経済産業省

資料7

# サイバー・フィジカル・セキュリティの確保に向けた研究開発の動き

平成30年8月3日

経済産業省　商務情報政策局

サイバーセキュリティ課

# サプライチェーンサイバーセキュリティに係る研究開発の推進

産業サイバーセキュリティ研究会（第2回）にて配布

- 総合科学技術・イノベーション会議の**研究開発プログラム（SIP）に「IoT社会に対応したサイバー・フィジカル・セキュリティ」プログラムを設置など**(※) 研究開発事業を拡充。
- 更に、**拠点化による中核的な研究開発体制の整備**や、研究成果の実装のための**認定・認証体制の強化**を推進。

## 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」

**平成30年3月30日：**
総合科学技術・イノベーション会議にて**課題決定**

**平成30年4月12日：**
**プログラムディレクター(PD)決定**
**後藤 厚宏 情報セキュリティ大学院大学 学長**

**平成30年度下半期：**
**研究開発開始を予定**

### 研究開発の内容

**■サプライチェーンのセキュリティ確保**

（例）
- IoT等の**エッジデバイスのセキュリティ確保**技術
- **取引先のセキュリティの確保状況を確認**するための基盤技術
- **AIを活用したサイバー攻撃の検知・解析**技術

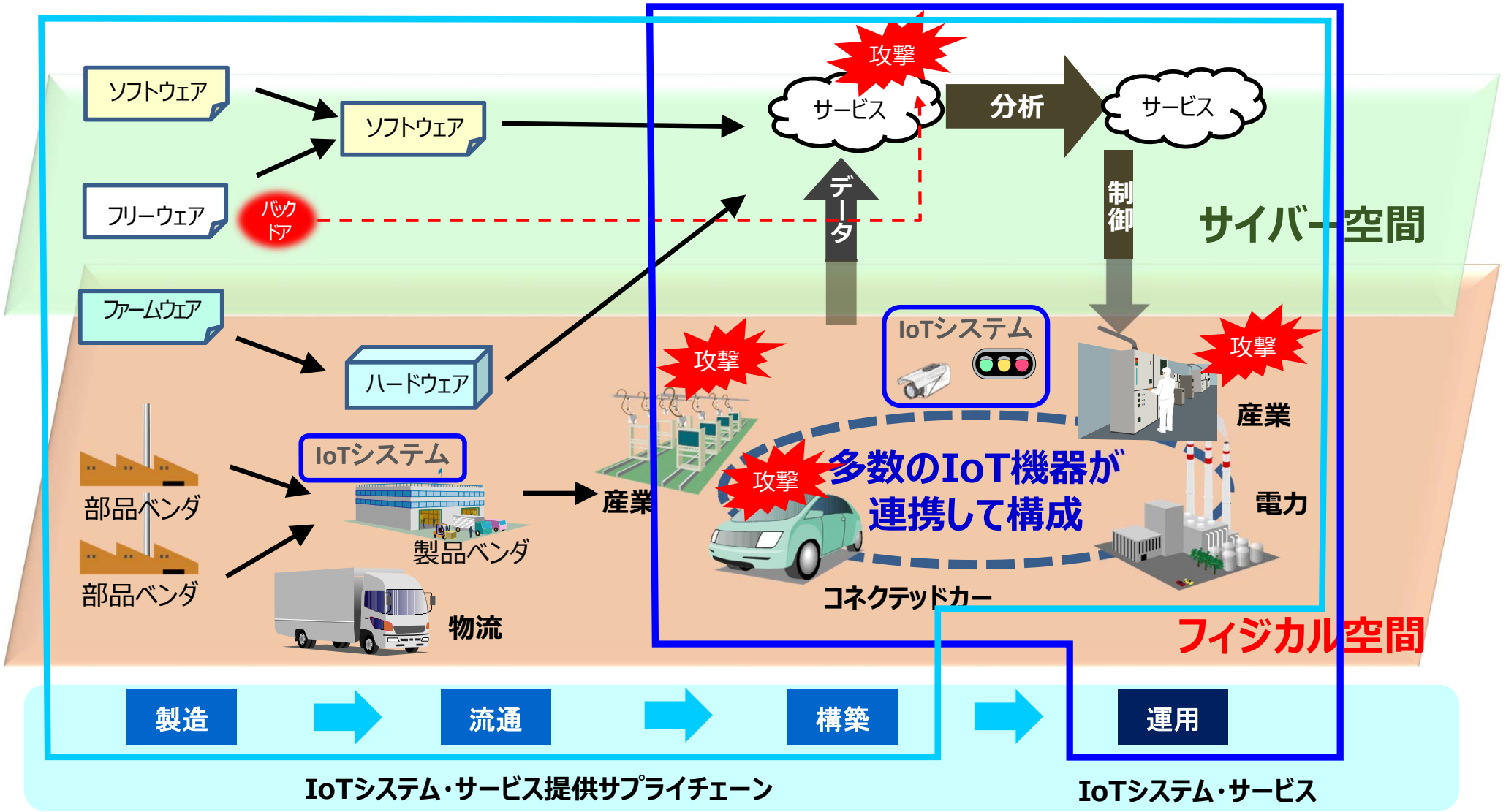
※ AIチップ・次世代コンピューティングの技術開発においてもセキュリティ技術の研究開発を推進

# 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」

**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**



# SIP第2期 - 研究開発の取組内容

## A.信頼の創出・証明

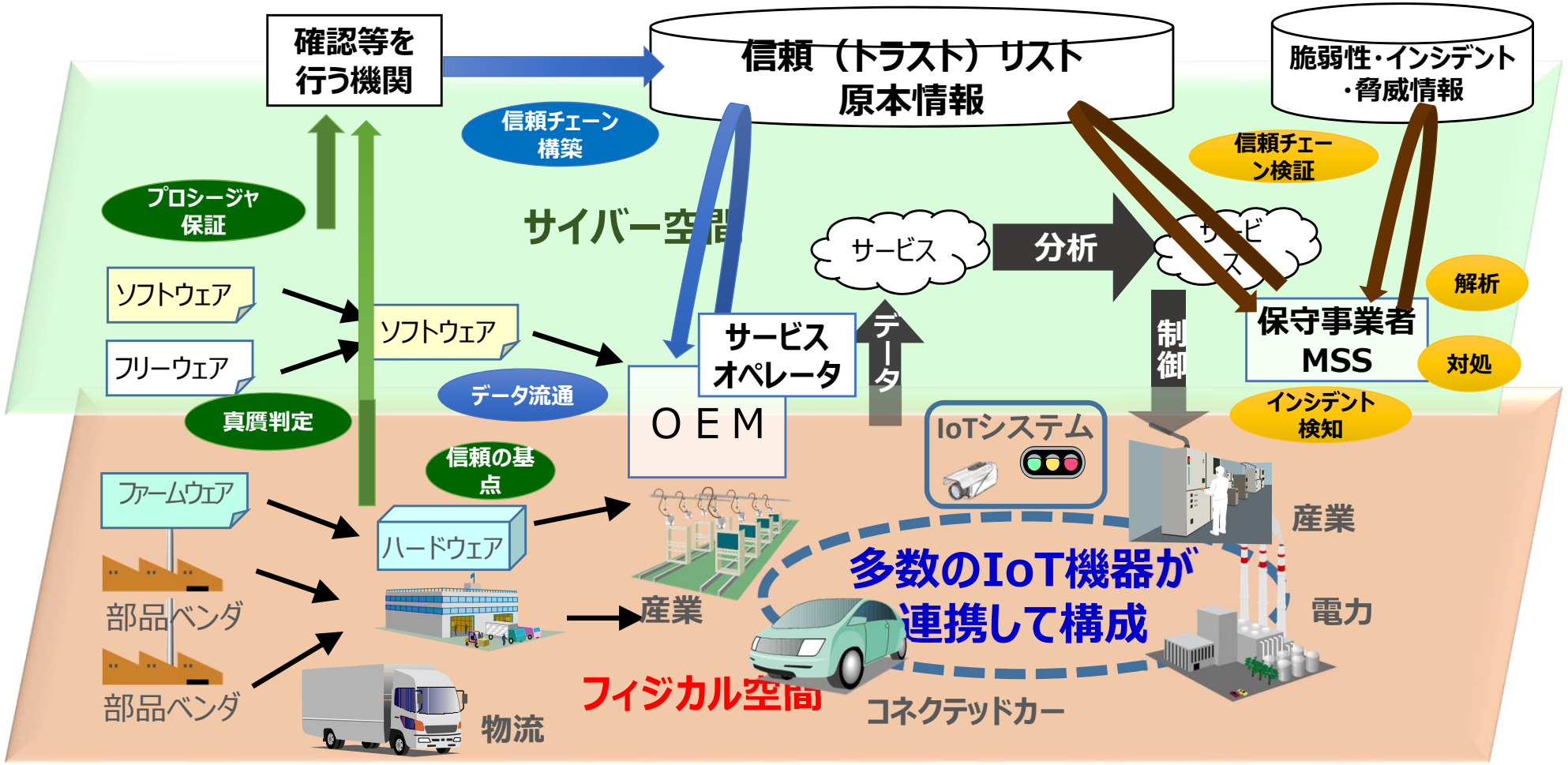
多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

## B.信頼チェーンの構築・流通

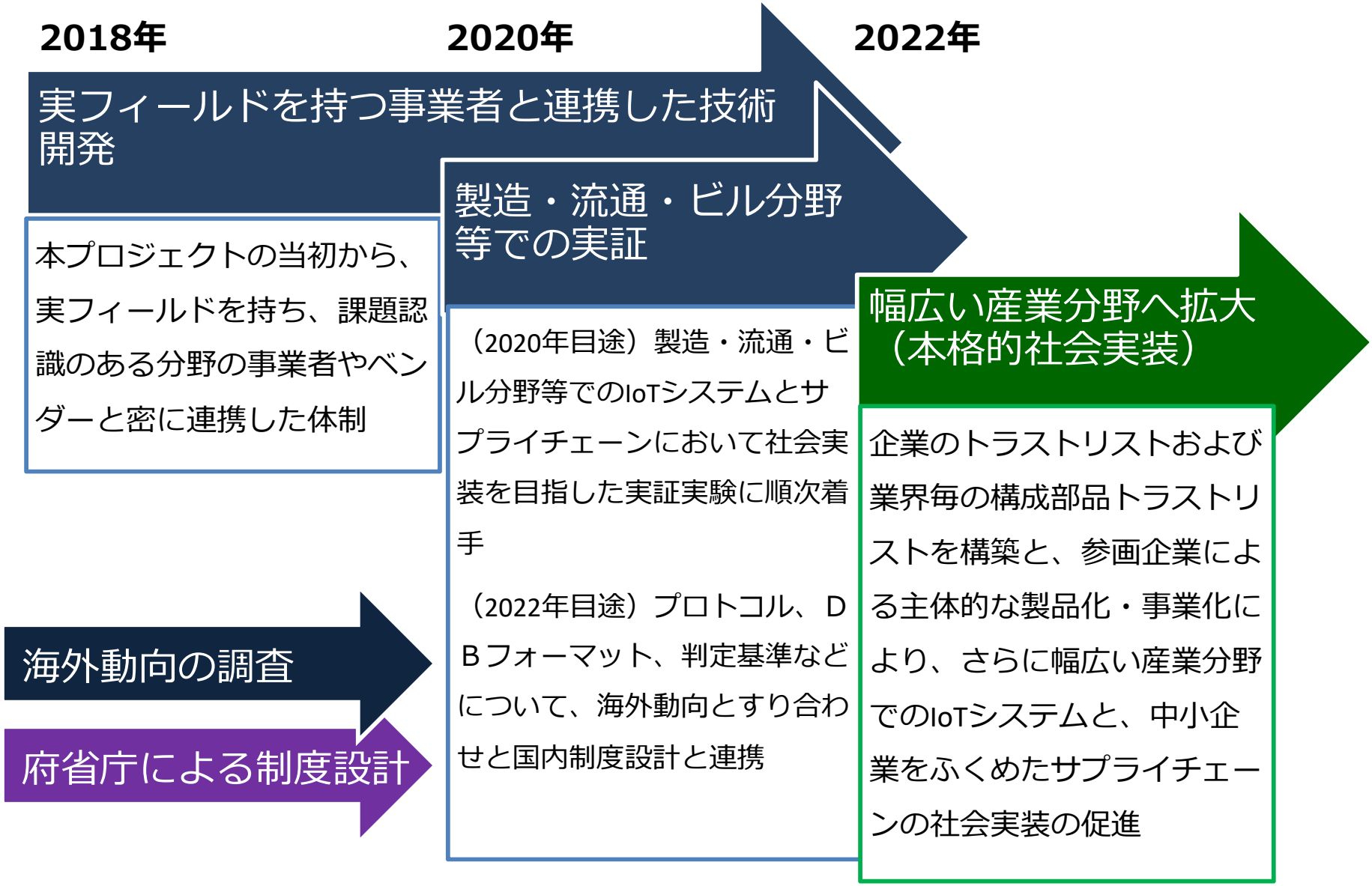
信頼チェーンを構築し、必要な情報をセキュアに流通させる技術

## 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



# SIP第2期 - 出口指向の研究推進

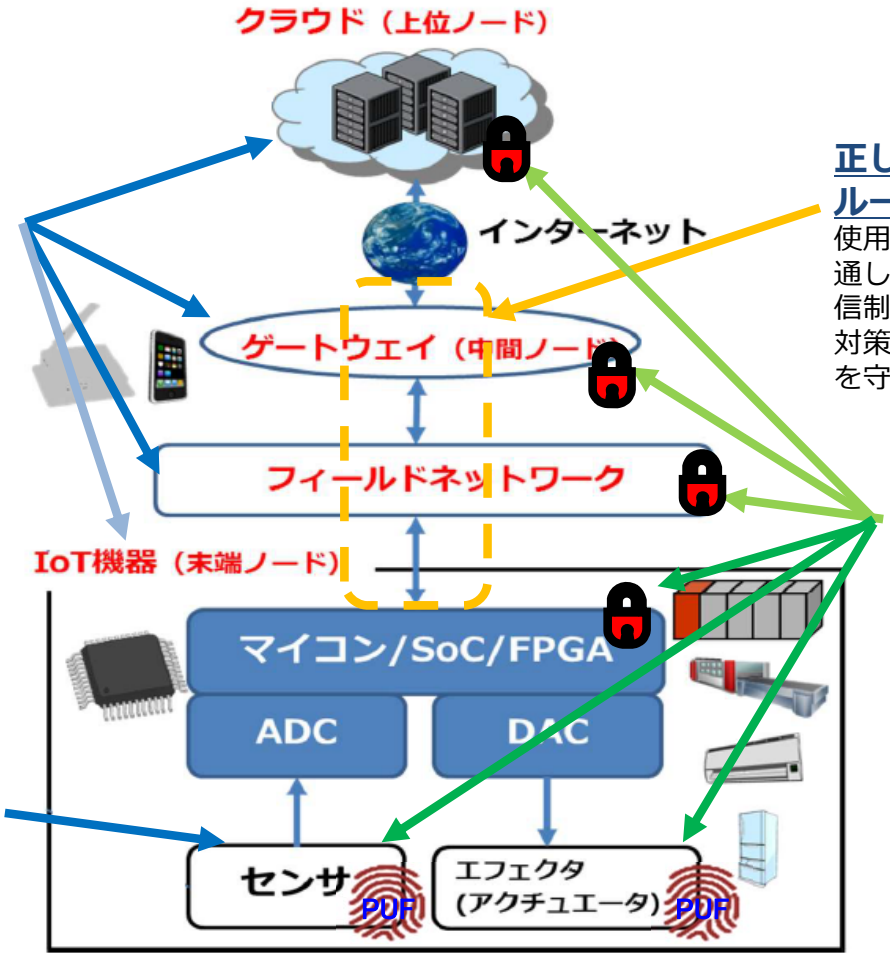


# （参考）AIチップ・次世代コンピューティングの技術開発におけるセキュリティ技術の研究開発（経済産業省）

## IoT時代におけるハードウェアセキュリティ基盤の構築

＜経済産業省＞

・高機能暗号や計測セキュリティ、通信制御機器、複製不可能デバイスなどのハードウェアセキュリティ基盤を構築することで、多様なIoT機器からクラウドまでセキュアな環境を実現




**高機能暗号**
クラウドからフィールドネットワークまでのセキュリティ課題を解決する為の、高機能暗号を高速・低消費エネルギーで実現するチップとソフトウェアの要素技術の開発。

**正しい通信だけを許可するルータ等の通信機器**
使用するサービスを元に自動で通してよい通信のみを通す「通信制御」により、セキュリティ対策を個別に実施できない機器を守る。

**複製不可能デバイス**
製造プロセス中のゆらぎなど複製困難な特性(PUFなど)を利用して実現。デバイス固有のIDや暗号鍵に利用することで、安価に機器認証・偽造品防止する要素技術の開発。

(PUF: Physical Unclonable Function)

**計測セキュリティ**
センサ等による情報取得に対する脅威への対策に関する要素技術の開発。