# IoT社会に対応した サイバー・フィジカル・セキュリティ

『サイバー・フィジカル・セキュリティ対策基盤』の研究開発

SIP PD 後藤厚宏



# IoTリスクとサプライチェーンリスク

loT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



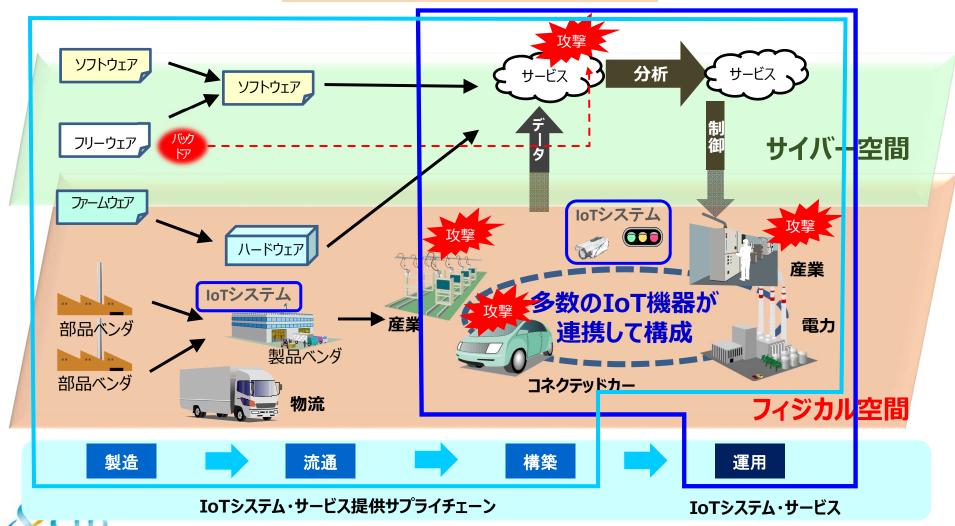
# Society 5.0=サイバー・フィジカル高度融合システムの課題

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



20180627 意見交換会

3

# 『サイバー・フィジカル・セキュリティ対策基盤』研究開発の重要性 (All Japanで取組み意義)

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(サイバー犯罪による経済損失の回避)

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

製造業等が国際調達に参入する機会を確保

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



# 『サイバー・フィジカル・セキュリティ対策基盤』研究開発

#### 社会実装

実証実験(製造・流通・ビル等)・ 国内制度設計と連携

loTシステム・サービス のセキュリティ確保



信頼のチェーン

信頼の創

出·証明

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





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

信頼 チェーン の検証・ 維持 信頼 チェーン の構築・ 流通



# 研究開発の取組み内容(1)

• 信頼の創出:信頼の基点の埋め込みと保護

• 信頼の証明:システムの構成要素の真贋判 定と構成するプロシージャの適格性保証

目標:多種・大量の小型IoT機器にコスト 性能面で適用可能

信頼の創 出・証明

検証:信頼チェーンとして 正常に運用できていること を検証する技術

• 維持:信頼チェーンの異常

検知·対処技術

信頼の チェーン 構築:信頼チェーンを構築するプロトコル(トラストリストの登録・更新、参照)技術、と調達システム連携

• 流通:広域分散型の信頼 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 信頼チェー ンの構築・ 流通

目標:中小企業を含む大規模サプライチェーンが多数重 層構造となるスケール(構成組織数が1万以上)に対応



# 研究開発の取組み内容(2)

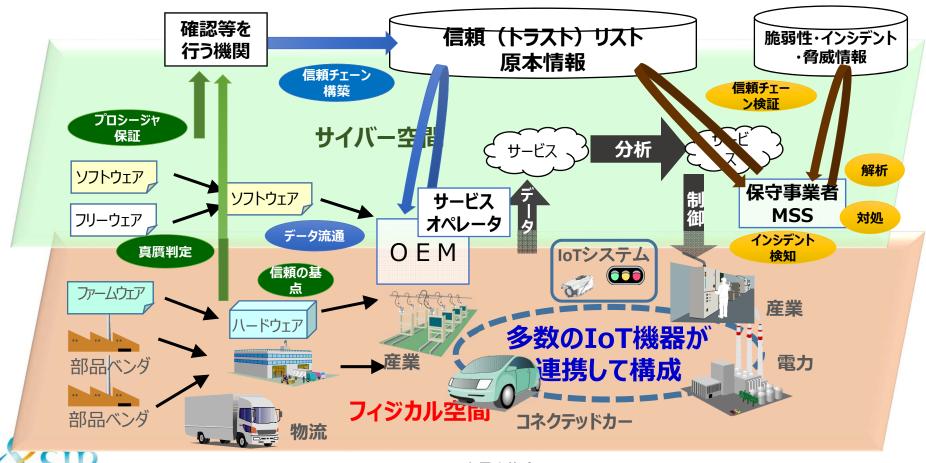
#### A.信頼の創出・証明

#### B.信頼チェーンの構築・流通

#### c.信頼チェーンの検証・維持

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

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 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



# 出口指向の研究推進

2018年

2020年

2022年

実フィールドを持つ事業者と連携した技術

開発

本プロジェクトの当初から、 実フィールドを持ち、課題認 識のある分野の事業者やベン ダーと密に連携した体制

製造・流通・ビル分野

等での実証

(2020年目途) 製造・流通・ビ ル分野等でのIoTシステムとサ プライチェーンにおいて社会実「企業のトラストリストおよび 装を目指した実証実験に順次着 手

について、海外動向とすり合わ でのIoTシステムと、中小企 せと国内制度設計と連携

幅広い産業分野へ拡大 (本格的社会実装)

業界毎の構成部品トラストリ ストを構築と、参画企業によ (2022年目途) プロトコル、D る主体的な製品化・事業化に Bフォーマット、判定基準など より、さらに幅広い産業分野 業をふくめたサプライチェー ンの社会実装の促進

## 海外動向の調査

府省庁による制度設計



# 出口指向の取組み

#### 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

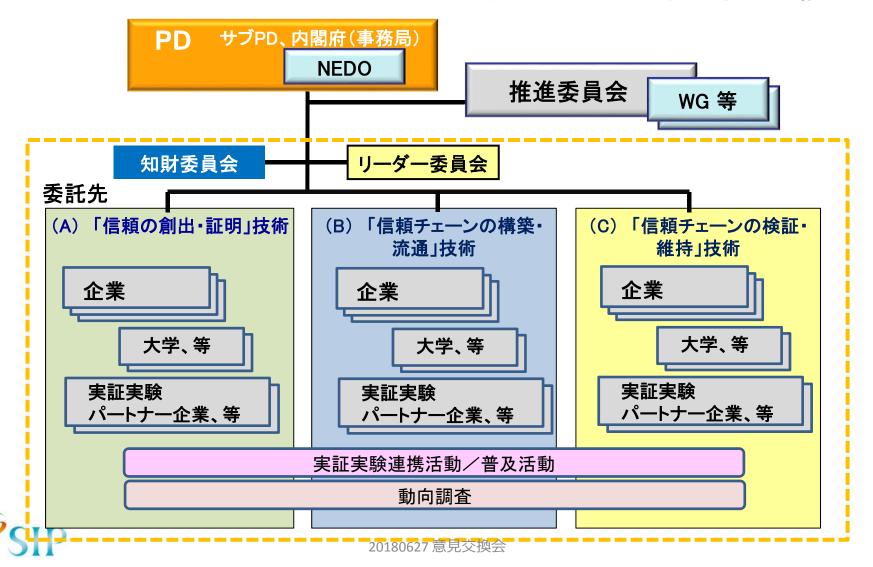
#### 普及のための方策

- 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



## 実施体制

● 研究開発の成果を主体的に<u>実用化・事業化できる企業を中心</u>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。



10

# 『サイバー・フィジカル・セキュリティ対策基盤』研究開発の目標

社会面の 目標

社会全体の安全・安心を確立し、Society5.0がもたらす約90兆円の価値創出を支える

産業面の 目標

- 幅広い産業分野の国際競争力を高める(輸出主体の製造業の参入機会の確保)
- 2030年までにサプライチェーン対策が求められる中 小企業の50%に成果導入

制度面の 目標

- 各産業分野のセキュリティポリシーの策定活動と連携
- 産業界の個別ニーズに応じた**制度整備に貢献**する

グローバル ベンチマー ク

• 国内に加え、**海外の要件にも適用**できるかの検証を行い、世界に対する優位性を確認する



# Society5.0に向けた取組みとしての位置づけ

● Society 5.0として実現を目指す様々なサービス・システムのサイバーセキュリティを確保する

