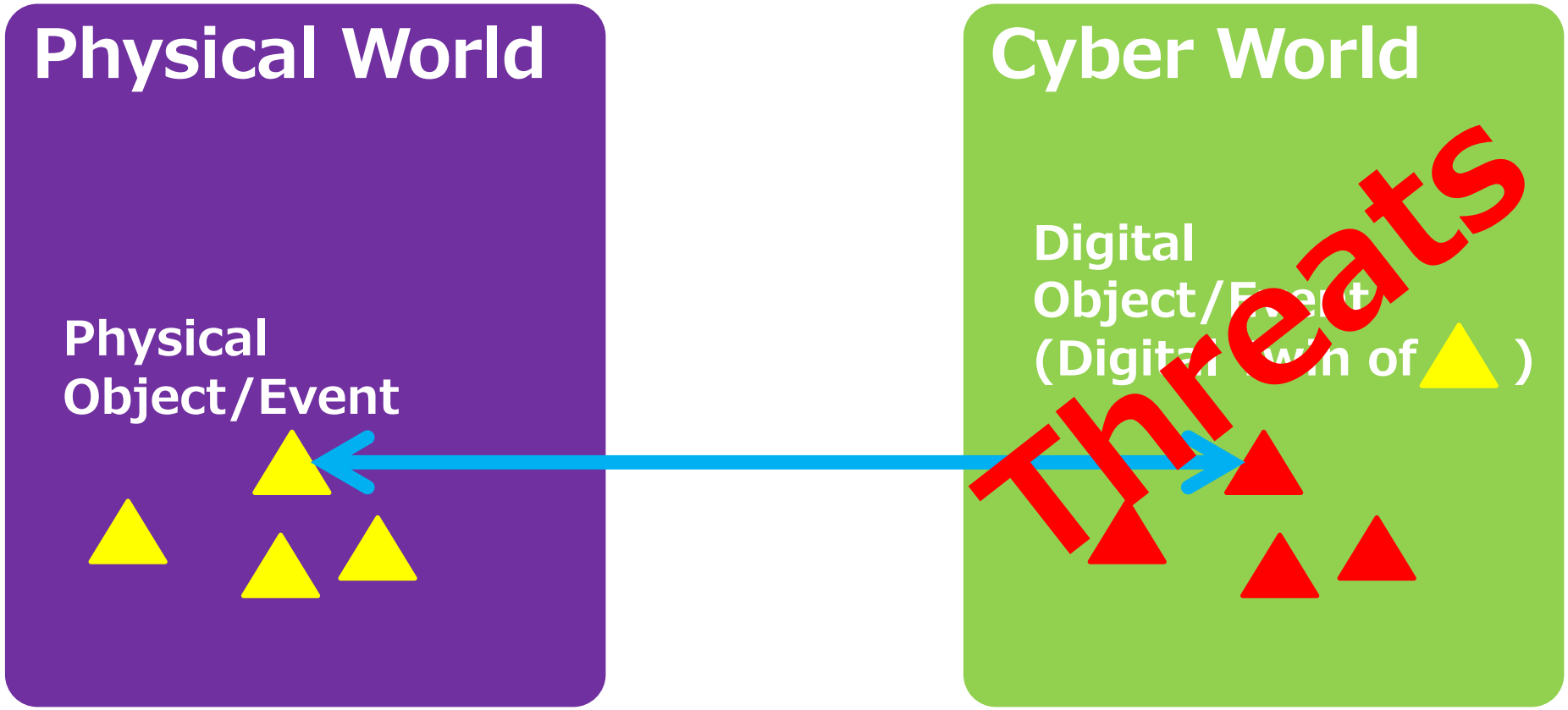
CPS/IoTのプロセス



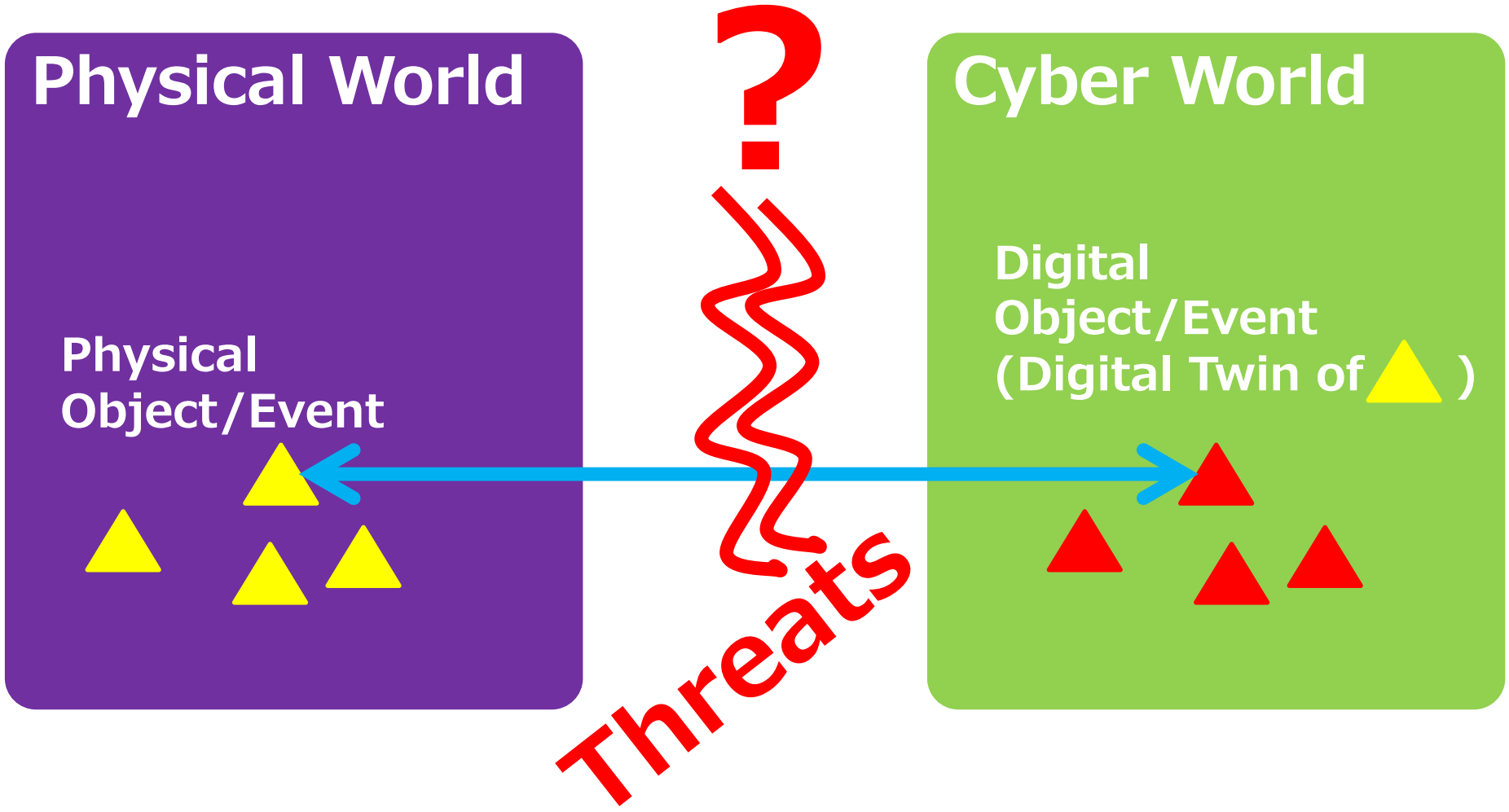
フィジカル空間の脅威はサイバー空間にも及ぶ



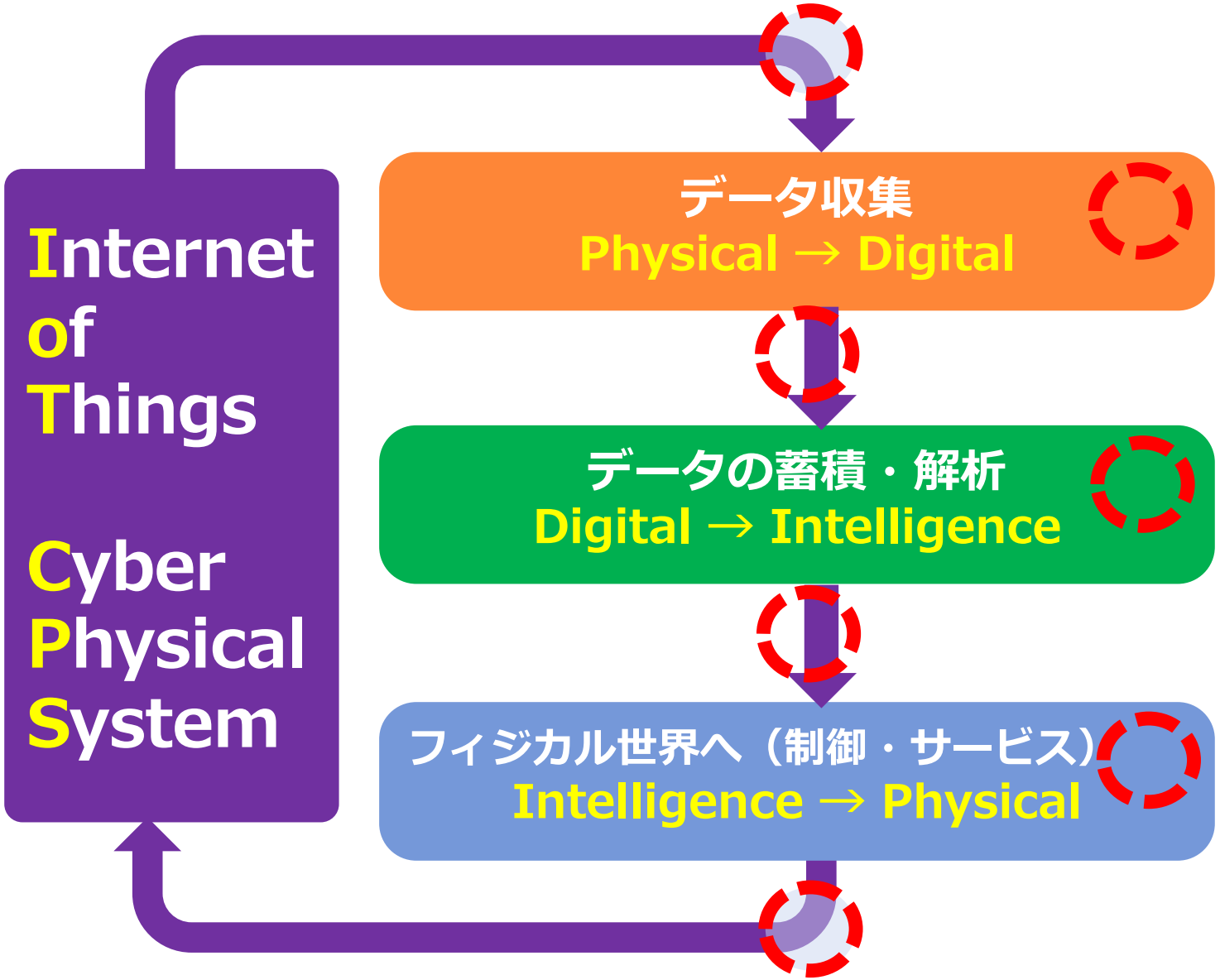
サイバー空間の脅威はフィジカル空間にも及ぶ



フィジカル空間とサイバー空間の対応を揺るがす脅威



サイバーフィジカルセキュリティの研究課題



- ID管理／認証
- 通信のセキュリティ
- 蓄積のセキュリティ
- 処理のセキュリティ
- 計測のセキュリティ
- 制御のセキュリティ
- 管理のセキュリティ
- トラストの置き方

…

における新しい展開

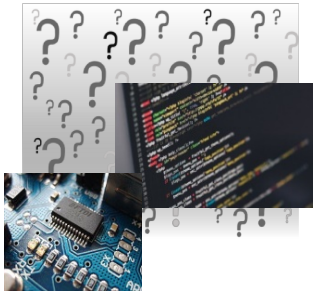
- 計算リソース、
- エネルギー、
- ライフタイム、
- 環境変化
- 未知の脅威

…

にどう立ち向かうか

- 何を標準化するか
  ルール化するか

問題意識と目指すこと



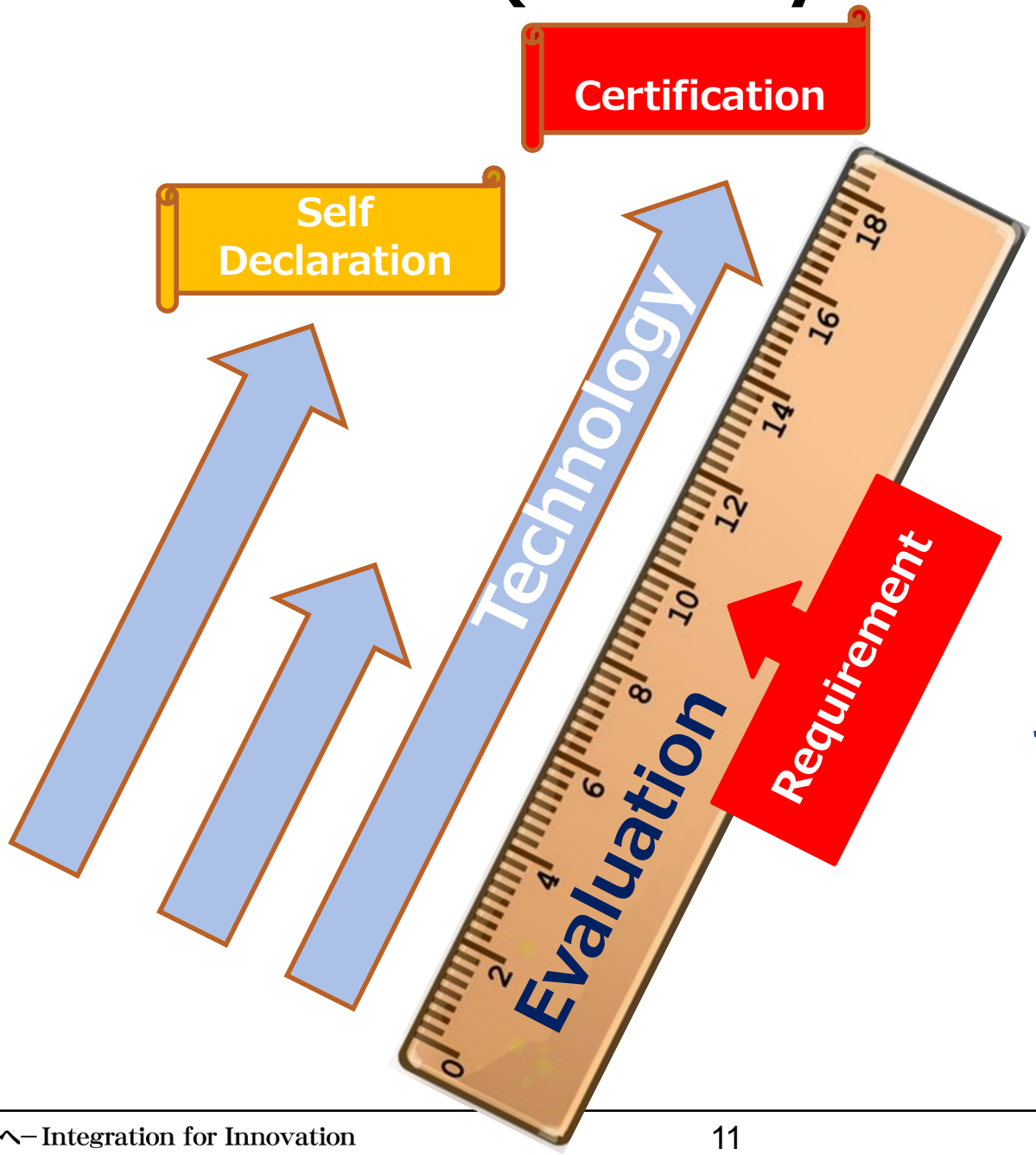
- セキュリティのレベルやセキュアであるか否かの把握や判定は非常に難しい。
  - 攻撃手法は日々変化し、対策の裏をかかれる可能性もある。
  - 被害が出て初めて認識される場合が多い。
- セキュリティレベルを正確に把握できるようにすることは、費用対効果を最適化し、本来提供すべき産業的付加価値を最大化する上で必要不可欠であるが以下のような課題がある。

- セキュリティのレベルの分け方、セキュリティの示し方の妥当性
  - 根拠を示せない場合、議論の場の政治的な力関係で決まる場合もある。
  - → 公正に議論を行うための学術的な根拠データの取得能力の強化。

- 求められるセキュリティレベルを満たしていることを示すための負荷軽減
  - レベルを満たしていることを客観的、かつ、分かり易く示すことは、人的にも費用的にも負荷が大きい。
  - → 負荷軽減手法やツール群強化のための研究開発。
  - → セキュリティについて納得するための使われる制度（セキュリティ保証スキーム）作り。

新しい技術、そのセキュリティ評価方法・セキュリティ保証スキームの開発と社会実装

セキュリティ保証(Security Assurance)



セキュリティ保証は
- ✓ 評価技術
- ✓ 強化技術
- ✓ 保証スキーム(制度)

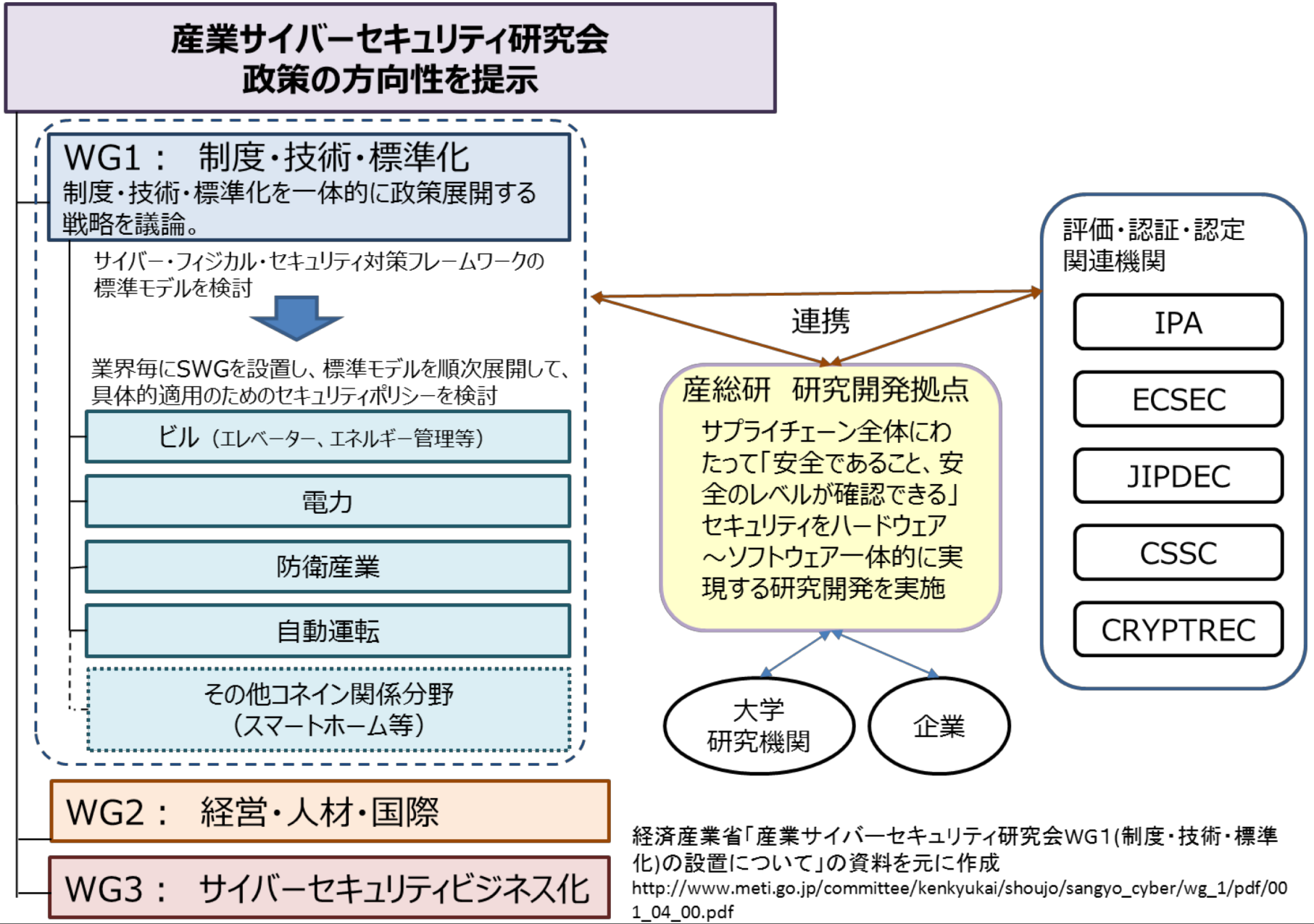
によりなされる

サイバーセキュリティ戦略
Society 5.0

大学・企業・評価機関・行政機関
頑張っているが、、、
研究に根差して総力を結集するための
サイバーフィジカルセキュリティの研究拠点が
必要

産総研・情報技術研究部門が母体

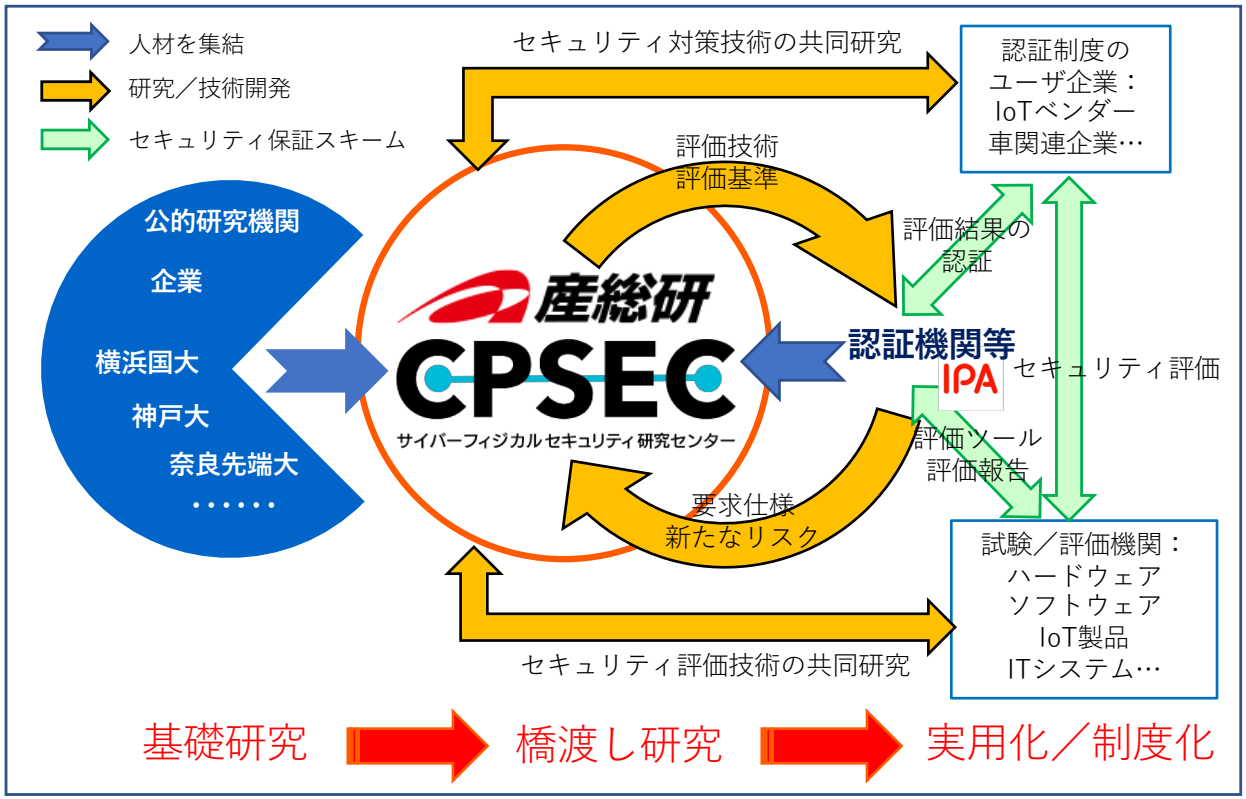
経済産業省産業サイバーセキュリティ研究会



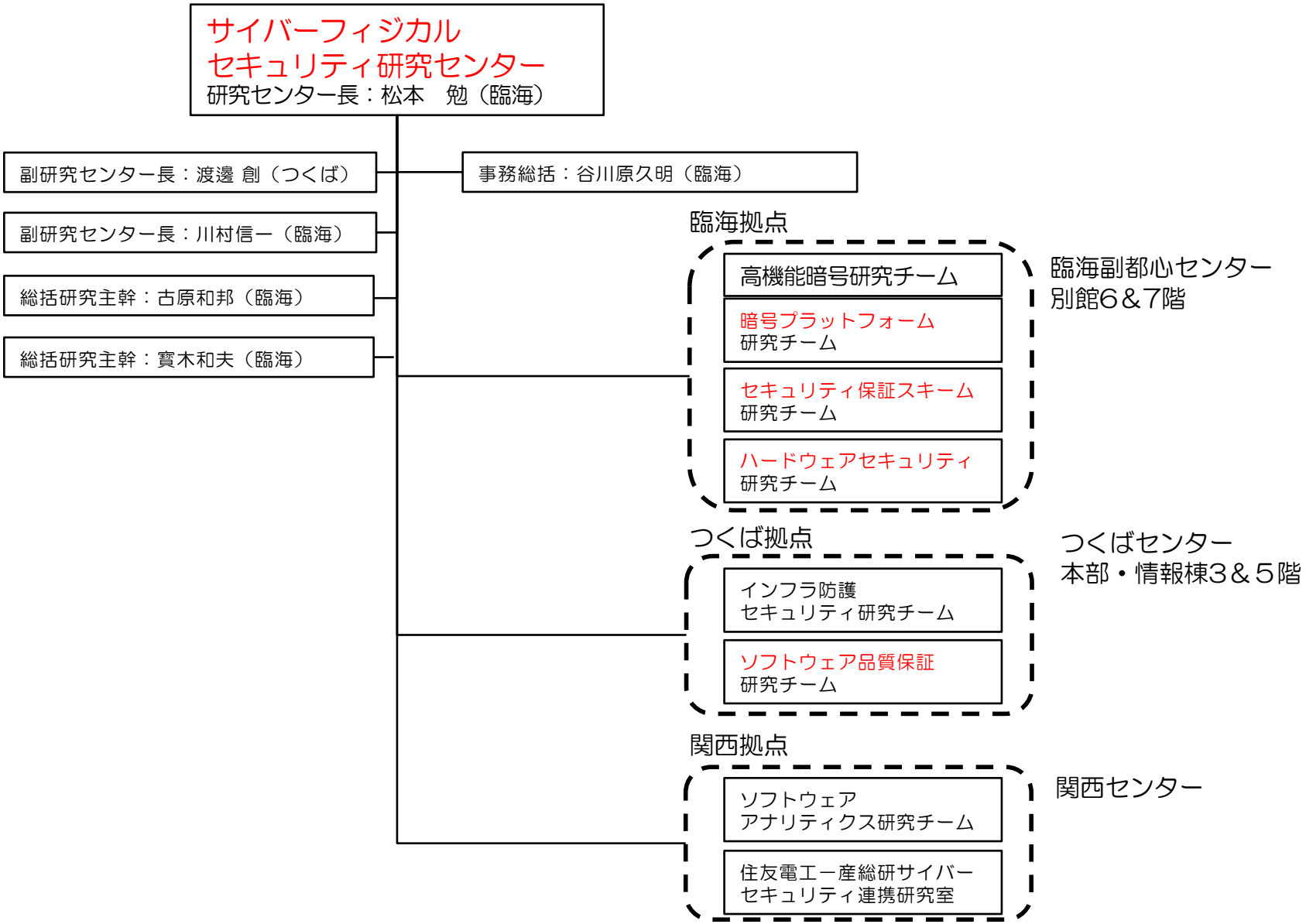
経済産業省「産業サイバーセキュリティ研究会WG1(制度・技術・標準化)の設置について」の資料を元に作成
http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_04_00.pdf

産総研サイバーフィジカルセキュリティ研究センター

- サイバーフィジカルセキュリティの研究拠点として設置（2018年11月～2025年3月）
- 産総研、企業、大学、試験／評価機関等から研究者や技術者をセンターに集結
  12月17日現在総員115名＝職員等(産総研の身分を有する者)88名+外来研究員等(含む学生)27名
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」までを技術面からサポート
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積



体制　研究センター設立当初の拠点および組織構成



○ センター幹部およびセンター付き

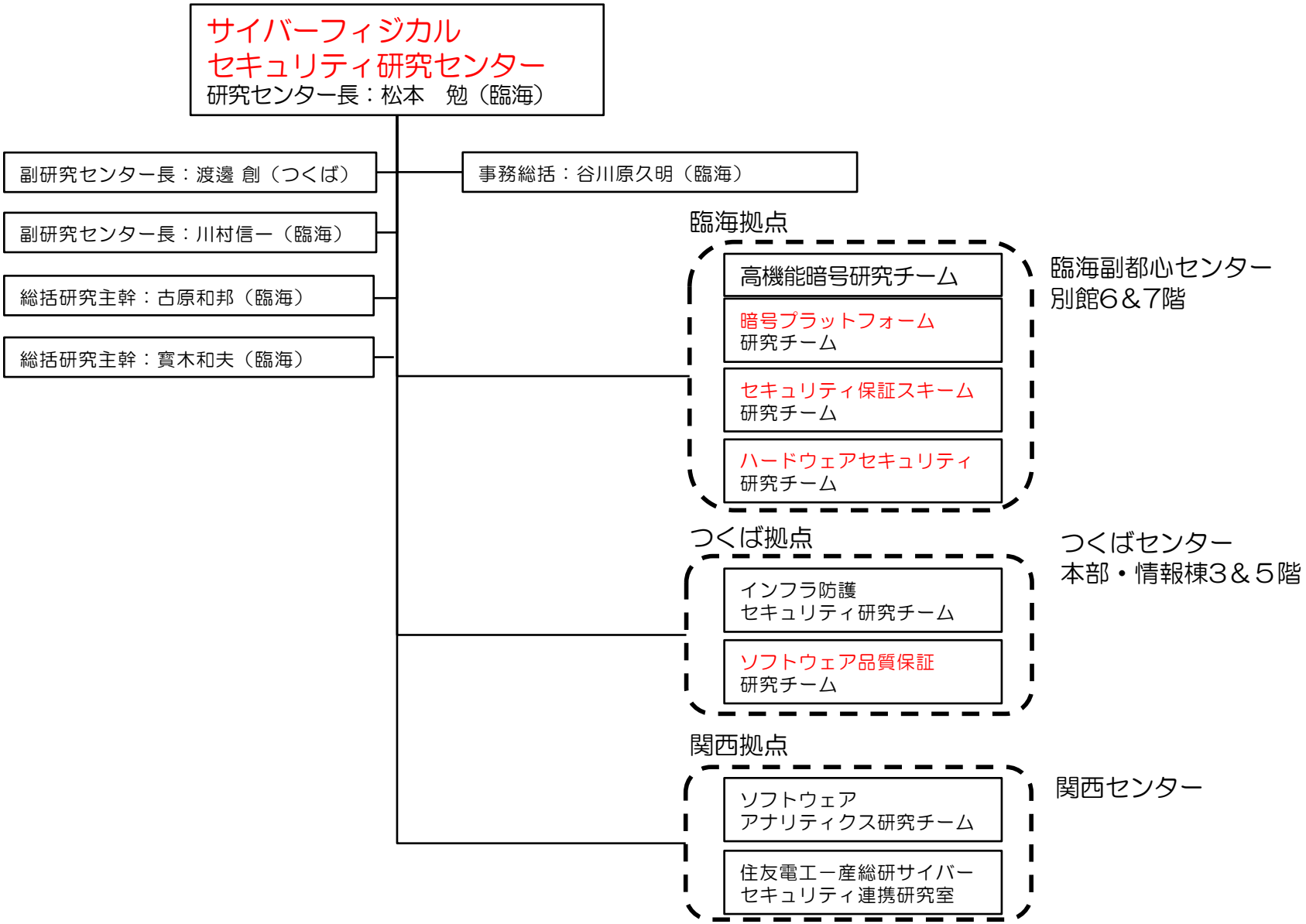
名前	役職
松本　勉	研究センター長
渡邊　創	副研究センター長
川村　信一	副研究センター長
古原　和邦	総括研究主幹
寶木　和夫	総括研究主幹
三科　雄介	特定集中研究専門員(研究)

○ 特定フェロー、顧問

名前	役職
井上　克郎	特定フェロー
今井　秀樹	名誉リサーチャー
中島　一郎	顧問
植村　泰佳	顧問

研究チーム

体制　研究センター設立当初の拠点および組織構成

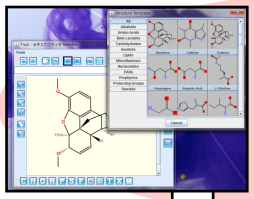


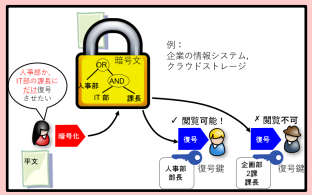
○ 高機能暗号研究チーム

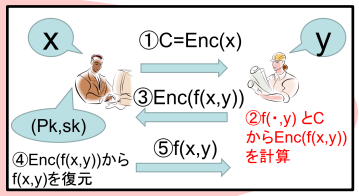
名前	役職
花岡　悟一郎	研究チーム長
松田　隆宏	主任研究員
Schuldt Jacob	主任研究員
山田　翔太	研究員
坂井　祐介	研究員
森田　啓	産総研特別研究員
大畑　幸矢	産総研特別研究員
石田　愛	産総研特別研究員

高機能暗号研究チーム

文部科学大臣表彰 科学技術賞受賞



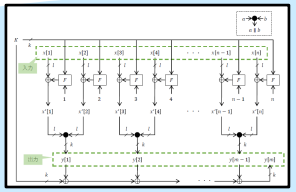




暗号化状態でのデータ処理等が可能な新暗号技術
（＝**高機能暗号**）の開発

ドコモモバイル サイエンス賞受賞

耐量子計算機暗号
（東芝共研）



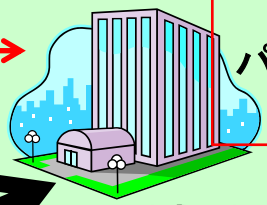
秘密分散の安全性評価
（ZenmuTech共研）

ファジー署名の安全性証明
（日立共研）

IF付ジャーナル等への
多数採録を目指す
目的基礎研究

企業のニーズに応える
橋渡し研究

ニーズに応じた高機能暗号の
理論設計・安全性証明



日立・東芝・三菱電機・
パナソニック・KDDI総研・
ZenmuTech等

外部企業・機関

・最新の安全性概念
・最新の数学的手法
・最新の攻撃手法
：
トップ国際会議・
IF付ジャーナル

最先端の
知見の抽出

国際的成果
を創出

暗号理論における
国際的研究競争

本研究
チーム

ニーズの
抽出
シーズの
提供

標準・最新暗号技術の
安全性に関する知見の入力

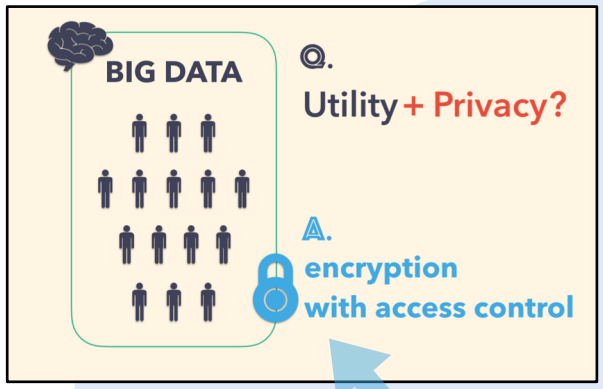
NISC・IPA・
CRYPTREC等

最先端の**暗号理論的知見**を
有することへの「**信頼**」を確立

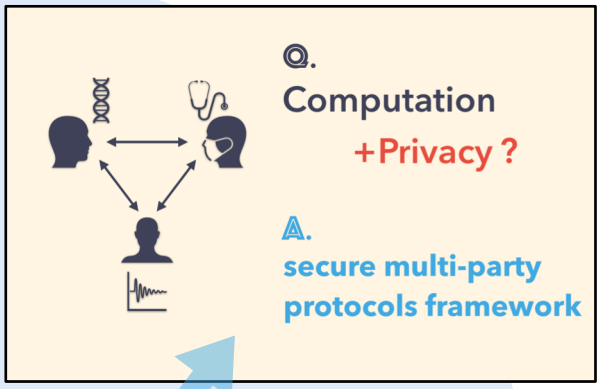
○ 暗号プラットフォーム研究チーム

名前	役職
Attrapadung Nuttapong	研究チーム長
須崎　有康	主任研究員
村上　隆夫	主任研究員
照屋　唯紀	研究員

暗号プラットフォーム研究チーム

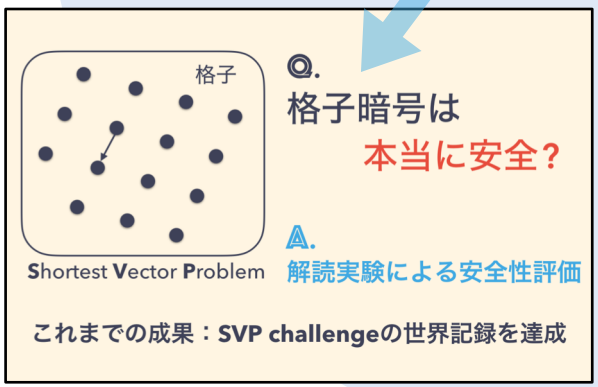


最先端暗号技術(関数暗号や差分プライバシ等)による**セキュアシステム**の設計

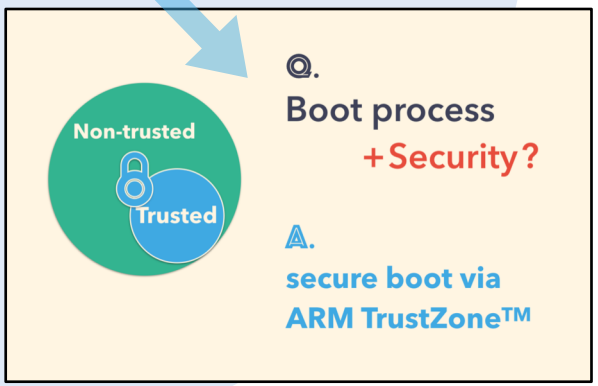


汎用的秘匿計算フレームワークの設計・ライブラリ開発

本研究チーム：システムセキュリティの様々なレイヤで ソフトウェア・フレームワークを設計・開発



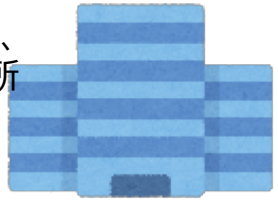
耐量子暗号(特に格子暗号) の解読**実験による安全性評価**



セキュアブートの設計・開発

外部企業・機関

三菱電機、パナソニック、NTT、日立、KDDI研究所



設計した汎用的フレームワークの中で、ニーズに沿った応用機能を提供

橋渡し研究

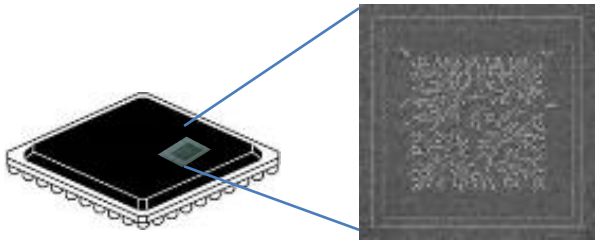
目的基礎研究

権威ある国際学会・ジャーナルへの論文採録による安全性保証

○ ハードウェアセキュリティ研究チーム

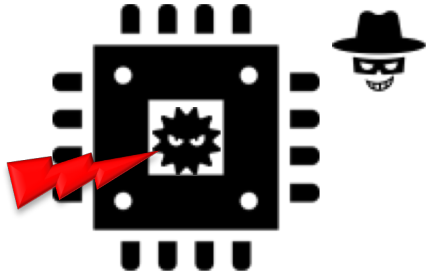
名前	役職
川村　信一	研究チーム長(兼務)
坂根　広史	主任研究員
今福　健太郎	主任研究員
堀　洋平	研究チーム付(兼務)
法元　盛久	招聘研究員
永田　真	招聘研究員
林　優一	招聘研究員

ハードウェアセキュリティ研究チーム



ナノ人工物などによる
コピー困難な個体識別

センサーとアクチュエーター
のセキュリティ



ハードウェアなどに仕掛けられた
不正機能(トロイの木馬など)への対応

ハードウェアや物理特性の観点からセキュリティの強化と評価 に貢献
得られた研究成果を対策基準、評価・認証制度などへ反映

攻撃可能性
などの検証

対策技術/
対策基準などの策定

評価・認証
パイロット実証

評価・認証のスキーム化については、セキュリティ保証スキーム研究チームと連携

○ セキュリティ保証スキーム研究チーム

名前	役職
吉田　博隆	研究チーム長
高木　浩光	主任研究員
辛　星漢	主任研究員
秋葉　澄孝	主任研究員
山田　朝彦	招聘研究員

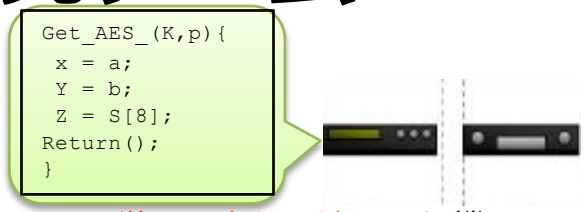
セキュリティ保証スキーム研究チーム

課題①：洗練されたノウハウ・最適化したツールを用いる攻撃者（ホワイトハッカー）視点の脆弱性分析

・攻撃者視点で社会的によく知られた攻撃から、論文の攻撃まで調査検討し、攻撃類型を集約
・製品評価のため、論文の攻撃の適用可能性を種々のメトリクスの観点でのスコアリング等により体系評価
・日進月歩の攻撃進化に対応する攻撃DBの保守

課題②：サイバーセキュリティの自己評価とサプライチェーンのリスク管理の観点からの新要件導出方法の策定

・成熟したICT分野のセキュリティ設計・評価に関するISO/IEC 15408を基本とし、NIST SP800-171等の近年のリスク評価・管理及び関連セキュリティ要件を分析
・システム仕様から、脅威を網羅的に分析し、論理的・低作業コストで要求を導出



課題③：厳しい実装環境下の新機器・システムに搭載する、暗号等のセキュリティ機能実装の妥当性検証

・SWやHWの新テクノロジーや、超低実装リソース、厳しいシステム要件を調査
・実装・システム要件を踏まえ、課題②で導出したセキュリティ要件に対し、課題①で抽出した攻撃類型のどこまで対策するかを明確化

関係機関と連携しながら、技術基盤を整備し、評価認証と国際標準化につなげる

新技術を迅速かつ確実に出口へつなげるためのセキュリティ保証スキームを実現

複数の研究プロジェクトや実証フィールドにおいて、横断的に技術育成と成果展開を実施

プロジェクト例：NEDOプロジェクト提案「SIP(第二期)/IoT社会に対応したサイバー・フィジカル・セキュリティ」

連携体制　電子商取引安全技術研究組合（ECSEC）、松本勉教授（横浜国大）、永田真教授（神戸大学）、池田誠教授（東京大学）
本間尚文教授（東北大）、林優一教授 (奈良先端大)、三菱電機（株）

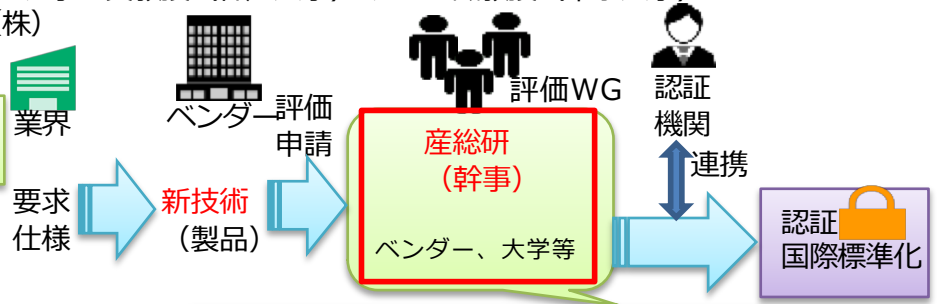
組込製品用チップを信頼の基点としてセキュリティ保証スキームを実現

組込製品用チップ(SCU)の脆弱性分析技術の集約

ハード改ざん等の脆弱性については、ハードウェアセキュリティ研究チームと連携

SCUアプリケーション分野別セキュリティ要求のまとめ

SCU認定とセキュリティ保証スキーム運用の技術的支援



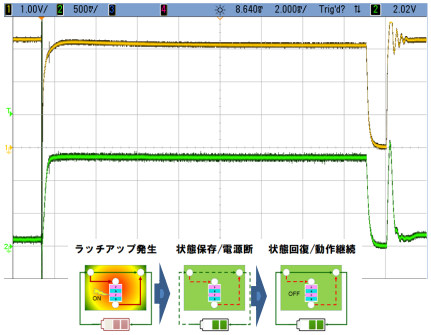
○ インフラ防衛セキュリティ研究チーム

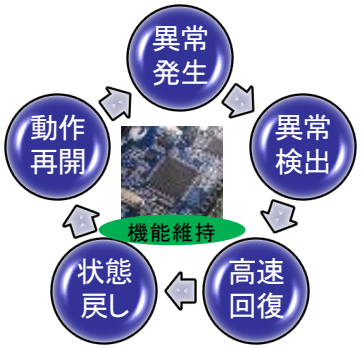
名前	役職
大崎　人士	研究チーム長
佐藤　豊	主任研究員
瀬河　浩司	主任研究員
半田　剣一	招聘研究員

インフラ防護セキュリティ研究チーム

従来のセキュリティ研究の概念にとらわれない研究を行います

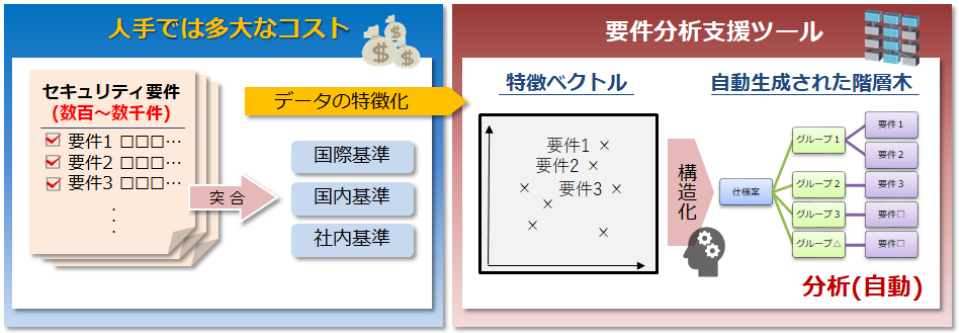
電磁波等の電気ノイズに耐える技術





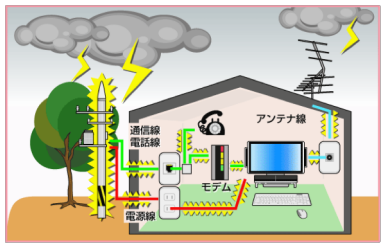
組込み、マイクロOS、チップの技術を組み合わせて、
動作中の電子機器を止めずに異常から回復させる

規約系文書を分析・設計する技術

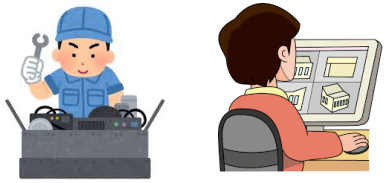


統計処理、言語処理、人工知能の技術を組み合わせて、
規約系文書の特徴抽出、文書の分析・設計を支援する

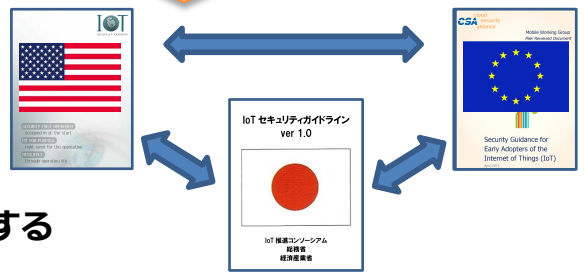
ソフトウェア技術を生かして、安全で信頼できる社会をめざす



身の回りの電子機器のノイズ耐性を強化して、
安心できる生活環境を実現する



人間の創造力を生かせる社会づくりに貢献する



セキュリティ規約の相対関係を明確にして、
地域や組織ごとの事情の違いを理解する

○ ソフトウェア品質保証研究チーム

名前	役職
大岩　寛	研究チーム長
田中　哲	主任研究員
Affeldt Reynald	主任研究員
小方　一郎	主任研究員
川本　祐輔	研究員

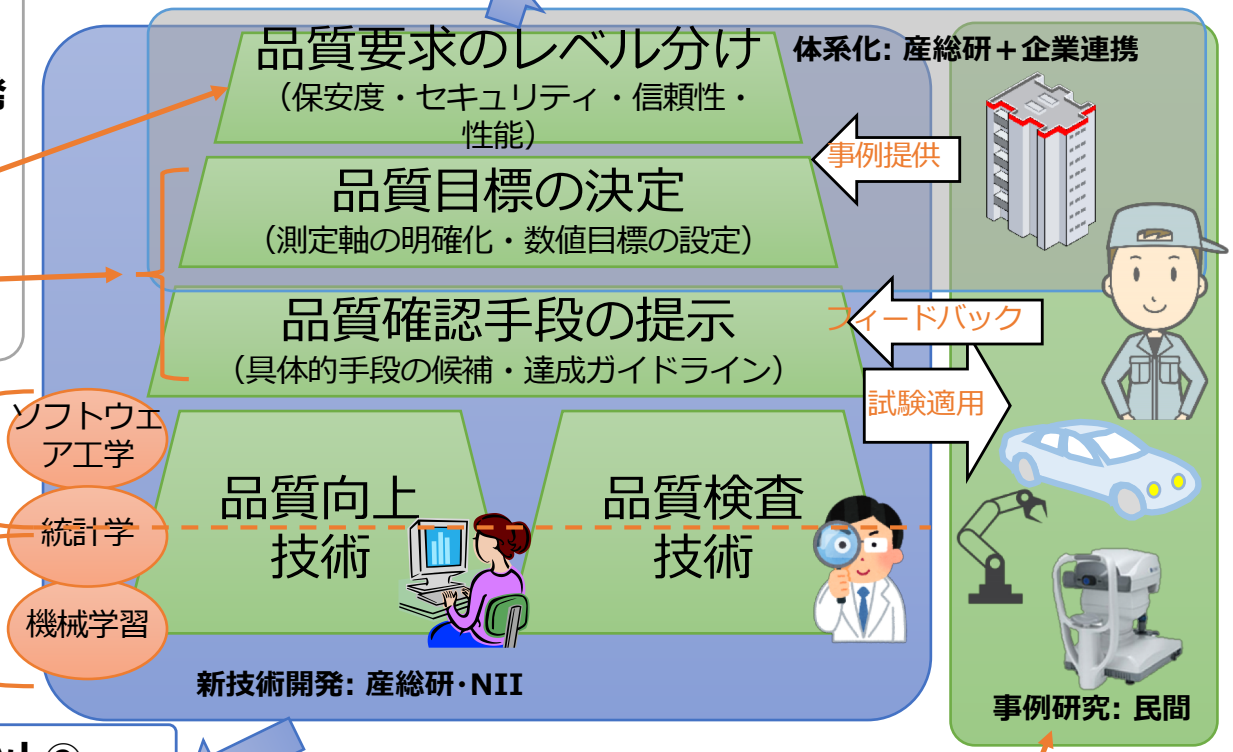
AI品質保証プロジェクト

アウトプット①:
フォーラム・デファクト標準としての
安全性基準・確認ガイドライン
→ 将来のJIS/ISO化を想定

実施項目1:
品質要件の明確化に関する研究と
品質保証エコシステム（保証プロセス）の開発

1-1: AI利用製品の品質要件の明確化と
レベル分けに関する研究
1-2: AI利用製品の品質保証のための
実装プロセスに関する研究

AIソフトウェアに特化した
具体的な品質保証技術
実施項目2: AIの品質を実装時・検査時・
実用時それぞれで管理し担保する
技術の研究開発（短期）
実施項目3: 高品質AIシステムのための
AI基礎技術の研究開発(中長期)



アウトプット②:
具体的技術・ツール

実施項目4: 製品レベルでの品質保証実証研究
グランドチャレンジを設定し、実応用を研究として実施

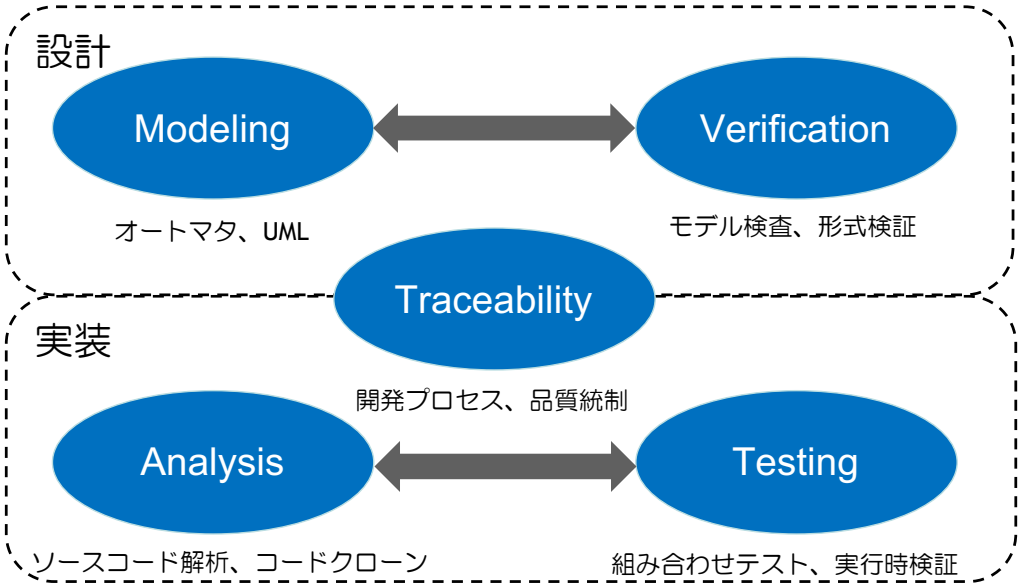
アウトカム③:
産業界の技術力・
国際競争力強化

- 社会基盤としての基準作りと、それを実現する技術をセットで並行開発
- 産業界との密接な連携
  - 〔先導研究から〕企業との連携による実事例分析・基準作りへの反映
  - 〔本格研究から〕実事例での実際の技術適用とフィードバック

○ソフトウェアアナリティクス研究チーム

名前	役職
森　彰	研究チーム長
磯部　祥尚	主任研究員
西原　秀明	主任研究員
北村　崇師	主任研究員
崔　銀恵	主任研究員
井上　純	研究員

ソフトウェアアナリティクス研究チーム

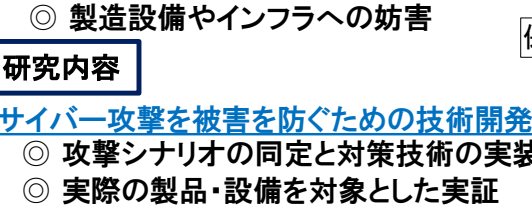


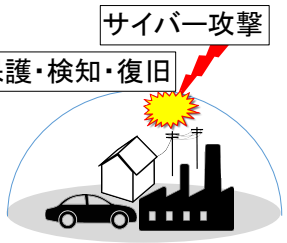
住友電工−産総研
サイバーセキュリティ連携研究室

IoT製品や設備に対するサイバー攻撃
- ◎ 車載システムの乗っ取りと遠隔操作
- ◎ 製造設備やインフラへの妨害

研究内容

サイバー攻撃を被害を防ぐための技術開発
- ◎ 攻撃シナリオの同定と対策技術の実装
- ◎ 実際の製品・設備を対象とした実証





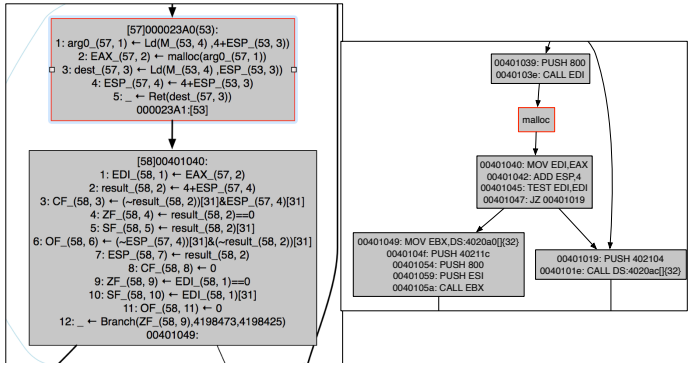
室長　森彰

H28.6.1設立

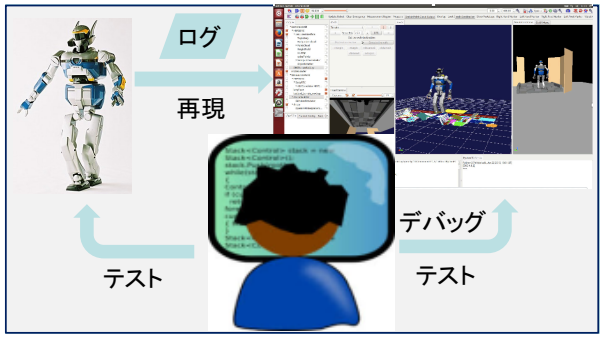
ソフトウェアの品質を向上させることでIoT製品のセキュリティを高める

井上 克郎教授（大阪大学大学院 情報科学研究科）
森井 昌克教授（神戸大学大学院 工学研究科）

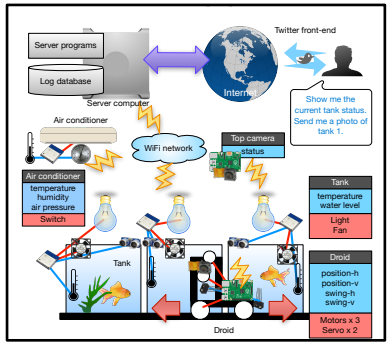
水野 修教授（京都工芸繊維大学 情報工学・人間科学系）
飯田 元教授（奈良先端科学技術大学院大学 情報科学研究科）



ファームウェア解析による脆弱性自動検査



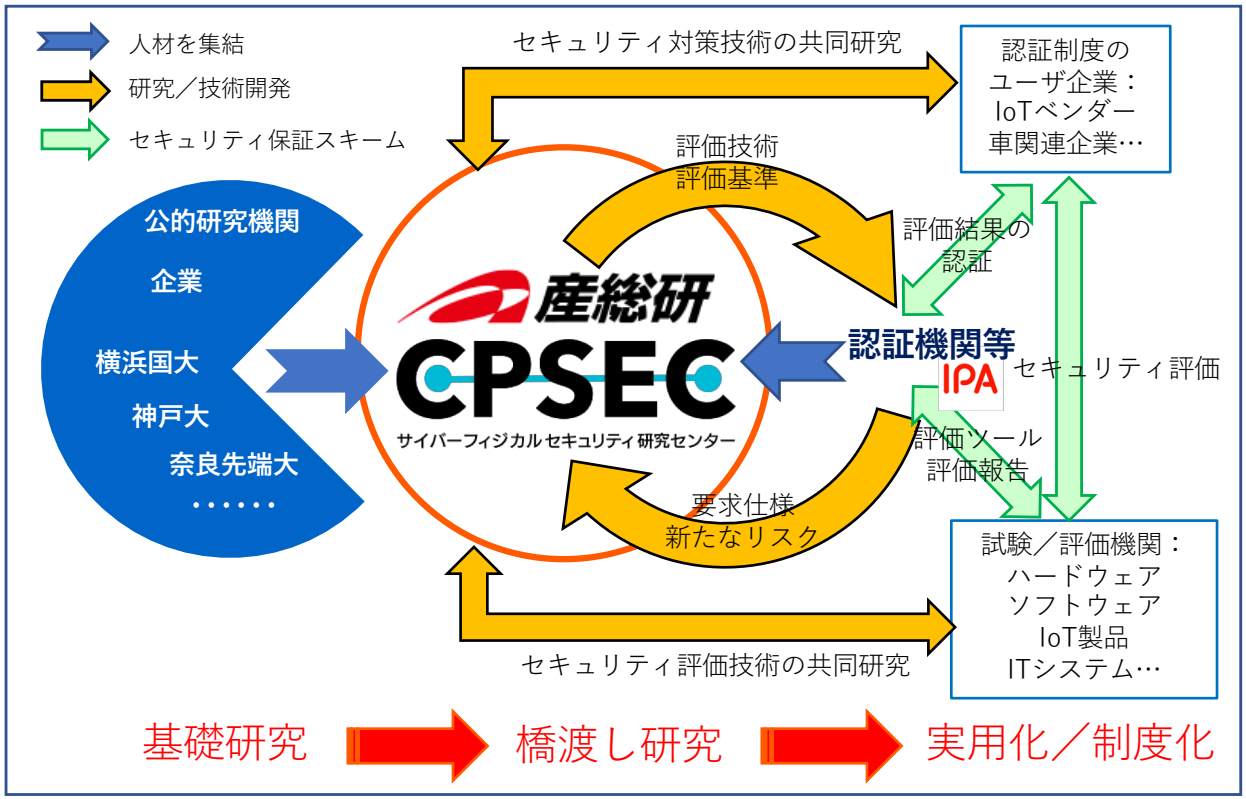
ロボットシステムの高信頼化



IoTシステムのログ解析と異常検知

産総研サイバーフィジカルセキュリティ研究センター

- サイバーフィジカルセキュリティの研究拠点として設置（2018年11月～2025年3月）
- 産総研、企業、大学、試験／評価機関等から研究者や技術者をセンターに集結
  12月17日現在総員115名＝職員等(産総研の身分を有する者)88名+外来研究員等(含む学生)27名
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」までを技術面からサポート
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積



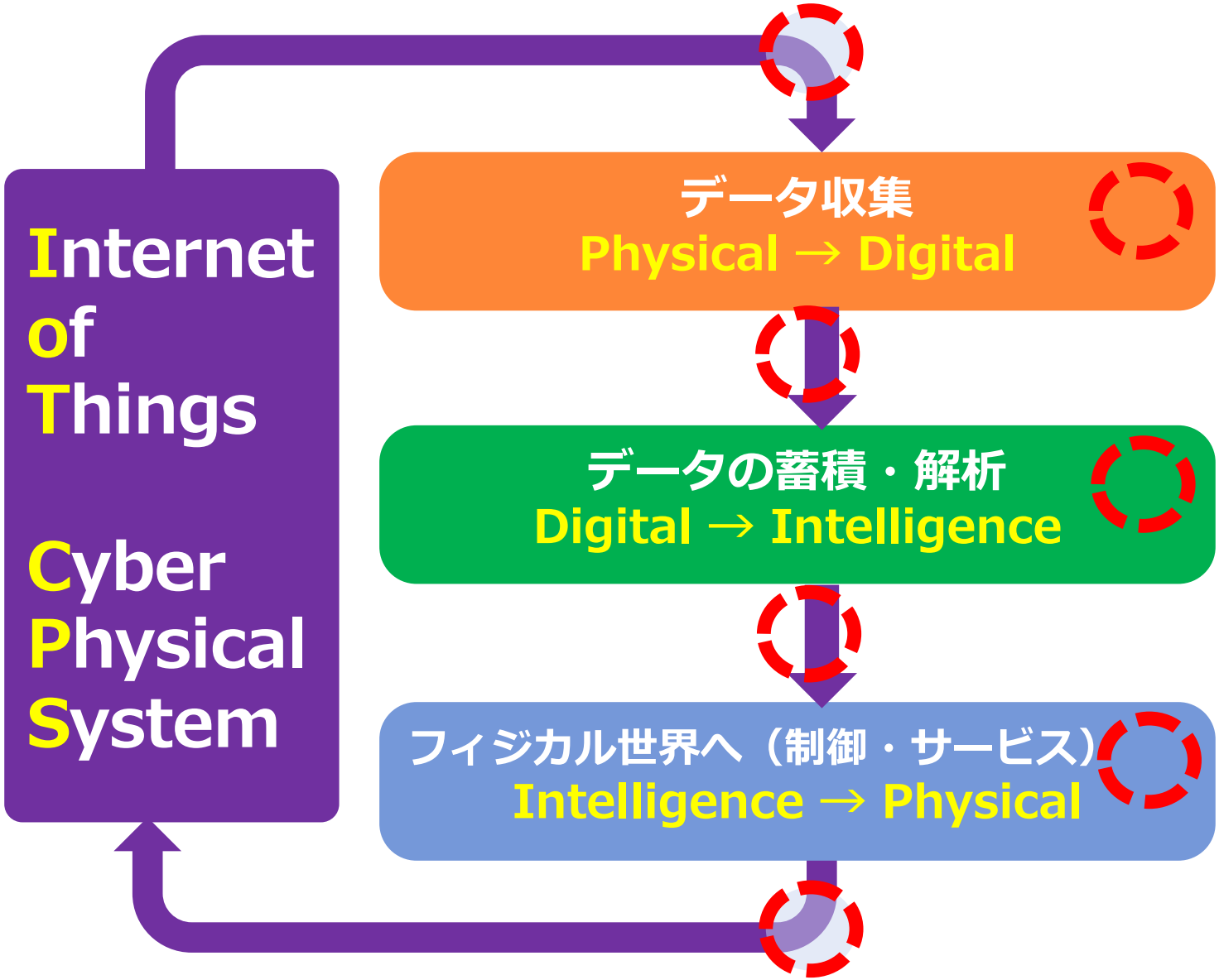
CPSECとして新規採択された研究開発プロジェクト

- 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
  - (A1) IoTサプライチェーンの信頼の創出技術基盤の研究開発
    - 代表：ECSEC組合　共同提案者：産総研
  - (B1) 分野毎の特性を踏まえた信頼チェーンの構築技術の研究開発
    - 代表：日立製作所（再委託：産総研）
  - (C1) 信頼チェーンの検証技術の研究開発
    - 代表：日立製作所（再委託：産総研）

- NEDO 高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発／ 研究開発項目①革新的AIエッジコンピューティング技術の開発
  - AIエッジデバイスの横断的なセキュリティ評価に必要な基盤技術の研究開発
    - 代表：産総研

      AIエッジ入出力　AIエッジ処理　AIエッジID管理

サイバーフィジカルセキュリティの研究課題



- ID管理／認証
- 通信のセキュリティ
- 蓄積のセキュリティ
- 処理のセキュリティ
- 計測のセキュリティ
- 制御のセキュリティ
- 管理のセキュリティ
- トラストの置き方

…

における新しい展開

- 計算リソース、
- エネルギー、
- ライフタイム、
- 環境変化
- 未知の脅威

…

にどう立ち向かうか

- 何を標準化するか
  ルール化するか

CPSECと連携しませんか？
未解決テーマ：大歓迎

CPSECと連携しませんか？
未解決テーマ：大歓迎

CPSECに来ませんか？

サイバーフィジカルセキュリティ研究センターの概要と戦略

2018年12月17日

国立研究開発法人 産業技術総合研究所
情報・人間工学領域

サイバーフィジカルセキュリティ研究センター長

松本　勉