プログラムの概要紹介

プログラムディレクター
情報セキュリティ大学院大学　学長

後藤 厚宏

戦略的イノベーション創造プログラム SIP

IoT社会に対応した サイバー・フィジカル・セキュリティ

内閣府 SIP プログラムディレクタ（PD）

サイバーセキュリティ戦略本部

情報セキュリティ大学院大学

後藤　厚宏

広義IoTがもたらす価値創造

SIP第2期
2018～2022

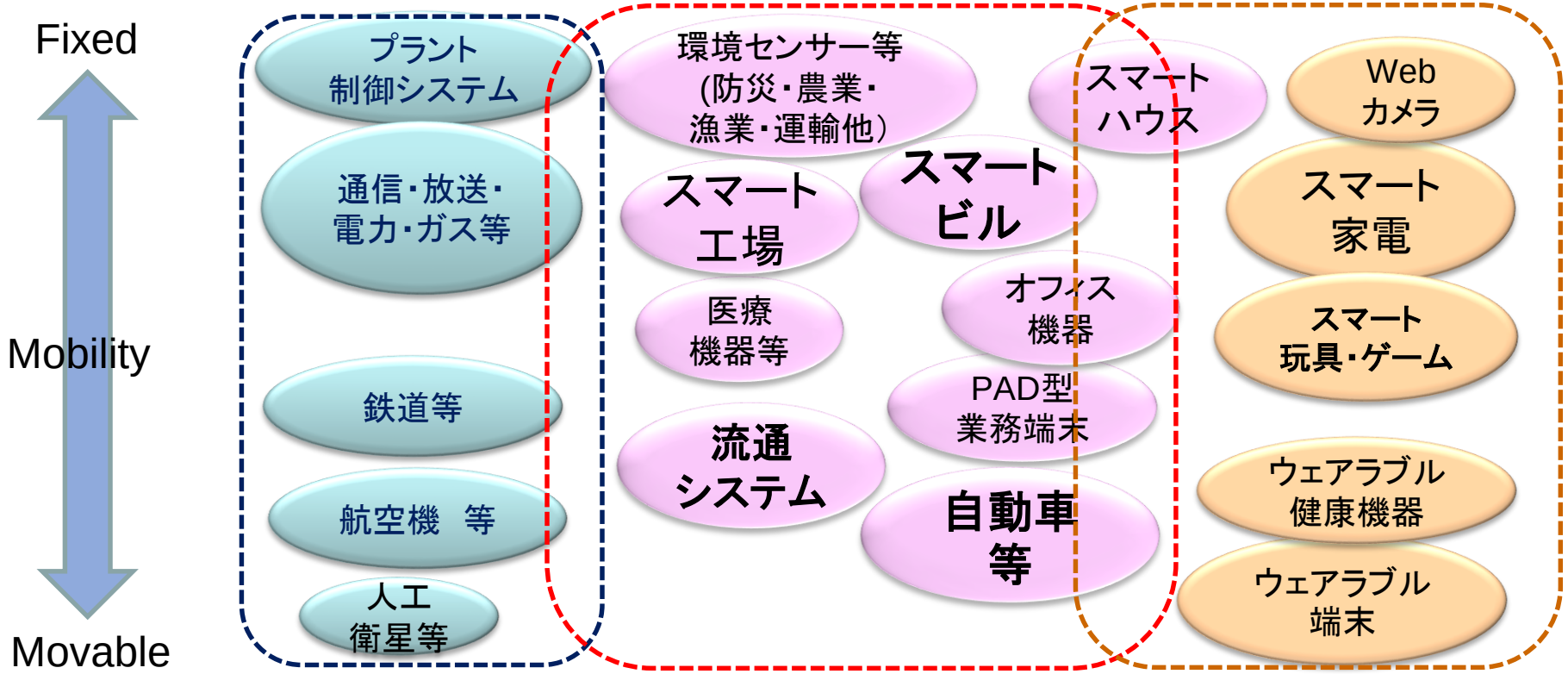
重要インフラの革新
「インフラIoT」

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」

第1期SIP「重要インフラ等のサイバーセキュリティ確保」
(2015―2019)

第2期SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」
(2018―2022)



IoTリスクとサプライチェーンリスクは喫緊の課題

SIP第2期
2018～2022

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5月から

IoTリスク：IoT機器が社会インフラへサイバー攻撃

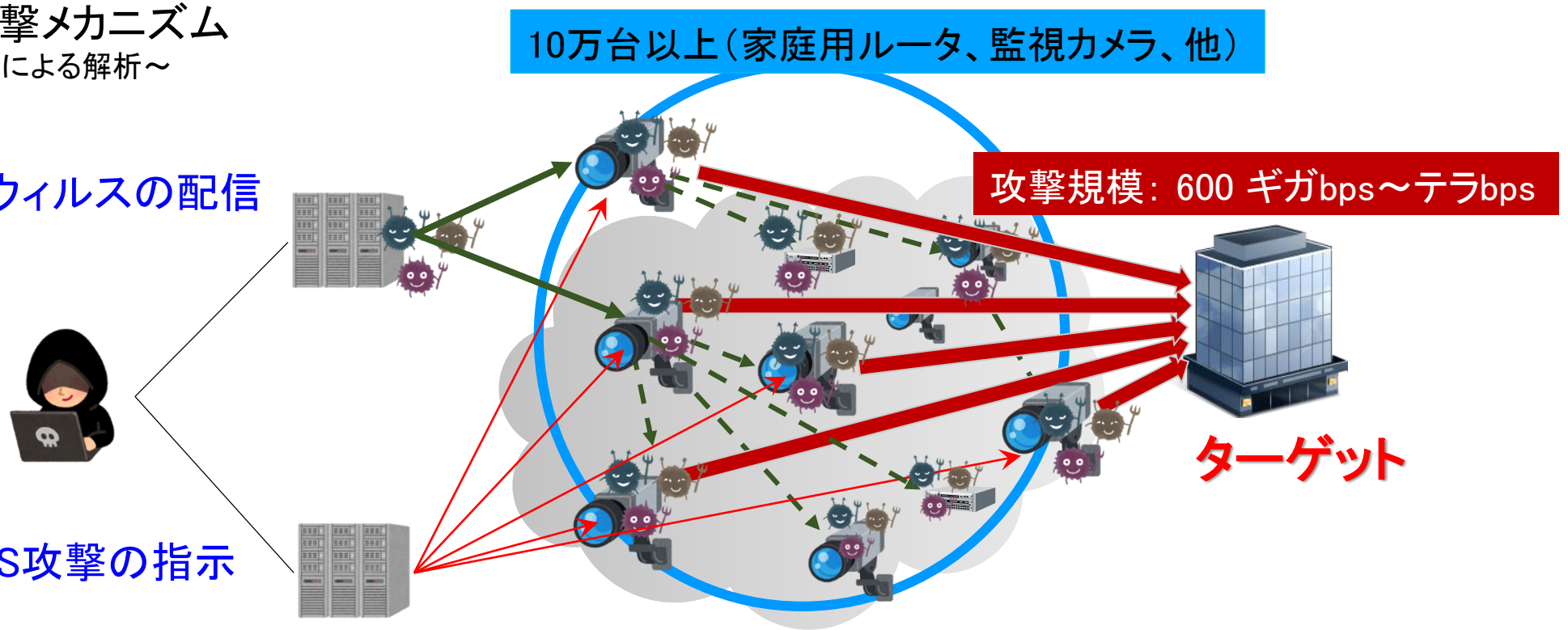
SIP第2期
2018～2022

■ Miraiの事案：脆弱性のあるIoT機器が大規模DDoS攻撃の踏み台

【事例1】 DDoS攻撃（2016/10）により約6時間にわたりインターネットサービスが不安定（Twitter, Amazon, Netflixが使えない！）

【事例2】 ドイツテレコムのホームルータをマルウェア感染させる攻撃（2016/11）により、90万人が影響を受ける

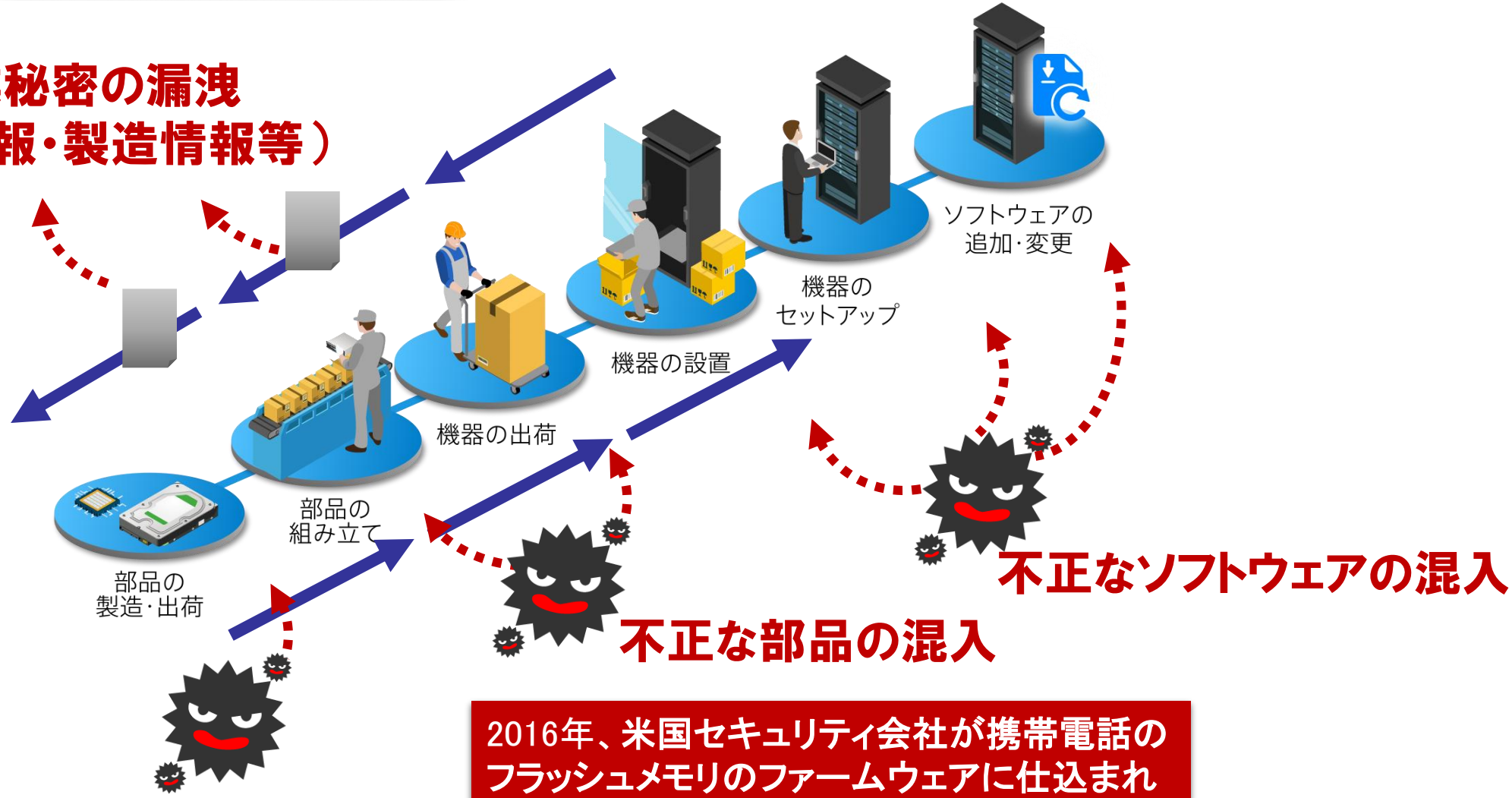
Miraiの攻撃メカニズム
～NTT研究所による解析～



同様の脆弱性を持つ多数の機器が感染し、一斉に遠隔操作される

サプライチェーンリスク:「混入」「改ざん」「漏洩」

SIP第2期
2018～2022

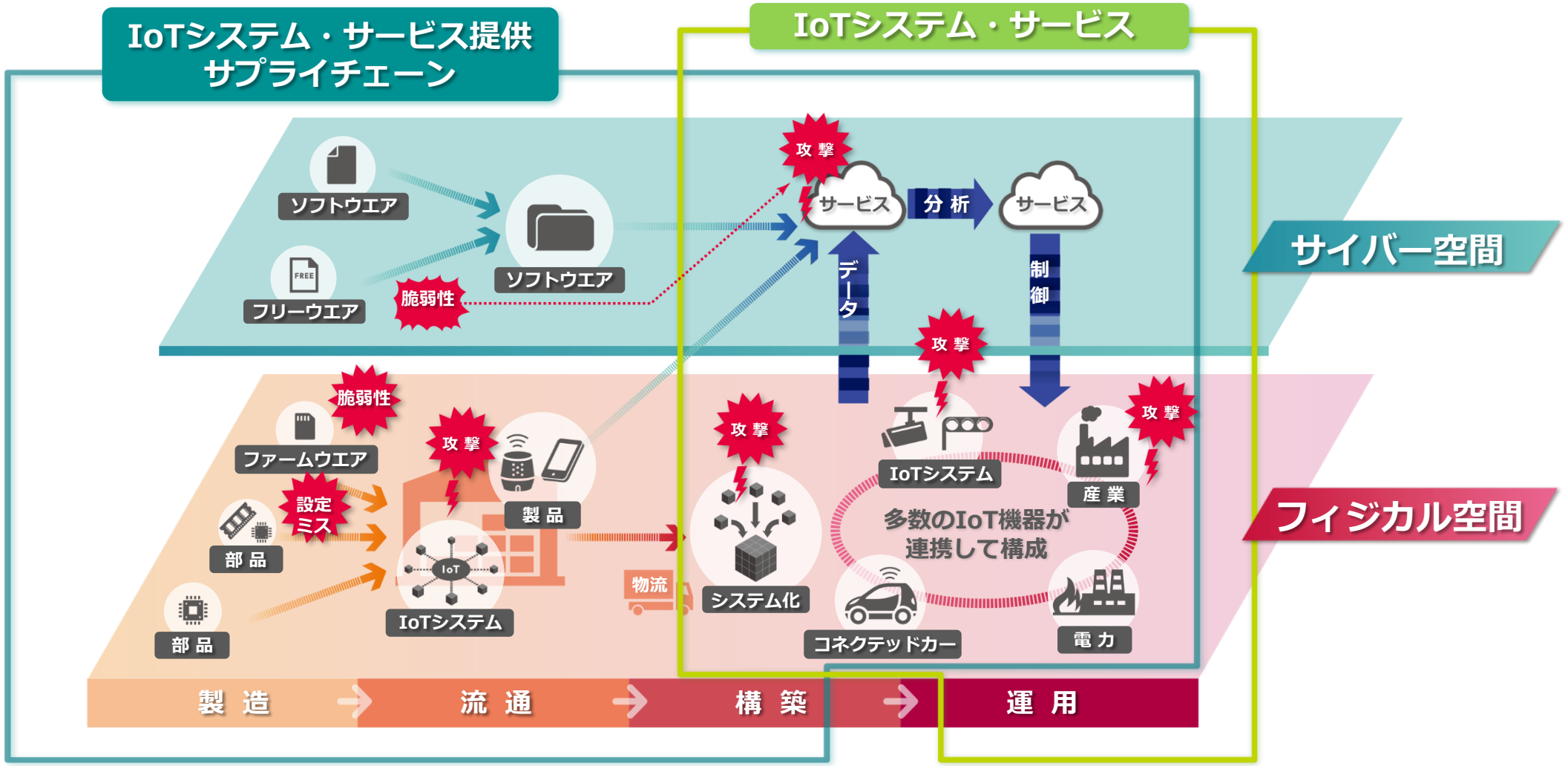


2016年、米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。

サイバー・フィジカル・システムのセキュリティ課題

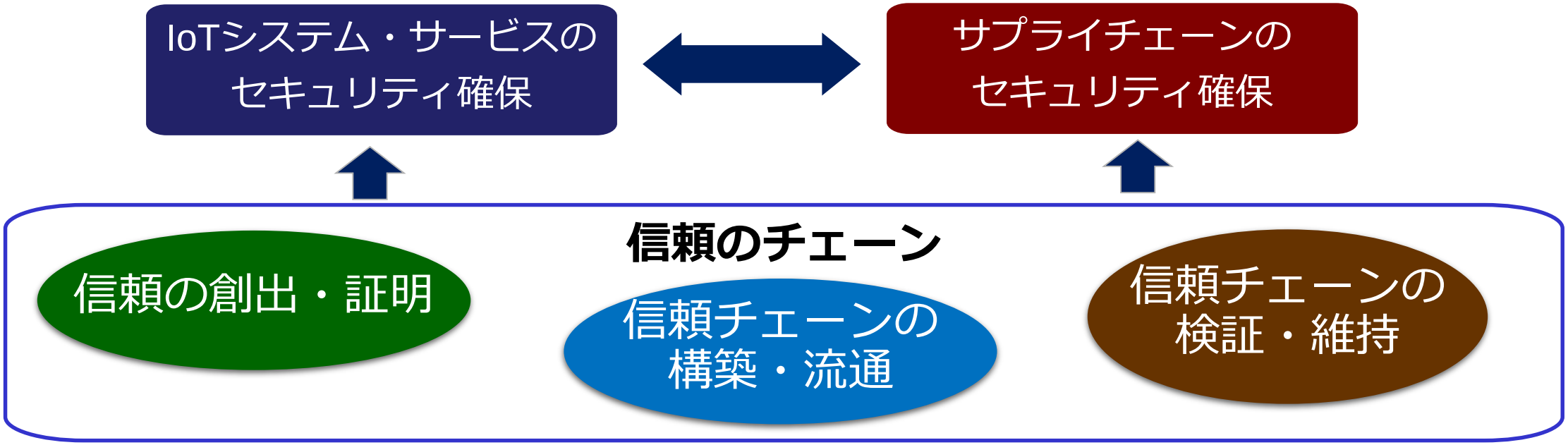
SIP第2期
2018～2022

サプライチェーンのセキュリティ確保 ⟷ **IoTシステム・サービスのセキュリティ確保**



「信頼のチェーン」によるセキュリティ確保

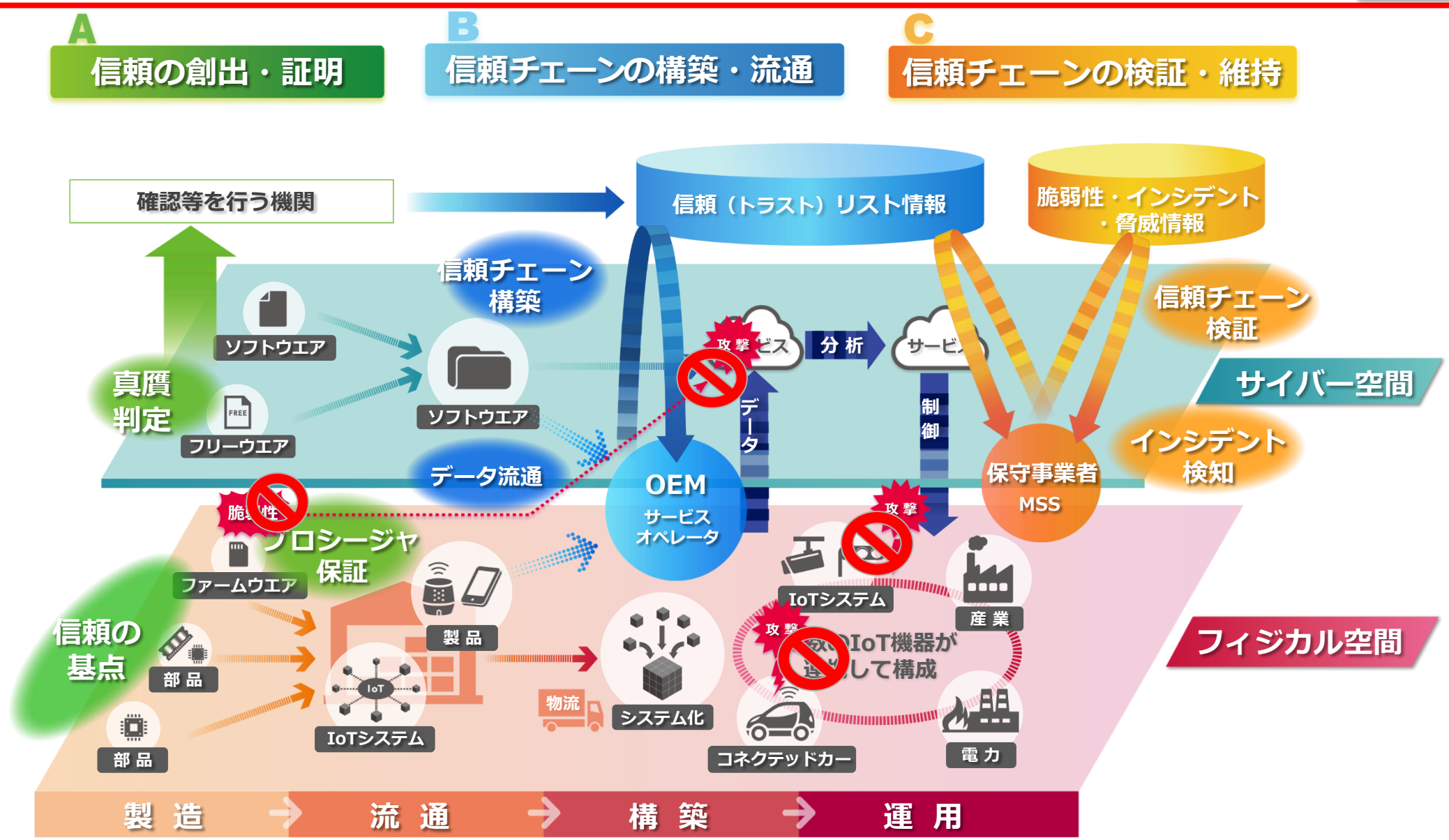
SIP第2期
2018～2022



- ◆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
- ◆幅広い産業分野の国際競争力を高め、輸出主体の製造業の**参入機会の確保**する
- ◆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%**に成果導入を目指す

サイバー・フィジカル・セキュリティのエコシステム

SIP第2期
2018～2022



研究開発の実施チーム体制

SIP第2期
2018～2022

PD　後藤 厚宏
subPD　今瀬 真、瓜生 和久
内閣府(事務局), NEDO

サイバー・フィジカル・セキュリティ　推進委員会
NISC，総務省，経産省，防衛省，他
学会、産業界の有識者

WG等　海外動向WG　成果普及WG　実証評価WG

リーダー委員会　知財委員会

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		D 動向調査
A1	A2	A3	B1	B2	C1	C2	
ECSEC 産総研 (横国大、神戸学、東大、東北大、NAIST、三菱電機)	NTT NEC (FFRI)	日立 NEC KDDI総研 (ATR、早稲田大)	日立 NEC KDDI総研 (産総研、セコム、ATR)	富士通 (NII, 名大)	日立 NEC KDDI総研 (産総研、ATR)	NTT NEC 日立 三菱 (阪大、金沢工大)	NEC

(2018年度)

関係府省との連携状況

NISC

・サイバーセキュリティ戦略の重点項目のひとつ

経産省

・サイバーフィジカルセキュリティフレームワークの実現技術としての役割

総務省

・NOTICE プロジェクトと連携するIoTセキュリティ技術

NOTICE (National Operation Towards IoT Clean Environment)

実フィールドで実証し社会実装へ

SIP第2期
2018～2022

2018年

2020年

2022年

技術開発と実フィールド事業者連携

実フィールドを持つ事業者やベンダーと密に連携した体制作り

製造・流通・ビル分野等での実証

（2020年目途）IoTシステムとサプライチェーンにおいて社会実装を目指した**実証実験に順次着手**

（2022年目途）**海外動向，国内制度**設計と連携・すり合わせ

幅広い産業分野へ拡大（本格的社会実装）

幅広い産業分野でのIoTシステムと，**中小企業を含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・グローバルな調整

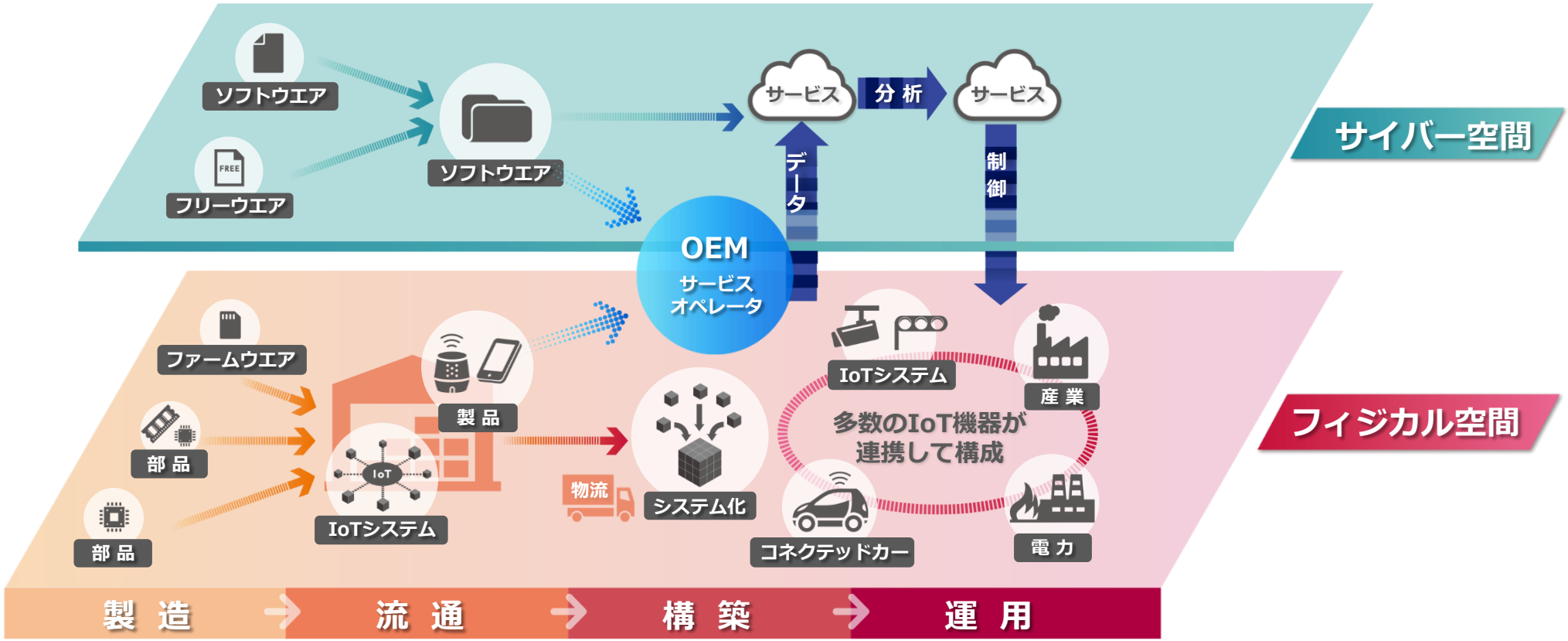
本日ご紹介する研究開発状況

SIP第2期
2018～2022

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



A　信頼の創出・証明：信頼の基点

SIP第2期
2018～2022

A
信頼の創出・証明

SCU（セキュア暗号ユニット　Secure Cryptographic Unit）

IoT機器内のICチップに搭載する“軽く、速く、強い”信頼の基点となるユニット

データの暗号化・復号、デジタル署名生成・検証、ストレージ、通信データ・プログラムの保護、システムのセキュアブート等、暗号技術が必要なほとんどの用途に活用できる。

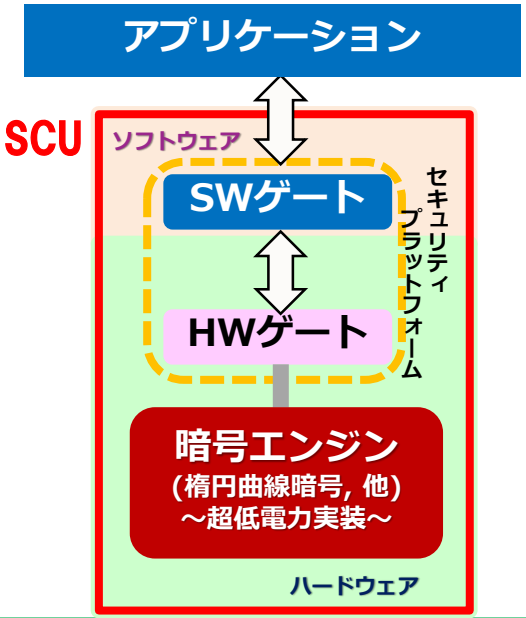
■ **ハードウェア暗号エンジン**

256ビットの楕円曲線暗号の処理につき
- 末端ノード向け：1ミリワット級の超低電力および十キロゲート級の小面積・低コストを達成
- 中間ノード向け：10,000回/秒以上の超高速動作を達成

物理乱数生成器、共通鍵暗号等も実装

■ **セキュリティプラットフォーム（ソフトウェアゲート＆ハードウェアゲート）**

仮にアプリケーションが改竄され、暗号エンジンへの不正アクセスを試みたとしても、ソフトウェアゲート（SWゲート）とハードウェアゲート（HWゲート）から構成されるセキュリティプラットフォームが不正アクセスを検出し阻止する。

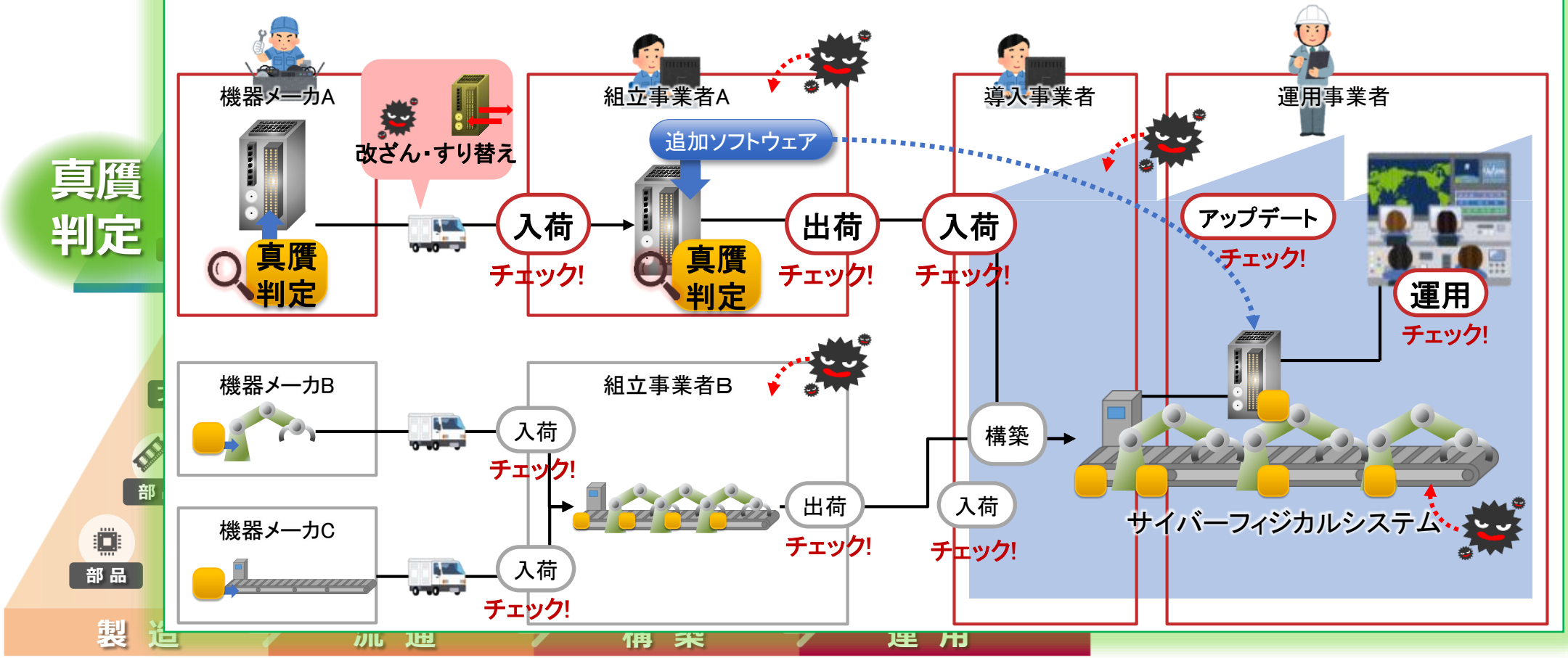


A　信頼の創出・証明：真贋判定

SIP第2期
2018～2022

A
信頼の創出・証明

サプライチェーンの各事業者が手軽に機器の完全性を確認できる技術

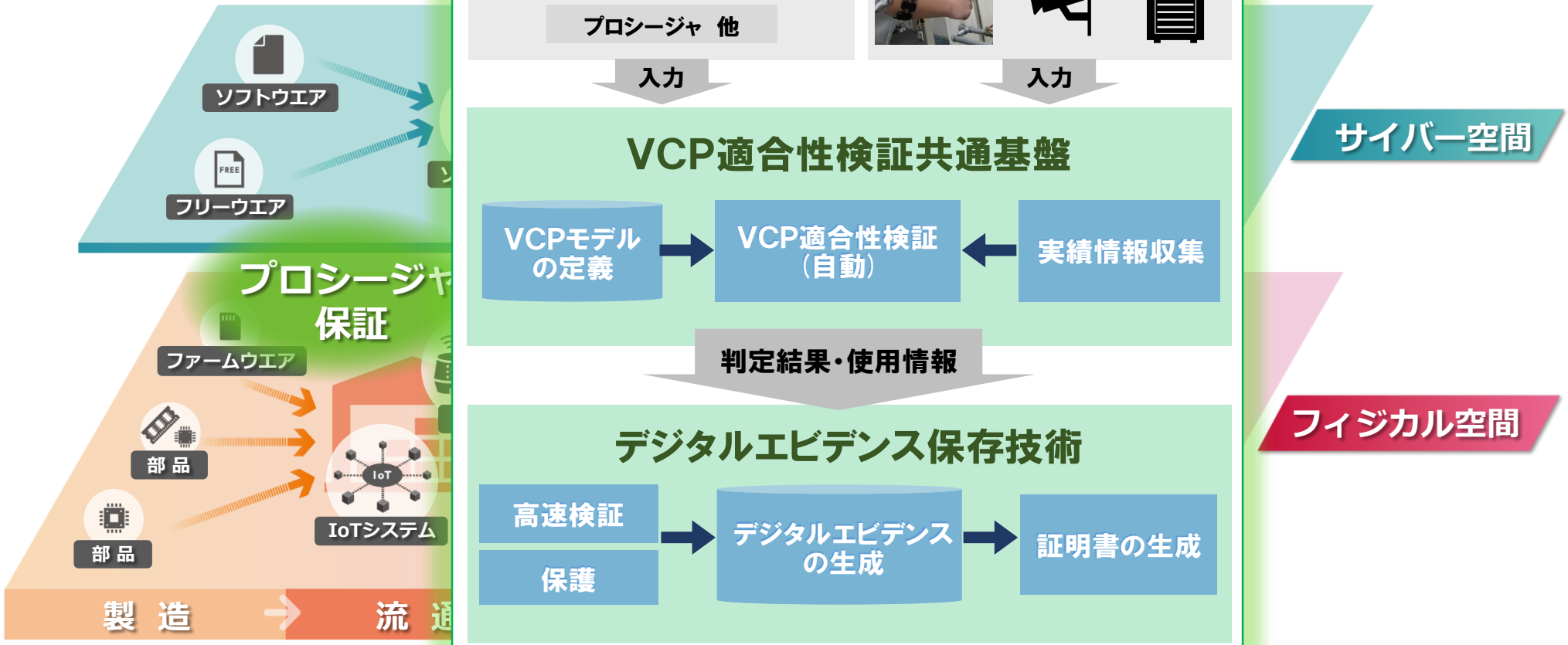


A　信頼の創出・証明：プロシージャ保証

SIP第2期
2018～2022

A
信頼の創出・証明

VCP：価値創造プロセス
Value Creation Process



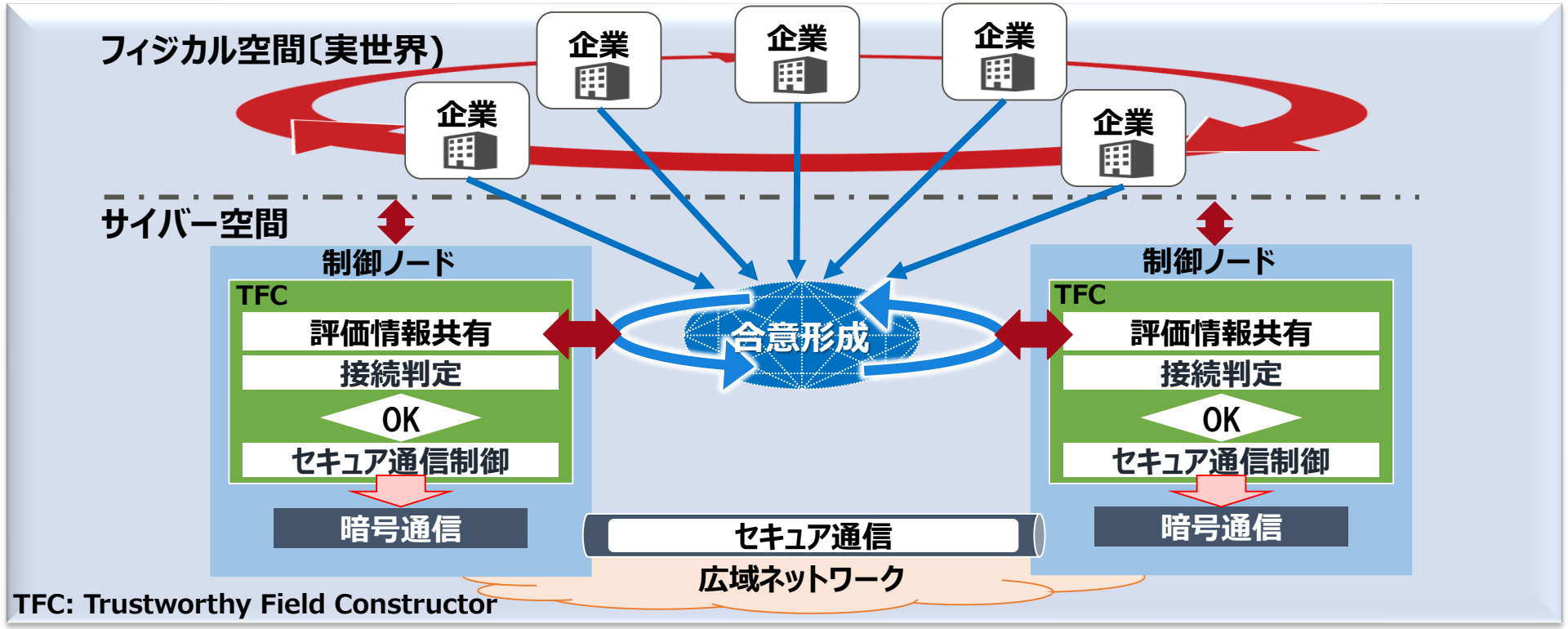
B　信頼チェーンの構築・流通

SIP第2期
2018～2022

B
信頼チェーンの構築・流通

サイバー空間上の合意形成に基く安心・安全なデータ流通機構

各参加企業が起点となり、参加企業全体で合意形成し、動的に「信用できる場」を形成



ー空間

ル空間

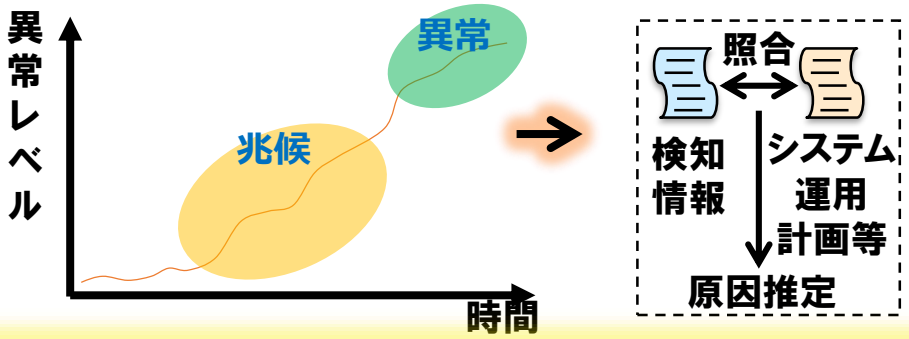
C　信頼チェーンの検証・維持

SIP第2期
2018～2022

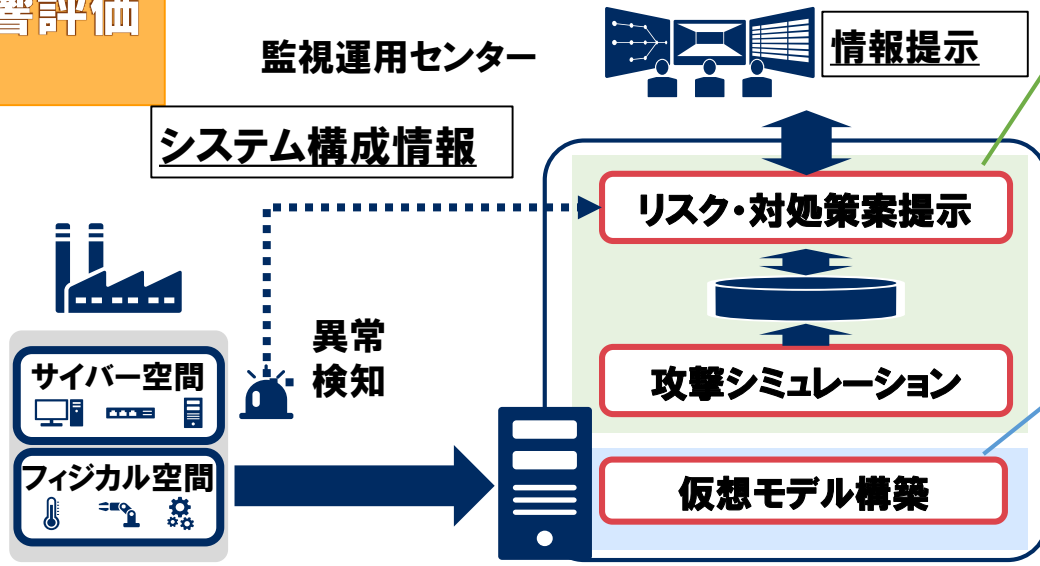
即時の検知・原因推定

即時監視技術

即時異常検知技術・原因推定技術



発生時の影響評価と対処



■ **対処策実行支援技術**
仮想モデル上での攻撃シミュレーションに基づき、対処策を提示

■ **仮想モデル構築技術**
実システムを用いずにサイバー攻撃リスクを分析するための仮想モデルを構築

頼チェーンの検証・維持

インシデント検知と対処

サイバー空間

フィジカル空間

サイバー・フィジカル・セキュリティの実証の取組み

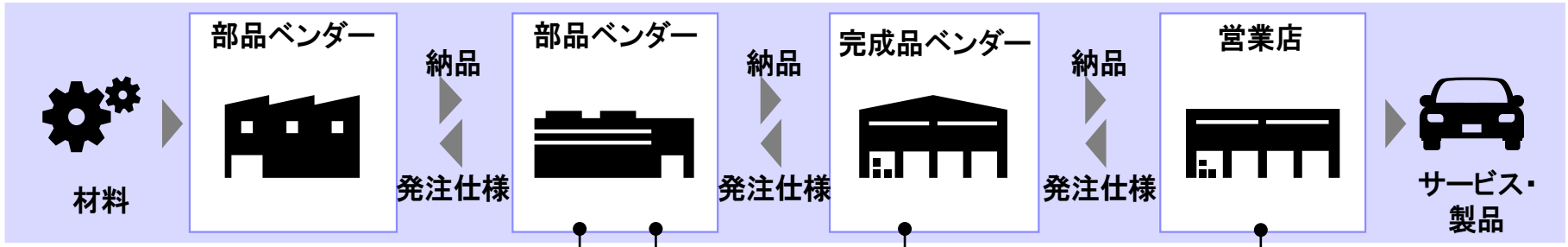
SIP第2期
2018～2022

A 信頼の創出・証明

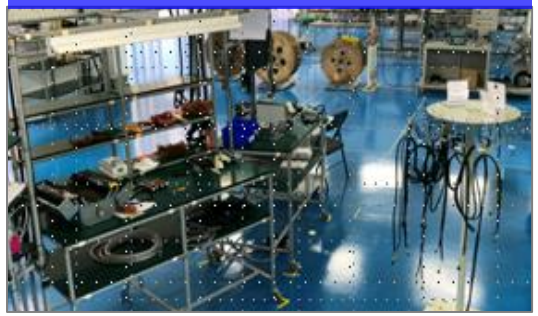
B 信頼チェーンの構築・流通

C 信頼チェーンの検証・維持

サプライチェーン全体の信頼を確認できる世界

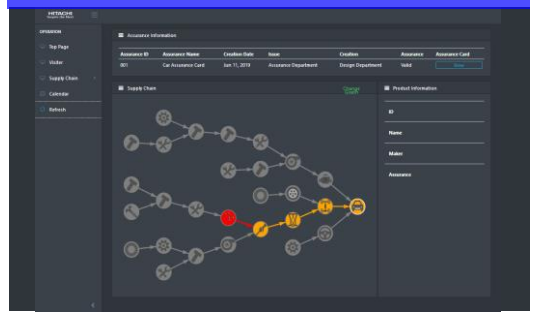


生産支援システム



製品管理システム

営業店支援システム



ー空間

ン空間

製 造 → 流 通 → 構 築 → 運 用

プロジェクト推進のためのワーキンググループ

SIP第2期
2018～2022

実証評価WG： 実証実験から社会実装へ

- 実証実験において実用性や実効性を効果測定する手法の調査・検討と，国内外の技術ベンチマーキング
- 他SIP，他国プロ等との連携した実証実験の検討

成果普及WG： 普及のための方策

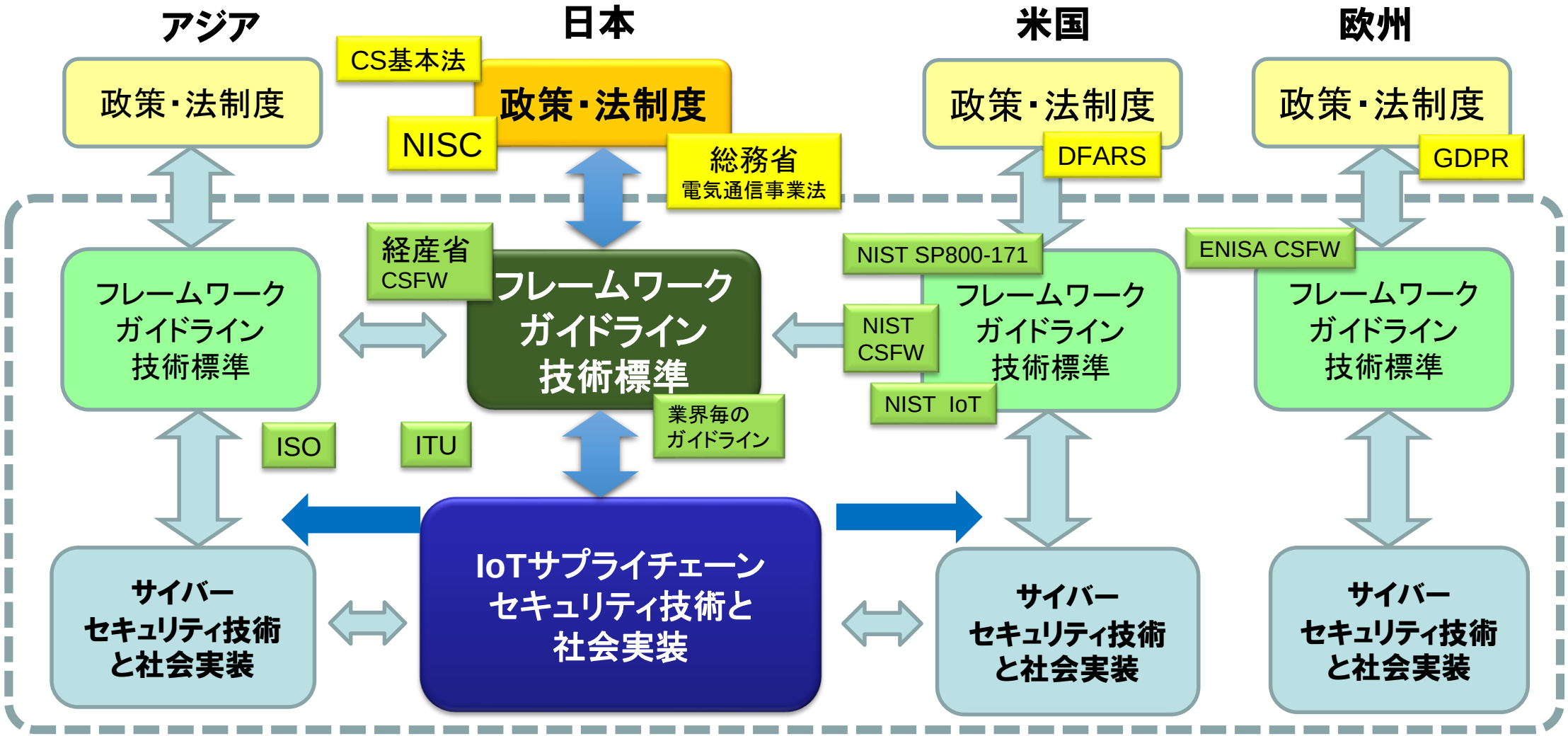
- 参画企業による事業化（製品化）と各産業分野への導入の推進
- 共用検証センター等，中小企業などが成果を活用し易い環境作りの検討
- シンポジウム企画・開催や海外イベント出展などによる本取り組みの国内外発信

海外動向調査WG： グローバル連携策

- 各テーマで実施する国内内外の関連動向調査状況の集約・共有
- 国際連携活動として米国NIST，欧州ENISA等への積極的な提言活動

グローバルな協調と競争

SIP第2期
2018～2022



NISC: National center of Incident readiness and Strategy for Cybersecurity

NIST: National Institute of Standards and Technology
ENISA: European Union Agency for Network and Information Security

IoT社会に対応したサイバー・フィジカル・セキュリティ

SIP第2期
2018～2022

本日のシンポジウムへの ご参加ありがとうございます

PD　後藤厚宏